hyperproof

2024 IT Risk and Compliance Benchmark Report

CHARTING THE GOVERNANCE, RISK, AND COMPLIANCE UNIVERSE

A comprehensive look at how companies are responding to the ever-evolving compliance and risk landscape

Table of Contents

FOREWORD

Redefining Trust: **Navigating the GRC Galaxy**

FOREWORD

Redefining Trust: **Navigating the GRC Galaxy**

Hyperproof's fifth annual IT Risk and Compliance Benchmark Report is here.

Each year, we ask over 1,000 IT and GRC professionals about their organizational priorities for the coming year and operational aspects, like changes to budgets, staffing, challenges, and much more.

The survey also dives deep into the market's current state and outlines trends and best practices based on how top teams are responding to the ever-changing risk and compliance landscape.

2023 was the year of risk: a milestone year where the new SEC requirements forced C-Suites and boards to truly understand their own risk levels. As a result, they began to dig into their organizations' risks more and ask tougher questions. This pushed GRC professionals to level up their responses to risk and marked a significant shift away from checkbox compliance toward strategic compliance operations. Organizations needed to prove to both external market regulators and to their customers and prospects that they were doing everything possible to mitigate risk.

Now – beyond leadership pressures – GRC professionals are asked to navigate a new galaxy of new regulations and external stakeholders, including regulatory bodies, who demand true transparency.

Now – beyond leadership pressures – GRC professionals are asked to navigate a new galaxy of regulations and external stakeholders, including regulatory bodies, who demand true transparency. They are also balancing the needs of an expanded set of internal stakeholders as companies are increasingly working to democratize risk and compliance management across organizations. This has resulted in increased cross-team collaboration, forcing GRC and IT professionals to consolidate tech to a single solution, all in the pursuit of redefining trust for their organizations.

Things get even more complicated when considering that the very concept of "trust" has been upended in the security and GRC community. For example, the Zero Trust security model, first popularized over a decade ago, has garnered mixed reactions from GRC professionals. Marketing hype quickly co-opted the term, creating confusion and misunderstanding about the actual definition of Zero Trust and driving skepticism about its practical, real-world implementation.

Thus, even the word "trust" in the cybersecurity community has become muddled with uncertainty leaving GRC professionals wondering: what does redefining trust actually look like?

According to our survey, the key to reclaiming trust lives within your data, processes, and workflows. Overwhelmingly, more GRC professionals than ever are reducing data silos between risk management and compliance operations so they can get a clearer view of their true compliance postures. This shift for clarity is also being driven by GRC becoming a strategic differentiator rather than simply a cost center, and you will see this theme throughout our data.

In addition to the data derived from our survey results, this report includes exclusive industry insights from Hyperproof and how you can leverage this data to accelerate your business.

> *Overwhelmingly, more GRC professionals than ever are reducing data silos between risk management and compliance operations.*

So, what will the impact be in 2024?

Our survey results revealed that more companies than ever are viewing GRC as a holistic process and taking steps toward getting a complete view of their risk environment and regulatory obligations. Centralizing strategy, unifying risk and compliance data, and revamping the approach to cybersecurity are becoming more popular strategic objectives among respondents, especially with the rise of AI technology dismantling barriers and fostering collaboration among various GRC functions. This means the criteria for which GRC technology is being evaluated against in the purchase cycle is rapidly expanding.

Disparate point solutions are no longer good enough, and internal audit, risk, IT, and compliance committees are looking for a single solution to best address their needs. The question is: **which team's priorities will take precedence?**

With increased interest in artificial intelligence (AI) also comes concern around AI compliance risks, and regulators are feeling the pressure to quickly adapt to keep up. GRC professionals should prepare for an onslaught of new regulatory updates.

> *Disparate point solutions are no longer good enough, and internal audit, risk, IT, and compliance committees are looking for a single solution to best address their needs.*

The Biden Administration and Europe will move forward with more regulation of AI, New York will move forward with enforcement of its newly updated cybersecurity rule, 23 NYCRR Part 500, and California will do the same with its newly updated privacy law, The California Privacy Right Act.

All of that progress will inform GRC professionals' understanding of how much regulation their organizations will face and what business needs to prioritize. Strengthening the fundamentals of your compliance program – **gaining better visibility into reporting**, automating more workflows, improving control testing and analytics, increasing the accuracy of risk assessments, and improving audit trails and documentation – will be key to adapting to this expanding landscape.

Statistical Stargate:

Illuminating the Top Findings in Numbers

Illuminating the Top Findings in Numbers

49%

struggle with identifying critical risks to prioritize remediations

Although the vast majority of respondents are highly confident in their ability to address risks, our results show that their workflows have yet to be optimized.

18%

have aligned their compliance and risk activities

Although this number remains low, it represents an 80% increase from 2023 where 10% of respondents reported having an integrated view on how they manage risks and have tied risk and compliance activities together.

14%

use spreadsheets to manage their IT compliance

Although GRC software usage for risk tracking, risk management, IT compliance management, and third-party risk management is on the rise, the use of spreadsheets has increased by 40% year-over-year.

Illuminating the Top Findings in Numbers

83%

have a centralized GRC program

This is a notable increase from last year's report, where only 68% of respondents reported having a centralized GRC program.

19%

manage IT risks in siloed departments, processes, or tools

Last year, 31% managed IT risks in silos, indicating that GRC silos are reducing and teams are looking for more unified solutions.

59%

experienced a data breach in the last 24 months

Unfortunately, breaches are on the rise; this is a notable increase from last year's report, where only 42% experienced a breach during the same time frame.

Illuminating the Top Findings in Numbers

69%

expect to spend more money on IT risk in 2024

Although the macroeconomic climate and other reputable industry surveys indicate budgets are flattening or reducing, our survey data indicates that GRC professionals expect their budgets to increase in 2024.

80%

view AI strategy for their teams' operations as important

Those who use a mostly automated integrated governance, risk, and compliance tool were also more likely to consider AI strategy very important.

60%

expect to spend more time on IT risk in 2024

As regulatory scrutiny continues to increase, GRC professionals are dedicating at least 6% more of their time year-over-year to IT risk.

CHAPTER 1

Navigating Tomorrow, Unifying Today: **Integrating Risk and Compliance**

CHAPTER 1

Navigating Tomorrow, Unifying Today: Integrating Risk and Compliance

> Data silos between risk management and compliance operations are reducing, but those still operating in silos are more likely to experience a breach.

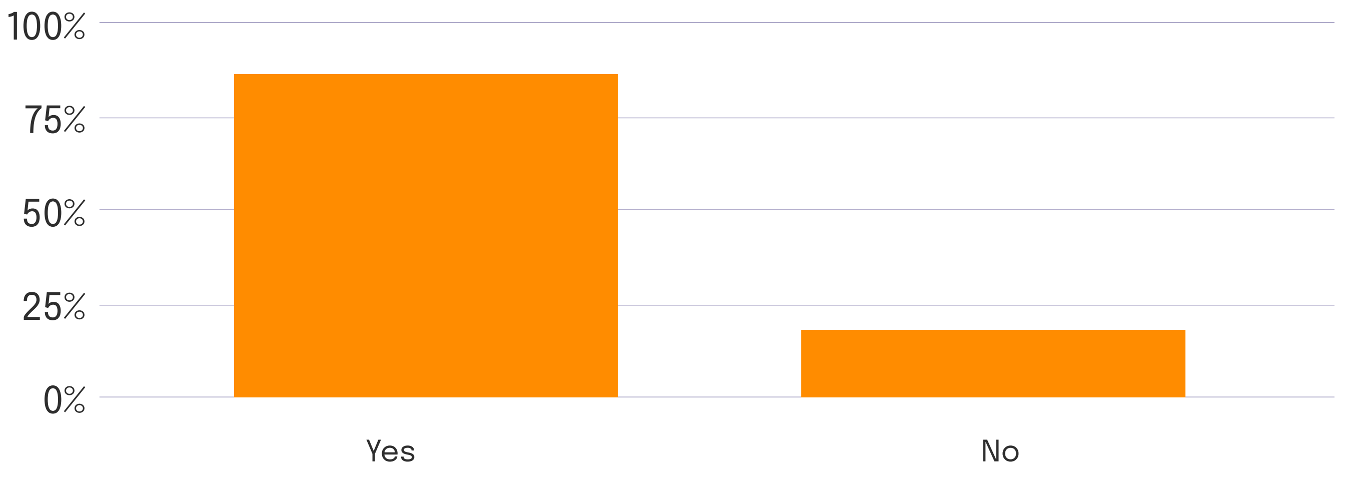
Respondents are moving toward unifying risk and compliance management operations, with **only 19% of respondents saying they manage IT risks in siloed departments, processes, or tools** vs. 31% in 2023. This indicates a greater industry shift toward unifying risk and compliance management. Some respondents have taken it a step further with 18% saying they have an integrated view of how to manage their unique set of risks, up from a mere 10% in last year's report. This trend shows a push toward a more unified approach to GRC, where collaboration and having a complete, transparent view of an organization's risk is the priority. It also emphasizes that GRC solutions need to raise the bar on their product offerings to satisfy the needs of teams across the organization beyond typical GRC stakeholders.

Those who were slow to make the shift away from a siloed approach were more likely to experience a breach. 84% of respondents who have not tied risk and compliance activities together experienced a supply chain disruption related to cybersecurity that affected ability to deliver goods or services, and **70% of respondents who have not integrated risk and compliance activities experienced a breach in the last 24 months**.

The push toward centralization

Last year, 68% of respondents reported having a centralized GRC program, a figure that **has witnessed a substantial leap to 83% in 2024.** This shift towards centralization holds promise for a more integrated and streamlined approach to governance, risk, and compliance. However, the optimism surrounding centralized GRC programs is met with a stark reality: **only 18% of respondents have successfully tied together risk and compliance activities**. This disconnect between high confidence and the actual integration of GRC processes reveals a persistent challenge reminiscent of last year's report, where confidence in addressing risk did not align with the efficacy of risk management processes.

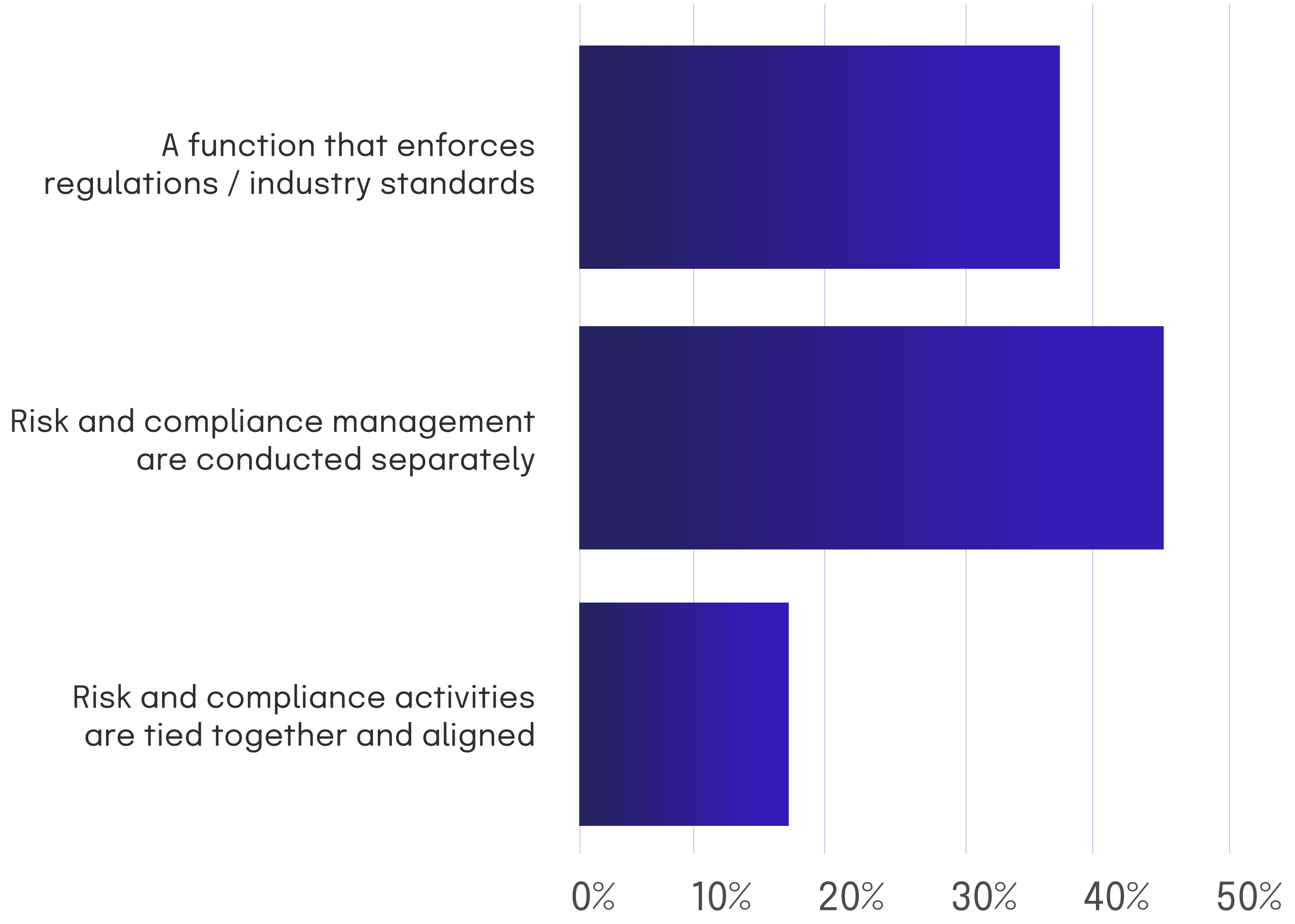
Does your organization have a centralized GRC program that works across business units and geographies?



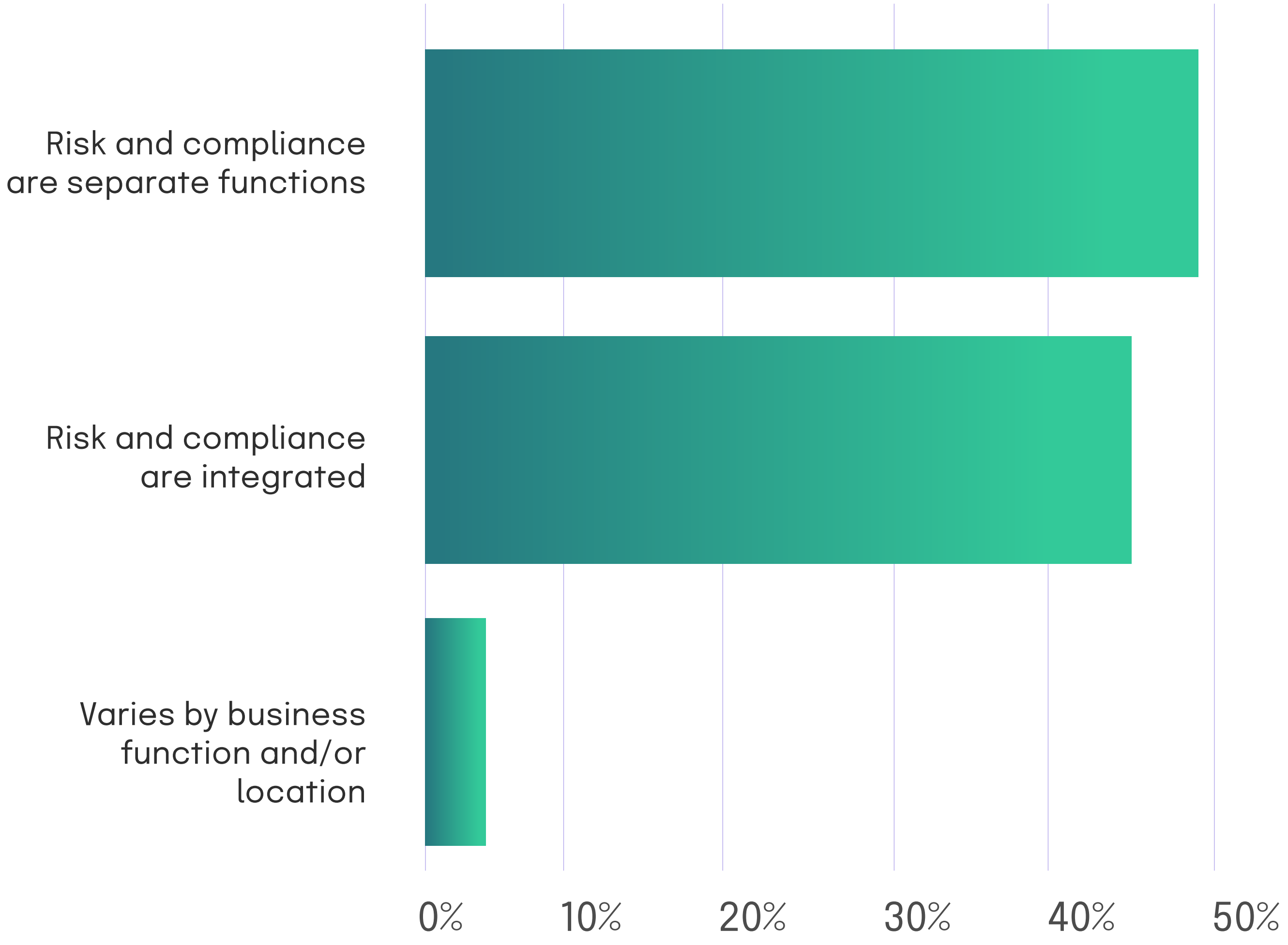
In a noteworthy transformation, **the percentage of respondents who view risk management and compliance operations as separate activities has decreased from 57% to 45% year-over-year.** Though we are seeing a market trend towards unification, the pace of change still suggests that organizations do not necessarily see or understand a clear way to get there easily.

Despite this decrease, nearly half of respondents still manage their risk and compliance functions separately. In fact, the number of those who have integrated risk and compliance responsibilities decreased by 13% year-over-year.

What statement best reflects how your organization views the purpose of the compliance function?



Is the risk management function a distinct and separate function from the compliance function at your organization?



Siloed approaches continue to create dangerous risks

Yet, amidst this positive shift, challenges persist. While 91% of respondents managing IT risks in siloed departments assert that their risk mitigation practices meet their companies' objectives, the reality paints a different picture. **Those who manage risk and compliance in silos are more likely to experience breaches,** with 70% of respondents in this category facing security incidents in the last 24 months.

In contrast, the numbers reveal a significant drop in breach incidents for those adopting an integrated, automated approach – only **46% of respondents using a GRC tool experienced a breach**. This stark contrast underscores the critical importance of moving beyond siloed approaches and towards integrated, automated solutions for effective risk and compliance management, since **those with an integrated and automated approach are less likely to experience a breach**.

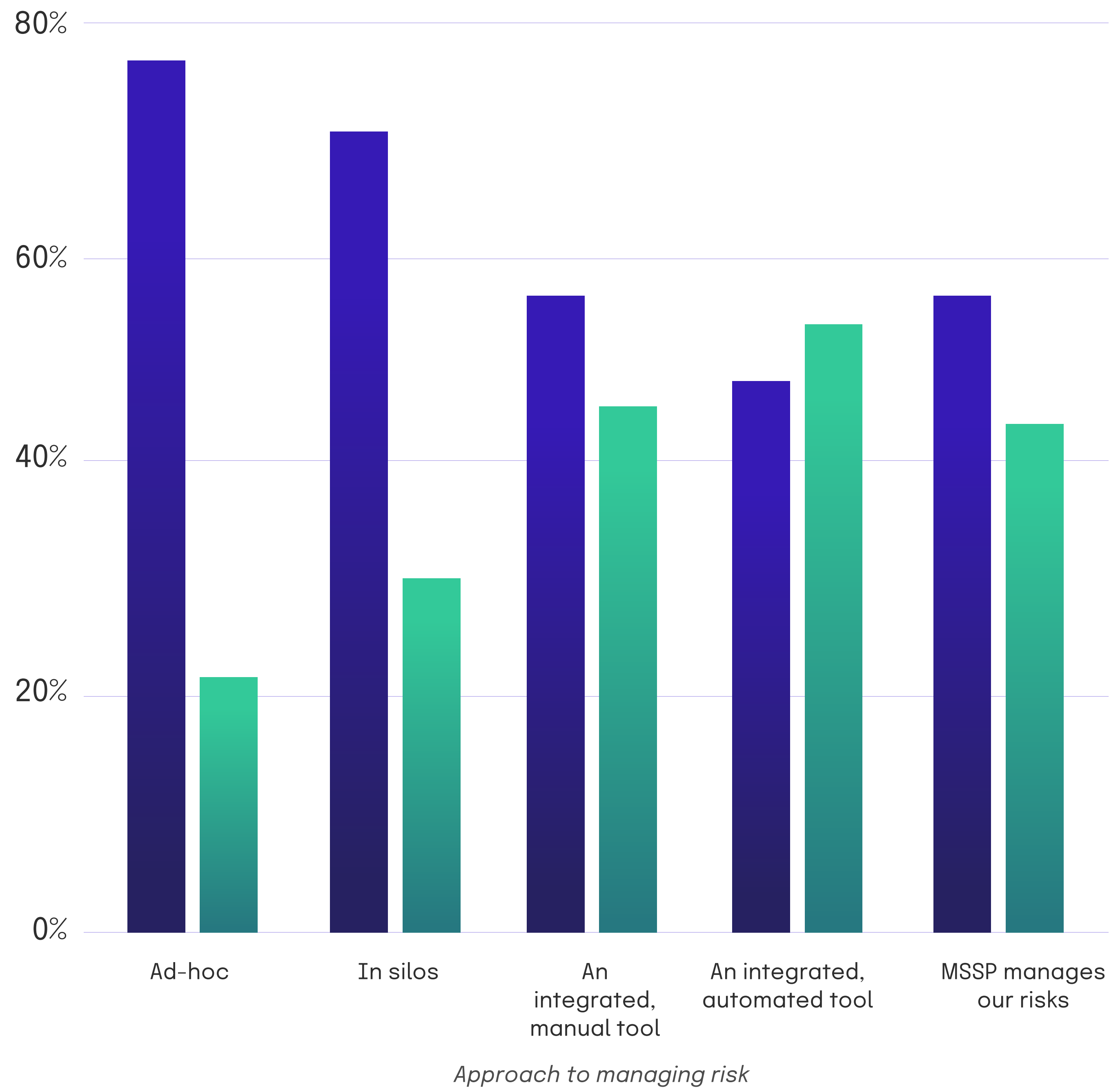
KEY STAT

70%

managing risk and compliance ***in silos*** *experienced a breach*

Notably, those with MSSPs managing their risks were also 22% more likely to experience a breach than those with an integrated, automated tool. Respondents managing risk themselves had markedly better outcomes than those outsourcing risk management to MSSPs, indicating that relying on external risk management professional services might actually open companies up to more vulnerabilities.

Has your organization experienced a breach in the last 24 months?



Why are organizations with integrated risk and compliance activities less prone to data breaches and more efficient in managing their compliance programs?

We found that these integrated organizations are more likely to be attentive to the controls they've put in place to ensure that security objectives are met. Organizations in the integrated cohort are better at identifying controls for risk mitigation, identifying and assessing risks, flagging control deficiencies, assessing control effectiveness, aligning controls with risks, and remediating issues than organizations in the other two cohorts.

How well is your company doing in performing each of the following risk management actions?

Summary of: Meets company objectives

How respondents view the purpose of the compliance function:

	Function that enforces regulations or industry standards	Risk and compliance activities are conducted separately	Risk and compliance activities are tied together and aligned
Identify and assess risks	92%	90%	94%
Identify controls	66%	68%	75%
Validate controls against standard controls	73%	71%	71%
Align controls with risks	67%	68%	76%
Monitor and automate controls testing	75%	75%	71%
Flag exceptions, review, and remediate	66%	67%	70%
Assess controls effectiveness	76%	76%	78%
Capture, track, and report deficiencies	67%	67%	73%

Most commonly used compliance frameworks

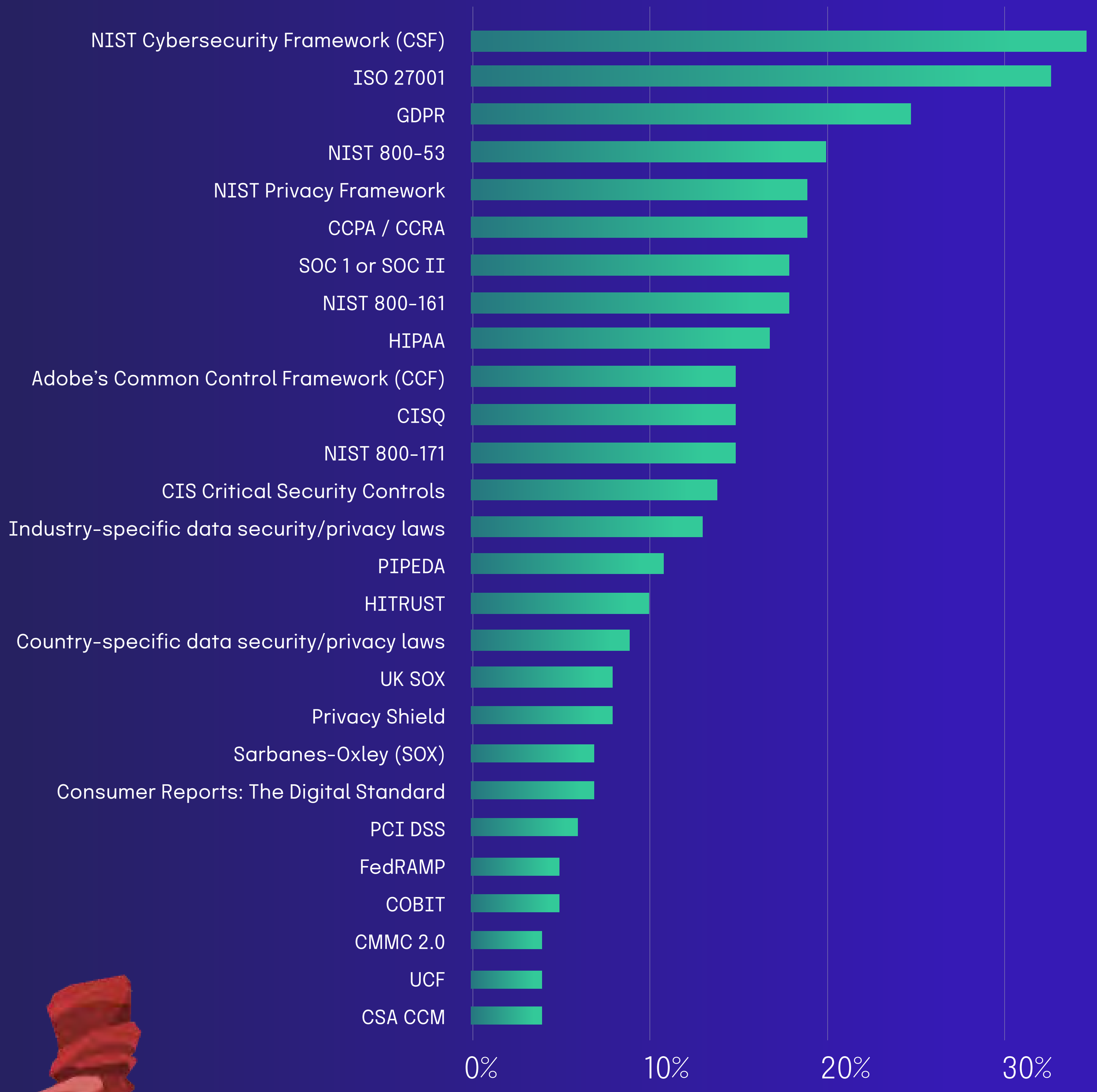
NIST CSF remained the most commonly used compliance framework year-over-year, while COBIT saw the most significant drop: 77% decrease. ISO 27001, unsurprisingly, was the second most common framework, followed by GDPR, which rose in usage by 56% year-over-year.

KEY STAT

NIST CSF

is the most commonly used compliance framework year-over-year

Which cybersecurity and/or data privacy compliance frameworks does your organization adhere to or plan to adhere to in the next 12 months?

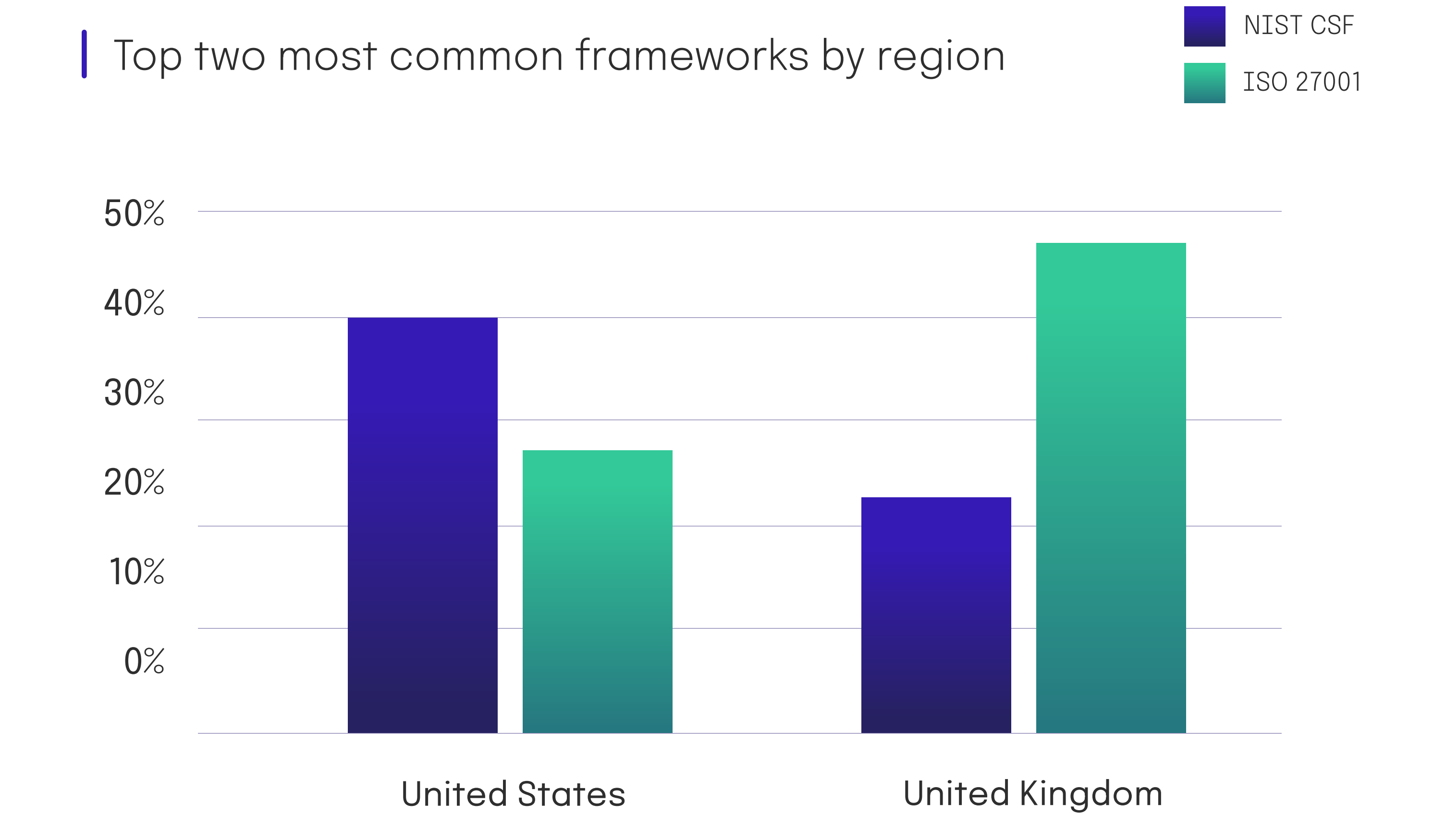


Segment differences

BY REGION

NIST CSF was the most widely used framework overall, but it has been adopted at a much higher rate for US-based companies. 40% of respondents headquartered in the US use NIST CSF, versus only 23% in the UK. Additionally, 47% of respondents based in the UK use the ISO 27001 framework – the second-most popular framework overall – as opposed to only 27% of US respondents. This aligns with the general perception that while NIST CSF is the most commonly used framework in the US, ISO 27001 is a more ubiquitous framework around the world and more commonly adopted in the UK. Interestingly, 18% of respondents in both the UK and US use SOC I and SOC II, indicating that the framework is becoming more widespread globally.

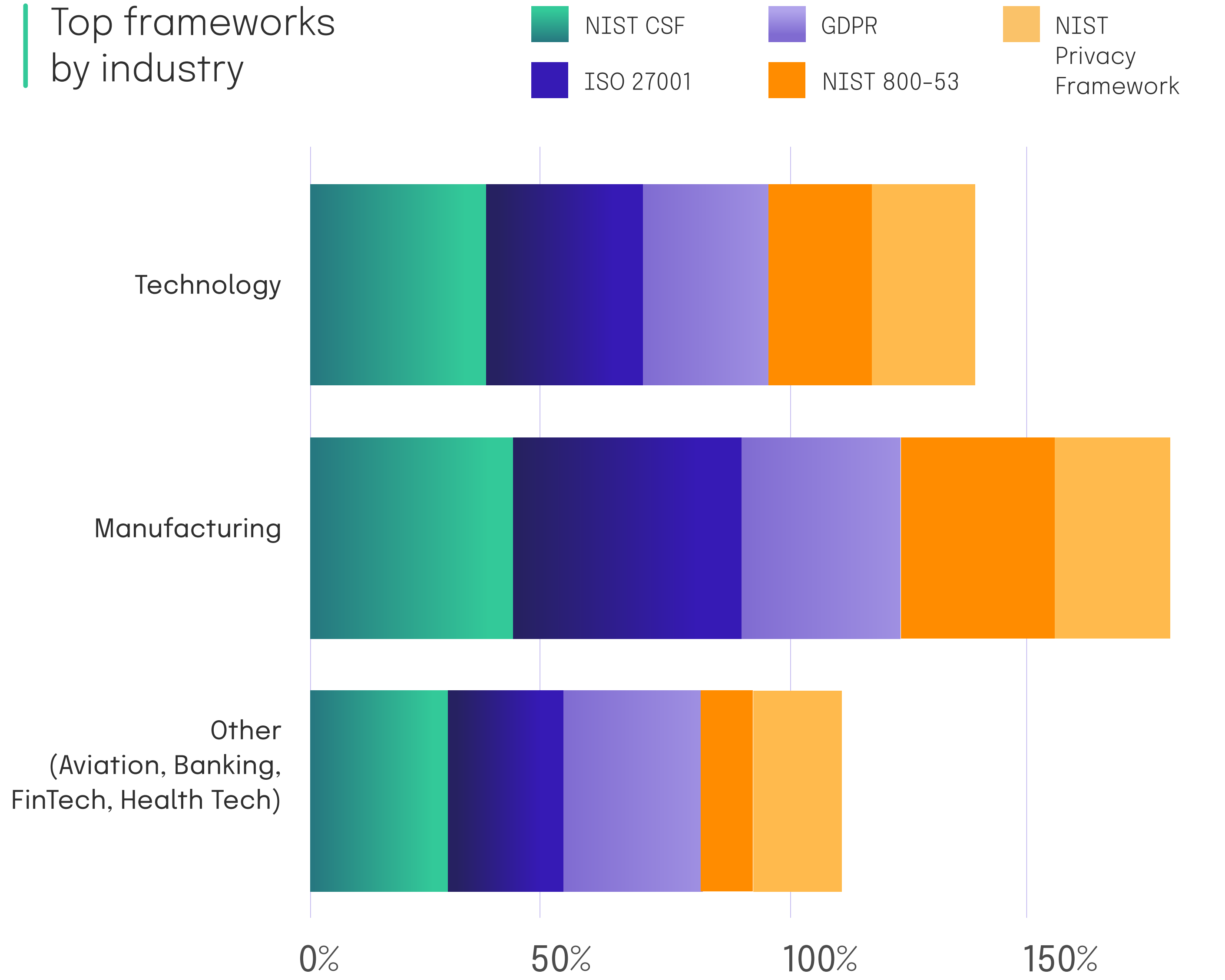
Top two most common frameworks by region



BY INDUSTRY

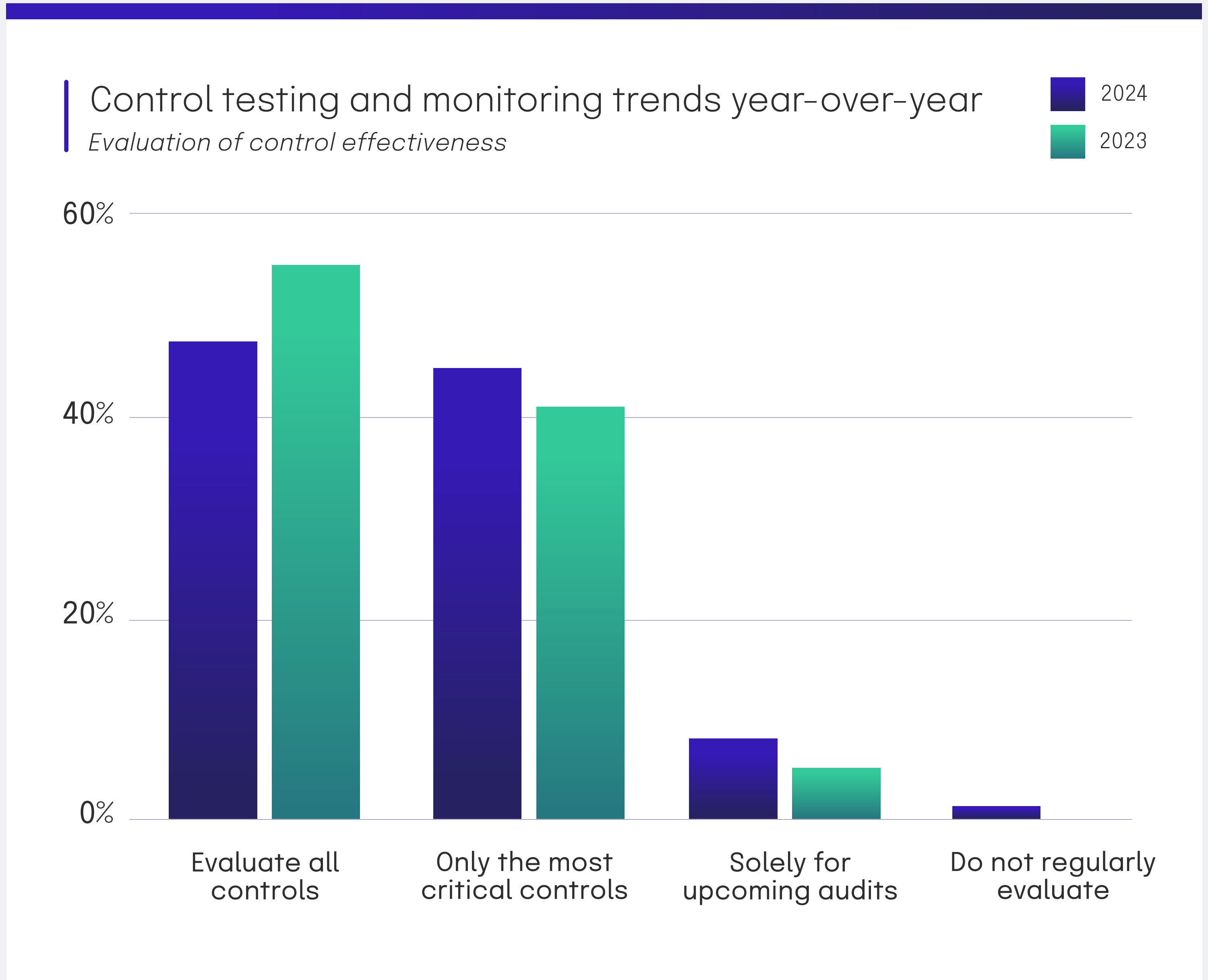
When looking at the top five most popular frameworks used by the industries surveyed, we found that NIST CSF was the most commonly used framework by the technology industry. The manufacturing industry stood apart as using ISO 27001 the most, and the aviation, banking, FinTech, and health tech industries adhered to the GDPR framework the most out of the top five frameworks.

Top frameworks by industry



Control testing and monitoring trends

We saw a year-over-year drop in the number of respondents who test all of their controls, as opposed to those who test only the most critical controls or test controls as-needed for their next audit. One explanation for this drop is that in 2023, GRC teams received fewer resources than the previous year, which required them to prioritize and only focus on the critical controls essential for their businesses.

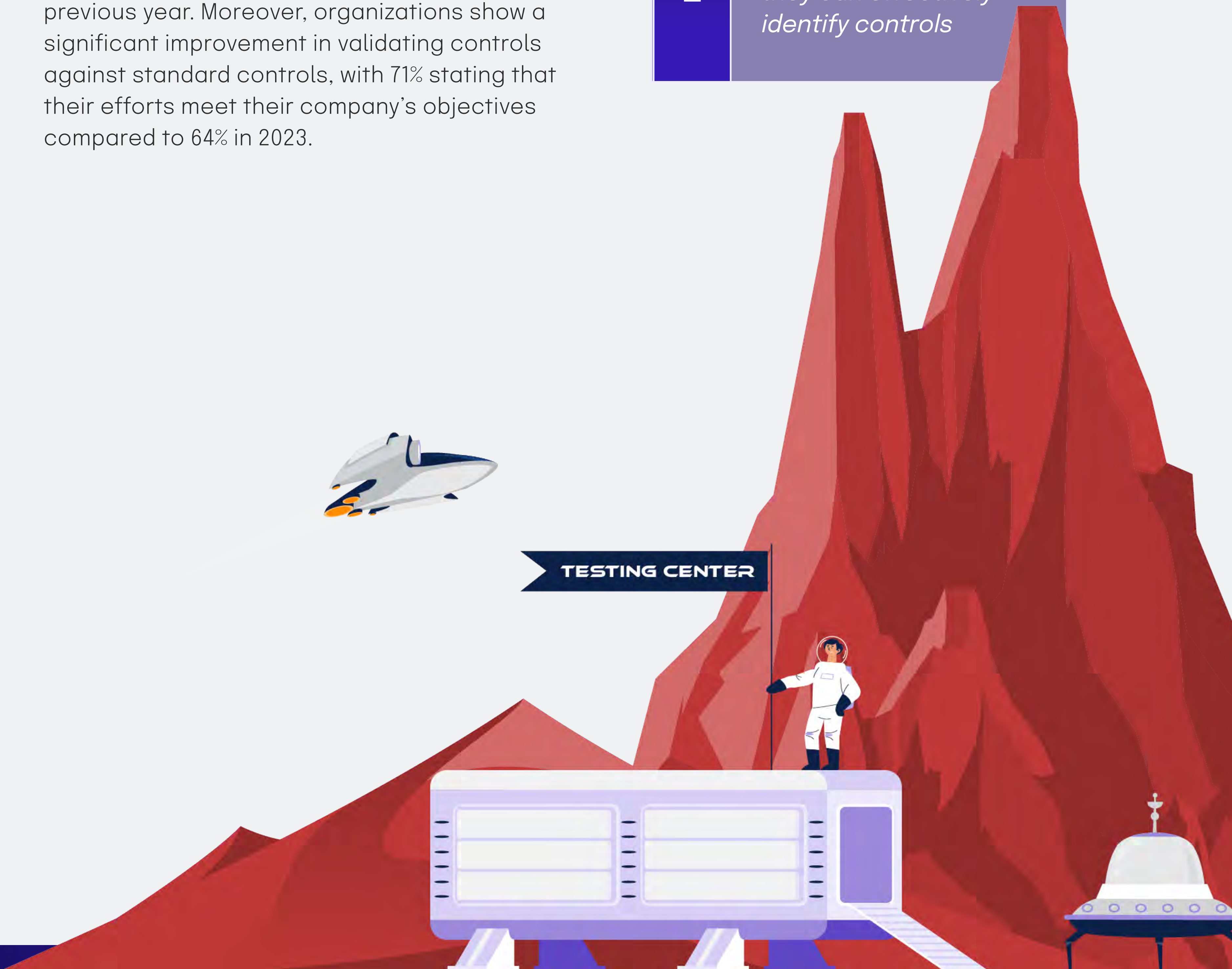


While the trend towards effective controls monitoring and automation sees a 9% decrease year-over-year, there are notable successes in specific aspects. A commendable 71% of organizations state they can effectively identify controls, maintaining consistency with the previous year. Moreover, organizations show a significant improvement in validating controls against standard controls, with 71% stating that their efforts meet their company's objectives compared to 64% in 2023.

KEY STAT

71%

of organizations state they can effectively identify controls

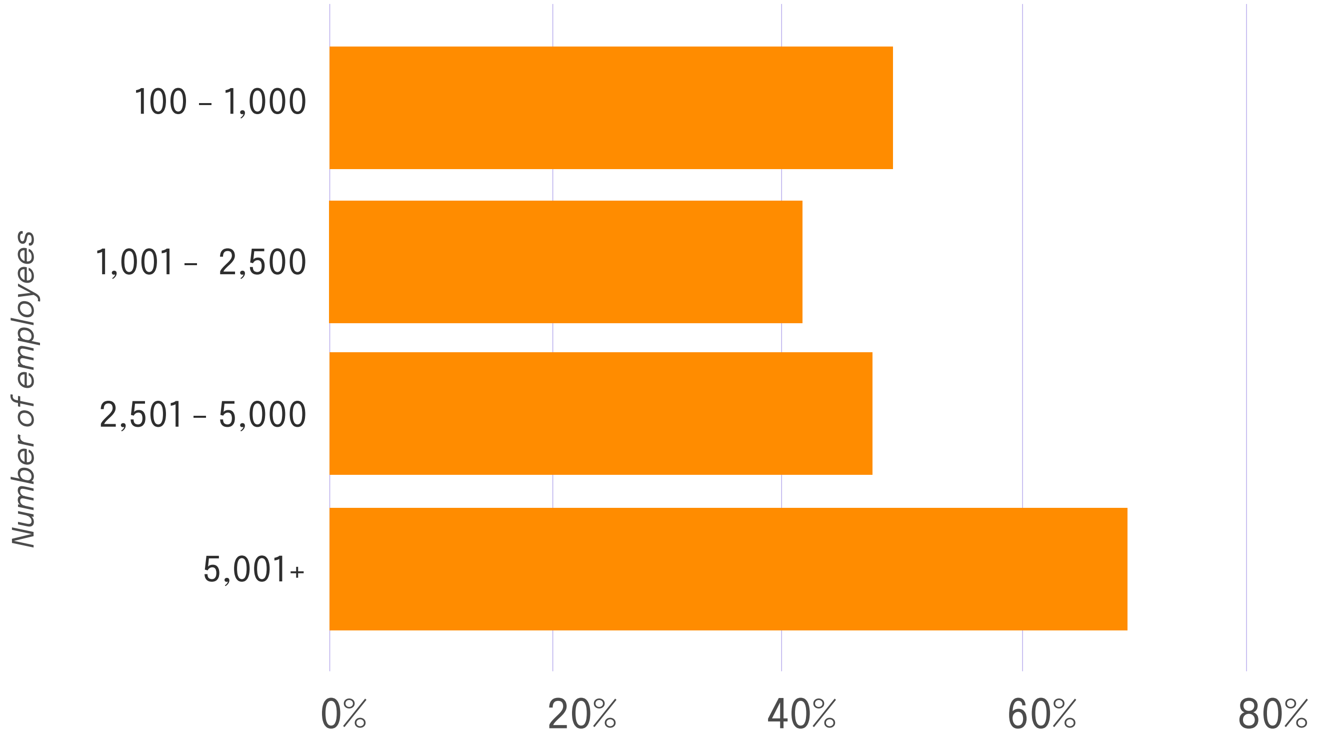


Large organizations are more likely to test all controls

67% of large organizations with 5,000+ employees test all of their controls, more than any other company size surveyed, likely due to the fact that they have more extensive and complex operations involving numerous business units, departments, and processes. The scale of their operations requires a comprehensive approach to control testing to ensure that all facets of the organization are adequately assessed for risks and compliance. Testing all controls becomes essential to manage the complexity of their business landscape. They are also frequently subject to a broader array of regulatory requirements due to their size, industry influence, and geographic reach. Compliance with these regulations demands thorough control testing to demonstrate adherence to various standards and mitigate legal and regulatory risks.

Do you evaluate all controls in your organization?

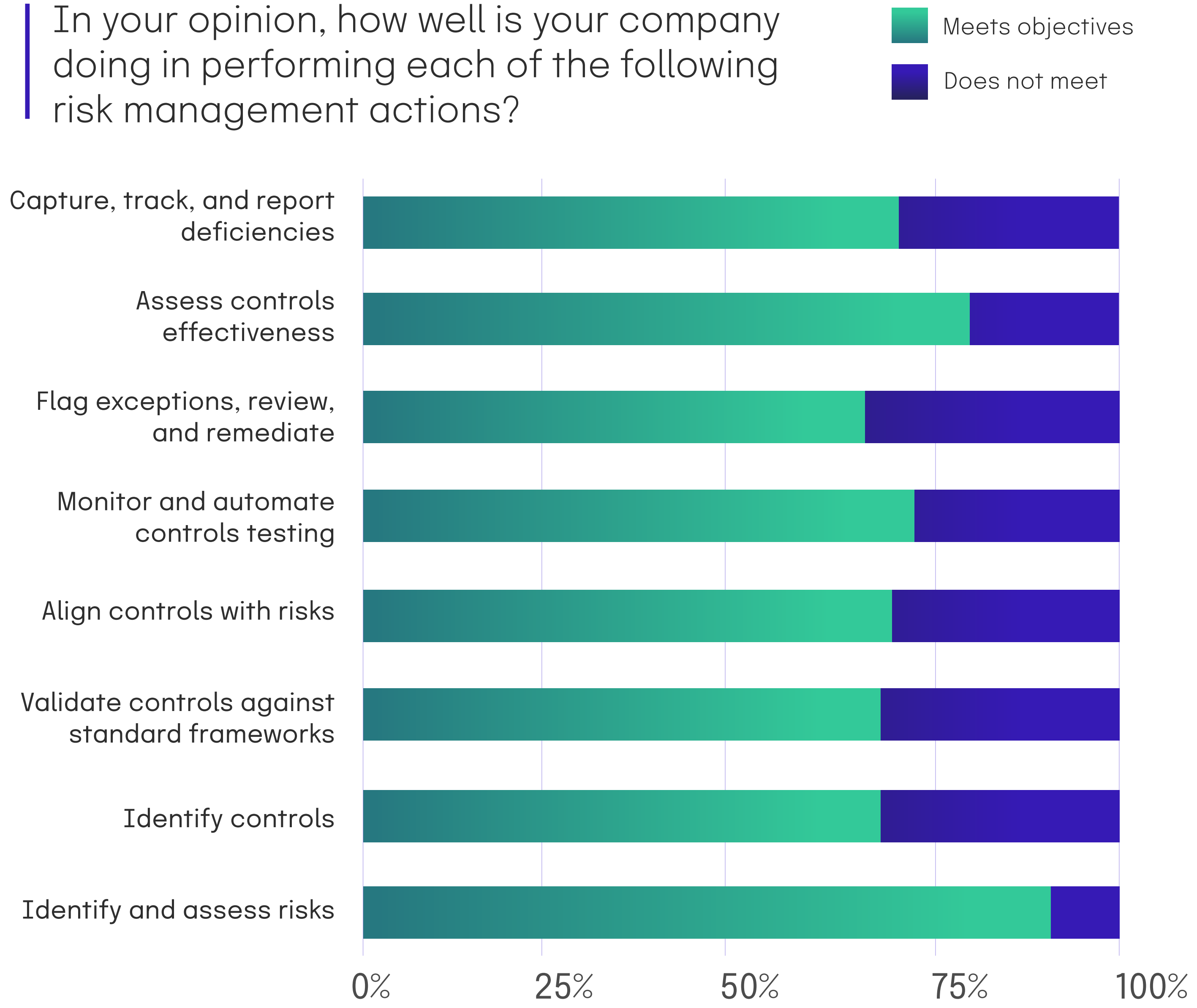
By company size



Aligning controls with risks

72% of organizations surveyed state that their efforts to align controls with risks meet their company's objectives. Although this marks a slight decrease of 6% year-over-year, the majority of organizations continue to emphasize the importance of aligning controls with identified risks.

In your opinion, how well is your company doing in performing each of the following risk management actions?

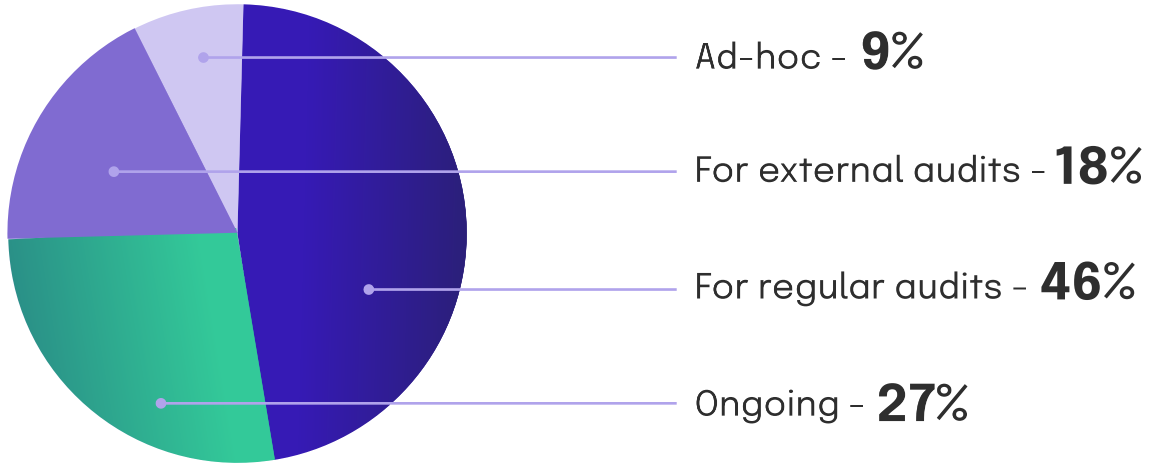


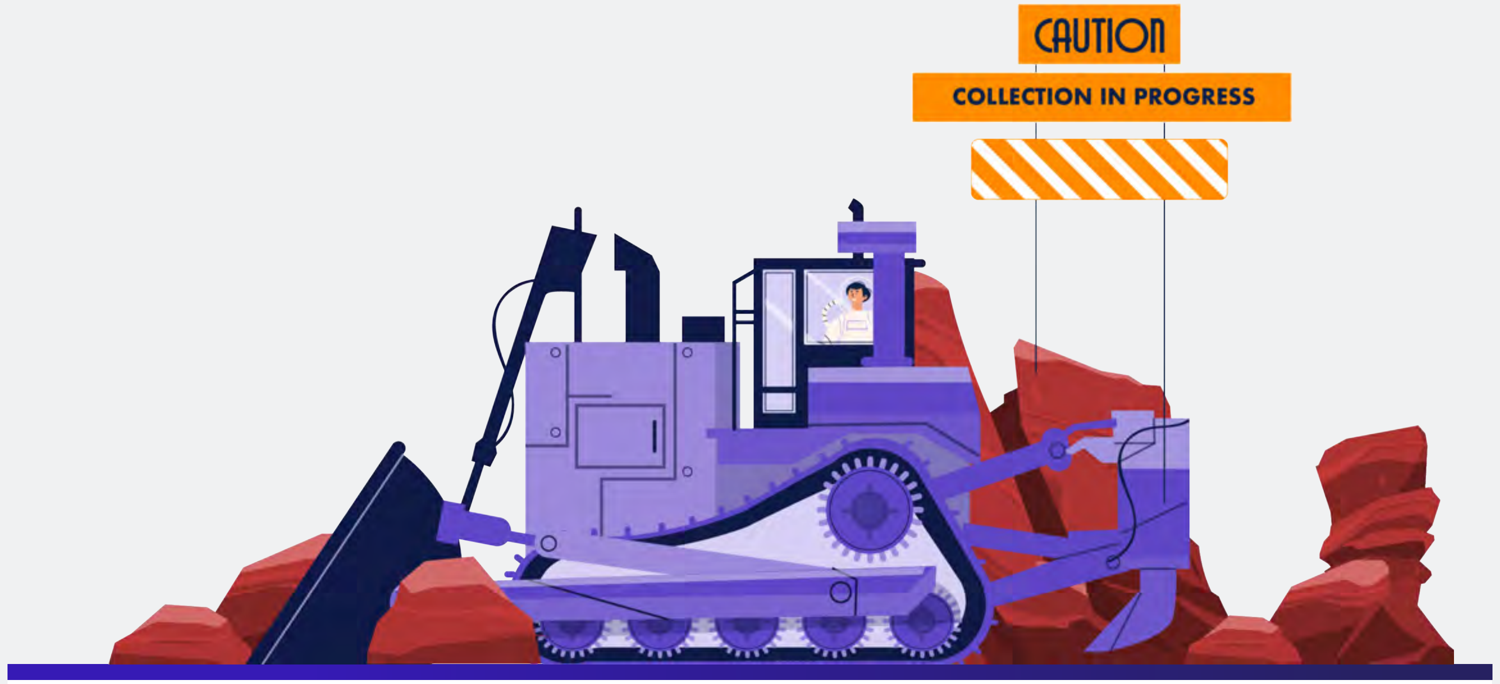
Tackling the evidence collection burden

As with previous years, evidence collection continued to be where teams spent a significant amount of time. Last year, 52% of respondents stated that they collected evidence in response to internal and external audits, and that number remains relatively consistent in 2024. However, the number of those who collect evidence continually increased by 58% year-over-year, demonstrating that continuous evidence collection is becoming more of a standard for GRC professionals.

Diving deeper, we wanted to see if evidence collection habits lead to differing results between these segments. Earlier in this chapter, we found that **those who integrate risk and compliance activities manage controls more effectively than the other two cohorts.** We found that these organizations, compared to the other two groups, are more diligent in collecting evidence needed to verify that controls are operating effectively. In fact, **they're far more likely than other organizations to collect evidence on an ongoing basis as part of a continuous compliance program.**

Choose the statement that most accurately reflects how your organization approaches evidence collection:





Choose the statement that most accurately reflects how your organization approaches evidence collection:

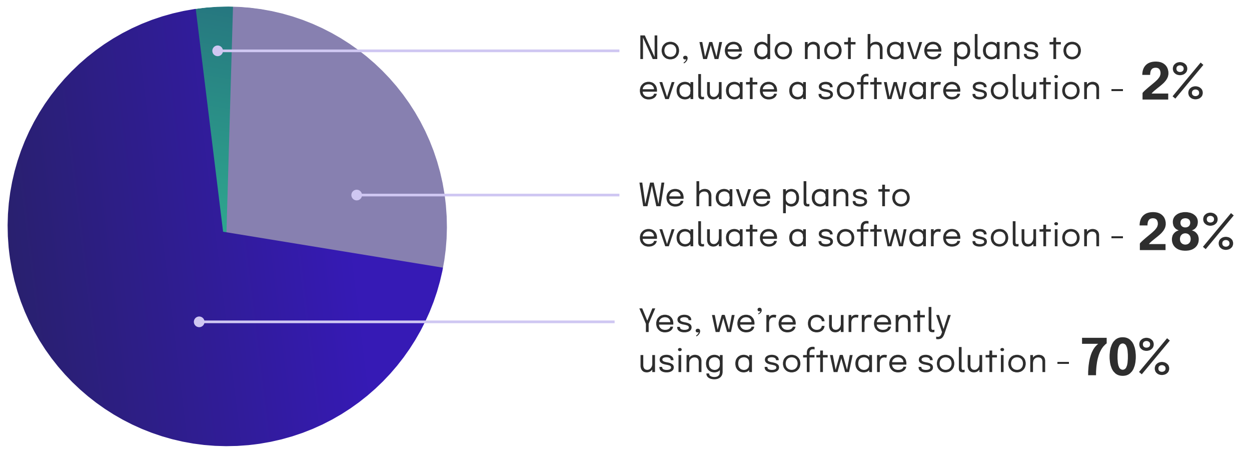
How respondents view the purpose of the compliance function:

	Function that enforces regulations or industry standards	Helps us mitigate risks but risk and compliance activities are conducted separately	Our risk and compliance activities are tied together and aligned
We collect evidence only for external audits	33%	11%	3%
For internal or external audits; conducting internal audits regularly	44%	57%	25%
On an ad-hoc basis	5%	8%	19%
On an ongoing basis, as part of a continuous compliance program	18%	24%	53%

IT compliance technology and tools

The GRC industry's growing reliance on integrated tools and technologies is notable this year. As discussed earlier in this chapter, 83% of respondents have a centralized GRC program, indicating a significant rise from 68% in the preceding year. This upward trend emphasizes the increasing popularity of GRC solutions in organizations, highlighting a concerted effort to streamline processes across business units and geographies.

Are you using or have you evaluated software that can help you automatically monitor and test your organization's security controls, assets, and compliance status?

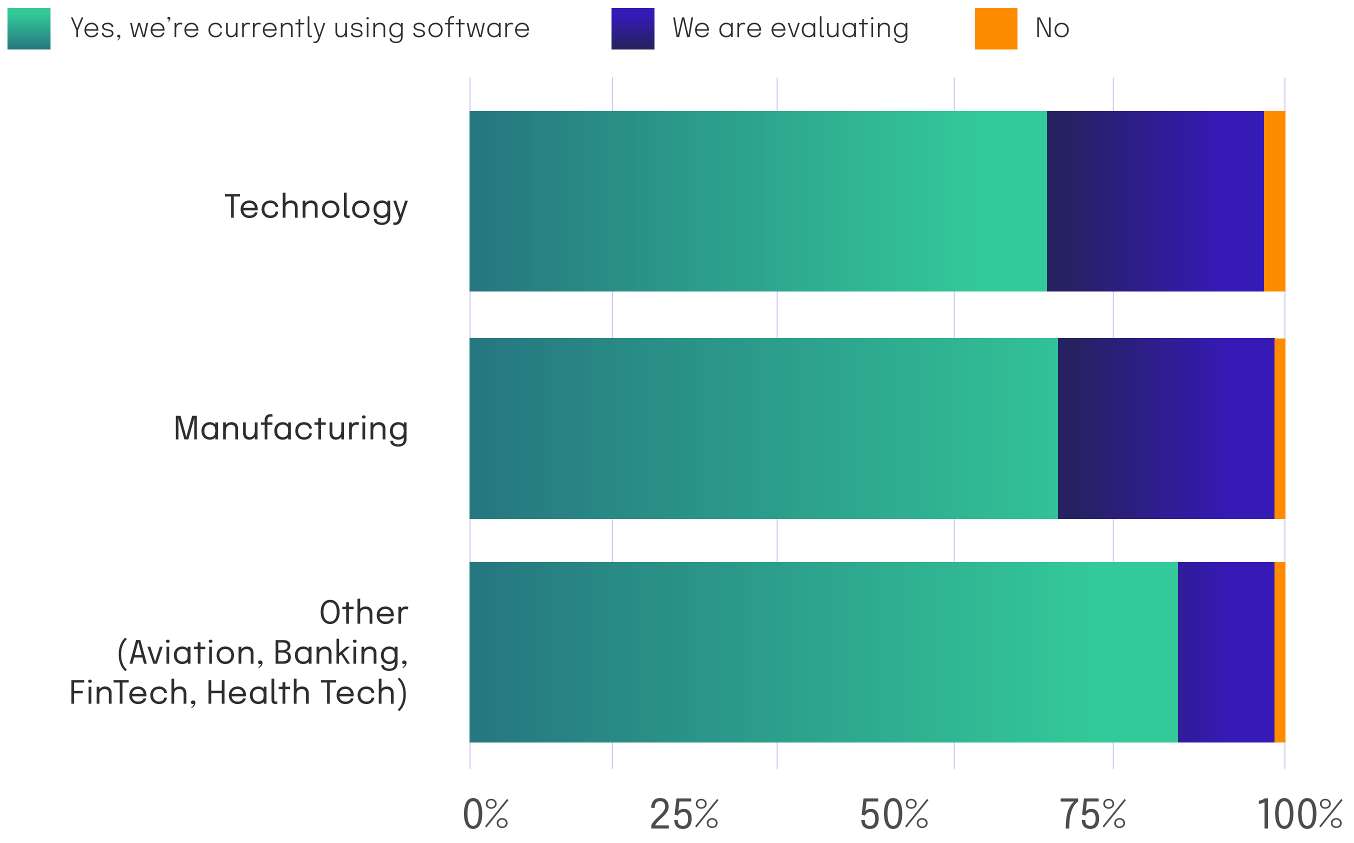


A substantial 70% of respondents currently employ software to monitor security controls and report on compliance postures, underlining respondents' proactive approach to managing compliance. Additionally, 28% have plans to evaluate similar software in 2024, signifying a continued focus on adopting technology tools to enhance visibility into compliance postures. The data paints a picture of a shifting industry landscape, as organizations increasingly turn to technology-driven solutions to save time on administrative tasks, provide transparency and visibility into their risk postures, and make room for strategy.

Segment differences by industry

Of the industries surveyed, the aviation, banking, FinTech, and health tech industries most frequently reported using a software tool to monitor security controls and report on their compliance postures. These industries are subject to highly regulated environments with stringent compliance requirements. Regulatory bodies impose specific standards and guidelines related to data security, privacy, and industry-specific practices. Using specialized software tools helps these industries automate the monitoring of security controls to ensure continuous compliance with regulatory mandates.

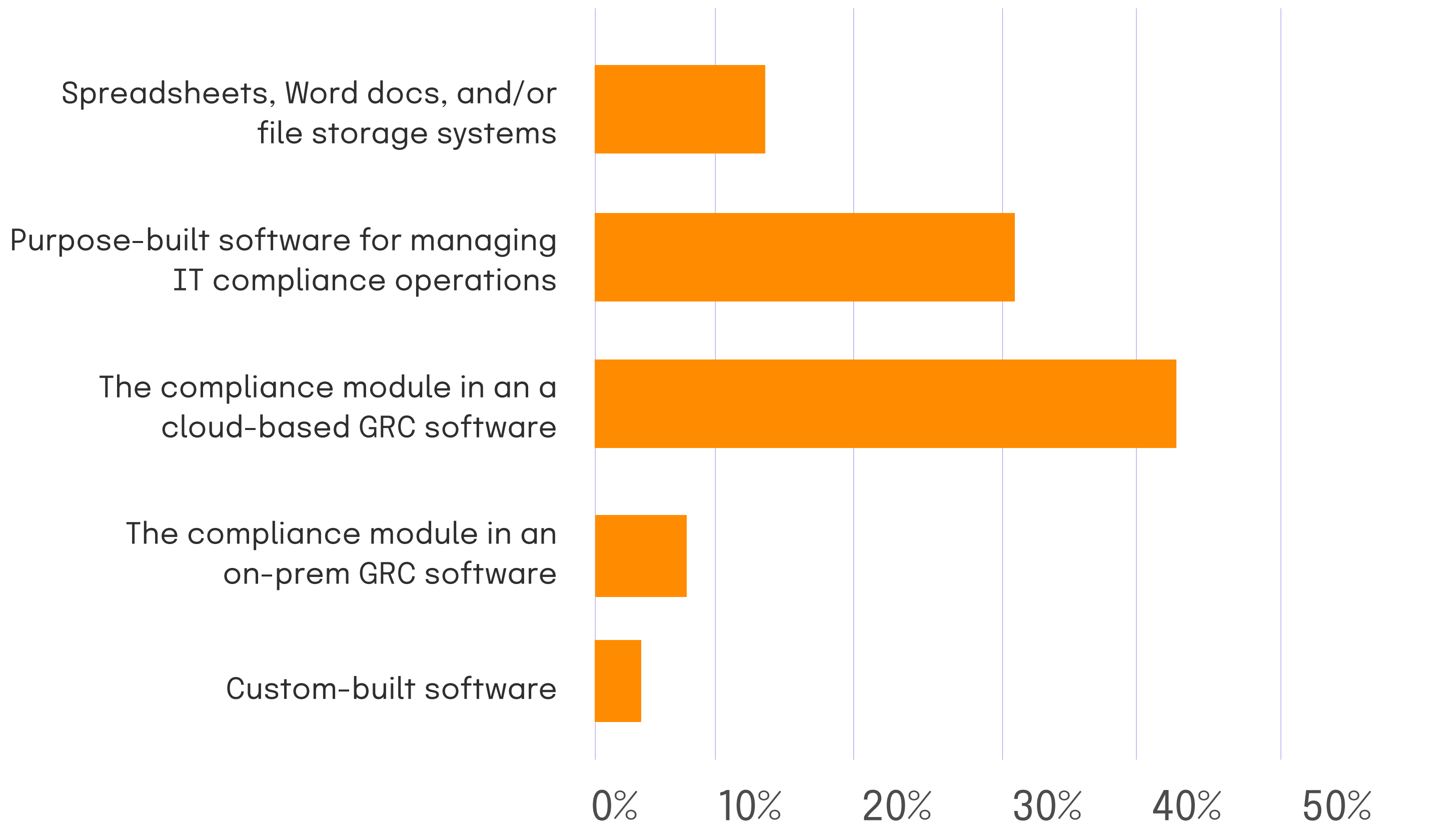
Are you using, or have you evaluated, software that can automatically monitor and test your organization's security controls, assets, and compliance status?



Using technology to streamline manual processes

More respondents are using GRC software for automation purposes, like evidence collection, issue tracking, remediation, control monitoring, and risk and compliance reporting. This percentage increased from 58% to an impressive 69% year-over-year, highlighting a growing reliance on automation to streamline complex compliance-related tasks. These changes reflect a broader industry recognition of the efficiency and effectiveness of software tools in addressing the challenges posed by compliance requirements.

What tools are you using to manage your IT compliance effort?



The largest portion of respondents use a cloud-based GRC tool at 42%, while purpose-built software for IT compliance operations sees an increase year-over-year, rising from 21% last year to 31% in 2024, emerging as the second most commonly employed tool.

KEY STAT

42%

use a cloud-based GRC tool

The diminishing preference for on-premises GRC software – which **decreased from 15% to 8% year-over-year** – continues to demonstrate the steady march to the cloud. Meanwhile, the usage of spreadsheets, Word documents, and file storage systems experienced a slight increase from 10% to 14%, and custom-built software usage decreased from 7% to 4% year-over-year. One explanation for the increase in spreadsheet usage is that over the last year, many GRC teams suffered budget cuts and were forced to revert back to these solutions.

These shifts in tool preferences highlight evolving strategies in IT compliance management, with organizations increasingly turning to purpose-built software and reevaluating their reliance on specific solutions.

Manual processes while switching between tools

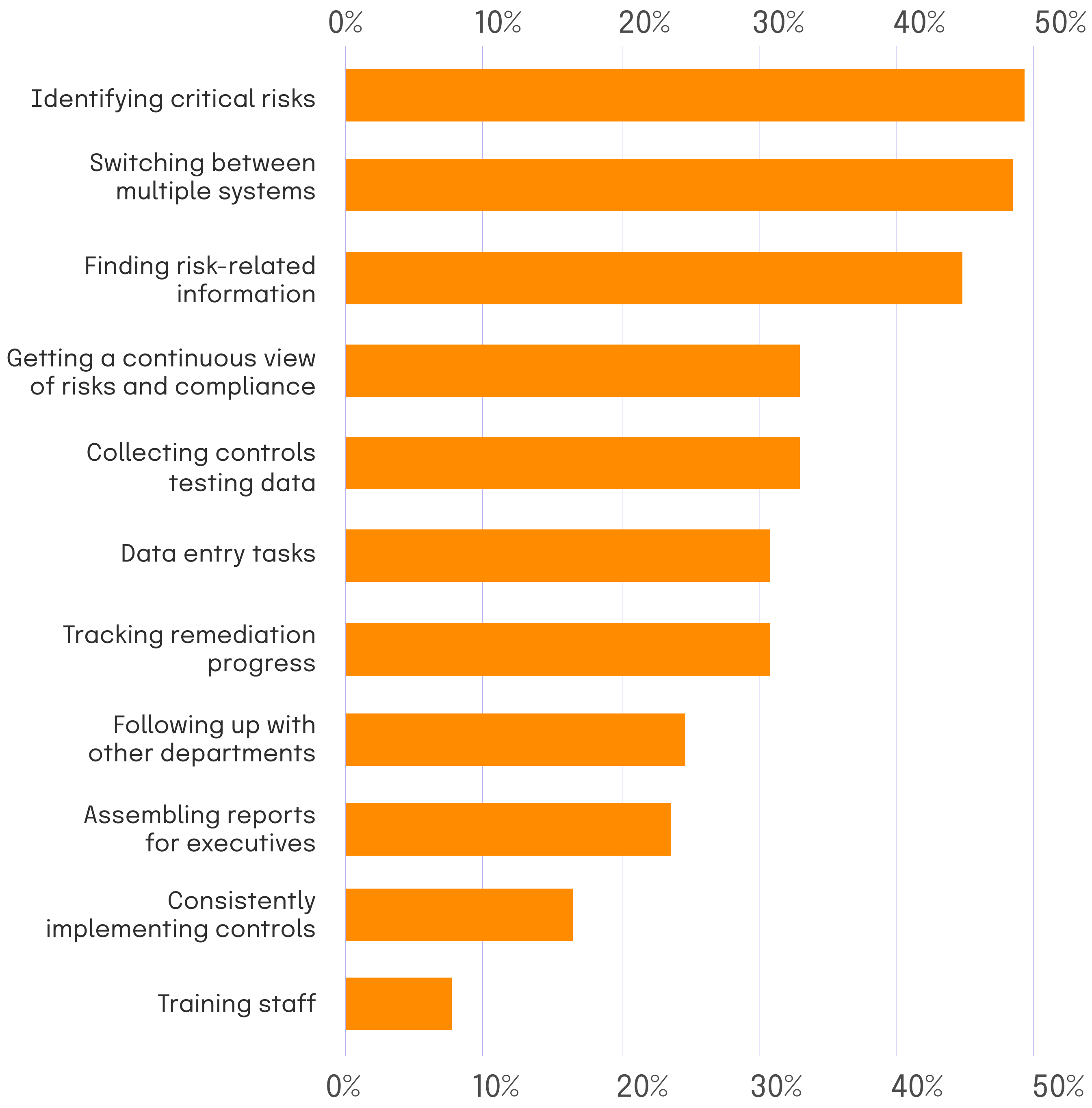
While the predominant challenge for respondents remains the identification of critical risks for prioritizing remediations, we observed a noteworthy shift in the struggle to manage these challenges efficiently. The most significant change unfolds in **a 26% increase in the difficulty of switching between multiple systems for risk management at 48% this year.** Moving between discrepant platforms was the second-most painful task respondents struggled with, signaling a progressive industry inclination toward centralizing risk and compliance management data and solutions. The persistence of this struggle also indicates that many organizations are still navigating the complex landscape of multiple technology tools, underscoring the need for a more consolidated and integrated approach.

KEY STAT

48%

struggle with switching between risk management systems

What time-consuming tasks do you struggle with when managing security and data privacy risks in your internal environment?



Compliance professionals continue to grapple with time-consuming processes, especially when preparing for audits. Locating documentation and other information needed for the audit and identifying where critical risks are came in as the top most tedious tasks, illuminating that there is still work to be done to relieve the burden of these manual processes.

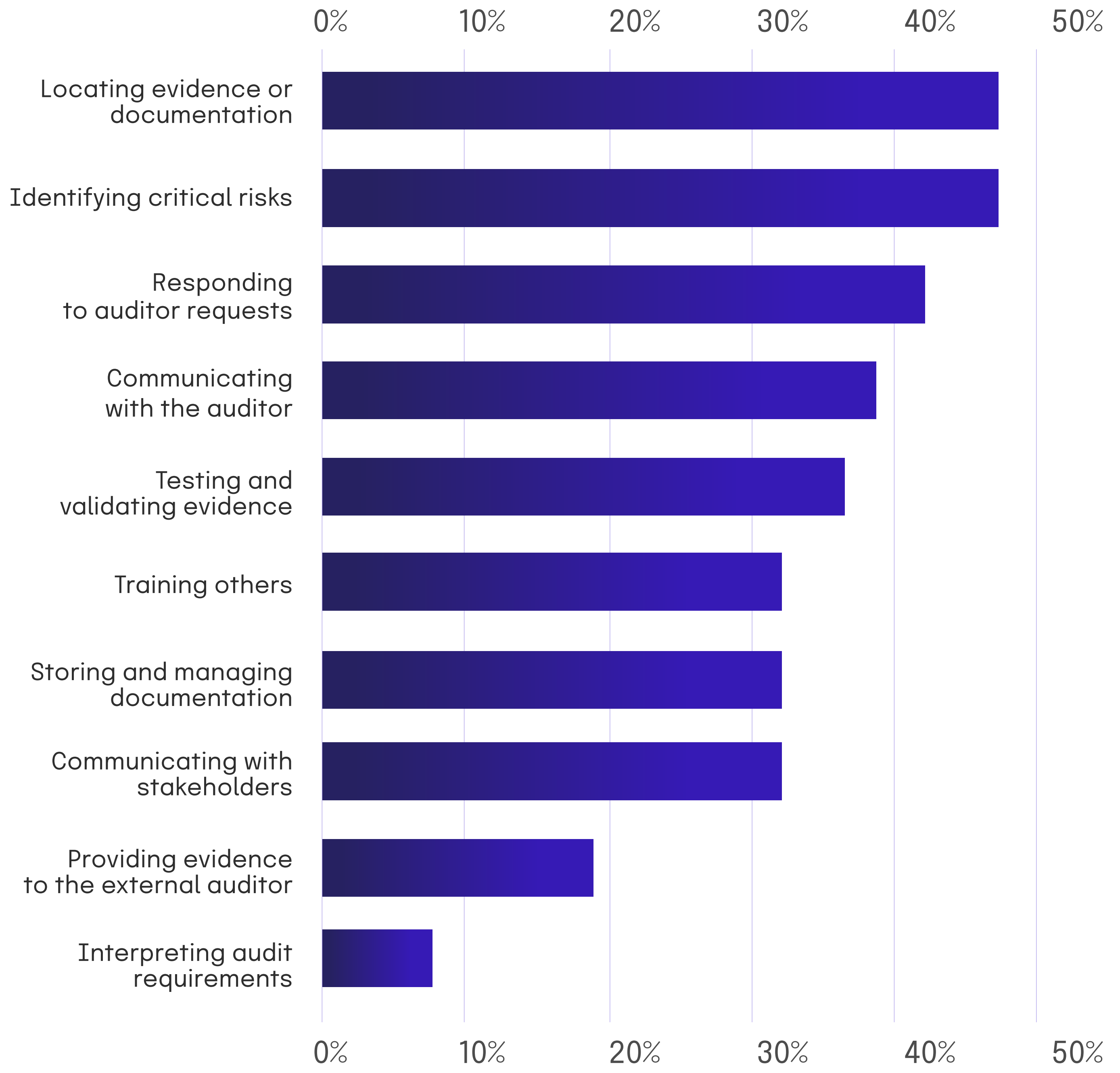
KEY STAT

52%

express confidence that AI will play a pivotal role in enhancing manual tasks

The quest for efficiency in GRC operations is further illuminated by the optimism of 65% of respondents who see AI as having the most potential to optimize their manual risk and compliance workflows. Additionally, 52% express confidence that AI will play a pivotal role in enhancing the completion of manual tasks. We will explore these statistics more in chapter two, where we dive into the transformative impact of AI in the GRC space. We will examine how organizations are leveraging this technology to overcome existing challenges, what concerns they have around emerging AI risks, and their thoughts on using AI responsibly.

What tasks do you find to be tedious or take longer than you'd like when preparing for audits?



CHAPTER 2

The Artificial Intelligence Paradox: **AI's Dual Role in GRC**

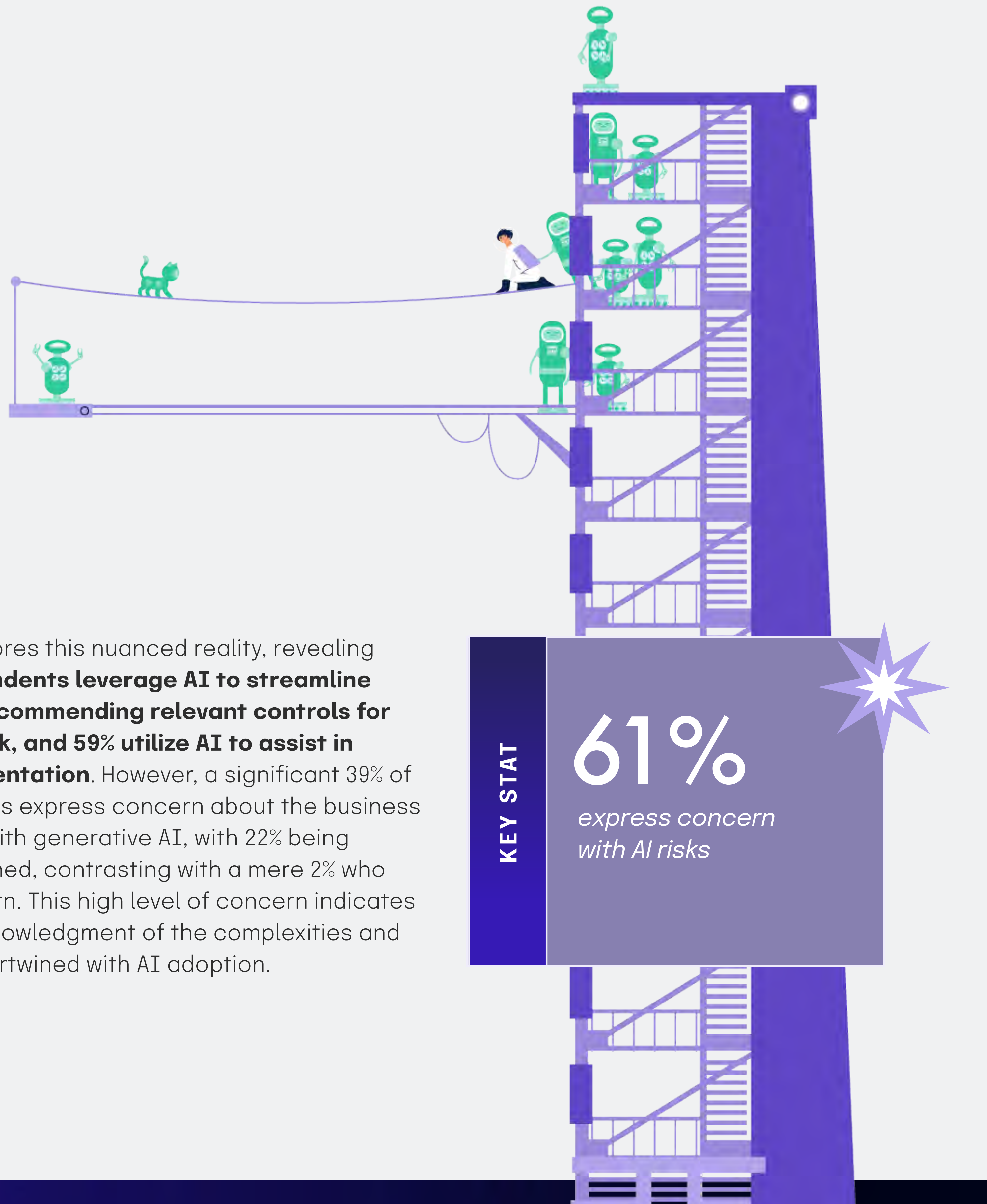
CHAPTER 2

The Artificial Intelligence Paradox: **AI's Dual Role in GRC**

> AI technologies are both enabling more sophisticated cyber attacks and helping defend against them.

It's no surprise that AI in cybersecurity presents a complex duality: AI simultaneously introduces new business risks while streamlining workflows for GRC professionals and helping stay abreast of innovative new cyberattacks, like deepfakes, more advanced phishing emails, better password guessing, neutralizing off-the-shelf security tools, and much more. Regulators around the world spent much of 2023 trying to understand how they should respond to the myriad cybersecurity, privacy, economic, and ethical risks that AI raises and began to take action near the end of the year. An expanding presence of global regulatory bodies demand that organizations backing AI assertions demonstrate transparency and furnish proof of their AI capabilities.

Walking the tightrope of using AI in cybersecurity is a difficult task that requires nuance. Organizations need to stay ahead of the latest advancements in AI to make informed decisions and leverage its transformative capabilities while keeping AI misuse top-of-mind. It all comes down to adopting AI technologies responsibly and judiciously, which requires continuous awareness, education, and a commitment to ongoing research.



The data underscores this nuanced reality, revealing that **61% of respondents leverage AI to streamline the process of recommending relevant controls for a given framework, and 59% utilize AI to assist in reviewing documentation**. However, a significant 39% of survey respondents express concern about the business risks associated with generative AI, with 22% being extremely concerned, contrasting with a mere 2% who express no concern. This high level of concern indicates the industry's acknowledgment of the complexities and potential risks intertwined with AI adoption.

KEY STAT

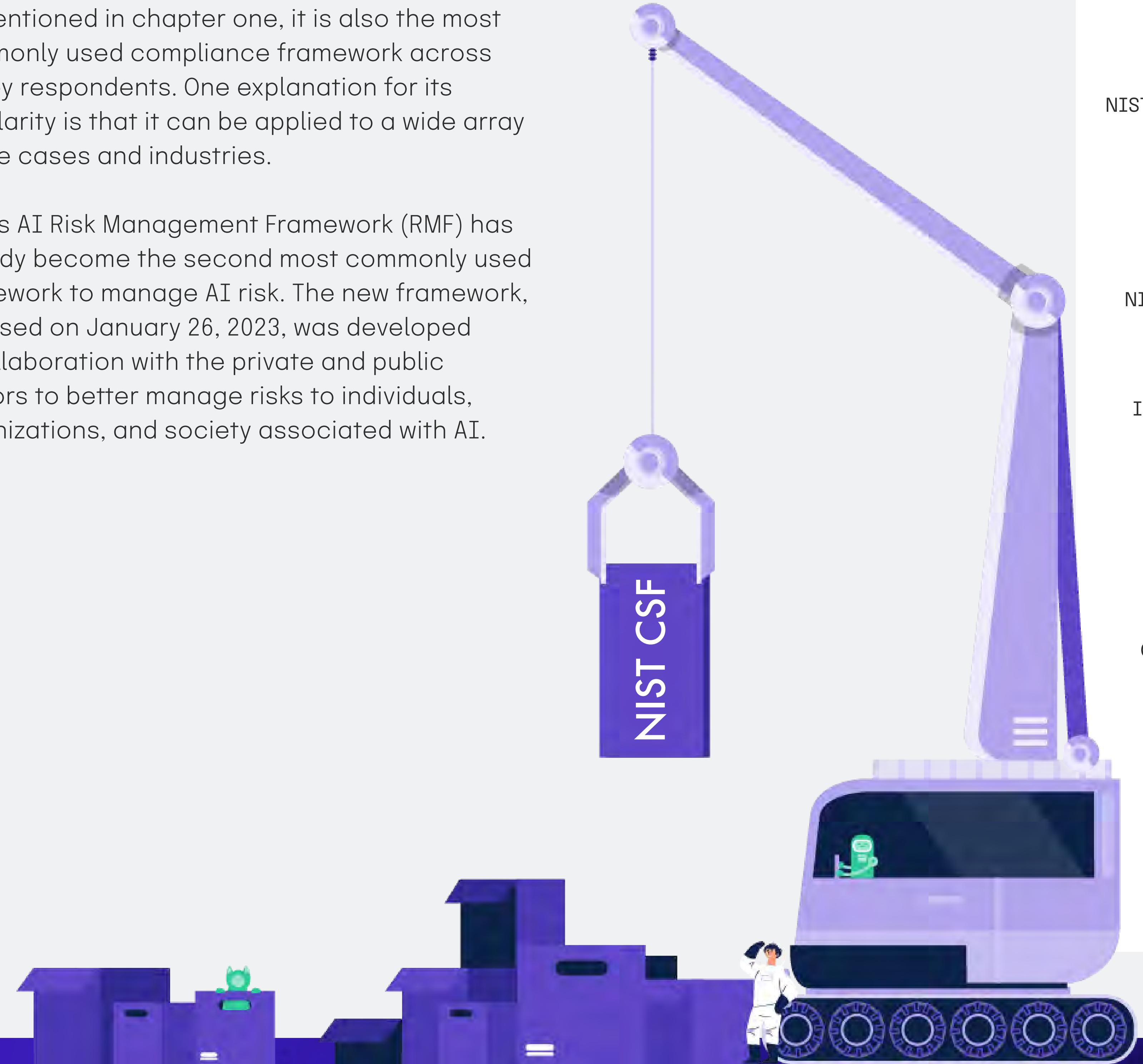
61%

express concern with AI risks

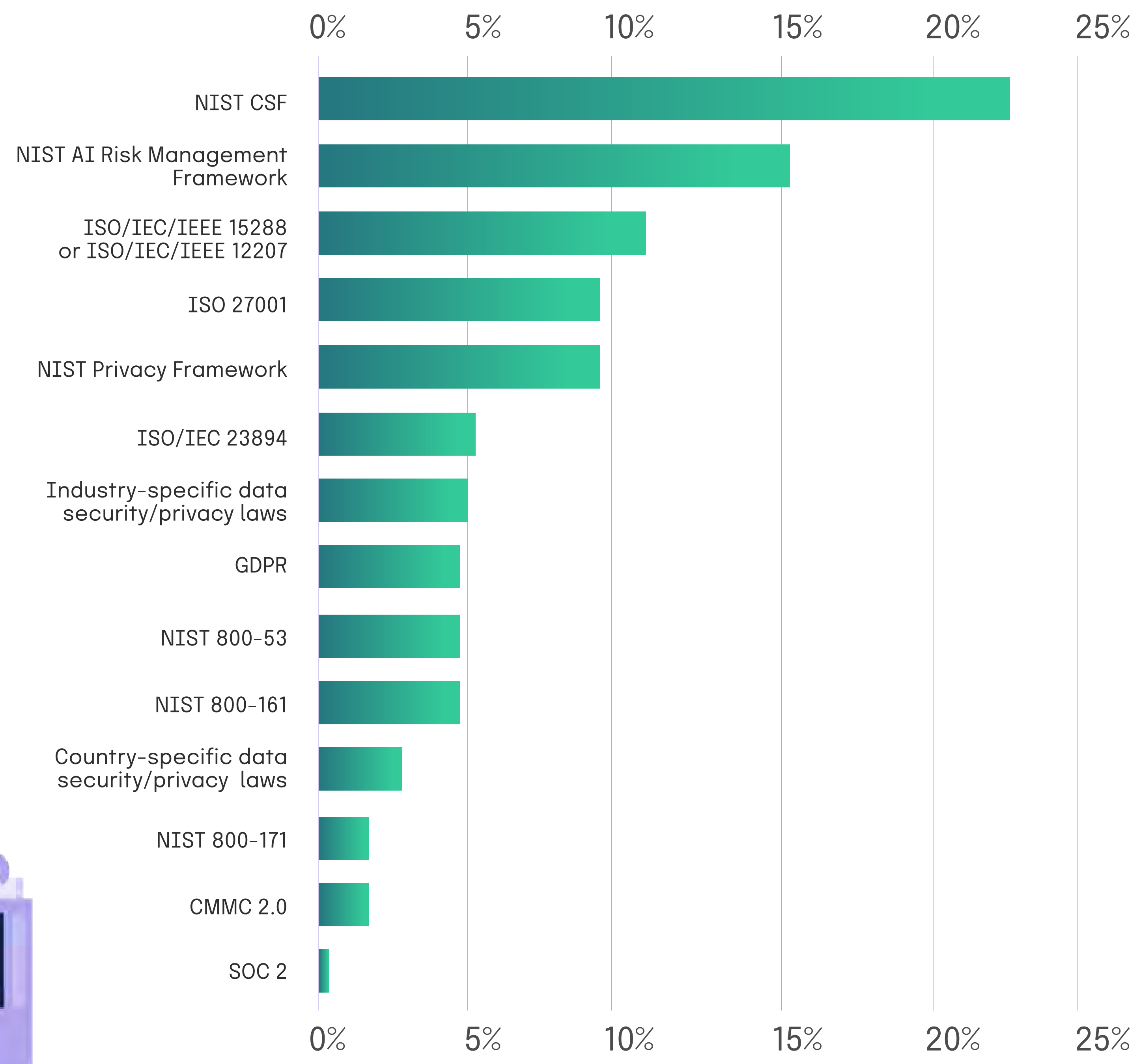
Frameworks used to manage AI risk

Unsurprisingly, NIST CSF is the most commonly used compliance framework to manage AI risk. As mentioned in chapter one, it is also the most commonly used compliance framework across survey respondents. One explanation for its popularity is that it can be applied to a wide array of use cases and industries.

NIST's AI Risk Management Framework (RMF) has already become the second most commonly used framework to manage AI risk. The new framework, released on January 26, 2023, was developed in collaboration with the private and public sectors to better manage risks to individuals, organizations, and society associated with AI.



Which of the following frameworks are you using to manage risk presented from generative AI?



Concern for AI risk

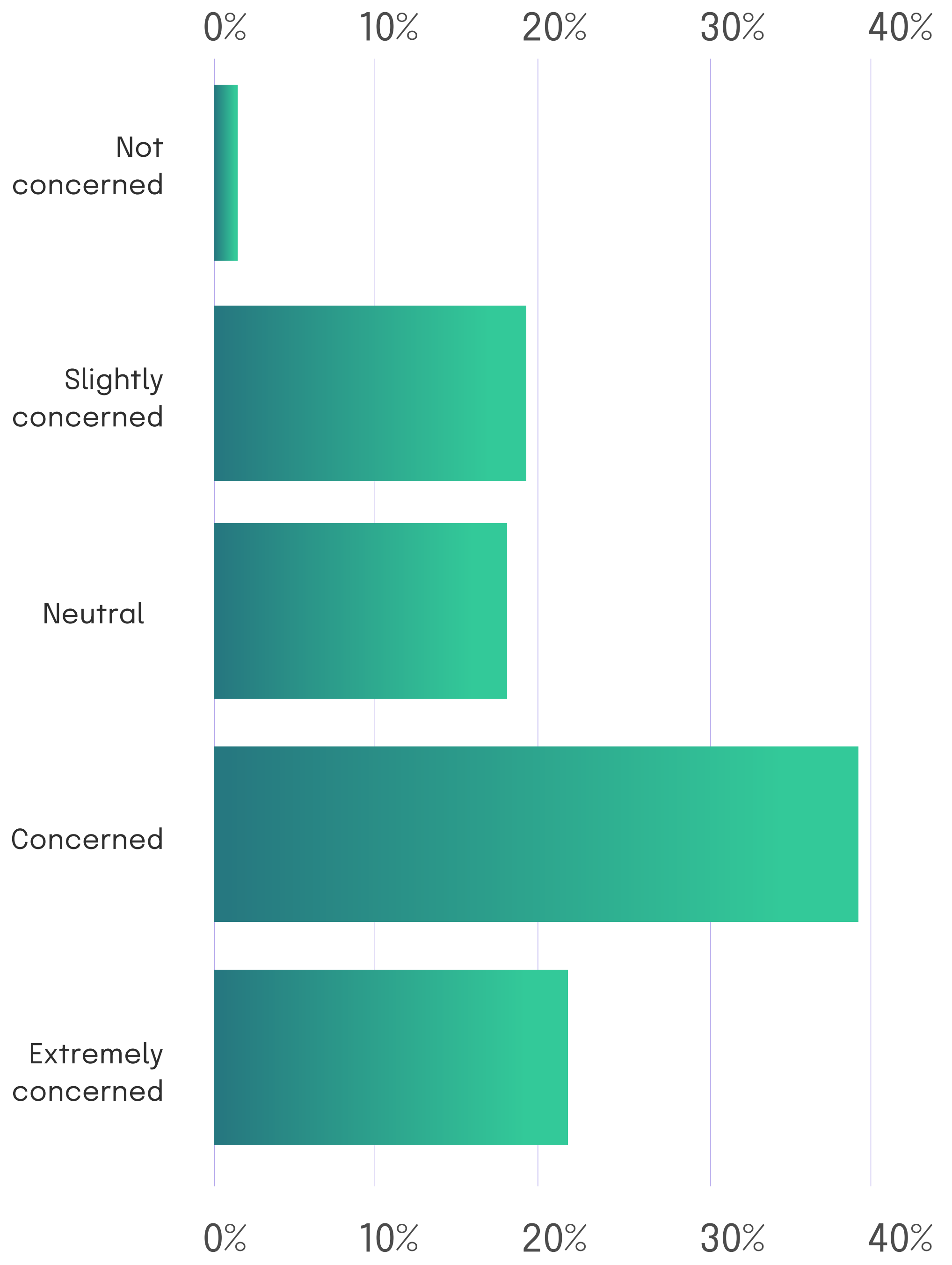
Concern for AI risk is high, with over half of respondents either concerned or extremely concerned about the business risks associated with generative AI.

This new and emerging technology presents a myriad of business challenges, from regulatory compliance violations to new security vulnerabilities.

> The rapid advancement of generative AI technology has outpaced many regulatory frameworks, and GRC professionals are grappling with how to ensure that AI applications comply with existing and emerging regulations.

This includes data protection laws, industry-specific regulations, and ethical guidelines that may govern the use of AI in various sectors. Data security and privacy concerns have emerged as well, since generative AI often relies on vast datasets to produce realistic outputs. These concerns vary and are distinct for companies that make AI products compared to organizations that are leveraging AI like a SaaS service. In both scenarios, GRC professionals must address data security and privacy concerns associated with the collection, storage, and use of sensitive data. Many generative AI models operate as black boxes, making it difficult to explain how they arrive at specific outputs. With little visibility into this data black hole, GRC professionals are concerned about their hindered ability to assess and manage the risks associated with AI-generated content.

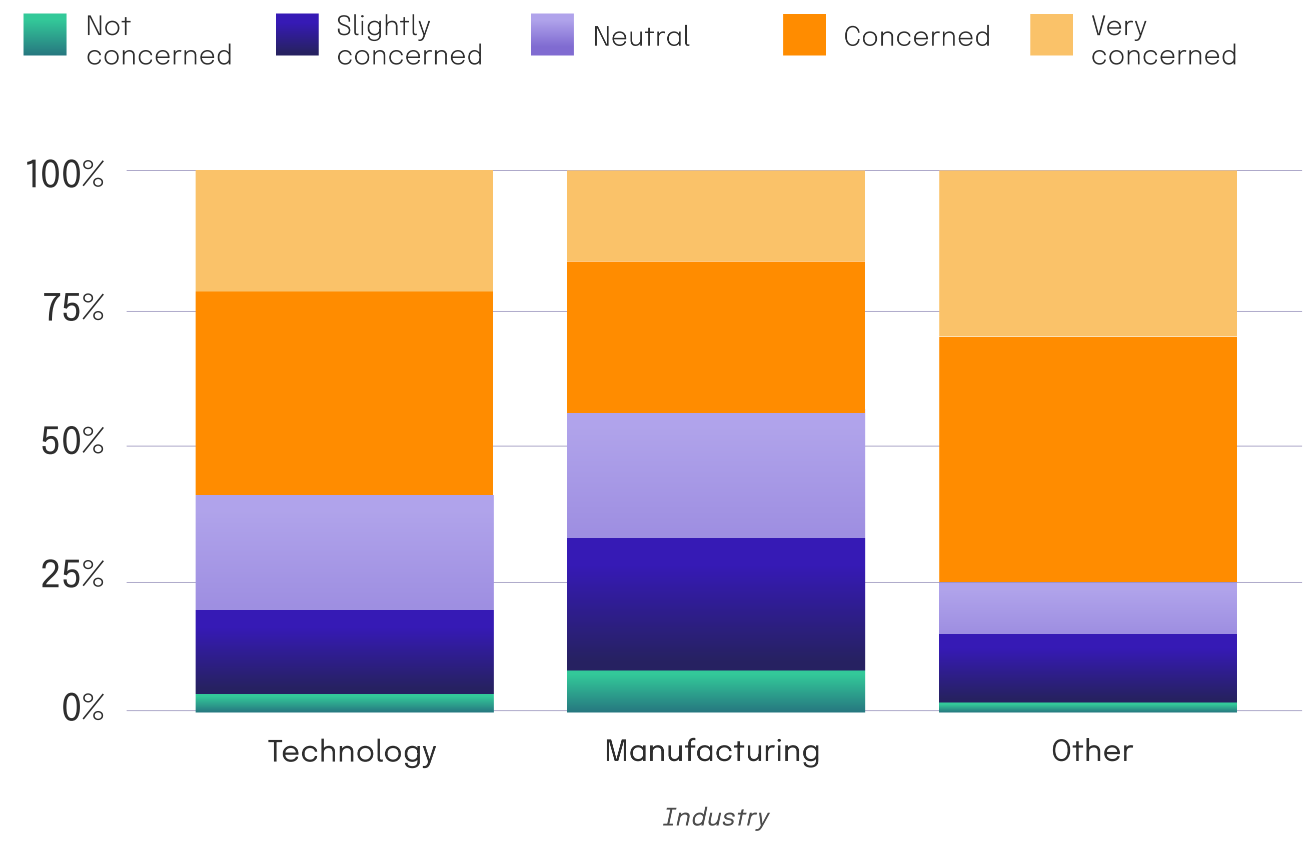
Coming into 2024, how concerned are you about the business risks associated with generative AI?



Segment differences by industry

Overall, the aviation, banking, FinTech, and health tech industries were more concerned with AI risk, with 44% reporting being "concerned" and 31% reporting being "very concerned." These industries may exhibit heightened concerns about AI risks due to industry-specific factors and regulatory environments that necessitate a more cautious approach to adopting AI. They are highly regulated, with stringent compliance requirements imposed by aviation authorities, financial regulators, and health organizations. Compliance with industry-specific regulations, as well as emerging AI regulations, is a priority. The complex regulatory landscape adds an additional layer of scrutiny, making these industries more vigilant about potential risks associated with AI.

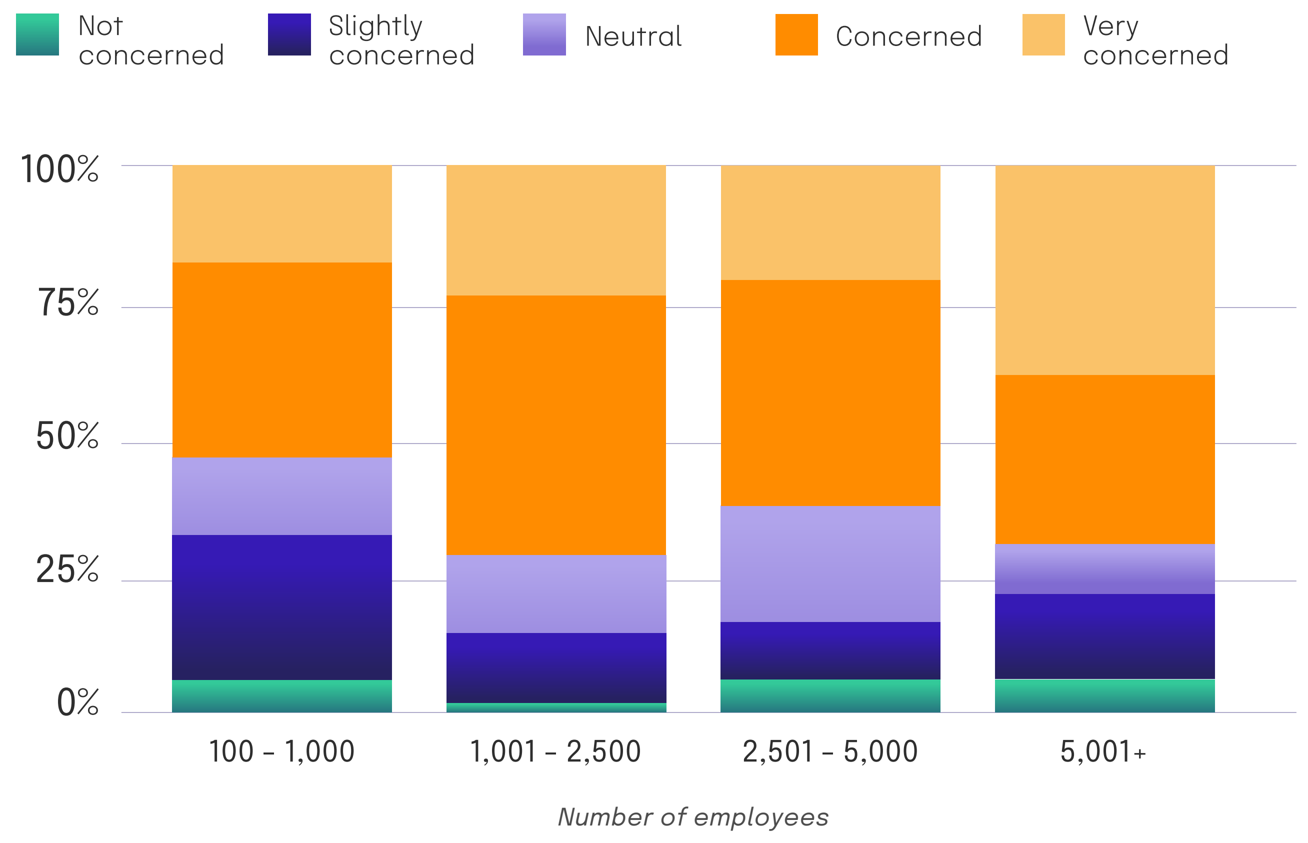
Coming into 2024, how concerned are you about the business risks associated with AI?



Larger companies are more concerned with AI risk

Larger companies often have more extensive and intricate operations, which involve handling massive amounts of data across multiple departments and functions. The sheer scale amplifies the potential impact of any AI-related issues, making these organizations more cautious and attentive to the associated risks. The complexity of larger organizations' IT ecosystems and business processes makes them more susceptible to the unintended consequences of AI implementation. Integrating AI into intricate systems may introduce unforeseen challenges, creating concerns about how AI interacts with existing technologies and processes.

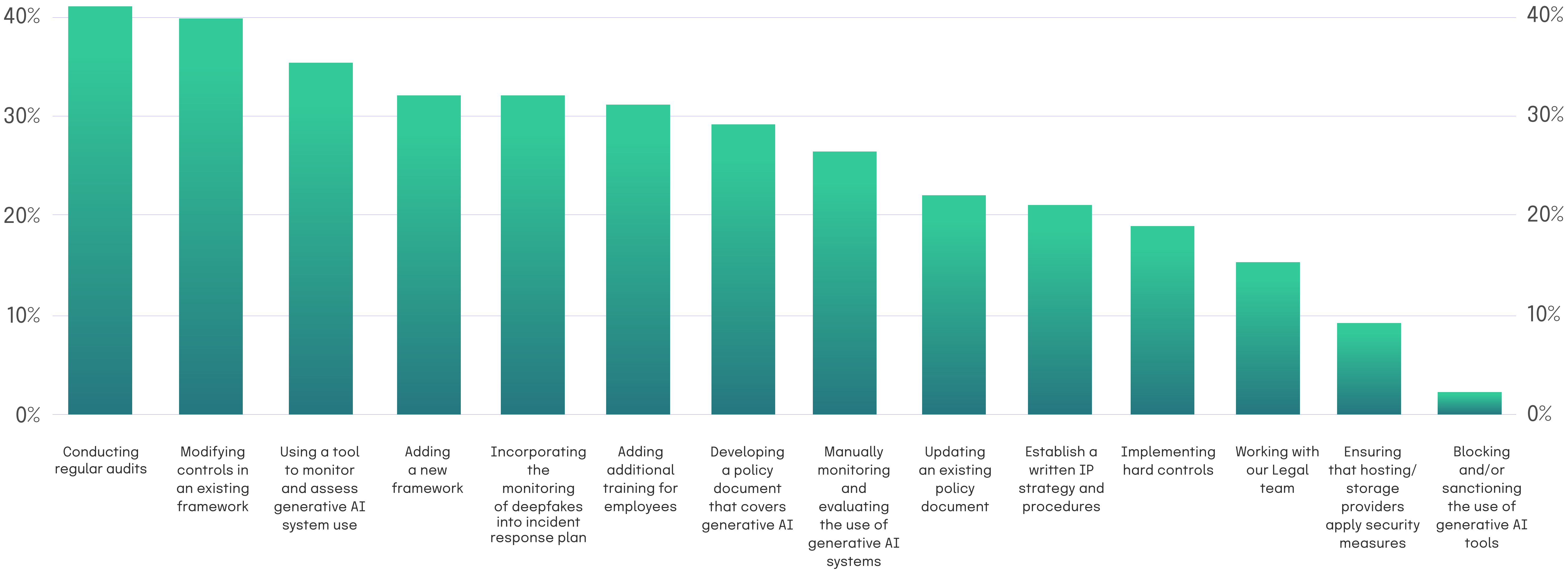
Coming into 2024, how concerned are you about the business risks associated with AI?



How respondents are addressing AI risk

Respondents are actively addressing AI risk by implementing various policies and procedures, the top being conducting regular audits to ensure compliance with generative AI-related policies and controls, closely followed by modifying controls in an existing framework their company is already using. These approaches are the result of companies rapidly adapting to the changes that AI risk introduced in 2023. Rather than start from scratch, the majority of respondents worked with resources they already had: existing controls, policies, and frameworks.

What policies or procedures do you plan on putting in place to mitigate business risk associated with AI and generative AI tools in 2024?



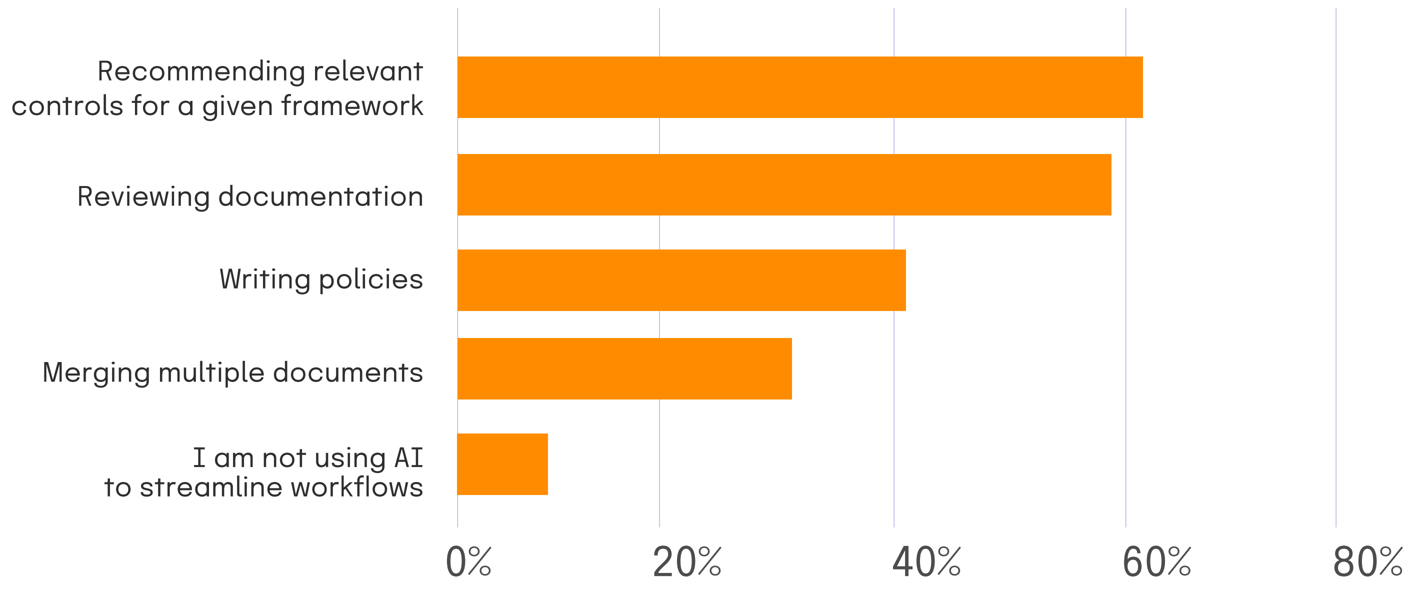
Using AI as a force accelerator

While AI presents a slew of new risks, respondents are also using it as a force accelerator. The integration of AI algorithms and machine learning methods enables GRC professionals to proactively report on the effectiveness of controls against cyber threats like malware, ransomware, and social engineering attacks. An overwhelming **80% of respondents consider AI strategy for their teams' operations as important or very important** in the coming year. Those utilizing mostly automated integrated GRC tools are more likely to prioritize AI strategy, emphasizing the interconnected nature of AI and efficient GRC operations.

Overwhelmingly, respondents are already using AI to streamline their risk and compliance workflows. Recommending relevant controls for a given framework was the most popular use case, followed by reviewing documentation.

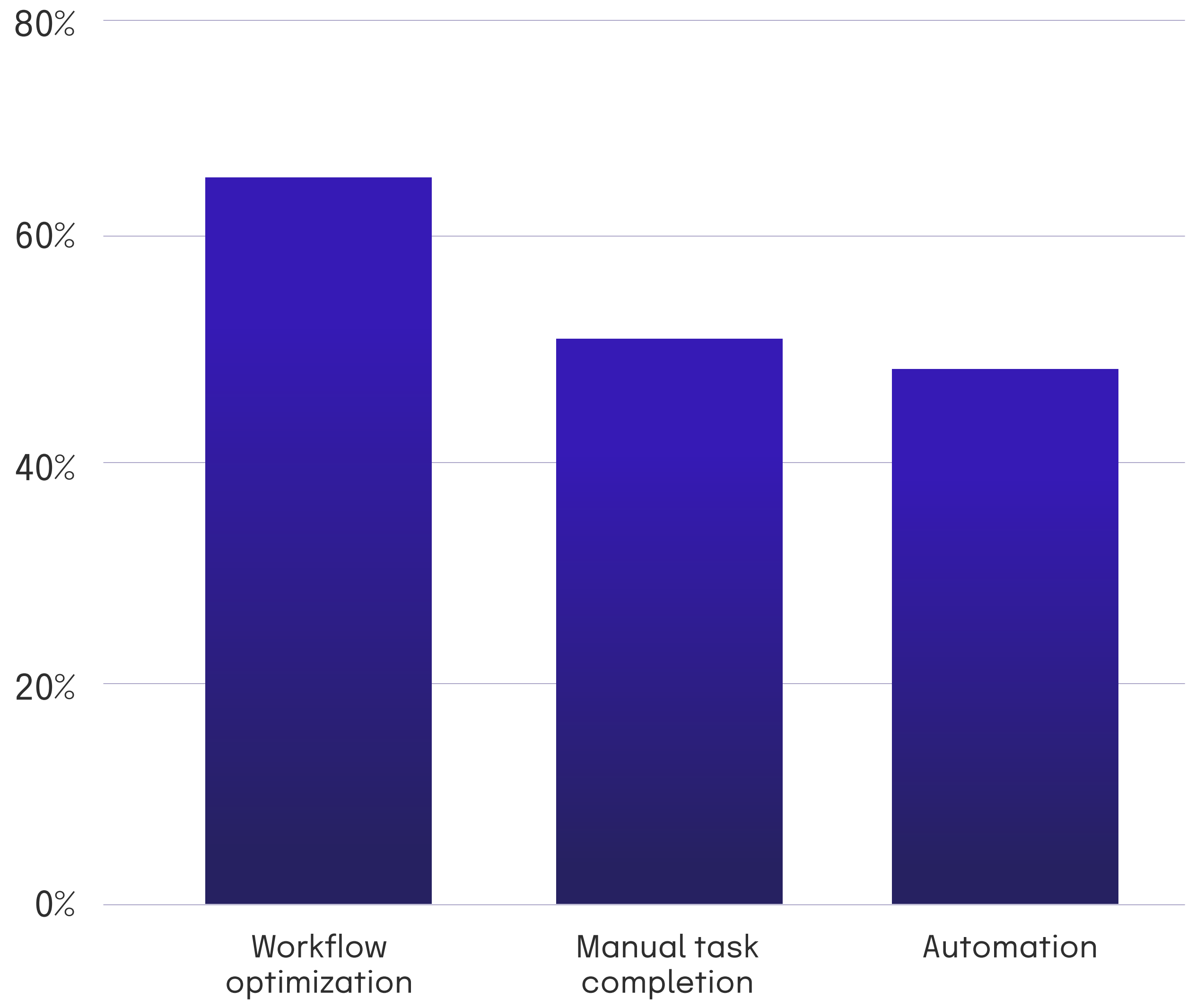
Are you using AI to streamline any workflows?

A: Yes



As we covered in chapter one, manual processes, like evidence collection, remain a burden for GRC professionals. Respondents agree that they see the most potential in optimizing their workflows with AI, especially because they are being asked to do more with fewer resources as the macroeconomic climate shifts.

What areas of AI do you see the most potential when applying to risk and compliance?



Responses to AI risk

Those who experienced breaches were more likely to care about AI risk

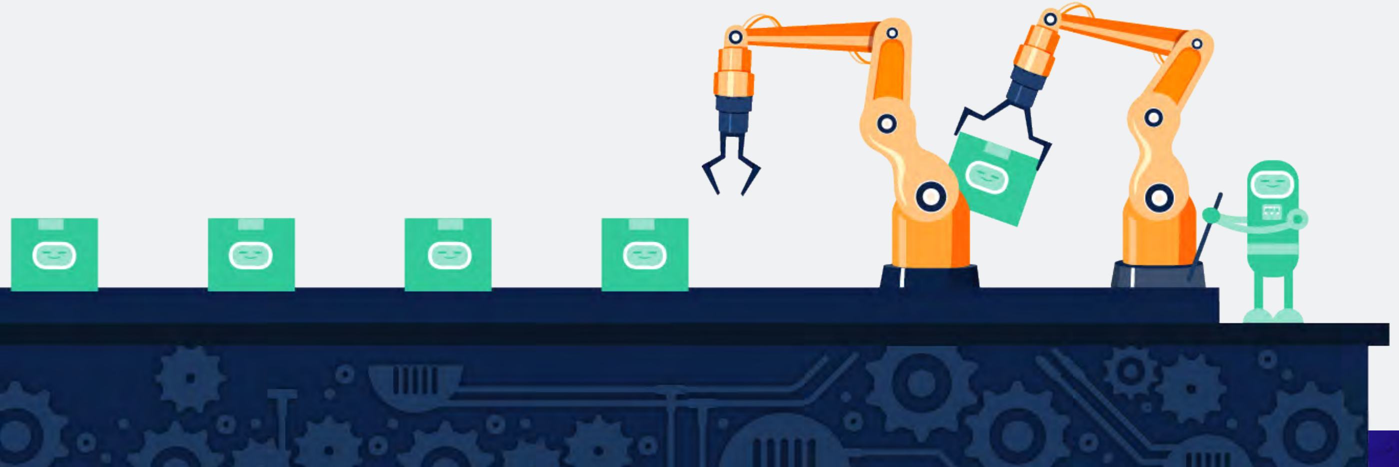
Data breaches from the last year impacted respondents' thinking around AI. Those who experienced supply chain disruptions or data breaches were more likely to incorporate AI strategy into their planning for 2024. 79% of respondents who identified as "extremely concerned" about the risks associated with generative AI experienced a breach in the last 24 months. The incidents likely highlighted the need for improved cybersecurity, supply chain resilience, and proactive risk management, with AI emerging as a strategic tool to address these challenges and enhance overall organizational cybersecurity efforts.

KEY STAT

79%

of respondents who are "extremely concerned" with AI risk experienced a breach in the last 24 months

Data breaches and supply chain disruptions often expose vulnerabilities in an organization's cybersecurity and operational processes. The firsthand experience of these incidents can heighten awareness among respondents, making them more attuned to the potential risks and challenges they face.



The aftermath of data breaches and supply chain disruptions may lead organizations to recognize the potential role AI can play in mitigating and managing risks.

AI can be leveraged for early detection of security threats, predictive analysis, and enhancing supply chain resilience, making it a strategic tool for addressing the identified vulnerabilities.

Organizations planning on integrating AI into cybersecurity practices are hoping to benefit from its advanced threat detection and response capabilities, taking a proactive approach to defending against evolving cyber threats emerging from AI technologies. Data breaches have prompted a strategic shift toward more proactive risk management.

40%

of respondents who experienced a breach incorporated monitoring of deepfake technology into their existing incident response plan

35%

of respondents who experienced a breach developed a policy document that covers generative AI tool usage

21%

of respondents who experienced a breach updated an existing policy document to cover generative AI

Respondents spending more time on GRC in 2024 are the most concerned with AI strategy

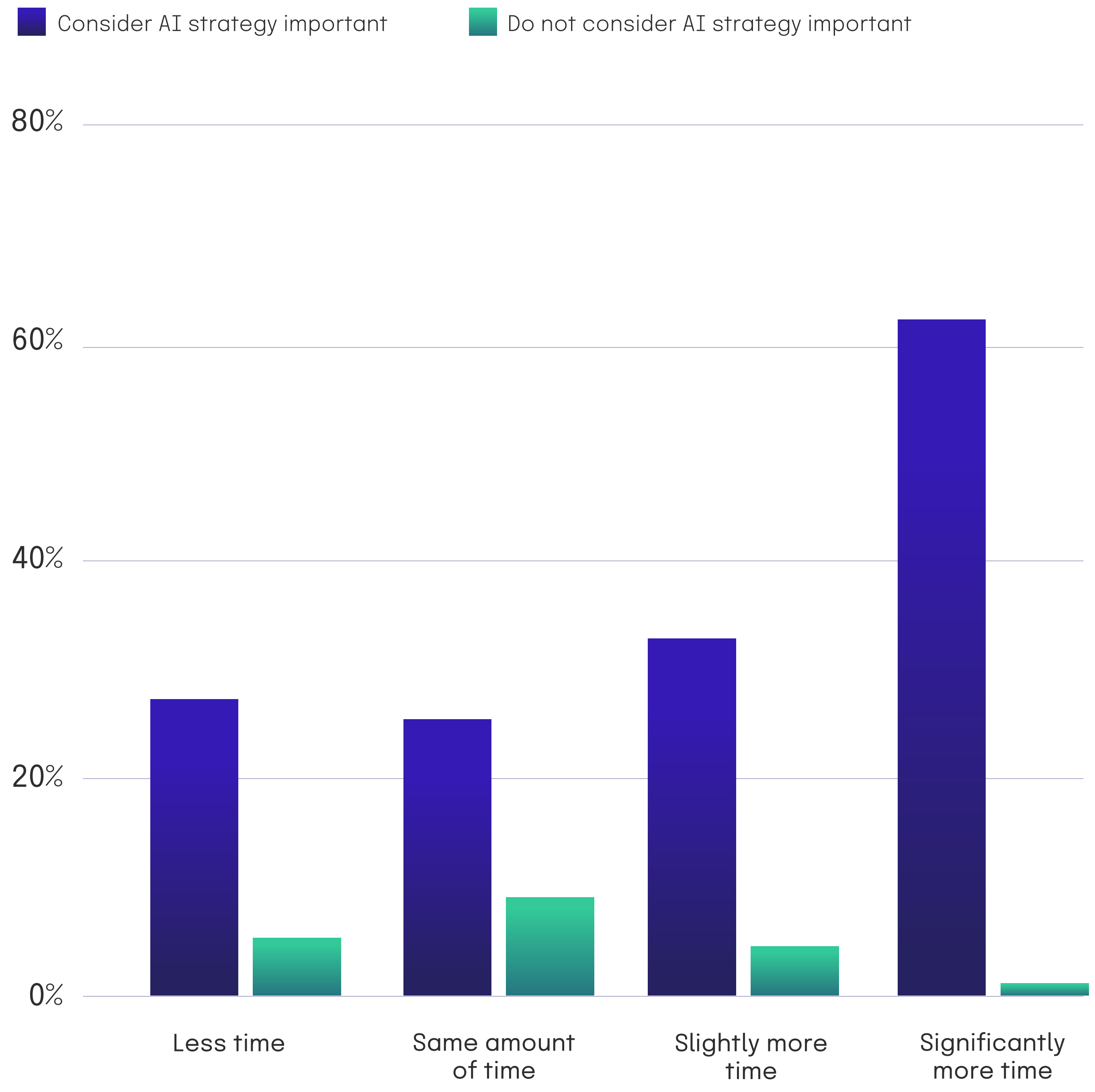
Respondents who anticipated spending significantly more time on governance, risk, and compliance in 2024 were the most focused on defining an AI strategy and considering it as a workflow optimization tool. The push towards AI strategy indicates a desire to align GRC practices more closely with broader business objectives. By optimizing workflows through AI, GRC professionals can contribute to overall organizational efficiency, resilience, and strategic success.

Respondents recognize the growing complexity of governance, risk, and compliance responsibilities and perceive AI as a tool to navigate and streamline intricate GRC processes, particularly in the face of evolving regulatory landscapes and dynamic risk environments. AI can automate routine and time-consuming processes, allowing GRC professionals to focus on more strategic and nuanced aspects of their roles. **Considering AI as a workflow optimization tool aligns with the goal of maximizing efficiency in GRC operations, which is a theme throughout our data.**

Additionally, as regulations become more complex and stringent, GRC professionals may view AI as a tool to ensure compliance through automated monitoring, reporting, and adaptation to changing regulatory requirements.

Respondents perceive AI as a tool to navigate and streamline intricate GRC processes.

How important it is to have an AI strategy for their teams operations vs. **anticipated time spent** on GRC in 2024

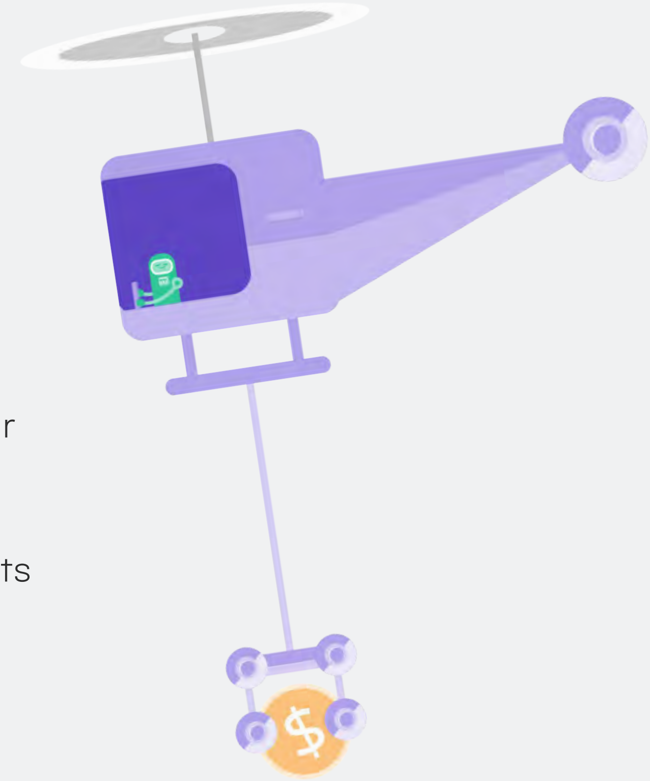


Respondents spending less money on GRC in 2024 are more likely to consider AI strategy important

Respondents anticipating spending less money on governance, risk, and compliance were more likely to consider AI strategy important. Many companies who fall into this cohort are being asked to do more with less and possibly looking toward AI technologies to streamline their processes. Respondents recognize that AI can be leveraged as a strategic tool to achieve GRC objectives without significant financial investments and as a means to maximize the impact of their limited resources.

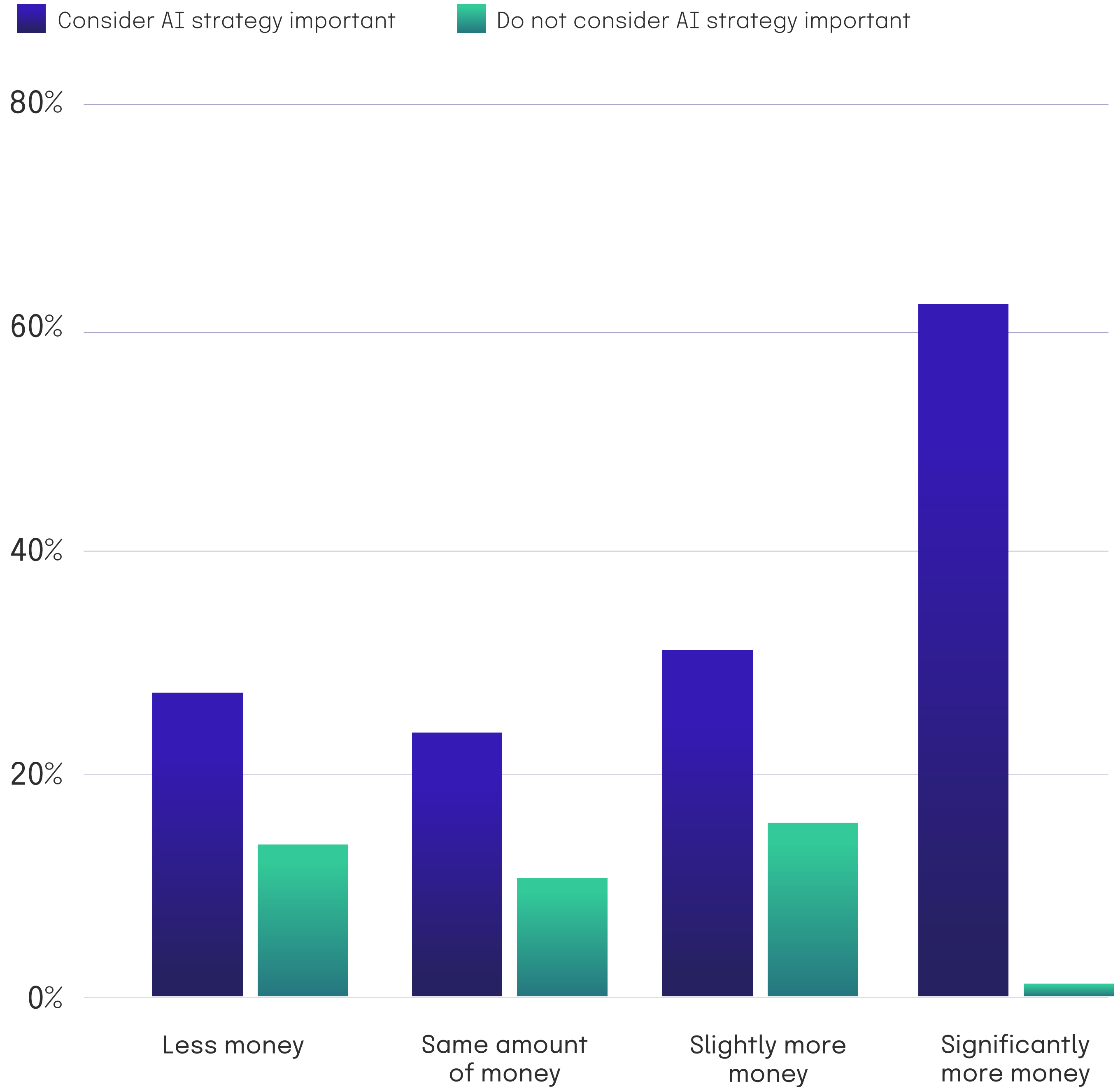
Anticipating spending constraints may lead respondents to prioritize strategic initiatives that deliver high value. AI, with its potential to optimize workflows and enhance risk management, may be seen as a critical strategic investment even in the face of budget limitations.

The importance placed on AI strategy could also be driven by a desire to achieve efficiency gains and process optimization within GRC functions. Respondents may recognize AI's potential to automate routine tasks, analyze data more effectively, and streamline GRC workflows, leading to improved operational efficiency and reduced cost.



> *AI, with its potential to optimize workflows and enhance risk management, may be seen as a critical strategic investment even in the face of budget limitations.*

How important it is to have an AI strategy for their teams operations vs. **anticipated money spent** on GRC in 2024

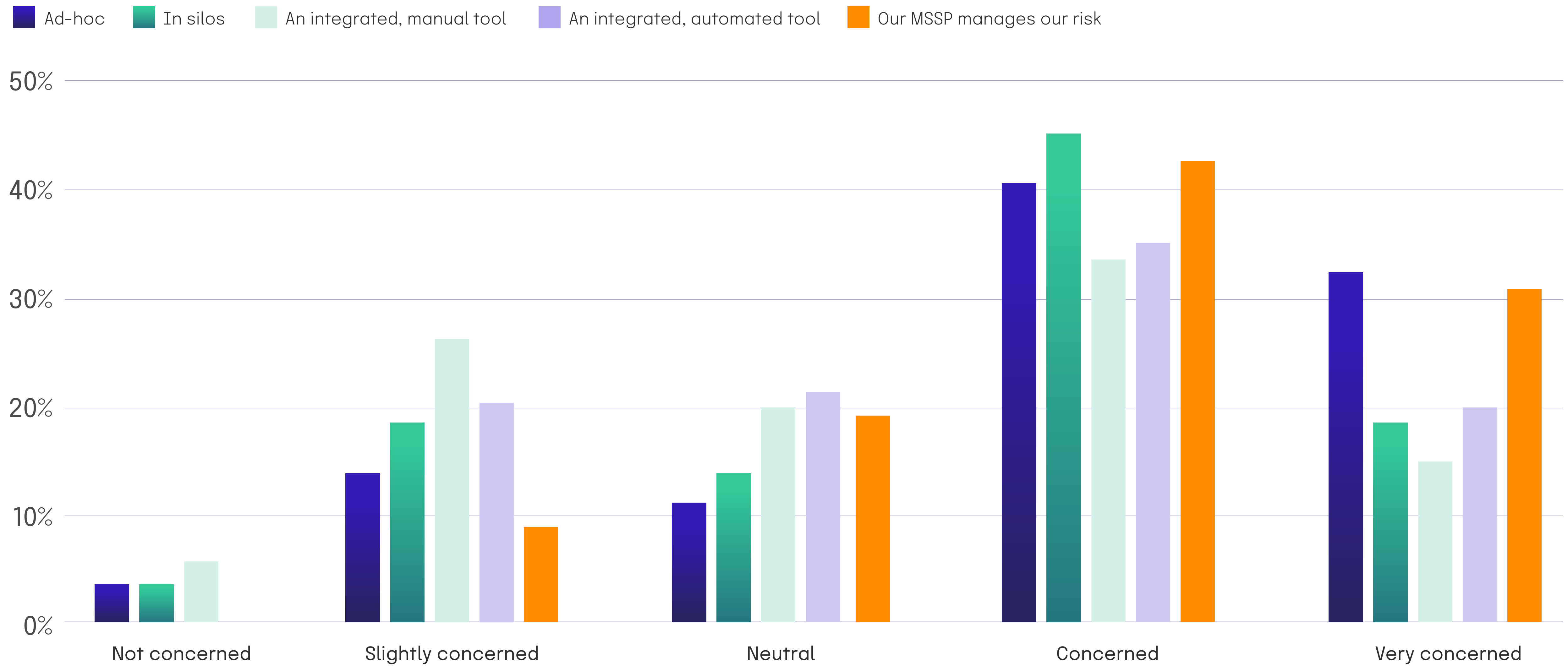


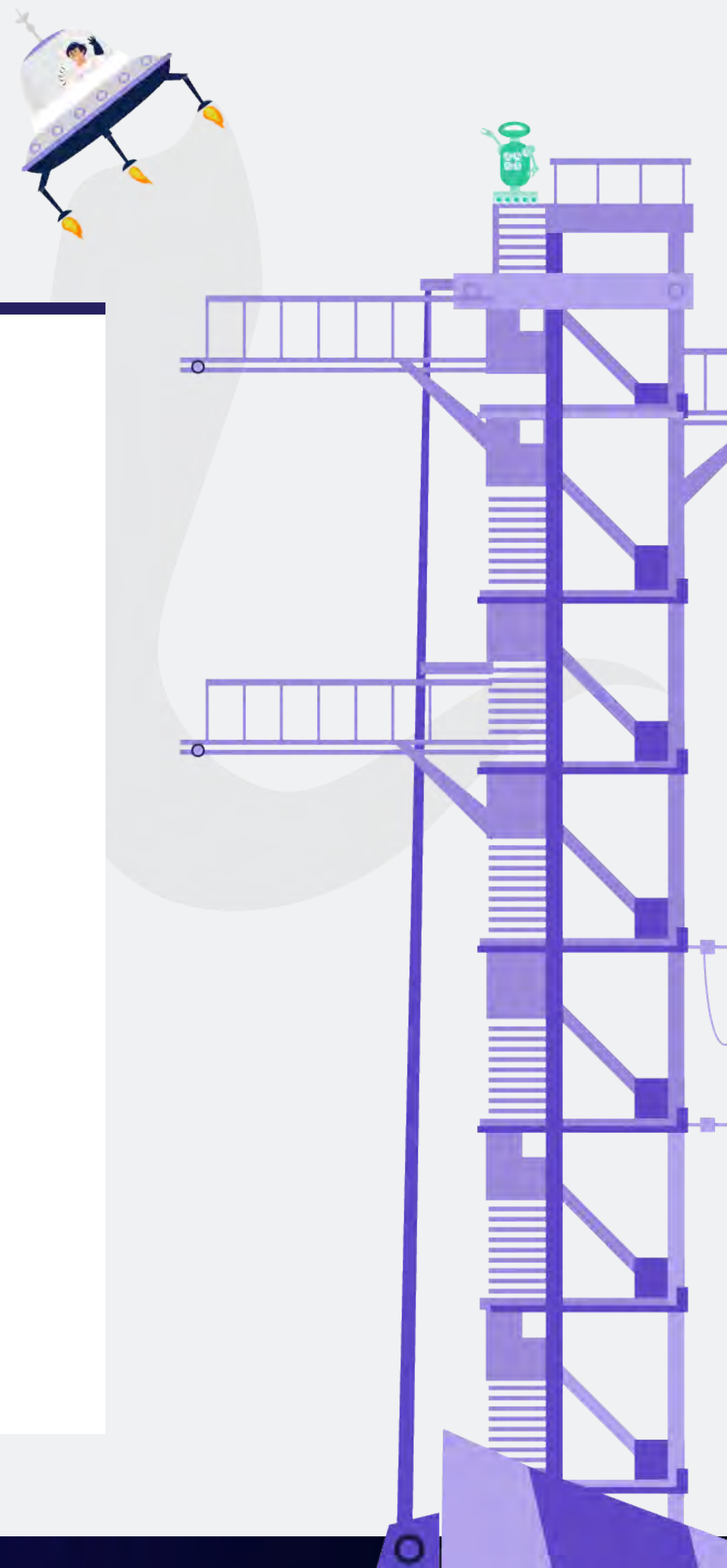
Respondents operating risk and compliance in silos are more concerned with AI risk

We also wanted to know if respondents' approaches to managing IT risk impacted their concern for AI risk. We found that respondents who manage risk and compliance in silos are more concerned about AI risk, which is likely due to their lack of visibility into their processes, risk management activities, and compliance postures.

Coming into 2024, how concerned are you with business risks associated with generative AI?

Approach to risk management





CHAPTER 3

New Frontiers: **Mapping the Risk Landscape**

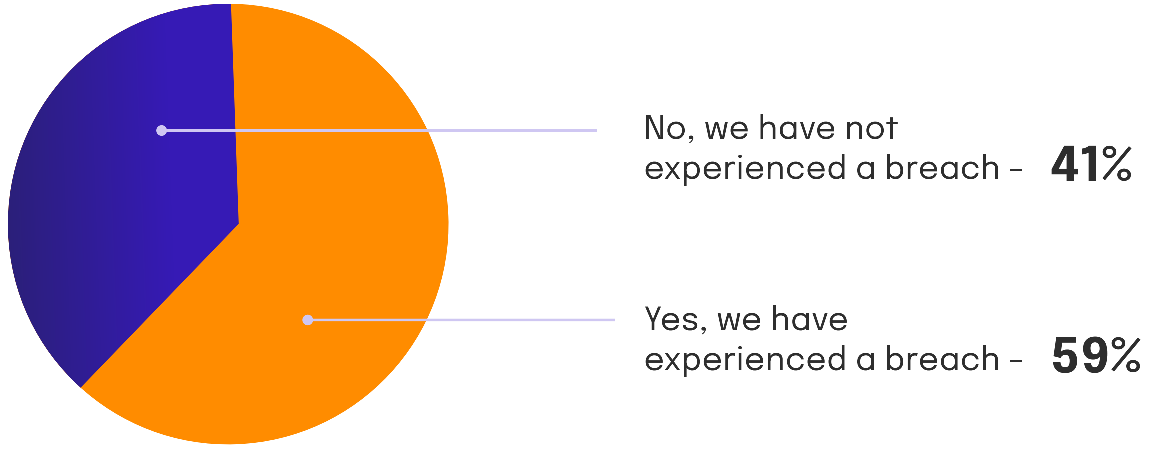
CHAPTER 3

New Frontiers: **Mapping the Risk Landscape**

Data breaches – and their business impacts – are on the rise.

In our 2023 report, 42% of respondents experienced a breach in the last 24 months. The latest survey paints a more concerning picture, revealing a notable spike to 59% – a 40% increase from the previous year – underscoring the increasing risk landscape.

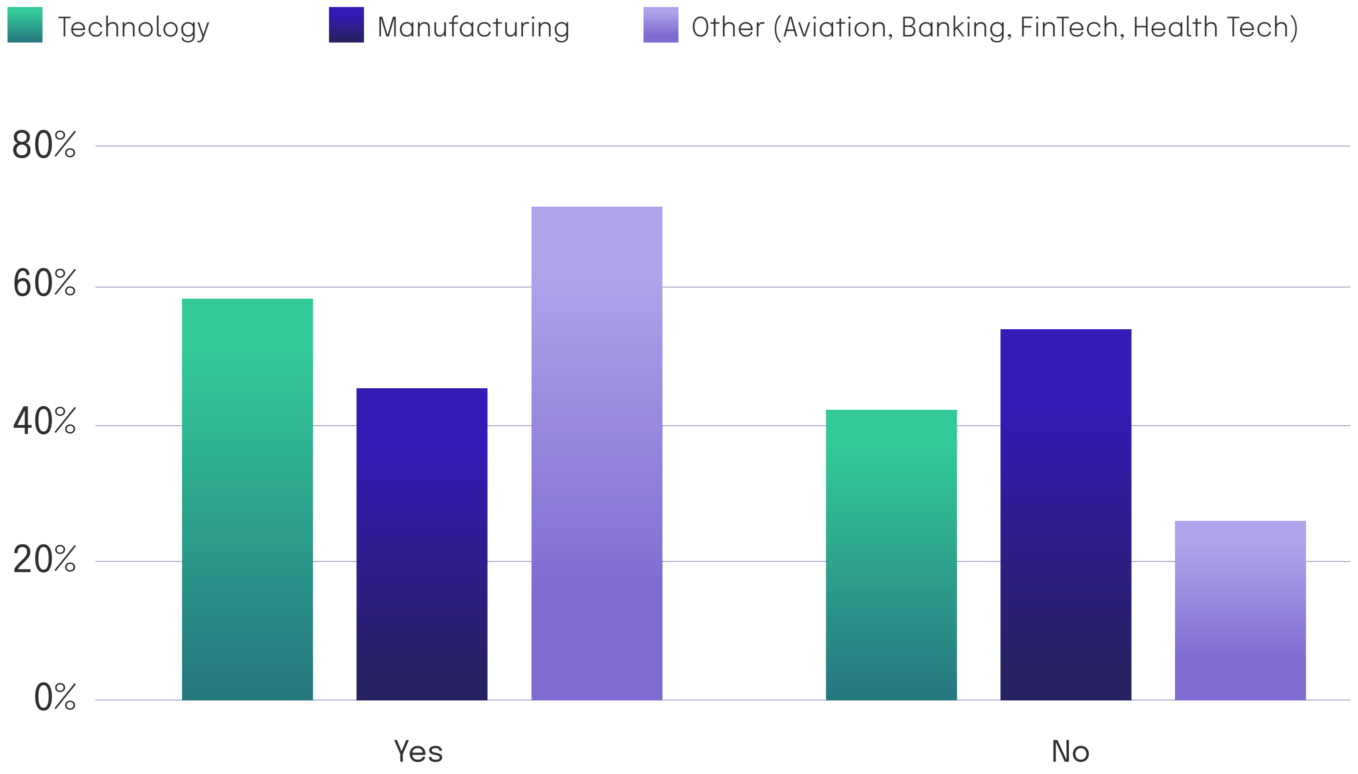
Has your organization experienced a breach in the last 24 months?



To keep up, organizations must proactively invest in cybersecurity measures, fine-tune risk management strategies, and maintain unwavering vigilance against the evolving landscape of cyber threats. The collaboration between cybersecurity and GRC professionals is also more crucial than ever, forming the cornerstone for building a resilient and secure business environment. By sharing risk data or having a consolidated view of risks, rather than a siloed view, collaboration can happen more freely – helping teams consolidate efforts and better streamline business security.

Security breaches are not confined to a specific industry; rather, they permeate across all surveyed sectors. From technology and manufacturing to other industries like aviation, banking, FinTech, and health tech, incidents occur across the board.

Has your organization experienced a breach in the last 24 months?



Biggest risk stressors

Maintaining a risk management program in the current landscape – with the potential legal and financial consequences of breaches, while threat actors continually innovate – is a stressful task. IT and GRC professionals are experiencing stress in a multitude of areas and respondents are looking for ways to mitigate it. Stress about cybersecurity risk – which has been the highest factor for the last two years – came in on top at 19%. Updating compliance requirements was the second highest stressor, followed by keeping up with the latest technology. Concern about AI technologies and their subsequent and unique risks has likely contributed to stress from keeping up with the latest technology, which we covered in detail in chapter two.

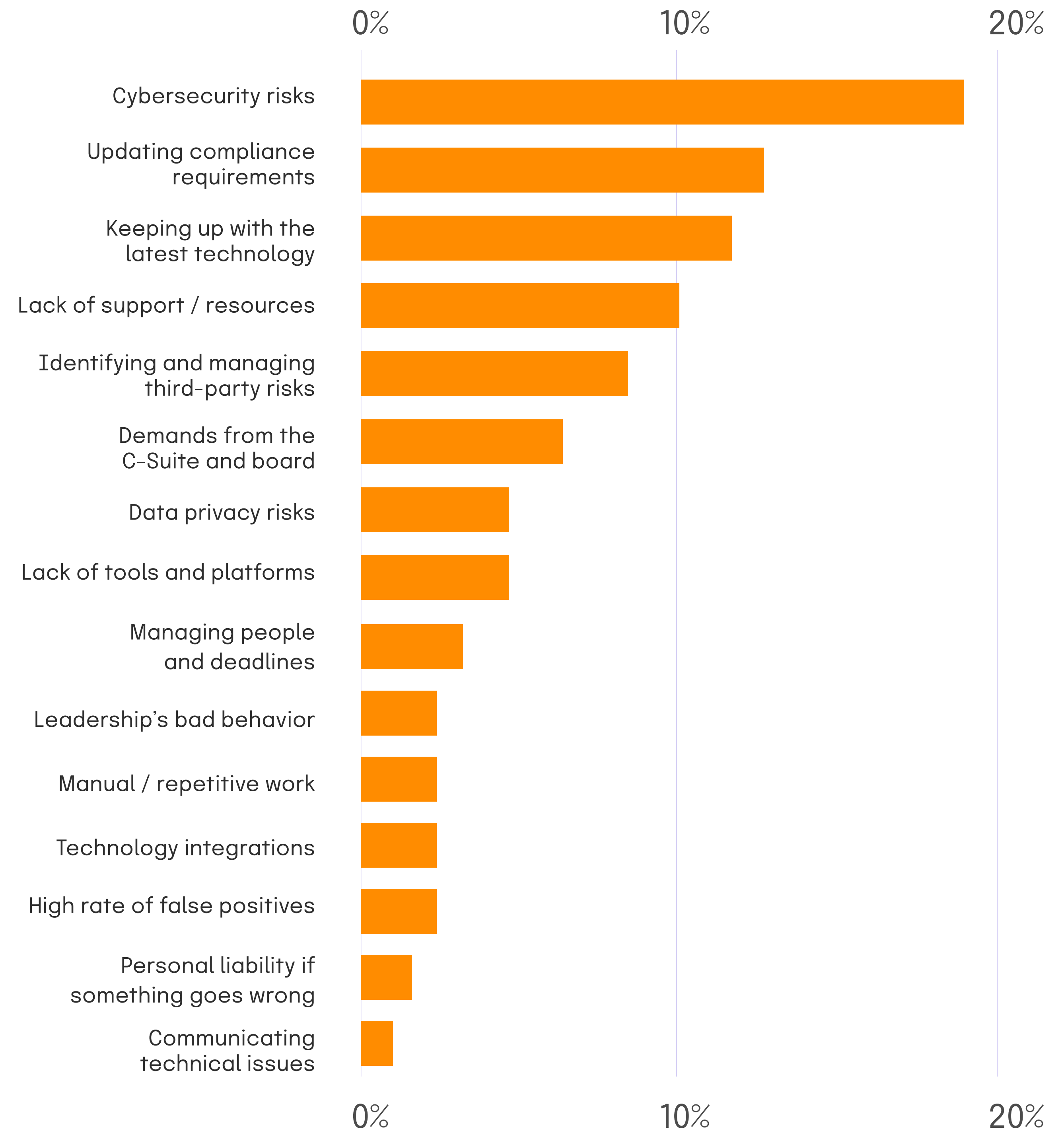
KEY STAT

19%

stress the most about cybersecurity risk

Notably, identifying and managing third-party risk came in at only 9%, **a 69% decrease** from last year. This may be in part due to the increase in adopting technology to help manage third-party risks in lieu of leveraging spreadsheets and other more manual tools. Nonetheless, this decline comes as a surprise, as third-party risk continues to be one of the greatest hurdles facing compliance and risk management teams. Third-party breaches and supply chain disruptions are increasing, showing that third-party risk remains a large part of the risk management picture. We'll dive deeper into third-party risk and its effects in chapter four.

Which of the following causes your job to be more stressful?



Actions taken to mitigate stress

With stress on the rise – and showing no signs of slowing – GRC and IT professionals understand the value of taking steps to mitigate it. The top action, coming in at 69%, is using GRC software to automate work around evidence collection, issue tracking, remediation, control monitoring, and/or reporting of risk and compliance activities. This statistic demonstrates a continued commitment to using technology tools, like GRC software, to operationalize and automate work around tedious tasks in the GRC space.

KEY STAT

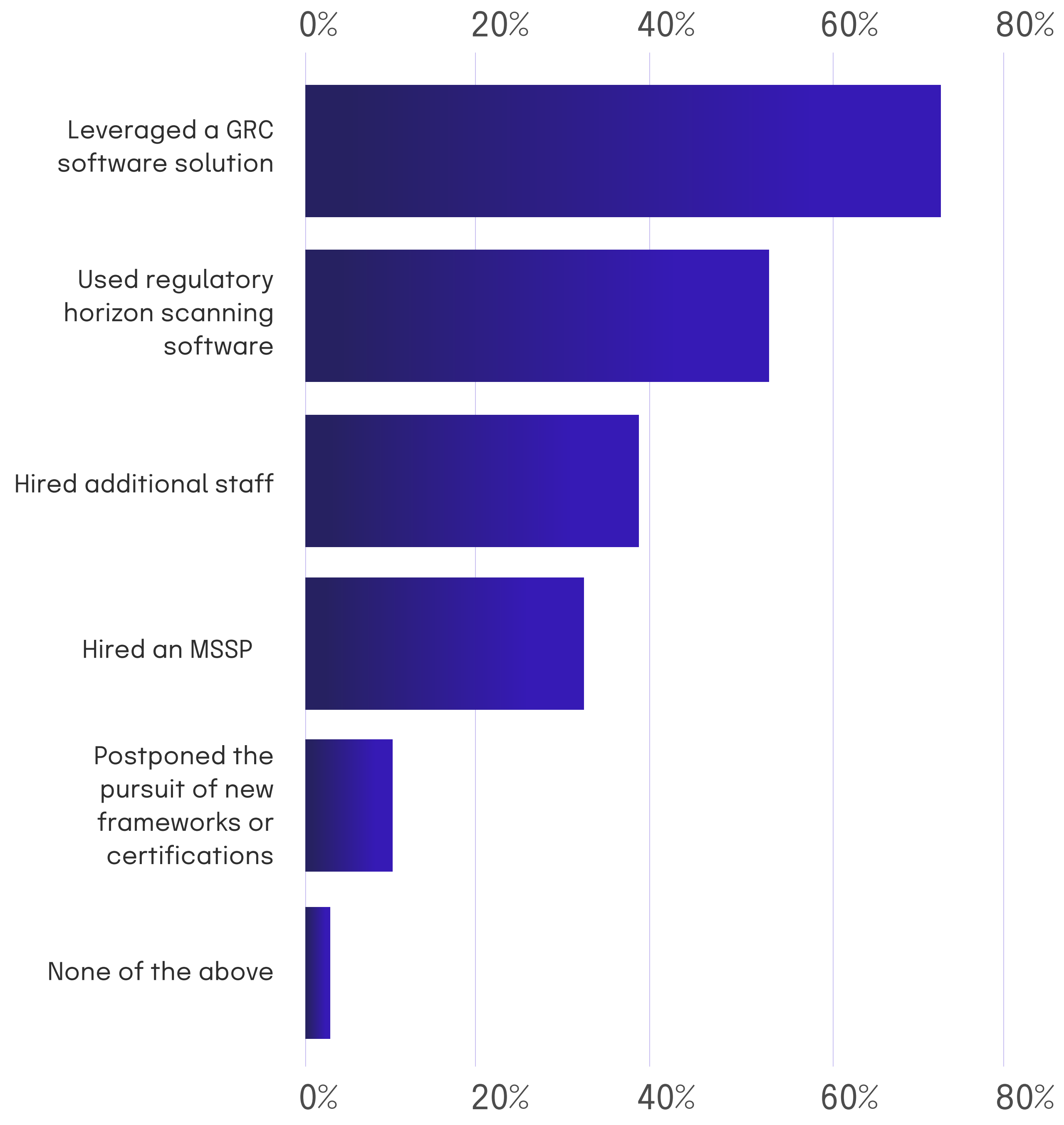
69%

use GRC software to automate work and streamline compliance activities

Following this tactic is using regulatory horizon scanning software (53%), a method of keeping up-to-date with both local and global regulatory changes that may impact your business operations. By monitoring these changes closely, GRC and IT professionals can simplify and streamline their strategies to better allocate their limited resources.

This year, just 7% of respondents chose to postpone the pursuit of new compliance frameworks/certifications. **This is a 78% improvement from last year, where 32% of respondents postponed new frameworks and certifications to mitigate stress.** This change demonstrates an improvement in overall risk management strategies. Business leaders understand that putting off the pursuit of new compliance frameworks or certifications is unsustainable if they are to ensure the profitability of their companies. Delaying new frameworks and certifications only opens organizations up to even more risks and can limit their business growth. Along with increased pressure to keep companies safe, there is also pressure to handle administrative tasks more efficiently.

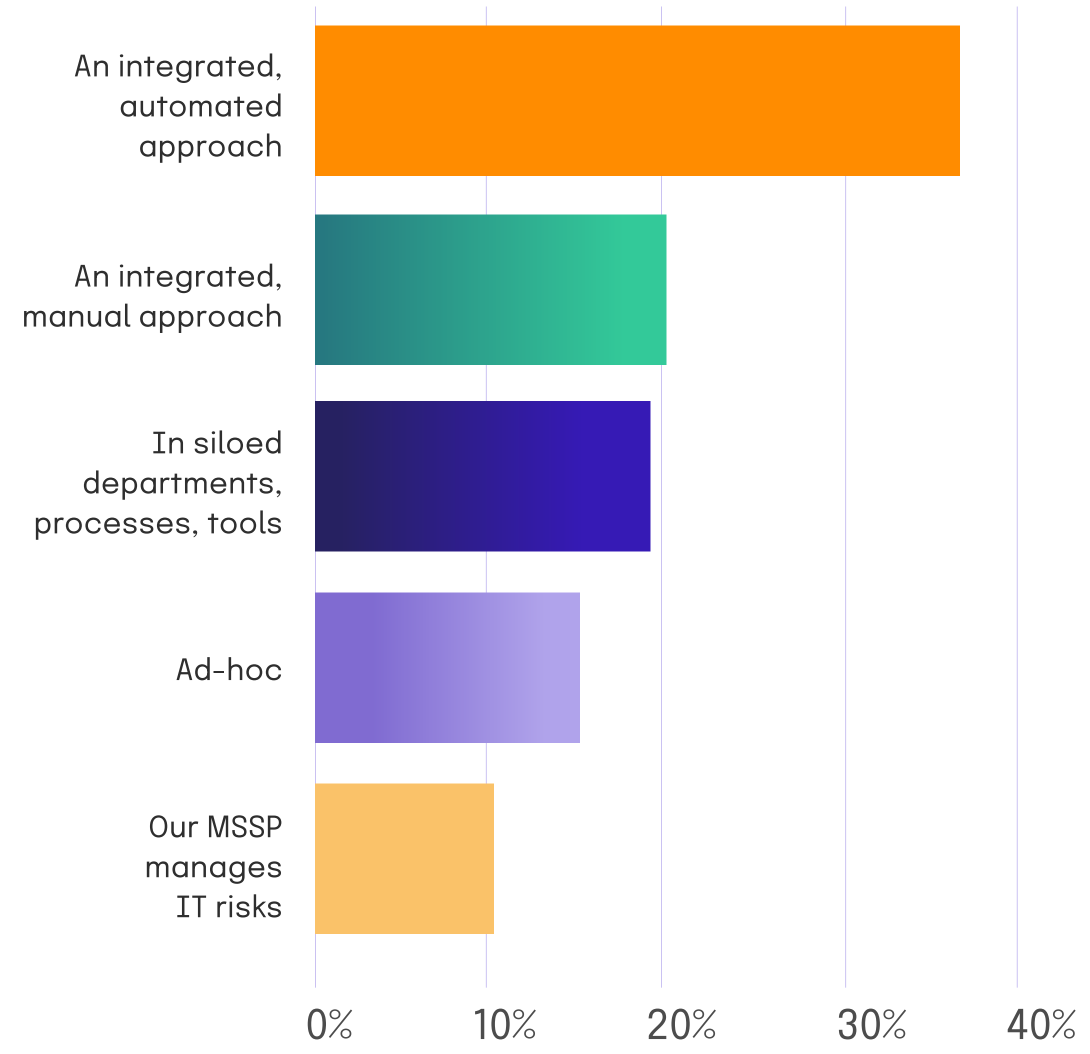
Have you or your team taken any of the following steps to mitigate stress in the past 12 months?



Approaches to managing risk

The number of companies reporting that they have pivoted from a siloed approach to managing IT risks across departments, processes, and tech to a more unified approach has dramatically improved. **90% in 2023 reported managing compliance and risk in silos, compared to a mere 19% this year.**

Describe your organization's approach to managing IT risk:



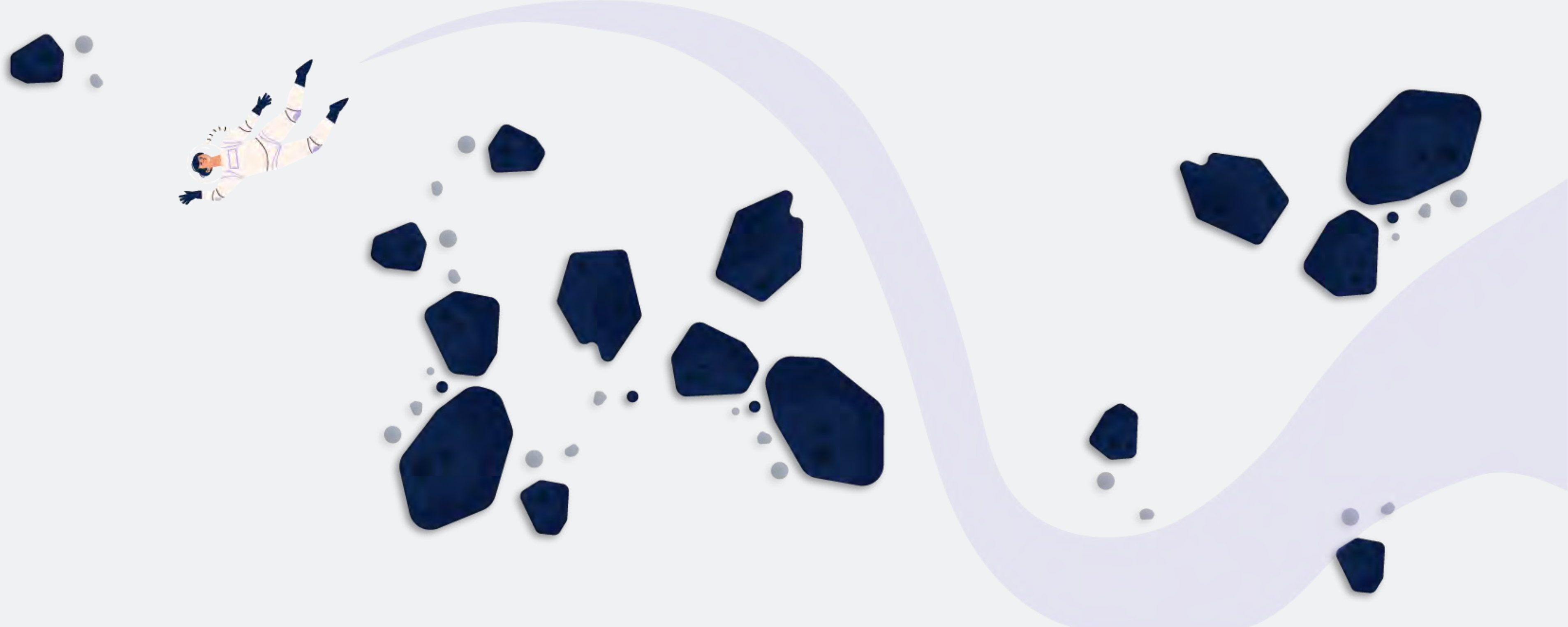
Best practices for risk management

Breaking down silos is only one part of effective risk management. To better understand what it takes to effectively manage risk, we asked respondents what actions they are taking based on 10 best practices outlined by experts at NIST, ISO, and other organizations:

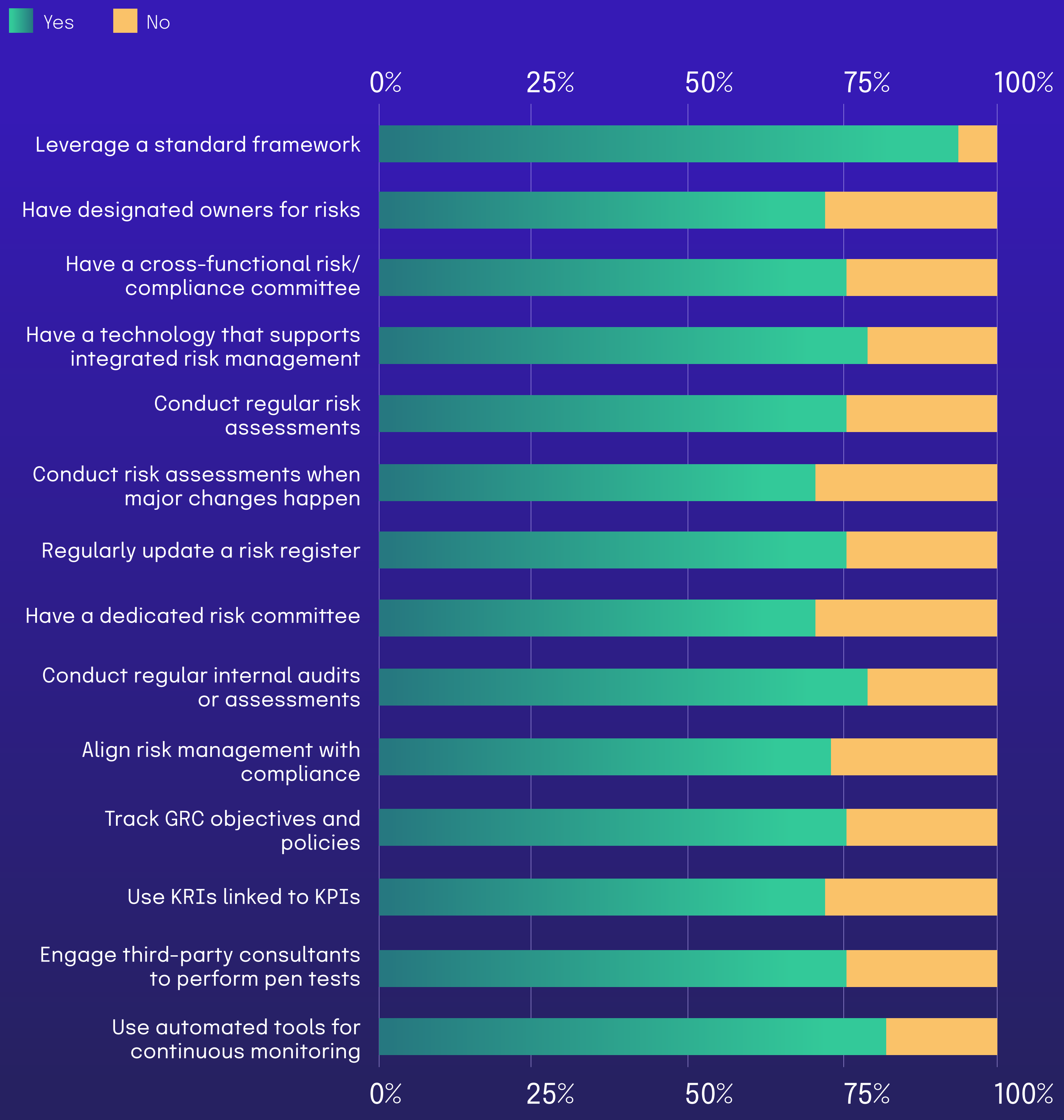
1. Using an IT risk management framework to identify and manage IT risks
2. Identifying clear roles and responsibilities and owners for various risks
3. Creating a cross-functional risk/compliance committee that meets regularly to execute risk management tasks
4. Putting together a technology architecture that supports integrated risk management
5. Conducting risk assessments on a cadence
6. Reassessing risks whenever major changes occur
7. Maintaining a risk register
8. Conducting internal audits/assessments of controls
9. Aligning risk management and compliance efforts
10. Having ongoing monitoring processes

We found that the vast majority of surveyed organizations have made commitments to manage their IT risks using a formal, disciplined approach. The most common action was leveraging a risk management standard or framework at 94% of respondents. Another leading action was leveraging automated tools like integrated GRC platforms to facilitate their programs. The use of GRC technology platforms makes monitoring and maintaining internal controls a significantly easier task, as opposed to the manual work that typically takes place when assessing control effectiveness. This emphasis on eliminating tedious, manual processes aligns with the conclusions of our past and present reports, demonstrating the shift in the market to adopt such technologies to ensure a more streamlined risk and compliance experience for their teams.

> *The use of GRC technology platforms makes monitoring and maintaining internal controls a significantly easier task*



Which of the following best represents the actions you've taken to formalize your commitment to risk management?



Companies with an integrated approach to compliance and risk management, in most cases, have formalized their approach to risk management more than those who did not. Respondents with an integrated approach more frequently used automated tools for continuous risk monitoring and controls testing. They were also more likely to map controls to the risks they mitigate, as well as having a dedicated risk committee that meets regularly to update and discuss the risk register. Of course, those with an integrated approach were also more likely to have the technology architecture to support integrated risk management.

Compared to respondents who handle risk and compliance separately, those who had an integrated approach were 13% more likely to conduct risk assessments (in addition to their scheduled risk assessments) whenever major changes occur that may change their risk profile and reprioritize risks. This demonstrates that taking an integrated approach to risk management and compliance helps accomplish more formalized risk management commitments.

The market is shifting to adopt integrated GRC technologies to ensure more streamlined risk and compliance management.

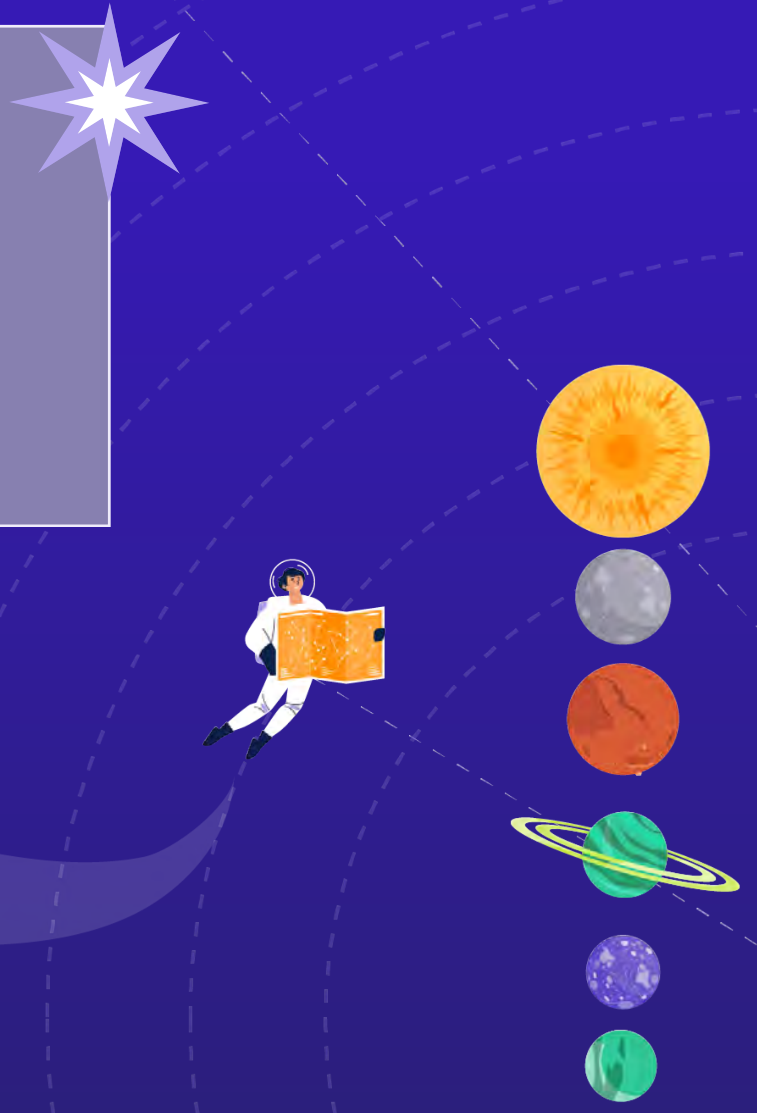
Which of the following best represents the actions you've taken to formalize your commitment to risk management?
Summary of actions taken:

	How respondents view the purpose of the compliance function:		
	Function that enforces regulations or industry standards	Risk and compliance activities are conducted separately	Risk and compliance activities are tied together and aligned
Use a risk management standard/framework	95%	95%	92%
Have designated owners for risks	67%	73%	75%
Have a risk/compliance committee	73%	75%	74%
Use technology that supports integrated risk management	73%	75%	80%
Conduct regular risk assessments	71%	76%	75%
Conduct risk assessments when major changes occur	70%	67%	77%
Regularly update risk register	75%	77%	74%
Have a dedicated risk committee	64%	67%	74%
Conduct regular internal audits on controls	75%	80%	74%
Align risk management and compliance efforts	70%	71%	74%
Track GRC with policies and risk mitigation controls	71%	74%	74%
Use KRIs linked to KPIs to monitor critical risks	68%	72%	72%
Engage third-party consultants for pen tests	76%	76%	72%
Use automated tools for continuous monitoring	72%	75%	82%

KEY STAT

81%

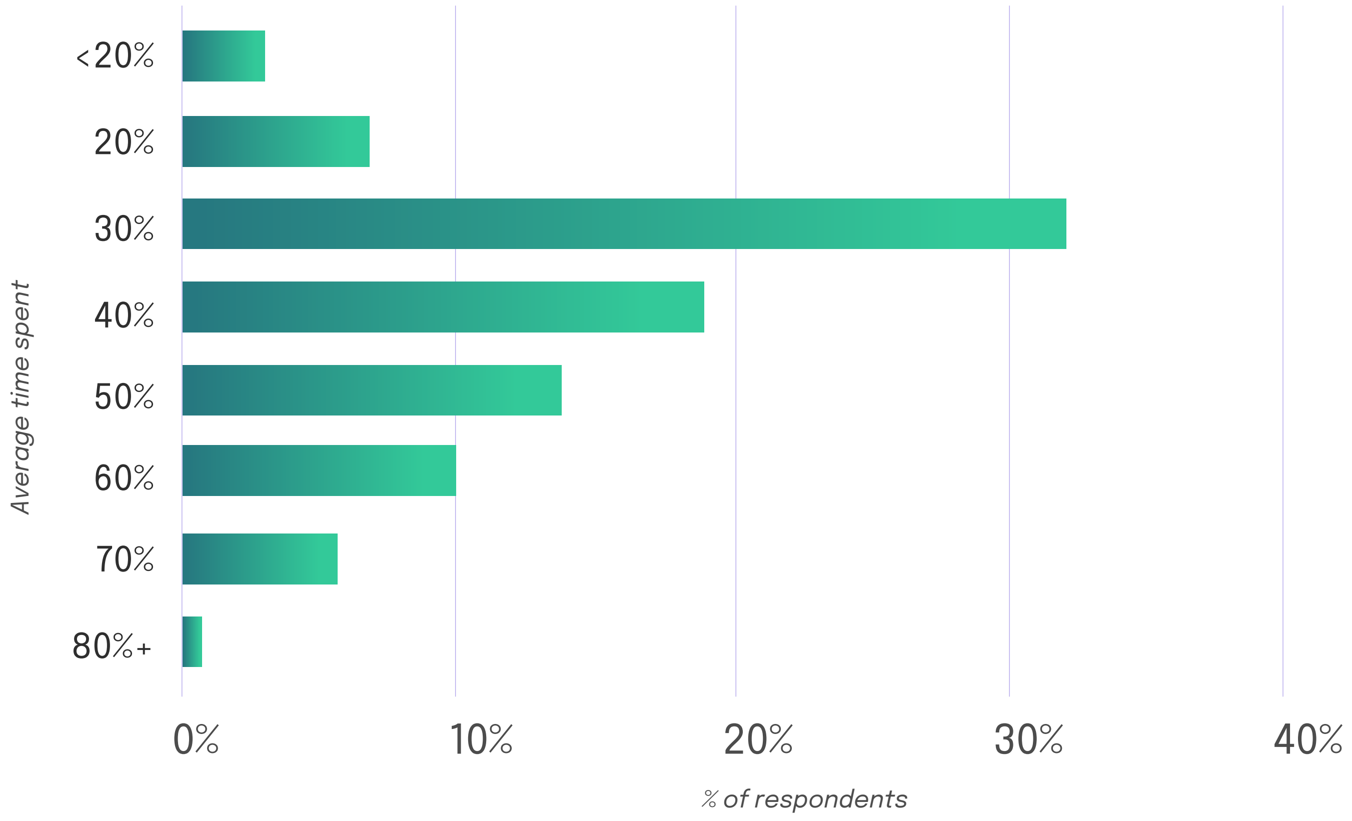
spent 30% or more time on manual processes



Manual risk management processes

Many of the processes facing risk and compliance stakeholders are extremely manual, creating one of the most critical challenges facing the industry. This year, we found that 81% of respondents spent 30% or more of their time on manual processes. Contrasting last year, where more than half of respondents dedicated 40% or more of their time to manual or administrative tasks, the proportion has decreased in 2024. Only 49% of respondents spend 40% or more of their time on such tasks, compared to 55% last year. Although time spent on manual tasks has decreased overall, there is still much room for improvement, like attributing more resources to GRC by additional headcount or investing in new technology.

What portion of your risk and compliance management team's time is spent on repetitive or administrative tasks?

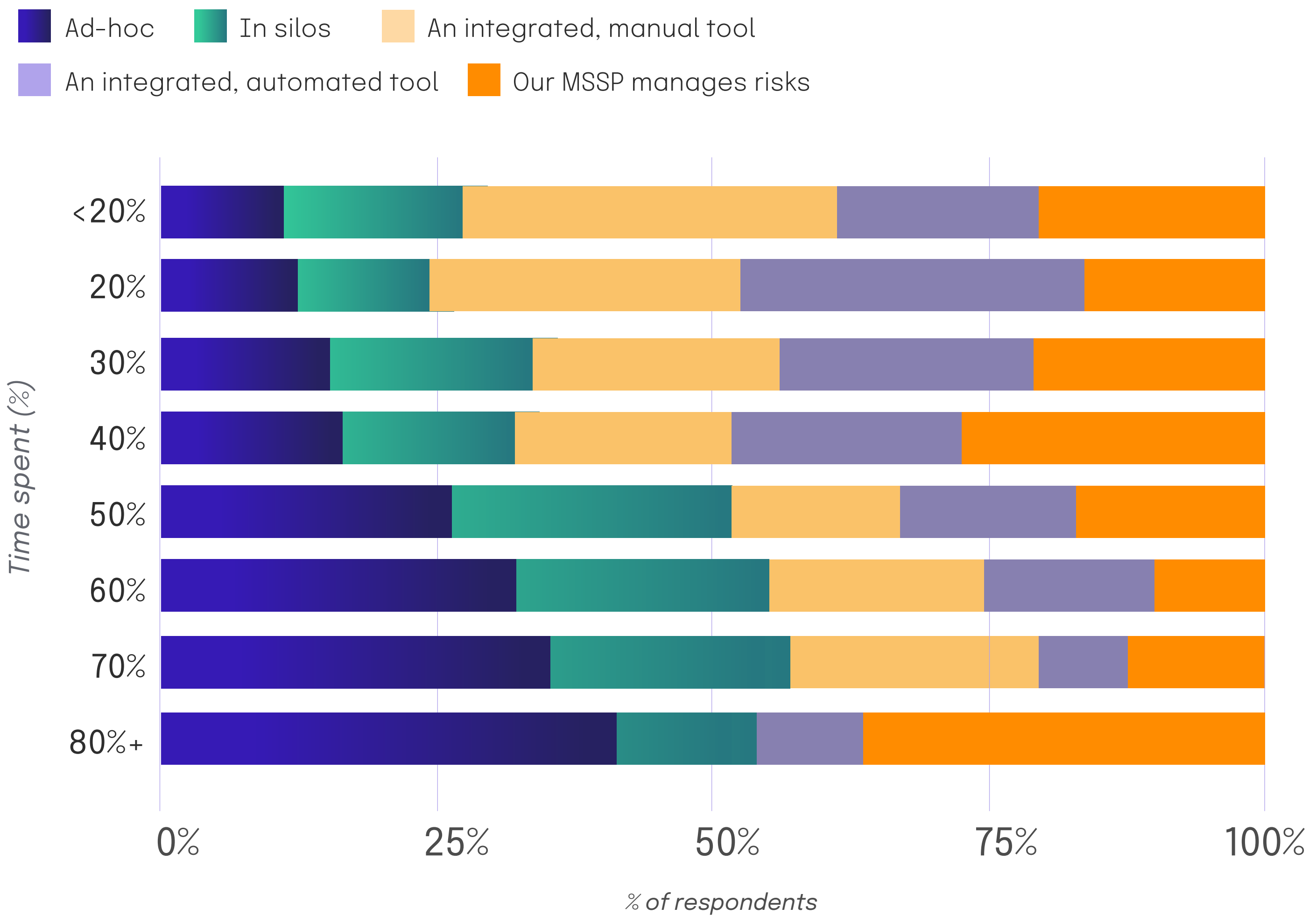


Time spent on manual tasks vs. approach to risk management

Respondents who operate risk and compliance in siloed departments were most likely to report that half of their time was spent on repetitive, administrative tasks. Companies that handled risk with an ad-hoc approach dealt with the most manual, repetitive tasks. **Those with an integrated, mostly automated tool had the fewest manual tasks, with only 20% of their time spent on manual work.**

Time spent on repetitive or administrative tasks:

Approach to risk management



Risk assessments have become more frequent

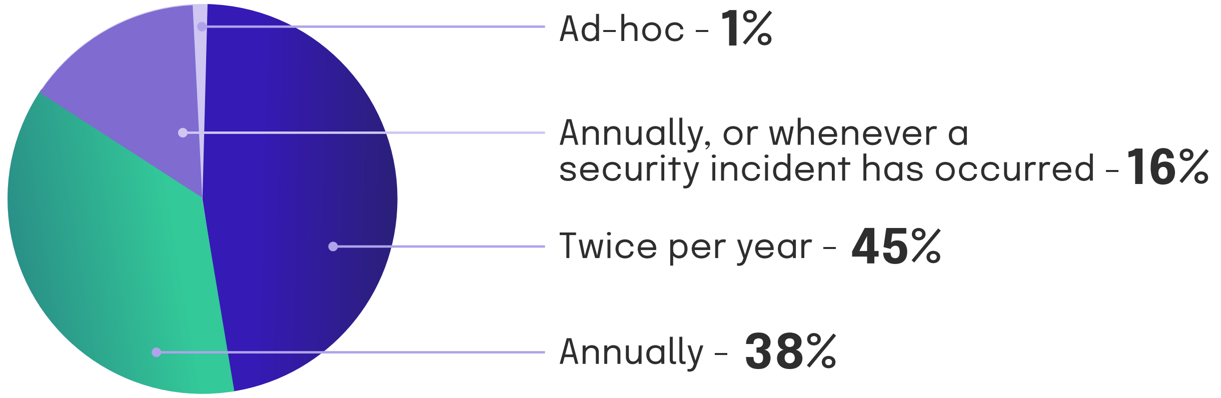
Risk assessments are a vital part of the risk management process, helping teams establish baselines and other trends for their risk programs. Only 38% of respondents reported conducting risk assessments annually, which is a 32% decrease from last year. However, the frequency in which respondents are conducting risk assessments has increased: 45% of respondents conduct risk assessments twice a year, up from 27% last year. Respondents conducting annual risk assessments in addition to whenever a security incident has occurred and/or there were major changes to their environments came in at 16%. Lastly, only 1% of respondents conduct risk assessments ad-hoc or as-needed.

KEY STAT

45%

conduct risk assessments twice a year, +27% YoY

How often does your organization conduct security risk assessments?

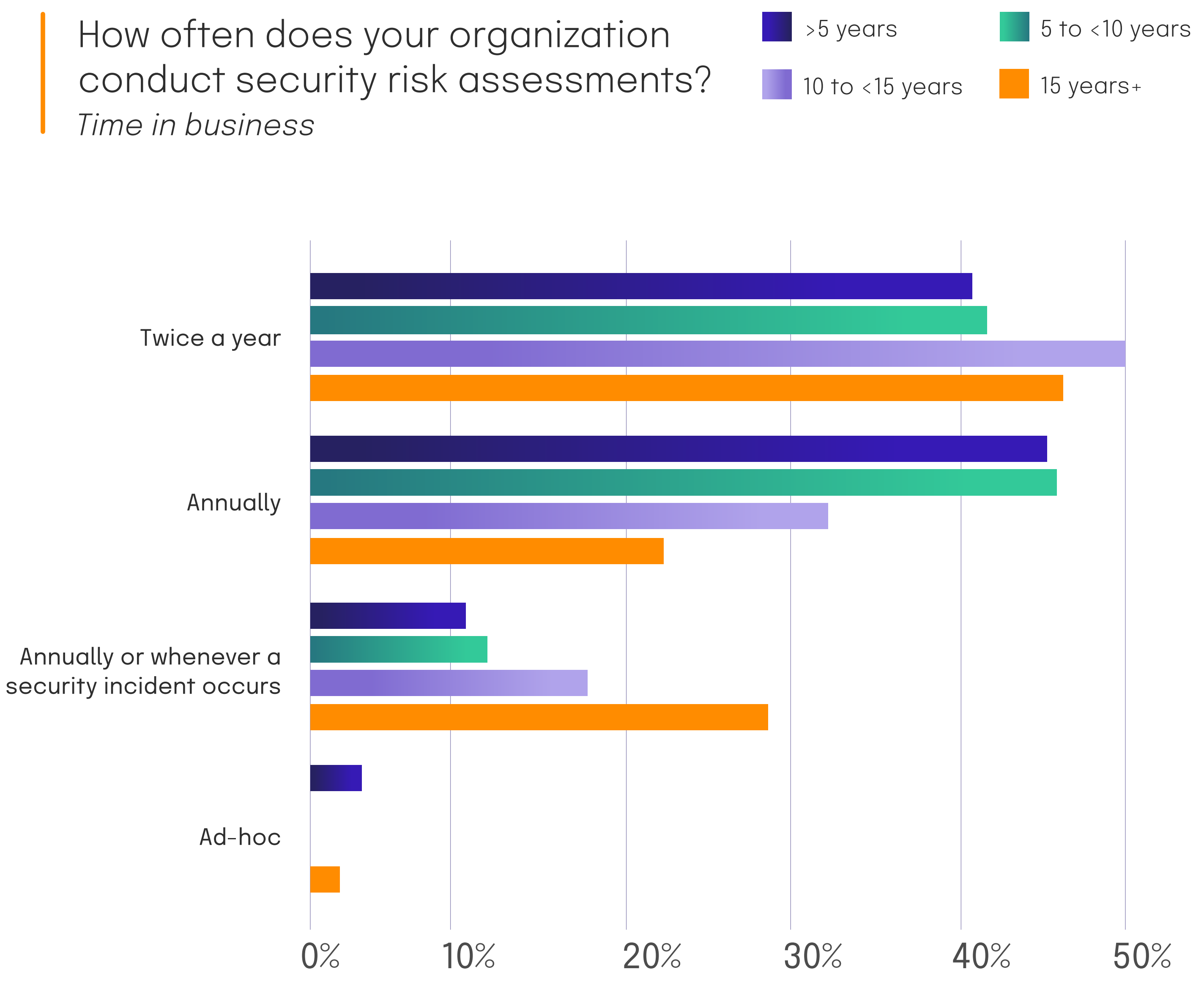


These changes demonstrate that the industry is shifting; **assessing risk once a year is no longer enough**. Teams are making changes to the fundamental aspect of their risk management programs because threats are continuing to rise. Unsurprisingly, mature companies that had more employees and a longer business tenure were more prone to conducting assessments twice a year, likely due to the size and complexity of their security compliance programs.

Additionally, organizations of all sizes agree that addressing risk ad-hoc is becoming a strategy of the past. This demonstrates the industry's commitment to improving strategies to help keep companies secure. Respondents are no longer waiting for something to happen; they are beginning to act more proactively, delving into the areas of risk that need to be addressed more frequently.

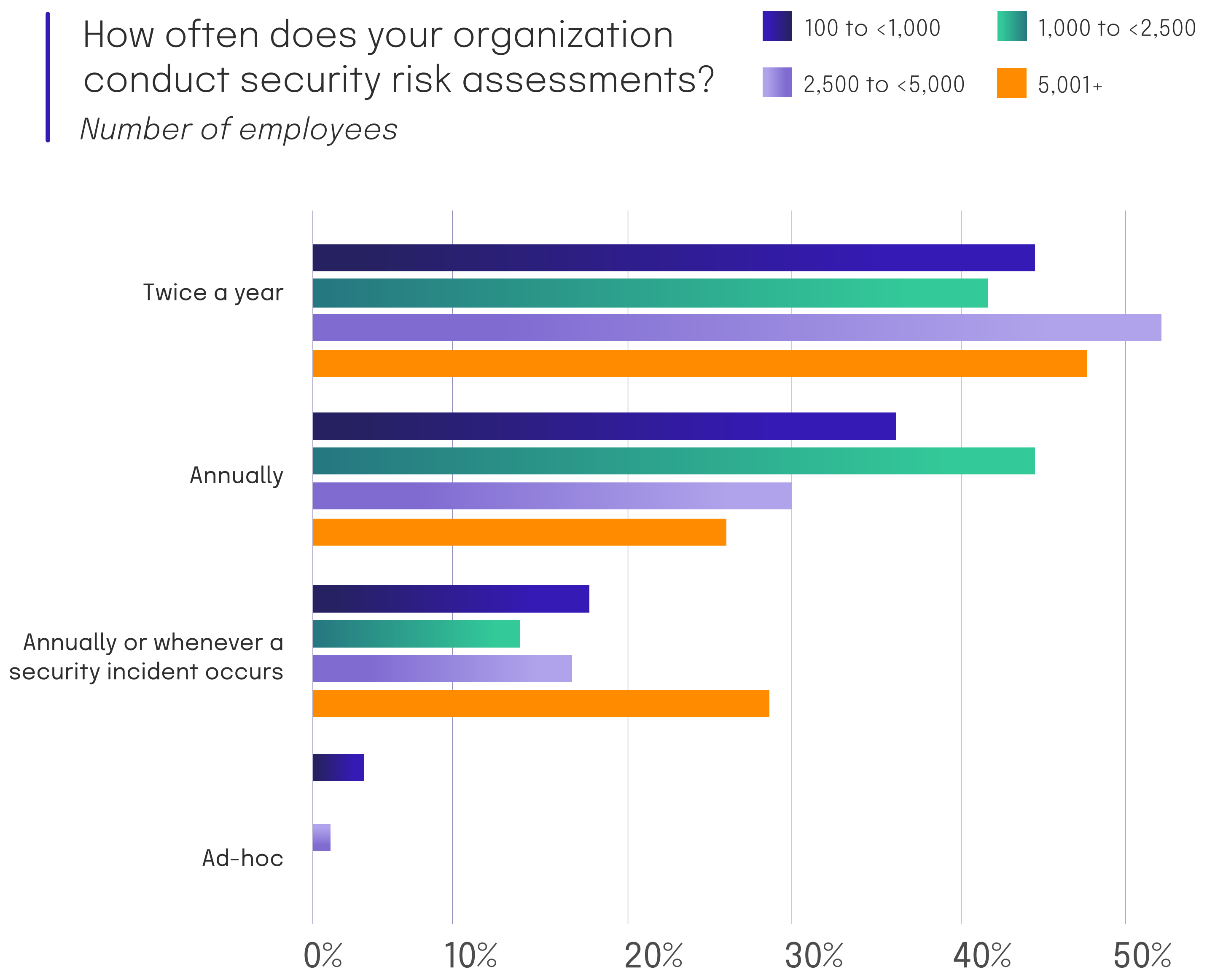
How often does your organization conduct security risk assessments?

Time in business



How often does your organization conduct security risk assessments?

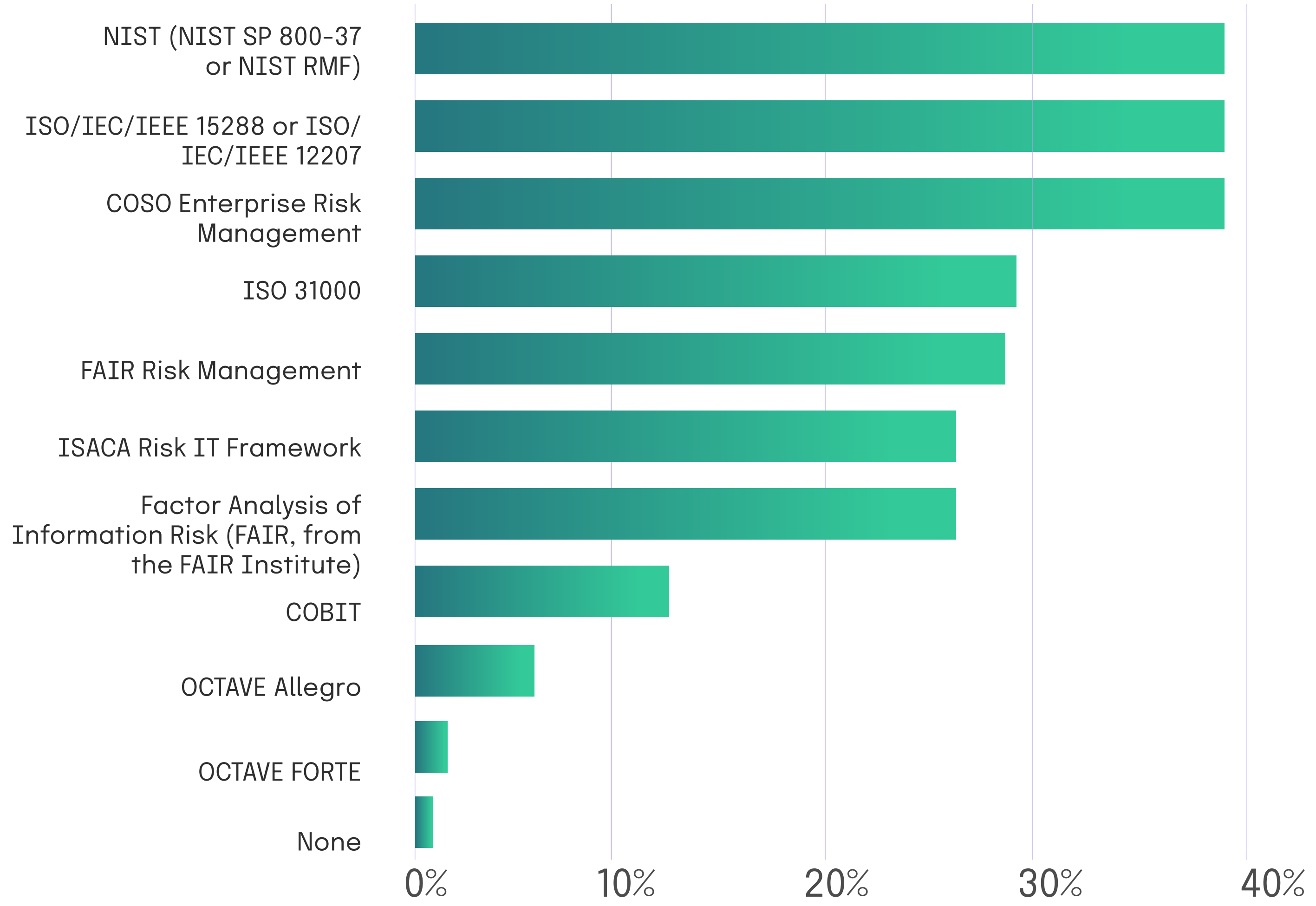
Number of employees



Risk management frameworks

This year, the top frameworks were NIST (NIST SP 800-37 or NIST RMF), ISO/IEC/IEEE 15288 or ISO/IEC/IEEE 12207, and COSO Enterprise Risk Management, all coming in at 39% of respondents. The next most commonly used frameworks were ISO 31000 at 29% and FAIR Risk Management at 28%. Trailing shortly behind are ISACA Risk IT Framework and Factor Analysis of Information Risk (FAIR, from the FAIR Institute) both at 26% of respondents.

Which of the following frameworks are you using to manage risks?

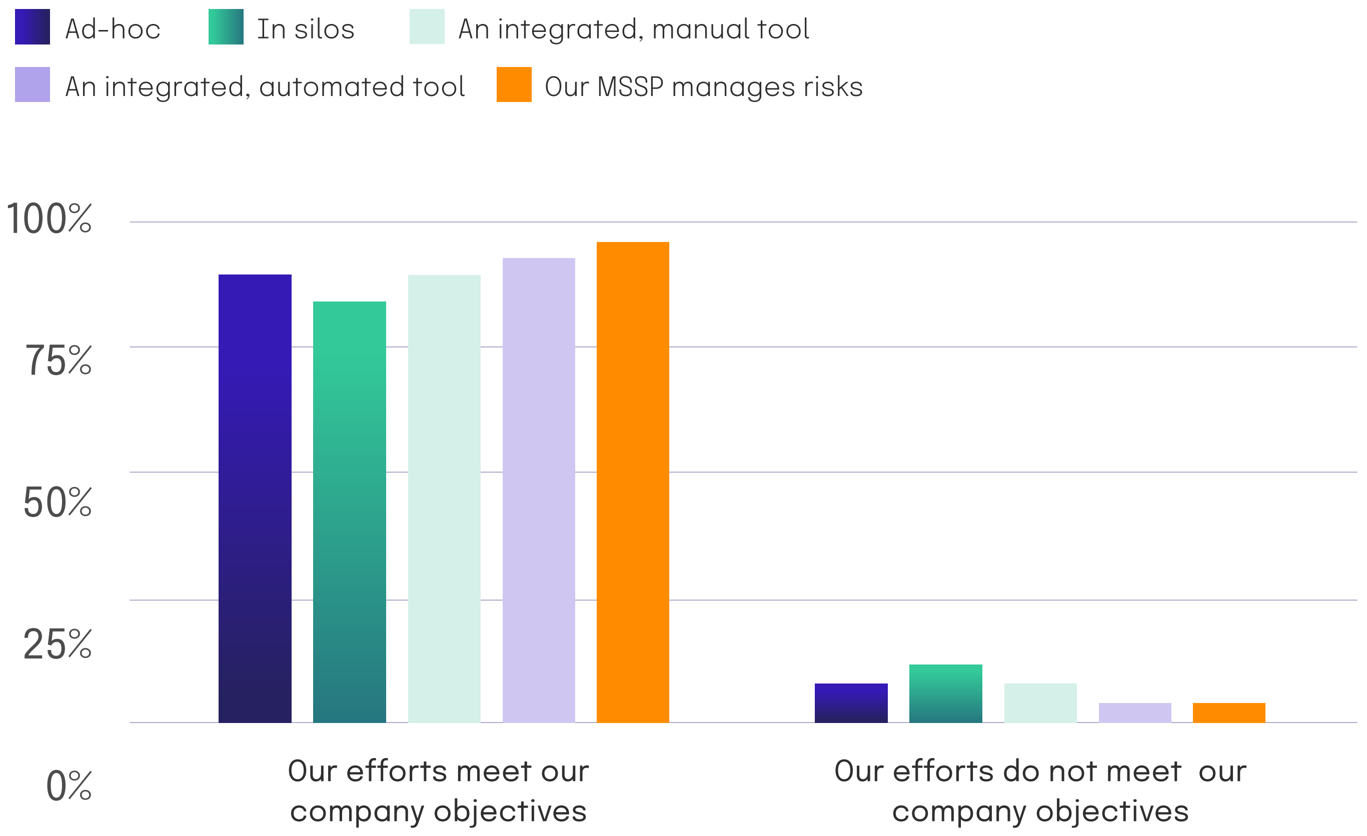


Addressing risk

While confidence to address risk remains high, companies addressing risk and compliance in silos are still more likely to experience a breach. As covered in chapter one, 92% of respondents say that the steps they've taken to identify and assess risk meet their companies' objectives, but when diving deeper, the results don't align. Across industry, company size, and location, the results were similar: overwhelmingly, confidence is high from respondents in the steps they've taken to identify and assess risks.

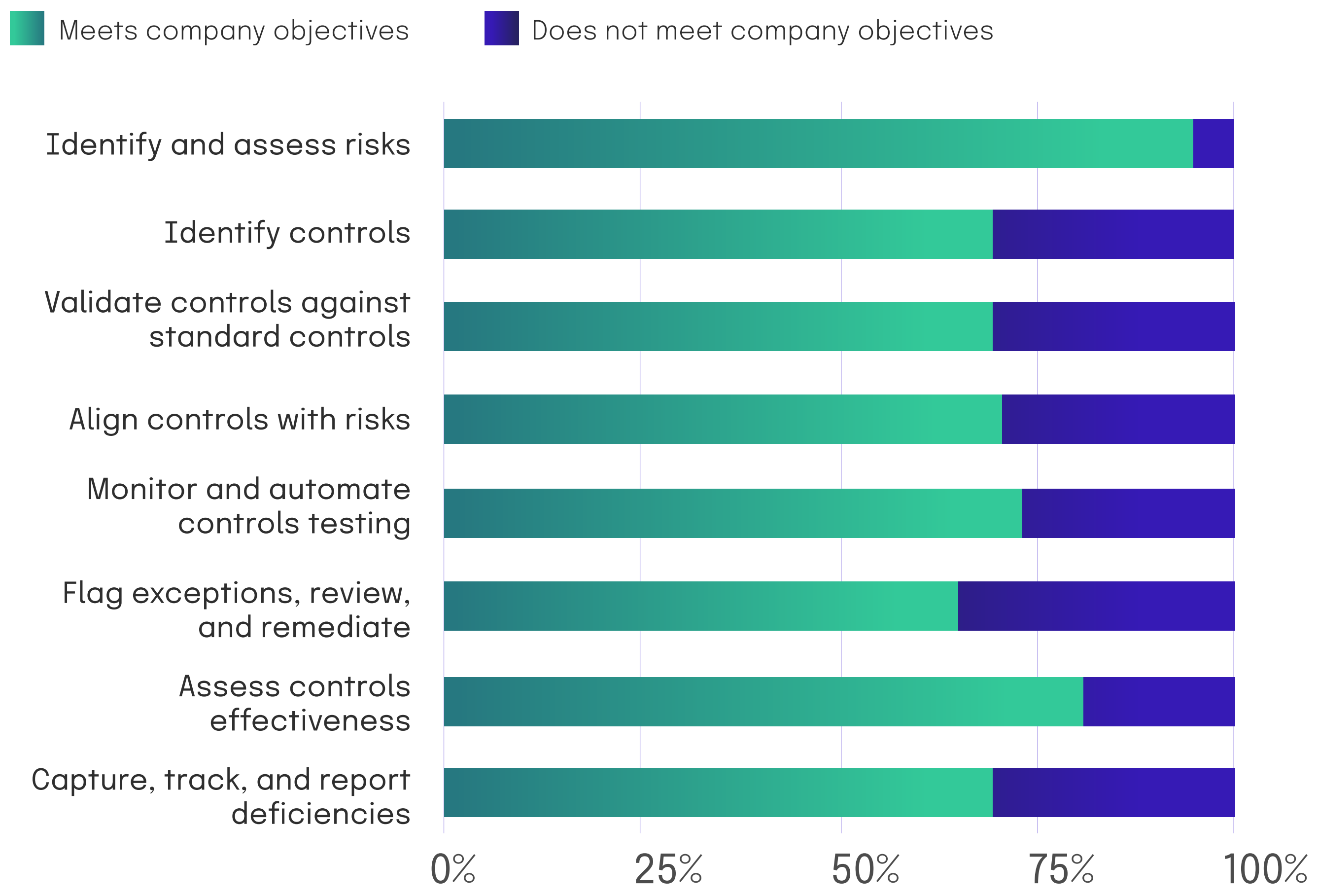
In your opinion, how well is your company doing in identifying and assessing risks?

Approach to risk management



Yet, as we dissect the outcomes based on whether companies faced a breach or not, confidence levels persist at a high. This might stem from either a sense of overconfidence among the surveyed IT and GRC professionals or the outcome of heightened vigilance in risk management strategies after a breach incident. Notably, the data underscores that, among all surveyed entities, those still operating in silos exhibited the least confidence in their capability to identify and assess risks. This resonates with our findings in chapter 1, emphasizing that **those operating within silos tend to encounter more breaches overall – and have less confidence in their ability to address risk.**

In your opinion, how well is your company doing in performing each of the following risk management actions?



The high confidence of identifying and assessing risks does not paint the entire picture. The average percentage of respondents not meeting objectives was 28% across all other aspects of risk management, including: identifying controls; validating controls against standard controls (in compliance frameworks); aligning controls with risks; monitoring and automating controls testing; flagging exceptions, reviewing, and remediating risk; assessing controls effectiveness; and capturing, tracking, and reporting deficiencies. The aspect of risk management that was least likely to meet a company's objectives was flagging exceptions, reviewing, and remediating risk – demonstrating a larger problem: **respondents can confidently identify and assess risk, but they struggle most with flagging exceptions, risk review, and remediation.**

Organizations grapple with complexities beyond mere identification and assessment of risks. The data highlights areas of improvement in various aspects of risk management, shedding light on the nuances that contribute to a comprehensive GRC strategy. While addressing these internal challenges, the industry is concurrently witnessing a surge in the investment and recognition of third-party risk.

> *Respondents can confidently identify and assess risk, but they struggle most with flagging exceptions, risk review, and remediation.*

This growing emphasis on third-party risk aligns with the broader narrative of organizations seeking more efficient and holistic approaches to GRC. The preceding discussion lays the groundwork, showcasing the hurdles in risk management processes. Now, we pivot towards a parallel trajectory where investment in technology and streamlined processes become crucial in addressing these challenges and fostering a resilient risk and compliance landscape, especially in regards to third-party risk.

CHAPTER 4

Understanding Third-Party Risks in Orbit

CHAPTER 4

Understanding Third-Party Risks in Orbit

Investment in third-party risk is continuing to grow.

As businesses continue to grow, their third-party footprint does as well. With these trends, the manual work only multiplies, making it more difficult for GRC and IT professionals to identify and mitigate third-party risks. Understanding first-party and third-party risks is a complex task that cannot be conducted manually at scale. A platform that can streamline these processes and provide reporting on respondents' compliance and risk postures builds trust for boards, investors, the public, and other stakeholders who need to understand the unique risks associated with customers, vendors, and even third-party cybersecurity companies.

GRC professionals agree: 85% of respondents are using a platform to manage risks and compliance operations, and **25% of respondents are using third-party modules in a GRC platform**. The significance of efficient compliance operations is now considered a brand differentiator, heightening the importance of GRC and the ability to guarantee adherence to regulatory standards.

KEY STAT

85%

use a platform to manage risk and compliance operations

The importance of having a proactive vendor risk program is only continuing to increase year-over-year. In fact, 62% of respondents experienced a supply chain disruption related to cybersecurity that affected their ability to deliver goods or services. Vendor risk emerged as a priority in 2023 and continues to be an accelerating threat. Answering an increasing number of vendor questionnaires is a manual process for GRC and IT professionals, especially as the number of vendors with access to sensitive data at different organizations grows. As companies scale, the number of questions and complexity of assessments for vendors has continued to increase.

KEY STAT

62%

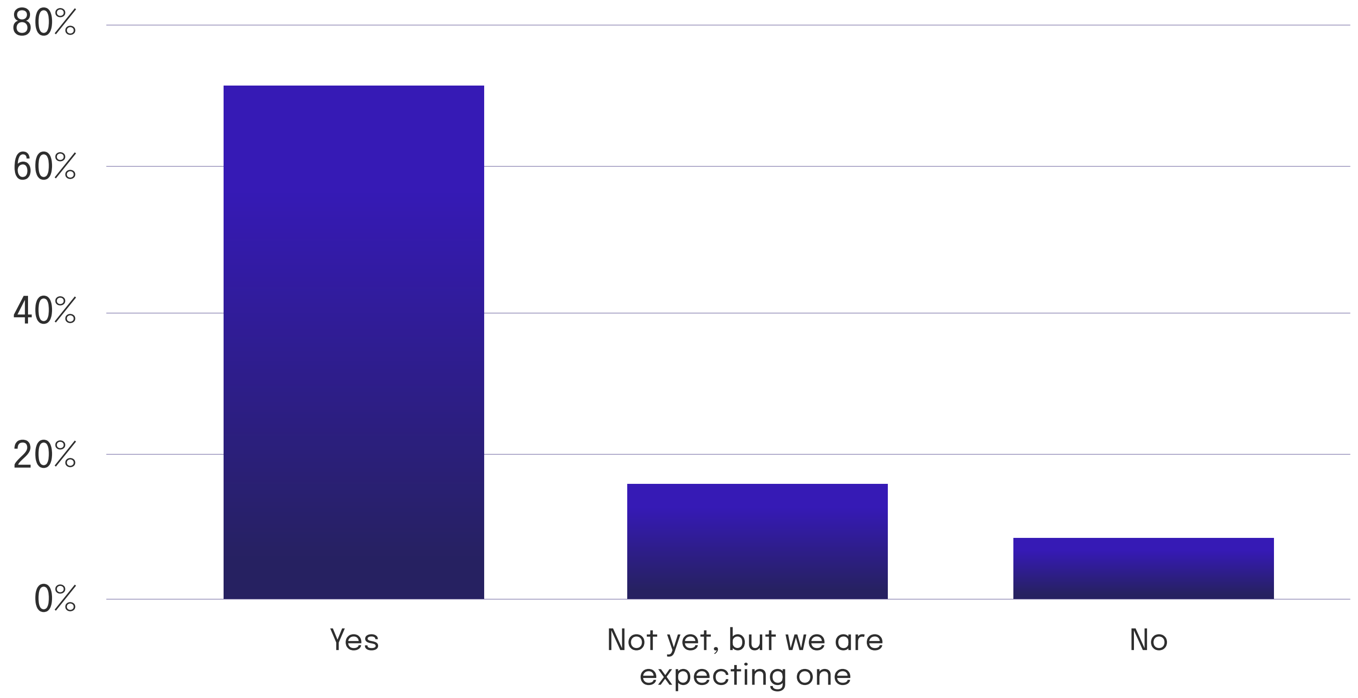
experienced a supply chain disruption related to cybersecurity

Third-party events experienced

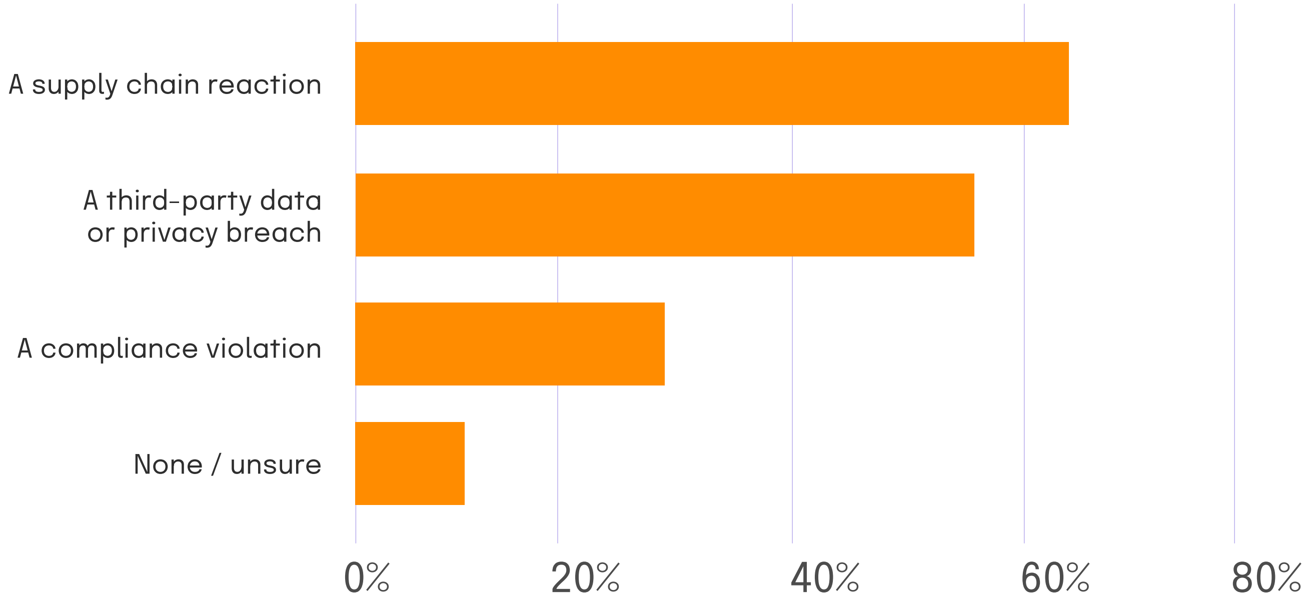
Unsurprisingly, third-party cyber incidents are expected to rise in 2024. Last year, 54% of respondents reported experiencing a supply chain disruption related to cybersecurity that affected their ability to deliver goods or services. This year, the number is up to 62% – an increase of 15% – providing evidence that third party and supply chain risks continue to prove difficult to manage, especially when it comes to cybersecurity.

89% of respondents experienced (or are expecting) an audit finding that they cannot promptly resolve related to third-party risk management. Compared to last year, where 74% had experienced or expected an audit finding, the data showed an 18% increase year-over-year, showing that third-party risk is continuing to grow.

Have you experienced an audit finding that you cannot promptly resolve related to third-party risk management?



Has your organization been impacted by any of the following events in the past year?



In our 2023 report, we found that only 46% of respondents experienced a third-party data or privacy breach affecting their organization's records or data. **This year, we found that 56% of respondents experienced a data or privacy breach due to a third-party, a 22% increase from the previous year.**

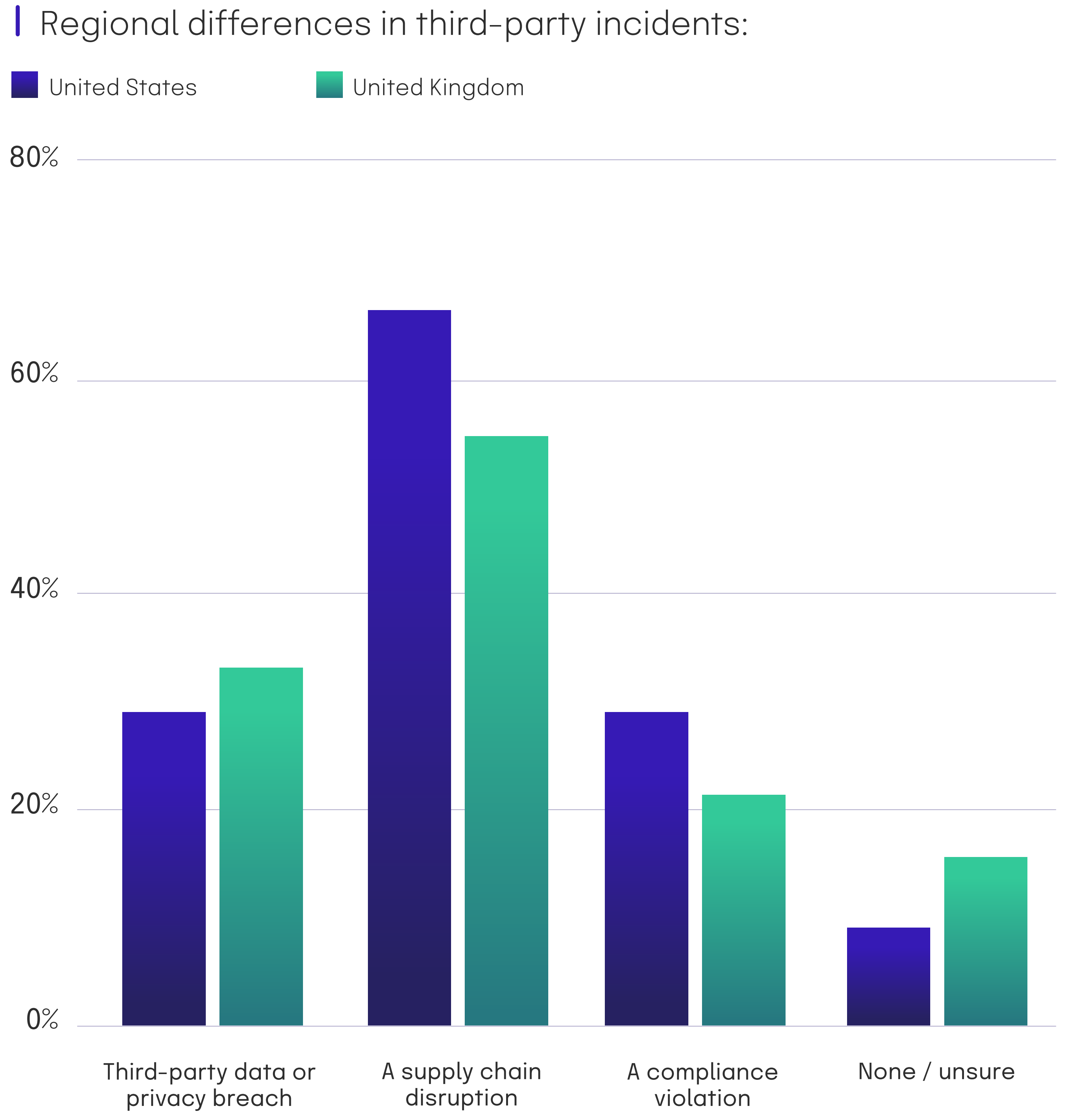
Meanwhile, the number of compliance violations related to organizations' third-party oversight reduced by 42%, coming in at 28% this year. This decrease is surprising, given that other aspects of third-party risk management have grown in frequency. Most of the third-party incidents experienced were related to data or privacy breaches and supply chain disruptions. However, with so many respondents expecting an audit finding, we may see the number of compliance violations related to third-parties grow in the coming year.

Segment differences

By region

US companies were more likely to experience supply chain disruptions related to cybersecurity, however, it's important to note that they were also the majority surveyed. 65% of respondents headquartered in the US experienced a supply chain disruption, as opposed to 55% in the UK. Additionally, 31% of respondents based in the US experienced a compliance violation related to their organization's third-party oversight versus 21% of UK respondents.

Overall, respondents headquartered in the UK were less likely to experience any negative third-party risk incidents, coming in at 14% lower than the US. The UK only surpassed the US in one category: third-party data or privacy breaches affecting organization's records or data. UK respondents were 19% more likely to experience a breach than those in the US. With regional differences in data privacy, usage, and standards, it is no surprise that the UK is much more stringent with their processes. The UK had more breaches overall but faced fewer third-party events, likely due to their tighter laws and policies around third-party risk.

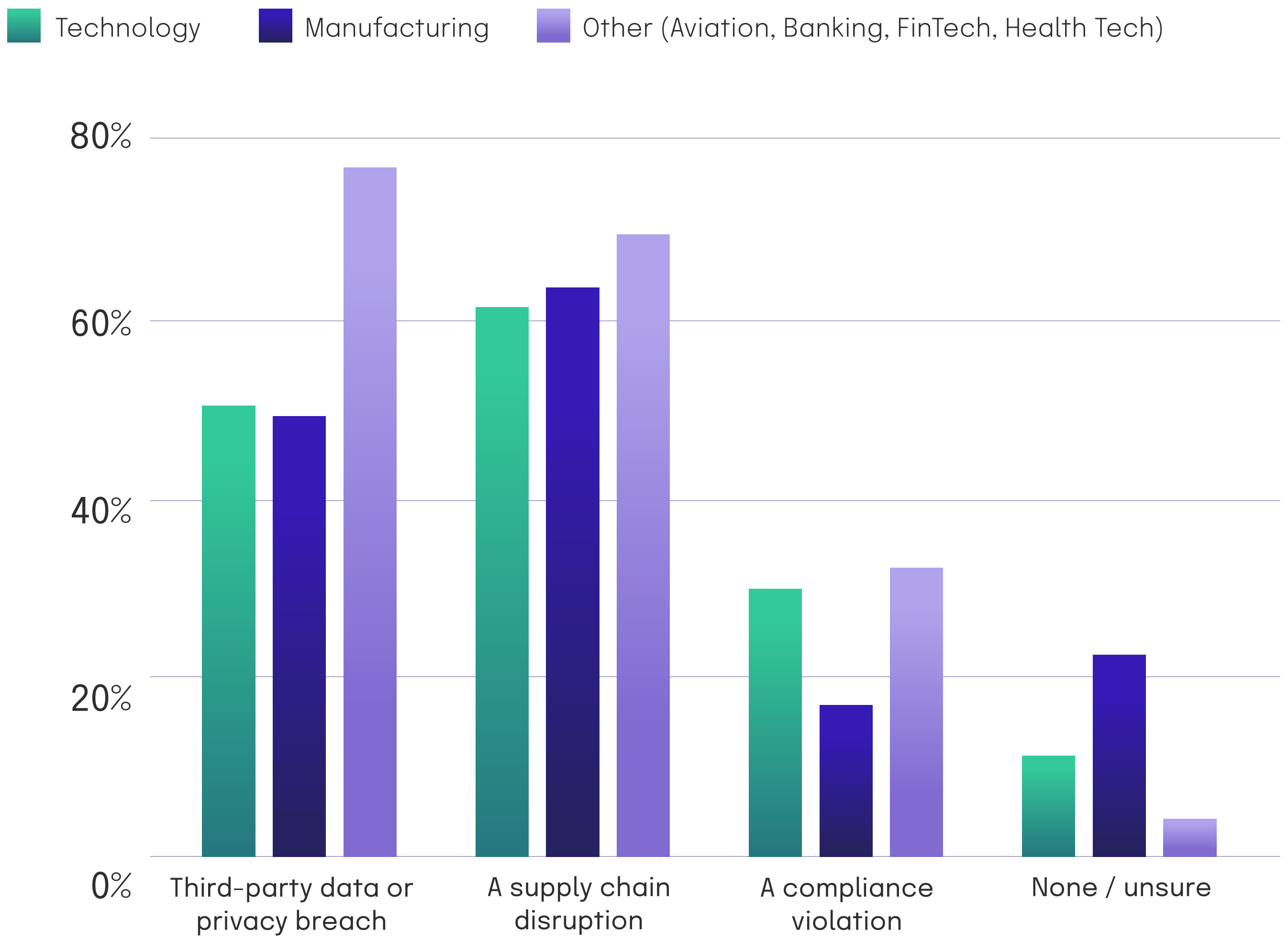

Regional differences in third-party incidents:
United States
United Kingdom
80%
60%
40%
20%
0%
Third-party data or privacy breach
A supply chain disruption
A compliance violation
None / unsure

By industry

Technology companies were far more likely than manufacturers to experience a compliance violation related to their organization's third-party oversight. 29% of technology companies experienced a compliance violation compared to only 18% of respondents in the manufacturing industry.

Has your organization impacted by any of the following events in the past year?

By industry



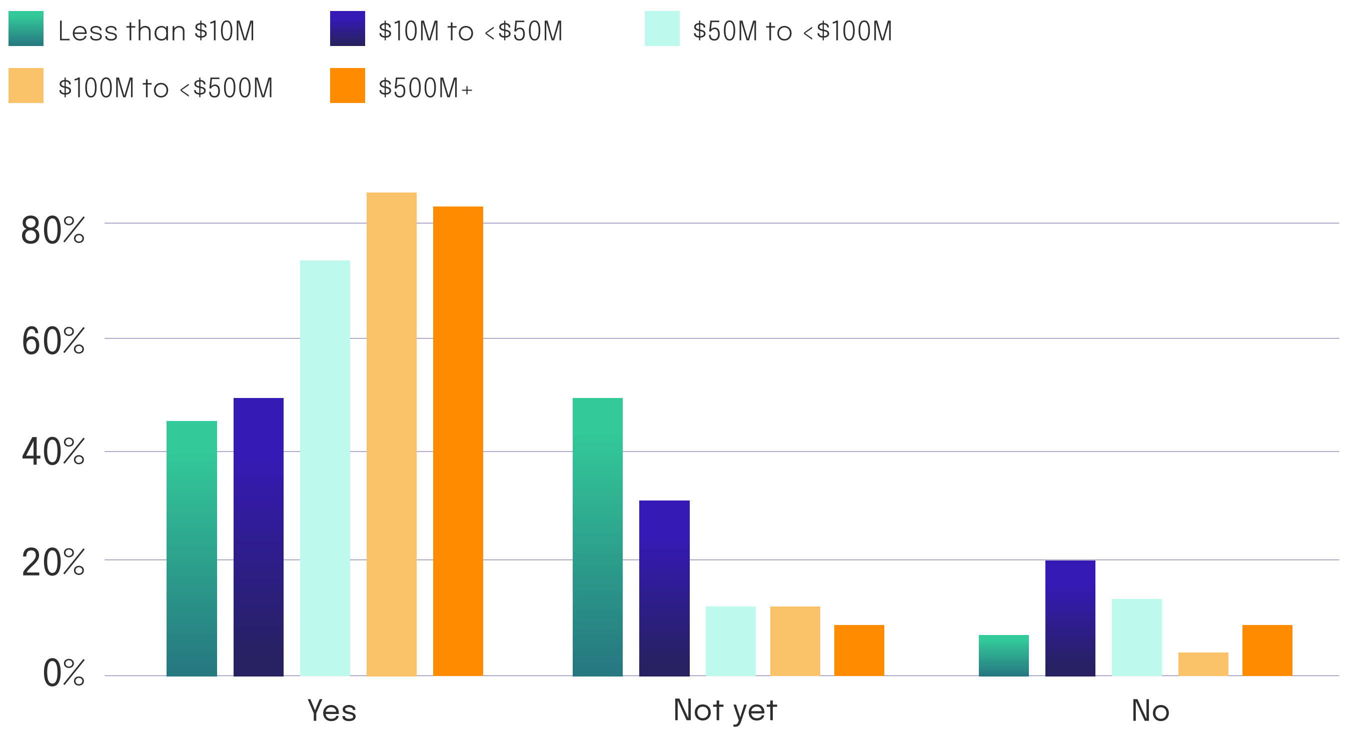
By revenue

Respondents with revenue of over $100M were more likely to experience a third-party data or privacy breach than those with revenue under $100M. 65% of those with revenue of $100M to less than $500M experienced a breach, while 61% of respondents with revenue of $500M+ experienced a breach.

At the other end of the revenue bands, respondents with revenue of less than $10M were more likely to expect or be unsurprised by an audit finding than all other segments at 49%. Respondents with revenue of $10M to less than $50M were more likely to have an audit finding than all segments above $50M at 32%.

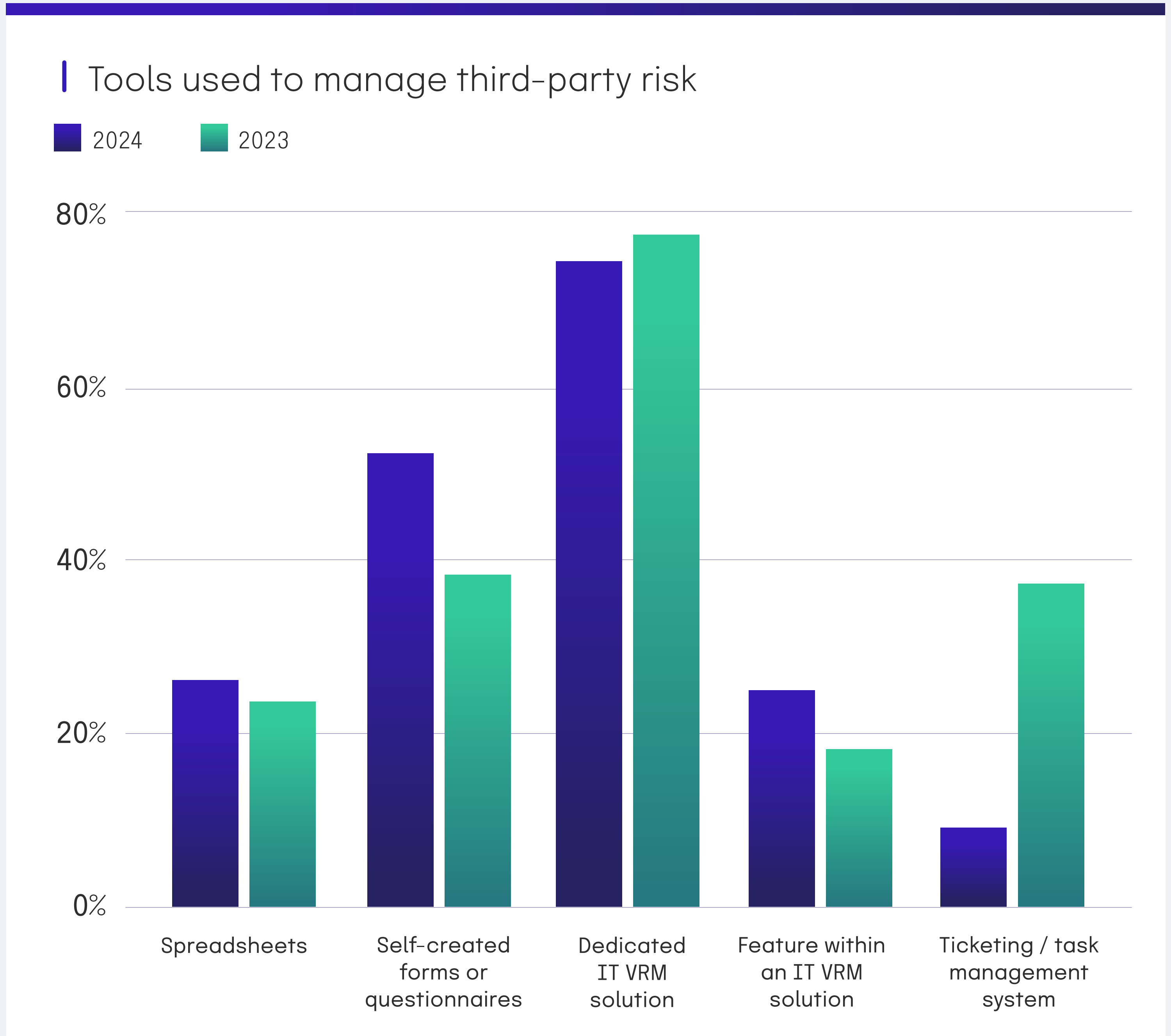
Have you ever experienced (or are you expecting) an audit finding that you cannot promptly resolve related to third-party

By company revenue



Tools used to manage third-party risk

There are many disparate tools used by teams to manage third-party risk. This lack of integration and connection between tools helps make third-party risk more difficult to manage for many industry professionals.



KEY STAT

74%

use a dedicated IT VRM solution

Due to budget consolidations and increased calls for efficiency, **respondents are less happy using discrepant point solutions: they want a platform that includes vendor risk management but also connects to all of their other GRC work.** 74% of respondents – the majority – are using dedicated IT VRM solutions, falling just 4% year-over-year. Meanwhile, 25% are using other features within a GRC solution, up 24% from last year. The numbers show that the industry is slowly shifting toward integrated solutions and away from tools like ticketing and task management systems, which were down 63% this year.

Spreadsheets saw a slight increase in use, up 13% in the last year, but remained low. Other features within a GRC solution were the least used tools at 25%. We also saw an increase in the usage of forms/questionnaires made in Microsoft Office and Google Suite tools to manage third-party risk, jumping up from 39% to 52% of respondents year-over-year.

As demonstrated in this chapter, third-party risk management proves to be a difficult hurdle for companies. Despite being an essential part of business, third-party risk poses some of the largest regulatory and legal threats to organizations. What can be done with the limited resources given to these teams? We'll explore the themes of time and budget in chapter five, where we delve into the data surrounding spending in IT risk and compliance departments.

CHAPTER 5

The Time and Budget Chronicles

CHAPTER 5

The Time and Budget Chronicles

> Optimism for sufficient resourcing is disconnected from economic drivers.

Last year, respondents expected headcount to increase, budgets to go up, and an increase in cross-functional resources. However, the volatile macroeconomic climate and pushes for more efficiency in the GRC space changed the changed the landscape of budgeting across departments, and resources declined as the year progressed. Several adjacent benchmark reports, like Deloitte's *2023 Global Future of Cyber Survey Report*, predicted flat or declining cybersecurity budgets for 2024, yet 69% of respondents expect to spend more money on IT risk management in 2024. The potential reality of a decrease in budget could be due to various factors, including shifting organizational priorities and the consolidation of risk and compliance management. Budgets are dictated by CFOs and boards, forcing security and risk teams to have to learn how to communicate more effectively with these stakeholders to advocate for their needs. This is causing IT and risk teams to look for insights from their tech stack that showcase how their work relates to unlocking higher level company objectives.

KEY STAT

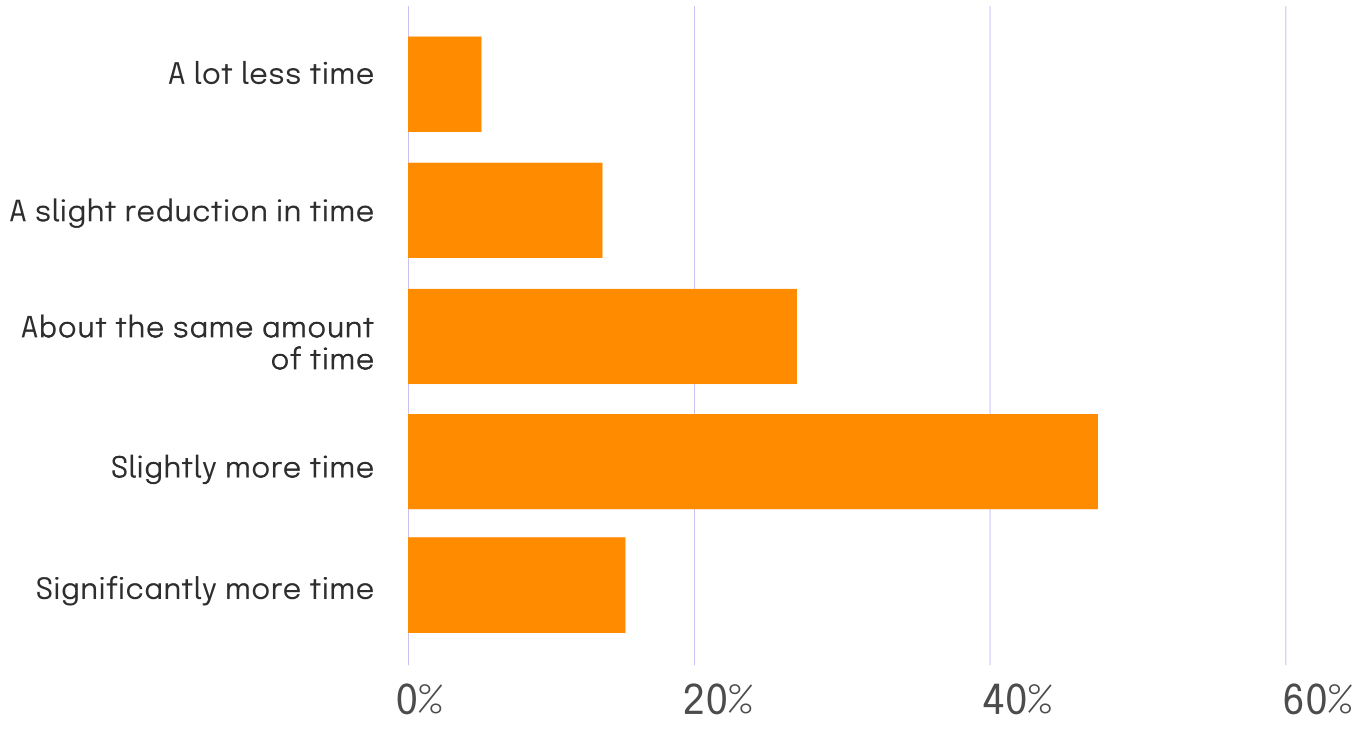
69%

expect to spend more money on IT risk management in 2024

Respondents are anticipating spending more time on IT risk this year

Respondents are gearing up to invest more time in IT risk management and compliance in 2024, with **60% expecting to spend more time** compared to 57% in the previous year. Notably, only 35% of respondents expected to spend more time on IT risk management in 2022, which is a 88% change over the last two years. This trajectory reflects how much more time and focus companies are dedicating to strategic risk and compliance management, especially as regulatory scrutiny increases each year.

Do you anticipate your organization will spend more, less, or about the same **amount of time** on IT risk management and compliance in 2024 vs. 2023?



Companies with higher revenues anticipate spending the most time on IT risk

74% of companies with revenue over $500 million – the vast majority – anticipate spending more time on IT risk in 2024. 52% anticipate spending slightly more time, and 22% anticipate spending significantly more time. This is likely due to the complexity of their operations, as these companies have a broader digital footprint with a larger tech stack.

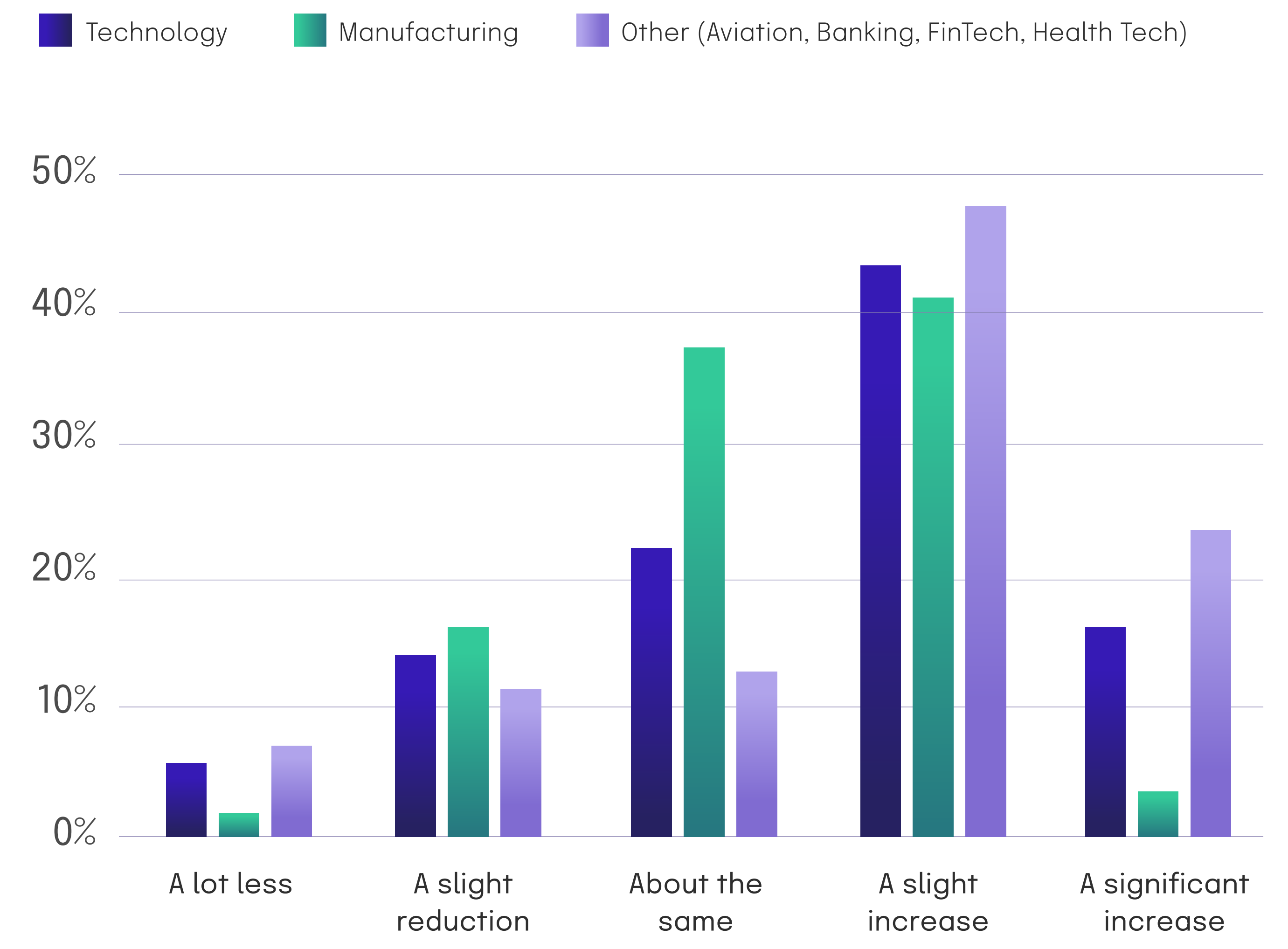
Anticipated time spent in 2024 by revenue

	Revenue				
Anticipated time spent	<$10M	$10M – <$50	$50M – <$100	$100M – <$500	$500+
A lot less	2%	7%	11%	3%	4%
A slight reduction	20%	20%	22%	11%	8%
About the same	21%	36%	24%	25%	14%
A slight increase	44%	30%	33%	46%	52%
A significant increase	13%	6%	10%	15%	22%

Segment differences by industry

Other industries, such as banking, aviation, FinTech, and health tech anticipate spending significantly more time than manufacturing and technology industries on IT risk management in 2024. 23% of respondents in these cohorts anticipate spending significantly more time on IT risk in 2024, which could be due to the emerging risks in their industries.

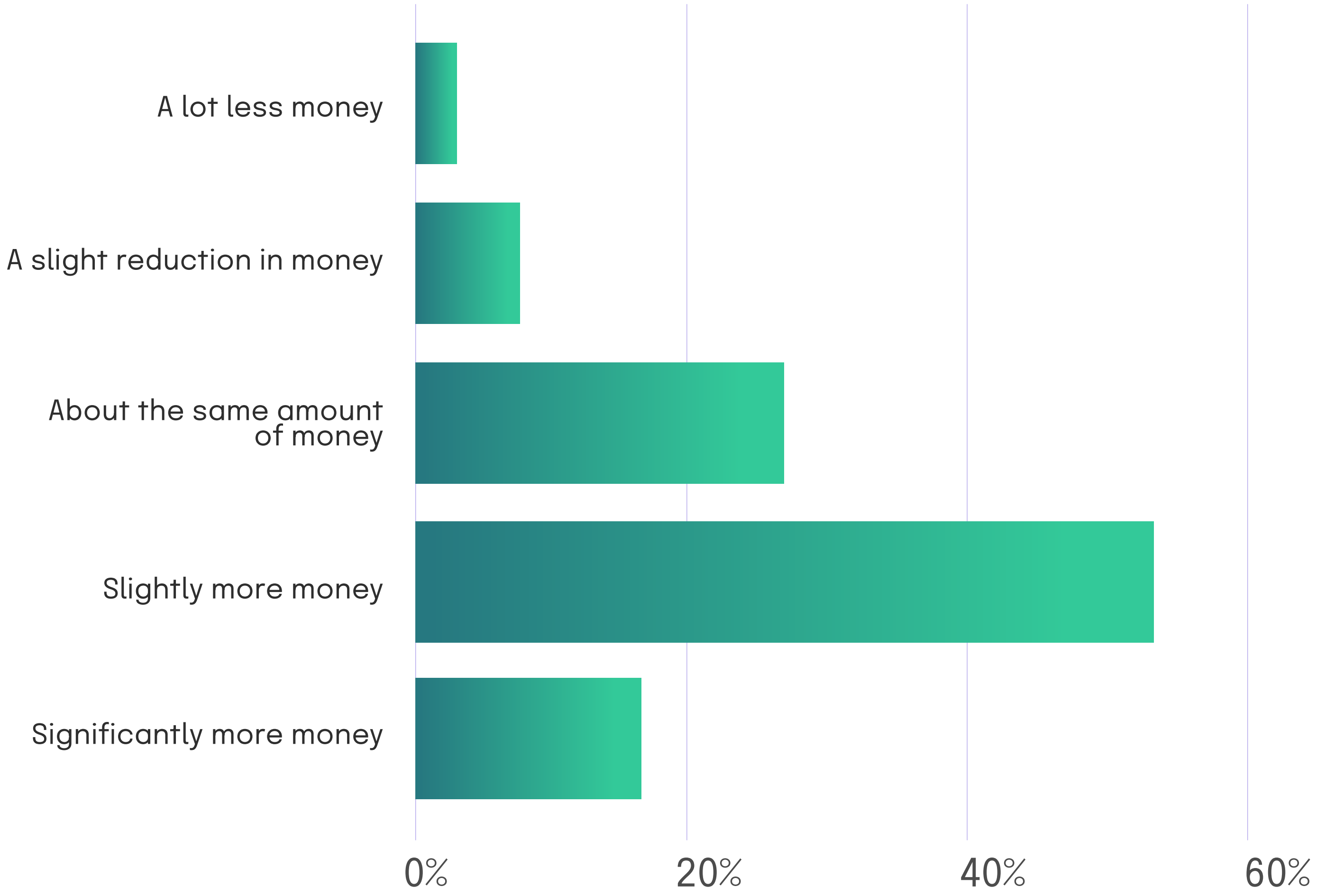
Anticipated time spent on GRC by industry



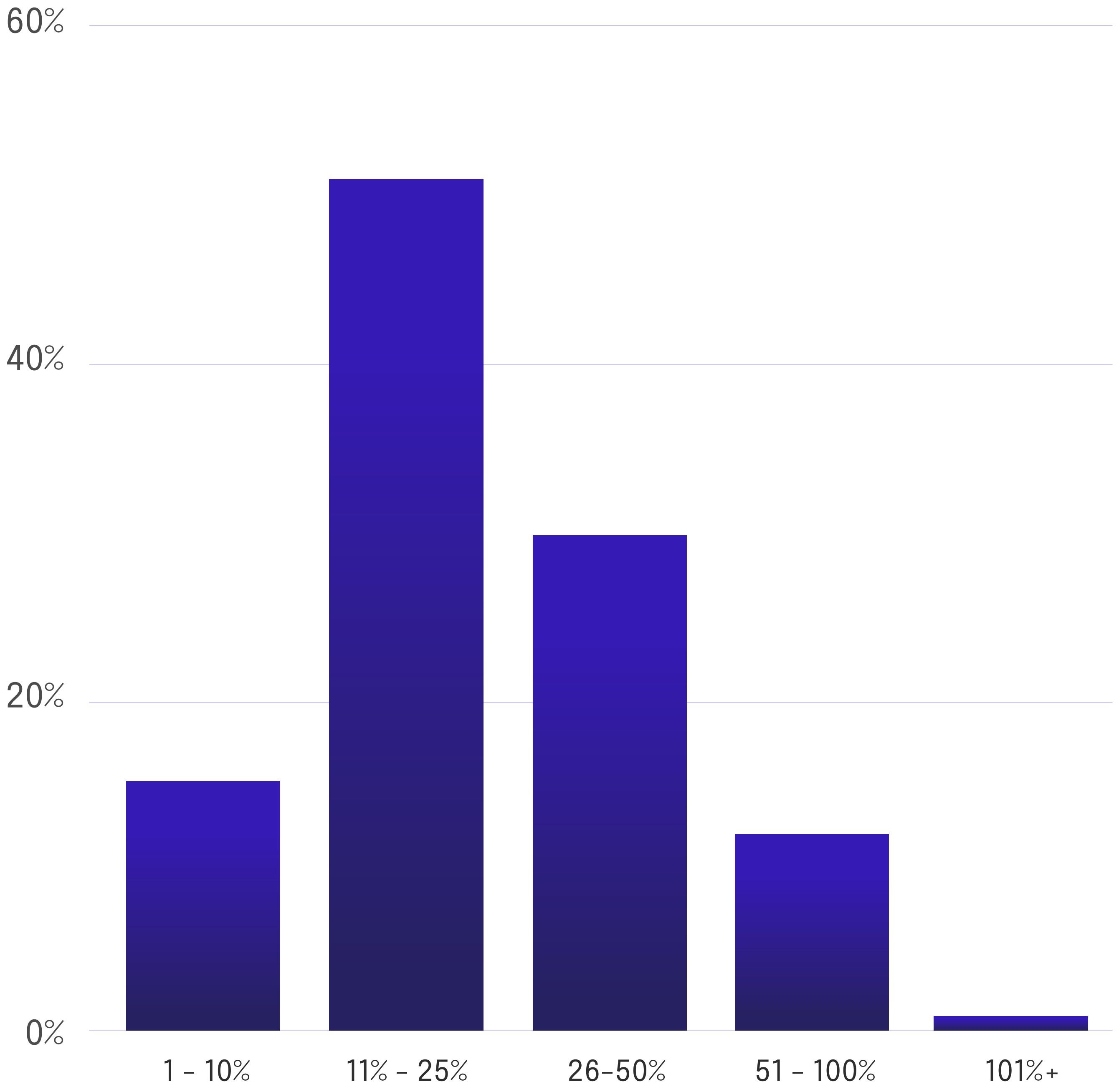
Anticipated budget increases

On average, respondents estimate to increase their budgets by 29% this year, compared to 25% in 2023. Of those increasing budgets, 47% expect to boost spending by 10-25% compared to only 40% in the previous year, signaling a slight increase in resource allocation.

Do you anticipate your organization will spend more, less, or about the same **amount of money** on IT risk management and compliance in 2024 vs. 2023?



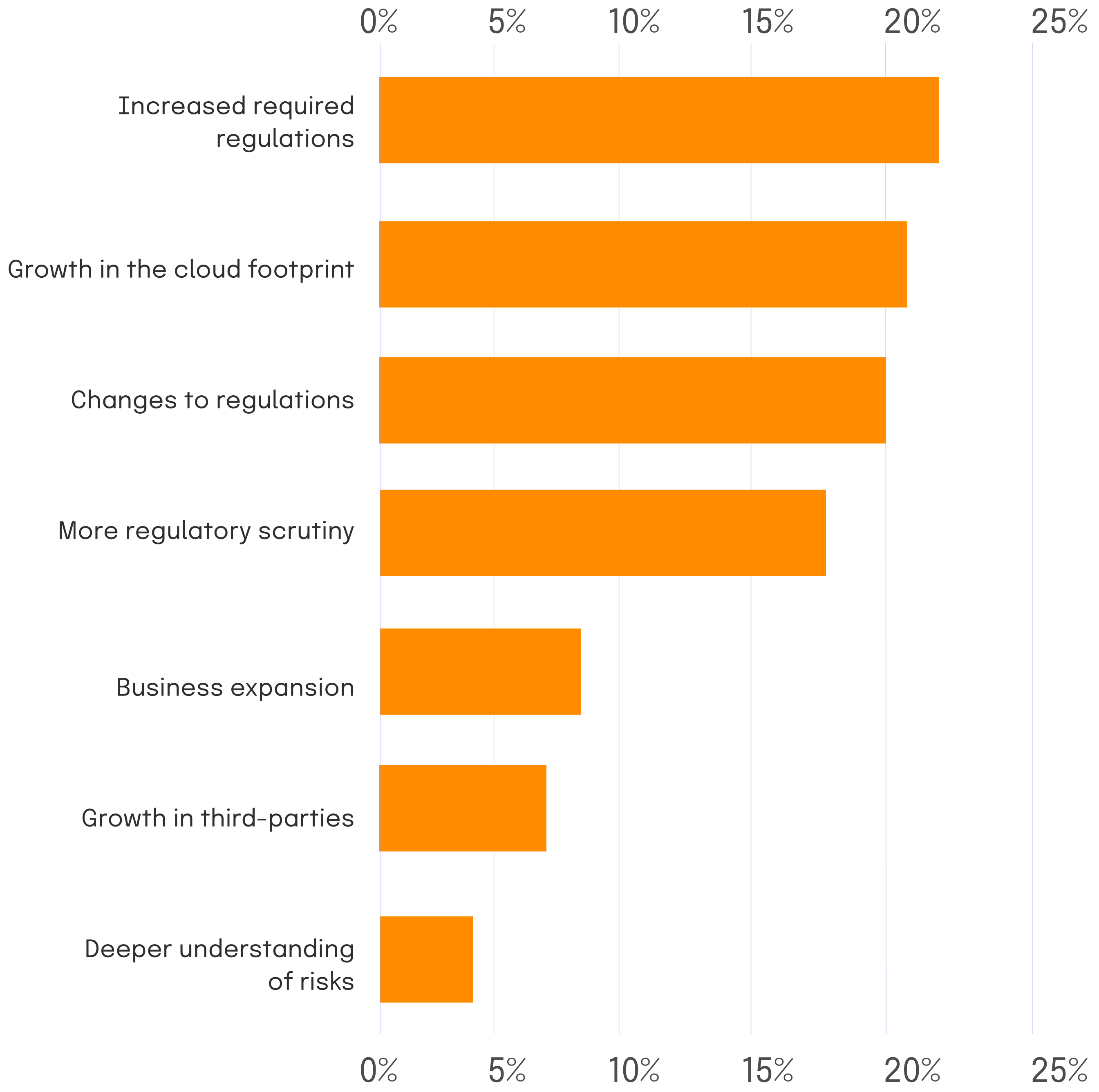
How much do you plan to increase your GRC budget in the next 12-24 months?

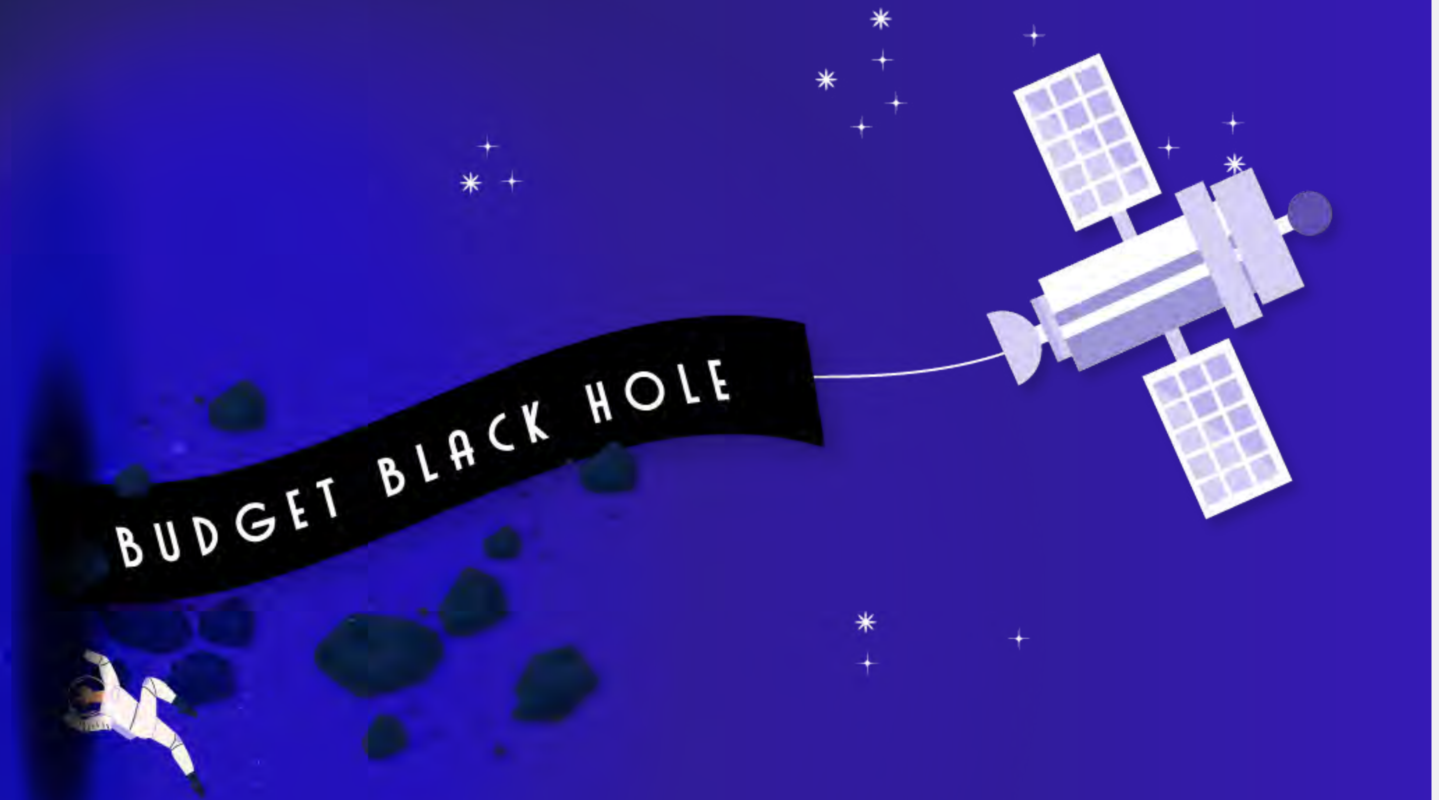


Drivers of increased spending

What's driving this anticipated spend increase? Increased regulatory changes and stricter enforcement are front and center for IT compliance and risk professionals. As governments and different regulatory bodies continue to get more active in defining new rules and regulations, companies are wary of being able to keep up. This is compounded by the fact that most companies are seeing their tech stacks expand year-over-year, predominantly in the cloud, which is expanding their risk footprints. This is leading companies to look for solutions that can help them keep up with regulatory changes while also enabling them to better monitor and manage risks across their organization.

What are the top factors driving IT risk and compliance spend increase?

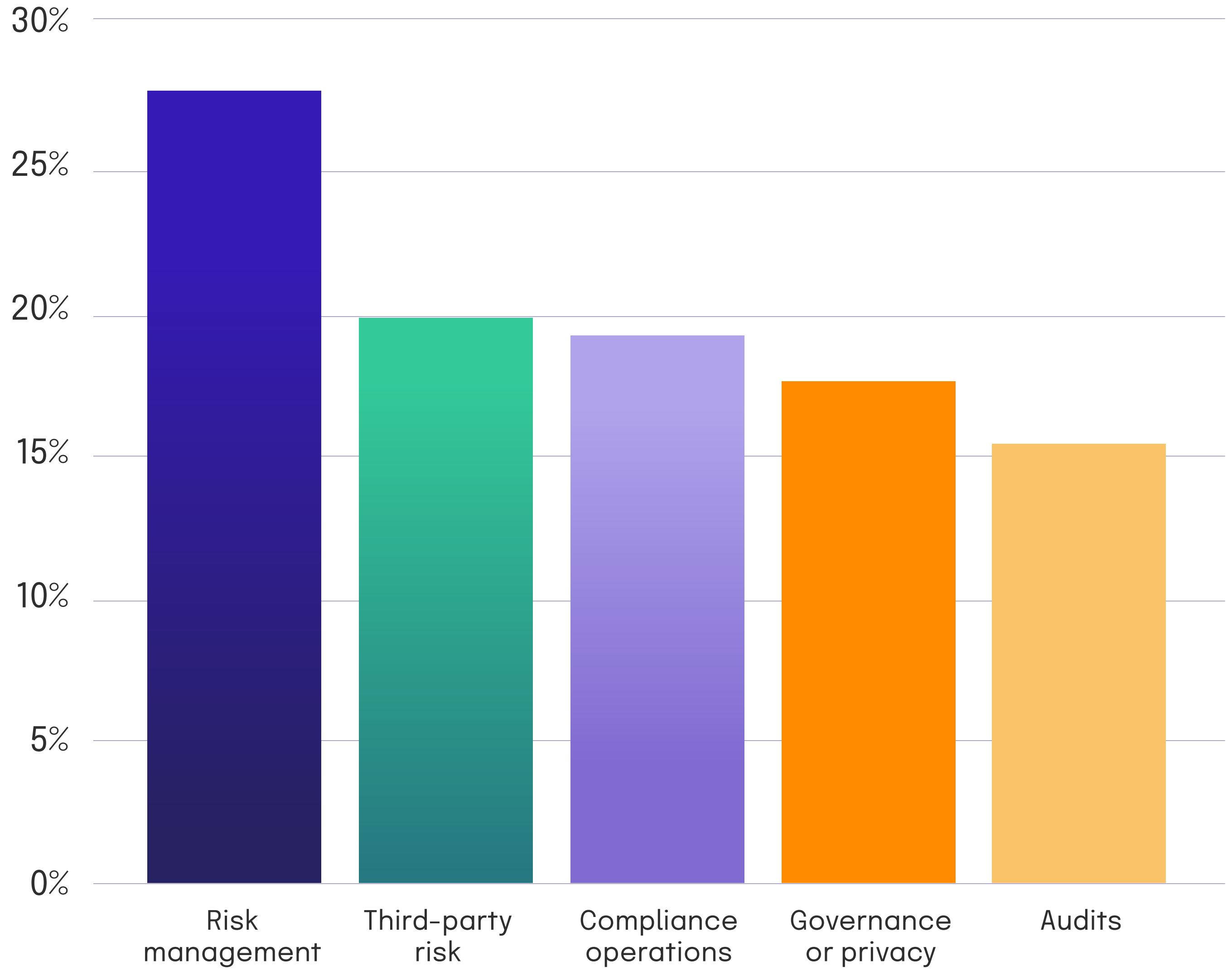




Where budgets are going

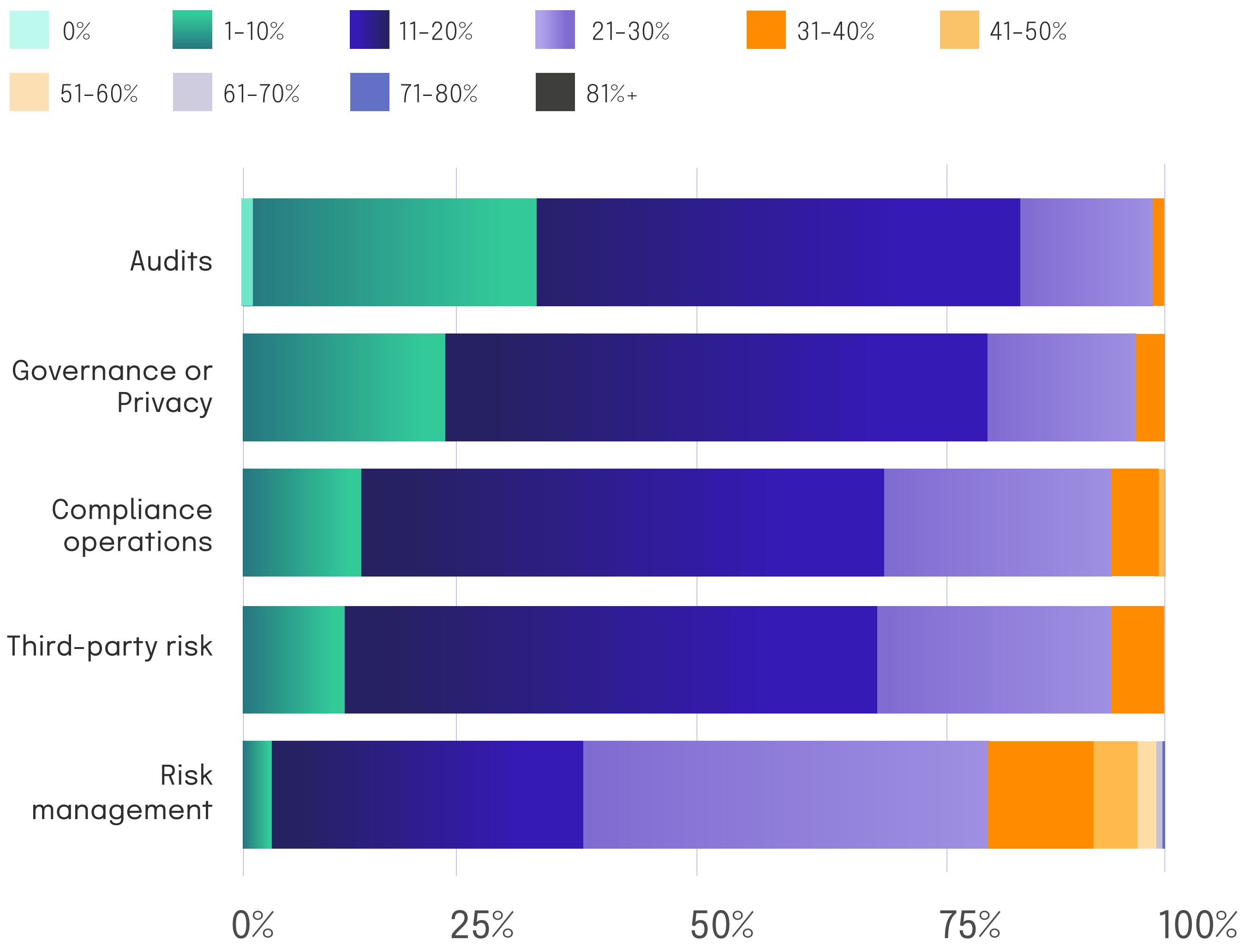
The majority of organizations are allocating funds toward risk management in 2024, further emphasizing the growing importance of managing risks and the need for transparency across organizations to communicate risk to stakeholders.

Average anticipated spend allocation for all respondents:



We asked respondents what percentage of their total spend went to each category. Risk management is consuming the bulk of budgets, and audits are consuming the least. Only 33% of respondents dedicate less than 20% of their budgets toward risk management, compared to 69% allocating less than 20% of their budgets to third-party risk management. 68% of respondents said they spend less than 20% on compliance operations, and 83% of respondents intend to spend less than 20% on audits.

What percentage of your organization's GRC spend is in each of the following categories?



Anticipated spend vs. revenue

Companies with higher revenues expect to spend more overall. 75% of companies with revenue of over $500M expect to spend more money on IT risk in 2024, compared to only 65% of companies with less than $10M in revenue and 59% of companies with $10M-<$50M in revenue. This is likely due to the resources available at these companies and the complexities of their risk management needs across product lines, locations, markets, and technology systems.

Anticipated spend in 2024 by revenue

	Revenue				
Anticipated spend in 2024	<$10M	$10M – <$50	$50M – <$100	$100M – <$500	$500+
A lot less	2%	1%	8%	3%	3%
A slight reduction	11%	5%	12%	3%	6%
About the same	21%	35%	22%	22%	16%
A slight increase	54%	50%	45%	52%	51%
A significant increase	11%	9%	12%	21%	24%

Teams equipped with the resources they need are able to achieve their goals

Several highly publicized breaches in 2023 have made business operations more challenging for both B2B and B2C companies, and proactive businesses are not only maintaining their existing cybersecurity attestations (like SOC 2 and ISO 27001), but expanding the number of external validations to demonstrate their trustworthiness.

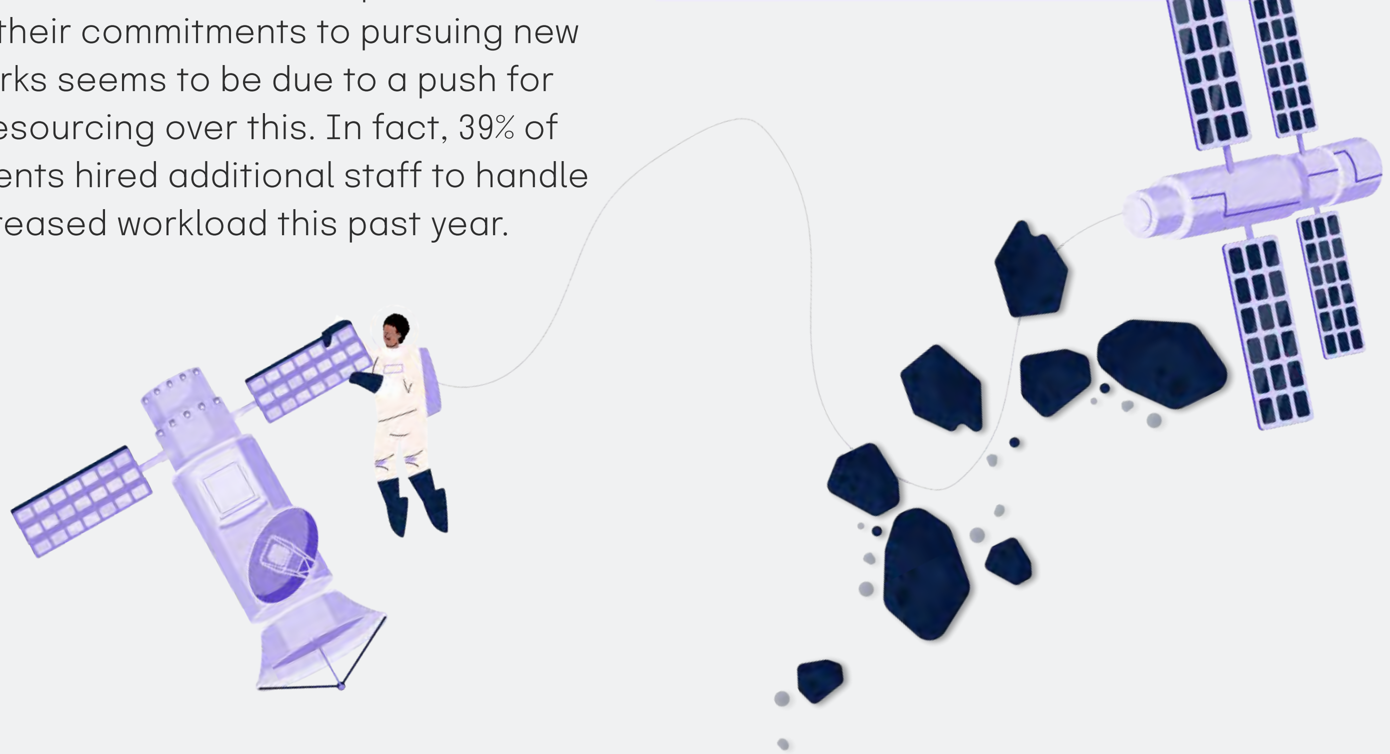
Last year, nearly one-third of respondents said they had to postpone the pursuit of new compliance frameworks or certifications due to insufficient resources. As we covered in chapter three, this year, **only 7% of respondents** said they had to postpone the pursuit of new compliance frameworks or certifications due to insufficient resources, a decrease of 78% year-over-year.

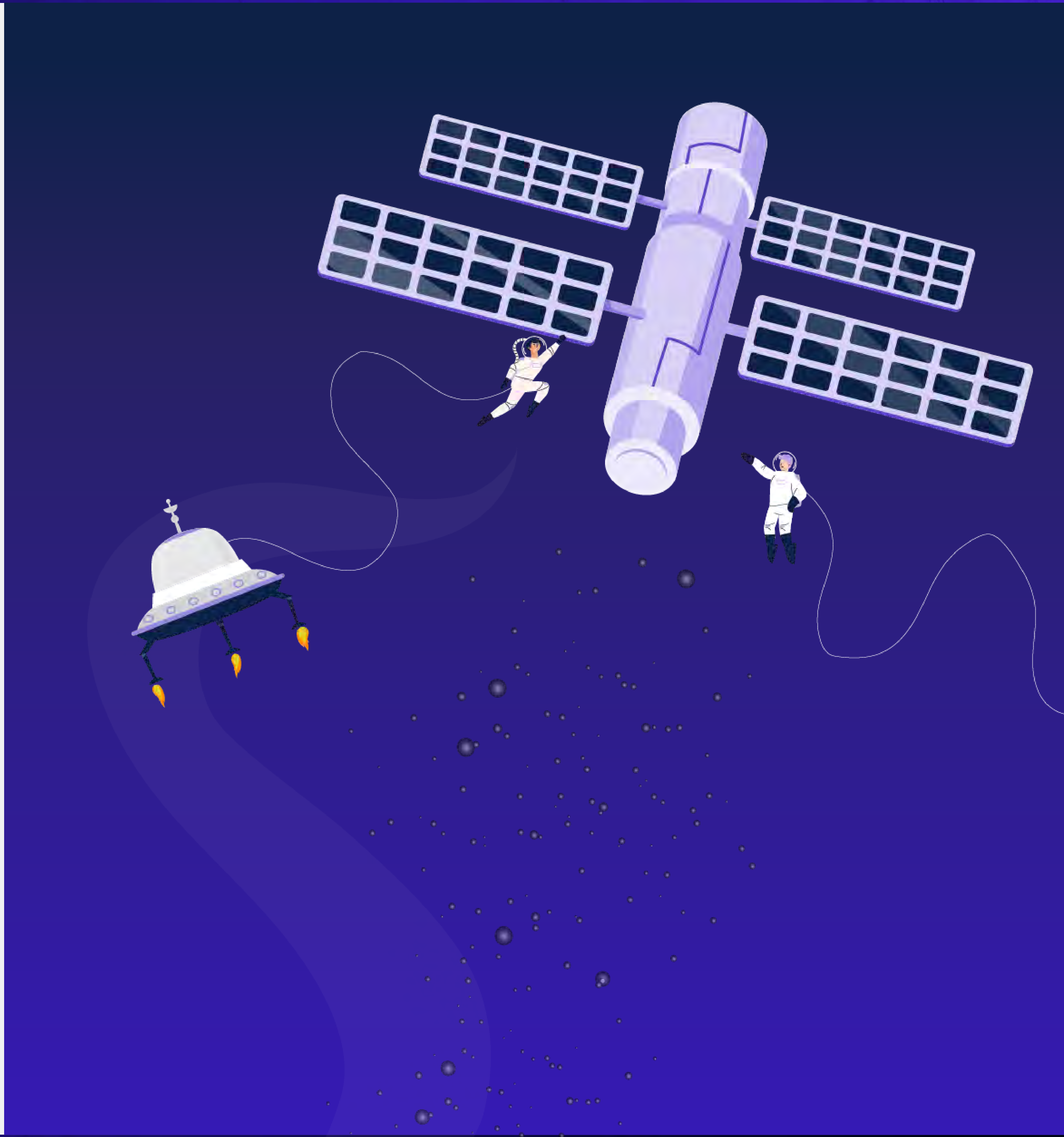
KEY STAT

69%

leveraged a GRC software in the past 12 months to mitigate stress

The shift in the number of companies keeping their commitments to pursuing new frameworks seems to be due to a push for proper resourcing over this. In fact, 39% of respondents hired additional staff to handle their increased workload this past year.





Risk and compliance services outsourced

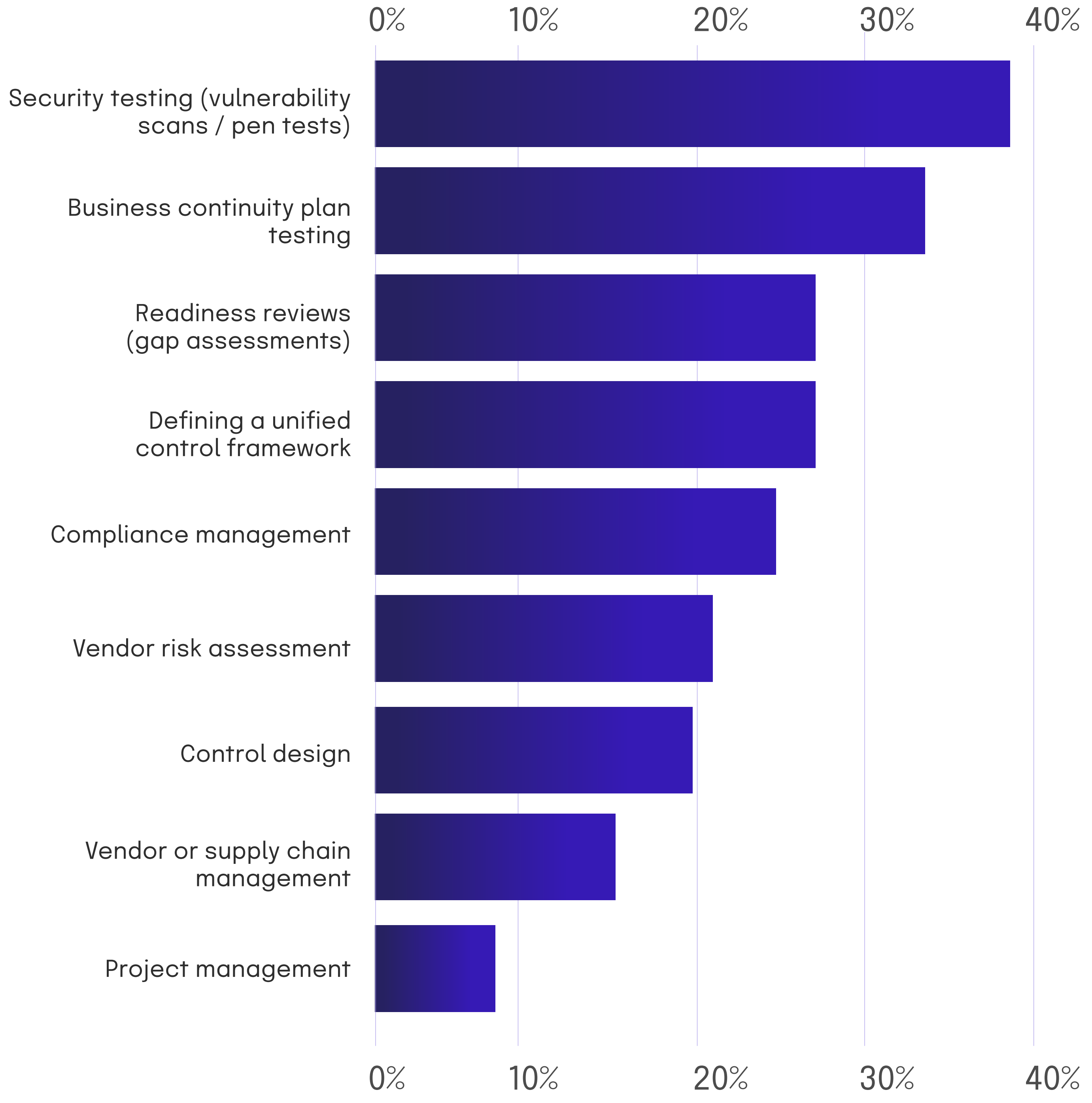
It is difficult for organizations to hire enough staff to fully address all their risk management, security, and compliance program's needs. GRC expertise is relatively scarce and talent is expensive. 10% of all surveyed respondents outsource one or more IT compliance activity to third-party advisory firms, with the leading service being policy generation and the second being IT security and asset management. Notably, these are both documentation burdens that companies are using AI to streamline, as we explored in chapter two. It's possible that companies will leverage AI tools for these processes in lieu of outsourcing them to increase efficiency in 2024 – yet another change to the GRC landscape.

KEY STAT

10%

outsource one or more compliance activities to third-party advisory firms

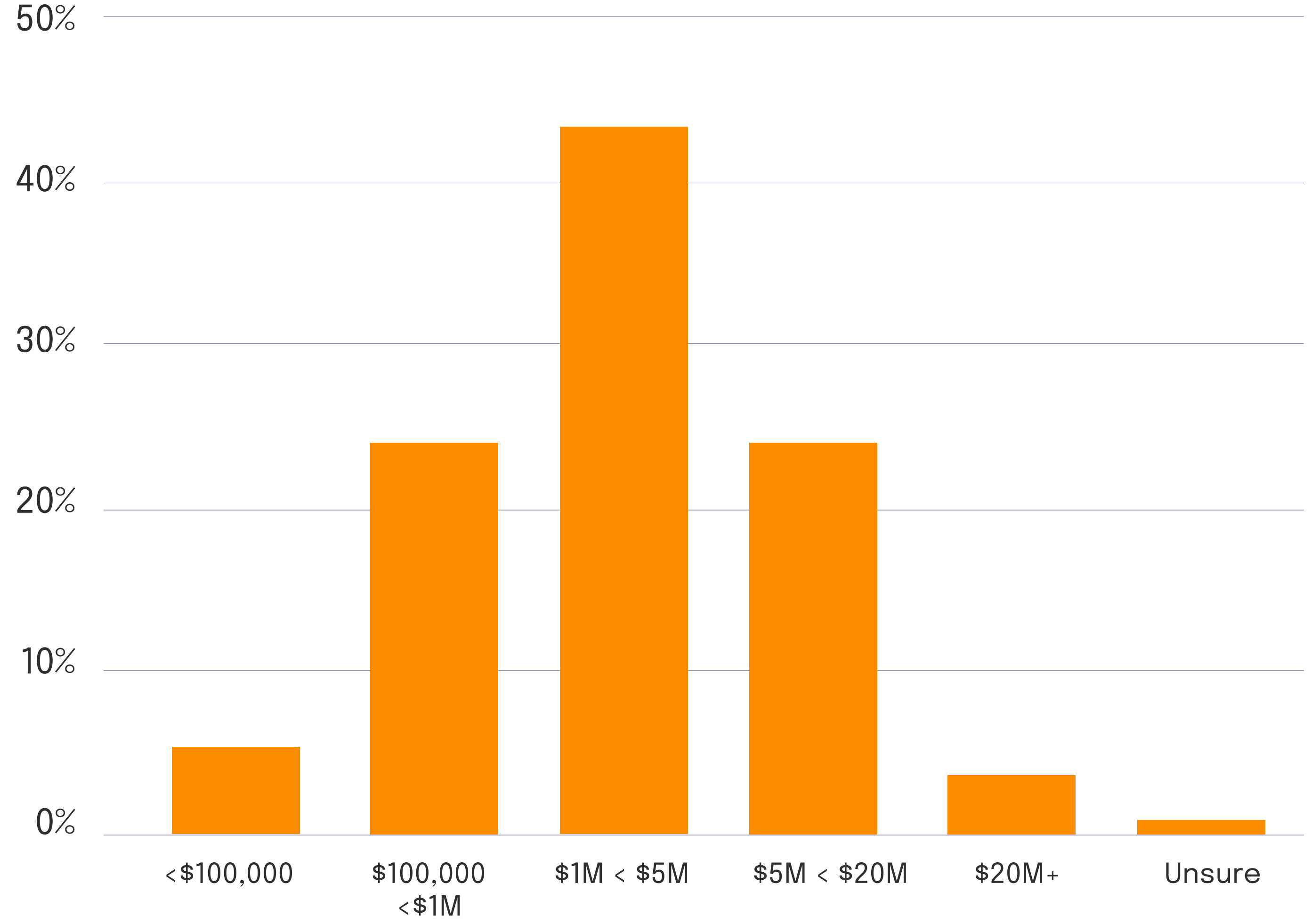
Select all the services that you outsource to consulting or security and compliance advisory firms:



Financial impact of data breaches

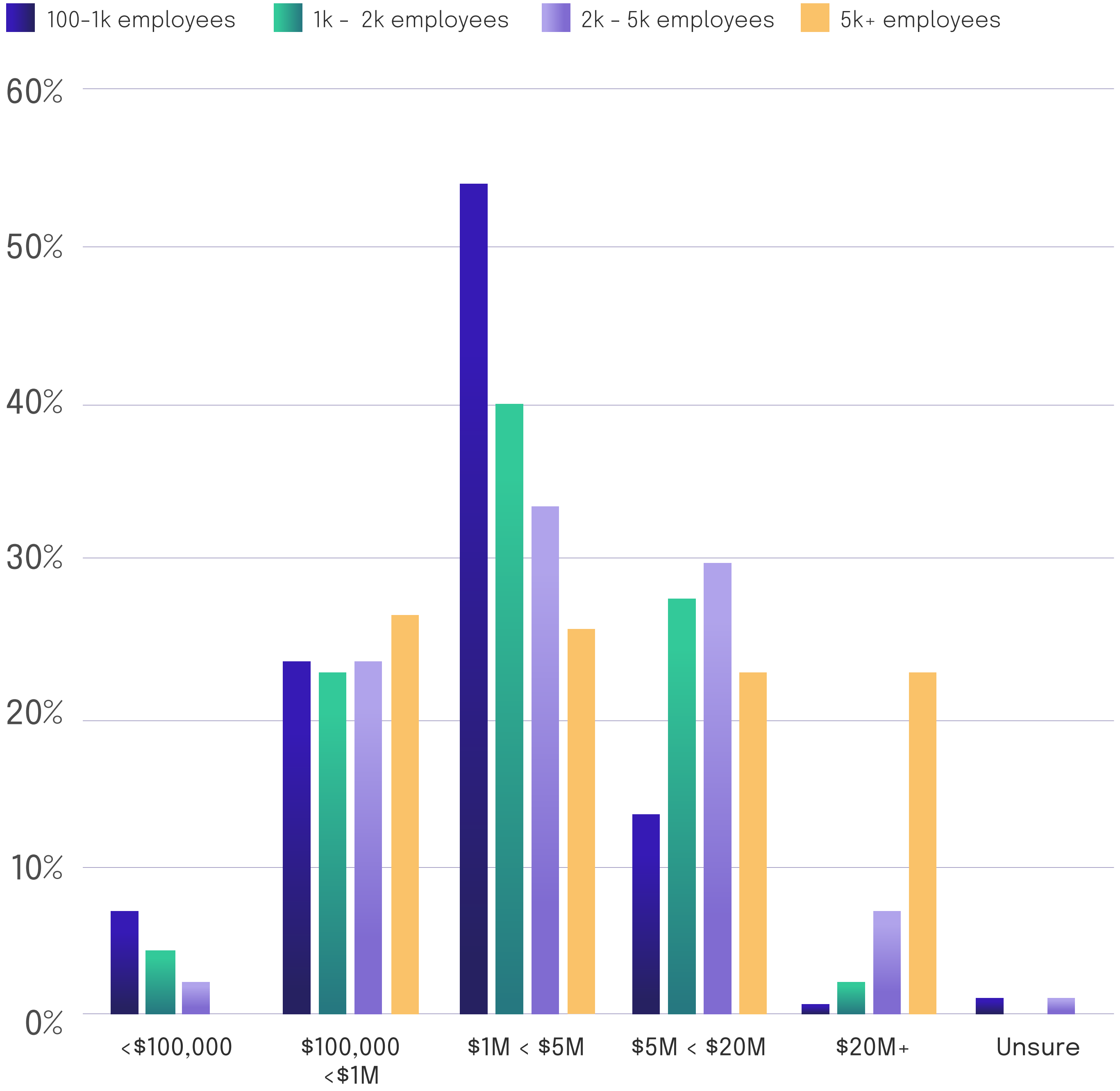
The impact of data breaches remains a significant concern for businesses. As we covered in chapter three, 59% of those surveyed experienced a data breach within the last 24 months. **43% of those organizations reported losing between $1M to less than $5M** via a data breach, an increase of 10% compared to last year. Notably, for the last three years, respondents reported losing $1M to less than $5M more than any other amount.

How much did your organization incur as a result of a data breach?



How much did your organization incur as a result of a data breach?

By organization size



CHAPTER 6

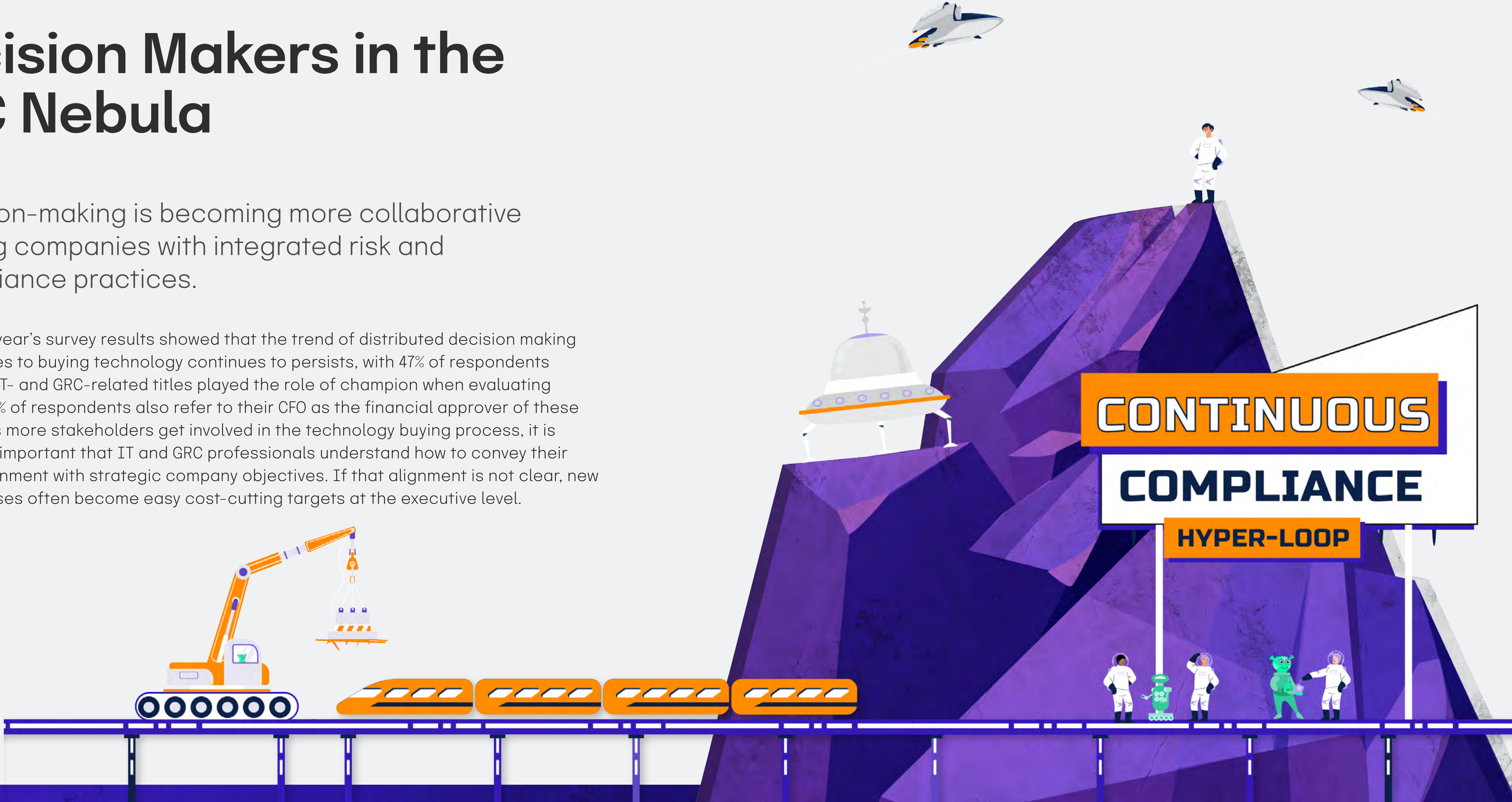
Decision Makers in the GRC Nebula

CHAPTER 6

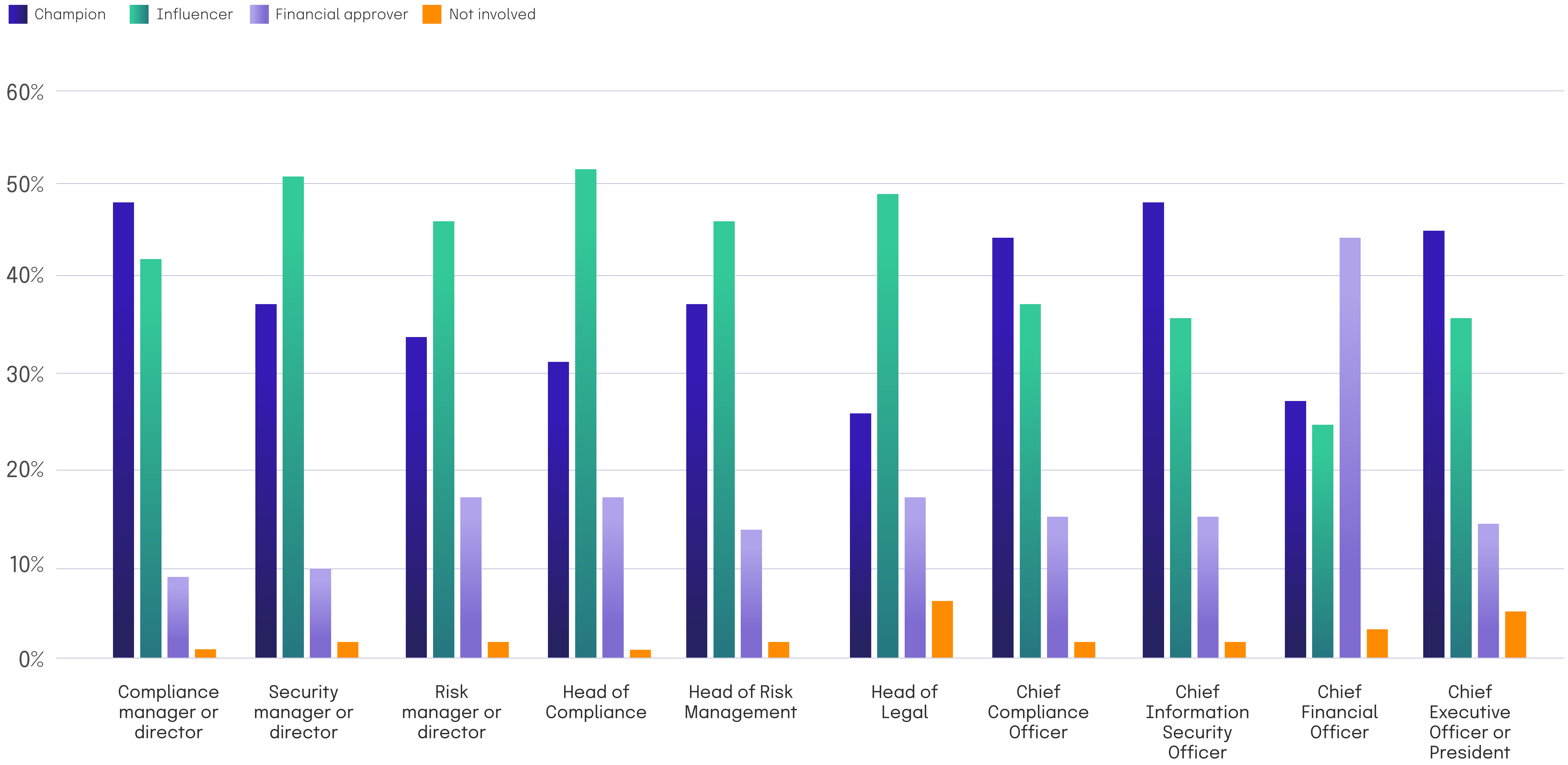
Decision Makers in the GRC Nebula

> Decision-making is becoming more collaborative among companies with integrated risk and compliance practices.

Overall, this year's survey results showed that the trend of distributed decision making when it comes to buying technology continues to persists, with 47% of respondents saying that IT- and GRC-related titles played the role of champion when evaluating new tech. 45% of respondents also refer to their CFO as the financial approver of these decisions. As more stakeholders get involved in the technology buying process, it is increasingly important that IT and GRC professionals understand how to convey their needs in alignment with strategic company objectives. If that alignment is not clear, new tech purchases often become easy cost-cutting targets at the executive level.

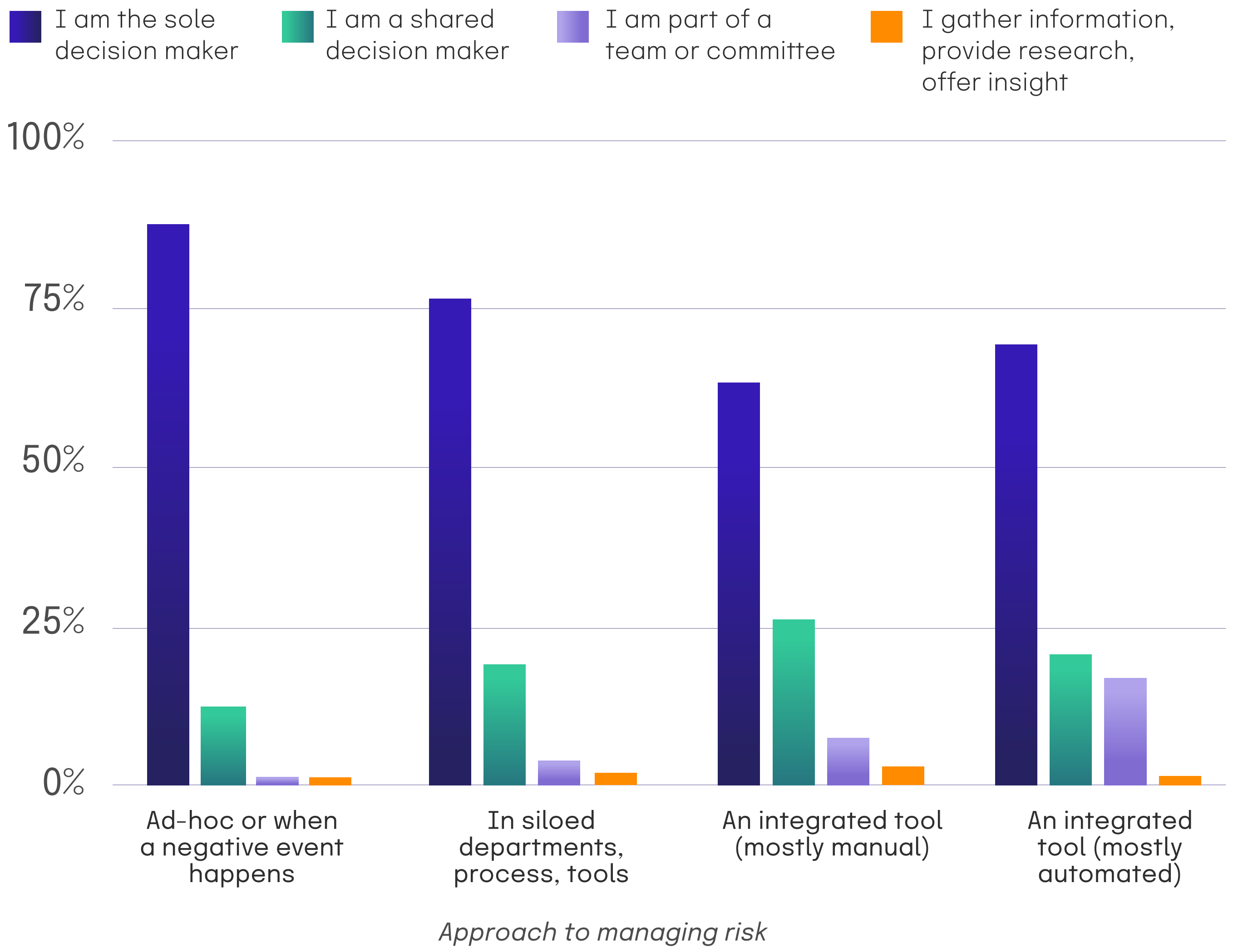


Who are the decision-makers involved when buying compliance or risk technology?



Diving deeper, we can see that whether or not companies have integrated their risk and compliance efforts impacts their decision making strategies. Those in the cohort who manage risk ad-hoc or when a negative event happens and who manage risk in siloed departments or tools are more likely to be the sole decision makers for cybersecurity and risk management decisions. Those who leverage integrated tools are more collaborative with their decision making.

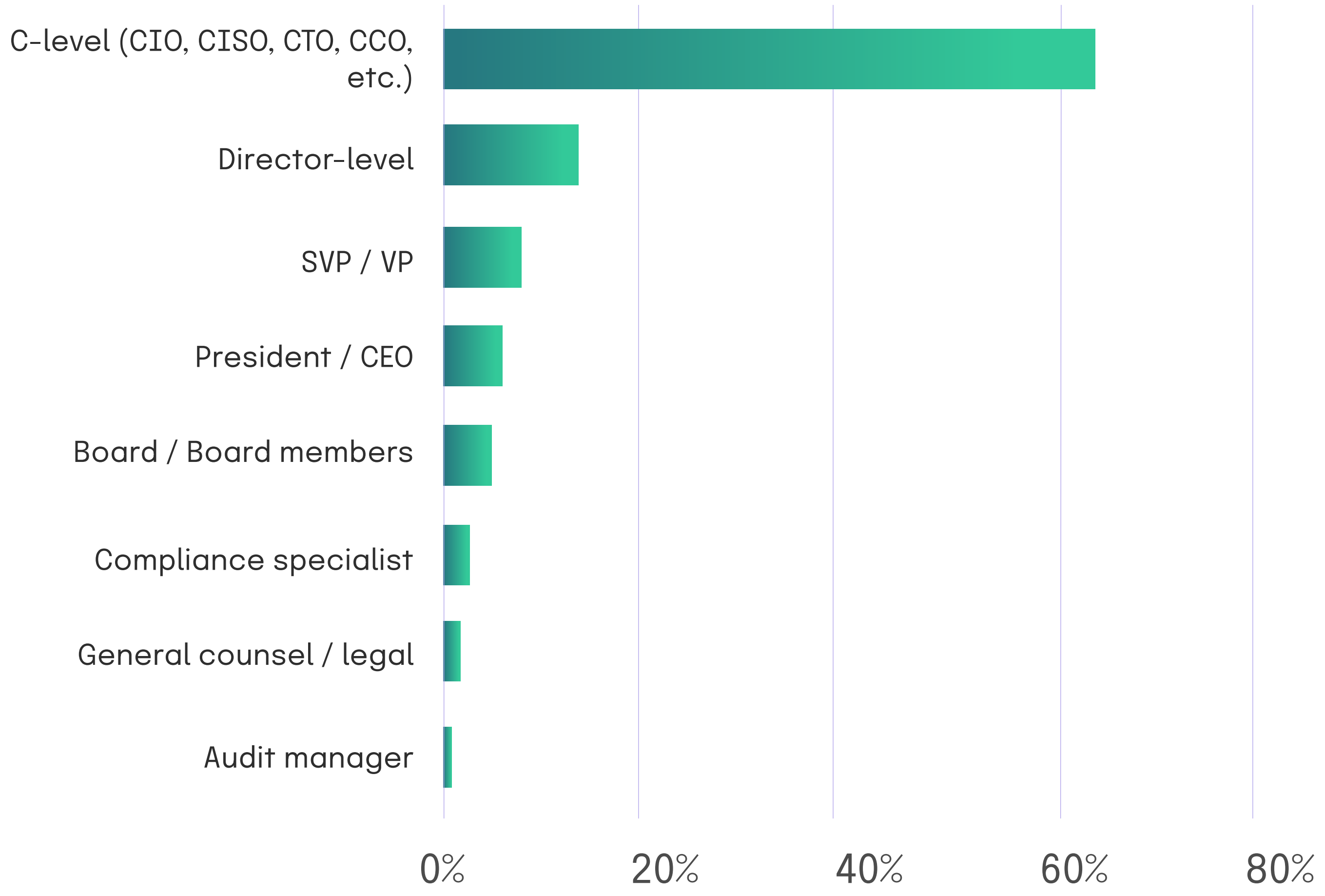
Which best describes your involvement in decisions regarding cybersecurity and risk management for your organization?



Who oversees compliance?

Overall, those in charge of security, IT risk, and compliance decisions have high standing within their organization as well as significant formal authority. Compared to a year ago, the head of the compliance function is now more likely to report to a C-level executive vs. a lower level position (e.g., director) in their organization. Last year, 53% of respondents reported C-level executives as the highest level position overseeing compliance, **and that number has risen to 63% this year**. This is a sign that more organizations have become aware of the strategic importance of an effective compliance program over time.

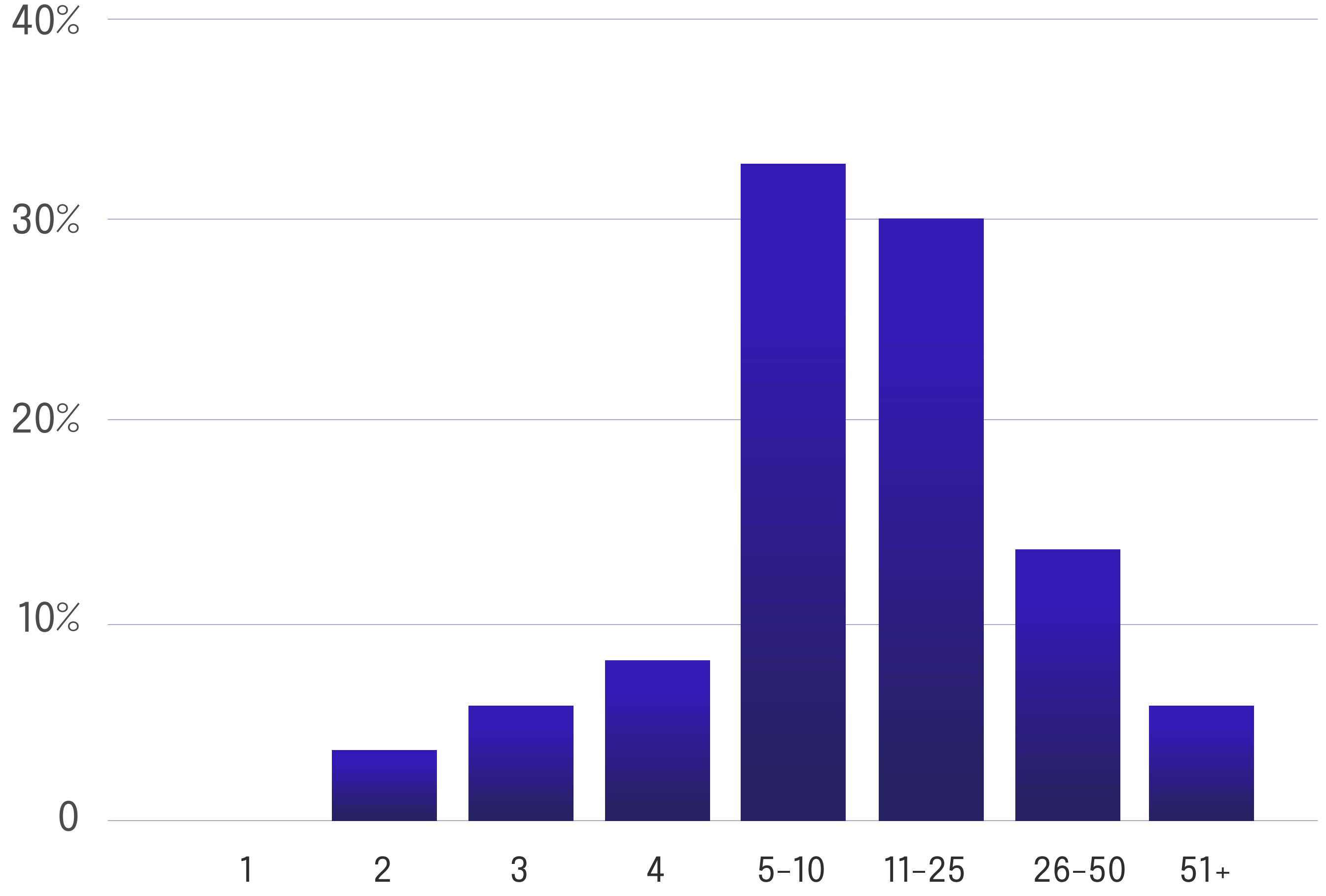
What is the highest level overseeing compliance?



Compliance team sizes have grown year-over-year

Year over year, staff sizes have grown. **The majority of organizations surveyed (83%) have five or more full-time employees dedicated to compliance**. This is a significant increase from last year's data, where 73% of respondents reported having five or more full-time employees dedicated to the compliance function.

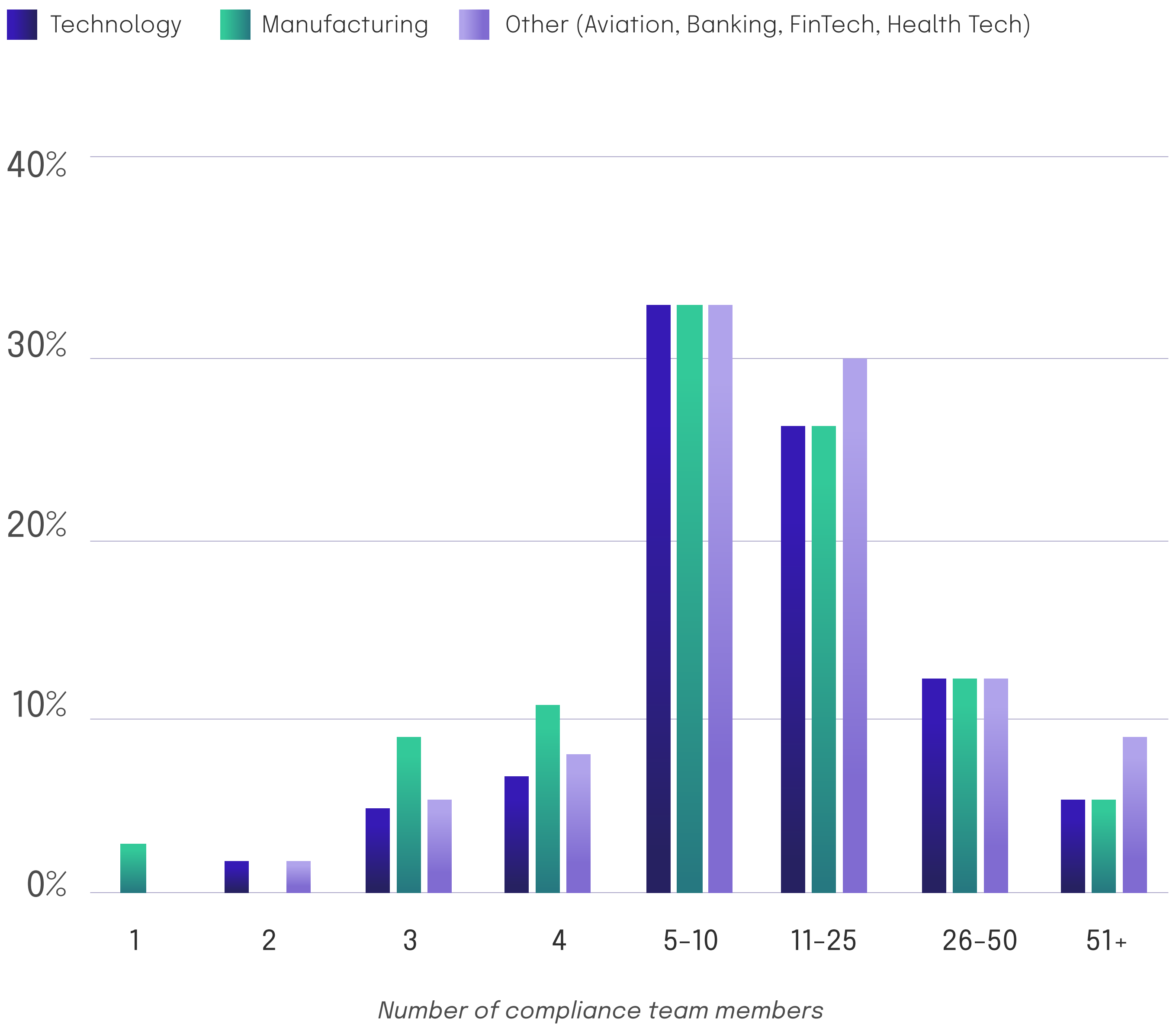
How many full time staff are dedicated to infosec / cybersecurity function at your organization?



Team sizes by industry

Team sizes across industries are almost identical, indicating that compliance teams function similarly across various verticals.

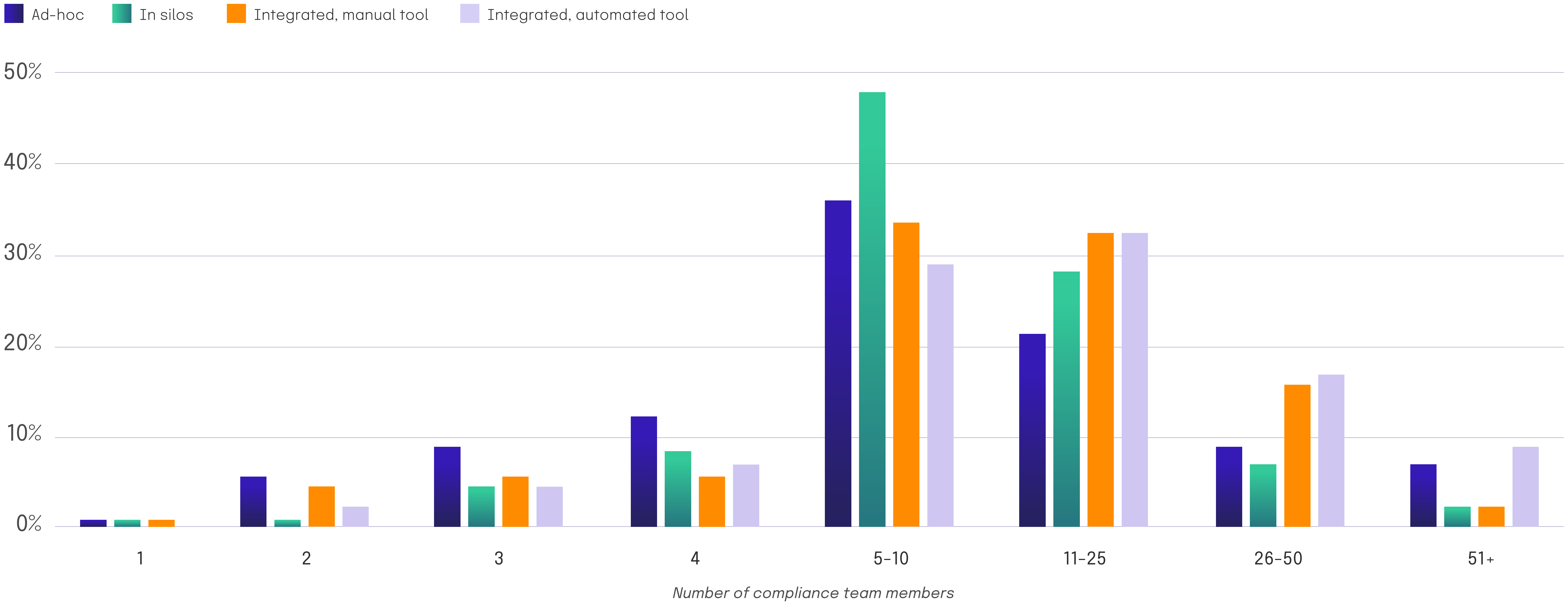
Compliance team size vs. industry surveyed



Team sizes and approaches to managing risk

Those managing risk and compliance in silos were more likely to have a team size between 5-10 people, while those taking an integrated approach with a manual or automated tool tended to have larger team sizes of 10-25 people.

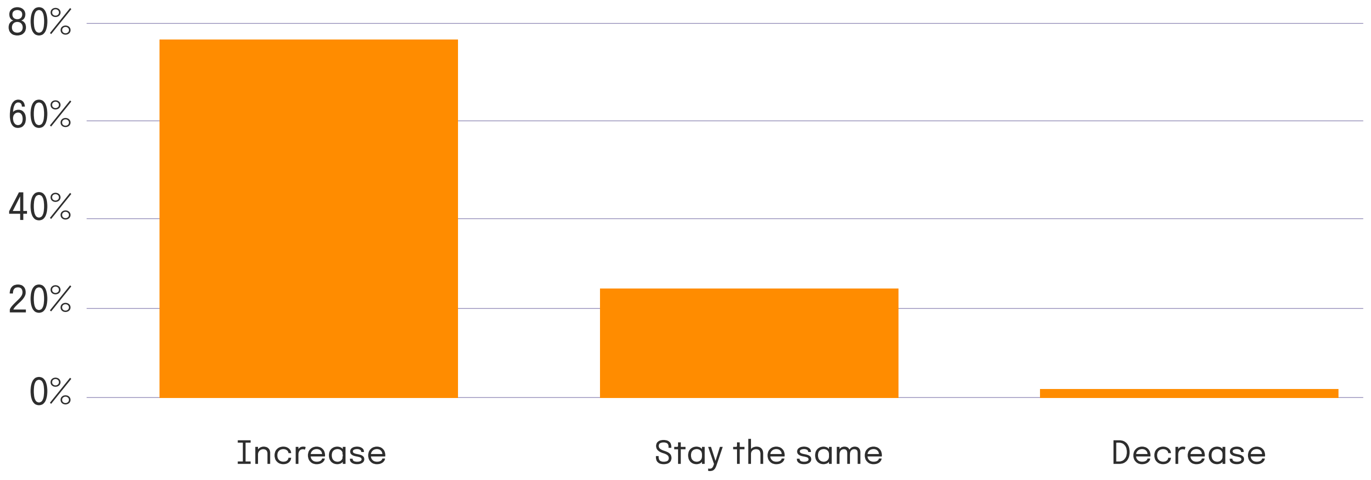
Compliance team size vs. approach to risk management



What's next for compliance team growth

The majority of respondents expect their teams to grow in size in the next two years. Last year, **70% of respondents anticipated an increase in their compliance teams, while this year, that figure has grown to an even more pronounced 77%**. This significant increase reflects a heightened recognition of the importance of information security and data privacy within organizations, prompting them to invest in expanding their compliance teams. Conversely, the proportion of respondents expecting no change in personnel remained relatively stable, with 30% last year and 23% this year. Notably, there were almost no respondents expecting a decrease in personnel in either year, indicating a strong commitment to bolstering compliance efforts in the face of evolving cybersecurity and data privacy challenges. **Macroeconomic outlooks differ from these results; GRC professionals are receiving pressure from key stakeholders to increase efficiency without adding headcount, which is counter to the optimism our respondents have about their team growth in the coming years.**

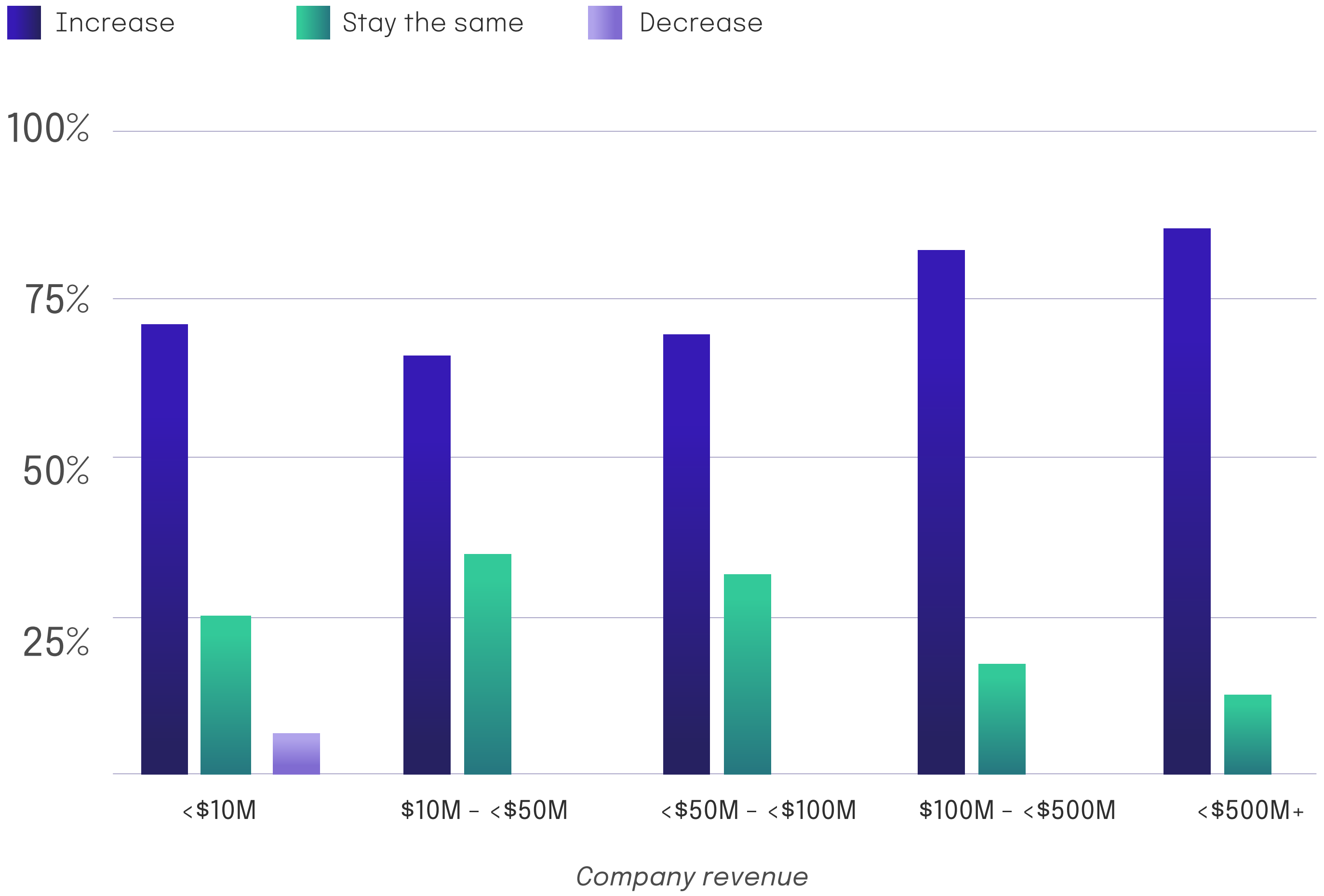
In the next two years, which best describes the growth of your company's compliance team focusing on information security / data privacy in terms of personnel?



Growth by revenue

The only segment anticipating a decrease in team size is companies with revenue under $10M. This could be due to the fact that companies at this revenue stage typically prioritize automation over strategic risk management and are relying on solutions that lean toward checkbox compliance. Companies with revenues of over $500M are anticipating the most growth in 2024 – these companies, with their risk management complex needs, typically invest in GRC solutions and resources that enable them to strategically and proactively address risk.

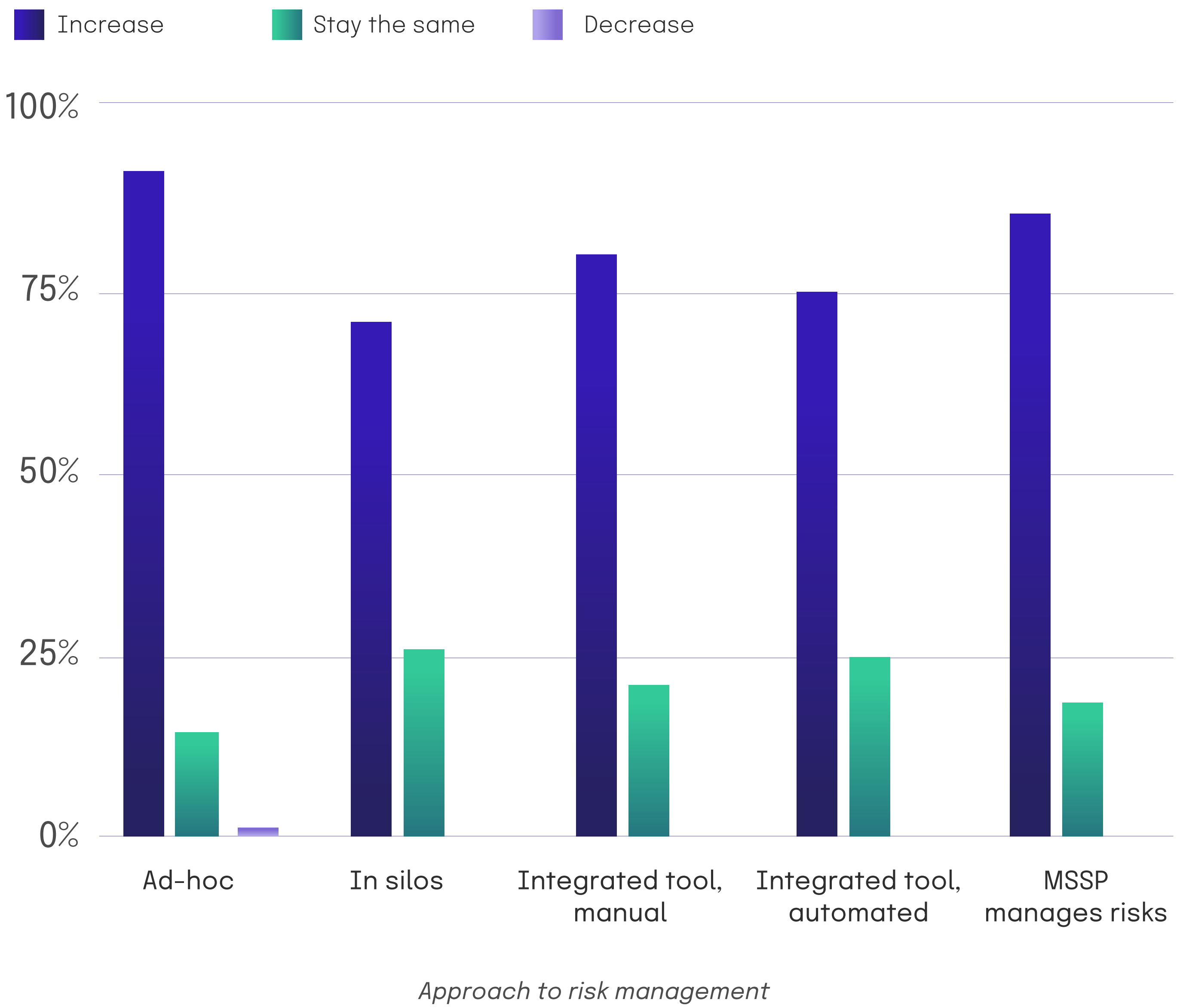
Expected team growth vs. revenue



Growth by approach to risk management

Respondents managing risk ad-hoc are the most likely to grow their teams in 2024, likely due to a need to manage their growing manual processes.

Expected team growth vs. approach to risk management

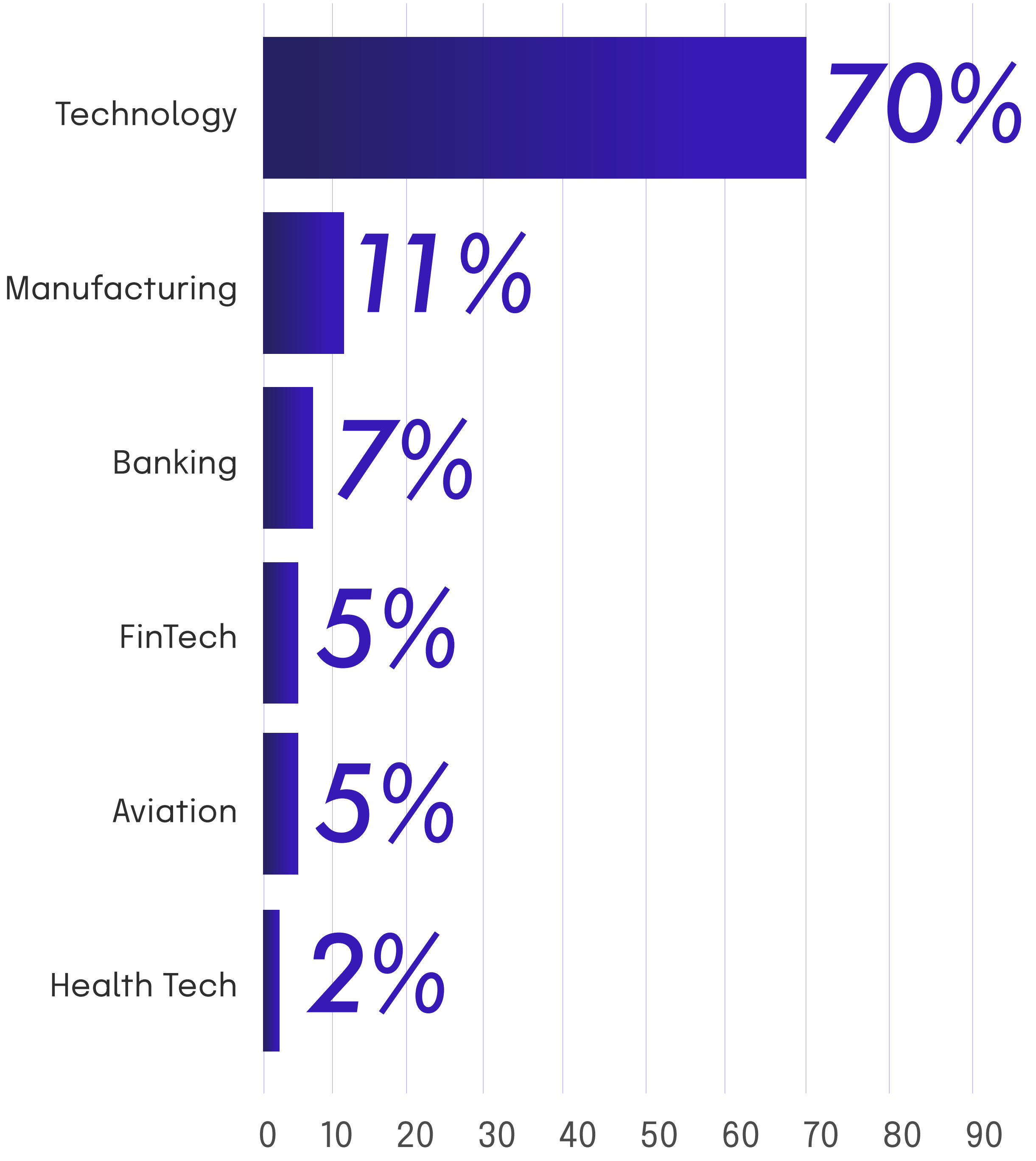


2024

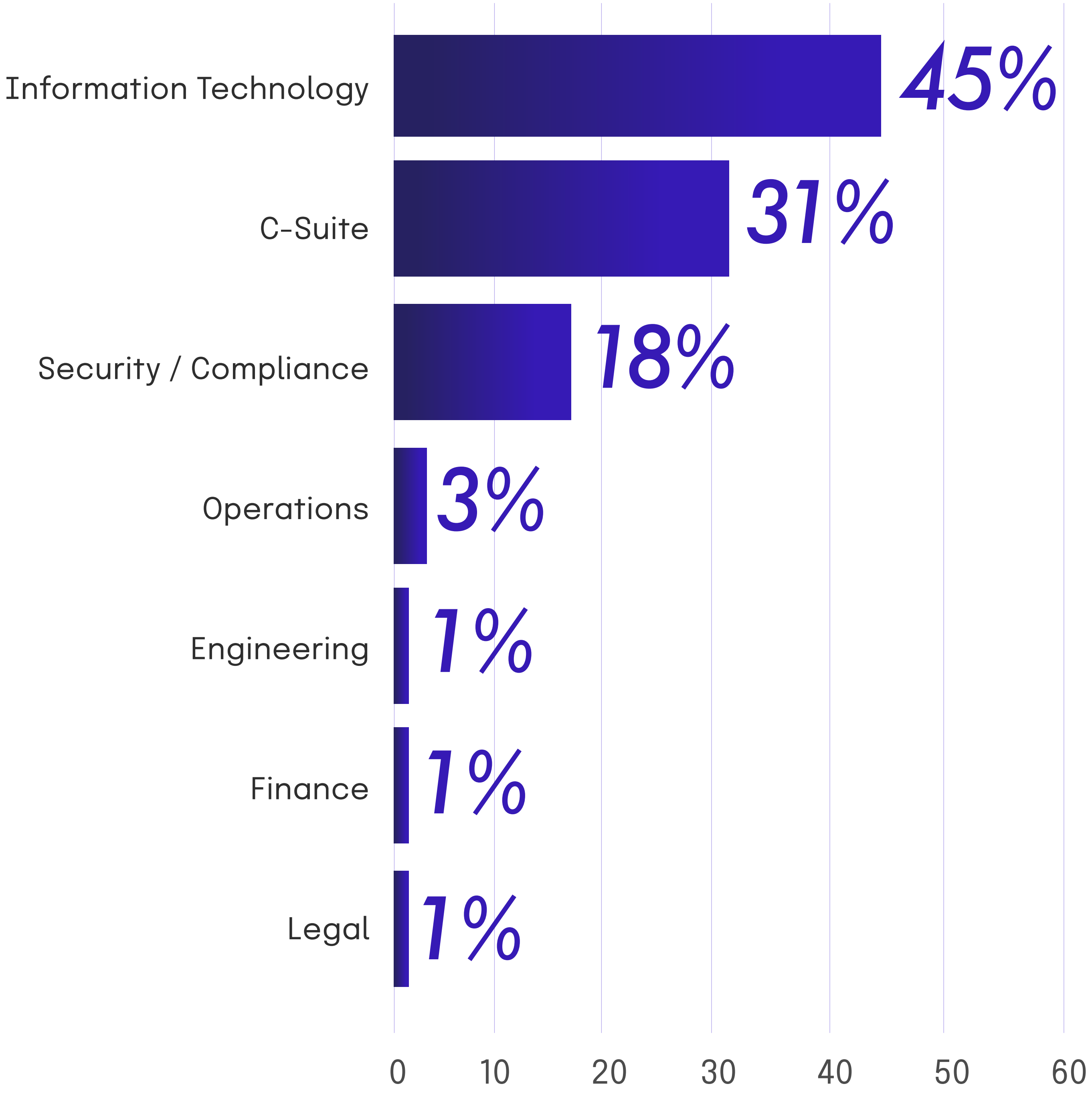
Survey Methodology

The 2024 IT Risk and Compliance Benchmark Survey gathered **1,001 responses during November, 2023**.

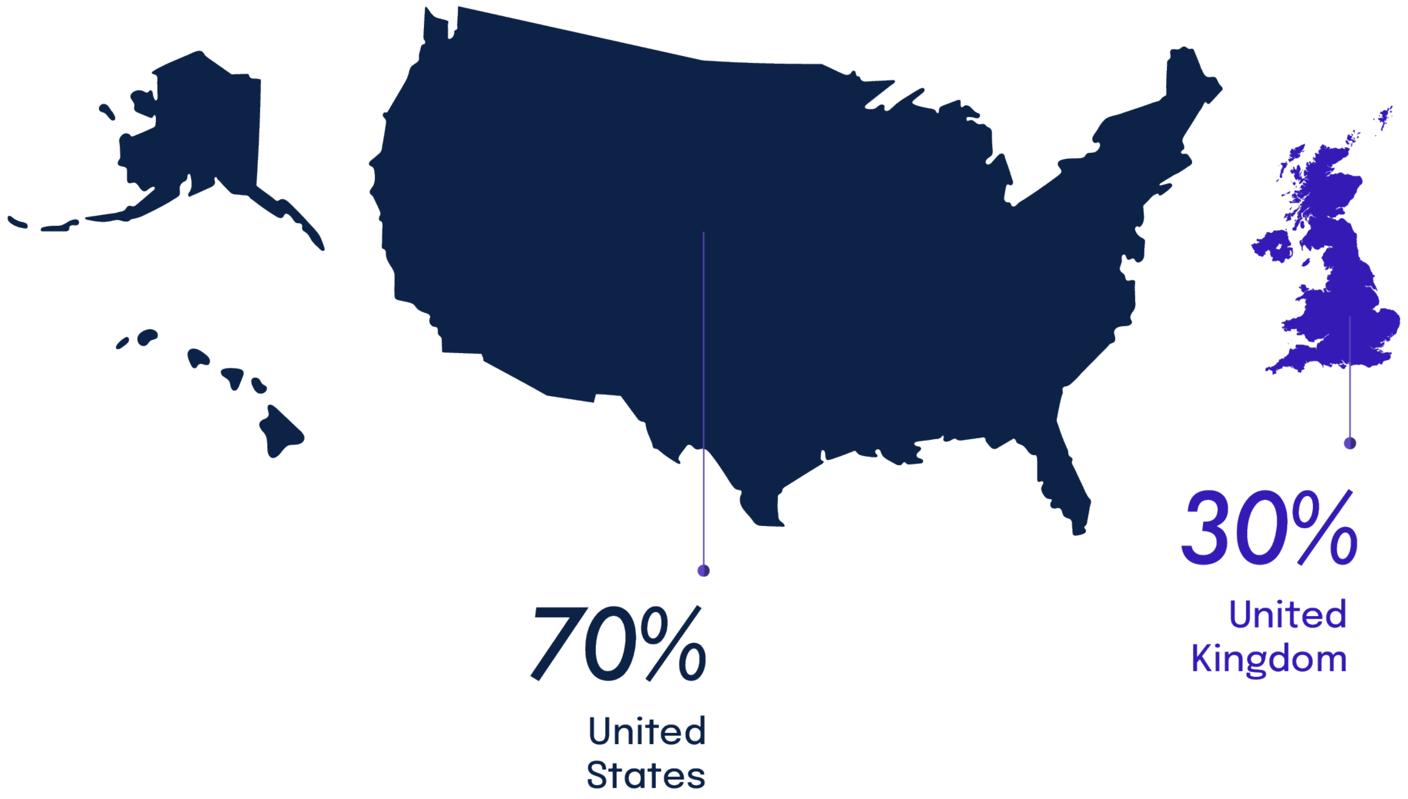
Industries surveyed



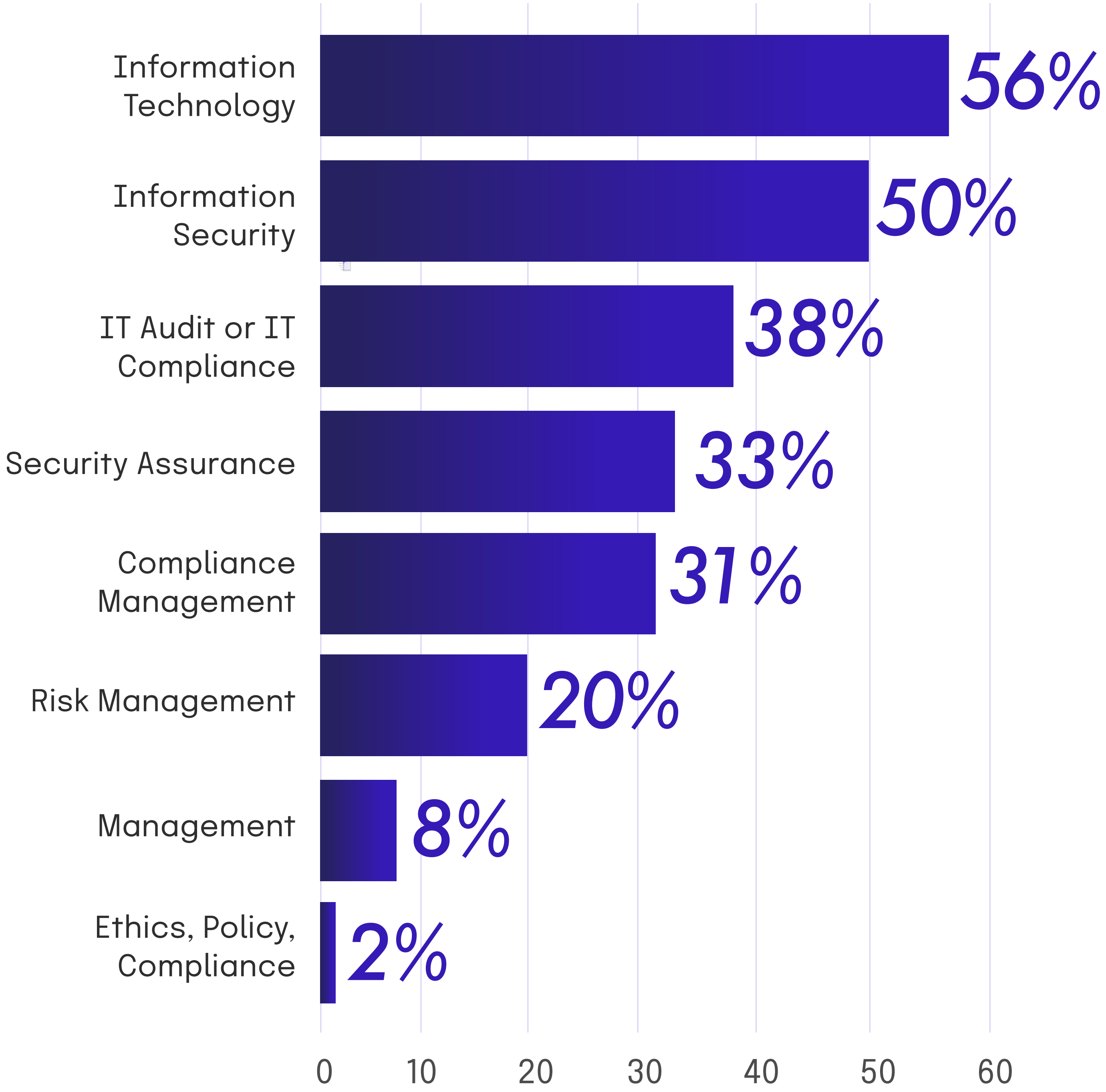
Departments



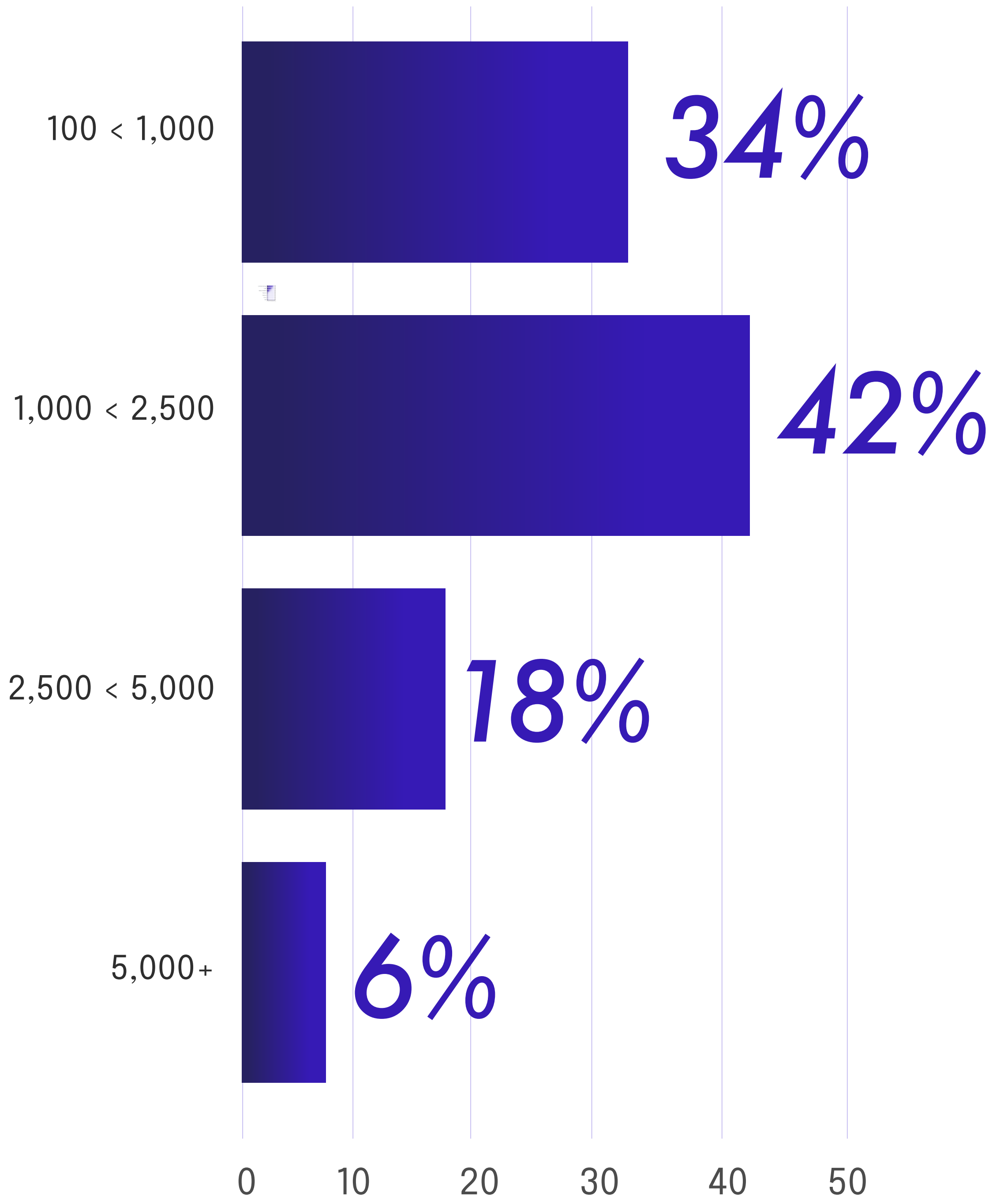
Locations surveyed



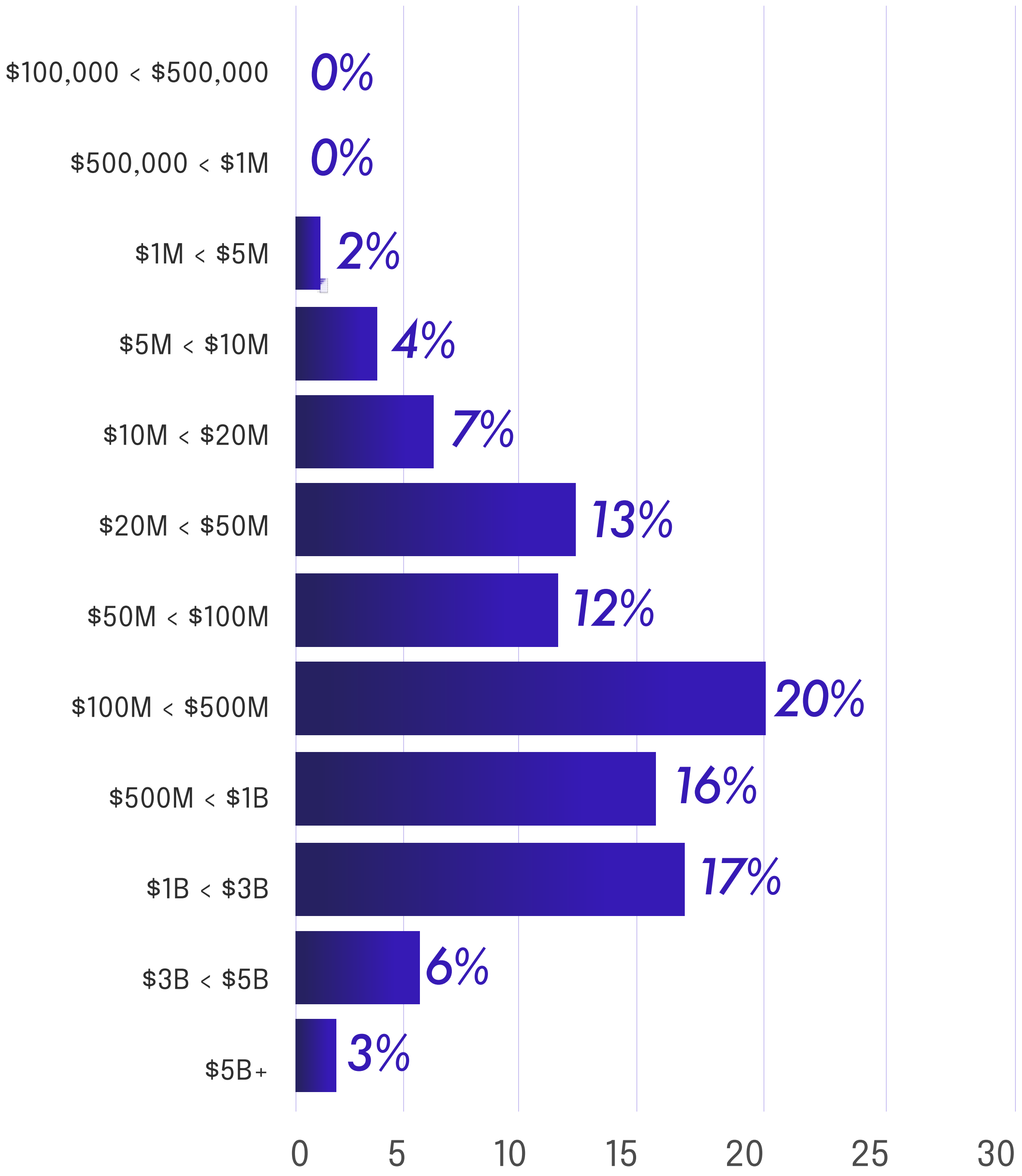
Job functions



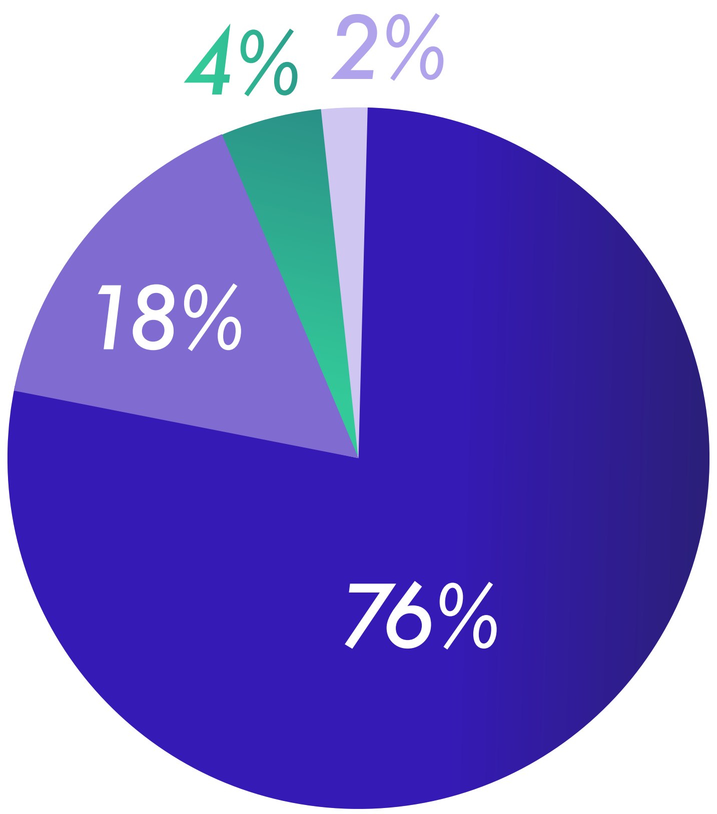
Organization size



Company revenue

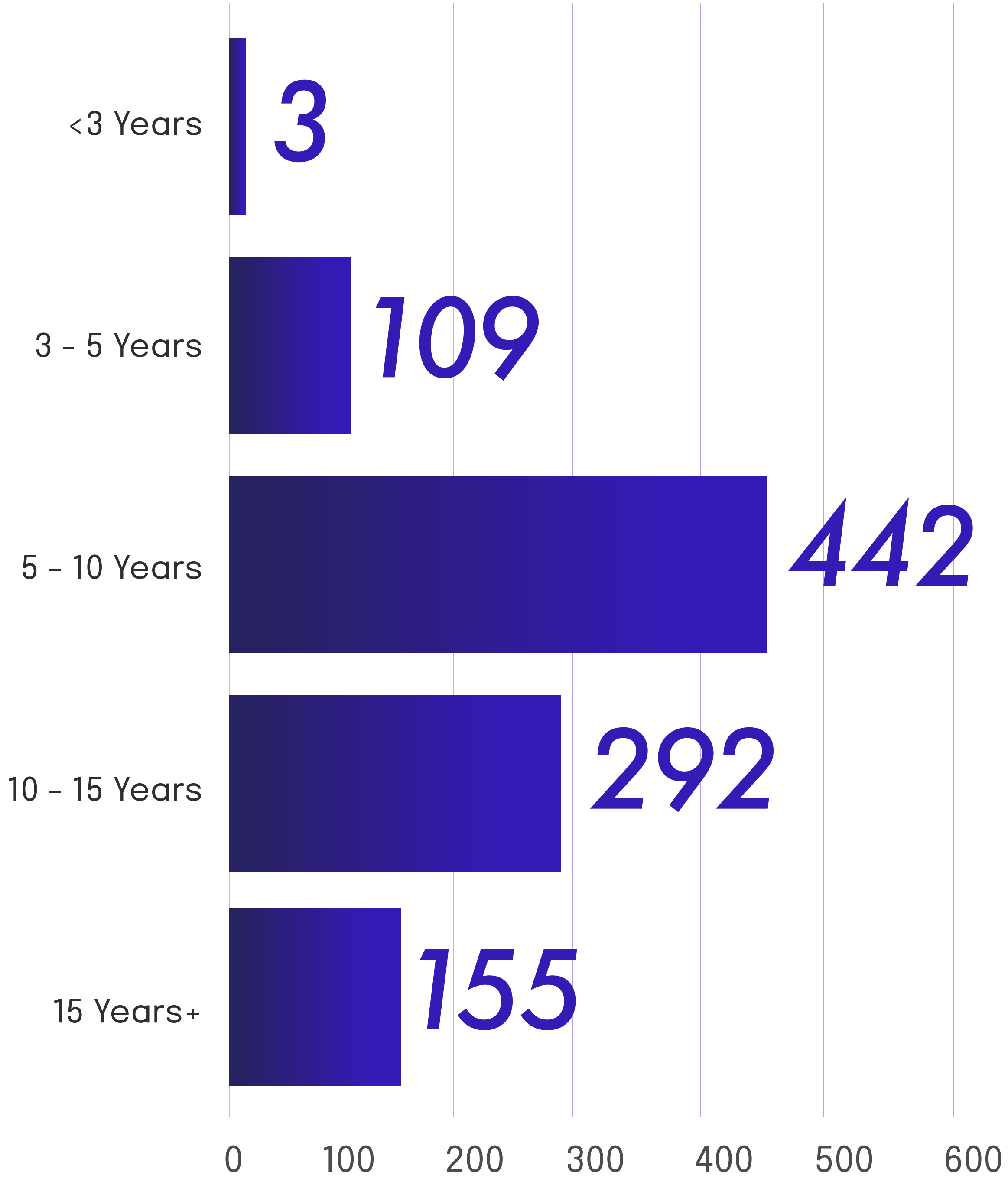


Decision-making capabilities



- ■ I am the sole decision maker
- ■ I am part of a team involved with decisions
- ■ I am a shared decision maker
- ■ I gather information, provide research, offer insights regarding decisions

Business tenure



hyperproof

Hyperproof is a risk and compliance management platform that empowers IT, security, and compliance teams to automate and scale their workflows without the burden of jumping between multiple legacy platforms and spreadsheets. The Hyperproof platform enables teams to get complete visibility into their organizational risks, streamline the audit process, and reduce their ever-growing compliance workloads. Hyperproof is trusted by leading organizations like Veeva Systems, Fortinet, Motorola, Outreach, and 3M.

To learn more about Hyperproof, visit **hyperproof.io**

hyperproof

Get a Demo

2024 IT Risk and Compliance Benchmark Report

CHARTING THE GOVERNANCE, RISK, AND COMPLIANCE UNIVERSE