2026 SOC 2 Audit Benchmark Report

Table of Contents

Aggregate Anonymized Insights from Lazarus Alliance SOC 2 Examinations

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

N = 75	6–10 wks	71%	88%
Completed SOC 2 Examinations	Typical Formal Fieldwork Window	With ≥1 Exception (53 of 75)	Required Additional Evidence (66 of 75)

Lazarus Alliance, Inc.
CPA Firm · SOC 2 Examinations
A2LA-Accredited FedRAMP 3PAO • Authorized CMMC C3PAO (CPN 10251) • PCI DSS QSA • Veteran-Owned Small Business

Publisher: Lazarus Alliance, Inc., Scottsdale, Arizona

1. Purpose & Methodology

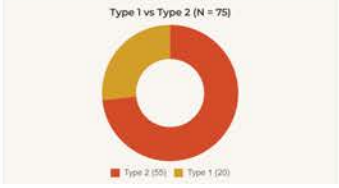
This benchmark report aggregates anonymized findings from **N = 75** SOC 2 examinations (Type 1 and Type 2) performed by Lazarus Alliance between January 2025 and June 2026. Figures represent observed patterns across the examination population and are intended to provide service organizations with realistic expectations for duration, evidence, exceptions, and scope decisions.

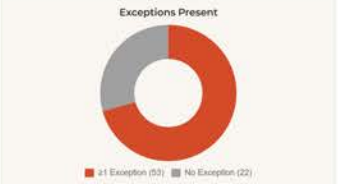
Scope of Data: Completed SOC 2 examinations only (readiness assessments and gap analyses excluded). Both first-time and renewal examinations are included. Trust Services Criteria combinations vary (Security only through full five-criteria reports). Percentages use N = 75 unless otherwise noted.

Disclaimer: *These benchmarks are observational and do not constitute guarantees of future performance, report outcomes, or timelines. Individual results vary based on control maturity, system description quality, evidence readiness, and scope. Lazarus Alliance maintains independence under AICPA professional standards.*

2. Executive Summary – Key Benchmarks

Metric	Observed Value	Notes
Sample size	**N = 75**	Completed SOC 2 Type 1 & Type 2 examinations
Typical formal fieldwork window	6–10 weeks	From kickoff / evidence acceptance to draft report
Examinations with ≥1 exception	71% (53 of 75)	Median 2 exceptions when present
Required additional evidence	88% (66 of 75)	At least one clarification cycle
Type 2 share of dataset	73% (55 of 75)	Type 1: 27% (20 of 75)
First-time vs renewal	42% first / 58% renewal	N = 75
Average evidence volume	~1,450 artifacts	Range roughly 400 – 4,200





3. How Long Does a SOC 2 Audit Take?

Quick Answer

Formal fieldwork for a SOC 2 examination typically runs **6–10 weeks** from kickoff / evidence package acceptance to draft report. End-to-end timelines including readiness, remediation, and report finalization commonly range from **3 to 9 months**, with Type 2 and first-time examinations generally taking longer than Type 1 and renewals.

Formal examination window

- **Typical formal fieldwork:** 6–10 weeks
- **Faster end of range:** Mature renewals with clean Type 2 observation periods and complete evidence
- **Longer end of range:** First-time Type 2 examinations, multi-criteria scope, or significant mid-exam evidence remediation

End-to-end phases

Phase	Typical Duration	Notes
Readiness / gap analysis	4–12 weeks	Control design, system description, evidence planning
Remediation & evidence packaging	4–16 weeks	Longer for first-time Type 2 (observation period)
Formal examination fieldwork	6–10 weeks	Kickoff → draft report
Exception remediation & report finalization	2–6 weeks	Depends on exception severity and management response

Type 2 examinations require an observation period (commonly 3–12 months). That period is not part of formal fieldwork duration but is a critical driver of overall calendar time to a Type 2 report.

Factors that shorten or lengthen duration

- **Shorten:** Complete system description, practice-mapped evidence, mature access/logging/change controls, prior SOC 2 experience, focused criteria set
- **Lengthen:** First-time examinations, incomplete evidence, multi-criteria scope without preparation, weak system description, mid-exam control gaps

4. 7 Most Common SOC 2 Audit Exceptions

Across N = 75 examinations, **71% (53 of 75)** had at least one exception. When exceptions were present, the median number was **2**. The following areas generated exceptions most frequently:

#1
Access Control & User Provisioning
Incomplete joiner/mover/leaver evidence, delayed deprovisioning, or insufficient periodic access reviews. Least-privilege not fully evidenced for privileged roles.

#2
Change Management
Changes implemented without complete approval trails, missing testing evidence, or emergency changes not retrospectively documented.

#3
Logging, Monitoring & Alerting
Incomplete log coverage for in-scope systems, alerts not reviewed on defined cadence, or retention gaps during the observation period (Type 2).

#4
Risk Assessment & Vendor Management
Risk assessments not updated on the stated cadence; vendor due diligence incomplete for critical subservice organizations; SOC reports from vendors not obtained or reviewed.

#5
System Description Accuracy
System description that does not match the implemented environment, incomplete boundary, or missing complementary user entity controls (CUECs).

#6
Security Configuration & Vulnerability Management
Baselines not maintained; vulnerability scanning incomplete or remediation outside stated SLAs without documented risk acceptance.

#7
Incident Response & Continuity Testing
Incident response or disaster recovery plans exist but lack evidence of testing within the required period; lessons-learned not documented.

Exceptions related to multi-factor authentication coverage, encryption key management, and board/management oversight also appeared, particularly in first-time examinations.

5. How Much Evidence Does a SOC 2 Audit Require?

Quick Answer

Average evidence volume was **~1,450 discrete artifacts** (range roughly 400–4,200). **88% (66 of 75)** of examinations required at least one round of additional evidence. Quality and mapping to Trust Services Criteria matter more than raw file count.

Metric	Value
Average discrete artifacts	~1,450
Observed range	~400 – 4,200
Required additional evidence	88% (66 of 75)
Most common additional requests	Access reviews, change tickets, log samples, vendor SOC reports, system description updates

Common evidence deficiencies

- Screenshots without dates, system identifiers, or context
- Policies without operational proof (tickets, reviews, logs)
- Incomplete samples for the Type 2 observation period
- System description that drifts from the live environment
- Missing vendor SOC reports or due-diligence records for critical subservice organizations
- Access reviews that are incomplete or not performed on the stated cadence

Organizations that pre-mapped controls to evidence and maintained living system descriptions required fewer clarification cycles.

6. SOC 2 Type 1 vs Type 2: What Our Audit Data Shows

Attribute	Type 1	Type 2
Share of dataset	27% (20 of 75)	73% (55 of 75)
Focus	Design of controls at a point in time	Design + operating effectiveness over a period
Typical formal fieldwork	Often shorter (lower end of 6–10 weeks)	Full 6–10 weeks more common
Evidence demand	Lower (point-in-time)	Higher (observation period samples)
Exception rate	Somewhat lower	Higher — operating effectiveness is tested
Common use case	First report, rapid market need	Customer / enterprise requirement; ongoing assurance

Type 2 reports dominate the dataset and customer demand. Type 1 remains useful as a first step or when a point-in-time design opinion is sufficient. Organizations moving from Type 1 to Type 2 should plan for a full observation period and stronger operational evidence — the step-up in evidence rigor is material.

7. First SOC 2 Audit vs. Renewal: What the Data Shows

Attribute	First-Time	Renewal
Share of dataset	42% (32 of 75)	58% (43 of 75)
Typical duration	Longer end of range	Shorter end of range
Exception rate	Higher	Lower
Evidence readiness	More clarification cycles	More complete packages
System description	Often immature	Usually refined from prior year

First-time examinations consumed more calendar time and generated more exceptions and evidence requests. Renewal examinations benefited from prior system descriptions, established control ownership, and institutional knowledge of sampling and evidence expectations. Organizations preparing for a first SOC 2 should budget extra time for system description quality and operational evidence, not only policy documentation.

8. Scope & Complexity

Trust Services Criteria selection

- **Security only** — most common starting point; still the majority of first-time reports
- **Security + Availability** — frequent for SaaS and infrastructure providers
- **Security + Confidentiality** — common when handling sensitive customer data
- **Three or more criteria** — more common in renewals and enterprise-facing providers; higher evidence and testing load

Scope drivers of effort

- **System boundary clarity** — well-defined product / service boundaries reduced testing friction
- **Number of in-scope systems and locations** — multi-product or multi-region environments increased sampling and evidence volume
- **Subservice organizations** — critical vendors without current SOC reports created exceptions and follow-up
- **Criteria count** — each additional Trust Services Category expands control population and evidence demand
- **Type 2 observation period length** — longer periods require more samples and sustained control operation

Practical scoping guidance

1. Start with a clear system description and boundary before expanding criteria.
2. Prefer a clean Security-only Type 1 or Type 2 over a rushed multi-criteria first report.
3. Identify critical subservice organizations early and obtain their SOC reports.
4. For Type 2, align observation period length with operational readiness — longer is not always better if controls are not stable.
5. Treat renewals as an opportunity to refine scope and system description, not only to "pass again."

9. Key Insights for Service Organizations

- **1. Budget real time for the system description.** Inaccurate or incomplete descriptions drive exceptions and delay.
- **2. Map evidence to criteria before fieldwork.** 88% of examinations still needed additional evidence; pre-mapping reduces cycles.
- **3. Expect exceptions.** 71% of examinations had at least one; quality of management response matters.
- **4. Type 2 is a different evidence game than Type 1.** Plan the observation period deliberately.
- **5. First-time audits cost more calendar time.** Renewals benefit from institutional knowledge — invest in that knowledge early.
- **6. Scope discipline pays off.** Clear boundaries and right-sized criteria sets outperform ambitious, under-prepared scopes.

10. Authors, Reviewers & How to Cite

Lead Author
Michael D. Peters, CEO & Founder, Lazarus Alliance, Inc.
Delaware CPA firm principal; A2LA-accredited FedRAMP 3PAO; Authorized CMMC C3PAO; PCI DSS QSA. 26+ years in proactive cybersecurity, audit, and compliance.

Technical Review
SOC 2 Examination Team, Lazarus Alliance (AICPA professional standards).

How to Cite This Report
Peters, M. D. (2026). *2026 SOC 2 Audit Benchmark Report: Aggregate Anonymized Insights from Lazarus Alliance SOC 2 Examinations* (Version 1.0). Lazarus Alliance, Inc. https://lazarusalliance.com/2026-soc-2-audit-benchmark-report/

Recommended short citation: Lazarus Alliance (2026). 2026 SOC 2 Audit Benchmark Report (N=75).

11. About & Contact

Lazarus Alliance is a Delaware CPA firm providing SOC 2 examinations, 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 SOC 2 Audit Benchmark Report

Additional Analysis

1. How Long Does a SOC 2 Audit Take?
2. 7 Most Common SOC 2 Audit Exceptions
3. How Much Evidence Does a SOC 2 Audit Require?
4. SOC 2 Type 1 vs Type 2: What Our Audit Data Shows
5. First SOC 2 Audit vs. Renewal: What the Data Shows
6. Scope & Complexity

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

(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

Submit

Looking for something?

Search Go