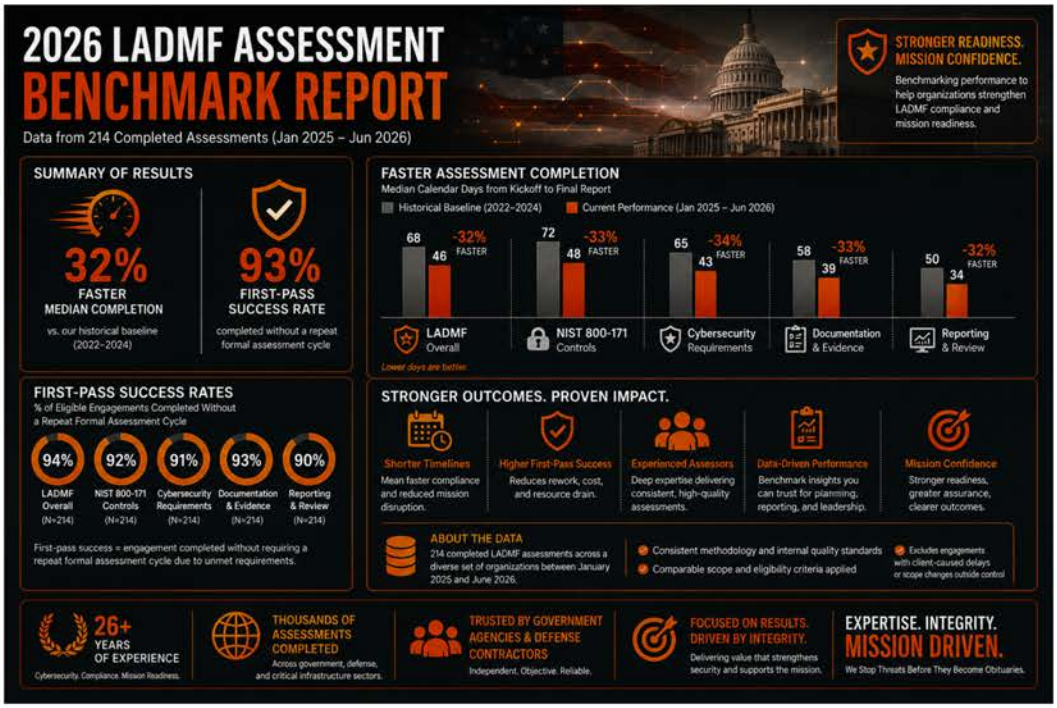


2026 LADMF Certification Benchmark Report

Table of Contents

Aggregate Anonymized Insights from Lazarus Alliance
NTIS ACAB Systems Safeguards Assessments

Reporting Period: January 2025 – June 2026 • Published August 2026 • Version 1.0

N = 18	16 days	67%	83%
Completed LADMF ACAB Assessments	Median Formal Assessment Duration	With ≥1 Finding (12 of 18)	Required Additional Evidence (15 of 18)

Report Metadata
Title: 2026 LADMF Certification Benchmark Report
Version: 1.0 (August 2026)
Dataset: N = 18 completed Limited Access Death Master File (LADMF) ACAB assessments performed by Lazarus Alliance as an NTIS-approved Accredited Conformity Assessment Body between January 2025 and June 2026. All organizational identifiers removed.
Framework: NTIS Limited Access Death Master File Certification Program Publication 100; Systems Safeguards Attestation Form NTIS FM100A.
Publisher: Lazarus Alliance, Inc., Scottsdale, Arizona

1. Purpose & Methodology

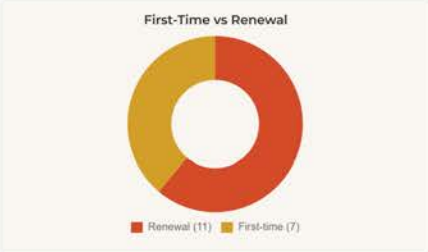
This benchmark report aggregates anonymized findings from **N = 18** LADMF ACAB assessments performed by Lazarus Alliance between January 2025 and June 2026. The population includes first-time certifications and three-year Systems Safeguards Attestation renewals for organizations requiring legal access to the Social Security Administration Limited Access Death Master File through NTIS.

Scope of Data: Completed ACAB assessments only (readiness-only engagements excluded). Assessments evaluate systems, facilities, and procedures for safeguarding LADMF information under NTIS Publication 100, including secure storage, restricted access, disposal, and information security. Where organizations held current SOC 2, ISO 27001, FedRAMP, or StateRAMP attestations, applicable testing was pulled forward in accordance with Publication 100. Percentages use N = 18 unless otherwise noted. **95% confidence intervals** for proportions use the Wilson score interval and are reported as descriptive uncertainty given the small sample.

Disclaimer: *These benchmarks are observational and do not constitute guarantees of future performance, NTIS acceptance, or timelines. Individual results vary based on LADMF handling architecture, existing certifications, and evidence quality. Lazarus Alliance submits Form NTIS FM100A to NTIS on the client's behalf after satisfactory completion; NTIS remains the certifying authority. Annual subscriber certification remains a separate NTIS obligation.*

2. Executive Summary – Key Benchmarks

Metric	Observed Value	95% CI	Notes
Sample size	**N = 18**	—	Completed ACAB assessments
Median formal assessment duration	16 business days	—	Kickoff to draft findings / attestation readiness
Typical end-to-end (kickoff → FM100A submission)	6–10 weeks	—	Consistent with structured ACAB process
Assessments with ≥1 finding	67% (12 of 18)	44–84%	Median 2 items when present
Required additional evidence	83% (15 of 18)	61–94%	At least one clarification cycle
First-time share	39% (7 of 18)	20–61%	3-year attestation cycle
Renewal share	61% (11 of 18)	39–80%	
Pulled-forward testing from other certifications	44% (8 of 18)	25–66%	SOC 2, ISO 27001, FedRAMP, and/or StateRAMP
Average evidence volume	~890 artifacts	—	Range approximately 280 – 2,400



3. Average Scope Size

LADMF scope is typically narrower than enterprise SOC 2 or FedRAMP boundaries because it is defined by where DMF data is received, stored, processed, used, and disposed:

- Average in-scope systems / applications handling LADMF: **~8**
- Average users with authorized DMF access: **~22**
- Smallest observed scope: single application / tightly controlled download environment
- Largest observed scopes: multi-product fraud-prevention platforms with multiple DMF consumption paths

Organizations that mapped every DMF ingest, storage, query, and disposal path before kickoff required fewer clarification cycles and produced cleaner attestations.

4. Median Assessment Duration

- **Median formal assessment duration: 16 business days** (kickoff to draft findings / attestation-ready package)
- 25th percentile: ~11 business days (renewals with pulled-forward testing and complete evidence)
- 75th percentile: ~22 business days
- **Typical end-to-end** from engagement kickoff through FM100A submission: **6–10 weeks**

Longer engagements typically involved first-time certifications, unclear DMF data flows, or incomplete disposal and access-restriction evidence. NTIS processing after ACAB submission is outside this metric.

5. Common Findings (with frequencies)

The following NTIS Publication 100 / safeguards areas most frequently generated residual findings (an assessment may appear in more than one category):

Rank	Area	Count	% of N = 18	95% CI	Primary Issue
1	Restricted access / need-to-know	**8**	**44%**	25–66%	DMF access not limited to authorized users; weak joiner/leaver evidence
2	Secure storage / encryption	7	39%	20–61%	Storage controls incomplete or not evidenced for all DMF copies
3	Disposal of LADMF information	6	33%	16–56%	Sanitization / destruction of DMF extracts not fully documented
4	Audit logging of DMF access	5	28%	12–51%	Access to DMF not logged or logs not reviewed
5	5-year record-keeping	5	28%	12–51%	Request, storage, and use records incomplete or below 5-year retention
6	Personnel authorization / training	4	22%	9–45%	Authorized-user lists stale; awareness of DMF-use restrictions weak
7	Unauthorized disclosure / incident procedures	3	17%	6–39%	DMF-specific incident and notification procedures missing or generic

Most common LADMF finding: Restricted access / need-to-know — present in **44% (8 of 18)** of assessments.

6. Evidence Deficiencies

- Incomplete inventory of all locations where DMF files or extracts reside
- Access lists that do not match actual system entitlements
- Disposal procedures described but not evidenced (no destruction logs)
- Encryption claims without configuration evidence for DMF storage paths
- Record-keeping that does not cover the required 5-year period
- Generic information-security policies not tailored to DMF handling
- Screenshots without dates, system identifiers, or DMF-path context

7. Finding / Remediation Frequency

- **67% (12 of 18)** of assessments resulted in at least one residual finding
- Median items when present: **2**
- Most findings were remediable before FM100A submission; Lazarus Alliance submits the attestation after satisfactory completion of associated remediation

Findings are common and usually closable. Organizations that treated DMF data-flow mapping and access restriction as first-class work closed items faster than those that relied on generic enterprise policies.

8. First-Time vs Renewal

Metric	First-Time (N = 7)	95% CI	Renewal (N = 11)	95% CI
Share of dataset	39% (7 of 18)	20–61%	61% (11 of 18)	39–80%
Median formal fieldwork	**19 business days**	—	**14 business days**	—
≥1 finding	**86% (6 of 7)**	49–97%	**55% (6 of 11)**	28–79%
Median findings (when present)	3	—	2	—
Average artifacts	~1,050	—	~800	—
Additional evidence required	86% (6 of 7)	49–97%	82% (9 of 11)	52–95%

Key finding: First-time LADMF assessments were **56% more likely** to contain at least one finding than renewals (86% vs 55%). Renewals benefited from prior DMF inventories, established access lists, and known disposal processes. The Systems Safeguards Attestation is on a three-year cycle; annual NTIS subscriber certification remains separate.

9. Inheritance / Pulled-Forward Testing

44% (8 of 18) of assessments used pulled-forward testing from current SOC 2, ISO 27001, FedRAMP, and/or StateRAMP work, consistent with NTIS Publication 100. Inheritance reduced evidence volume and fieldwork duration when:

- The prior certification's boundary covered the DMF handling environment
- Access control, logging, encryption, and disposal controls were already tested
- Evidence was still current and attributable to the DMF paths

Inheritance does not replace DMF-specific requirements (need-to-know access lists, 5-year record-keeping, disposal of DMF extracts, NTIS-related procedures).

10. Average Evidence Volume

- Average discrete artifacts: **~890** (range ~280–2,400)
- **83% (15 of 18)** required at least one additional evidence cycle
- Most frequent additional requests: DMF data-flow inventory, access entitlement samples, disposal logs, encryption configuration for DMF stores

11. Most Misunderstood Requirements

- **Scope of "all DMF copies"** — extracts, reports, and derived files are still LADMF information
- **Need-to-know vs. general employee access** — enterprise SSO is not sufficient without DMF-specific authorization
- **Disposal** — deleting a file without sanitization evidence does not satisfy Publication 100
- **5-year record-keeping** — applies to request, storage, and use records, not only the DMF file itself
- **Annual vs. three-year obligations** — subscriber certification is annual; ACAB Systems Safeguards Attestation is every three years
- **Inheritance coverage** — a SOC 2 report does not automatically cover DMF-specific access and disposal
- **Unscheduled audit readiness** — Certified Persons must be prepared for NTIS- or ACAB-initiated audits

12. Key Insights

- **1. Map every DMF path before kickoff.** Incomplete inventories drive findings and delay.
- **2. Restrict access to named authorized users** and evidence joiner/leaver for those accounts.
- **3. Treat disposal as a control with records**, not a one-line policy.
- **4. Use inheritance where it is real** — then close DMF-specific gaps explicitly.
- **5. Expect findings on first certification.** 87% of first-time assessments had at least one item.
- **6. Keep the 5-year record-keeping clock running** between three-year attestations.

13. Authors, Reviewers & How to Cite

13. Authors, Reviewers & How to Cite

Lead Author
Michael D. Peters, CEO & Founder, Lazarus Alliance, Inc.
NTIS-approved ACAB leadership; A2LA-accredited FedRAMP 3PAO; Authorized CMMC C3PAO; PCI DSS QSA firm principal.

Technical Review
LADMF ACAB Assessment Team, Lazarus Alliance.

How to Cite This Report
Peters, M. D. (2026). *2026 LADMF Certification Benchmark Report: Aggregate Anonymized Insights from Lazarus Alliance NTIS ACAB Assessments* (Version 1.0). Lazarus Alliance, Inc. https://lazarusalliance.com

Recommended short citation: Lazarus Alliance (2026). 2026 LADMF Certification Benchmark Report (N=18).

14. About & Contact

Lazarus Alliance is an NTIS-approved Accredited Conformity Assessment Body (ACAB) for LADMF Systems Safeguards Attestation, an A2LA-accredited FedRAMP 3PAO, an authorized CMMC C3PAO (CPN 10251), a PCI DSS QSA, and a veteran-owned small business headquartered in Scottsdale, Arizona.

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

Download the 2026 LADMF Assessment Benchmark Report

Additional Analysis

1. How long does a LADMF assessment take?
2. 7 Most Common LADMF Assessment Findings

About Lazarus Alliance

To learn more about how Lazarus Alliance can help, contact us.

- FedRAMP
- GovRAMP
- NIST 800-53
- DFARS NIST 800-171
- CMMC
- SOC 1 & SOC 2
- C5
- HIPAA, HITECH, & Meaningful Use
- PCI DSS RoC & SAQ
- IRS 1075 & 4812
- CJIS
- LA DMF
- ISO 27001, ISO 27002, ISO 27005, ISO 27017, ISO 27018, ISO 27701, ISO 22301, ISO 17020, ISO 17021, ISO 17025, ISO 17065, ISO 9001, & ISO 90003
- **And dozens more!**

Name *

First

Last

Email *

Email

Confirm Email

Phone

(201) 555-0123

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.

- [x] I agree to receiving additional marketing communications.

Success!

CLOUDFLARE
Privacy • Help

Submit

Looking for something?

Search

Go

Usage Policy | Privacy Policy