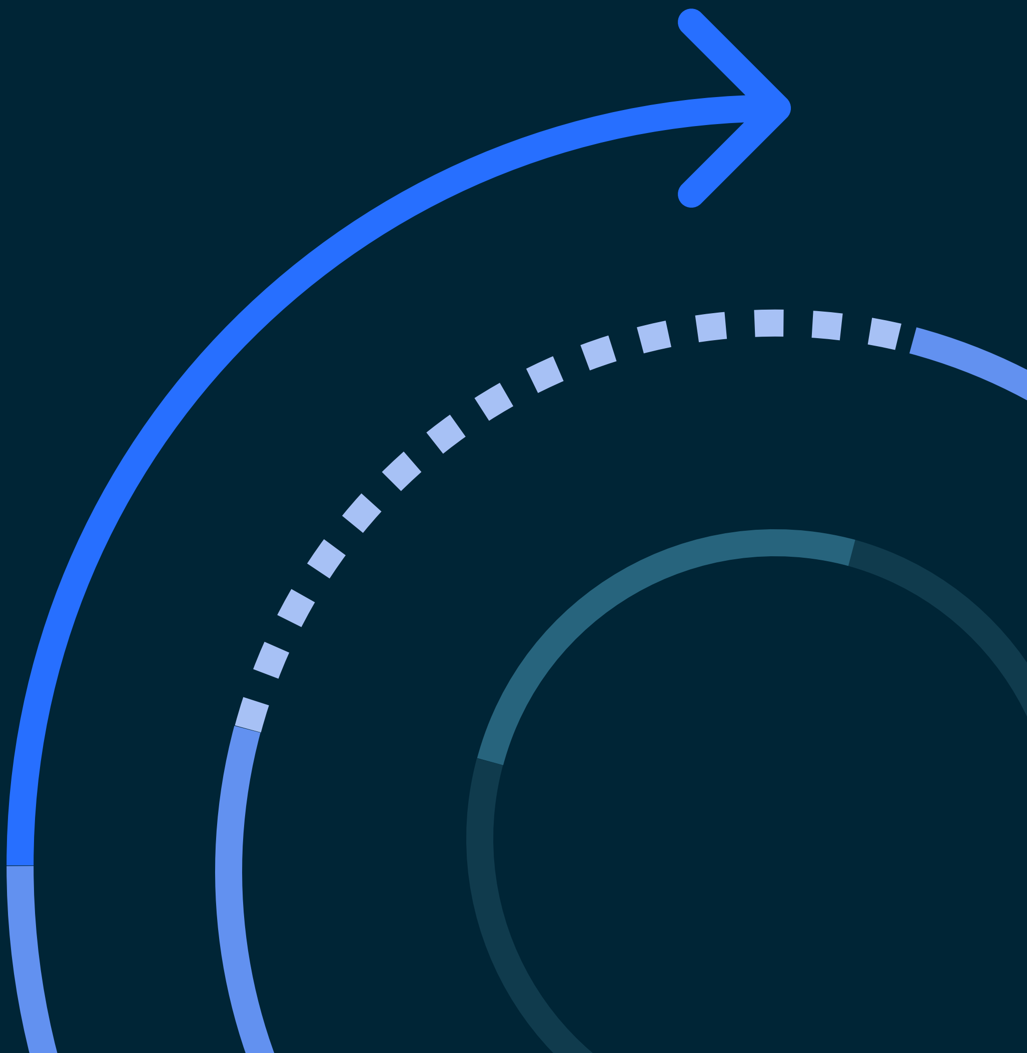
The State of GRC 2025: From Cost Center to Strategic Business Driver

aws PARTNER Security Software Competency

Presented by Drata



DRATA

Table of Contents

Executive Summary 03

Key Findings: Current GRC Dynamics 05

GRC Crunch: Caught between compliance complexity and business growth 06

AI's Impact on GRC 08

GRC Programs Maturing into Growth Centers and Trust Builders 11

The Rise of the Trust Management Platform 15

Growth of Trust and Automation on the Horizon 16

Executive Summary

Governance, Risk, and Compliance (GRC) has long been a critical business function, but in 2025 it is drawing more attention than ever before. Violations and fines regularly make headline news and increased cybersecurity threats demand more resources and attention than in previous years. Organizations have responded by bringing GRC front and center as a measurable enabler to business success. **According to a Wakefield Research survey for Drata of 300 U.S. IT and security professionals at companies with 250 to 1,500 employees, nearly all companies (96%) believe that GRC is rising in the spotlight.**

Consequently, GRC's role, responsibilities, and position within companies is evolving. Businesses are pushing GRC teams to the next level — beyond managing risk and maintaining compliance but also expecting GRC teams to demonstrate greater ROI for the business with optimized GRC programs and strategic investments in new compliance frameworks. When that strategy is successful, 98% of professionals surveyed believe GRC achievements are worth touting to customers and other critical stakeholders to build internal and external trust and help demonstrate GRC's impact on strategic business growth.

But getting there is not simple or easy. Executing a comprehensive GRC program remains a taxing journey, demanding tremendous effort from critical (and already overburdened) professionals across a range of departments and teams — from IT and Legal to Operations, Finance, and Engineering. Despite increased budgets and elevated awareness, GRC remains exhausting, highly manual, and complicated work.

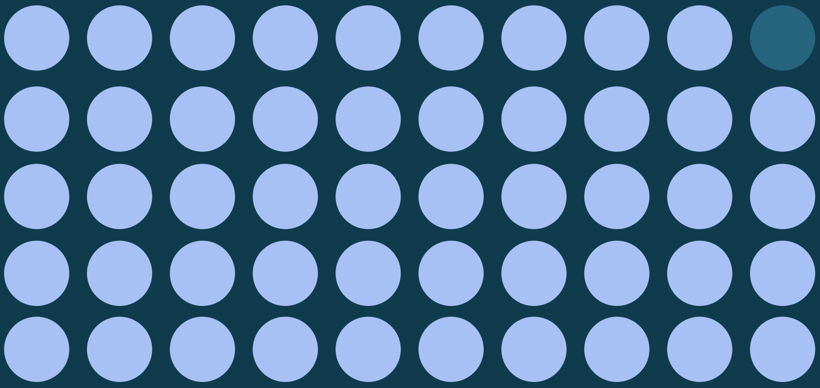
GRC leaders have reasons to be optimistic:

- AI, automation, and intelligent development tools are making operating GRC functions easier
- Security and trust assurance technology is enabling proactive, transparent communication with stakeholders, accelerating deal cycles
- Integrated systems and analytics dashboards are tying GRC efforts to business metrics (i.e. revenue won)

Plus, approaches such as 'Shift Left' will ease the load for many, allowing GRC teams to focus on less day-to-day task management and more strategy and planning.

99%

Of companies surveyed, **99% have implemented Shift Left,** are in the process, or plan to in the next 12 months.



The 'Shift Left' Approach

Trust Management Platforms are helping GRC teams adopt the "Shift Left" approach, integrating compliance processes sooner in development. Shift Left can reduce costs and eliminate security and compliance issues before projects get into production, which also helps speed up time to market.

Key Findings

Current GRC Dynamics

96%

cite high-profile breaches and compliance fines as reasons GRC is getting more attention

45%

are worried about balancing compliance and innovation

43%

say data privacy and protection challenges are a concern

46%

cite increasing regulatory complexity as a concern that keeps them up at night

36%

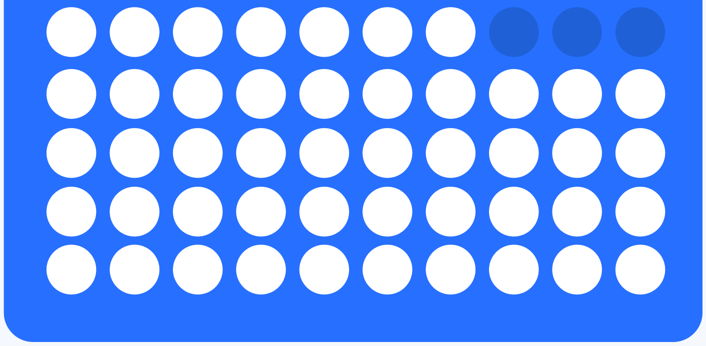
fear talent shortages most

51%

are experiencing brand safety and reputation issues due to security or data breaches

93%

have critical aspects of their GRC program that require manual intervention and need to be automated



GRC Crunch: Caught between compliance complexity and business growth

As the complexity of the security and compliance landscape grows, GRC teams are strapped for additional resources and time.

52%

are exhausted identifying new frameworks requiring compliance, and integrating those into existing programs

48%

struggle to keep pace with updates to existing compliance frameworks and identifying areas needing attention

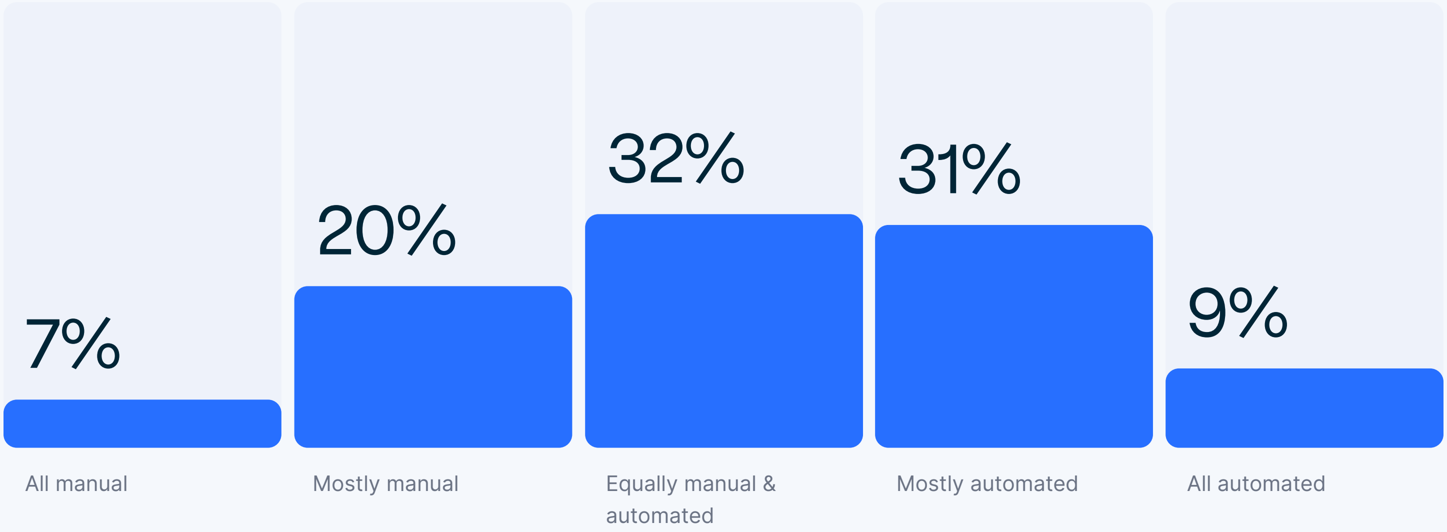
What's more, GRC teams face mounting pressure as companies now expect more robust, mature internal GRC programs to unlock revenue, sell faster, build customer trust, expand globally and into new market verticals, and drive new business.

But their plate is already overflowing. Those who perform GRC functions are managing an average of eight compliance frameworks with 60% managing at least five. In the next 12 months, companies expect to add even more, six additional compliance frameworks on average, to already stretched GRC teams.

Existing automation technologies promise to alleviate much of that work and significant overlap in requirements across frameworks make adoption more likely, but implementation still lags. While GRC functions tend to be more automated (40%) than manual (28%), for the majority (83%) it's a mix of both. Fintech and SaaS companies lead the charge in automated GRC (43%) compared to other industries (40%), but the vast majority of tasks have manual elements.

Question:

Are GRC functions at your organization more manual or more automated?



Out of all companies surveyed, 93% would like to see more critical aspects of GRC functions become automated that are manual today.

The reason: Manual interventions account for 14 hours per week on average, with the Retail sector spending more than 19 hours per week on average in cumbersome manual work. Automation could alleviate that burden, freeing time for more strategic priorities.

AI’s impact on GRC — the Good, the Bad, the Automated

The rise in AI-specific regulations like NIST AI RMF and ISO 42001 add yet another layer of complexity for GRC teams to manage. 100% of companies surveyed expect employees to increase their use of AI technologies in the next 12 months, yet only 10% have a GRC program fully prepared to manage it.

Question:

How prepared is your GRC function to manage increased use of AI among employees?

10%

are completely prepared

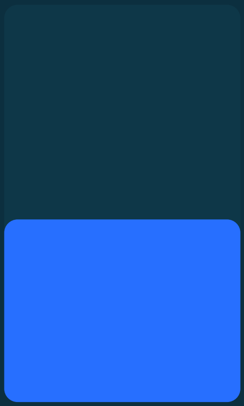
44% of companies also anticipate a massive or complete overhaul of the GRC function itself as a result of AI. 73% expect to see the shift in the next six months or sooner.

Question:

How much of an impact do you believe AI is having or will have on your organization’s approach to GRC?

44%

believe AI will cause a complete overhaul or massive impact



AI’s impact on GRC

GRC teams can see the benefits of leveraging AI

46%

believe AI will improve regulatory compliance

44%

believe AI will increase data security

42%

anticipate enhanced risk management plus streamlined security reviews and questionnaires

40%

think AI will reduce errors in compliance tasks

40%

predict enhanced decision-making and predictive insights

37%

anticipate a streamlined audit process

AI impact expectations for GRC teams also varies by company size. Smaller companies (less than 1,000 employees) are the most optimistic about AI's impact on regulatory compliance optimizations (51%) compared to larger businesses (39%). They also feel more likely to benefit from enhanced decision making with AI's predictive insights (44% versus 34%).

On the flip side, slightly larger companies (1,000 - 1,500 employees) anticipate more improvements to streamlined security and questionnaire reviews (48%) than smaller businesses expect (38%) as well as reduction in human errors (46% for larger companies, 36% for smaller organizations).

Leadership is the most optimistic for these positive effects: C-level and senior executives are more hopeful for AI impact (42%) in comparison to mid-level employees (30%).

Early AI adopters are already seeing the impact on GRC and Security team efficiency.

> Vendor security assessments were becoming a full time job for our team, so we tried AI Questionnaire Assistance. It has reduced assessment completion from 2–3 hours to 15–20 minutes. That's a significant reduction in workload.
>
> **Jamie Pine**, Information Security Engineer @ JAMF
> SafeBase powered by Drata Customer

Yet, concerns linger as GRC teams are still expected to maintain standards of governance and control while risk exposure grows from AI usage. Many shared fears center around AI biases impacting GRC decision making (43%) and AI hallucinations giving improper GRC guidance (39%).

GRC teams must balance AI's transformative potential with the capabilities, impact, and security of various technologies as they navigate a rapidly evolving landscape.

GRC Programs Maturing into Growth Centers and Trust Builders

Companies with strong, mature GRC practices in place enter new markets more quickly and effectively, adapt to changing regulatory landscapes, and close revenue faster.

Yet, survey results demonstrate that most GRC programs are not where they need to be in terms of maturity. 41% of companies see themselves at an adolescent stage, monitoring and scaling, or shy of full maturity (37%). While optimization programs have begun for many, few have been fully realized.

How mature is your GRC program?

41% of companies surveyed see their current program as still in a developmental stage - monitoring and scaling

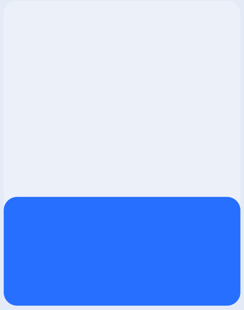
41%

Adolescent stage

37% of companies surveyed see their current program closing in on full maturity

37%

Nearing full maturity

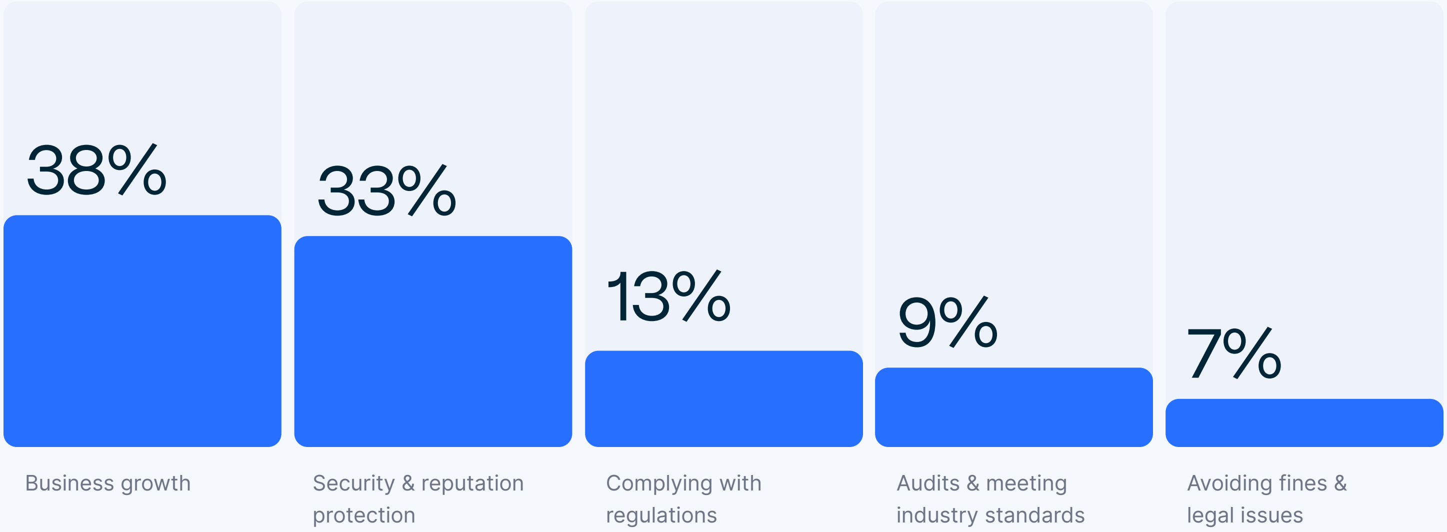


GRC Programs Maturing into Growth Centers and Trust Builders

As part of this evolution, companies are looking to expand GRC’s position from regulatory requirement and cost center to strategic business and trust enabler as well.

Question:

What is the primary focus of your organization’s Governance, Risk, and Compliance (GRC) program?



GRC Programs Maturing into Growth Centers and Trust Builders

Trends are emerging as companies identify ways to reprioritize GRC's position and priorities to drive maturity.

The majority of survey respondents see GRC as a business driver (98%), and have a dedicated person in charge of GRC (91%). GRC leaders, CISOs, CCOs, and COOs investing in these strategies are improving operational efficiency, enhancing decision-making, and strengthening brand reputation as a result. Cumbersome, manual processes are being replaced with AI automation, cross functional workflows are streamlined with workplace productivity tool integrations, and continuous controls monitoring is enhancing risk management and resource allocation.

01

Adding a dedicated GRC leader to oversee strategy and drive outcomes

91%

of companies who now have a dedicated person in charge of GRC

02

Making revenue growth a key priority for GRC investments and programs

38%

of companies say the primary focus of GRC programs is business growth

03

Building strong GRC programs to safeguard the company's brand and demonstrate commitment to security

33%

of companies say the primary focus of their GRC program is reputation protection and security

04

Transparently sharing GRC impact to build trust internally and externally

98%

of companies see GRC as a business driver

05

Moving from a reactive to proactive stance in protection, communication, and showcasing ROI

74%

of companies describe their GRC program as proactive vs 26% who see their role as reactive

Many companies see business growth as the primary focus for GRC (38%). Sales and customer success teams proactively and transparently share a company's security posture with both prospects early in deal cycles and customers during renewals to build and maintain customer trust, streamline security reviews, and accelerate time to close and renew. These are provided in a self-service, customer-centric fashion, allowing these reviews to be conducted on the customer's timeline.

Data from these reviews also supports strategic decisions made by GRC teams, such as, "Which reports, artifacts, and policies are requested the most by customers?" because reputation protection and security are a focus for organizations as well (33%). This allows GRC teams to truly be proactive (74%) vs reactive (26%) by using a data-driven position to inform decisions around maintaining and growing their GRC posture.

Lastly, when coupled with data from opportunities, data from these interactions also helps solve the ROI equation many GRC teams want to answer: "How much revenue did our GRC efforts unlock?" Answering that question helps quantifiably showcase the benefits while operational GRC functions contribute to overall business objectives.

> We are seen as sales enablement and a partner...You look at our customers and their legal teams are interested in it. They can say here is all the documentation that you need to get through that first hurdle...it really streamlines the process.
>
> **Cynthia Miller**, Senior Director, Security Assurance @ Gitlab
> SafeBase powered by Drata Customer

Trust Management Platforms are increasingly adopted as GRC programs mature, integrating governance, risk, and compliance into a unified framework.

What Trust Management Platforms offer:

01

Continuous monitoring

Utilizes real-time data and automated processes to provide ongoing oversight of an organization's security posture and compliance status.

02

Risk assessment & mitigation

Helps identify, categorize, and manage potential risks to the organization's operations and reputation.

03

Compliance management

Ensures adherence to relevant laws, regulations, and industry standards.

04

Transparency & communication

Facilitates the sharing of security and compliance information with stakeholders, often through features like Trust Centers.

05

Performance management

Provides tools for assessing and improving the maturity of an organization's security and compliance programs.

06

Automation & efficiency

Leverages technology to streamline processes, reduce manual effort, and improve accuracy in managing trust-related activities.

07

AI assisted questionnaire response

Streamlines the inbound security review response process with AI generated answers.

08

Robust CRM integrations

Share the right trust reports with the right customers and prospects.

09

Analytics dashboards

Demonstrate the impact of security and GRC enabled revenue, accelerated time to close, and prioritize open deals needing review.

Growth of Trust and Automation on the Horizon

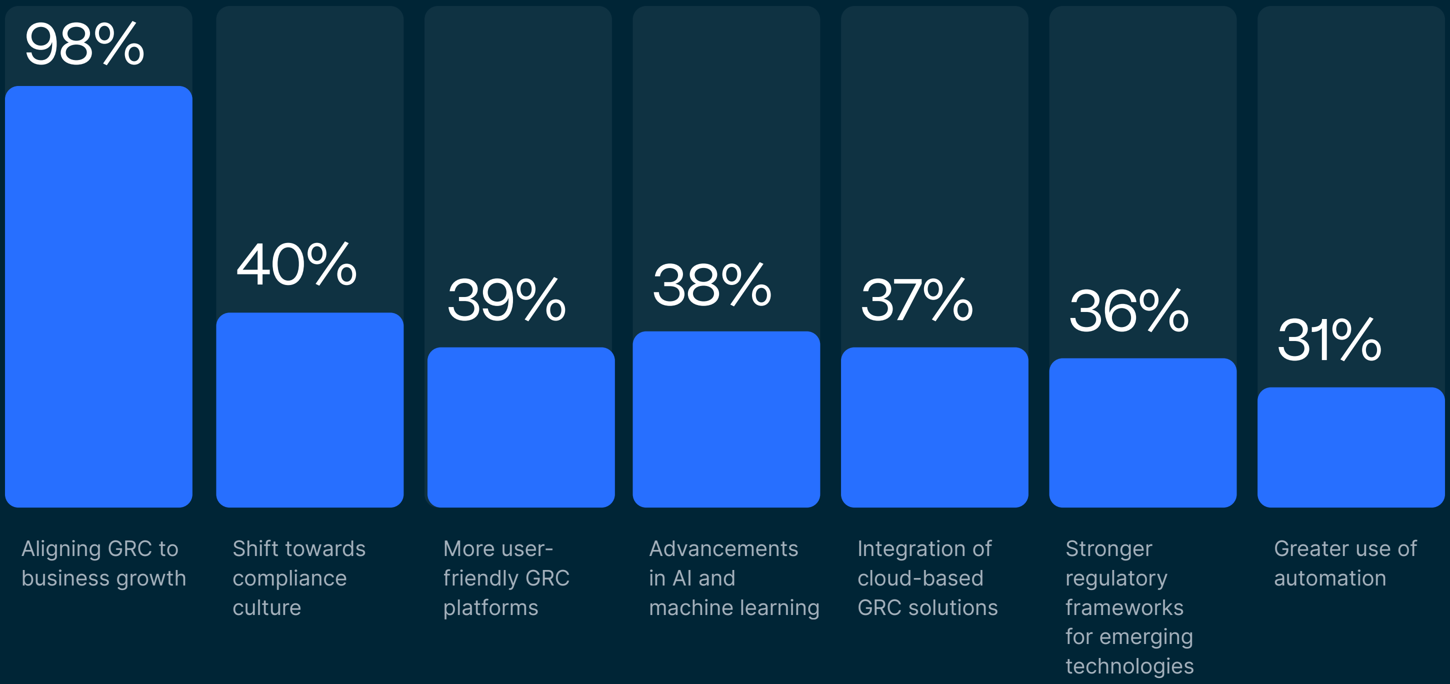
GRC — as a defined discipline — emerged only two decades ago. While individual components of governance, risk management, and compliance have existed for much longer, their integration into the GRC framework we recognize today was partly driven by corporate scandals in the early 2000s and subsequent introduction of stricter regulations.

Since then, complexity for GRC teams has only grown.

But professionals are optimistic that technology innovations and enhanced business focus on GRC will lead to positive outcomes.

Question:

Which of the following trends will positively impact GRC?



Growth of Trust and Automation on the Horizon

GRC teams stand at the cusp of a transformative era. In the next five years, their role in building customer trust will be paramount.

Leading GRC teams will evolve from risk mitigators to strategic business enablers, leveraging advanced technologies to drive innovation and efficiency while championing transparency in an increasingly complex digital landscape.

In this new frontier, GRC will not just safeguard the business—it will actively propel it forward, turning compliance into a competitive advantage and trust into a tangible asset. The GRC function of tomorrow will be a cornerstone of organizational resilience. It will drive business growth, and ensure customer confidence in an ever-changing global market.

Methodological Notes

The Drata Survey was conducted by Wakefield Research among 300 U.S. IT & Security Professionals ranging from GRC-related and IT Security titles that work for companies with 250 – 1,500 employees from High-Tech, SaaS, FinTech, HealthTech and Retail industries , between November 21st and December 11th, 2024, using an email invitation and an online survey.

Results of any sample are subject to sampling variation. The magnitude of the variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. For the interviews conducted in this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 5.7 percentage points from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample. Small base size, findings are directional.