Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/insights/mandated-cybersecurity-compliance-testing/

COMPLIANCE TESTING

Scheduling Mandated Penetration Tests Ahead of Audit Deadlines

Every framework you answer to expects penetration testing and vulnerability assessment on its own clock, and an auditor looks for a methodology driven test, closed findings and a retest record. Schedule the testing, the fixes and the retest as one program now. Call (800) 868-8189 at any hour.

Published October 17, 2019 · Updated October 30, 2026

Primary Reference for This Guide

Start with NIST Cybersecurity Framework 2.0.

By Joseph Caruso, Founder, CEO and CTO, Global Digital Forensics

Why Testing Early in the Year Keeps Audits on Schedule

GDF plans penetration testing and vulnerability assessments around your systems, business requirements and regulatory program. We work with your security team and internal auditors to define the scope, schedule the work and document the findings. Discuss your testing requirements with an expert.

What Each Framework Actually Requires and Where the Clocks Run

The mandates read differently and are satisfied by overlapping work. New York's 23 NYCRR Part 500 requires penetration testing of the covered entity's information systems from both inside and outside the information systems' boundaries at least annually, together with vulnerability assessments at a frequency set by the risk assessment, and it ties the whole program to an annual submission due April 15. PCI DSS version 4.0.1, published through the PCI Security Standards Council document library, requires in Requirement 11 that external and internal penetration testing follow a defined methodology, that segmentation controls isolating the cardholder data environment be tested and that vulnerability scans run on a recurring schedule with rescans after remediation.

We align testing and reporting with your organization’s contracts and assessment criteria. Each finding identifies the affected system, supporting evidence and recommended action. The report gives your security team and internal auditors a common record for the next decision.

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

The Difference Between a Scan, a Penetration Test and Evidence an Auditor Accepts

A vulnerability scan is an automated comparison of observed services and versions against a database of known weaknesses, and it is valuable as a recurring control. Whether a weakness is exploitable, whether an attacker could chain two medium findings into a domain compromise and whether the systems holding regulated data are reachable from an attacker's position are the questions a penetration test answers. A penetration test is a person with a methodology attempting exactly those things, documenting each step with timestamps and screenshots and stopping at the boundaries the rules of engagement set. Auditors know the difference and ask for the tester's methodology, the scope definition and the evidence of manual work. Our penetration testing and vulnerability assessment services are delivered as separate records for that reason.

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 the rules of engagement and the methodology, presents findings with severity ratings and reproduction detail, documents remediation and closes with a retest record showing each finding's status. A letter of attestation summarizing the engagement is often requested by customers and examiners, and it draws its weight from the record behind it. A penetration test records the environment as it stood during the testing window, so we present it as a point in time result and pair it with the recurring scans and change management that carry the posture forward between tests. An organization that plans around that pairing treats the annual test as one part of a continuous program.

Mapping One Engagement to Many Frameworks

The frameworks overlap enough that a single well scoped engagement can satisfy several, provided the scope is the union of what each requires rather than the intersection. For Part 500 that means the covered entity's systems and the paths into them from affiliates. For PCI it means the cardholder data environment, the systems connected to it and the segmentation controls that isolate it, each tested on its own terms. For CMMC it means the enclave where controlled unclassified information lives and the boundary around it. For HIPAA it means the systems that create, receive, maintain or transmit protected health information. We draw those boundaries on one diagram during scoping, and where they overlap the same test serves every framework whose boundary it falls within.

The report is organized so each audience goes straight to its own evidence. A framework matrix maps every finding and every tested control to the Part 500 section, PCI requirement, SP 800-171 practice or trust services criterion it bears on, and the methodology section explains how the scope satisfies each framework's definition of coverage. Internal auditors use the matrix to populate their workpapers. The CISO uses the technical appendix to drive remediation. Leadership uses the executive narrative, and where litigation or enforcement exposure exists, the engagement can run under legal direction from the start. The audit and legal preparation packages on this site set out the records each framework's reviewer expects, with a dedicated NYDFS package for Part 500 entities.

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

Phases of the Annual Testing Program

The program opens with scoping against the framework boundaries described above and a rules of engagement document that fixes the systems, the testing windows, the techniques permitted and the escalation path if something unexpected is found. External testing comes first, covering internet facing services, web applications and remote access, followed by internal testing from the position of a compromised workstation or a contractor's network segment, aimed at the systems that hold regulated data. Where the framework or the risk profile calls for it, application testing of the systems that process the regulated data and social engineering against the people who administer them are added. Findings are reported to the CISO as they are confirmed so remediation starts while testing continues.

The remediation window is scheduled into the program rather than left to chance, with a length that reflects the organization's change management cadence and the likely volume of findings. Retesting follows, confirming each finding's closure with the same evidence standard as the original, and the final report with its framework matrix and attestation letter is delivered before the earliest audit or submission date. Recurring vulnerability scans continue between annual tests on the schedule each framework requires, with rescans after remediation documented in the same record. Organizations that treat the annual test as one event in a continuous program arrive at each audit with evidence already in hand, and those that want board level reporting on the program's results can draw on our executive cyber risk advisory work.

Scope and Timing Decisions That Carry an Audit

Audit results turn on scope and timing. A scope that covers the internal systems holding regulated data as well as the perimeter meets Part 500 and PCI on their own terms. A penetration test report with its methodology answers the auditor's first question, and the scan report sits beside it as the record of the scanning control. Testing scheduled early enough that critical findings are closed before the audit date spares leadership a choice between a qualified result and a certification over open items. A report with full reproduction detail lets the internal team fix and verify each finding. A funded retest documents closure, and prior years' reports kept on file give auditors the trend and remediation history they increasingly ask to see.

Compensating controls deserve the same attention. Frameworks allow organizations to meet a requirement through an alternative measure that is documented and shown to be effective, so we test the compensating control and give the auditor test evidence alongside the assertion. The affiliate boundary is another, and it belongs in scope even when the parent company runs security for the group, which our Part 500 evidence guide addresses in detail. Defense contractors gain from tracing where controlled unclassified information actually flows before a CMMC assessment, so the enclave boundary they describe follows it, and our DFARS and CMMC note covers how that boundary is drawn. Each of these is settled during scoping when the right people are at the table.

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

Preparing for the First Call and What Auditors Receive

Preparation sets how quickly the engagement can be scoped and keeps the budget focused on the testing itself. The CISO or security lead assembles the list of frameworks the organization answers to with the dates of the next audit or submission for each, the current asset inventory and network diagrams, the prior year's testing reports with remediation records and the list of open findings from any audit. Internal audit identifies the evidence format its workpapers require. The compliance lead identifies whether any framework carries enforcement exposure that calls for the engagement to run under legal direction. Where regulated data lives in systems operated by a parent, affiliate or third party, the contracts and access arrangements that govern those systems are gathered so the scope can include them.

What each party receives is settled in scoping and delivered in the final report. The senior governing body and executives receive a narrative that states what was tested, what was found, what was fixed and what remains, in terms that support a certification decision. The CISO and engineering teams receive the technical appendix with reproduction detail and remediation guidance for every finding. Internal auditors receive the framework matrix and the retest record. The report is delivered in the form the engagement's structure requires, and where a regulator later asks how a finding was identified or closed, the same engineers who did the work can answer. Financial services entities can see how this fits their sector in our financial services practice overview.

Unified Compliance Testing That Satisfies Multiple Frameworks in One Engagement

Global Digital Forensics works directly with CISOs and internal auditors to design consolidated annual security testing programs. Rather than paying multiple vendors to test overlapping systems, our senior architects scope a single, rigorous manual penetration testing and vulnerability assessment engagement mapped simultaneously to all of your regulatory frameworks. Start with our audit and legal preparation packages and call (800) 868-8189 today to lock in your testing and retesting window well ahead of your audit deadline. The initial consultation is free.

Testing Cadence by Framework

The guide explains that one well scoped engagement can satisfy several frameworks when the scope is the union of what each requires. This table sets out the testing and submission cadence each framework imposes and the boundary that defines its scope, so a compliance lead can build the calendar backward from the earliest clock. Read the scope column when drawing the one diagram that covers every framework. The cadences are published requirements, and an auditor checks each one against dates.

Testing and submission cadence by framework and the boundary that defines each scope.

Framework	Testing cadence	Scope boundary
23 NYCRR Part 500	Penetration test at least annually, submission by April 15	Covered entity systems and paths from affiliates
PCI DSS v4.0.1	Penetration test annually and after change, scans quarterly	Cardholder data environment and its segmentation

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

Framework	Testing cadence	Scope boundary
PCI DSS service providers	Segmentation validation every six months	The isolation between the environment and other networks
DFARS and CMMC	Assessment against SP 800-171, three year cycle for some levels	The enclave holding controlled unclassified information
HIPAA Security Rule	Periodic risk analysis and vulnerability management	Systems that handle protected health information
SOC 2 and ISO 27001	Evidence that testing occurred and findings closed	The systems within the audit or certification scope

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 the list of frameworks you answer to with the date of the next audit or submission for each, the asset inventory and network diagrams, last year's testing reports and remediation records, the open audit findings and the internal auditor who will rely on the report. Our engineer asks where the regulated data lives for each framework, which systems a parent, affiliate or third party operates, when testing windows are available, how quickly your teams can remediate and what evidence format your auditors expect. You then receive a written scope drawn as the union of your framework boundaries, a calendar that places testing, remediation and retesting ahead of your earliest deadline and a proposal for the engagement and its reporting. The initial consultation is free, and the hotline at (800) 868-8189 is answered 24/7.

Sources and Related Reading

Authorities cited in this guide: 23 NYCRR Part 500. Supplies the annual penetration testing, vulnerability assessment and April 15 submission requirements for New York financial services companies, in the amended regulation text published by the Department of Financial Services. PCI Security Standards Council document library. Hosts PCI DSS version 4.0.1 and its Requirement 11 penetration testing, segmentation testing and vulnerability scanning provisions summarized here, in the Council's current library. DFARS 252.204-7012. Establishes the adequate security, 72 hour reporting and 90 day image preservation duties for defense contractors, in the current acquisition.gov clause text. NIST SP 800-171 Revision 2. Lists the security requirements for controlled unclassified information, including vulnerability scanning and remediation, that CMMC Level 2 assessments test, in the Revision 2 text that 32 CFR 170.2 incorporates.

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

FREQUENTLY ASKED

Meeting the Audit Deadline

How far in advance should we schedule annual penetration testing?

Early enough that testing, remediation and retesting all complete before the earliest audit or submission date you face. The drivers are the size of the environment, the number of framework boundaries to cover, the likely volume of findings based on prior years and how quickly your change management process can close them. Organizations that test in the first half of their compliance year give remediation and retesting room to finish, and the auditor sees that room in the retest record.

Can one penetration test satisfy NYDFS, PCI DSS and SOC 2 at the same time?

Yes, if the scope is the union of what each framework requires and the report maps findings and tested controls to each. Part 500 needs the covered entity's systems tested inside and outside the boundary. PCI needs the cardholder data environment, connected systems and segmentation tested. SOC 2 needs evidence that testing occurred and findings were tracked. We draw the boundaries on one diagram during scoping and produce a framework matrix so each examiner goes straight to the evidence that applies to them.

What does annual compliance testing cost?

The initial consultation is free. The proposal reflects the number of systems and network segments in scope, the number of frameworks whose boundaries must be covered, whether application testing and social engineering are included, the depth of control validation required and the reporting each audience needs. Consolidating several frameworks into one engagement is almost always less expensive than separate vendor engagements for each, because the same test of a shared system serves every framework that covers it.

Is a vulnerability scan enough for our auditor?

For the scanning requirement, a properly scheduled scan with documented rescans after remediation is what the framework asks for. For the penetration testing requirement, auditors ask for the tester's methodology, the scope statement, evidence of manual exploitation attempts and a retest record, which come from a penetration test performed by a person working to a methodology. Presenting each record for the requirement it serves keeps a routine audit routine.

What happens if the test finds something critical right before the audit?

Fix it, retest it and document both, and agree with internal audit how the result is presented. Because we report findings as they are confirmed rather than at the end, the remediation window opens as early as the finding does. Where a framework allows a qualified certification or a documented remediation plan, the certifying officer weighs that against certifying over an open item. The retest record showing closure before the audit date is what turns a near miss into a demonstration that the program works.

Web Addresses for the Sources Cited

1. NIST Cybersecurity Framework 2.0: https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final

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

2. from both inside and outside the information systems' boundaries: https://www.dfs.ny.gov/cybersecurity/23-NYCRR-Part-500
3. PCI Security Standards Council document library: https://www.pcisecuritystandards.org/document_library/
4. DFARS 252.204-7012: https://www.acquisition.gov/dfars/part-252-solicitation-provisions-and-contract-clauses#DFARS_252.204-7012
5. NIST SP 800-171 Revision 2: https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final

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.