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

CONTINUUM GRC
Your Roadmap to Risk Reduction

August 2026
Independent customer-benchmark study
N = 275 programs

2026 COMPLIANCE OPERATIONS BENCHMARK REPORT

MONITORING, FINDINGS & DAY-TO-DAY CONTROL WORK

42%
Programs with continuous or monthly control testing on critical controls

38 days
Median time to close a compliance finding

2.4 FTE
Median internal compliance operations capacity (dedicated + matrixed)

61%
Operational work still driven by calendar, not by live control health

Executive summary | Methodology | Operations maturity | Monitoring & testing | Findings & exceptions | Policy operations | Team capacity | Time, labor & cost | Automation | Recommendations

EXECUTIVE SUMMARY

61%

Still run primarily on a pre-assessment calendar rather than continuous control health

38 days

Median days to close a compliance finding after it is logged

520 → 210

Annual operational hours, reactive programs versus automated continuous ops

Compliance operations is the work between assessments: testing controls, closing findings, refreshing policies, handling exceptions, and reporting status. In this sample, the programs that treated that work as a standing operating system — with owners, SLAs, and automated evidence — spent less than half the annual hours of programs that still surge before each audit. The gap is not ambition. It is cadence, ownership, and whether the GRC platform is the system of record for day-to-day work or only a pre-audit file cabinet.

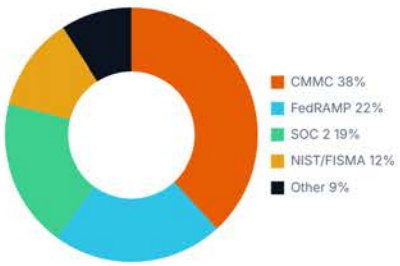
> Labor figures use a **$125 per hour** fully loaded blended rate. They cover internal monitoring, finding management, policy lifecycle, exception handling, and operational reporting. They exclude external assessor fees, remediation of failed technical controls, and one-time audit package assembly (covered in separate readiness analysis).

STUDY METHODOLOGY

Independent analysis of 275 active Continuum GRC customer programs from January 2025 through June 2026. Operational metrics are taken from in-platform task history, finding records, policy review dates, monitoring schedules, and reported FTE allocation for compliance operations roles.

Framework mix: CMMC 38%, FedRAMP/StateRAMP 22%, SOC 2 19%, NIST 800-53/FISMA 12%, other (PCI, ISO, CJIS, ITAR) 9%. Organization sizes range from mid-market to large enterprise; defense, cloud, and regulated commercial sectors dominate the sample.

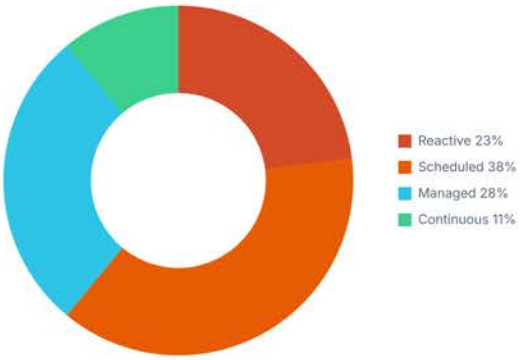
Sample mix by primary framework



OPERATIONS MATURITY

Four bands describe how programs run between formal assessments. Most sit in the middle: some scheduled testing, findings tracked in a tool, but still a large pre-assessment surge.

Operations maturity bands

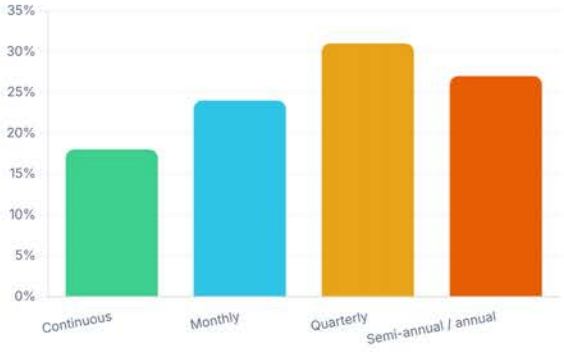


Band	Share	Typical pattern
Reactive	23%	Work spikes before assessment; thin monitoring between cycles
Scheduled	38%	Calendar-driven tests and policy reviews; findings closed slowly
Managed	28%	Owners, SLAs, continuous evidence on critical controls
Continuous	11%	Live control health, automated tickets, minimal pre-audit surge

MONITORING & TESTING

Critical controls that are tested only annually are the ones that fail late. Programs with monthly or continuous testing on high-risk families (access, logging, vulnerability, change) carried fewer last-minute findings.

Testing cadence for critical controls



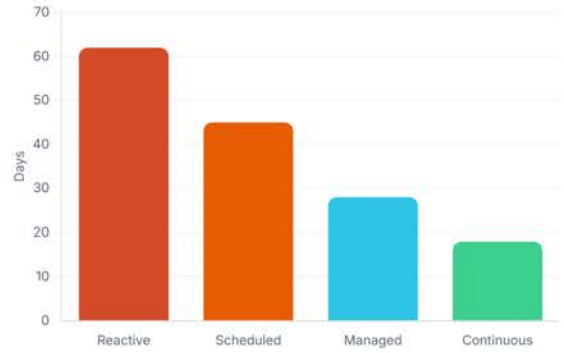
Cadence	Share of programs	Coverage
Continuous / automated	18%	
Monthly	24%	
Quarterly	31%	
Semi-annual or annual only	27%	

42% of programs test critical controls at least monthly (continuous + monthly). Those programs reported a median of 34% fewer open findings in the 60 days before formal assessment than annual-only programs.

FINDINGS, EXCEPTIONS & CLOSURE

Finding volume is less predictive of program health than age and ownership. Median time to close was 38 days. The worst quartile sat above 75 days — long enough for the same issue to reappear in the next assessment window.

Median days to close a finding



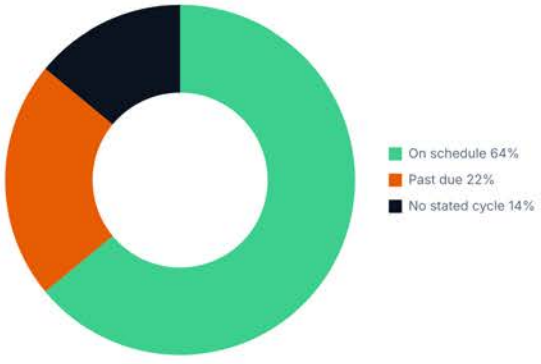
Finding and exception snapshot

Metric	Value
Median open findings at any time	14
Median days to close (all findings)	38
Median days to close (critical / high)	22
Findings older than 90 days	19%
Programs with formal exception register	47%
Exceptions with documented compensating control	61% of exceptions

POLICY OPERATIONS

Policy work is operational only when reviews, approvals, and acknowledgments run on a schedule with owners. Annual “policy day” still dominates a large share of the sample.

Policy review cadence



Metric	Value
Median policies in the controlled set	28
Policies reviewed on schedule (last cycle)	64%
Policies past stated review date	22%
Employee acknowledgment completion (required policies)	81%
Programs with automated acknowledgment workflow	53%

TEAM CAPACITY

2.4
Median FTE dedicated to compliance operations (full-time + matrixed)

47%
Of operational hours spent chasing owners and evidence, not analysis

1.6×
Pre-assessment month workload versus average month in reactive programs

Capacity is not only headcount. Reactive programs reported the same median FTE as managed programs but spent nearly half of those hours on chase-and-collect work. Continuous programs redirected that time into risk decisions, vendor oversight, and control improvement. Automation did not replace FTEs in this sample; it changed what those FTEs did.

TIME, LABOR & COST

Annual operational hours exclude formal assessment package assembly. They cover monitoring, finding management, policy lifecycle, exceptions, and internal reporting. Rate: **$125 per hour** fully loaded.

520 hrs
Annual operational hours, reactive programs

$65,000
Reactive annual labor at $125/hr

210 hrs
Annual hours, continuous / automated operations

$26,250
Continuous annual labor — 60% below reactive

Maturity	Annual hours	Annual labor	Median days to close finding	Versus reactive
Reactive	520	$65,000	62	Baseline
Scheduled	390	$48,750	45	−25%
Managed	280	$35,000	28	−46%
Continuous / automated	210	$26,250	18	−60%

Median annual labor avoided when a reactive program reaches continuous operations: **$38,750** ($65,000 → $26,250). Finding closure time falls from 62 days to 18 days in the same transition.

AUTOMATION OF COMPLIANCE OPERATIONS

60%
LESS LABOR

Continuous operations cut annual operational hours by 60%

Reactive programs: 520 hours / $65,000. Continuous and automated programs: 210 hours / $26,250. A.ITAMBot™ further accelerates policy drafts, finding narratives, and control-status write-ups by 92% on the authoring share of that work.

What high performers automate

What still needs humans

A.ITAMBot in operations

- Scheduled evidence collection for critical controls
- Finding tickets with owners and due dates from the GRC system
- Policy review reminders and acknowledgment workflows
- Exception register with compensating-control linkage

- Risk acceptance and residual-risk decisions
- Root-cause analysis on recurring findings
- Scope and inheritance changes
- Assessor interaction and live demonstrations

- 92% faster drafts for policy updates and finding responses
- Consistent language across control families and frameworks
- Less time rewriting the same narrative each cycle

RECOMMENDATIONS

1. Move critical controls (access, logging, vulnerability, change) to at least monthly testing. Annual-only testing is where late findings concentrate.
2. Give every finding an owner and a target close date on the day it is logged. Median closure should sit under 30 days for high-severity items.
3. Treat the exception register as a controlled list with compensating controls and review dates — not a permanent waiver pile.
4. Run policy reviews and acknowledgments on a standing schedule inside the GRC platform, not as a once-a-year campaign.
5. Measure two operational KPIs monthly: percent of critical controls tested on schedule, and median age of open findings.
6. Use Continuum GRC workflows and A.ITAMBot so operational hours go to decisions, not to hunting evidence and rewriting prose.

CONTINUUM GRC AND COMPLIANCE OPERATIONS

Continuum GRC (IT Audit Machine®) and A.ITAMBot™ are built for the work between assessments: continuous evidence, finding and exception workflows, policy lifecycle, and AI-assisted operational writing. In this sample, continuous and automated programs ran compliance operations at about 210 hours a year versus 520 hours for reactive programs — a 60% reduction — while cutting median finding closure time from 62 days to 18 days.

Compliance operations is not a smaller version of the audit. It is the system that makes the next audit uneventful. The benchmark is whether control health is visible every month, findings close on time, and the team's hours go to judgment rather than collection.

CONTINUUM GRC | Lazarus Alliance

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

For a program-specific compliance operations comparison, contact Continuum GRC.

Download 2026 Compliance Operations 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