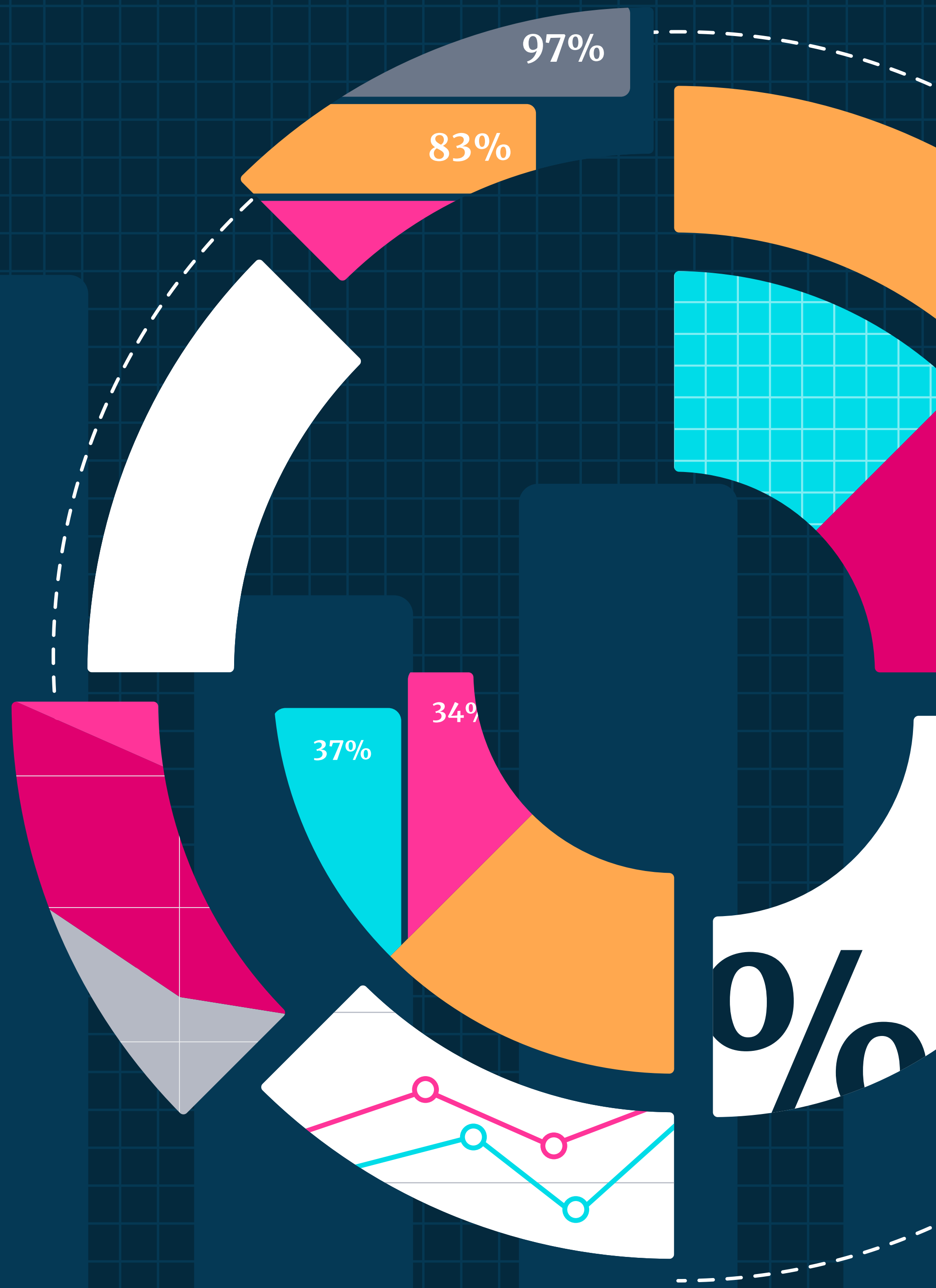
anecdotes

The State of Enterprise GRC Maturity

June 2025



GRC is taking Center Stage

Rising regulatory demands, growing public scrutiny over data privacy, and all the questions swirling around AI have thrust GRC into the limelight. It's no longer just a mandatory (cumbersome, reactive) function for mitigating risks and driving compliance. GRC has become a focal point for building trust, strengthening decision-making, and delivering measurable business value across the organization.

How are GRC professionals handling this shift? What best practices are emerging? And what does it take to run a truly mature GRC program in today's complex enterprise environment?

We surveyed 564 GRC professionals to find out. Because despite the growing expectations heaped on GRC teams, program maturity is an understudied topic. We designed the survey to assess how organizations run at different levels of GRC program maturity.

Rather than defining GRC maturity for participants, we asked them to self-report a GRC maturity level for their organization's program. Doing so allowed us to analyze what GRC maturity means to GRC practitioners, find patterns across self-reported maturity levels, and identify what characteristics and activities are common to organizations that see themselves at different stages of their GRC maturity journey.

GRC today builds trust and delivers measurable business value.

Mature GRC is Good for Business

We analyzed top GRC programs to see what sets them apart—and why it works.

Our findings show that organizations with highly mature GRC programs don't just reduce risk and preempt security incidents (valuable outcomes in their own right). They also deliver efficiency improvements and business value, from building trust to accelerating sales cycles.

In studying the most mature GRC programs, we learned that there are distinct hallmarks to how they use technology, collaborate across the business, and report to leadership. These findings provide actionable insights for GRC professionals at any organization to work more effectively and better support their business.

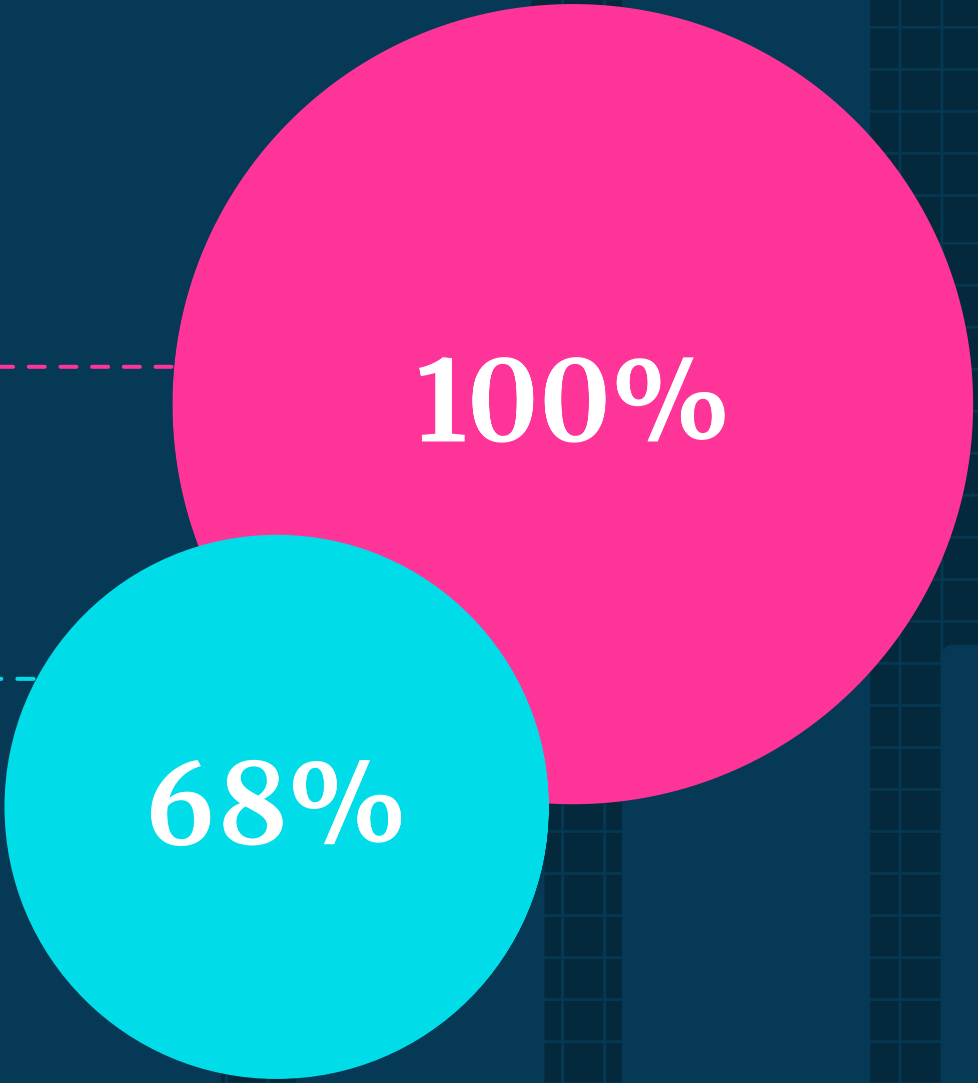
Discoveries about the challenges facing organizations at different stages of GRC maturity and organizational growth serve as roadmaps for GRC pros to avoid pitfalls and embed best practices on their path to full GRC maturity. on their path to full GRC maturity. It's a journey without an endpoint but with ample rewards along the way.

Top Takeaways

1. Embrace automation and AI

100% of "very mature"
GRC programs use automation

68% of "very mature"
GRC programs use AI



The most mature GRC programs automate a wide range of processes and have started using AI at higher rates than those with less mature programs.

Learn more | Skip to maturity tips

72%

71%

2. Stop relying on audits to find gaps

72% of all organizations still find at least half of their gaps and failures while preparing for or during audits

Most GRC programs take an audit-first approach instead of implementing continuous compliance, despite “real-time risk visibility” being the most chosen response when asked what the most reliable indicators of a mature GRC program are.

Learn more | Skip to maturity tips

3. Don’t let SOC 2 myths put your company at risk

71% of "very mature" GRC programs have a major blind spot

The most mature GRC organizations have a positive impression of SOC-in-a-Box solutions. In contrast, the least mature organizations, more likely to be familiar with these solutions, are skeptical of them.

Learn more | Skip to maturity tips

4. Win leadership support by learning how and what to report

57% of teams with the least mature GRC programs don't measure or know how to measure their GRC program's ROI

57%

Those with the most mature GRC programs tie reporting to business outcomes. Customer trust scores, sales cycle improvements, and the financial implications of compliance are just a few of the reports that earn leadership buy-in on the critical nature of GRC.

Learn more | Skip to maturity tips

73%

5. Win over leadership with custom frameworks

73% reported leadership sees GRC as a burden when they manage regulations separately (vs. a custom framework)

GRC professionals are underutilizing a key approach to efficiently manage multiple frameworks. While those who manage each regulation separately reported high levels of being perceived as a burden by leadership, the opposite was true with a custom framework approach (just 25%).

Learn more | Skip to maturity tips

The Findings

1.

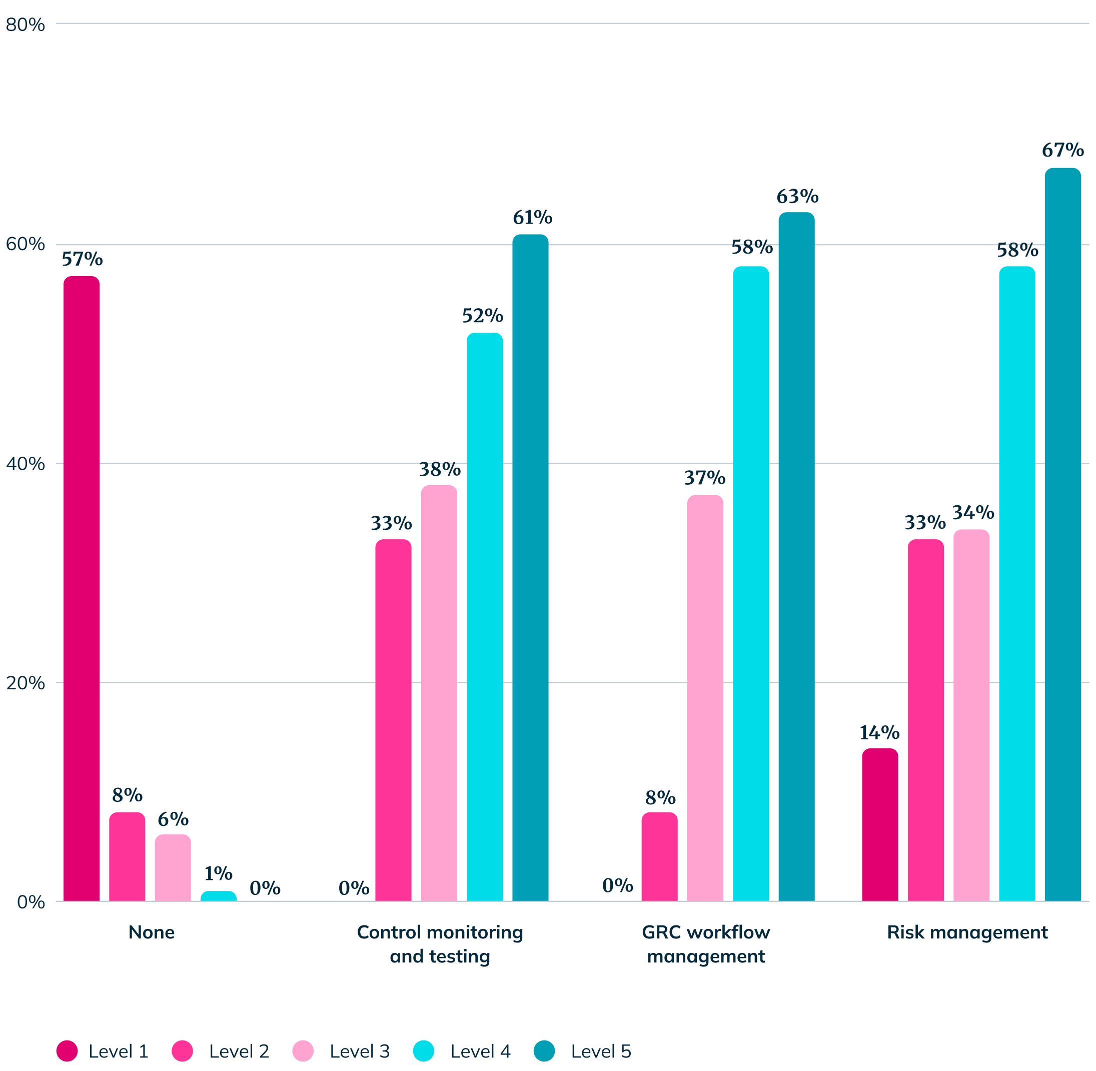
Mature GRC Programs Are Highly Automated and AI-assisted

Automation levels increase as program maturity increases

GRC program maturity and increasing automation go hand in hand. For those with the least mature GRC programs, the top response for "Which of these processes does your GRC team currently automate?" was "None" at a rate of 57%. Meanwhile, teams with very mature GRC programs automate multiple processes at significantly higher rates than less mature programs. Risk management, GRC workflow management, and control monitoring and testing are good examples (Figure 1).

Figure 1

Automation increases with GRC maturity level



The pattern is clear: The higher a respondent's GRC program maturity, the more likely they were to have automated processes in multiple areas (Figure 2).

On the flip side, each level except the most mature recognizes a lack of automation as a top 3 obstacle to achieving a fully mature GRC program (Figure 3) — and it was the second most commonly chosen obstacle to maturity in the survey overall (Figure 4).

Figure 2

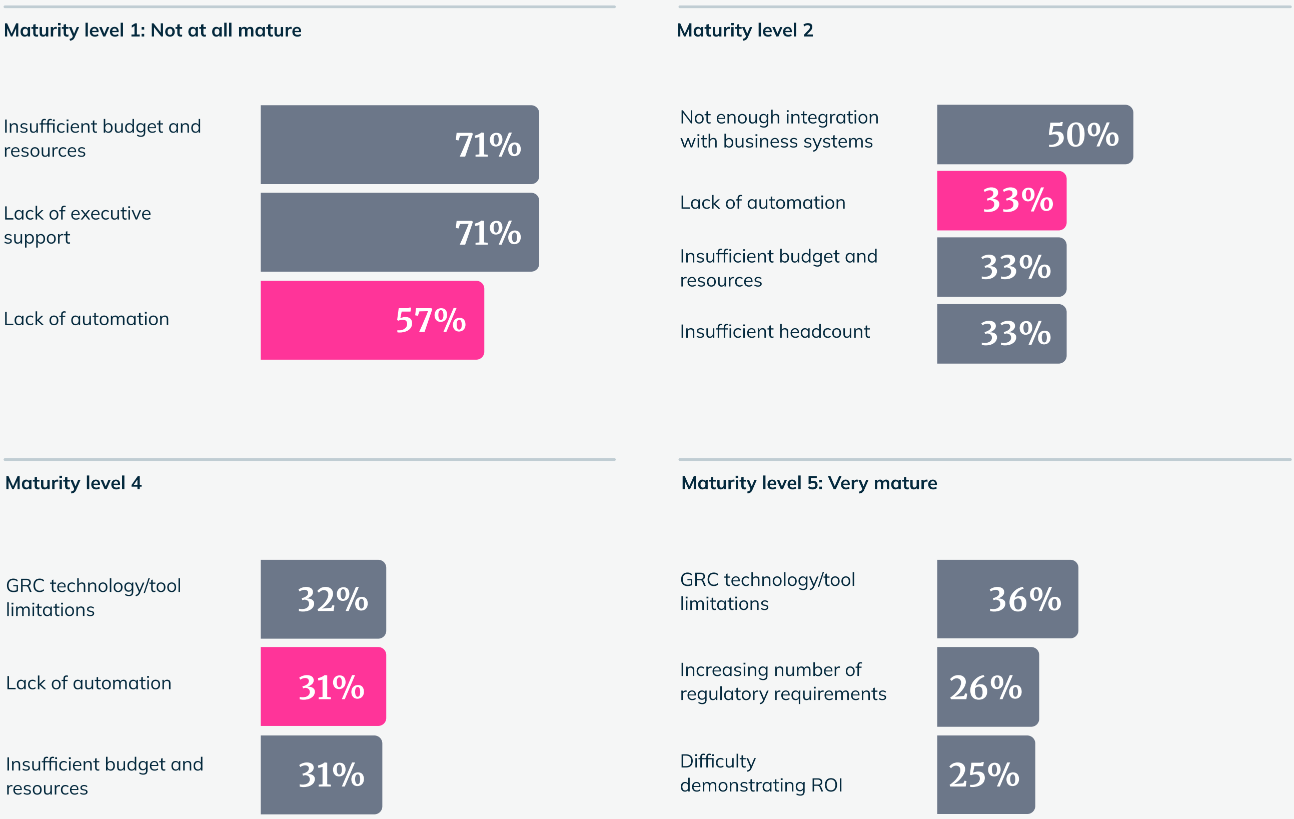
The most mature GRC programs automate more

Processes automated	Rated program very mature (5)	All responses
POLICY MANAGEMENT	48% ↑	43%
RISK MANAGEMENT	67% ↑	57%
CONTROL MONITORING AND TESTING	61% ↑	52%
GRC WORKFLOW MANAGEMENT	63% ↑	55%
EVIDENCE COLLECTION	44% ↑	37%
THIRD-PARTY RISK MANAGEMENT	47% ↑	41%
RESPONDING TO VENDOR ASSESSMENTS	39% ↑	31%
FRAMEWORK/AUDIT MANAGEMENT	45% ↑	40%
COMPLIANCE REPORTING AND DASHBOARDS	59% ↑	52%
INCIDENT RESPONSE WORKFLOWS	50% ↑	43%

GRC maturity depends on automation across critical processes.

Figure 3

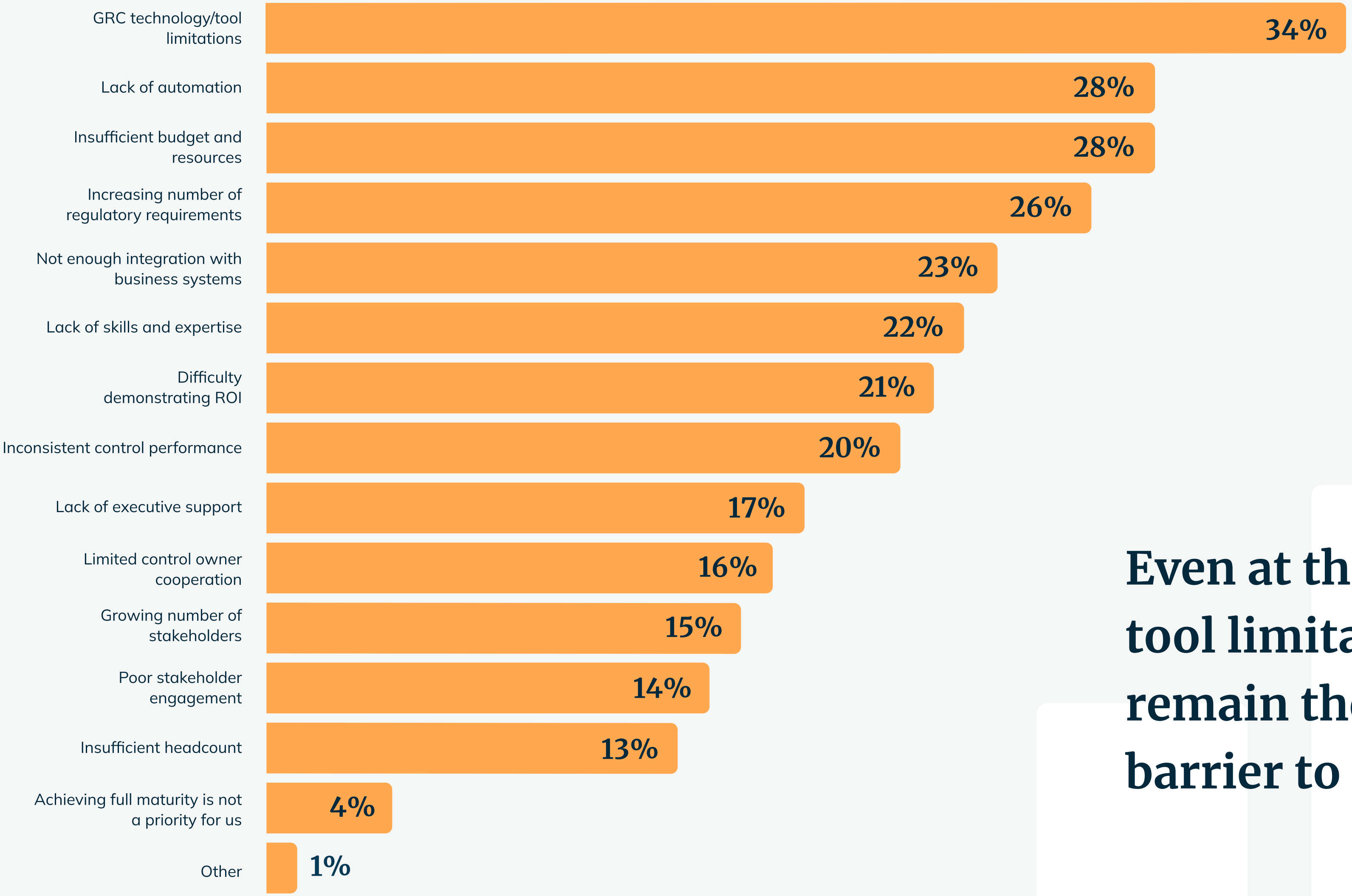
The top 3 obstacles to full GRC program maturity by current maturity level



For all but the most mature, lack of automation is a top roadblock to achieving full maturity.

Figure 4

The top obstacles to achieving a fully mature GRC program based on all responses



Even at the top, GRC tool limitations remain the biggest barrier to maturity.

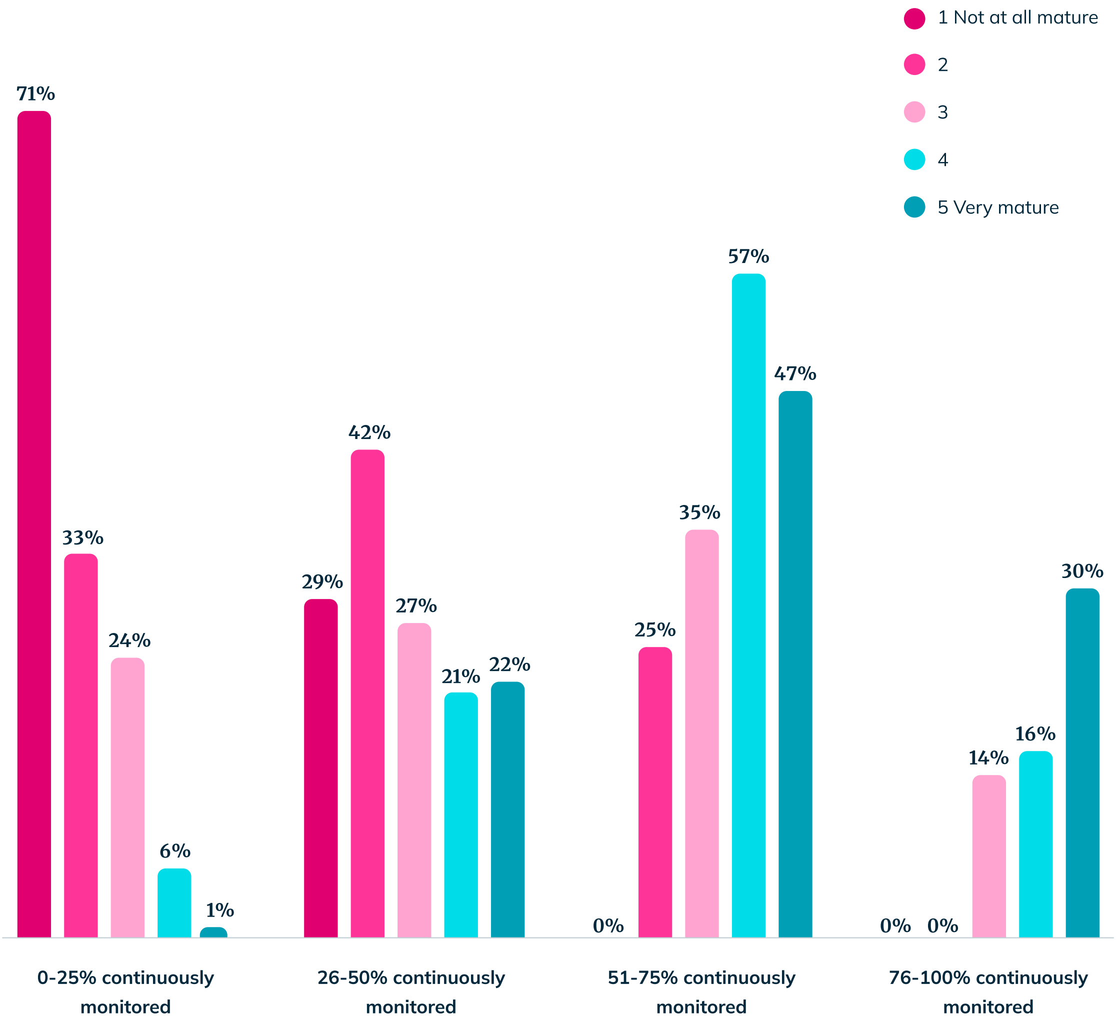
Automation unlocks the ability to continuously monitor security and compliance controls, which is also closely correlated to GRC program maturity (Figure 5).

But it doesn't stop with automation.

77% of "very mature" GRC programs continuously monitor over half their controls.

Figure 5

As continuous monitoring increases, so does GRC maturity



The highest level of GRC program maturity is also highly correlated with using AI in a wide variety of areas (Figure 6).

Top GRC programs are already operationalizing AI.

Figure 6

How very mature GRC programs are using AI in their programs (today or within the next 6 months)

Program Maturity	Rated Program Very Mature (5)	All Responses
WORKFLOW OPTIMIZATION	56% ↑	45%
DOCUMENT REVIEW AND SUMMARIZATION	52% ↑	39%
POLICY ANALYSIS	41% ↑	36%
GAP REMEDIATION	39% ↑	28%
REAL-TIME RISK DETECTION	53% ↑	47%
RESPONDING TO CUSTOMER QUESTIONNAIRES	31% ↑	25%
RECOMMENDING RELEVANT CONTROLS FOR A GIVEN FRAMEWORK	32% ↑	23%
RECOMMENDING HOW TO EXPAND YOUR PROGRAM BASED ON YOUR EVIDENCE	28% ↑	21%
THIRD-PARTY RISK MONITORING	33% ↑	27%
SECURITY INCIDENT PREDICTION	42% ↑	33%

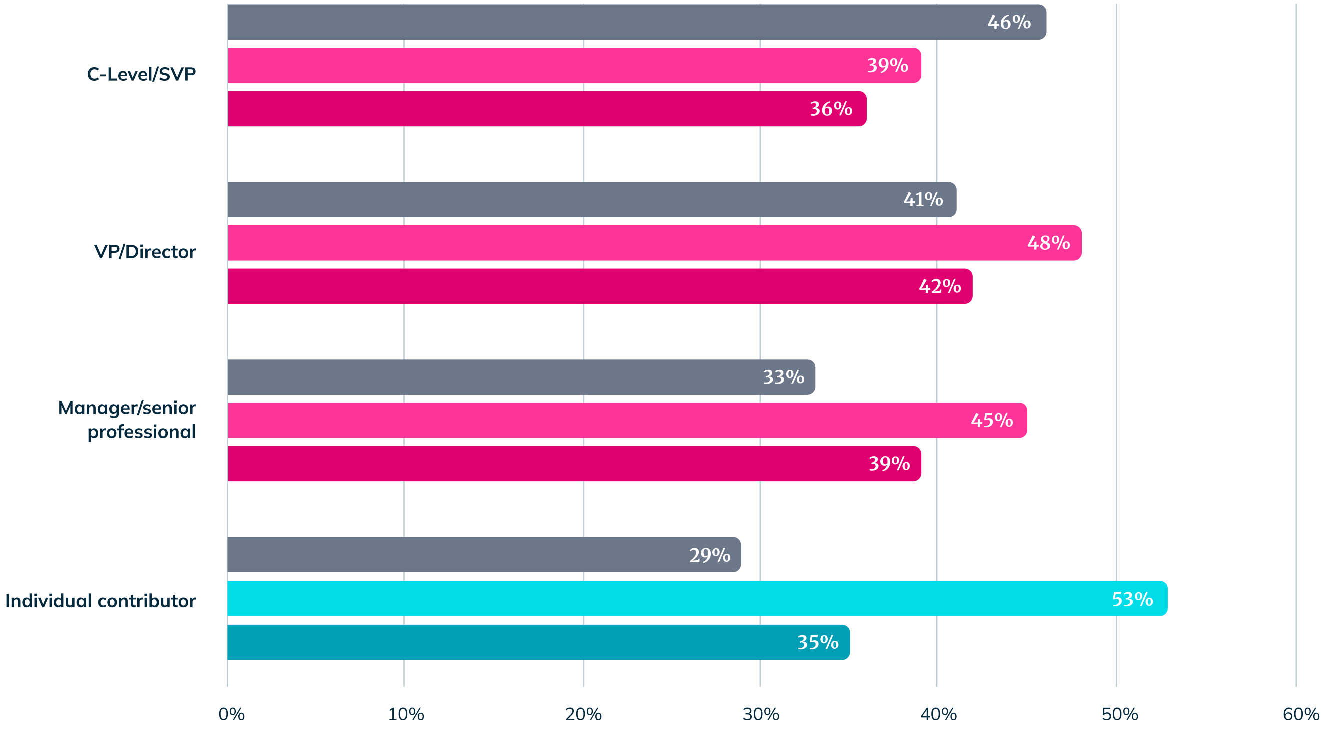
That said, GRC leaders may be missing AI's tactical potential. While management is in near lockstep about AI priorities, individual contributors (ICs) have different thoughts.

From senior professionals through the C-suite, management chose workflow optimization, real-time risk detection, and gap detection as the top three GRC processes they believe AI could most significantly improve. ICs see the challenge from a different perspective. Though they also see workflow optimization as ripe for AI improvement, they see big opportunity for policy analysis and document review and summarization (Figure 7).

Everyone is right. These are all critical issues. But leaders are considering more strategic concerns while ICs are looking at more tactical ways to use new technology.

Figure 7

Top three processes GRC professionals believe AI could significantly improve, by role



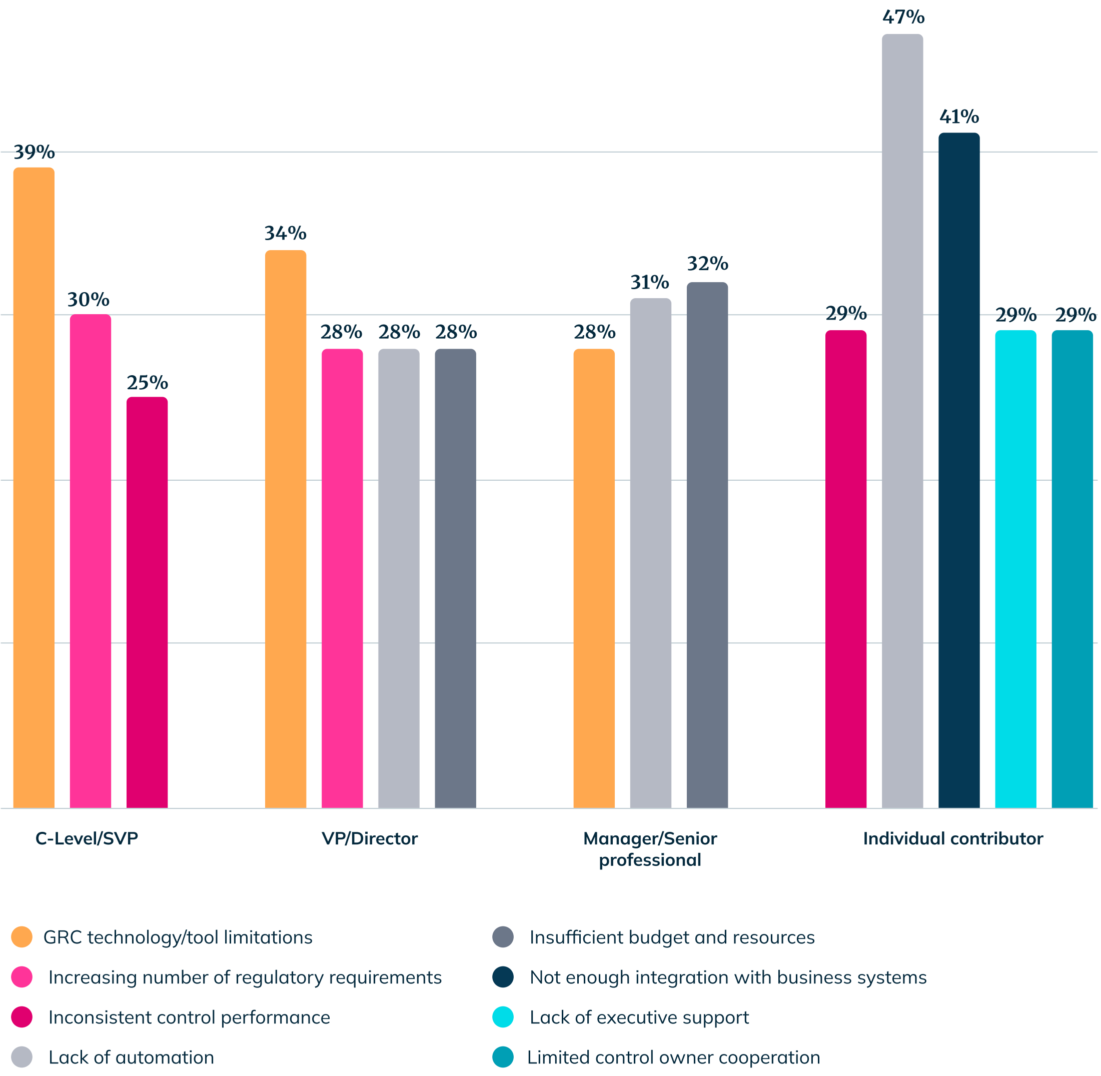
Differing AI goals reflect different obstacles

When asked to identify their top three obstacles to achieving full GRC maturity, ICs reported a lack of automation, not enough integration with business systems, and a three-way tie for inconsistent control performance, lack of executive support, and limited control owner cooperation (Figure 8).

Mid-level management echoed ICs, citing a lack of automation as a significant obstacle, but primarily focused on higher-level concerns. C-level and SVPs' reported obstacles barely overlapped with the many barriers listed by ICs.

Figure 8

Top three obstacles to achieving a fully mature GRC program by role



AI-enabled GRC tools can solve problems up and down the organization

At organizations where leadership sees GRC as a competitive advantage and/or business enabler, the program is more likely to use AI for a wide range of tactical processes, including document review and summarization, policy analysis, evidence collection, and responding to customer questionnaires (Figure 9).

Consider how AI can address all of the top obstacles mentioned by ICs:

- **Lack of automation:** AI enables and orchestrates process automation.
- **Not enough integration with business systems:** AI can collect and cross-map data from across business systems.
- **Inconsistent control performance:** AI unlocks real-time control performance monitoring and management with live GRC data.
- **Lack of executive support:** AI enables better, faster reporting to help win executive buy-in.
- **Limited control owner cooperation:** AI tools to facilitate collaboration with control owners, from automating data collection to reporting back on the business value of their efforts.

Solving ICs' problems will ladder up to solving the executives' top obstacles:

- **GRC technology/tool limitations:** When evaluating GRC tools, look to the ICs' tactical point of view to assess which functionalities matter.
- **Increasing number of regulatory requirements:** Keep up with evolving regulations by equipping your ICs with AI tools that help. ICs already want AI for policy analysis, document review, and summarization. They may not realize that GRC AI technology can also provide context-aware GRC program recommendations.
- **Inconsistent control performance:** AI can improve control performance with continuous monitoring, automatic risk recalculation, and context-aware guidance.

The data is in: automated, AI-driven GRC programs win leadership buy-in

Teams that use AI are also significantly more likely to report directly contributing to the business across many areas (Figure 10). Though more research would be needed to determine a causal relationship, it is likely a virtuous circle that goes both ways: Leaders who already value GRC invest in automation and AI tools for GRC programs, and GRC teams that use automation and AI in GRC demonstrate the business value of GRC to their leaders.

Figure 9

Organizations using AI are more likely to report positive leadership perception

How respondent uses AI in their GRC program	A competitive advantage	A risk reduction tool	A business enabler	All responses
WORKFLOW OPTIMIZATION	**54% ↑**	**53% ↑**	**56% ↑**	45%
DOCUMENT REVIEW AND SUMMARIZATION	**48% ↑**	**44% ↑**	**52% ↑**	39%
POLICY ANALYSIS	**42% ↑**	37%	**42% ↑**	36%
EVIDENCE COLLECTION	**42% ↑**	**39% ↑**	**45% ↑**	36%
GAP DETECTION	**53% ↑**	**48% ↑**	**54% ↑**	44%
GAP REMEDIATION	31%	**32% ↑**	**35% ↑**	28%
REAL-TIME RISK DETECTION	**52% ↑**	**53% ↑**	**57% ↑**	47%
RESPONDING TO CUSTOMER QUESTIONNAIRES	**30% ↑**	26%	**31% ↑**	25%
RECOMMENDING RELEVANT CONTROLS FOR A GIVEN FRAMEWORK	**30% ↑**	**27% ↑**	**29% ↑**	23%
RECOMMENDING HOW TO EXPAND YOUR PROGRAM BASED ON YOUR EVIDENCE	**29% ↑**	23%	26%	21%
THIRD-PARTY RISK MONITORING	**35% ↑**	**34% ↑**	**39% ↑**	27%
SECURITY INCIDENT PREDICTION	**39% ↑**	**38% ↑**	**40% ↑**	33%
REGULATORY CHANGE IMPACT ANALYSIS	**36% ↑**	**32% ↑**	**37% ↑**	28%

Competitive advantage ✓

Risk reduction tool ✓

Business enabler ✓

Figure 10

Organizations using AI are more likely to report directly contributing to business outcomes

How Respondent Uses AI In Their GRC Program	Reduce incident costs (quantified)	Audit efficiency gains (time/cost savings)	Sales cycle improvements (time to close)	Risk reduction metrics	Customer trust scores	Operational efficiency gains	All responses
WORKFLOW OPTIMIZATION	61% ↑	53% ↑	49%	51% ↑	54% ↑	56% ↑	45%
DOCUMENT REVIEW AND SUMMARIZATION	48% ↑	45% ↑	48% ↑	42%	47% ↑	48% ↑	39%
POLICY ANALYSIS	42% ↑	41% ↑	49% ↑	39% ↑	46% ↑	39%	36%
EVIDENCE COLLECTION	40% ↑	41% ↑	46% ↑	37%	45% ↑	40% ↑	36%
GAP DETECTION	52% ↑	50% ↑	46%	53% ↑	55% ↑	53% ↑	44%
GAP REMEDIATION	32% ↑	29%	37% ↑	31% ↑	39% ↑	33% ↑	28%
REAL-TIME RISK DETECTION	57% ↑	50%	49%	54% ↑	54% ↑	56% ↑	47%
RESPONDING TO CUSTOMER QUESTIONNAIRES	28%	27%	34% ↑	25%	34% ↑	27%	25%
RECOMMENDING RELEVANT CONTROLS FOR A GIVEN FRAMEWORK	28% ↑	26% ↑	32% ↑	27% ↑	30% ↑	29% ↑	23%
RECOMMENDING HOW TO EXPAND YOUR PROGRAM BASED ON YOUR EVIDENCE	25% ↑	24% ↑	34% ↑	23%	28% ↑	27% ↑	21%
THIRD-PARTY RISK MONITORING	32% ↑	31% ↑	32% ↑	34% ↑	33% ↑	36% ↑	27%
SECURITY INCIDENT PREDICTION	41% ↑	38% ↑	38% ↑	39% ↑	45% ↑	43% ↑	33%
REGULATORY CHANGE IMPACT ANALYSIS	35% ↑	35% ↑	31%	33% ↑	33% ↑	38% ↑	28%

Takeaway #1

Mature GRC programs embrace technology. AI has more potential than GRC leaders realize. Don’t overlook opportunities to solve your ICs’ most pressing tactical problems with AI — it will ladder up to higher-level strategic goals.

Take action

Champion and invest in GRC tools and platforms with thoughtful AI-driven automation that reduces the manual load for practitioners, streamlines collaboration with control owners, and helps leadership get faster insights from the data they already have.

2.

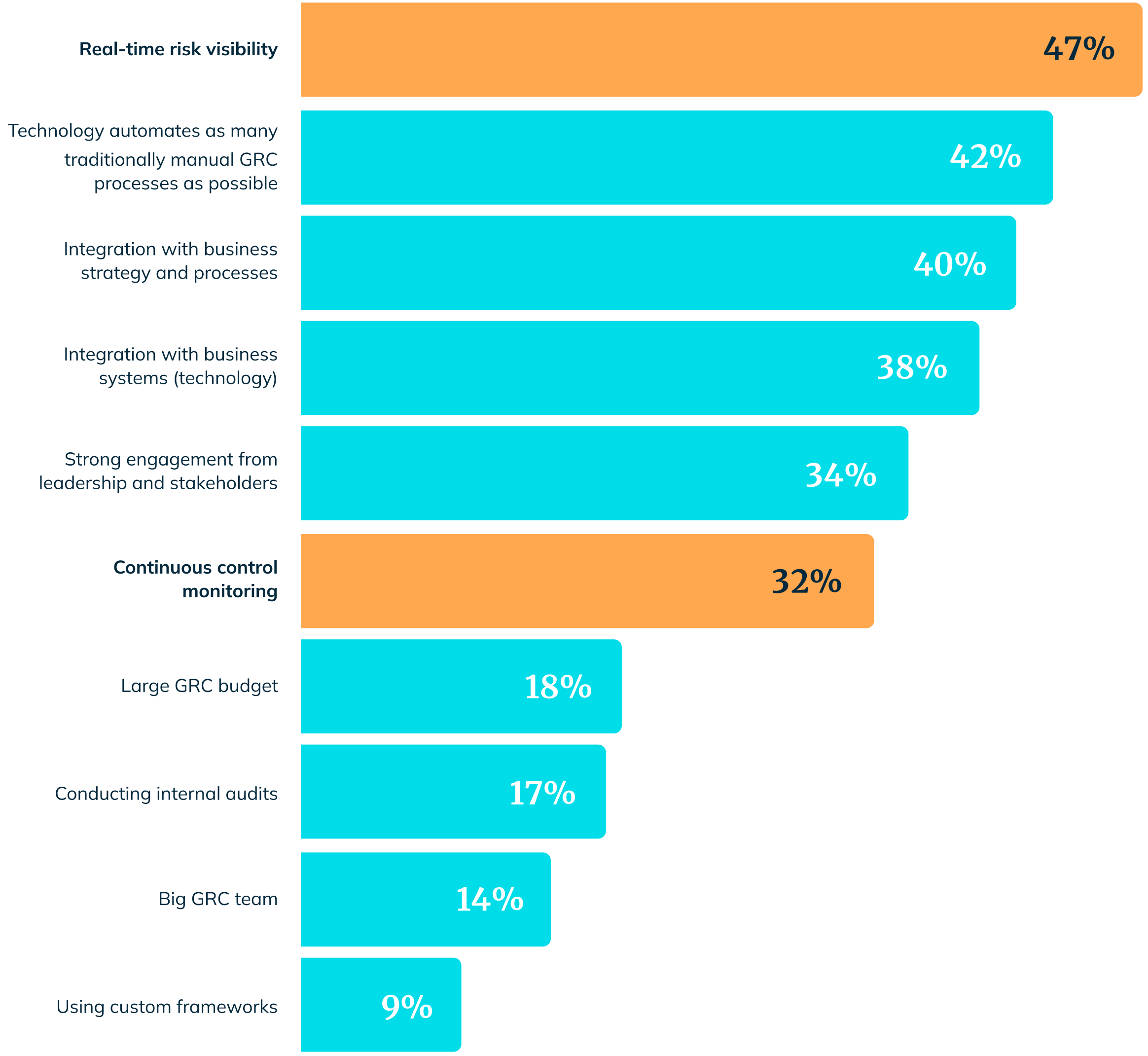
There's a Disconnect on Risk Visibility

GRC practitioners want real-time risk visibility

Overall, the most survey respondents picked real-time risk visibility as one of their top three indicators of a mature GRC program (Figure 11), demonstrating the importance of risk in a mature GRC program. It is interesting to note that far fewer respondents indicated continuous control monitoring, despite the fact that it's crucial to gaining true risk visibility.

Figure 11

Top indicators of a mature GRC program

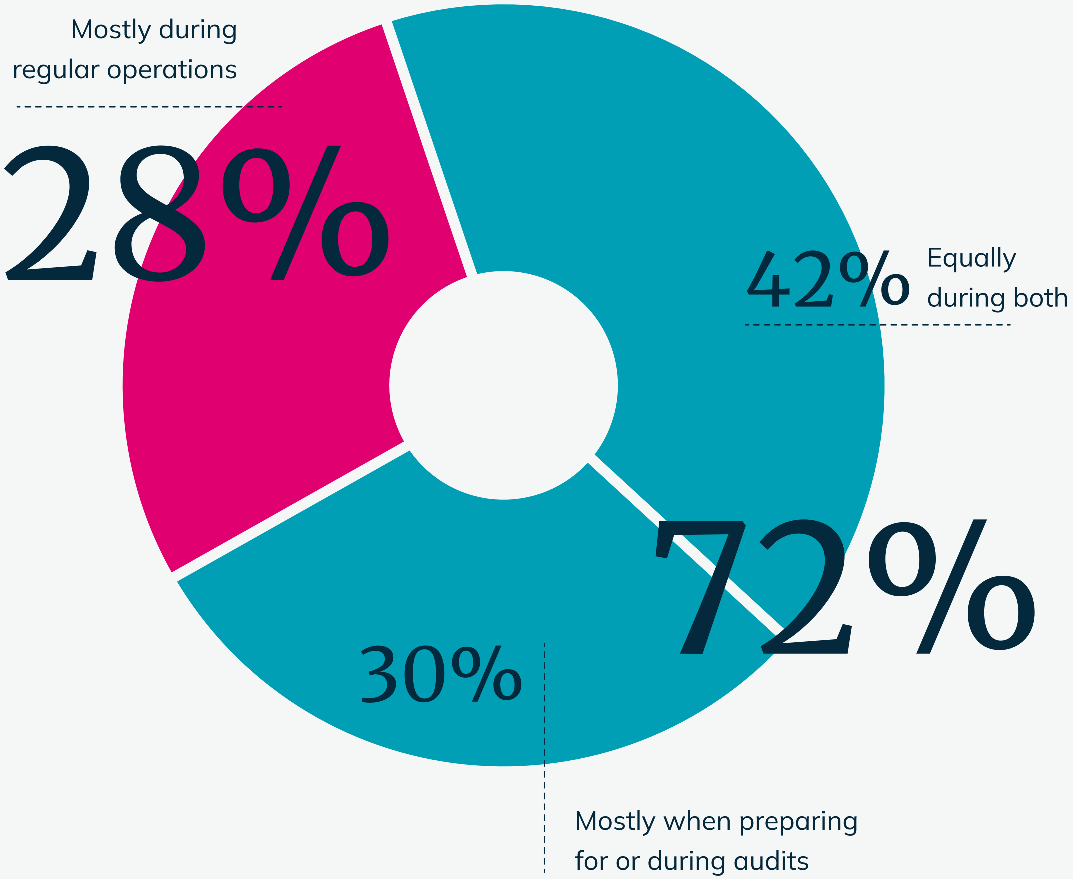


At the same time, only 28% of organizations continuously discover the majority of their control gaps and failures, while 72% find at least half during audits or audit preparation (Figure 12). Waiting for audits to identify gaps and failures is another obstacle standing in the way of real-time risk visibility.

This data highlights a disconnect between the desire for real-time insights and the operational reality of delayed gap detection. Teams know what they need; they just don't always know how to get there (or maybe they do, but don't have the tools). Meaningfully reducing risk calls for taking a risk-based approach to compliance, starting with a robust risk register and leveraging automation to monitor how controls affect risk posture in real time. With continuous control monitoring, a GRC team can detect gaps or failures and mitigate risk continuously instead of finding them at audit time.

Figure 12

When organizations usually discover control gaps or failures



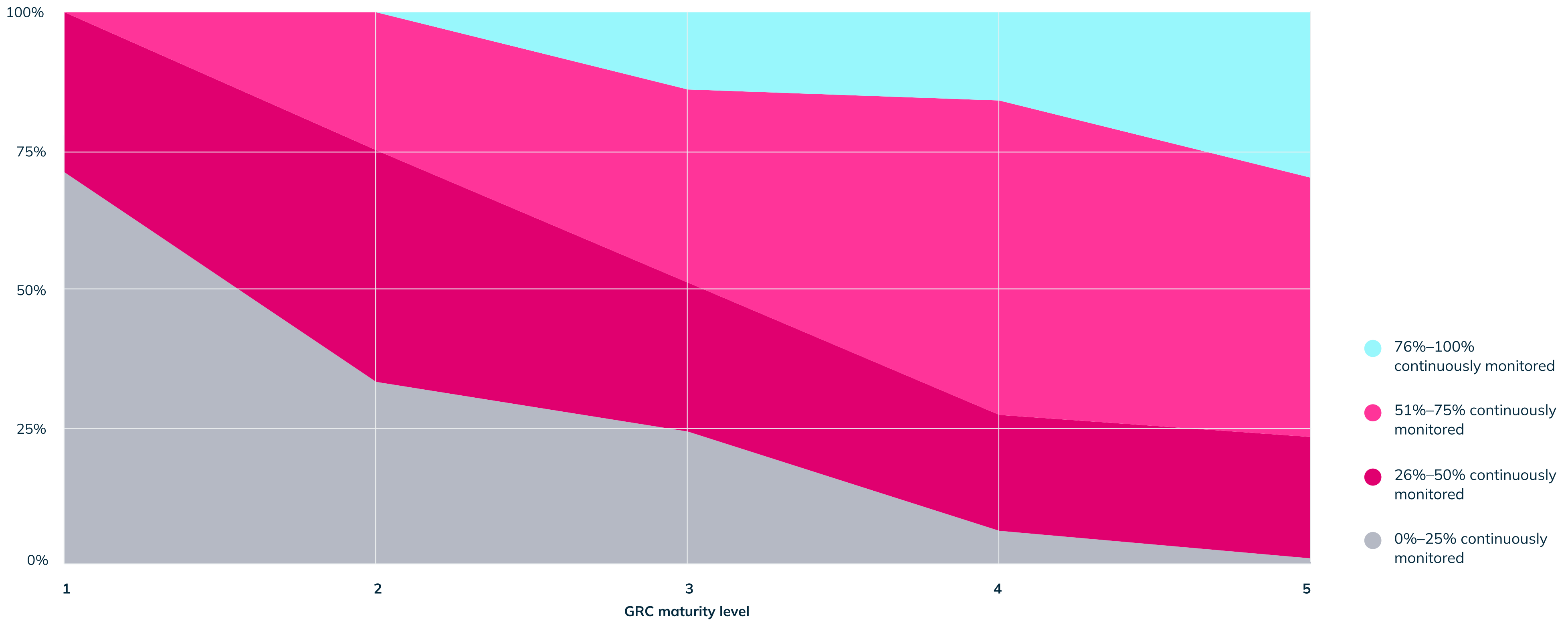
GRC teams pursue automation to achieve continuous monitoring

Automation is the key to real-time risk visibility and proactive GRC. The less automated an organization's GRC processes are, the fewer controls they report as continuously monitored.

And the respondents with the most mature GRC programs (self-reported levels of 4 and 5) achieve the highest rates of continuous control monitoring (Figure 13).

Figure 13

The percentage of controls continuously monitored increases with GRC maturity



Continuous control monitoring raises performance and confidence

As the rate of continuous control monitoring increases, the likelihood of finding control gaps and failures late steadily decreases (Figure 14). The improved ability to discover issues between audits reinforces the importance of continuous monitoring for risk visibility in day-to-day GRC operations.

When an organization continuously monitors 25% or less of their security and compliance controls, GRC professionals are far less likely to report being willing to testify to their program's efficacy in front of Congress. Even starting to implement continuous monitoring for 26–50% of controls provides a substantial boost to confidence (Figure 15).

Figure 14

When control gaps and failures are usually discovered by percentage of controls continuously monitored

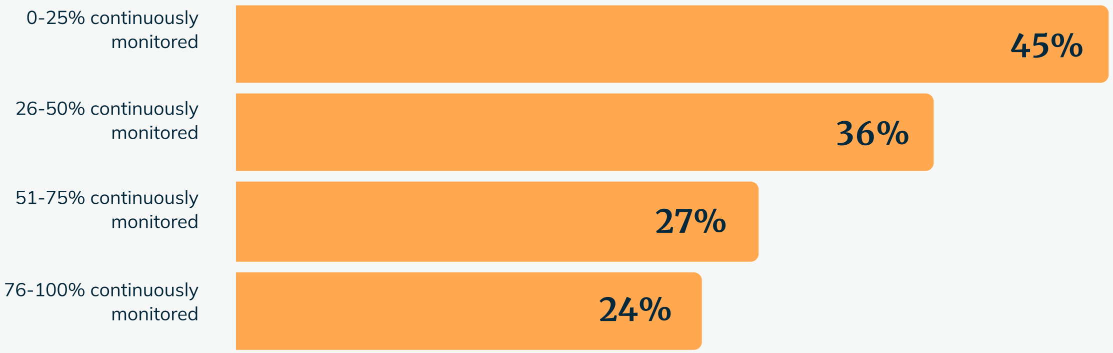
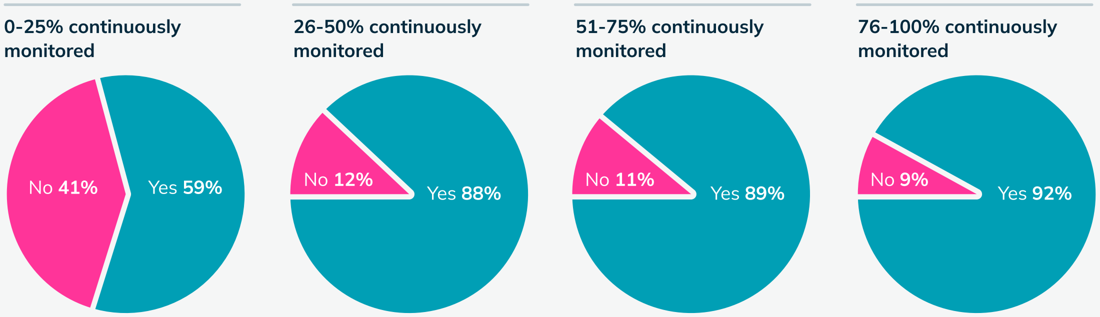


Figure 15

Continuous control monitoring and GRC professionals' confidence in their program



Takeaway #2

Organizations want real-time risk visibility, but aren’t prioritizing continuous control monitoring — the key to getting there.

Take action

Don’t wait for audit time to find problems. Continuously monitor controls to reduce audit surprises and catch small issues before they turn into costly incidents.

3.

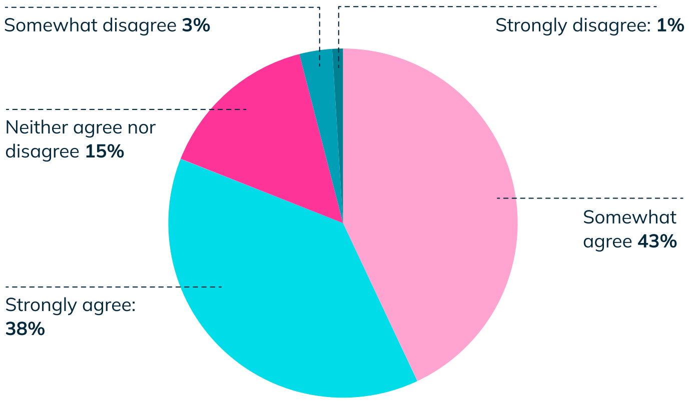
Even Mature GRC Teams Have SOC 2 Misconceptions

Most GRC practitioners overwhelmingly believe myths about SOC 2 and SOC-in-a-Box

Most respondents said that they view SOC 2 as an indicator of good security practices (Figure 16) and see the democratization of SOC 2 through SOC + audit packages, known as “Soc-in-a-Box” solutions, as a good thing (Figure 17).

Figure 16

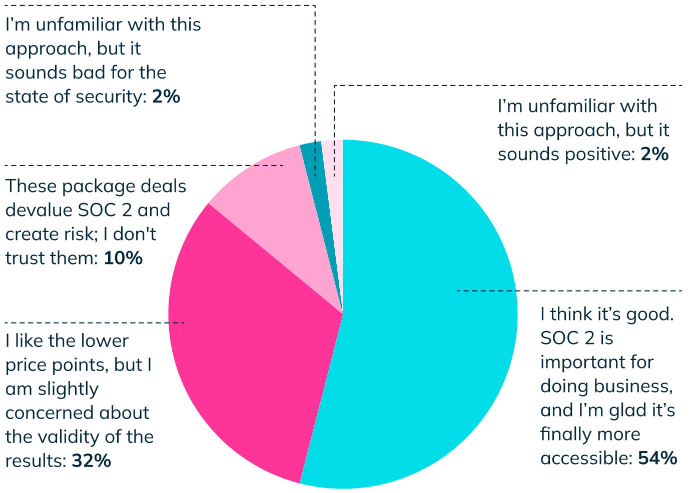
Most view SOC 2 certification as a sign that a company has good security practices.



On a scale of 1-5 how strongly do you agree with the following statement: A company with SOC 2 certification is a company with good security practices in place?

Figure 17

Most also think templated 'SOC-in-a-Box' offerings are a good thing.



In recent years, some technology vendors have started to offer SOC 2 + audits through one of their partners, providing a fast and relatively inexpensive solution.

The Rise of “SOC-in-a-Box”

SOC-in-a-Box “solutions” are templated, pre-packaged offerings that promise a faster, cheaper path to a SOC 2 report. Their one-size-fits-all approach may come with a tempting price tag, especially for organizations eager to start selling with the benefit of that shiny SOC 2 badge. But buyer beware: reducing SOC 2 to a box-ticking exercise with a rubber-stamped audit devalues the process and the entire profession. And it might just mean a potential customer doesn’t accept your report!

To learn more, read our guide: **Beyond the Checkbox: Why SOC-in-a-Box Solutions Don’t Cut It**

Why SOC 2 isn’t necessarily a reliable indicator of good security practices

A SOC 2 report earned through a rigorous audit process can indeed document an organization’s commitment to good security practices. But it’s not a given. Just because you get a SOC 2 Type II report that evaluates the effectiveness of controls over time doesn’t mean you’ve escaped the audit-based mindset.

Survey results revealed that respondents’ impressions of these SOC-in-a-Box offerings correlated with the effectiveness of their day-to-day GRC activities. Respondents with a positive impression of these offerings appear to over-rely on audits themselves, being far less likely to find most control gaps and failures during daily operations. Respondents who express concern about the SOC-in-a-Box approach are more likely to find the most control gaps and failures during regular operations than just at audit time, which reflects the proactive approach to identifying GRC issues necessary for program maturity.

In reality, a SOC 2 certification may or may not reflect good ongoing security practices. A better sign would be a high level of continuously monitored controls, which is correlated with higher levels of GRC program maturity (Figure 5, page 11).

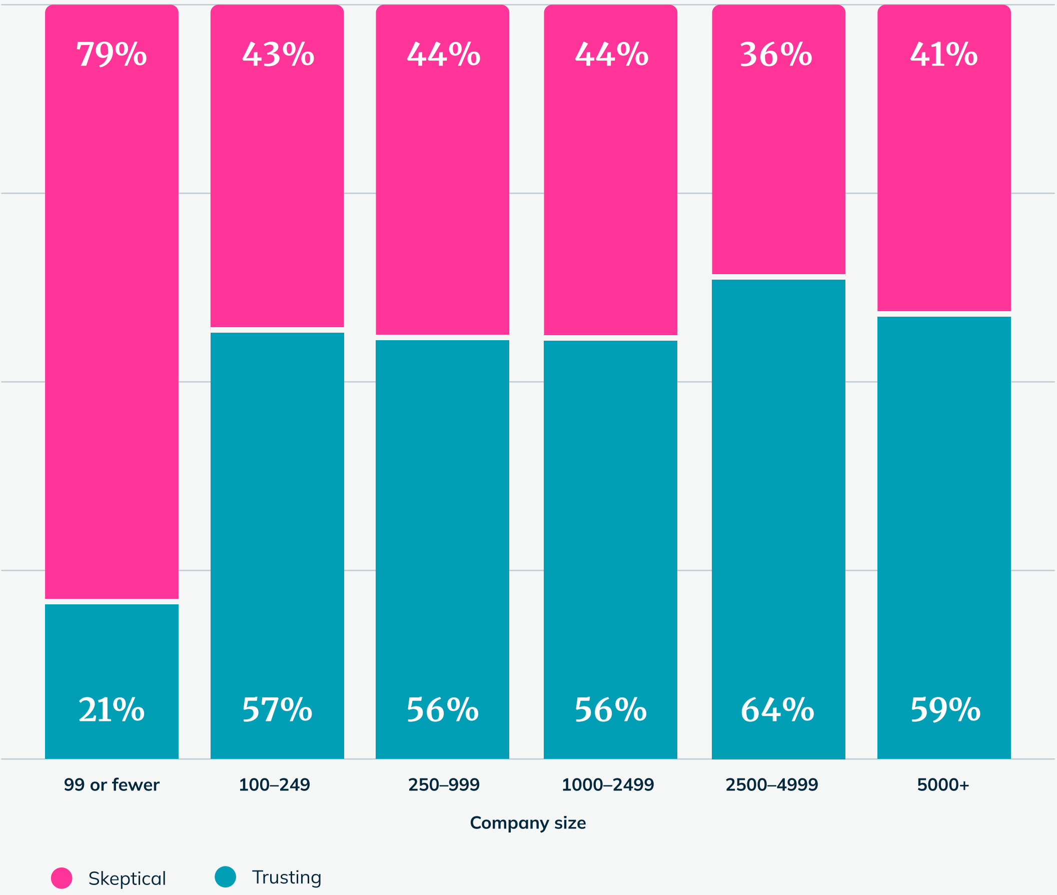
Beware SOC-in-a-Box — especially if you're not its target customer

The cost of a rigorous audit process used to mean SOC 2 certification was out of reach for many companies. In recent years, the combination of inexpensive SOC 2 solutions + low-grade audit firms (SOC-in-a-Box) has commoditized SOC 2.

The target audience for these offerings prove to be the most savvy about them. Survey respondents who reported the most skepticism of SOC-in-a-Box were at the smallest organizations (Figure 20) and those with the lowest GRC program maturity (Figure 21).

Figure 20

The smallest companies are most skeptical of SOC-in-a-Box



Respondents who rated their programs as most mature were the *least* skeptical about SOC-in-a-Box. While it's possible to read this as an indicator that all is well with these solutions, we see a far different reason for these results.

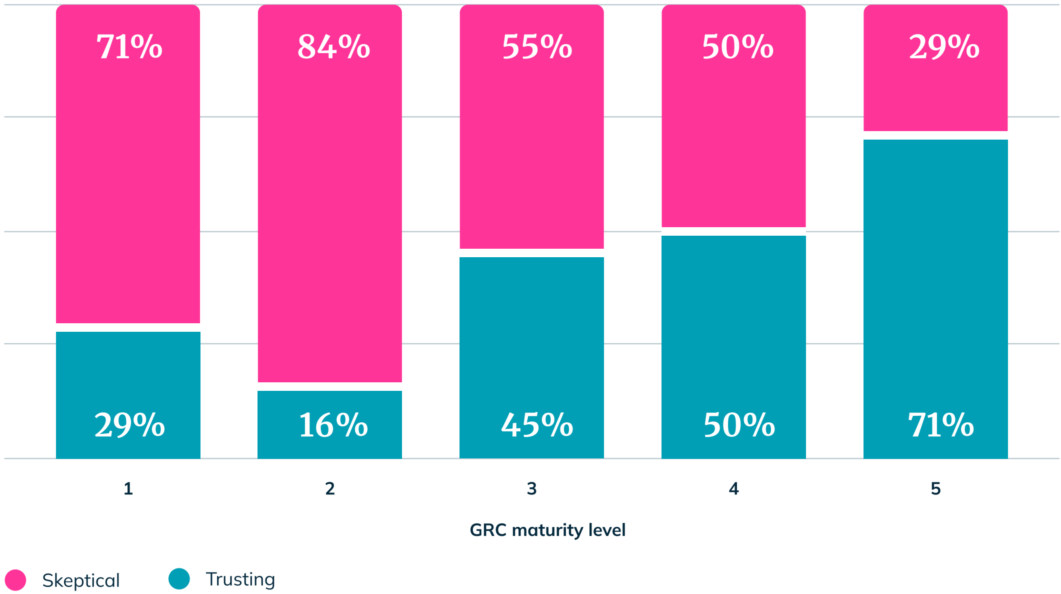
Larger companies with mature GRC programs are often beyond researching bundles that offer quick and fast SOC 2 reports. They're not the people actually working with these tools, seeing the processes they're going through, or working with the same auditors who take part in SOC-in-a-Box offerings.

We believe the people closest to these solutions — the target audience, who are more skeptical of them — are the ones who know what they're talking about.

Either way, if you use SOC 2 as part of your vetting process for vendors, partners, or M&A, it's important to know that not all SOC 2 reports are created equal. Trusting another organization's SOC 2 report without verifying it could be disastrous.

Figure 21

Companies early on their GRC maturity journey are the most skeptical of SOC-in-a-Box



When the people closest to the solution — the target audience — are skeptical, pay attention.

Takeaway #3

SOC 2 myths put companies at risk. SOC 2 isn't a reliable GRC maturity marker anymore, and trust in commodified SOC 2 packages is unfounded.

Take action

Move beyond the audit-driven mindset, which can lead to blind spots in your daily operations or security review, and pursue continuous monitoring. During security review, scrutinize third parties' SOC 2 reports to make sure they are in-depth, comprehensive, and signed by reputable auditors. Build a trust center to prove your GRC program's efforts, and look for trust centers as part of a security review.

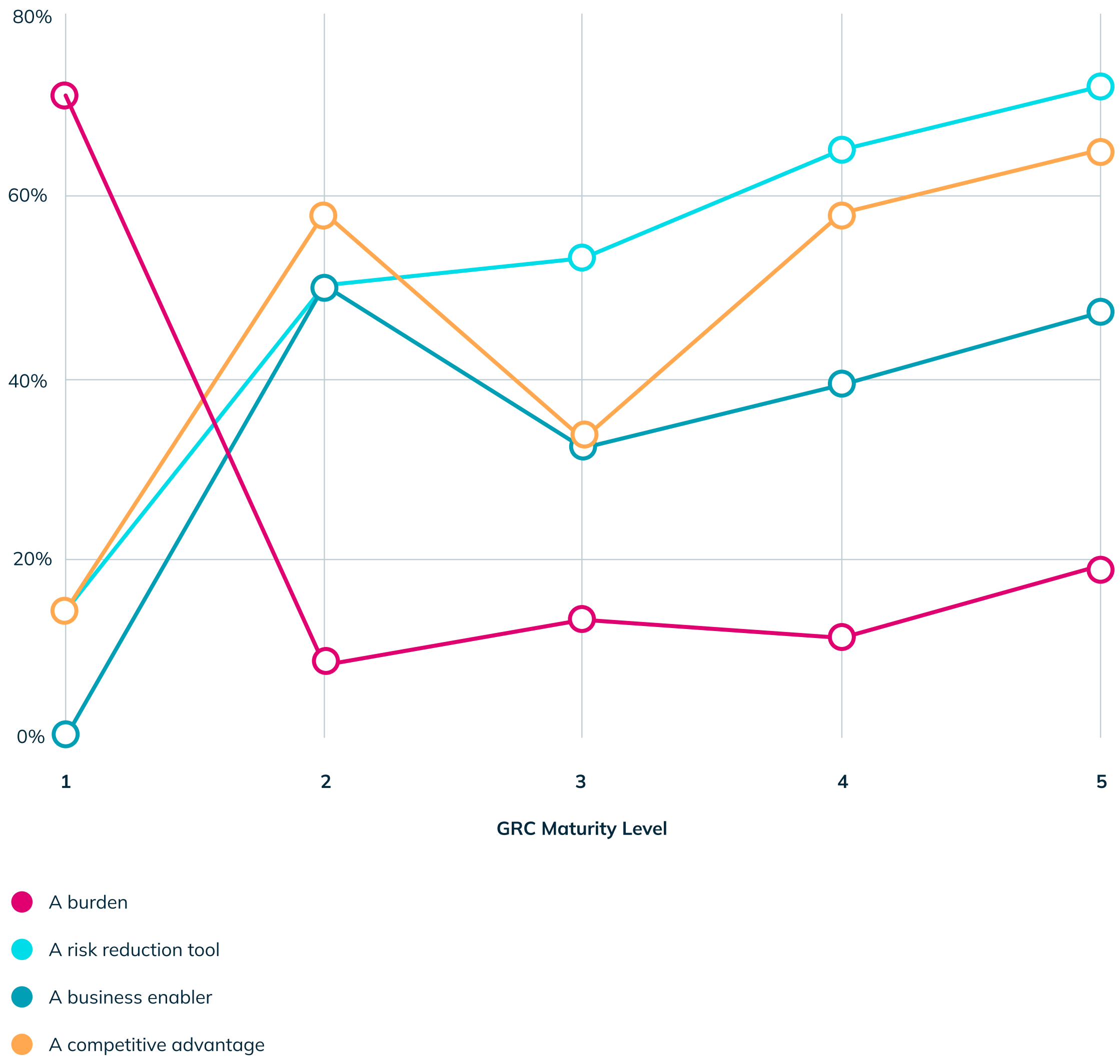
4. Reporting Can Make or Break Leadership's Perception of GRC

The least mature GRC programs aren't measuring success or winning executive support

Leaders don't see value in immature GRC programs, and there's not much reason they would. For GRC teams with the least mature programs, leaders overwhelmingly perceive GRC as a burden (71%). Fortunately, this negative perception quickly drops as maturity increases, and leaders' positive perceptions of GRC trend upward with increasing GRC maturity (Figure 22).

Figure 22

Leadership Perceptions of GRC by Maturity Level

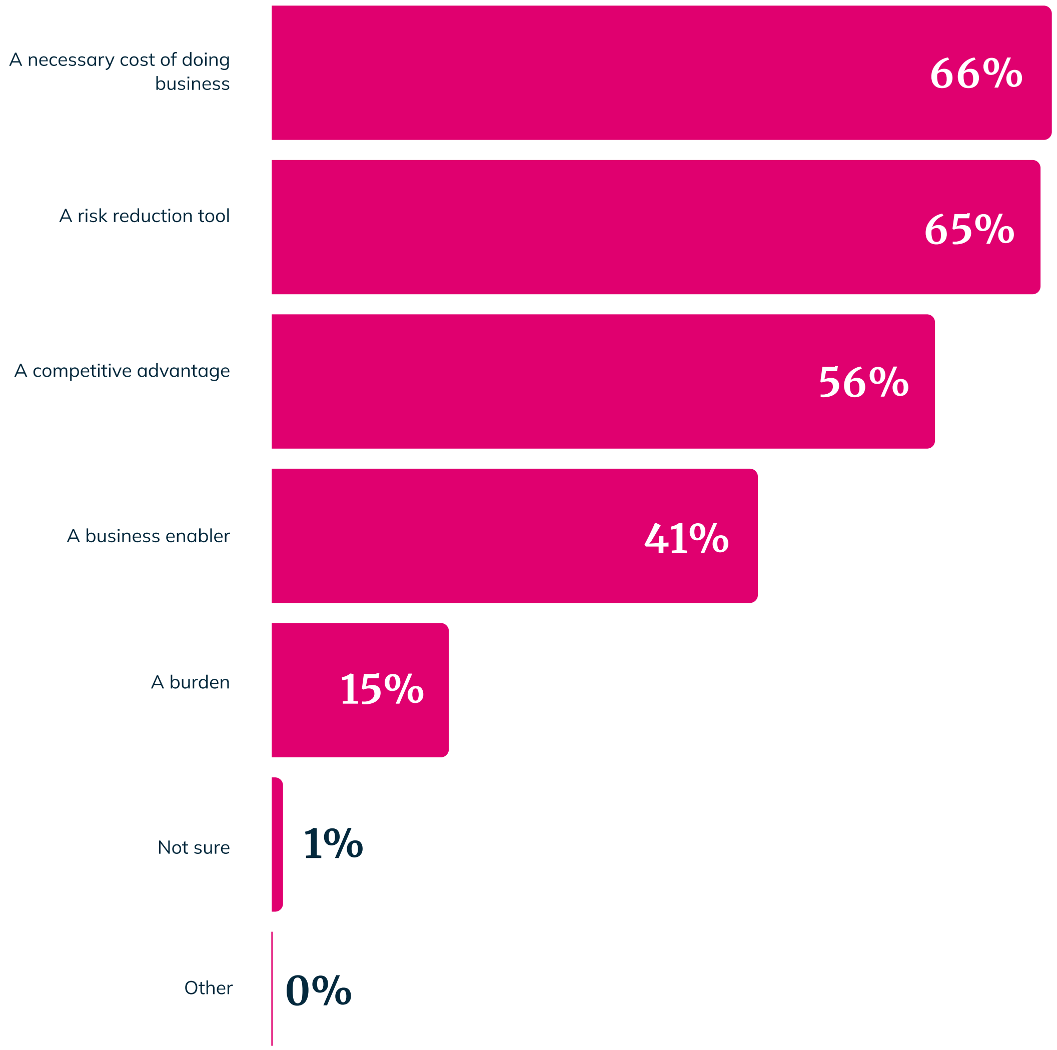


Use reporting to spotlight your work and shift leadership perception from burden to value

Reporting plays a crucial role in that shift. Organizations with highly mature GRC programs don't just focus on audit checklists—they connect their work to business outcomes. Less mature programs, if they report ROI at all, tend to focus on internal metrics like reducing risk or audit efficiency. The most mature programs are far more likely to prove ROI through measurable business impacts, such as customer trust scores (Figure 24).

Figure 23

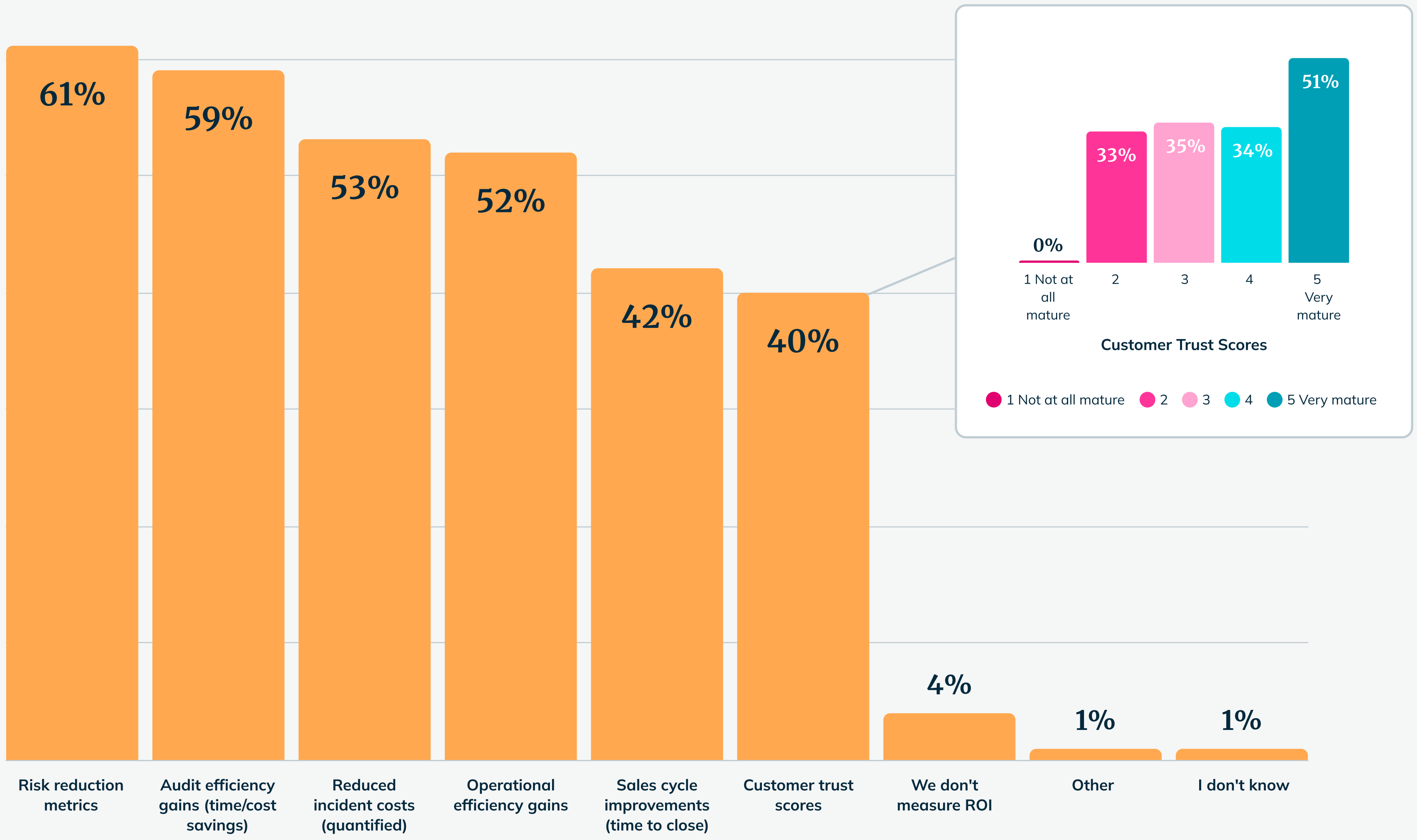
How respondents reported leadership sees GRC at their organizations



Respondents were able to select all that applied.

Figure 24

How do you prove the ROI of your GRC program?



Respondents were able to select all that applied.

Additionally, the most mature GRC programs are significantly more likely than less mature ones to report on three particular metrics:

- Operational efficiency and automation impact (up to 20% more likely)
- Regulatory changes and impacts (up to 38% more likely)
- Financial implications of compliance, such as fines avoided and cost savings (up to 35% more likely)

You might notice the last of these three speaks leadership's language most directly: money. Mature GRC programs use business metrics, like financials, as a standard practice in their reporting. Those who rated their programs very mature are more likely than those at a lower maturity level to do other business-focused reporting, too, such as:

- Reduced incident costs (up to 54% more likely)
- Sales cycle improvements (time to close) (up to 50% more likely)
- Customer trust scores (up to 51% more likely)

And there’s a broader lesson in how these teams report: they know their audience. Mature GRC programs speak to what leaders care about: business value, risk posture, and operational performance. They use reporting to make the case for continued investment, not just continued compliance.

How highly invested leaders prefer to see GRC reported

It’s worth looking at the type of reporting done by those who say they have highly supportive leaders. For example, according to the survey, leaders who see GRC as a competitive advantage and a business enabler are more likely to require reporting through metrics like the overall governance maturity score/trend.

5 Must-Have GRC Metrics & Reports

1. Compliance status against key frameworks (e.g., NIST, ISO 27001)
2. Regulatory changes and impacts
3. Overall governance maturity score/trend
4. Financial implications of compliance (e.g., fines avoided, cost savings)
5. Operational efficiency and automation impact

Takeaway #4

The right reporting is critical for GRC maturity. The most mature GRC organizations deliver metrics that tie directly to business results so they resonate with leadership and business stakeholders.

Take action

Wherever your program is on the GRC maturity journey, approach reporting as a vital feedback loop that helps leaders see the value of their investment. Use metrics that align with strategic priorities like cost savings, trust, and business enablement. Leverage automation and integrations to scale reporting so you can prove GRC's impact without piling on manual work.

*Exception: Those who rated their GRC programs at maturity level 2 were 8% more likely than even the most mature programs to report on sales cycle improvements. Though we have no direct evidence, logic suggests that this could very likely be because one of the first steps these teams are taking to mature their compliance programs is something like securing SOC 2 certification for the explicit purpose of accelerating sales cycles.

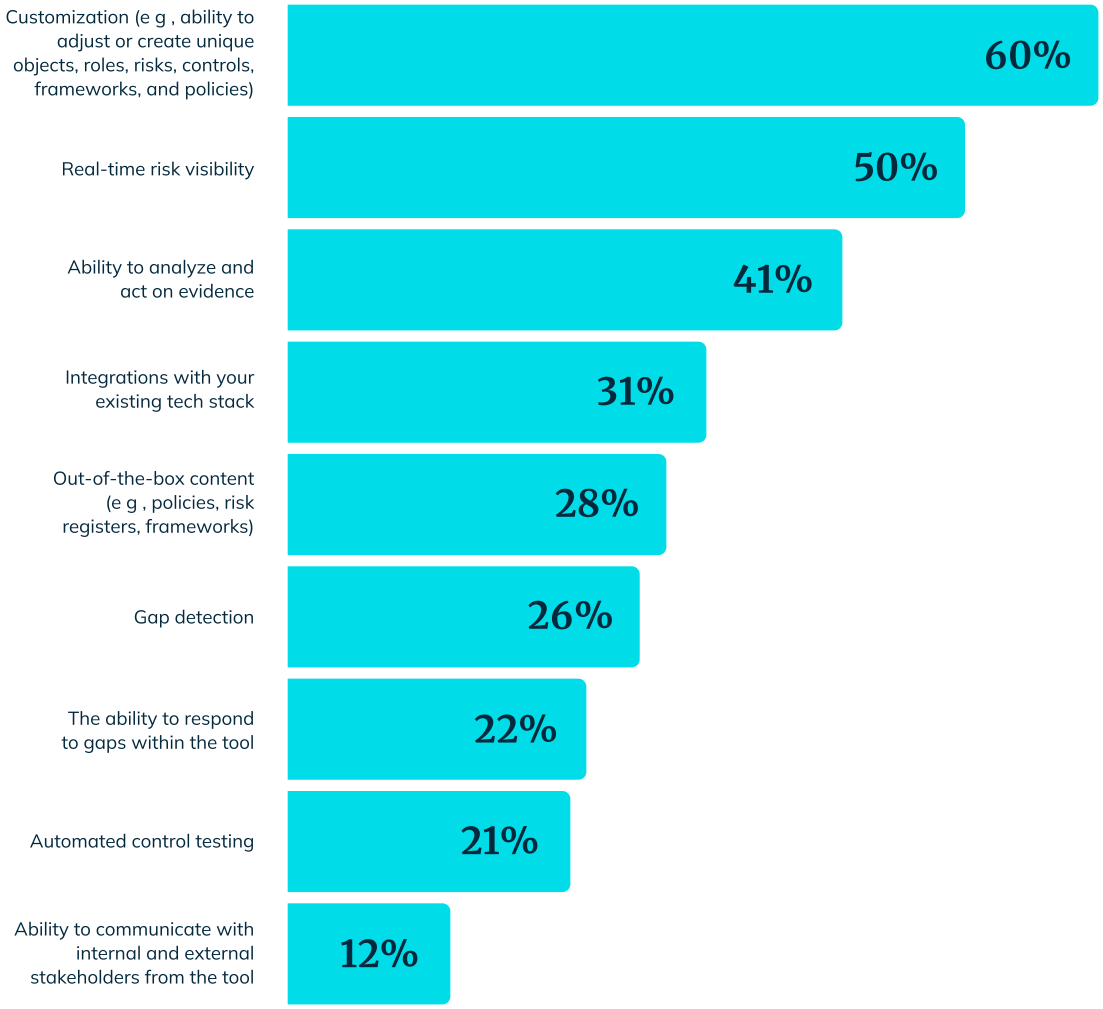
5. Custom Frameworks are GRC's Unsung Heroes

GRC professionals prioritize customization, but not custom frameworks

Scaling GRC means managing multiple frameworks. Customization is, by far, the respondents' most-wanted capability in a GRC tool or platform, with 60% of respondents choosing customization as one of their top 3 most important features (Figure 25). At the same time, slightly less than half of respondents report using a custom framework — a way to enjoy customization even without a GRC tool — to manage overlapping frameworks (Figure 26). As we'll soon see, they're missing out.

Figure 25

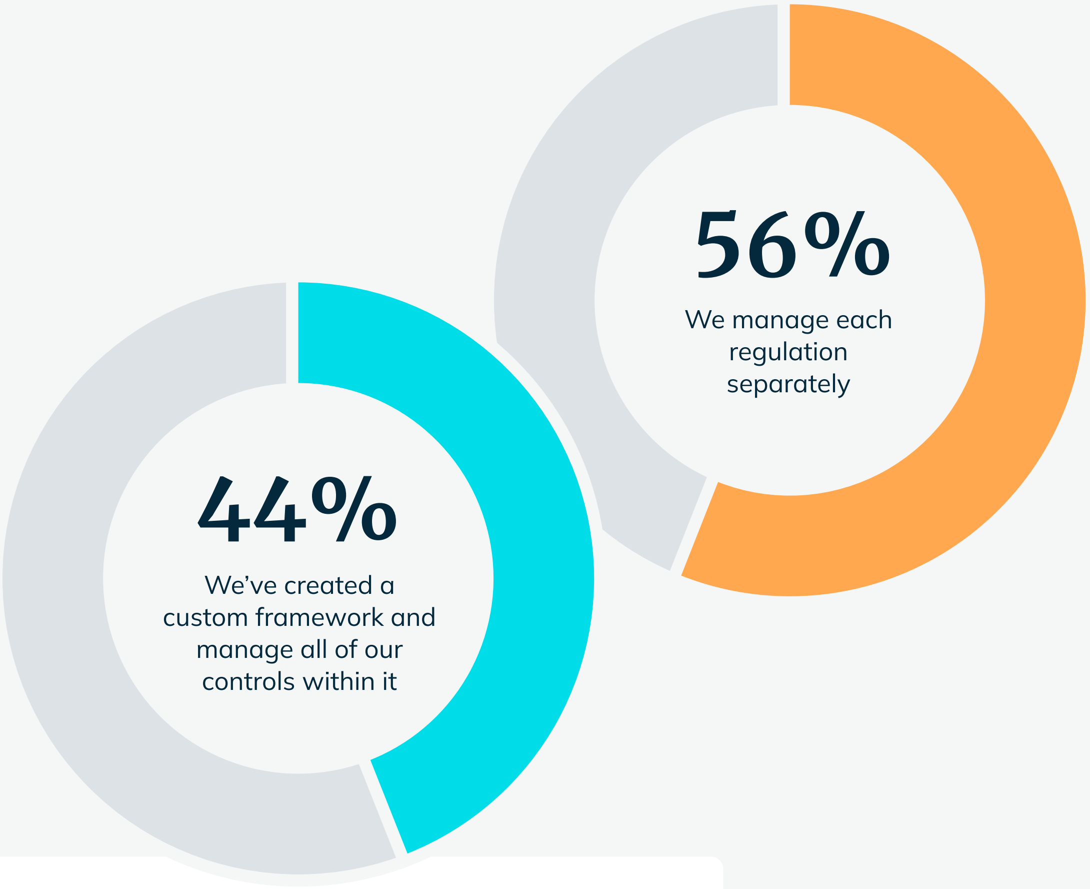
Of the following options, which are the most important in a GRC tool/platform?



Respondents could select up to 3 responses.

Figure 26

What is your approach to dealing with frameworks and regulations that overlap?



Leaders feel the difference when GRC programs use custom frameworks

The extra effort of managing each regulation separately is not just an internal challenge for the GRC team. If you need to collect the same piece of evidence for each framework, you are placing a greater burden on stakeholders as well.

When the GRC team juggles multiple separate frameworks, leadership is more likely to see GRC as a burden, presumably because of the added resources this approach requires.

On the other hand, leaders are much less likely to say GRC is a burden when they manage all controls in a custom framework (Figure 27, next page). Long time GRC practitioners also favor a custom framework. The more years of experience a GRC practitioner has, for example, the more likely they are to be managing controls using a custom framework (Figure 28, next page).

Figure 27

Leadership is far more likely to see GRC as a burden when regulations are managed separately

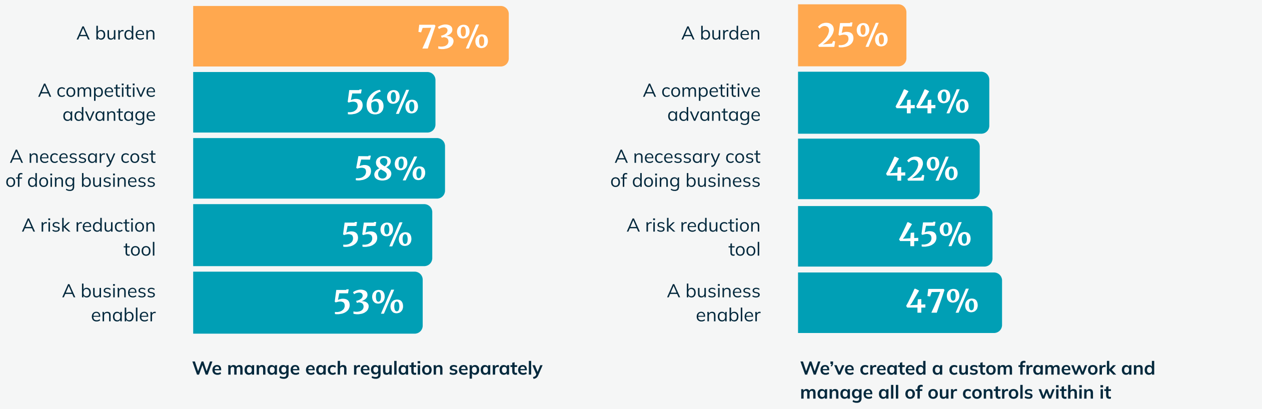
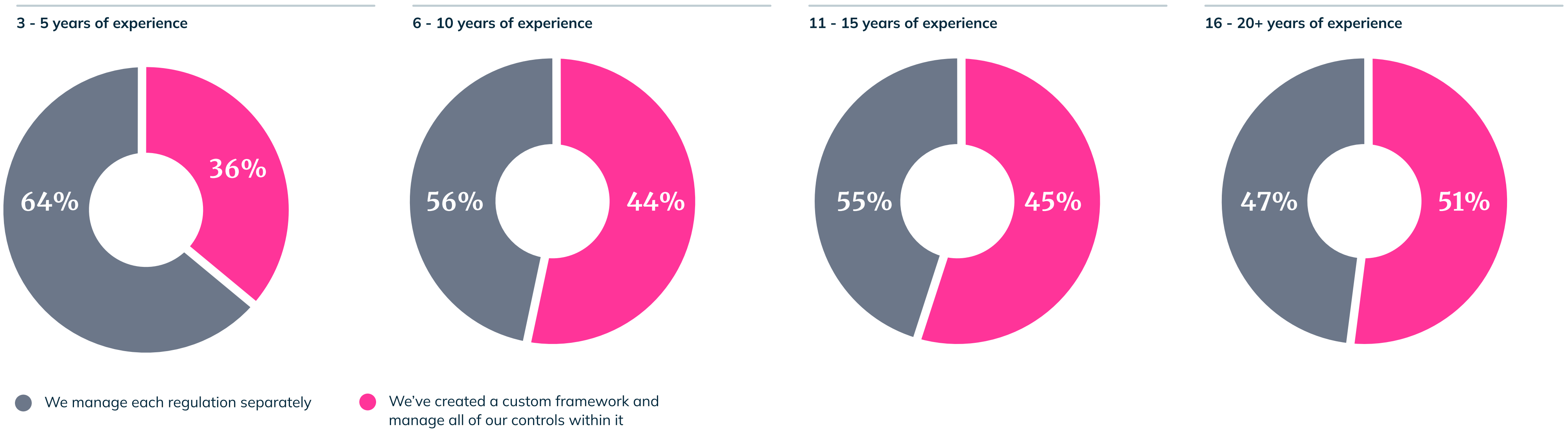


Figure 28

What is your approach to dealing with frameworks and regulations that overlap? By years of experience



Takeaway #5

Custom frameworks make it easier and more efficient to manage multiple compliance frameworks, reducing duplicated efforts. Listen to the wisdom of the most experienced GRC practitioners: Managing controls in a custom framework reduces compliance burdens (and leadership thinks so, too!).

Take action

Create a unified, custom framework to reduce rework, streamline audits, and free up your team to focus on higher-value activities that drive trust and business performance.

Conclusion: GRC maturity is a moving target, but the path is clear

This research affirms what many GRC professionals already sense: maturity is not about perfection—it's about proactivity, integration, and impact.

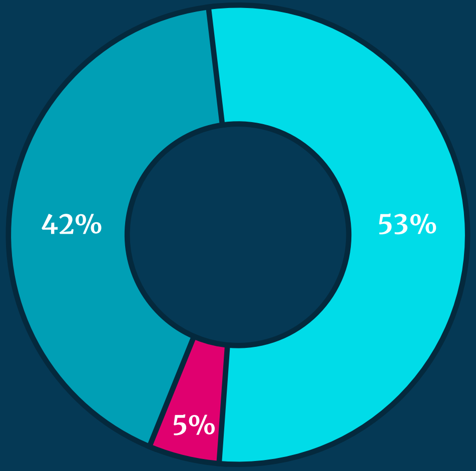
Organizations that rated themselves as most mature aren't just more automated. They report measurable ROI. They discover gaps when they happen. They use AI to solve both strategic and tactical challenges.

But even these mature teams have work to do. Too many still find gaps during audits. Too many still trust checkbox certifications. And too many aren't continuously monitoring their controls.

If you want to shift leadership perception, gain real-time visibility, and make your program a driver of trust, not just compliance, follow the patterns in this report. Start small, prove value, and scale what works.

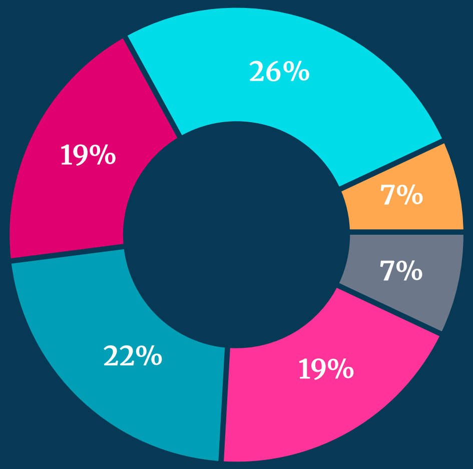
GRC maturity isn't a destination; it's a muscle. Build it by integrating more deeply across your business, investing in the right technologies, and reporting on what matters.

Demographics



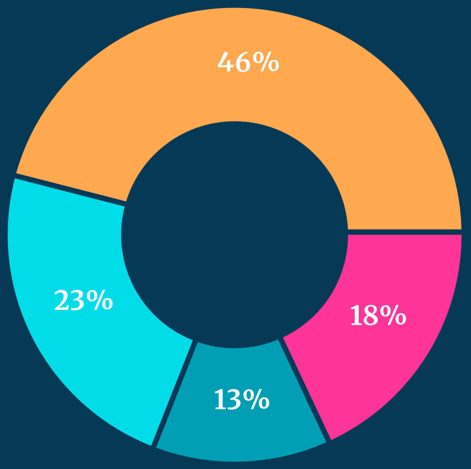
Department

- ● Information Technology (IT)
- ● Governance, Risk, and Compliance (GRC)
- ● Information Security (InfoSec)



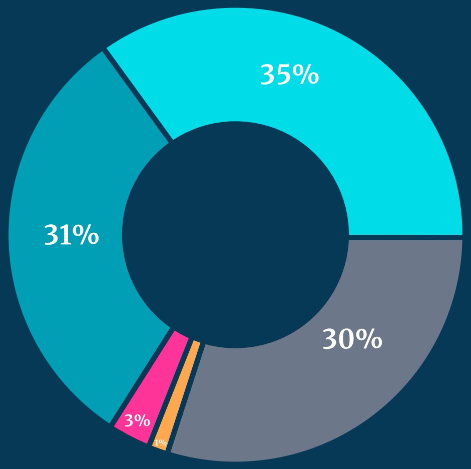
Company size

- ● 99 or fewer
- ● 100 - 249
- ● 250 - 999
- ● 1000 - 2499
- ● 2500 - 4999
- ● 5000 – 10,000+



Years of experience

- ● 3 - 5 years
- ● 6 - 10 years
- ● 11 - 15 years
- ● 16 - 20+ years



Role

- ● C-Level/SVP
- ● VP/Director
- ● Manager/senior professional
- ● Individual contributor
- ● Consultant/contractor

anecdotes

All Rights Reserved @ anecdotes.ai

Anecdotes enables GRC teams to strengthen and scale their GRC programs. By giving teams actionable GRC data, which is instantly mapped to any use case, coupled with AI-enhanced analysis tools and configurable automations, Anecdotes empowers GRC teams to quickly identify gaps—and attest to their organization's state of compliance with confidence. **For more information, visit anecdotes.ai.**