



VOKE CYBER PRESENTS

Compliance-to-Pentest Matrix

Which of 10 major compliance frameworks require penetration testing, what kind, and how often — one reference, no ambiguity.



UPDATED
Sept 2026

VERSION
2.0

AUTHOR
Louis Sanchez

"Do we need a pentest for compliance?" is the most common question we hear from vCISOs and IT leaders. The answer depends on the framework, and the language is rarely straightforward — some frameworks mandate it, others imply it, and a few leave it open to interpretation until an auditor or regulator decides otherwise.

This guide maps 10 major compliance frameworks to their actual penetration testing requirements, the citation behind each, and the gotchas that trip organizations up during audits.

Quick Reference Matrix

Side-by-side comparison across all 10 frameworks.

FRAMEWORK	REQUIREMENT	FREQUENCY	KEY CITATION	PENTEST TYPES
PCI DSS v4.0.1	REQUIRED	Annual + after significant changes	Req. 11.4.2 / 11.4.3	External, Internal, Segmentation
SOC 2	EXPECTED	Annual (de facto)	CC4.1, CC7.1	External, Internal, Web App
HIPAA	RECOMMENDED	Annual (industry standard)	45 CFR 164.308	External, Internal, Web App
ISO 27001	EXPECTED	Annual	A.8.8, A.5.36, A.8.34 (2022)	External, Internal, Web App
CMMC Level 2+	EXPECTED	Triennial + annual affirmations	Multiple practices	External, Internal, Web App
NIST CSF 2.0	RECOMMENDED	Not prescribed	ID.RA, PR.PS, DE.CM	Varies by implementation
FedRAMP	REQUIRED	Annual	FedRAMP Pentest Guidance	External, Internal, Web App
NY DFS (23 NYCRR 500)	REQUIRED	Annual	Section 500.5	External, Internal
GDPR	RECOMMENDED	Regular (not specified)	Article 32(1)(d)	External, Web App
EU AI Act	REQUIRED	Per risk assessment cycle	Art. 15(4)	AI/ML, Web App, API

REQUIRED Legally mandates security testing, by name or binding "shall be tested/resilient" language

EXPECTED Not explicitly mandated, but auditors will ask for it

RECOMMENDED Framework recommends security testing; pentest is the accepted method

10

Frameworks Covered

4

Require Pentesting

3

Expect Pentesting

3

Recommend Pentesting

How to Use This Guide

Pages 3–7 break down what each framework actually requires, the citation behind it, and the gotchas we see most often when scoping compliance-driven pentests. Four of these frameworks — PCI DSS, SOC 2, HIPAA, and ISO 27001 — have a full-length companion article at vokecyber.com/blog with worked examples and FAQs; look for the article title referenced in each section.

Payment & Service Organization Frameworks

PCI DSS v4.0.1 and SOC 2

PCI DSS v4.0.1

REQUIRED

Payment Card Industry Data Security Standard

CITATION Req. 11.4.2 (internal) & 11.4.3 (external) pentest; 11.3.1/11.3.2 scans (quarterly); 11.4.5/11.4.6 segmentation testing

FREQUENCY Annual + after significant changes. Segmentation testing: every 12 months (all entities), every 6 months (service providers).

SCOPE Cardholder data environment (CDE), connected systems, and systems that could impact CDE security. The pentest must validate that segmentation controls are operational and effective.

COMMON GOTCHAS

- "Significant change" is broadly defined — a firewall rule update or new VLAN qualifies and triggers a re-test.
- QSAs reject automated-only results; the test must include manual exploitation attempts.
- Segmentation testing is frequently overlooked — if you claim segmentation reduces scope, you must prove it works.

Full breakdown: "PCI DSS 4.0 Penetration Testing Requirements" — vokeycyber.com/blog

SOC 2

EXPECTED

Service Organization Control 2 (AICPA Trust Services Criteria)

CITATION CC4.1 names penetration testing explicitly as an evaluation method; CC7.1 covers vulnerability detection/monitoring.

FREQUENCY Not specified by the Trust Services Criteria. Annual, aligned to the audit period, is the de facto standard.

SCOPE Systems in scope for the SOC 2 report — production infrastructure and customer-facing applications.

COMMON GOTCHAS

- Organizations assume "Expected" means "optional" — auditors will ask for penetration test results, and not having one creates a finding or a qualification in the report.
- Remediation evidence matters as much as the test itself; auditors want findings, actions taken, and retest confirmation.

Full breakdown: "SOC 2 Penetration Testing Requirements" — vokeycyber.com/blog

Healthcare & Information Security Management

HIPAA and ISO/IEC 27001:2022

HIPAA

RECOMMENDED

Health Insurance Portability and Accountability Act

CITATION 45 CFR 164.308(a)(1)(ii)(A) risk analysis; 164.308(a)(1)(ii)(B) risk management. Pentesting isn't named explicitly, but it's the most effective way to identify the technical vulnerabilities both provisions require you to find and remediate.

FREQUENCY The Security Rule says "regular" without defining a cadence. Annual is the industry standard.

SCOPE All systems that create, receive, maintain, or transmit ePHI — EHR systems, patient portals, medical devices, cloud.

COMMON GOTCHAS

- OCR enforcement actions frequently cite a failure to conduct a thorough risk analysis — a scan alone does not meet this bar.
- Business associates are held to the same standard as covered entities — third-party vendors handling ePHI need their own testing program.

Full breakdown: "HIPAA Penetration Testing Requirements" — vokeycyber.com/blog

ISO 27001

EXPECTED

Information Security Management System (ISMS) — ISO/IEC 27001:2022

CITATION Annex A.8.8 (Management of Technical Vulnerabilities), A.5.36 (Policy/Standards Compliance), A.8.34 (Protection During Audit Testing) — 2022 revision.

FREQUENCY Aligned to the ISMS review cycle: surveillance audits every year, recertification every 3 years.

SCOPE Systems within the ISMS scope, defined during certification — typically production systems, corporate infrastructure, and externally-facing services.

COMMON GOTCHAS

- The standard says "technical compliance review," not "penetration test" — but auditors interpret this as requiring a pentest. Scans alone create a nonconformity risk.
- Findings must feed the risk treatment plan; a test without documented follow-up is a nonconformity.

Full breakdown: "ISO 27001 Security Testing Requirements" — vokeycyber.com/blog

Federal Contractor & Voluntary Frameworks

CMMC Level 2+ and NIST CSF 2.0

CMMC Level 2+

EXPECTED

Cybersecurity Maturity Model Certification

CITATION Maps to NIST SP 800-171 Rev. 2 (110 practices) — RA.L2-3.11.1 (risk assessment), CA.L2-3.12.1 (security assessment).

FREQUENCY Triennial assessment cycle with annual affirmations; most Level 2 work uses self-assessment, not third-party C3PAO review. DoD suspended the broader "Phase 2" C3PAO rollout in 2026 pending a Reform Task Force review.

SCOPE All systems that process, store, or transmit Controlled Unclassified Information (CUI) — endpoints, servers, network infrastructure, and cloud environments within the CUI boundary.

COMMON GOTCHAS

- CUI scope is routinely underestimated — systems that touch it indirectly (email, file shares, backups) are still in scope.
- The C3PAO requirement is in flux; check your specific contract's current clause rather than assuming a blanket exemption.

NIST CSF 2.0

RECOMMENDED

National Institute of Standards and Technology Cybersecurity Framework

CITATION ID.RA (Risk Assessment), PR.PS (Platform Security), DE.CM (Continuous Monitoring). Intentionally non-prescriptive.

FREQUENCY Not prescribed — risk-based. Annual testing is the most common implementation.

SCOPE Determined by the organization based on critical assets, business processes, and risk appetite.

COMMON GOTCHAS

- NIST CSF is voluntary, but many regulatory frameworks reference it as a baseline — if you claim alignment, you need evidence of testing.
- Insurance carriers increasingly reference CSF maturity tiers in underwriting — claiming a tier without testing is a misrepresentation risk.

Federal Cloud & Financial Services

FedRAMP and NY DFS (23 NYCRR 500)

FedRAMP

REQUIRED

Federal Risk and Authorization Management Program

CITATION FedRAMP CSP Penetration Test Guidance (Rev 5); transitioning to Key Security Indicators under FedRAMP 20x for Low/Moderate baselines.

FREQUENCY Annual pentest. Monthly scanning. Continuous monitoring with ConMon reporting.

SCOPE The entire FedRAMP authorization boundary — system components, interconnections, and data flows.

COMMON GOTCHAS

- The penetration test must be performed by an accredited 3PAO — internal testing or a non-accredited firm does not satisfy the requirement.
- FedRAMP 20x becomes mandatory for new Low/Moderate authorizations by Jan 1, 2027, replacing Rev 5's catalog with Key Security Indicators; Rev 5 stays in force for existing authorizations and the former High baseline.

NY DFS (23 NYCRR 500)

REQUIRED

New York Department of Financial Services Cybersecurity Regulation

CITATION Section 500.5 ("Vulnerability Management," renamed by the 2023 Second Amendment).

FREQUENCY Annual pentest (unchanged since 2017). Risk-based automated scanning and manual review replaced the old fixed bi-annual assessment, effective May 2025.

SCOPE All information systems storing, processing, or transmitting nonpublic information (NPI) — banks, insurers, and financial services firms licensed by NY DFS.

COMMON GOTCHAS

- Applies to any financial services firm operating in New York, even if headquartered elsewhere.
- A pentest that turns up evidence of a prior breach can trigger a 72-hour notification obligation to the Superintendent — and a separate 24-hour clock for extortion payments.

EU Data Protection & AI Regulation

GDPR and the EU AI Act

GDPR

RECOMMENDED

General Data Protection Regulation (EU)

CITATION Article 32(1)(d) — a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational security measures.

FREQUENCY "Regularly" is undefined. Annual testing is the accepted standard.

SCOPE All systems processing personal data of EU residents — applications, databases, APIs, third-party integrations.

COMMON GOTCHAS

- Applies to any organization processing EU residents' data, regardless of where the company is located — US companies with EU customers are in scope.
- Fines are two-tiered: Article 32 (security) failures cap at 2% / €10M (Art. 83(4)), not the 4% / €20M tier reserved for rights/consent violations.

EU AI Act

REQUIRED

Regulation (EU) 2024/1689 on Artificial Intelligence

CITATION Article 15(4) — high-risk AI systems shall be resilient against attempts by unauthorized third parties to exploit vulnerabilities.

FREQUENCY Throughout the AI system lifecycle, aligned to the Article 9 risk management cycle.

SCOPE High-risk AI systems per Annex III — the model, training pipeline, inference infrastructure, and all interfaces.

COMMON GOTCHAS

- High-risk obligations took effect August 2, 2026 and are already in force — this is no longer a future deadline.
- Traditional pentesting alone is insufficient; AI systems need specialized testing for model evasion, data poisoning, and adversarial inputs.

Need a Compliance-Driven Pentest?

We scope every engagement to your compliance requirements. Tell us which frameworks apply, and we deliver a test that satisfies your auditors — with retesting included.



Louis Sanchez

Founder & Principal Security Consultant, Voke Cyber — OSCP, OSWA, CISSP, CCSK

Get Started

The requirements in this guide are verified against current framework documentation as of September 2026. Frameworks evolve — CMMC, FedRAMP, and NY DFS all changed materially in 2025–2026 — so revisit this guide or vokecyber.com/resources/compliance-pentest-matrix for the latest version.

Web: vokecyber.com

Email: info@vokecyber.com

Phone: (765) 422-5464

Get a quote: vokecyber.com/get-started