Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/penetration-testing-readiness-checklist/

READINESS CHECKLIST

Penetration Test Readiness: Scope, Schedule and Retest Before Audit

An auditor looks for a scoped test, remediated findings and a retest, all completed before the deadline. This checklist is what to assemble before the tester arrives.

Why the Calendar Decides Whether the Test Counts

GDF maps your contractual and regulatory requirements to a defined testing scope, evidence plan and reporting schedule.

The reason readiness matters more than the test itself is that the evidence an auditor accepts has a shape. It begins with a scope statement that explains why the systems tested are the systems the framework cares about, continues through signed rules of engagement and a documented methodology, presents findings with severity and reproduction detail, records remediation and closes with a retest showing each finding's status. A test that starts with the scope defined produces a report that explains its own coverage. A test scheduled with time for remediation and retest closes with a retest record for each finding. Both come from readiness, and the items below are what to assemble before the tester's first day.

The Order of Readiness, From Boundary to Retest

We work with your security, compliance and legal teams to agree on the priorities and deliverables.

With the boundary drawn, the rules of engagement follow: the systems in and out of scope, the test windows, whether production or an identical staging environment is tested, the credentials and roles the tester will use, the techniques permitted and the escalation contacts who can be reached during testing. Then the supporting records are gathered. The last twelve months of findings and threats, which PCI expects the methodology to consider. The vulnerability scan history, internal and external, with rescans after changes. The segmentation controls as configured. Finally, before the test begins, remediation owners and change windows are named for each system in scope, because a finding fixed within the window can be retested within it. Our penetration testing and vulnerability assessment services are delivered as separate records because auditors treat them as separate controls.

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

Who Owns the Scope, the Rules and the Fixes

The compliance officer owns the deadlines and the framework matrix. The CISO or security lead owns the scope and signs the rules of engagement, and where litigation or enforcement exposure exists, the engagement can run under legal direction from the start. Network engineering owns the diagrams and the segmentation configuration and stays available during internal testing. Application owners own the credentials, the test accounts and the staging decision for each application. IT operations owns the remediation calendar and the change windows. The tester owns the methodology, the evidence and the retest record, and works within the scope the organization sets.

Give the people who will try to help a defined role in the plan. A system administrator with a patch to apply during the test routes it through the escalation contact, so the report and the retest baseline describe the same environment. A network engineer who sees the tester approaching a segment leaves the firewall rules as they stand, so the finding reflects the environment the assessor will review. A developer who sees the alerts start checks the rules of engagement before touching a test account, because the test is authorized. The rules of engagement name a single escalation path for exactly these moments, and every change made during the window is recorded so the report and the environment tell one story.

What Auditors Look For in a Completed Test

The first thing an auditor checks is that the test is a test. A vulnerability scan compares observed services against a database of known weaknesses and is valuable as a recurring control, and the penetration test builds on it by checking whether a weakness is exploitable, whether two medium findings chain into a domain compromise and whether the regulated systems are reachable from where an attacker would stand. The second is coverage: production, or a staging environment identical to it, and the internal segment as well as the external perimeter, so the report covers what the requirement covers. The third is the retest. An auditor reads a finding as closed once the tester has confirmed the fix.

The quieter items are documentary. A methodology written down and adopted by the organization as its own lets the entity show it defined and followed one. A scope statement that explains how each listed host relates to the framework's boundary answers the coverage question before it is asked. A segmentation test dated after the most recent network change is what the requirement calls for. And an attestation letter carries the weight of the engagement record behind it. The audit and legal preparation library on this site sets out the records each framework's reviewer expects, so the engagement file can be assembled alongside the test.

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

How GDF Supports Compliance Officers, Internal Auditors and Security Teams

Global Digital Forensics has delivered security testing and forensic examinations since 1992 from sixteen US offices. Our penetration testing engagements begin with scoping against the framework boundaries, a rules of engagement document the organization signs and a methodology the organization can adopt as its own. Testing proceeds from outside and inside, with every finding confirmed by exploitation where it is safe to do so and evidence captured at each step. After remediation we retest each exploitable finding and record the result. The deliverable is organized the way an assessor reads it: methodology, scope with the boundaries tested, dates, findings with evidence, remediation, retest results and a framework matrix that maps each finding and control to the Part 500 section, PCI requirement, SP 800-171 practice or trust services criterion it bears on.

Internal auditors use the matrix to populate their workpapers. The CISO uses the technical appendix to drive remediation. The executive narrative serves leadership and the legal team, and where exposure exists the engagement runs under legal direction so the findings reach the people who need them in the form they need. Our clients include Fortune 1000 companies and AmLaw 100 firms, and our examiners have testified in federal and state courts when a security posture became a litigated question. The initial consultation is free. If the filing date is closer than the time you need for testing, remediation and retest, call (800) 868-8189 and we will build the calendar backward from the deadline with you on the first call.

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

The Checklist at a Glance

The readiness items to assemble before a penetration test, who owns each one, where it lives and how quickly it goes stale.

Item	Who acts	Where it lives	How fast it expires
Framework deadlines	Compliance officer	Part 500 April 15 filing, PCI assessment date, SOC 2 period end	Fixed by the regulator or assessor
Scope and boundary diagram	Security lead with network engineering	Network and data flow diagrams, CDE definition	Stale after any significant change
Rules of engagement	CISO signs with legal review, tester countersigns	Signed engagement file	Renewed for each test window
Prior twelve months of findings and threats	Security operations	Ticketing system and the last report	PCI expects the prior twelve months reviewed
Vulnerability scan cadence	Security operations with the scan vendor	ASV portal and internal scanner	PCI quarterly, with rescans after changes
Segmentation controls	Network engineering	Firewall and access control configurations	PCI annual, every six months for service providers
Remediation owners and change windows	IT operations	Change management calendar	Retest starts once the fixes land
Retest record and attestation	Tester, then compliance files it	Final report, framework matrix, attestation letter	Point in time, stale after the next change

FREQUENTLY ASKED

Scans, Staging and Who Signs

Does our quarterly vulnerability scan satisfy the penetration testing requirement?

The scan and the test are separate controls. PCI DSS treats scanning under Requirement 11.3 and penetration testing under Requirement 11.4 as different controls with different cadences, and other frameworks draw the same line. A scan identifies known weaknesses automatically. A penetration test is a person following a documented methodology to show whether those weaknesses are exploitable and whether regulated systems can be reached. Keep the scans running and schedule the test separately.

How far ahead of the audit should the test start?

Far enough for three things to finish: the test itself, your team's remediation of what it finds and the tester's retest confirming the fixes. Build the calendar backward from the earliest framework deadline you answer to, and allow for the change windows your operations team will need. With the retest complete well before the filing, the record covers the period the auditor reviews.

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

Can we test a staging environment instead of production?

Staging works when it is identical to production in configuration, segmentation and data flows and the assessor accepts that it is. Where the environments differ, the test runs on production so it covers what the requirement covers. The rules of engagement should record the decision and the justification. For segmentation testing in particular, the controls that isolate the cardholder data environment are tested as deployed.

Who should sign the rules of engagement?

The security lead or CISO who owns the scope, with the legal team involved where litigation or enforcement exposure exists, and the tester countersigns. The document names the systems in and out of scope, the windows, the permitted techniques, the escalation contacts and the stop conditions. It is renewed for each test window, and any change during the test is recorded against it.

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

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.