NIST 800-53 Moderate

Pentesting Requirements

A practical guide for IT leaders, MSPs, and SaaS teams navigating FedRAMP Moderate, U.S. federal systems, and regulated environments.

Contents

01 Quick Summary

WHAT IT LEADERS NEED TO KNOW

If your organization is pursuing FedRAMP Moderate authorization or supporting federal customers, penetration testing is not optional. Here is the simplified version:

AT A GLANCE

- Annual independent penetration testing is expected.
- Vulnerability scanning alone is not enough.
- Both internal and external attack surfaces must be tested.
- Web applications, APIs, cloud infrastructure, and boundary protections are typically in scope.
- Retesting after remediation is expected before assessments are considered complete.
- Under FedRAMP Rev 5, annual red team exercises are now also required for Moderate environments.
- Continuous monitoring expectations are increasing under FedRAMP 20x.

02 What Is FedRAMP Moderate?

BACKGROUND & CONTEXT

FedRAMP Moderate is a U.S. federal security baseline used for cloud service providers (CSPs) handling sensitive but unclassified government information. The framework is built on NIST SP 800-53 security controls and is commonly required for:

- SaaS providers selling to government agencies.
- MSPs supporting federal contractors.
- Organizations handling Controlled Unclassified Information (CUI).
- Cloud platforms pursuing federal authorization.

For many IT leaders, the biggest challenge is translating abstract compliance controls into practical technical requirements. This guide focuses specifically on the penetration testing and security validation expectations behind FedRAMP Moderate.

Key Terms

TERM	PLAIN ENGLISH MEANING
Authorization Boundary	The systems, applications, cloud infrastructure, and services included in your FedRAMP assessment.
CUI	Controlled Unclassified Information - sensitive government-related information requiring protection.
CSP	Cloud Service Provider.
3PAO	Third-Party Assessment Organization authorized to perform FedRAMP assessments.
CA-8	The NIST control covering penetration testing.
RA-5	The NIST control covering vulnerability scanning.
Red Team Exercise	A simulated adversary exercise focused on testing detection and response capabilities - distinct from a pentest.

03

Required Controls

WHAT PENTESTING IS REQUIRED FOR NIST 800-53 MODERATE?

NIST 800-53 Moderate does not mandate a specific annual pentest on a fixed schedule. What it requires is penetration testing and vulnerability assessments as part of a continuous monitoring program. Three controls directly drive this. A fourth set indirectly requires testing as part of broader system assurance obligations.

CA-8: Penetration Testing (Core Requirement)

CA-8 is the primary pentesting control. A compliant pentest under CA-8 must:

- Be conducted at least annually.
- Cover both internal and external attack surfaces.
- Be performed by independent testers - not your internal team.
- Validate exploitability, not just identify vulnerabilities.
- Produce a formal report including proof of exploitation, attack paths, business impact per finding, risk ratings, remediation guidance, and retest confirmation.

RA-5: Vulnerability Monitoring & Scanning (Also Required)

RA-5 governs ongoing vulnerability scanning - a distinct activity from pentesting, but the baseline it establishes matters.

- Regular vulnerability scans (typically monthly or quarterly).
- Coverage of all internal and external components.
- Severity-based remediation timelines.
- Validation rescans after fixes are applied.

> **Scanning is not Pentesting**
>
> Vulnerability scanning identifies potential weaknesses automatically. Penetration testing actively validates whether vulnerabilities can be exploited in real-world attack scenarios. Scans alone do not satisfy the CA-8 requirement - and FedRAMP assessors know the difference.

CA-2: Security Assessments (Pentest Evidence Supports This)

CA-2 requires broader technical evaluation and control validation activities. A pentest report directly contributes evidence for CA-2 compliance, including controls testing, technical evaluation of implemented safeguards, and continuous monitoring evidence.

SI-2, SI-4, SC-7: Controls That Indirectly Trigger Testing

CONTROL	WHY IT MATTERS
SI-4	Validates monitoring and detection effectiveness - pentest results confirm detection capability.
SI-2	Significant infrastructure changes often require a new pentest.
SC-7	Segmentation and boundary protections must be validated through testing.

04 Pentest Scope

WHAT SHOULD BE IN SCOPE?

The authorization boundary determines pentest scope. In practice, any system that stores, processes, or transmits Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) should generally be included.

COMPONENT	TYPICAL TESTING FOCUS
External Perimeter	Public-facing assets, IP ranges, DNS infrastructure.
Internal Network	Segmentation, lateral movement paths.

Web Applications & APIs	Authentication, authorization, business logic, and any app handling FCI/CUI.
Cloud Infrastructure	AWS, Azure, GCP - configuration review and exploitation testing.
Boundary Protections	WAF, VPN, SSO, IAM - tested for bypass and misconfiguration.
Configuration Reviews	Key systems assessed for hardening gaps.

What FedRAMP Moderate Does Not Explicitly Require

The following are not directly mandated by the standard, though assessors may expect them depending on system complexity or agency requirements:

- Mobile application pentesting.
- Source code or white-box reviews.
- Social engineering campaigns.
- OWASP Top 10-specific reporting formats.

Important Update: Red Team Exercises (CA-8(2)) Now Required for Moderate

Under NIST 800-53 Rev 5 and the FedRAMP Rev 5 baseline (finalized May 2023), CA-8(2) red team exercises have been added to both the Moderate and High baselines. In addition to the standard annual penetration test, Moderate CSPs must now conduct annual red team exercises that simulate real adversary attempts to compromise organizational systems.

Red team exercises differ from pentests in focus: rather than finding and exploiting as many vulnerabilities as possible, red teams assess detection, defense, and response capabilities. For many IT leaders this represents a major shift - FedRAMP is moving beyond vulnerability discovery toward validating defensive maturity.

Pentesting vs. Red Teaming

PENTESTING	RED TEAMING
Focuses on finding and exploiting vulnerabilities	Focuses on testing detection and response capabilities
Usually time-boxed and scoped to specific systems	Simulates realistic adversary behavior across the environment
Prioritizes exploit validation and remediation evidence	Prioritizes operational resilience and defensive maturity

05 Assessor Expectations

WHAT AUDITORS COMMONLY EXPECT IN PRACTICE

Although FedRAMP guidance allows flexibility, most 3PAOs and assessors conducting FedRAMP Moderate reviews expect a practical annual testing package covering the following:

TYPICALLY EXPECTED

- External network penetration test.
- Internal network penetration test.
- Web application / API pentest.
- Cloud environment review (AWS / Azure / GCP).
- Credentialed testing where applicable.
- Remediation retest before report is finalized.
- Annual red team exercise (CA-8(2) - Rev 5).

COMMONLY RECOMMENDED

- Regular vulnerability scanning program (RA-5).
- Segmentation validation testing.
- Detection and response validation exercises.
- Cloud infrastructure configuration review.

06 FedRAMP 20x

WHAT'S CHANGING FOR MODERATE AUTHORIZATION

In March 2025, GSA announced FedRAMP 20x - the first major modernization of the program in over a decade. For MSPs helping clients pursue or maintain FedRAMP Moderate authorization, this is the most significant change to understand right now.

What FedRAMP 20x Changes

- Replaces static, documentation-heavy assessments with continuous, automated validation.
- Introduces Key Security Indicators (KSIs) - machine-readable metrics that prove controls are active and effective in real time, rather than via screenshots or policy documents.
- Requires risk-based remediation timelines - critical vulnerabilities with known exploits must be closed faster; lower-risk findings get more flexibility.
- Phase 2 (currently underway) is targeting approximately 10 Moderate pilot authorizations before wide-scale rollout.

What FedRAMP 20x Does Not Change

- CA-8 (penetration testing) remains a requirement - human-led pentests are not replaced by automation.
- CA-8(2) (red team exercises) also remains required for Moderate systems under Rev 5.
- Pentester independence requirements remain in place.
- Annual pentest cadence is still the expected baseline for Moderate systems.

Key Takeaway for IT Leaders & MSPs

Automation is increasing - but manual offensive security validation is not disappearing. FedRAMP 20x makes the path to Moderate authorization faster and more automated, but the pentesting requirement is not going away. If anything, continuous monitoring expectations increase the value of working with a pentesting partner whose reports are detailed, remediation-focused, and retest-confirmed.

07

Common Question

DO PENTESTERS NEED TO BE U.S.-BASED?

This is one of the most frequent questions MSPs ask when evaluating pentesting partners for FedRAMP-scoped work.

Short answer: No. FedRAMP itself has no U.S. citizenship or residency requirement for pentesters. The FedRAMP Program Management Office has directly confirmed there is no government-wide citizenship requirement.

What the framework does require:

- Testers are independent from the organization being tested.
- Personnel undergo appropriate background screening as described in the System Security Plan.
- The CSP discloses its personnel screening approach to the sponsoring agency.

Agency-Level Exception

Individual agencies may impose their own citizenship or CONUS-location requirements as part of their Authorization to Operate (ATO) contract. This is especially relevant for DoD environments, ITAR/EAR-regulated systems, or agency-specific contracts. Always confirm agency-specific requirements before scoping an engagement.

08

Resources for MSPs

CMMC & FEDRAMP COMPLIANCE

Software Secured: NIST SP 800-115 & Pentesting — softwaresecured.com

Explains how NIST SP 800-115 (the how-to-test standard) relates to 800-53 (the controls standard). Useful framing for client conversations about why pentesting is required and what it should cover.

DoD CMMC Official FAQs (Q33-Q37) — dodcio.defense.gov/CMMC

Primary source for MSP and ESP classification under the CMMC final rule. Pentesters and IR firms are explicitly carved out of ESP definitions.

Secureframe: CMMC Compliance Guide — secureframe.com/blog/cmmc

Covers the CMMC program rule, enforcement timeline, Level 2 certification requirements, and the 110 NIST 800-171 controls underlying CMMC. Regularly updated as the program evolves.

Secureframe: Pocket Guide to CMMC for MSPs — secureframe.com/msp-resources/cmmc-guide-for-msps

MSP-specific guide to navigating CMMC for clients in the Defense Industrial Base. Covers scope, certification levels, and what MSPs need to have ready before their clients' audits.

FedRAMP.gov: 20x Program Overview — fedramp.gov/20x

Official GSA source. Live roadmap for the FedRAMP 20x modernization, Phase 1 and Phase 2 details, and KSI framework.

Secureframe: FedRAMP 20x Roadmap — secureframe.com/blog/fedramp-20x-roadmap

GRC automation platform. Most current practitioner-level breakdown of Phase 2 Moderate milestones with confirmed dates as of January 2026.