Continuum GRC · FedRAMP Authorized GRC Platform · Roadmap to Risk Reduction

CONTINUUM GRC
Your Roadmap to Risk Reduction

August 2026
Confidential customer-benchmark analysis
N = 275 programs

2026 AUDIT READINESS BENCHMARK REPORT

AUDIT READINESS & EVIDENCE MANAGEMENT

sufficient evidence.

1,842
Average unique artifacts per program

2.6
Average artifacts mapped per control

41 vs 127
Median evidence age (days): continuous vs. manual

74%
Prep-time reduction in high-automation programs

EXECUTIVE SUMMARY

9%
Controls with zero mapped evidence at assessment start

31%
Controls with at least one required artifact older than 90 days

5.8 wks
Average evidence-package assembly time across all programs

The decisive differentiator is not how much evidence exists, but whether it is current, attributed, mapped to the exact control or objective, and retrievable without reconstruction. Lazarus Alliance assessments have consistently shown that a large share of initial findings stem from incomplete evidence of ongoing operation rather than missing technical controls.

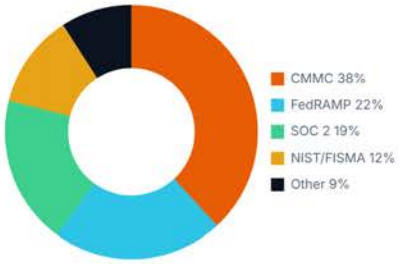
> Continuum GRC customers that treat evidence as an operational byproduct — not a pre-audit project — enter assessments with fewer gaps, fewer last-minute requests, and shorter fieldwork. High-automation programs assembled packages in 2.3 weeks versus 9.4 weeks for largely manual peers.

STUDY METHODOLOGY

Data was drawn from 275 active Continuum GRC customer programs spanning January 2025–June 2026. Metrics reflect in-platform evidence inventories, control mappings, timestamps, collection method (integration/scheduled vs. manual), and assessment-related activity.

Programs range from mid-market defense contractors and SaaS providers to larger enterprise and cloud environments. All figures are anonymized aggregates. "Evidence" means a distinct mapped artifact: policy, procedure, configuration export, log extract, ticket, review record, screenshot with metadata, or test result.

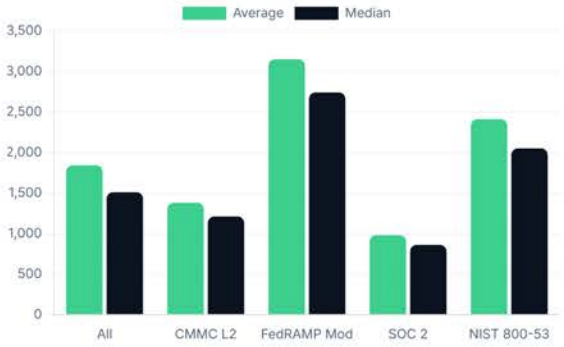
Sample mix by framework



EVIDENCE VOLUMES

Volume is high and highly variable. More artifacts do not automatically mean better coverage. Top-quartile readiness programs did not have the highest raw counts — they had tighter mapping and less duplication.

Average unique artifacts by framework



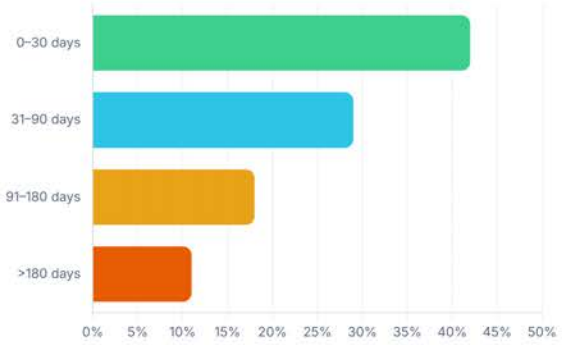
Segment	Average	Median	Typical range
All programs (N=275)	1,842	1,510	420–7,800+
CMMC Level 2	1,380	1,210	650–2,900
FedRAMP Moderate	3,150	2,740	1,800–8,200
SOC 2 Type II	980	860	420–2,100
NIST 800-53 / FISMA-style	2,410	2,050	1,100–5,400

FedRAMP volumes are driven by control count (~323 at Moderate), inheritance documentation, and technical testing. CMMC volumes are driven by 110 practices plus ~320 assessment objectives. SOC 2 volumes are lower because of a smaller control set and heavier reuse of system-generated evidence.

EVIDENCE AGE & FRESHNESS

Auditors evaluate whether a control operated during the period, not whether a document exists today. Stale evidence is one of the most common sources of follow-up and findings.

Age distribution of mapped artifacts



Freshness snapshot

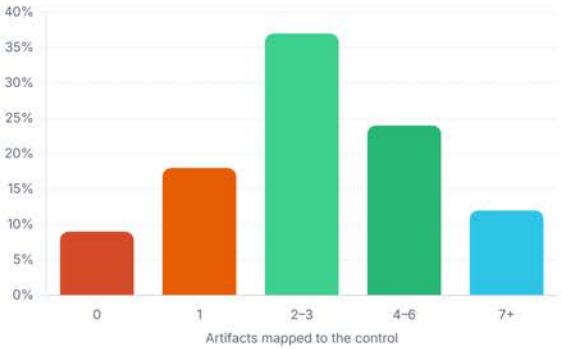
Metric	Value
Share of artifacts 0–30 days	42%
Share 31–90 days	29%
Share 91–180 days	18%
Share older than 180 days	11%
Median age — continuous / integrated	28 days
Median age — manual upload	94 days

> Evidence older than ~90 days at submission often fails the contemporaneous-operation test for Type II and period-based assessments. Reconstruction after the fact is visible to experienced assessors.

CONTROL-TO-EVIDENCE RATIOS

Sufficiency is both quantity and quality. A single policy rarely proves operating effectiveness. Overall average: **2.6 artifacts per in-scope control**. Top-quartile programs averaged 3.4, with near-zero unmapped controls.

Mapped artifacts per control



Artifacts mapped	Share of controls	Coverage
0	9%	
1	18%	
2–3	37%	
4–6	24%	
7+	12%	

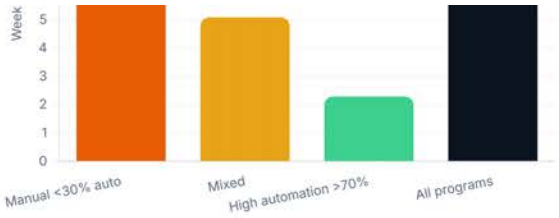
High performers typically followed a practical rule of three for operational practices: written policy or standard, procedure/runbook, and a dated artifact proving the procedure ran. Controls most likely to have zero or one artifact: audit-review practices, account-management recertification, media protection, and poorly documented inheritance.

AUDIT PREPARATION

Preparation time is the visible cost of an evidence program that is not continuous. 62% of programs still reported last-minute evidence requests or at least one artifact rejected for incompleteness, missing attribution, or age.

Package-assembly time by collection maturity

Collection maturity	Typical time	Effort
Largely manual (<30% automated)	9.4 weeks	~220 hours
Mixed	5.1 weeks	~110



		hours
High automation / continuous (>70%)	2.3 weeks	~48 hours
All programs (average)	5.8 weeks	—

Most frequent bottlenecks

01
Chasing owners for dated operating evidence

02
Re-exporting cloud, IdP, and SIEM reports that had already aged

03
Remapping after scope or inheritance changes

BENEFITS OF AUTOMATION

Among Continuum GRC programs using A.ITAMBot™ for control narratives, SSP language, procedure drafts, evidence mapping, and readiness write-ups, technical writing and audit-readiness authoring accelerated by **92%** versus the same work performed manually.

92%
FASTER

A.ITAMBot™ accelerates technical writing and audit readiness

Measured across authoring tasks in the N=275 sample: system security plan narratives, control implementation statements, policy and procedure drafts, evidence-to-control mapping notes, gap write-ups, and POA&M language. Manual baseline for this workstream: 208 hours. A.ITAMBot-assisted baseline: 17 hours.

191 hrs
Labor hours avoided per assessment writing cycle

$23,875
Direct labor savings per cycle at $125 fully loaded hourly rate

$47,750
Annualized savings at two writing/readiness cycles per year

208 → 17
Hours of technical writing and readiness authoring, before vs. after A.ITAMBot

Labor hours by authoring task

Labor cost by authoring task ($125/hr)

Authoring workstream	Manual hours	A.ITAMBot hours	Time saved	Labor saved
SSP / control implementation narratives	96	8	88 hrs (92%)	$11,000
Policy and procedure drafts	40	3	37 hrs (93%)	$4,625
Evidence mapping and implementation statements	48	4	44 hrs (92%)	$5,500
Readiness gaps, findings language, and POA&M text	24	2	22 hrs (92%)	$2,750
Total technical writing & readiness authoring	**208**	**17**	**191 hrs (92%)**	**$23,875**

Where the 92% shows up in practice

Technical writing

Audit readiness

Labor and calendar

- First-draft SSP and control narratives from mapped evidence and live control context
- Consistent language across CMMC, FedRAMP, SOC 2, and NIST libraries
- Fewer rewrite cycles caused by incomplete or stale source material

- Gap write-ups and objective-level coverage notes produced as evidence is mapped
- POA&M and remediation language generated from the same control record
- Assessor-facing packages that start from current, hashed artifacts instead of reconstructed prose

- 191 hours returned to control owners and compliance staff each cycle
- Writing workstream compressed from roughly five weeks to about two days
- Stackable with the broader 74% package-assembly reduction in high-automation programs

Labor dollars use a blended fully loaded rate of **$125 per hour** (compliance analyst, control owner, and technical writer mix). Figures cover authoring and readiness writing only. They do not include assessor fees, tooling licenses, or remediating failed controls. High-automation collection remains a separate 74% reduction in package-assembly time (220 hours → 48 hours).

FRAMEWORK-SPECIFIC INSIGHTS

CMMC Level 2

The evidence gap is operational, not documentary. Assessors expect policy → procedure → dated proof of execution, often across 90+ days. Inheritance and CRM quality remain frequent weak points. Artifact hashing and six-year retention raise the bar on integrity and indexing.

FedRAMP

Volume and inheritance documentation dominate. 3PAO packages require technical test results, SSP/SAP/SAR alignment, and continuous-monitoring artifacts. Reused SOC 2 or NIST evidence still needed re-formatting and FIPS/boundary alignment.

SOC 2 Type II

Smaller control set and heavier reliance on system-generated evidence. Freshness and period coverage matter more than raw count. Programs already collecting continuously for CMMC or FedRAMP typically reused 35–45% of artifacts.

Cross-framework reuse averaged **41%** of artifacts among programs that maintained a unified control library.

WHAT HIGH PERFORMERS DO DIFFERENTLY

- Evidence is generated by operations (scheduled reviews, ticket workflows, integrations), not assembled for the audit.
- Every in-scope control or objective has an owner and a defined evidence standard before collection starts.
- Artifacts are mapped once and reused; inheritance and shared-responsibility matrices are living documents.
- Freshness is measured monthly (median age, percent older than 90 days) as a standing KPI.
- The assessor package is an export of an already-current repository — index, hashes, timestamps — not a new project.

RECOMMENDATIONS

1. Set an evidence standard per control family. Default for operational practices: policy + procedure + operating artifact.
2. Drive the unmapped-control rate below 3% and the >90-day artifact rate below 15% before scheduling fieldwork.
3. Automate recurring operational evidence: access reviews, log reviews, vulnerability remediation, training, and configuration drift.
4. Maintain a single mapped library. Do not collect the same proof separately for each framework.
5. Measure two ratios monthly: percent of controls with current evidence, and median artifact age.
6. Hash and index the assessment set. Retain per framework rules (six years for CMMC artifacts from status date).

CONTINUUM GRC AND CONTINUOUS READINESS

Continuum GRC (IT Audit Machine®) and A.ITAMBot™ were built for this problem: centralized evidence, control-to-artifact mapping, scheduled and integrated collection, cryptographic hashing, inheritance and CRM support, readiness dashboards, and assessor-ready exports. In this sample, A.ITAMBot accelerated technical writing and audit-readiness authoring by 92%, turning a 208-hour writing cycle into 17 hours and avoiding approximately $23,875 in labor per cycle.

Customers that used those capabilities at high maturity entered assessments with fewer gaps and substantially less scramble. The 2026 data is unambiguous. Audit readiness is an evidence-management discipline. Volume without freshness and mapping creates work. Continuous, mapped, dated evidence — and AI-assisted technical writing — creates a defensible posture.

CONTINUUM GRC | Lazarus Alliance

Source: Anonymized aggregate data from 275 Continuum GRC customer programs, January 2025–June 2026.

For methodology questions or a program-specific benchmark comparison, contact Continuum GRC.

2026 Audit Readiness Benchmark Report

REQUEST A PERSONALIZED DEMO

Speak with our team using the form below or call us at 1-888-896-6207 for assistance.

Name *

First | Last

Email *

Email | Confirm Email

Phone

(201) 555-0123

Company *

How may we assist you? *

Do you want Managed Services, or Readiness Services? *

- [ ] Risk Management Services
- [ ] Compliance Management Services
- [ ] Readiness Services and Technical Writing
- [ ] Something not listed?

What type of subscription are you interested in? *

- [ ] MSP (Provider Managing Multiple Clients)
- [ ] Enterprise (Managing your Company)
- [ ] Subscribers (Limited Access to Pre-Configured Modules)

- [ ] Something not listed?

Did you want to become an integration partner?

- ○ Yes
- ○ No

What questions do you have? *

What is your hosting preference?

- ○ AWS Hosting (Commercial)
- ○ FedRAMP Authorized AWS GovCloud hosting (Federal and State Government)
- ○ AWS EU Hosting (Commercial)

Which services are you interested in? *

- [ ] GovRAMP
- [ ] FedRAMP
- [ ] SOC 1-2-3
- [ ] CMMC, NIST 800-171 & 800-172
- [ ] NIST 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
- [ ] COSO SOX
- [ ] NERC CIP
- [ ] CIS
- [ ] MPA Content Security Best Practices (TPN)
- [ ] FTC SafeGuards
- [ ] CTPAT
- [ ] ITAR
- [ ] EUCS
- [ ] SSDF NIST 800-218
- [ ] Something not listed

Which Governance & Policy subscription modules are you interested in? *

- [ ] GovRAMP
- [ ] FedRAMP
- [ ] SOC 1-2-3
- [ ] CMMC, NIST 800-171 & 800-172
- [ ] C5 ENS EUCS
- [ ] PCI DSS QSA & SAQ
- [ ] ISO
- [ ] HIPAA NIST 800-66

- [ ] Privacy, CCPA, CPRA, PIPEDA, DPIA, LGPD
- [ ] CJIS
- [ ] NIST 800-53
- [ ] NERC CIP
- [ ] SEC, NFA & FINRA
- [ ] Something not listed

Download our company brochure.

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

Success! CLOUDFLARE Privacy • Help

Submit

Looking for something?

Search Go