Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/insights/businesses-dealing-with-pci-falling-short-on-regular-vulnerability-scans-and-pen-testing/

PCI DSS COMPLIANCE TESTING

PCI DSS 4.0.1 Penetration Testing and Segmentation Validation

PCI DSS Requirement 11.4 calls for manual penetration testing and segmentation validation alongside the quarterly scans, and the assessor checks each on its own cadence. Confirm what was tested, when and how before the assessor asks. Call (800) 868-8189 at any hour.

Published March 30, 2015 · Updated October 30, 2026

Primary Reference for This Guide

Start with PCI Security Standards Council document library.

By Robert Knudsen, Computer forensics and cybersecurity examiner, Global Digital Forensics

Why PCI DSS Penetration Testing Mandates Call for Manual Testing

Merchants, e commerce platforms, hospitality groups and payment processors subject to the Payment Card Industry Data Security Standard v4.0.1 are well served by separating quarterly automated vulnerability scanning under Requirement 11.3 from the annual and post change manual penetration testing mandated under Requirement 11.4. Under PCI DSS 4.0.1, organizations perform comprehensive application layer and network layer manual penetration testing of the Cardholder Data Environment and also validate every segmentation control separating the CDE from the broader corporate network at least annually, and every six months for service providers.

Thorough Manual Testing and Segmentation Validation With Verification Retesting

Global Digital Forensics partners with compliance officers, internal auditors and security engineers to execute PCI DSS 4.0.1 compliant manual penetration testing and segmentation validation engagements. Our certified testers evaluate payment web applications, API payment gateways, point of sale networks and CDE firewall boundaries using rigorous industry methodologies. When our engineers uncover a segmentation gap or application flaw, we provide clear remediation guidance and perform verification retesting once your team applies the fix, delivering an audit ready attestation package for your Qualified Security Assessor.

© 2026 Global Digital Forensics, Inc. All rights reserved.

What Requirement 11.4 Requires of a Merchant or Service Provider

Scanning and penetration testing both produce a report with findings, and the standard treats them as different controls with different cadences. Requirement 11.3 governs vulnerability scanning, internal and external, on a quarterly basis and after significant changes, with external scans performed by an Approved Scanning Vendor. Requirement 11.4 governs penetration testing, and its sub requirements are specific. The entity must define and follow a documented penetration testing methodology that covers the whole cardholder data environment perimeter and critical systems, tests from inside and outside the network, includes application layer and network layer testing, reviews threats and vulnerabilities seen in the prior twelve months and retains results and remediation records. Internal and external penetration tests are performed at least once every twelve months and after any significant infrastructure or application change, and exploitable vulnerabilities found are corrected and retested. The current standard and its supporting documents are published in the PCI Security Standards Council document library.

Segmentation carries its own requirement. Where segmentation is used to isolate the cardholder data environment from other networks, penetration testing on the segmentation controls is performed at least once every twelve months and after any change to the segmentation controls or methods, and it must confirm that the controls are operational and effective and isolate all out of scope systems from systems in scope. Service providers test segmentation at least once every six months and after changes. Multi tenant service providers have a further obligation to support their customers' external penetration testing. These are the cadences an assessor will check against dates, and the reason we tell compliance officers that the penetration test and the segmentation validation each carry their own dated record, separate from a scan vendor's quarterly PDF. The penetration testing service page describes how our engagements map to each sub requirement.

How a PCI Penetration Test Runs From Scope to Report

Scoping decides whether the test will count, so it is the longest conversation. We begin with the entity's own cardholder data environment definition: the systems that store, process or transmit cardholder data, the systems connected to them and the systems that could affect their security. From the network diagrams and data flow diagrams we identify every segmentation boundary, every path from the corporate network or the internet into the environment, and every application that handles card data, including payment pages, APIs and point of sale back ends. The rules of engagement then fix the test windows, the production versus staging question, the credentials and roles to be tested and the escalation contacts. The test covers the cardholder data environment as it runs in production, with the internal segment and the external perimeter tested together, and scoping confirms that coverage.

Testing proceeds from outside and inside. External work covers the internet facing perimeter and applications. Internal work starts from a position on the corporate network and attempts to reach the cardholder data environment across each segmentation control, then tests the systems inside it at the network and application layers. Every finding is confirmed by exploitation where it is safe to do so, with evidence captured, and rated against the methodology. After the entity remediates, we retest each exploitable finding and record the result. The deliverable is a report organized the way a Qualified Security Assessor reads it: methodology, scope with the systems and boundaries tested, dates, findings with evidence, remediation and retest results, and an attestation of the segmentation testing. The assessor can tie each element directly to its sub requirement, which is what keeps an assessment on schedule.

© 2026 Global Digital Forensics, Inc. All rights reserved.

The methodology document deserves its own attention because assessors ask for it before they ask for the report. The standard expects the entity to define and follow a methodology that is based on industry accepted approaches, covers the entire perimeter and the critical systems, includes testing from inside and outside the network, addresses the application and network layers, considers the threats and vulnerabilities experienced in the prior twelve months and specifies how results and remediation activities are retained. We provide a methodology the entity can adopt as its own, aligned to the sub requirements and to the testing we actually perform, so that the document, the engagement and the report tell one consistent story when the assessor compares them. An entity that owns its methodology also controls scope changes rather than inheriting them from whichever vendor tested last.

Scoping and Cadence Practices That Carry an Assessment

The first practice is scoping each test to the segmentation controls and the internal cardholder data environment as well as the external IP range, so every annual report covers the whole requirement. The second is treating every significant change as significant: a firewall replacement, a new payment gateway, a migration of the point of sale back end to a cloud provider or a network expansion that connects the corporate wireless to the card environment. Each of those triggers a new test and a new segmentation validation, and assessors look for them in the change records. The third is documenting the retest. A report that pairs each exploitable finding with evidence of remediation and retesting documents the retest the standard requires.

Timing carries equal weight. Each test is scheduled within twelve months of the previous one, and a service provider validates segmentation every six months, so the calendar itself is part of the evidence. The methodology document is kept as the entity's own record, separate from the tester's report, because the standard expects the entity to define and own it. The penetration test and the vulnerability scan feed each other: the methodology considers the vulnerabilities seen in the prior year, so the scan results go to the testers. Our audit preparation packages list the diagrams, change records and prior reports to assemble before a test, and a vulnerability assessment ahead of the penetration test removes the noise so the manual effort goes where it matters.

Preserving the Record for a Card Data Breach Review

A card data breach brings the card brands, the acquiring bank and often a mandated forensic review, and the first hours shape the record that review works from. Point of sale systems, payment servers and the segmentation firewalls hold logs that roll over quickly, and memory on a compromised payment server may hold the scraper and the card data it collected. The first steps are to isolate the affected systems, keeping them powered on where possible, capture volatile memory, image the disks and export the firewall, VPN, authentication and application logs with their timestamps intact, and then rebuild. The merchant's own staff and its managed service provider focus on isolation and preservation under the direction of counsel, and remediation follows once the record is fixed, which preserves the sources a later review reads for how the attacker got in and how long the exposure lasted.

Our data breach analysis engagements reconstruct the intrusion path, the dwell time, the systems touched and the data exposed from that preserved record, and report the findings to counsel for the brand and bank obligations and for state notification statutes. The approach follows NIST SP 800-61 Revision 3 and the forensic process in NIST SP 800-86, and the report states what the record shows, which log sources were

© 2026 Global Digital Forensics, Inc. All rights reserved.

available for each period, and how the attacker's path relates to the segmentation controls. That last point matters, because the same report frequently becomes the basis for the remediation plan and for the next penetration test's scope, and an entity that treats the breach review and the testing program as one continuous record is far better placed with its assessor and its acquirer.

Schedule Your PCI DSS 4.0.1 Penetration Test and Segmentation Audit

Start with our audit and legal preparation packages, or call Global Digital Forensics at (800) 868-8189 to scope your PCI DSS testing engagement. The initial consultation is free.

Requirement 11 Scanning Against Penetration Testing

The guide explains that PCI DSS treats scanning and penetration testing as different controls with different cadences, and this table keeps them distinct. This table separates Requirement 11.3 from 11.4 and the segmentation obligation across what each requires, who performs it and how often, so a compliance officer can check the program against the dates an assessor will ask for. Read the cadence column, because service providers validate segmentation every six months while merchants do so annually. The penetration test and the segmentation validation each carry their own dated record alongside the quarterly scan.

PCI DSS Requirement 11 scanning, penetration testing and segmentation validation by requirement, performer and cadence.

Control	What it requires	Cadence
Requirement 11.3 external scans	Scans by an Approved Scanning Vendor	Quarterly and after significant change
Requirement 11.3 internal scans	Internal vulnerability scanning	Quarterly and after significant change
Requirement 11.4 penetration test	Inside and outside, application and network layers	At least annually and after significant change
Requirement 11.4 remediation	Exploitable findings corrected and retested	After each test
Segmentation validation, merchants	Confirm the environment is isolated from out of scope systems	At least annually and after change
Segmentation validation, service providers	The same validation on a tighter clock	At least every six months and after change
Methodology document	A defined, industry based testing methodology	Defined and owned by the entity

The massive financial fraud case study describes mapping how a third party processor collected and transmitted transaction data, the kind of payment data flow understanding a PCI segmentation review depends on.

© 2026 Global Digital Forensics, Inc. All rights reserved.

How to Begin and What Happens on the First Call

Our Penetration Test Readiness: Scope, Schedule and Retest Before Audit sets out the items to secure in the order they expire. Have ready your current cardholder data environment definition, network and data flow diagrams, the date and scope of the last penetration test and segmentation validation, the most recent scan reports, any significant changes since and your assessment date. The examiner asks whether you are a merchant or a service provider, how segmentation is implemented, which payment applications and APIs are in scope, whether production or staging will be tested and who your Qualified Security Assessor is. You then receive a written scope mapping the engagement to each sub requirement of 11.4, the test windows, the retest provision and the timing against your assessment, with a proposal. The initial consultation is free, and the hotline at (800) 868-8189 answers 24/7.

Technical References and Further Reading

Earlier reporting on this subject: Fortune, Why system testing, a critical aspect of data security, is worsening, March 23, 2015.

Authorities cited in this guide: PCI Security Standards Council, Document Library (PCI DSS v4.0.1 and supporting documents). Publishes the current PCI DSS text including Requirement 11.3 scanning and Requirement 11.4 penetration testing and segmentation cadences, version 4.0.1. NIST SP 800-61 Revision 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management. Provides the incident response structure applied when a cardholder data environment is breached, final version published 2025. NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response. Describes the collection, examination, analysis and reporting phases for the post breach review, final version 2006.

FREQUENTLY ASKED

PCI Testing Before the QSA Arrives

Is a vulnerability scan the same as a penetration test under PCI DSS?

They are separate controls. Scanning is Requirement 11.3: automated internal and external scans at least quarterly and after significant changes, with external scans run by an Approved Scanning Vendor. Penetration testing is Requirement 11.4: manual testing under a documented methodology from inside and outside the network, at the network and application layers, at least once every twelve months and after significant changes, with exploitable findings corrected and retested. A scan finds known vulnerabilities by signature. A penetration test attempts to exploit them and chain them to reach cardholder data. Assessors check for both, on their own cadences.

© 2026 Global Digital Forensics, Inc. All rights reserved.

How often does segmentation have to be tested?

At least once every twelve months and after any change to the segmentation controls or methods for most entities, and at least once every six months and after changes for service providers, under the current PCI DSS text published in the Council's document library. The test must confirm the controls are operational and effective and that out of scope systems are isolated from the cardholder data environment. A firewall rule change, a new VLAN that touches the environment or a migration of a payment system is a change that triggers a new test regardless of the calendar.

What counts as a significant change that requires a new test?

The standard leaves the entity to define significant changes in its own methodology, and assessors expect that definition to be reasonable. In practice it includes replacing or reconfiguring firewalls or segmentation devices, adding or moving systems that handle cardholder data, deploying a new payment application or major release, changing the network architecture around the environment, migrating to or between cloud providers and onboarding a new third party connection. We help compliance teams write the definition so that change management flags the events automatically rather than leaving the judgment to whoever notices.

Do we have to test the whole corporate network or only the cardholder data environment?

The penetration test covers the cardholder data environment perimeter and the critical systems inside it, from both outside and inside the network. Segmentation testing then verifies that the rest of the corporate network is in fact isolated, which requires testing from the out of scope segments toward the environment. So the corporate network serves as the starting position for the internal and segmentation testing, and the full test concentrates on the cardholder data environment. For an entity with a flat network, the cardholder data environment spans the whole network, and segmenting first narrows the scope accordingly.

What determines the cost of a PCI penetration test?

The number of systems and applications in and connected to the cardholder data environment, the number of segmentation boundaries to validate, whether payment applications and APIs require authenticated role based testing, how many locations or point of sale networks are involved, whether testing must be performed in restricted maintenance windows and how much remediation and retesting is expected. A small merchant with a hosted payment page and a well segmented network is a short engagement. A service provider with several environments on a six month cadence is a program. We scope it in writing after the free initial consultation.

Web Addresses for the Sources Cited

1. PCI Security Standards Council document library: https://www.pcisecuritystandards.org/document_library/
2. NIST SP 800-61 Revision 3: https://csrc.nist.gov/pubs/sp/800/61/r3/final
3. NIST SP 800-86: https://csrc.nist.gov/pubs/sp/800/86/final
4. Fortune, Why system testing, a critical aspect of data security, is worsening, March 23, 2015: https://fortune.com/2015/03/23/pci-compliance-pentesting/

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed November 3, 2026.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.