



news · Jan 20, 2026

State of GRC 2026: Benchmarks, Trends, and What's Actually Changing

An authoritative look at the state of GRC in 2026 — regulatory shifts, framework adoption, budget benchmarks, automation trends, and what's ahead for 2027.

 Justin Leapline

On this page

Governance, risk, and compliance doesn't look anything like it did five years ago. The compliance team that was a backwater cost center in 2020 is now the difference between closing enterprise deals and watching them slip to competitors. The auditor who used to come once a year now wants continuous evidence. The "annual risk assessment" is giving way to real-time dashboards.

This is our 2026 State of GRC report — a synthesis of what we're seeing across hundreds of conversations with GRC practitioners, audit firms, security leaders, and buyers. We've combined that with publicly available regulatory guidance, industry survey ranges, and what our customers actually do day-to-day. The goal: give GRC leaders, founders, and practitioners a clear, honest snapshot of where the industry stands and where it's heading.

No vendor chest-thumping. No fabricated precision. Just the practical picture as we see it.

Executive Summary

The headline findings from this year's analysis:

- **Multi-framework is the new normal.** Most mid-market and enterprise organizations we work with are now managing three or more frameworks concurrently. Single-framework programs are increasingly rare outside of very early-stage startups.
- **Regulatory volume is accelerating, not stabilizing.** Between NIST CSF 2.0, PCI DSS v4.0.1, CMMC rollout, the EU AI Act, and the ongoing wave of US state privacy laws, compliance teams are absorbing more net-new regulatory requirements in 2026 than in any recent year.
- **Automation has crossed the chasm.** AI-assisted evidence collection, control mapping, and questionnaire response are no longer experimental. Practitioners who haven't adopted some form of automation are falling behind on capacity, not sophistication.
- **Compliance budgets are growing — but not as fast as requirements.** Industry benchmarks suggest GRC spend has been climbing steadily, but regulatory scope is growing faster. That gap is where burnout lives.
- **Vendor risk is the weakest link.** Third-party and supply chain incidents continue to dominate the breach headlines. Most TPRM programs are still catching up.
- **Team burnout is a measurable problem.** The compliance practitioners we speak to report unsustainable workloads. Turnover in GRC leadership roles is higher than it

was three years ago.

- **The GRC category is maturing.** The platforms, the language, the expectations from auditors and buyers — all of it is converging toward a more mature, continuous, automation-forward model.

Let's dig in.

Section 1: The Shifting Regulatory Landscape

If there's one theme that defines 2026, it's that the regulatory environment isn't settling down. Every year for the past decade, we've heard some version of "compliance will stabilize once X gets finalized." It never does. If anything, the pace is picking up.

NIST CSF 2.0 Is Reshaping Internal Frameworks

NIST CSF 2.0, released in February 2024, has quietly become one of the most influential changes to GRC programs in a decade. The addition of the **Govern** function elevated cybersecurity from a technical concern to a board-level governance issue. That change is now showing up in how organizations structure their internal programs.

We're seeing a meaningful number of organizations restructure their internal risk frameworks around CSF 2.0's six functions (Govern, Identify, Protect, Detect, Respond, Recover), even when they're ultimately audited against SOC 2 or ISO 27001. NIST CSF works as a connective tissue — a [framework of frameworks](#) that maps cleanly to nearly everything else.

PCI DSS v4.0.1: The End of the Grace Period

PCI DSS v4.0 brought significant changes, and the grace period for "best practice" requirements ended March 31, 2025. As of 2026, those requirements are fully enforceable — and we're seeing the consequences in the field. Organizations that deferred their 4.0 readiness work are now paying for it in rushed remediation, expanded scopes, and more expensive assessments.

Key provisions now in full effect:

- Multi-factor authentication for all access into the cardholder data environment
- Minimum 12-character passwords (up from 7)
- Client-side script integrity monitoring (in response to Magecart-style attacks)
- Targeted risk analyses for several specific requirements
- The Customized Approach, which adds flexibility but requires significantly stronger documentation

For deeper PCI guidance, see our [PCI DSS framework overview](#) and [compliance levels breakdown](#).

CMMC Is Moving From Theory to Reality

The DoD's Cybersecurity Maturity Model Certification program has shifted from "coming soon" to "happening now." The final rule (32 CFR Part 170) and the acquisition rule changes (48 CFR) are reshaping procurement for the Defense Industrial Base.

What we're observing in 2026:

- **Level 1 self-assessments** are ramping up significantly as primes push requirements down to subcontractors.
- **Level 2 C3PAO assessments** are backlogged in many regions, with waits extending multiple months.
- **Level 3 DIBCAC assessments** remain rare but are increasingly visible in conversations among defense contractors.

Companies that waited to begin CMMC preparation are now discovering that the assessor ecosystem doesn't have infinite capacity. Many are finding that their target certification dates slipped because of queue times, not readiness gaps. See our [CMMC implementation timeline](#) and [CMMC levels guide](#) for practical planning.

The EU AI Act Is Creating a New GRC Discipline

The EU AI Act is the first comprehensive, risk-based regulation for artificial intelligence. Its risk tiers — unacceptable, high, limited, and minimal — impose obligations that GRC teams are now being asked to operationalize. This includes:

- Documented risk management systems for high-risk AI
- Data governance and training data quality requirements
- Technical documentation and record-keeping
- Transparency and human oversight controls
- Post-market monitoring obligations

Many organizations are extending their existing ISMS to cover AI governance, often mapping AI controls against ISO/IEC 42001. We expect AI governance to become a standing element of enterprise GRC programs within the next 12-18 months.

State Privacy Laws: The Patchwork Continues

The US state privacy law landscape keeps expanding. California, Virginia, Colorado, Connecticut, Utah, Iowa, Indiana, Tennessee, Texas, Oregon, Montana, Delaware, New Jersey, New Hampshire, Kentucky, Minnesota, Maryland, and more — each with overlapping but distinct requirements. There is still no federal privacy law consolidating this mess.

For most mid-market companies, the practical approach is to align to the most restrictive applicable law (typically CCPA/CPRA in California or the broader interpretations emerging in Colorado) and treat that as the floor for privacy program design. We'll say this with confidence: **if you're still operating on a state-by-state compliance basis instead of a unified privacy program, you're wasting cycles.**

Section 2: Framework Adoption Trends

We're seeing clear directional shifts in which frameworks are growing, which are plateauing, and how organizations are sequencing their compliance strategy.

Which Frameworks Are Growing Fastest

Based on what we observe across our customer base and conversations with the broader GRC community:

Framework	Adoption Trajectory	Primary Driver
SOC 2 Type II	Still growing	US enterprise buyer demand
ISO 27001:2022	Accelerating	International expansion, Annex A modernization
CMMC Level 2	Rapidly growing	DoD contract requirements
ISO/IEC 42001	Emerging	AI governance mandates
HITRUST CSF	Growing in healthcare	Payer and hospital preference
NIST CSF 2.0	Steady, foundational	Internal program structure
PCI DSS 4.0.1	Maintenance phase	Card brand enforcement
FedRAMP	Steady	Federal cloud procurement

A few observations worth calling out:

- **ISO 27001 is no longer just for international companies.** We're increasingly seeing US-headquartered SaaS companies pursue ISO 27001 in parallel with SOC 2 because enterprise buyers in regulated industries are starting to ask for it even in domestic deals.
- **CMMC is pulling in adjacent frameworks.** Organizations pursuing CMMC are often also evaluating FedRAMP, NIST 800-171, and NIST 800-53. These programs overlap substantially, and sophisticated GRC teams are building unified control catalogs.
- **ISO/IEC 42001 is the fastest-rising emerging framework.** Questions about AI management systems have moved from "what's that?" to "how do we get there?" inside of 18 months.

Multi-Framework Is the Default

In 2020, most early-stage SaaS companies were pursuing a single framework — usually SOC 2. In 2026, we rarely see companies stop at one. The typical trajectory we observe:

1. **Pre-Series A:** SOC 2 Type I as a starter.
2. **Series A–B:** SOC 2 Type II + ISO 27001.
3. **Series B+ in regulated verticals:** Add HIPAA, PCI DSS, HITRUST, or CMMC depending on industry.
4. **Enterprise / multinational:** Layer in GDPR operationalization, state privacy laws, AI Act compliance, and sector-specific frameworks.

By the time a company is past \$50M ARR in B2B SaaS, three or more active frameworks is the norm. This is why [control mapping across frameworks](#) has become such a critical capability — the overlap is where most of the leverage lives.

Sector Patterns

We see clear sector-based patterns in framework adoption:

- **B2B SaaS (horizontal):** SOC 2 Type II → ISO 27001 → selectively add sector-specific as buyers demand.
- **Healthtech:** HIPAA from day one, SOC 2 Type II early, HITRUST as enterprise health systems demand it.
- **Fintech:** SOC 2 Type II, PCI DSS (if applicable), and increasingly SOC 1 Type II for financial services customers.
- **Govtech / defense:** NIST 800-171 → CMMC Level 2 → FedRAMP where applicable.
- **AI / ML companies:** SOC 2 Type II, ISO 27001, and fast-moving toward ISO/IEC 42001.

Section 3: Cost and Resource Allocation

Let's talk numbers — with appropriate hedging. Compliance cost varies enormously based on scope, maturity, vertical, and tooling. That said, industry benchmarks give us workable ranges.

Typical GRC Budgets by Company Size

These are synthesized ranges based on what we see in the market. Treat them as rough order of magnitude, not precise benchmarks:

Company Size	Typical Annual GRC Spend	What's Included
Pre-seed / seed (under 25 employees)	\$20K–\$75K	First framework (often SOC 2 Type I), minimal tooling
Series A (25–75 employees)	\$75K–\$250K	SOC 2 Type II, basic GRC platform, fractional compliance lead
Series B (75–250 employees)	\$250K–\$750K	Multi-framework, full-time compliance lead, mature tooling
Growth stage (250–1,000 employees)	\$750K–\$2.5M	Compliance team, multiple frameworks, integrated tooling
Enterprise (1,000+ employees)	\$2.5M+	Dedicated GRC function, broad tooling stack, internal audit

GRC Headcount Benchmarks

A common question: "How big should our compliance team be?"

Rough industry benchmarks for mid-market B2B SaaS:

- **Under 100 employees:** 0.5–1.0 FTE dedicated to compliance (often a security engineer or CISO wearing the hat).
- **100–250 employees:** 1–2 dedicated FTE.

- **250–500 employees:** 2–4 dedicated FTE, typically including a compliance manager and analysts.
- **500–1,000 employees:** 4–8 FTE, often including a dedicated risk function.
- **1,000+ employees:** 8+ FTE with specialized roles (internal audit, privacy, risk, compliance operations).

Important caveat: these are benchmarks for companies with two to four active frameworks. Organizations with heavy regulatory exposure (healthcare, financial services, defense) run materially higher ratios.

Where the Money Goes

We see GRC spend broadly split across four categories:

Category	Typical Share of Budget
Audit and assessment fees	25–40%
Tooling and platforms	15–30%
Internal labor	25–45%
Remediation and implementation	10–25%

The ratio of tooling-to-labor has shifted meaningfully over the past five years. Organizations using modern **GRC platforms** spend a larger share on tooling and a smaller share on internal labor than those still running compliance on spreadsheets. Our **compliance cost benchmark** goes deeper on framework-by-framework costs.

Section 4: Automation Trends

Compliance automation has stopped being experimental. In 2026, we consider it table stakes. The question is no longer "should we automate?" but "how much of our program is automated, and how well?"

Where Automation Is Delivering Real Value

The highest-impact automation patterns we see consistently across our customer base:

- **Continuous control monitoring** — configuration checks running against cloud providers, identity systems, and endpoint fleets. Drift is detected in hours, not quarters.
- **Automated evidence collection** — integrations pull screenshots, reports, and logs on a schedule and attach them to the right controls. No more quarterly fire drills.
- **Control mapping across frameworks** — the single highest-value automation we see. Map a control once; satisfy requirements across every framework.
- **AI-assisted policy drafting and gap analysis** — reduces weeks of work to hours, though human review remains essential.
- **Questionnaire response automation** — security questionnaires that used to take a week now take a few hours.

Where Automation Falls Short

Automation isn't magic. The areas where it still underperforms expectations:

- **Nuanced risk assessment.** Automated risk scoring can produce misleading signals if the underlying asset and data inventories are weak.
- **Vendor risk scoring.** Most automated TPRM scoring is a useful triage tool, not a substitute for actual due diligence.
- **Evidence interpretation.** Collecting evidence is easy; knowing whether it actually demonstrates control effectiveness still requires human judgment.

The AI-in-GRC Reality Check

We're firmly in the early adoption phase for AI-powered GRC. A few honest observations:

- **AI drafting policies is genuinely useful**, but policies still need to reflect your actual environment, not a generic template.

- **AI-powered evidence interpretation is improving fast** but is not reliable enough to remove human review for audit-critical evidence.
- **Agents that autonomously handle compliance tasks end-to-end** exist in marketing decks more than in production environments. Practitioners should evaluate these with appropriate skepticism.

Section 5: Vendor Risk and Supply Chain

If one area of GRC is underinvested relative to its actual risk, it's third-party risk management (TPRM). Major incidents continue to originate from third parties — and we don't see the trend slowing.

What We're Observing

- **TPRM adoption is broad but shallow.** Most mid-market organizations have a vendor review process. Far fewer can confidently describe the real-time risk posture of their critical vendors.
- **Questionnaire fatigue is universal.** Both sides — buyers sending them and vendors answering them — describe the process as broken.
- **Trust centers and shared assurance models are gaining momentum.** Vendors who proactively publish certifications, reports, and standard responses significantly reduce questionnaire burden on both sides.
- **Fourth-party risk (your vendor's vendors) is emerging as a real concern,** particularly in critical supply chains.

Lessons From Major Incidents

Without naming specific companies: the pattern of supply chain incidents over the past two years has taught the industry a few recurring lessons.

1. **Static, point-in-time vendor assessments miss the real risk.** A vendor that was compliant last year may be compromised this quarter. Continuous monitoring of

- critical vendors is no longer a luxury.
2. **Concentration risk matters.** When a single upstream provider gets breached, it cascades to thousands of downstream organizations. Most TPRM programs do not map concentration risk well.
 3. **Incident response plans rarely account for third-party-origin incidents.** When the breach starts outside your perimeter, your standard IR playbook often doesn't apply cleanly.
 4. **Contractual controls are only as good as the verification behind them.** SLAs and security addenda are important, but they don't prevent incidents.

Section 6: Compliance Fatigue and Team Burnout

Let's be honest about something the industry doesn't talk about enough: the people doing this work are tired.

The Load Is Increasing Faster Than the Headcount

Across our conversations, compliance practitioners consistently describe:

- Managing more frameworks than they did two years ago, often with the same team size.
- Increasing volume and complexity of inbound security questionnaires.
- More frequent audits and assessments, with shorter gaps between them.
- Expanded scope to cover AI, privacy, and supply chain — often without corresponding budget increases.

Turnover in GRC Leadership

We're observing elevated turnover in senior GRC roles. The reasons are consistent:

- **Unrealistic timelines.** Boards ask for multiple frameworks simultaneously with insufficient resources.

- **Tooling gaps.** Programs that look sophisticated on paper often run on a patchwork of spreadsheets and manual processes.
- **Unclear ownership.** Compliance lives at the intersection of security, legal, IT, and HR. When accountability is diffuse, the compliance lead becomes the single point of failure.
- **Burnout compounding.** Audit cycles create recurring crunch periods. Without structural relief, each cycle gets harder.

What Actually Helps

We've watched teams recover from burnout. The patterns that work:

- **Automation investment**, especially in evidence collection and control mapping.
- **Clear ownership models** with named control owners outside the compliance function.
- **Realistic roadmaps** that sequence frameworks rather than stacking them.
- **Executive buy-in** that treats compliance as an operational capability, not a project.
- **Shared tooling** that gives every stakeholder visibility into the program without routing everything through the compliance lead.

Section 7: What's Ahead for 2027

Here's where we expect the next 12–18 months to take us. Call these educated predictions; we'll revisit them next year.

Predictions

1. **AI governance becomes a standard GRC workstream.** ISO/IEC 42001 adoption accelerates. Organizations that treat AI governance as "not compliance's job" will scramble to catch up.

2. **Continuous assurance pressures traditional audit cycles.** Auditors will increasingly rely on continuous evidence streams rather than point-in-time sampling. This is already happening quietly; it will become overt.
3. **CMMC enforcement reshapes the DIB supply chain.** Primes will push requirements more aggressively. Many sub-contractors will discover they missed the window.
4. **State privacy laws will continue proliferating**, with no federal preemption in sight. Unified privacy programs will become standard.
5. **Vendor risk management consolidates around trust-center models.** The questionnaire-as-default approach will fade in favor of shared assurance.
6. **Multi-framework-native platforms win.** Tools built for single-framework workflows will feel increasingly outdated against platforms designed for cross-framework operations.
7. **The compliance-as-growth-accelerator narrative goes mainstream.** More CFOs will treat GRC investment as revenue-enabling, not cost-center.
8. **Compliance automation commoditizes.** The table-stakes features of 2023 (integrations, evidence collection) will be baseline. Differentiation will shift to workflow, control mapping intelligence, and AI-native operations.

What Won't Change

A few things we don't expect to change meaningfully:

- **Compliance will still require judgment.** AI will handle more drafting and collection; humans will still make the decisions that matter.
- **Audits will still create crunch periods.** Even with continuous assurance, audit seasons will remain stressful.
- **Trust is still earned, not certified.** A report is a proxy for a program. Great programs produce great reports; the reverse isn't reliable.

Methodology Note

This report is a qualitative synthesis, not a formal quantitative survey. Our inputs:

- **Episki customer conversations and program reviews** across B2B SaaS, healthtech, fintech, and govtech verticals.
- **Practitioner interviews** with GRC leads, CISOs, and internal audit functions across multiple industries.
- **Public regulatory guidance** from NIST, AICPA, ISO, the PCI SSC, DoD, EU Commission, and US state attorneys general.
- **Publicly available industry benchmarks and survey data** from established security and compliance publications.
- **Audit firm and assessor commentary** shared in public-facing materials and industry conferences.

Where we give numeric ranges, those ranges represent directional benchmarks we observe in practice, not a single source of ground truth. Your program's reality may differ, and that's expected. We've deliberately avoided citing specific percentages to false precision; the goal here is orientation, not fabricated rigor.

FAQ

How many frameworks should a growing SaaS company plan for?

Most B2B SaaS companies we work with plan for three: SOC 2 Type II as the foundation, ISO 27001 for international reach, and a sector-specific framework (HIPAA, PCI DSS, HITRUST, or CMMC) as the vertical demands. Our [framework selector guide](#) walks through the sequencing decision.

Is the GRC category consolidating or fragmenting?

Both. The mid-market platform space is consolidating toward fewer, more capable multi-framework platforms. At the same time, adjacent categories (privacy management, AI governance, vendor risk) are fragmenting because they each have specialized needs.

The overlap between these categories is where the next wave of platform competition will happen.

How much should a Series A company budget for compliance in year one?

For a Series A B2B SaaS company pursuing SOC 2 Type II with a basic [GRC platform](#), \$75K–\$250K annually is a reasonable starting range. That covers audit fees, tooling, remediation, and a fractional or full-time compliance resource. Our [compliance cost benchmark](#) breaks this down in detail.

Is continuous monitoring replacing point-in-time audits?

Not replacing — supplementing. Audits remain the formal attestation mechanism. Continuous monitoring changes what happens in between audits: drift detection, evidence freshness, and control effectiveness tracking move from quarterly events to always-on operations.

Where should a compliance lead invest their first 90 days?

Three priorities: (1) establish a unified control catalog that maps to your active and planned frameworks; (2) assign named control owners for every control with clear accountability; (3) implement or validate automated evidence collection for the highest-volume controls. Everything else flows from these.

Is AI actually changing compliance work, or is it hype?

It's genuinely changing the work, but the change is uneven. Policy drafting, questionnaire response, and evidence collection are materially faster with modern AI assistance. Risk assessment and control interpretation still require human judgment. Treat AI as a force multiplier for practitioners, not a replacement for them.

The state of GRC in 2026 is more demanding, more automated, and more strategic than it has ever been. The teams that thrive will be the ones that treat compliance as a

continuous operational capability — not an annual project — and invest in the tooling, clarity, and executive support that make that posture sustainable.

Want to see what a modern, multi-framework-native GRC platform looks like? Episki gives growing teams framework mapping, evidence management, AI-powered workflows, and team collaboration in one workspace. [See how it works.](#)



Best Sprinto Alternatives in 2026
The top Sprinto alternatives in 2026 compared on pricing, framework...



The Agile Auditor: Rethinking Security's ...
Compliance theater — the appearance of security without the substance. There'..



Product

Features

Pricing

SOC 2

ISO 27001

HIPAA

PCI DSS

NIST CSF

CMMC

Company

[About](#)

[Now](#)

[Changelog](#)

[Terms](#)

[Privacy](#)

Industries

[Healthcare](#)

[Finance](#)

[SaaS](#)

[Government](#)

[E-commerce](#)

Resources

[Glossary](#)

[What is SOC 2?](#)

[What is ISO 27001?](#)

[What is HIPAA?](#)

[What is GRC?](#)

[vs Vanta](#)

[vs Drata](#)

[vs Secureframe](#)

[vs Sprinto](#)

Get started

[Sign up](#)

[Log in](#)

[Book a demo](#)

[Referral Program](#)

Subscribe to our newsletter

[Subscribe](#)