PCI DSS v4.0.1

Penetration Testing Requirements

A technical reference for security teams and IT leaders navigating PCI DSS v4.0.1 penetration testing, scoping, and compliance obligations.

Contents

Compliance Status

All 64 new or updated requirements introduced in PCI DSS v4.0.1 are now fully mandatory, including all 51 previously future-dated controls. No grace period remains. PCI DSS v4.0.1 is the sole active version; all assessments must reference v4.0.1 documentation.

v3.2.1 retired: March 31, 2024. v4.0 retired: December 31, 2024.

01 At a Glance

REQUIREMENTS SUMMARY

SCOPE	FREQUENCY	WHAT'S REQUIRED
All systems storing, processing, or transmitting cardholder data - servers, databases, APIs, network devices, and any component with indirect CDE access.	Annual minimum, and after every significant change to infrastructure, applications, or network segmentation.	External network pentest | Internal network pentest | Segmentation testing | Authenticated application testing | Retesting after remediation

Scanning is not Pentesting

Requirement 11.3 (automated scanning) and Requirement 11.4 (penetration testing) are separate, independent obligations. Automated scans identify known CVEs from signature databases. Penetration testing actively exploits vulnerabilities, chains findings, and uncovers logic flaws and access control failures that scanners cannot detect. A clean ASV scan report does not satisfy Req. 11.4. QSA auditors verify both independently.

02 PCI Compliance Levels

PENTEST OBLIGATIONS BY TRANSACTION VOLUME

PCI DSS compliance level is determined by annual transaction volume. Penetration testing requirements under Req. 11.4 are scope-driven, not level-driven - but compliance level determines assessment format (ROC vs. SAQ) and how testing is validated and enforced.

Level 1

CRITERIA	>6M transactions/year or card-brand designated
VALIDATION	Annual on-site QSA-led Report on Compliance (ROC).
PENTEST	Mandatory - full Req. 11.4 enforcement. Annual external and internal pentests, segmentation validation, retesting after significant changes. All results reviewed during on-site audit.

Level 2

CRITERIA	1M-6M transactions/year
VALIDATION	SAQ D or ROC if required by acquiring bank.
PENTEST	Required. SAQ D mandates full Req. 11.4 compliance - same obligations as Level 1. Less enforcement oversight, but liability rests entirely with the merchant.

Level 3

CRITERIA	20K-1M e-commerce transactions/year
VALIDATION	Typically SAQ D or SAQ A-EP.
PENTEST	SAQ D: full Req. 11.4 testing required. SAQ A-EP: external testing required for components affecting payment page behavior; reduced scope versus SAQ D.

Level 4

CRITERIA	<20K e-commerce OR up to 1M non-e-commerce transactions/year
VALIDATION	SAQ A / B / B-IP / C / C-VT, or SAQ D.
PENTEST	Only required if using SAQ D or SAQ A-EP. Other SAQs require quarterly vulnerability scans only.

Summary by Level

LEVEL	PENTEST REQUIRED?	TRIGGERING FORM	NOTES
Level 1	Yes	ROC (QSA-led)	Full Req. 11.4 enforcement
Level 2	Yes	SAQ D or ROC	Same obligations as Level 1
Level 3	Depends	SAQ D or A-EP	A-EP = limited scope; D = full
Level 4	Often not	SAQ A/B/C or D	Only SAQ D or A-EP trigger pentests

Common Misconception

Merchants at Levels 2-4 frequently assume pentesting is optional if no QSA shows up. If your SAQ type includes Req. 11.4 controls, the obligation is real and you are liable. Acquiring banks and card brands can elevate your level or require stricter validation at any time.

03

SAQ Types

A-EP VS. D - SCOPE AND PENTEST IMPLICATIONS

SAQ A-EP - E-commerce, Redirected Payment

For e-commerce merchants that do not directly receive cardholder data but whose website can affect the security of the payment transaction - for example, by loading third-party scripts or iframes on the checkout page.

- Cardholder data does not transit merchant servers, but the environment is in scope due to payment page influence.
- Approximately 140 applicable PCI DSS controls.
- Quarterly ASV vulnerability scans required.
- Penetration testing required for components that can affect payment page behavior.
- Requirements 6.4.3 and 11.6.1 apply: script inventory, integrity checks, and weekly tamper-detection review.

COMMON EXAMPLES

- You use Stripe or PayPal but your site hosts the payment page or loads scripts that interact with it.
- The cardholder is redirected to a third-party site to enter payment details, but your website loads content - scripts or iframes - that could be exploited to skim data.

SAQ D - High-Risk and Complex Environments

Applies to merchants that store, process, or transmit cardholder data on systems they control; all service providers; and e-commerce merchants that fully host their own payment pages.

- Approximately 300+ applicable PCI DSS controls - full standard in scope.
- Internal and external penetration testing required under Req. 11.4.
- Full system hardening, segmentation, logging, access control, and encryption obligations.
- SaaS providers whose platforms are used by merchants to process card transactions are service providers - your entire application is in scope for Req. 11.4 regardless of your customers' own assessments.

COMMON EXAMPLES

- You process credit cards directly through your servers or application backend.
- You store any PAN (Primary Account Number), encrypted or not.
- You are a SaaS provider offering services that handle or process cardholder data for your clients.

FEATURE	SAQ A-EP	SAQ D
Cardholder data stored	No	Yes or potentially yes

Cardholder data processed	No	Yes
Payment page hosted by merchant	Yes (affects page / loads scripts)	Yes or full environment
Applies to e-commerce only?	Yes	No - all merchant types
Number of controls	~140+	~300+
Penetration testing required?	Yes (relevant systems)	Yes - full Req. 11.4
Req. 6.4.3 / 11.6.1 apply?	Yes	Yes
Best for	E-commerce using a third-party processor where your site still loads payment scripts or hosts the payment page.	Merchants or service providers handling cardholder data directly, or SaaS platforms processing payments on behalf of clients.

04 Vulnerability Scanning

REQUIREMENT 11.3

Requirement 11.3 governs automated vulnerability scanning. It is a distinct and separate obligation from penetration testing (Req. 11.4). Both are mandatory; neither substitutes for the other.

11.3.1 - External Vulnerability Scans

FREQUENCY	Quarterly + after any significant environment change.
PERFORMED BY	Approved Scanning Vendor (ASV) only - must appear on the PCI SSC ASV list.
SCOPE	All internet-facing CDE systems. No High-severity findings permitted. Passing ASV report required before assessment closes.

11.3.2 - Internal Vulnerability Scans

FREQUENCY	Quarterly + after any significant environment change.
PERFORMED BY	Qualified internal staff or a third-party provider.
SCOPE	All in-scope internal systems. Authenticated scanning required per Req. 11.3.3 unless formally documented otherwise.

11.3.3 - Authenticated Scanning

APPLIES TO	All internal scans under Req. 11.3.2.
REQUIREMENT	Scanners must authenticate to target systems. Unauthenticated internal scans do not satisfy Req. 11.3.2 without documented justification. This is a standing requirement.

11.3.4 - Risk Ranking

FREQUENCY	Applied to every scan cycle.
REQUIREMENT	Each finding must be assigned a risk rank (High / Medium / Low) based on business impact. The risk-ranking methodology must be documented and consistently applied.

11.3.5 - Remediation and Re-scanning

FREQUENCY	As needed after each scan cycle.
REQUIREMENT	Vulnerabilities must be remediated and re-scanned to confirm resolution within the same quarter or before assessment closure for High findings.

05 Penetration Testing

REQUIREMENT 11.4 - ALL SUB-REQUIREMENTS MANDATORY

Req. 11.4 mandates active exploitation testing across all systems in the CDE. All sub-requirements are currently mandatory with no exceptions.

11.4.1 - External Penetration Test

- Annual minimum and after every significant change to the external attack surface.
- Covers all internet-facing assets: networks, servers, web applications, APIs, exposed management interfaces.
- Must use a recognized methodology: NIST SP 800-115, OWASP, PTES, or OSSTMM.
- Must be conducted by a qualified, independent tester - not the team that manages the tested environment.

11.4.2 - Internal Penetration Test

- Annual minimum and after every significant change to internal infrastructure.
- Covers internal systems within the CDE and the adjacent internal corporate network.
- Identifies vulnerabilities exploitable by malicious insiders or post-perimeter attackers.
- Must produce evidence of exploitation attempts, not only a vulnerability inventory.

11.4.3 - Remediation and Retesting

- All discovered vulnerabilities must be remediated according to risk priority.
- A retest must confirm successful remediation before the requirement is satisfied.
- QSA auditors may require granular timestamps: discovery date, remediation date, retest date.

11.4.4 - Segmentation Testing

- If network segmentation is used to reduce PCI scope, segmentation controls must be explicitly tested.
- Confirms no traffic path exists between out-of-scope systems and the CDE.
- Minimum twice per year and after any change to segmentation architecture.
- A failed segmentation test directly expands PCI DSS scope and can invalidate an entire assessment.

11.4.5 - Multi-tenant Segmentation (Service Providers)

- If infrastructure is shared across multiple customers, segmentation between customer environments must be tested annually and after changes.
- Applies to multi-tenant SaaS platforms, managed hosting providers, and shared infrastructure vendors.

> **Change-Triggered Retesting - Most Commonly Missed**
>
> A significant change to any in-scope system triggers a new pentest or targeted retest before that change reaches production. Examples: new auth flows, added payment processors, API version upgrades, infrastructure migration, CDN changes, new third-party scripts on payment pages.

PTaaS - Penetration Testing as a Service

The change-triggered retest requirement is the strongest operational argument for a PTaaS model. Traditional annual pentests work well for baseline compliance, but they create a coverage gap every time engineering ships a significant change between assessment cycles.

WHAT PTAAS ENABLES

- On-demand retesting capacity without initiating a full new engagement each time a change ships.
- Biannual or quarterly testing cadences that align with faster release cycles.
- Segmentation retesting after infrastructure changes - satisfying the twice-yearly Req. 11.4.4 obligation without scheduling a separate engagement.
- A continuous evidence trail for QSA auditors, replacing the single annual snapshot with documented testing across the full compliance period.

06

Authenticated Web App Testing

REQ. 11.4 - APPLICATION LAYER

Application-layer testing is required under Req. 11.4 for any web application or API that stores, processes, or transmits cardholder data, or that can affect the security of the payment environment. Unauthenticated surface testing does not satisfy this requirement.

Coverage Areas for Authenticated Testing

TEST AREA	WHAT GETS TESTED	PCI RELEVANCE
Auth and Session Management	Login flows, MFA bypass, session fixation, token expiry, password policy.	Weak auth is the most common initial CDE access vector.
Authorization and Access Control	Horizontal escalation, vertical escalation, IDOR.	Access control failures directly violate Req. 7.
Payment Page and Form Handling	Input validation, SQLi, XSS, form tampering, PAN/CVV leakage in logs.	Any flaw exposing raw cardholder data is a critical PCI finding.
API Security	Auth on all endpoints, rate limiting, mass assignment, IDOR, overly permissive responses.	APIs are the primary attack surface for card data theft in SaaS.
Business Logic Flaws	Price manipulation, checkout bypass, coupon abuse, transaction replay.	Invisible to automated scanners; frequently exploited in e-commerce breaches.
Third-Party Integrations	Script injection via CDN, insecure iframe handling, payment SDK misconfiguration.	Critical for SAQ A-EP - any page loading third-party scripts is in scope.

Testing Approach Comparison

APPROACH	COVERAGE	MEETS REQ. 11.4?	BEST FOR
Unauthenticated (Black Box)	Public surface only - login page, exposed endpoints.	Not on its own	Initial recon only
Authenticated (Grey Box)	Full app functionality for all logged-in roles.	Yes - required	Standard PCI web app pentest
Authenticated + Source Code (White Box)	Code-level review combined with active exploitation.	Yes - exceeds minimum	Apps that directly store PANs

SaaS Providers: Scope Note

If your platform is used by merchants to process card transactions, you are a service provider under PCI DSS. Your application is in scope for Req. 11.4 regardless of whether your customers are completing their own separate assessments. The pentest must cover the full authenticated surface: all customer-facing functionality, admin interfaces, and API layers that touch payment flows.

07

ROC vs. SAQ

ASSESSMENT FORMAT BY COMPLIANCE LEVEL

The Report on Compliance (ROC) is the formal output of a QSA-led on-site assessment. The Self-Assessment Questionnaire (SAQ) is completed by the merchant for lower-volume entities. Both require the same underlying security controls - they differ only in how compliance is validated.

ROC Requirement Thresholds

ENTITY TYPE	ROC REQUIRED?
Merchants - Level 1 (>6M transactions/year)	Yes, required annually
Service Providers - Level 1 (>300K transactions/year or high-risk)	Yes, required annually
Merchants - Levels 2-4	No - SAQ permitted unless acquirer or card brand mandates ROC

ROC vs. SAQ - Key Differences

FEATURE	ROC	SAQ
Who completes it	QSA or certified internal auditor	Merchant or service provider
Assessment depth	Comprehensive - all controls with documented evidence	Questionnaire - yes/no responses
Evidence requirement	Documented proof for every tested control	Less evidence required
Pentest validation	Results reviewed by QSA during on-site audit	Merchant self-attests; no QSA review

Who requires it	Card brands and acquiring banks (Level 1)	All other merchants (Levels 2-4)

What QSAs Examine in a ROC

Executive summary: business context, CDE scope, and cardholder data flows. Detailed testing results for all 12 PCI DSS requirements and every sub-control. Compensating controls documentation where applicable. Appendices: network diagrams, data flow diagrams, segmentation test results, pentest findings.

08 On-Site vs. Remote Assessments

QSA ASSESSMENT LOGISTICS

The PCI SSC requires QSAs to conduct on-site assessments as the default for PCI DSS validation. Remote assessment is permitted only under specific, documented circumstances.

ON-SITE: THE DEFAULT

QSA must be physically present at client premises.

Required for 'observe' procedures: physical access controls, secure media storage, hardware inspection.

Physical control verification cannot be replicated remotely without material reduction in assurance quality.

REMOTE: EXCEPTIONAL CASES ONLY

PCI SSC Remote Assessment Guidelines permit limited remote testing: document review, interviews, screen shares, video walkthroughs.

Applicable only when travel is genuinely impractical: remote-only staff, inaccessible data centers, legal restrictions.

Requires formal feasibility analysis and written justification included in the ROC. Each remotely-tested control must document method, objective, and rationale.

Hybrid Models Are Acceptable

On-site presence for physical controls combined with remote documentation review and interviews is acceptable when justified. Always confirm allowances with your acquiring bank or card brand before pursuing remote or hybrid formats - card brands may impose stricter requirements than the PCI SSC baseline.

09

IT Leader Action Checklist

ALL REQUIREMENTS CURRENTLY MANDATORY

Scoping and Inventory

- Define and document your CDE boundary
- Document all third-party service providers and their PCI DSS compliance status (Req. 12.8)
- Inventory all third-party scripts on payment pages (Req. 6.4.3)
- Assess whether network segmentation is in use and schedule twice-annual segmentation tests

Access Control and Authentication

- Enforce MFA for all access to the CDE, not only administrator accounts (Req. 8.3.1)
- Audit all service accounts with CDE access - disable unused accounts and rotate credentials
- Deploy phishing-resistant authentication (FIDO2/WebAuthn) where applicable (Req. 8.3.10.1)
- Enforce minimum 12-character passwords with complexity requirements

Vulnerability Management

- Schedule quarterly external ASV scans - confirm vendor is on the PCI SSC ASV list
- Document your risk-ranking methodology for scan findings (High / Medium / Low)
- Configure internal scans to use authenticated scanning for all applicable systems (Req. 11.3.3)
- Ensure rescan and remediation close within the same quarter for all High-severity findings

Penetration Testing

- Commission annual external and internal penetration tests against the full CDE scope
- Schedule authenticated web application testing for all in-scope applications
- Confirm tester independence - cannot be the team that built or manages the tested environment
- Establish a change-triggered retest process before any significant change reaches production
- Document methodology used: NIST SP 800-115, OWASP, PTES, or equivalent
- Retain pentest reports with full timestamps (discovery, remediation, retest) for QSA review

Payment Page Security (E-commerce)

- Implement script inventory and authorization for all payment page scripts (Req. 6.4.3)
- Confirm third-party processor manages all payment page security if using SAQ A-EP
- Deploy tamper-detection mechanism reviewed weekly for payment page changes (Req. 11.6.1)

Continuous Compliance

- Shift from annual compliance sprints to continuous, year-round evidence collection
- Train all staff on phishing, social engineering, and PCI DSS obligations annually
- Perform Targeted Risk Analysis (TRA) to define security control frequencies
- Confirm all third-party service providers complete their own annual PCI DSS assessments

10 Resources and Further Reading

AUTHORITATIVE SOURCES

PCI Security Standards Council	pcisecuritystandards.org

Primary source for PCI DSS v4.0.1 documentation, official FAQs, ASV list, and QSA directory.

PCI DSS v4.0.1 - Summary of Changes	pcisecuritystandards.org/document_library

Authoritative changelog covering v3.2.1 to v4.0 and v4.0 to v4.0.1. Required reading for teams transitioning from prior versions.

NIST SP 800-115 - Technical Guide to Pentesting	csrc.nist.gov

The methodology standard explicitly cited in PCI DSS. Defines what constitutes a technically sufficient penetration test.

Verizon Payment Security Report	verizon.com/business

Annual third-party data on compliance rates, common control failures, and breach trends across card data environments.

Software Secured: PCI DSS v4.0.1 Pentesting Guide	softwaresecured.com

Req. 11.4 scoping, SAQ type implications, and pentest delivery for SaaS and e-commerce merchants.

Software Secured: Pentesting for Compliance	softwaresecured.com

PCI levels, SAQ types, ROC vs. SAQ distinctions, and structuring a compliant engagement from scoping through remediation.