RegScale

2026 | SECOND ANNUAL

State of Continuous Controls Monitoring Report

TABLE OF CONTENTS

Opening Remarks

There's no sugarcoating the reality of manual GRC. Organizations are wasting thousands of person-hours annually just collecting evidence. Critical security work gets delayed because compliance eats every available resource. Teams are manually juggling frameworks and scrambling to complete audits with processes that just can't scale.

This year's data shows that AI and automation are transforming manual GRC processes and delivering significant time savings for those who have made the leap. Unfortunately, most organizations are stuck in the gap between knowing what works and actually implementing it.

The disconnect is massive: **94% of organizations believe that Continuous Controls Monitoring will improve both compliance and security — but only 28% are actually doing it.**

The good news is that most organizations are moving in the right direction. Companies are automating evidence collection, integrating compliance into CI/CD pipelines, and improving their board reporting. But there's still a long way to go.

This report lays out where the GRC industry stands today: what's working, what's not, and where we should go from here. The gap between aspiration and implementation won't close on its own — but these insights offer a roadmap to get started.

Dale Hoak
RegScale CISO

Strategic Advisors

Roland Cloutier
Partner/Principal, The Business Protection Group; Former CSO TikTok, Byte Dance, ADP & EMC

Alex Tosheff
Board member, advisor, investor, former CSO VMWare & CISO PayPal

Executive Summary

Welcome to the second annual State of Continuous Controls Monitoring Report from RegScale.

For 2026, the report advances our research into how organizations approach the challenge of continuous compliance in an increasingly complex regulatory landscape.

To create the report, we surveyed over 250 InfoSec leaders — including CISOs, CIOs, Chief Risk Officers, and VPs and Directors of Security — across a range of industries: tech, manufacturing, business services, retail, healthcare, financial services, government, and more. This year's findings reveal an industry in transition, one that's making progress toward automation and continuous monitoring but still facing significant barriers to widespread adoption.

The research paints a clear picture of organizations that have recognized the need for change but are struggling to implement it at scale. While 95% of our respondents have implemented some automation in their GRC processes, only 4% have achieved full automation. Only 28% monitor their security controls continuously in real-time, while 72% still rely on periodic assessments.

The burden on GRC teams is sizable and ongoing: 83% report that manual compliance work causes moderate or major delays in meeting regulatory requirements. Evidence collection is a prime example, with 58% of organizations dedicating over 2,000 person-hours annually to this one manual task.

Yet there are bright spots in the data. AI adoption is delivering universal improvement in Cyber GRC, with 100% of AI adopters reporting positive outcomes and 64% seeing significant or transformational benefits. Organizations are also achieving major time savings through automation, with 23% cutting time spent on compliance tasks by more than half. And CCM — Continuous Controls Monitoring — stands to provide invaluable real-time visibility and efficiency for GRC teams.

We begin the report by examining the true cost of manual processes and the framework overload that's overwhelming GRC teams. We then explore the automation gap: where organizations are succeeding and where they're still struggling, including key barriers to progress. Finally, we dive deep into AI adoption, ROI measurement, and the evolving demands of board-level reporting before looking ahead to the future of CCM.

Whether you're a CISO building the business case for automation investment, a GRC leader drowning in manual evidence collection, or a board member seeking better visibility into organizational risk, this report provides the data and insights you need to understand where the industry stands today and where it's headed tomorrow.

An Overburdened Industry

THE TRUE COST OF MANUAL PROCESSES

The GRC industry is drowning in manual work— and it's costing organizations far more than they realize.

The numbers paint a stark picture: **83% of organizations report that manual compliance work causes moderate or major delays** in meeting deadlines and regulatory requirements. In highly regulated industries, these delays can mean heavy reputational risks, missed market opportunities, failed audits, or regulatory penalties.

The human cost is equally staggering.

88%

of organizations are spending at least 500 person-hours annually on evidence collection alone, with 58% burning through over 2,000 person-hours each year on this single task.

That's one full-time employee doing nothing but gathering compliance evidence year-round.

For larger organizations juggling multiple frameworks, the reality is often several employees dedicated solely to this repetitive work. Every hour spent manually collecting screenshots, tracking down documentation, and compiling evidence packages is an hour not spent on strategic security initiatives, threat analysis, or innovation.

The pressure is taking its toll. The excess of manual work has forced organizations to make difficult choices about which GRC activities to delay or cut entirely.

44% of organizations have delayed or eliminated control testing and monitoring — one of the most critical activities for maintaining a strong security posture. Another **41% have scaled back training and awareness programs, and 33% have postponed policy updates and governance reviews.**

The result? A landscape where under-prepared and under-resourced GRC programs are the default rather than the exception.

85%

of organizations report delaying or eliminating GRC activities due to resource constraints.

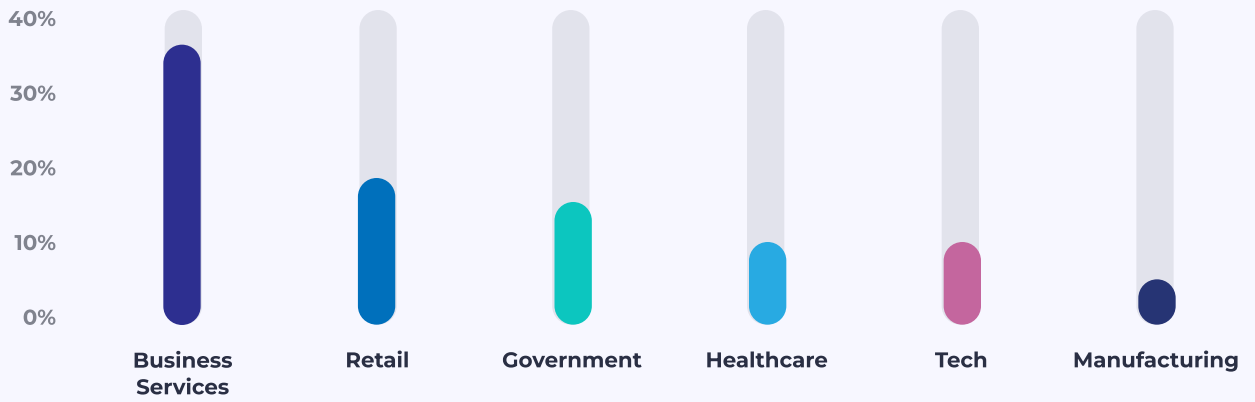
Which of the following GRC activities, if any, has your organization delayed or eliminated due to resource constraints?

Control testing and monitoring	**44%**
Training and awareness programs	**41%**
Policy updates and governance reviews	**33%**
Compliance audits / assessments	**30%**
Business continuity planning	**26%**
Vendor risk management / third-party oversight	**22%**
Incident response planning / exercises	**19%**

Shrinking Budgets, Vanishing Teams: A Sizable Minority

While most organizations upped their GRC spending in 2025, some sectors have seen significant cutbacks in GRC budget and / or headcount.

Percentage of organizations seeing cuts, by sector



Gone are the days when a company could manage compliance within a single framework.

According to the research, **72% of organizations are juggling 6 or more different compliance frameworks, and 22% are juggling more than 10.**

The overlap between frameworks can be significant, but the differences are often substantial enough to require separate evidence packages, unique control mappings, and distinct reporting processes. And with 31% of organizations still performing framework mapping manually, the picture remains bleak.

In order, the three most common frameworks are:

1. **NIST Cyber Security Framework (CSF)**
   used by 80% of organizations.

2. **ISO 27001**
   used by 65% of organizations.

3. **Cyber Risk Institute (CRI) Profile**
   used by 36% of organizations.

Many organizations are also layering industry-specific requirements on top of these foundational standards, like HIPAA for healthcare, PCI DSS for payments, and SOC 2 for SaaS providers.

But the challenge isn't just managing existing frameworks; it's keeping pace with new ones.

Over a third of organizations report that more than

50%

of their current compliance workload is dedicated to regulatory requirements introduced in just the last five years.

A further 6% of organizations are particularly burdened, with over 75% of their current workload focused on new requirements.

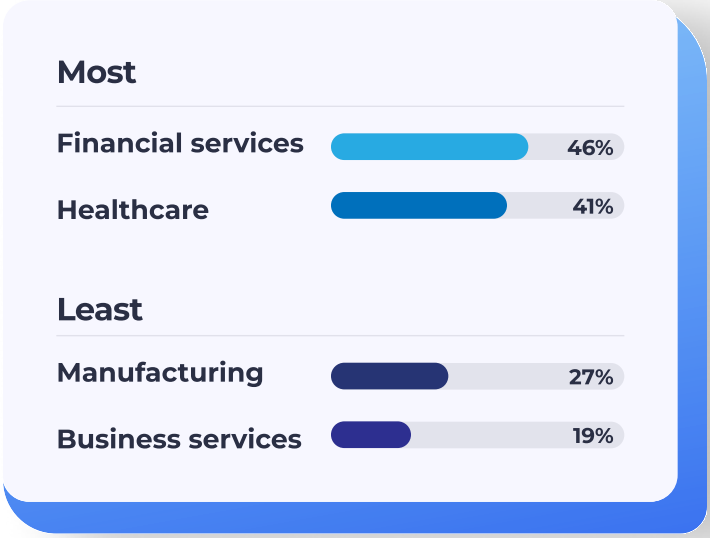
The proliferation of regulatory requirements creates a treadmill effect, with organizations running faster just to stay in place. New regulations demand attention and resources. Existing frameworks evolve. Cross-border operations add jurisdictional complexity. And all the while, manual work balloons.

The complexity has cascading effects. When organizations spend the majority of their GRC resources on keeping up with recent regulatory changes, they have less capacity for improving their security posture, implementing new technologies, or taking a proactive approach to risk management.

Reeling from Regulatory Requirements

While every industry has seen a proliferation of frameworks and regulations, some have been hit harder than others.

Which industries are most and least likely to be spending more than half their current compliance workload on new requirements introduced in the last five years?



Ranking Regulatory Burden by Industry

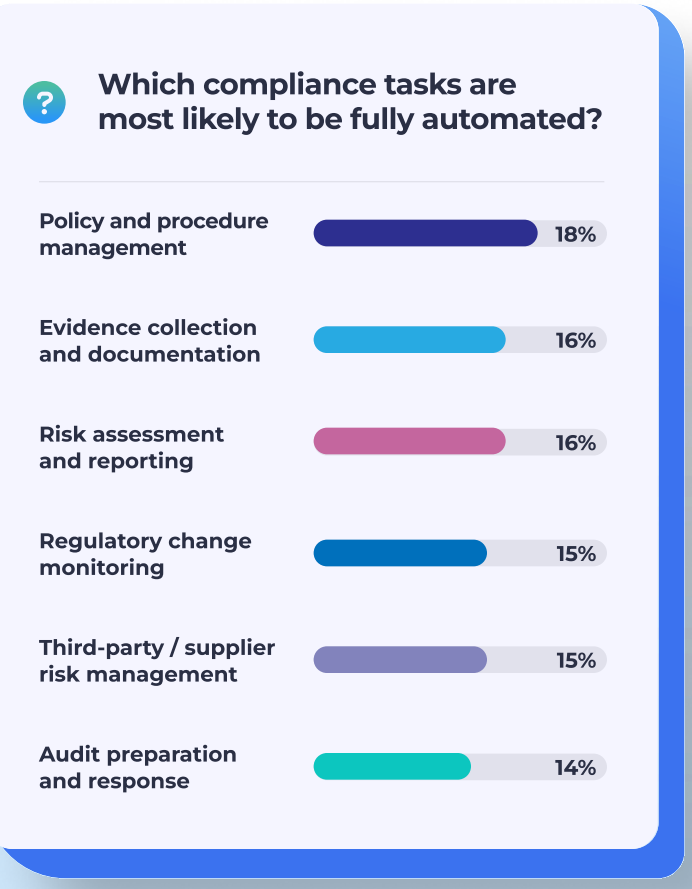
It's not uncommon for a company to juggle multiple frameworks, but which sectors have the most organizations managing 6+ frameworks?

The Road to GRC Automation

AUTOMATION GAPS: ASPIRATION VS. REALITY

Nearly every organization recognizes that automation is essential for modern GRC. The question is no longer whether to automate, but how much and how quickly.

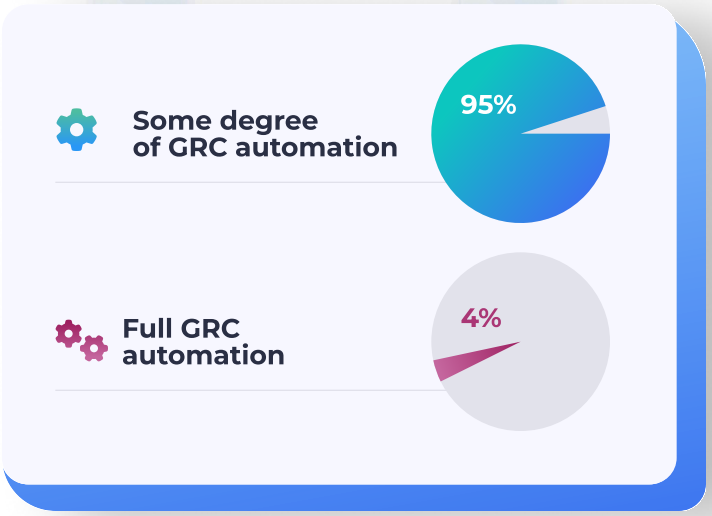
Progress is happening, but it's incremental. On average, 48% of organizations report being mostly or fully automated across various GRC activities. However, the depth of that automation remains limited, with the majority still operating in hybrid or mostly manual modes.



The good news?
95% of organizations have implemented some degree of automation in their GRC processes.

The bad news?
Only 4% have achieved full automation.

This 91-point gap reveals an industry in transition, caught between the reality of legacy manual processes and the potential of fully automated risk and compliance operations.



Where Automation Takes Hold — And Where It Doesn't

Not all compliance activities are equally suited to automation, and organizations are making strategic choices about where to deploy their limited resources.

Policy and procedure management leads the automation curve, with 18% of organizations achieving full automation in this area. The structured nature of policy work (version control, approval workflows, distribution tracking) makes it a natural fit for automated systems.

Evidence collection and documentation follows closely, with 16% of organizations fully automating this process. Given that 58% of organizations spend over 2,000 person-hours annually on manual evidence collection, the ROI potential here is substantial.

Audit preparation and response lags a bit at 14% full automation, despite being one of the most time-intensive and high-stakes compliance activities. The complexity of auditor interactions, the need for contextual explanations, and the variability of auditor requests make this area more resistant to automation. Yet it's also where delays and inefficiencies are most costly.

What does this mean? **Organizations are committed to automation — but they're automating where it's easiest, not necessarily where it's most needed.** Closing this gap will require not just better tools but also a fundamental rethinking of how GRC work gets prioritized.

> Organizations are being asked to move faster, manage greater risk, and do more with fewer resources — yet traditional, siloed control testing is costly, manual, and insufficient for today's complexity. Continuous Control Monitoring provides a scalable, technology-enabled way to shift from sample-based testing to full-population monitoring, clarify ownership across lines of defense, reduce duplication, and improve control effectiveness while lowering cost.
>
> **Alex Tosheff**
> Board member, advisor, investor, former CSO VMWare & CISO PayPal

Meeting the GRC resource crisis – or just postponing It?

72%

of organizations have increased their GRC team headcount or budget to cope with the proliferation of frameworks and the persistence of manual work.

15%

But is it enough? Only 15% of organizations have avoided delaying or eliminating any GRC activities due to resource constraints.

The takeaway: Organizations should be investing strategically, devoting their increased budget and headcount to technology and skilled staff that can implement AI and automation for maximum efficiency.

Last year, 94% of respondents said that they see Continuous Controls Monitoring as improving both compliance and security.

Despite this almost-universal recognition of the importance of CCM, most organizations still haven't achieved continuous visibility into their security controls.

This year, **only 28% of organizations monitor their security controls continuously in real-time, while 72% rely on periodic assessments**—42% of which are assessments conducted monthly, quarterly, semi-annually, or annually. In other words, more than two out of five organizations are always fairly out of date in their understanding of their compliance posture, and nearly three-quarters lack real-time monitoring. In fast-moving threat environments and rapidly evolving regulatory landscapes, that lag can be costly.

The adoption of compliance as code, which embeds compliance directly into development workflows, tells a similar story. **Only 21% of organizations have fully integrated compliance as code into their CI/CD pipelines, with another 45% reporting moderate use and 27% reporting minimal or no use at all.**

These numbers are up from last year, when only 14% of organizations had fully integrated compliance as code. But for a world that increasingly depends on software and cloud infrastructure, the limited adoption of compliance as code represents a significant missed opportunity.

Only 28%

of organizations have implemented continuous monitoring

Only 21%

of organizations have fully adopted compliance as code

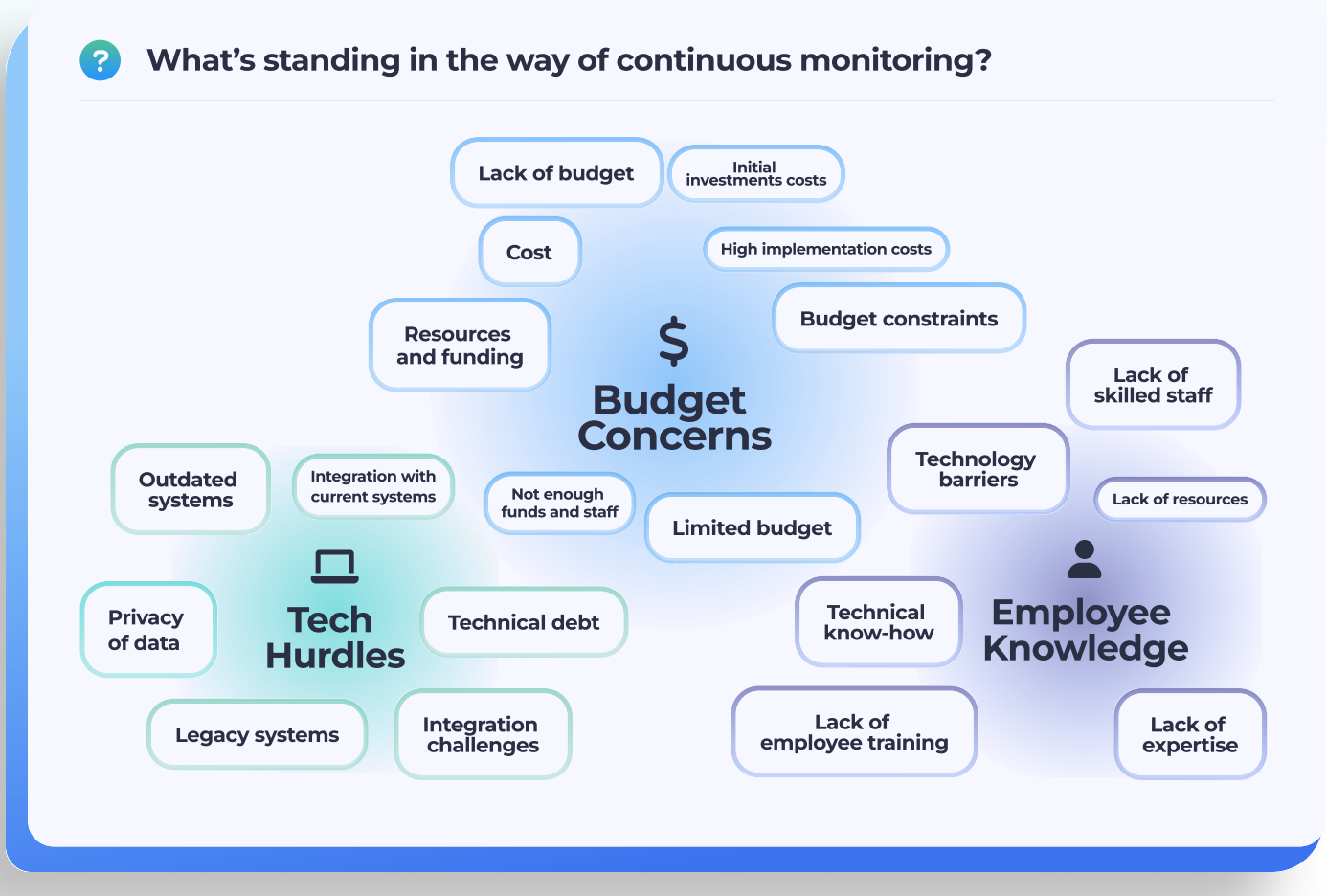
In Their Own Words: Leaders Report Top Barriers to CCM

The barriers to adopting CCM are well-documented and frustratingly persistent. When we asked organizations what prevents them from adopting real-time compliance monitoring, the responses clustered around familiar themes.

Budget constraints dominate the conversation, with **31% of respondents mentioning high costs or limited funds.** The upfront investment required for continuous monitoring tools, integration work, and process redesign can be substantial, and it's often difficult to make the business case in resource-constrained environments.

Integration challenges are a close second, appearing in 23% of responses. The reality is that many GRC teams are working with a patchwork of tools and platforms that weren't designed to work together. As a result, adding continuous monitoring capabilities often requires significant architectural changes, custom integrations, or wholesale replacement of existing systems.

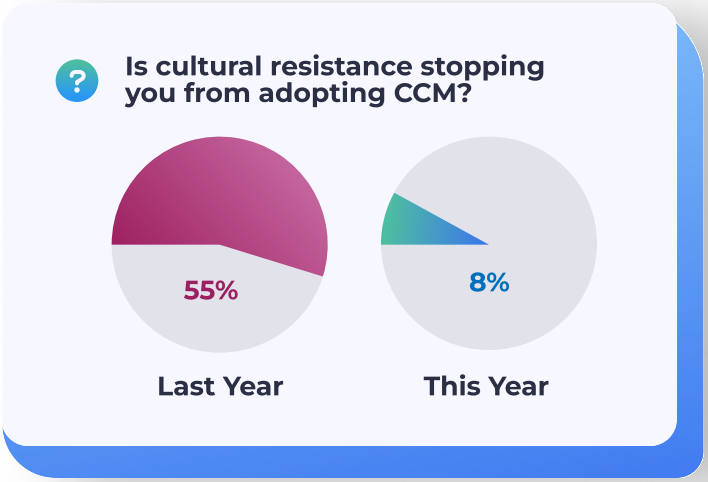
Skills gaps only compound the problem. Continuous monitoring requires a different skill set than traditional periodic assessments, one that combines compliance knowledge with technical capabilities in automation, APIs, and data analysis. Finding professionals who bridge both worlds remains challenging — so much so that **23% of respondents cited a lack of skilled employees as a major obstacle.**



Persistent Challenges

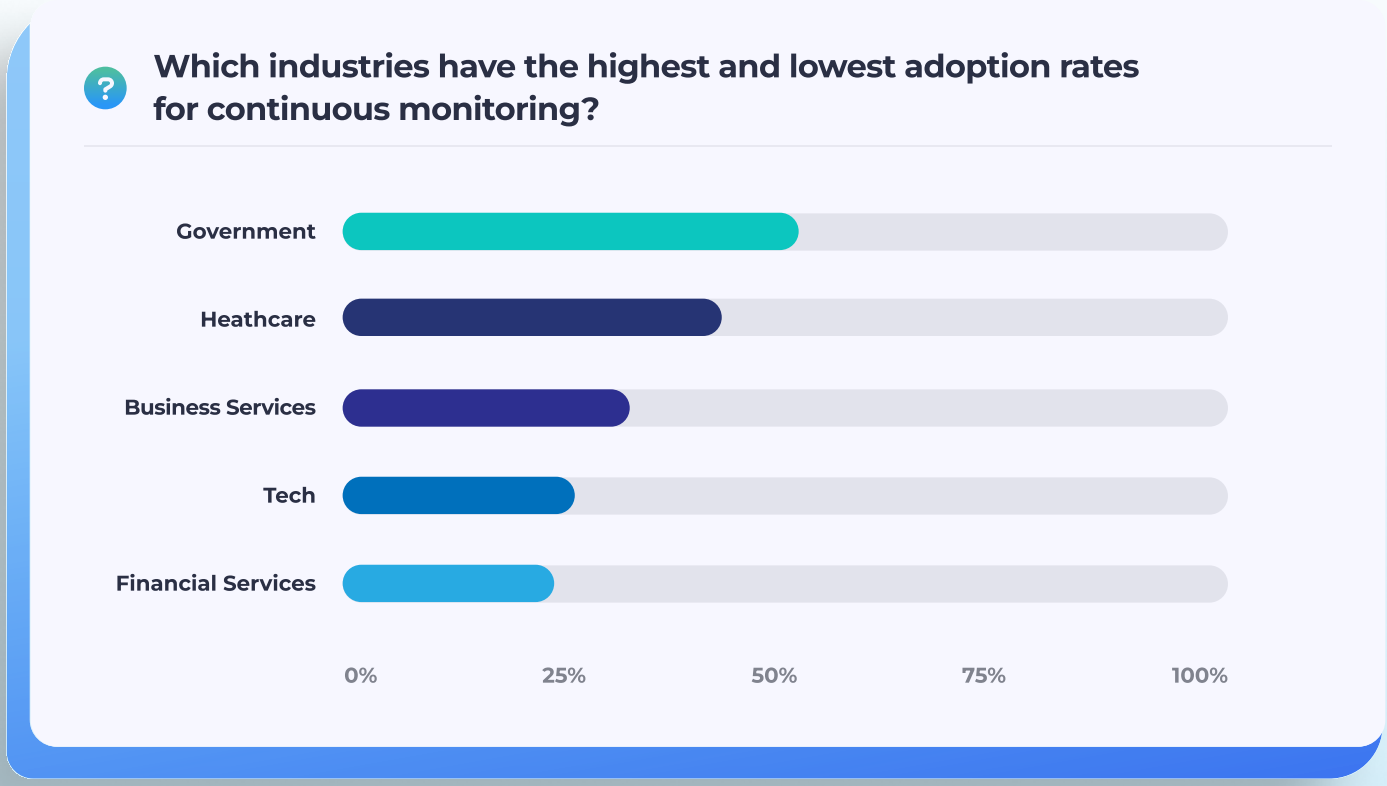
Many of these barriers have persisted virtually unchanged. Last year, for instance, 31% of GRC leaders noted that financial constraints were their biggest obstacle — an identical figure to this year's report.

One significant change, however, was the willingness to adopt continuous monitoring and automation. **More than 55% of GRC leaders last year identified cultural resistance as the primary obstacle to change, compared to only 8% of respondents this year.** This suggests that the desire for continuous monitoring has skyrocketed in the last year, even as logistical barriers cause implementation to lag.



The appetite for continuous monitoring is widespread, but adoption will require more than just better tools. It will demand new business models, better integration standards, robust training and recruiting, and a fundamental shift in how organizations approach GRC.

Always On: Continuous Monitoring by Industry



Artificial intelligence has been steadily moving from buzzword to business reality — and the results are overwhelmingly positive for the GRC industry.

100%

of organizations that have introduced AI into their compliance processes have seen improvement, with 64% experiencing significant or transformational improvement.

This unanimous success rate is remarkable in an industry often characterized by cautious adoption and slow, measured progress.

The YoY growth in AI adoption is also significant. Last year, our 2025 State of CCM Report revealed that only 18% of CISOs were using GenAI tools in their compliance programs. The rapid rise in adoption is likely due to robust preparation; last year, 72% of respondents said they had developed policy and process language to ensure responsible AI use, suggesting that AI adoption was underway.

Despite the compelling success stories, most organizations face significant hurdles in AI implementation. **48% cite budget constraints as a limiting factor,** echoing the same resource challenges we see with CCM adoption.

But there are also AI-specific obstacles:

- **56%** struggle with integrating AI tools into their existing systems.
- **41%** face a lack of skilled personnel and technical expertise.
- **42%** are limited by regulatory uncertainty or compliance concerns.

Governing AI Responsibly

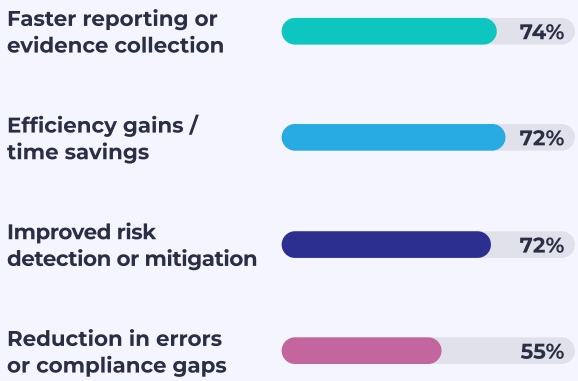
Because of these concerns — or perhaps in spite of them — organizations are taking AI governance seriously. **100% of organizations have implemented safeguards for governing AI in compliance,** suggesting that the "move fast and break things" approach is rightfully not being applied to GRC operations.

The most common safeguards include regular audits or assessments of AI systems (61%), employee training on responsible AI use (60%), and human oversight of AI outputs (60%). These measures reflect a mature understanding that AI is a tool to augment human judgment, not replace it entirely.

Other popular governance mechanisms include internal policies and procedures (57%), dedicated AI compliance teams (39%), and restrictions on high-risk AI applications (49%). Additionally, 37% of organizations have established formal AI ethics boards to ensure official oversight of AI governance.

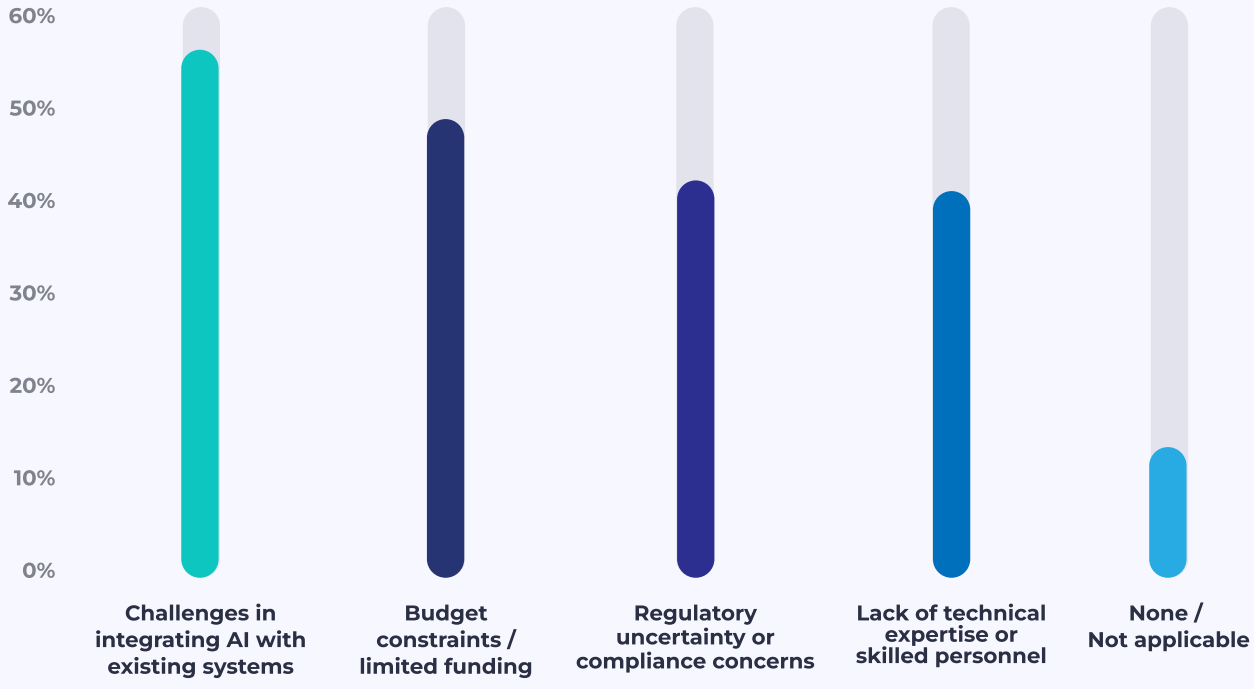
The combination of universal positive outcomes and universal governance implementation paints a picture of an industry that is embracing AI thoughtfully. Organizations are seeing real benefits — but they're also building guardrails to ensure those benefits don't come at the cost of compliance integrity or regulatory risk.

How organizations measure the ROI of AI tools in their GRC programs



Specific AI Implementation Challenges

Which of the following factors currently limit your organization from implementing AI in compliance processes?



Measuring What Matters

THE REAL ROI OF GRC AUTOMATION

For CISOs and compliance leaders seeking budget approval of their automation initiatives, the numbers are compelling.

97% of organizations saved time by automating some or all of their compliance tasks and processes. Nearly a quarter of organizations (23%) achieved major time reductions of over 50%, while more than a third (36%) achieved moderate time reductions of 26-50%. Even basic automation efforts are paying dividends, with 38% of organizations reporting modest time savings in the 1-25% range.

One of the most tangible benefits appears in auditor and regulator interactions, historically one of the most time-intensive and stressful aspects of compliance work.

84%

of organizations report improved efficiency in audit preparation thanks to automation, while 81% report faster responses to auditors or regulators

This is likely because automated systems can pull evidence packages in minutes rather than days when audit requests arrive, meaning that compliance teams can respond with confidence rather than scrambling.

68% of organizations also report more comprehensive or organized evidence packages, suggesting that automation doesn't just make compliance faster; it makes it better. Automated systems maintain consistency and ensure completeness in ways that manual processes often miss.

Unsurprisingly, the organizations seeing the most substantial ROI are those incorporating AI capabilities. **50% of organizations attribute the majority of their automation ROI to mostly or all AI-driven automation,** compared to only 20% who credit mostly or all traditional automation. The remaining organizations (29%) report that the source of their ROI is evenly split between traditional and AI-driven automation.

Top 4 Benefits Achieved by Automating Auditor/ Regulator Interactions

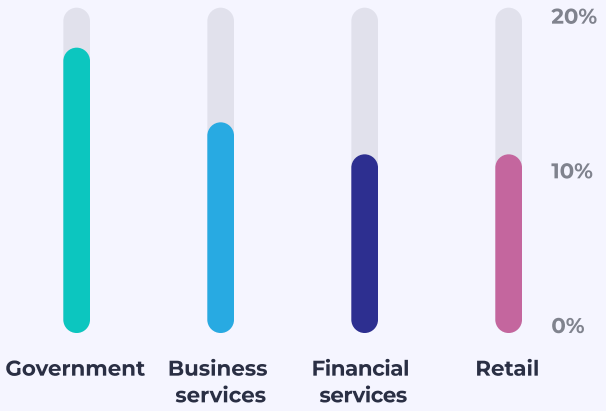
1. Improved efficiency in audit preparation
2. Faster responses to auditors or regulators
3. More comprehensive or organized evidence/security packages
4. Reduced audit findings

> Having led security operations at global companies, I've seen firsthand how manual compliance processes create cascading failures. Every day an organization delays automation, they're making an implicit choice: pay now in tech investments, or pay later in time, audit findings, and organizational risk. The 2,000+ person-hours that most organizations are burning on annual evidence collection are part of an unforgiving equation. The cost of transformation is real, but the cost of standing still is catastrophic.

Roland Cloutier
Partner/Principal, The Business Protection Group; Former CSO TikTok, ByteDance, ADP & EMC

Extreme Evidence Collection

In several industries, more than one in ten organizations are spending over 5,000 person-hours — the equivalent of two full-time GRC employees — on collecting evidence each year. **For these industries in particular, automating evidence collection will have massive ROI.**



SHOW ME THE MONEY: BOARD REPORTING

Despite seeing positive outcomes, most organizations struggle to track and communicate their automation ROI effectively.

Only 26%

of organizations say their current compliance tool provides excellent or comprehensive ROI tracking, with 19% reporting poor or limited ROI visibility.

Another 55% describe their ROI measurement capabilities as fair or good: **functional but not ideal.**

This visibility gap creates a paradox: organizations are on their way to achieving real efficiency gains and time savings, but they often can't quantify those benefits in ways that resonate with their boards. Without comprehensive ROI tracking, it becomes harder to justify continued investment in automation.

And boards are paying attention. The 2025 Gartner Board of Directors Survey found that 81% of respondents viewed cybersecurity-related risks as business risks, not just technology risks. Boards want to see ongoing, real-time results from their compliance programs — and not for the sake of a checklist but for the wellbeing of the entire enterprise.

The challenge is compounded by tool sprawl, with **the average organization using 3-4 GRC tools.** Without a single pane of glass, data gets siloed across platforms, different stakeholders see different versions of the truth, and tracking time savings and efficiency gains becomes significantly harder.

There's also the ongoing question of how to measure and communicate automation ROI more effectively. Organizations are tracking a number of different metrics: 74% track the speed of reporting or evidence collection, 72% measure general efficiency gains and time savings, 55% monitor reductions in errors or compliance gaps, and 72% assess improvements in risk detection or mitigation.

Integration: The Path Forward

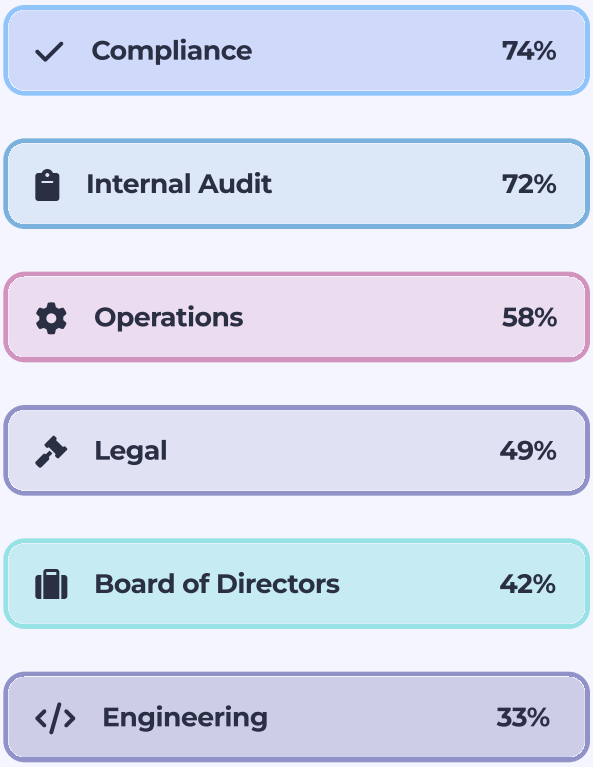
Despite these challenges, organizations are making progress. 53% report moderate integration between their GRC platform and enterprise risk management and board-level reporting processes, with an additional **38% achieving full integration with seamless data flow and reporting.**

That 38% figure represents the gold standard: a single source of truth for compliance and risk data that flows seamlessly from controls testing to risk assessments to board reporting. In these organizations, board members can access real-time dashboards, drill into specific frameworks or business units, and understand compliance posture without waiting for manually compiled reports.

The remaining 10% of organizations — those with limited integration or no integration at all — face a more difficult path. Manual data aggregation, inconsistent reporting, and delayed visibility create friction at exactly the moment when boards are demanding faster insights and continuous visibility.

Who Needs Access to Your GRC Data?

Modern GRC platforms increasingly serve many stakeholders. Most organizations report requests for data access across multiple departments.



One surprising takeaway? Boards aren't waiting for quarterly presentations anymore. They're looking for unfettered access to compliance data, real-time risk dashboards, and the ability to drill down into specific findings.

CLOSING REMARKS

The 2026 State of Continuous Controls Monitoring reveals an industry at an inflection point. Organizations almost unanimously recognize that automation is essential and that continuous monitoring represents the future. Yet the gap between recognition and implementation remains stubbornly wide.

The data tells a story of progress and paradox. On one hand, 95% of organizations have implemented some automation, 100% of AI adopters report positive outcomes, and significant time savings are being realized across the board. On the other hand, only 4% have achieved full automation, 72% lack continuous real-time monitoring, and 83% still experience moderate or major delays due to manual work. The industry is moving forward, but not fast enough to keep pace with the escalating complexity of regulatory requirements.

On one hand,

95%

of organizations have implemented **some GRC automation.**

On the other hand,

Only 4%

of organizations have achieved **full automation.**

Looking Ahead: 2026 and Beyond

In the near term, we expect to see continued adoption of AI-driven automation, particularly as tools mature and integration challenges diminish. The percentage of organizations achieving strong ROI from AI-driven automation will grow, making the business case for compliance as code and CCM increasingly difficult to ignore.

By 2030, we envision a GRC landscape that looks radically different from what we have today. Continuous Controls Monitoring will be the default rather than the exception. Manual evidence collection will be relegated to edge cases and legacy systems. Board-level integration and real-time risk visibility will be table stakes.

But this future isn't inevitable; it requires deliberate strategy and action. Organizations will need to address the ROI visibility gap so their AI and automation investments can be properly justified. They need to build the skills, partnerships, and platforms to enable true continuous monitoring. And they need to shift their perspective on compliance from burden to strategic enabler.

The tools exist. The business case is proven. The only question is whether organizations will act with the urgency that the data demands. The cost of delay — measured in person-hours, audit findings, and organizational risk — can no longer be ignored.

The time for continuous monitoring is now.

RegScale

Embrace Continuous Controls Monitoring with RegScale

Book a Demo

Available In:

AWS Marketplace

Microsoft Azure Marketplace

FedRAMP Marketplace

sales@regscale.com

regscale.com

Methodological Notes

The 2026 State of Continuous Controls Monitoring Report, authored and analyzed by Dr. Gabrielle Hovendon, is based on a survey conducted among 253 InfoSec leaders from organizations with more than 1,000 employees. Respondents were surveyed in September and October 2025, using an email invitation and an online questionnaire. All responses were validated for completeness and relevance. As with all survey-based research, results are subject to sampling error and may not reflect the views of the entire population.