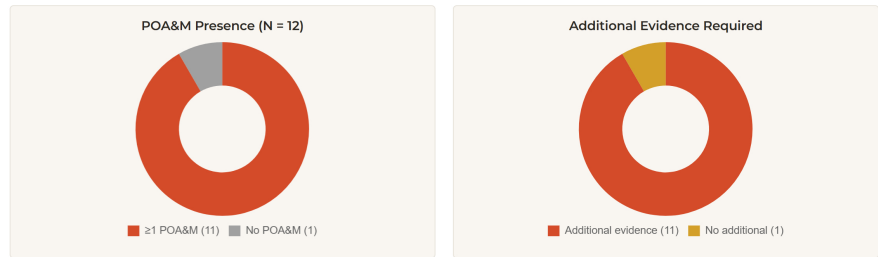


2. Executive Summary – Key Benchmarks

Metric	Observed Value	Denominator / Notes
Sample size	N = 12	Completed FedRAMP 3PAO assessments
Average authorization boundary size	~85 system components / ~210 assets	Wide range by service model
Median formal assessment duration	42 business days	Kickoff to draft SAR / Security Assessment Report
Assessments with ≥1 POA&M	92% (11 of 12)	Median ~6 items when present
Percentage requiring additional evidence	92% (11 of 12)	At least one clarification / evidence request cycle
Single-system / tightly bounded vs. complex multi-component	58% / 42%	N = 12
Average evidence volume	~3,400 discrete artifacts	Range approximately 1,200 – 9,500



3. Average Scope Size

Authorization boundary size is a primary driver of assessment effort:

- Average in-scope system components / services: ~85
- Average assets (instances, containers, network devices, endpoints in boundary): ~210
- Smallest observed boundary: focused SaaS service with limited supporting infrastructure
- Largest observed boundaries: multi-service platforms with extensive inheritance and customer-configurable elements

CSPs that maintained clear, current System Security Plans (SSPs), accurate data-flow diagrams, and well-documented control inheritance consistently experienced more efficient testing and fewer boundary-related findings.

4. Median Assessment Duration

Formal assessment duration is measured from assessment kickoff (accepted evidence package / readiness to test) through delivery of the draft Security Assessment Report.

- **Median formal assessment duration: 42 business days**
- 25th percentile: ~28 business days (mature packages, tighter boundaries)
- 75th percentile: ~58 business days
- Longer engagements typically involved complex multi-component systems, heavy inheritance validation, or significant mid-assessment evidence remediation

Note: Agency or JAB review cycles, package iteration after 3PAO delivery, and continuous monitoring cadence are outside this formal assessment duration metric.

5. Common Failed Objectives

The following NIST SP 800-53 control areas most frequently generated residual findings (partially implemented or not satisfied) across the N = 12 assessments:

Rank	Control Family / Examples	Primary Issue Observed
1	AU (Audit & Accountability) — AU-2, AU-3, AU-6, AU-12	Incomplete event coverage, review cadence, or log protection
2	CM (Configuration Management) — CM-2, CM-3, CM-6, CM-8	Baselines not maintained; change control gaps; incomplete inventories
3	AC (Access Control) — AC-2, AC-3, AC-6, AC-17	Account management, least privilege, remote access evidence gaps
4	IA (Identification & Authentication) — IA-2, IA-5, IA-8	MFA coverage, authenticator management, federation evidence
5	SI (System & Information Integrity) — SI-2, SI-3, SI-4	Flaw remediation timelines; monitoring coverage
6	CA (Assessment, Authorization, Monitoring) — CA-2, CA-5, CA-7	POA&M quality; continuous monitoring evidence
7	SC (System & Communications Protection) — SC-7, SC-8, SC-13	Boundary protection; encryption implementation evidence

Controls related to supply chain risk (SR), contingency planning testing (CP), and personnel security also appeared frequently among residual findings, particularly for CSPs with rapid growth or complex subservice organizations.

6. Evidence Deficiencies

Evidence quality — not volume alone — determined assessment efficiency. Common deficiencies:

- **SSP and control implementation statements** that were generic or not aligned to the actual architecture
- **Screenshots and exports without context** (missing system identifiers, timestamps, or configuration paths)
- **Incomplete or non-representative log samples**
- **Missing or outdated configuration baselines and inventories**
- **Inheritance claims** lacking current customer responsibility matrices, shared responsibility documentation, or subservice organization evidence
- **POA&M entries** that were vague, lacked milestones, or did not map cleanly to residual risk
- **Continuous monitoring artifacts** that did not demonstrate ongoing operational effectiveness

CSPs using structured evidence repositories mapped to 800-53 controls and maintaining living SSPs required fewer clarification cycles.

7. POA&M Frequency

- **92% (11 of 12)** of assessments resulted in at least one POA&M item
- Median number of POA&M items when present: ~6
- Most common categories: audit logging, configuration management, access control, vulnerability remediation, and continuous monitoring evidence

In FedRAMP, POA&Ms are an expected and normal part of the authorization process. Well-formed POA&Ms with clear milestones, residual risk statements, and remediation owners are treated as manageable; poorly defined or open-ended POA&Ms create friction in agency / JAB review.

8. Authorization Boundary Complexity

Analogous to "enclave vs. enterprise" scoping in other frameworks, FedRAMP assessments varied by boundary complexity:

- **58% (7 of 12)** — single-system or tightly bounded service with limited external dependencies
- **42% (5 of 12)** — complex multi-component, multi-service, or heavily inherited architectures

Tighter, well-documented boundaries correlated with shorter formal assessment durations, lower evidence volume, and fewer residual findings related to external interfaces and inheritance. Complex boundaries more frequently generated findings in boundary protection, external system services, and shared responsibility clarity.

9. Average Evidence Volume & Additional Evidence Requests

- Average discrete artifacts submitted: ~**3,400** (policies, procedures, SSP excerpts, diagrams, configurations, logs, scan results, tickets, training records, etc.)
- Observed range: approximately 1,200 to 9,500 artifacts
- **92% (11 of 12)** required at least one round of additional evidence after initial package review
- Most frequent additional requests: expanded log samples, baseline details, MFA / access path proof, inheritance documentation, and continuous monitoring records

Volume alone was a weak predictor of success. Practice-mapped, contextualized, and current evidence moved assessments faster than large undifferentiated document dumps.

10. Most Misunderstood Requirements

- **Continuous monitoring (CA-7 and related)** — treating assessment as a point-in-time event rather than demonstrating ongoing operational effectiveness
- **Control inheritance and shared responsibility** — incomplete or outdated customer responsibility matrices; unsupported claims about what the CSP vs. customer vs. subservice organization provides
- **Configuration baselines (CM-2 / CM-6)** — presenting generic hardening guides as maintained, version-controlled baselines for the actual production environment
- **Audit record content and review (AU-3 / AU-6)** — logging some events without ensuring required content, protection, retention, and documented review
- **Authenticator management and MFA (IA-2 / IA-5)** — incomplete coverage across privileged, remote, and federated access paths
- **POA&M quality (CA-5)** — vague milestones, missing residual risk, or lack of clear ownership
- **Boundary and data-flow accuracy** — SSP diagrams that do not match the implemented architecture or external connections

11. Key Insights for CSPs

- **1. Keep the SSP and boundary living documents.** Out-of-date architecture descriptions create immediate friction.
- **2. Map evidence to 800-53 controls before kickoff.** Assessors spend less time requesting clarification when artifacts are already control-tagged.
- **3. Prioritize AU, CM, AC, and IA.** These families accounted for a disproportionate share of residual findings.
- **4. Treat continuous monitoring as first-class evidence,** not an afterthought.
- **5. Expect POA&Ms and prepare high-quality ones.** 92% of assessments had at least one item.
- **6. Validate inheritance early.** Unsupported or stale shared-responsibility claims are a recurring source of delay.

12. Authors, Reviewers & How to Cite

Lead Author

Michael D. Peters, CEO & Founder, Lazarus Alliance, Inc.

A2LA-accredited FedRAMP 3PAO leadership; Authorized CMMC C3PAO; PCI DSS QSA firm principal; Delaware CPA firm. 26+ years in proactive cybersecurity, audit, and compliance.

Technical Review

FedRAMP Assessment Team, Lazarus Alliance (3PAO delivery and quality assurance under ISO/IEC 17020 and FedRAMP requirements).

How to Cite This Report

Peters, M. D. (2026). *2026 FedRAMP Assessment Benchmark Report: Aggregate Anonymized Insights from Lazarus Alliance FedRAMP 3PAO Assessments* (Version 1.0). Lazarus Alliance, Inc. <https://lazarusalliance.com/2026-fedramp-assessment-benchmark-report/>

Recommended short citation: Lazarus Alliance (2026). 2026 FedRAMP Assessment Benchmark Report (N=12).

13. About & Contact

Lazarus Alliance is an A2LA-accredited FedRAMP Third-Party Assessment Organization (3PAO), an authorized CMMC C3PAO (CPN 10251), a PCI DSS Qualified Security Assessor (QSA), and a veteran-owned small business headquartered in Scottsdale, Arizona. Since 2000 the firm has specialized in proactive cybersecurity, audit, and compliance services across FedRAMP, CMMC, SOC 2, NIST, ISO, and related frameworks.

Lazarus Alliance, Inc.

27743 N. 70th Street, Suite 100, Scottsdale, AZ 85266
1-888-896-7580 • client-support@lazarusalliance.com
<https://lazarusalliance.com>

© 2026 Lazarus Alliance, Inc. All rights reserved. Proactive Cybersecurity®, Cybervisor®, and IT Audit Machine® are trademarks of Lazarus Alliance or its affiliates. Aggregate data is anonymized; individual assessment outcomes remain confidential.

© 2026 Lazarus Alliance, Inc. • Proactive Cybersecurity® • A2LA-Accredited FedRAMP 3PAO
Scottsdale, Arizona • 1-888-896-7580 • lazarusalliance.com

Download the 2026 FedRAMP Assessment Benchmark Report

Additional Analysis

- [1. How Long Does a FedRAMP Assessment Take?](#)
- [2. 7 Most Common FedRAMP Assessment Findings](#)
- [3. How Much Evidence Does a FedRAMP Assessment Require?](#)
- [4. FedRAMP Authorization Boundary Complexity](#)
- [5. 7 Most Misunderstood FedRAMP Requirements Observed in Assessments](#)
- [6. FedRAMP POA&M Benchmarks](#)

Talk with one of our experts

Our Lazarus Alliance Cybervisor™ teams have experience performing thousands of assessments for organizations providing services to clients around the world.

We're here to answer any questions you may have.

Name *

First

Last

Email *

Email

Confirm Email

Phone

Company *

Which service categories are you interested in? *

- ☐ IT Audit & Compliance
- ☐ Risk Assessment & Management
- ☐ IT Pre-Acquisition Assessment Services
- ☐ Vulnerability & Penetration Testing
- ☐ Governance & Policy Analysis
- ☐ Privacy Audit
- ☐ Cybervisor Security Advisory Services

Which services are you interested in? *

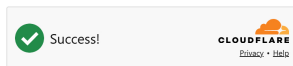
- ☐ StateRAMP

- ☐ FedRAMP
- ☐ FedRAMP Moderate Equivalency
- ☐ SOC 1-2-3
- ☐ CMMC, NIST SP 800-171 & SP 800-172
- ☐ NIST SP 800-53, SCA-V
- ☐ PCI DSS QSA & SAQ
- ☐ ISO 27001
- ☐ ISO 27017
- ☐ ISO 27018
- ☐ ISO 27701
- ☐ ISO 22301
- ☐ ISO 9001
- ☐ ISO 90003
- ☐ ISO 42001
- ☐ HIPAA NIST 800-66
- ☐ CJIS
- ☐ IRS 1075
- ☐ IRS 4812
- ☐ ACAB LA DMF
- ☐ FDA 21 CFR Part 11 GxP
- ☐ MARS-E
- ☐ NIST CSF
- ☐ CBFP: FFIEC, SEC, NFA & FINRA
- ☐ C5
- ☐ Privacy, CCPA, CPRA, PIPEDA, DPIA, LGPD
- ☐ Risk Management
- ☐ IT Pre-Acquisition Assessment Services
- ☐ COSO SOX
- ☐ NERC CIP
- ☐ FTC SafeGuards
- ☐ CTPAT
- ☐ ITAR
- ☐ SSDF NIST SP 800-218
- ☐ Something not listed

How may we assist you? *

Download our company brochure.

☒ I agree to receiving additional marketing communications.



Submit

Looking for something?

Search

Go

