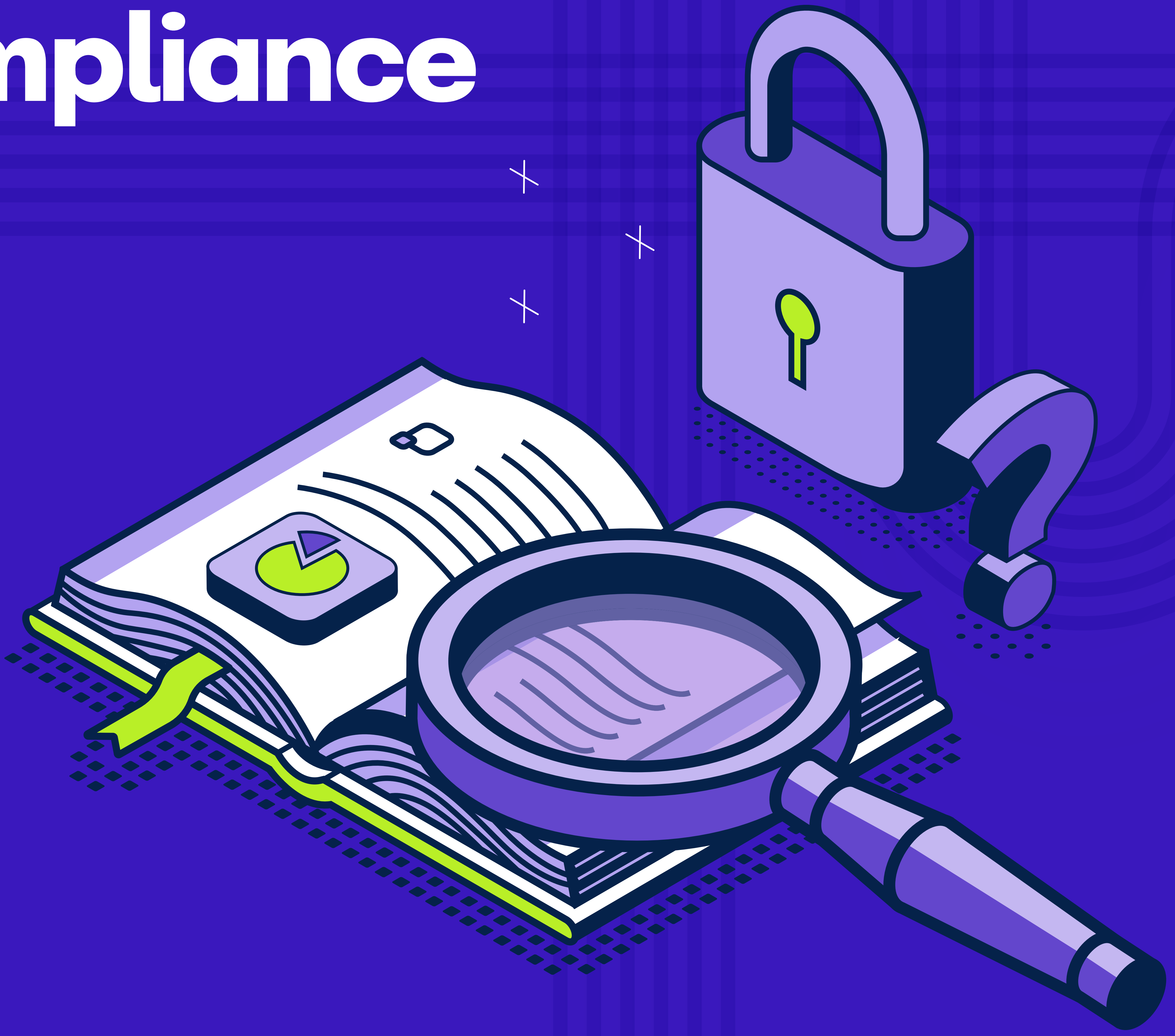
SPRING 2025

2025 IT Risk and Compliance Benchmark Report

The Reader's Digest Issue



A PUBLICATION BY hyperproof

TABLE OF CONTENTS

FOREWORD

2024 was a milestone year for governance, risk, and compliance (GRC). As companies grappled with increasing regulatory demands, growing stakeholder expectations, and an ever-expanding risk landscape, the importance of GRC programs rose to prominence. This push resulted from several drivers, including new government regulations like the Digital Operational Resilience Act (DORA) and NIS2. Meanwhile, tech stack overlaps at companies and reliance on vendors continues to deepen, causing third-party risk to expand. Regulatory bodies in the US also continued to expand their oversight of cybersecurity practices, requiring organizations to demonstrate proactive risk management. We anticipate the regulatory climate in the United States will be more complex in 2025.

Increasing AI adoption also added complexity to the equation due to new emerging risks like cybersecurity threats, ethical concerns, and potential operational disruptions. Organizations found themselves needing to mature their GRC programs and provide the frameworks needed to manage these risks while enabling innovation. As a result, GRC is no longer seen as a back-office function – it is a public-facing responsibility that influences brand reputation and your ability to land and expand new markets.

GRC maturity is no longer a back-office function – it is a public-facing responsibility that influences brand reputation and your ability to land and expand new markets.

So, what's the impact for 2025?

The findings of this survey reflect a decisive trend: organizations are responding to the changes seen in 2024 and making deliberate efforts to mature their GRC practices, not just for compliance but as a strategic imperative for long-term resilience and success. From integrating technology solutions that centralize risk and compliance activities to fostering cross-functional collaboration and embedding a culture of accountability, these efforts are reshaping the GRC space. Our findings highlight a shift in perspective within the market: **GRC teams are looking to mature their practices, as they are no longer seen as a check box exercise but a driver of operational excellence and strategic growth.**

As you explore the insights provided in this report, we invite you to consider how these trends align with your own organization's journey, especially in the coming year. Whether you are in the early stages of building a GRC program or refining a well-established program, there is much to learn from the collective experience of your peers. Together, we have an opportunity to elevate the role of GRC in shaping a more resilient, responsible, and forward-looking business environment.

Top Findings in Numbers

91%

of respondents have a centralized team to manage GRC

This is the highest number we've ever seen in the six years we have conducted this survey, up from 88% in the previous year.

60%

of respondents who manage risk ad-hoc or when a negative event happens experienced a data breach in 2024

Respondents who use integrated and automated GRC tools are less likely to experience a data breach at only 41%.

63%

of respondents said their GRC budgets will increase in the next 12 to 24 months

The majority of respondents expect budgets to go up for the second year in a row.

72%

of surveyed companies plan to grow their compliance teams in 2025

The majority of respondents are confident about their ability to expand their teams despite economic uncertainty in 2025.

52%

of respondents reported that their teams spend between 30% and 50% of their time on administrative tasks like manual data entry

Although respondents are confident that they have taken steps to mature their GRC programs, they still spend a significant amount of time on manual processes.

74%

of respondents said their annual security budget is over $1 million

Most of the surveyed organizations are making a substantial investment in security. Only 22% of respondents reported that their annual security budget is under $1 million.

59%

of respondents test all controls as opposed to only the most critical controls

This is an increase of 26% year-over-year, signifying a major industry shift to proactive compliance management strategies.

55%

of respondents said they use a common controls framework to streamline their GRC processes

Using a common controls framework (CCF) has become a standard best practice, differing from our results in previous years.

CHAPTER 1

GRC Programs Are Maturing

A common theme in this year's findings is the importance of centralized and cohesive approaches to GRC. Organizations that consolidate GRC activities under a single team report better consistency and efficiency in managing risks. In 2024, Hyperproof released our own **GRC Maturity Model** to provide a commonly accepted way for companies to assess and improve their own GRC capabilities. The model is segmented into four levels:

Traditional: reactive with insufficient or no planning

Initial: beginning to define processes at a departmental level

Advanced: establishing defined, repeatable processes at the organizational level

Optimal: proactively using measurements to continuously improve performance

Each level is defined by unique characteristics to help organizations identify where their company might be on the path to GRC maturity. Our findings revealed that respondents are approaching GRC maturity with four key strategies aligned to the Hyperproof GRC Maturity Model: centralizing GRC efforts, leveraging a common controls framework (CCF), conducting quarterly risk assessments, and adopting comprehensive risk management programs with people, processes, and technology. As you explore this chapter, we encourage you to review the Hyperproof GRC Maturity Model to see where your organization lands and whether you have implemented the four strategies outlined below.

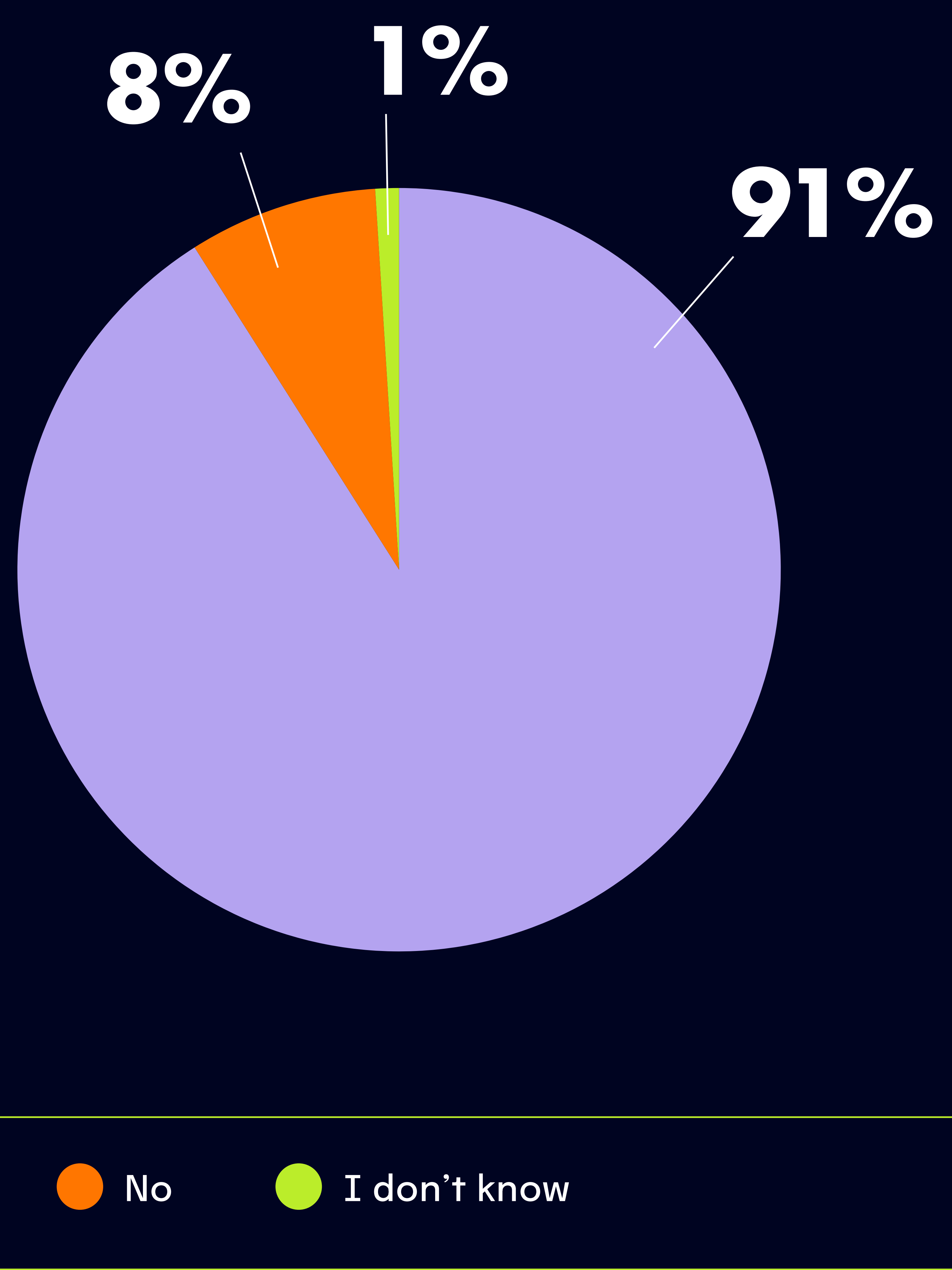
STRATEGY 1:

Centralizing enterprise-wide risk and compliance efforts under a single team

Most notably, we found that 91% of respondents reported having a centralized team responsible for GRC activities. This is up from last year, where 83% of respondents reported having a centralized team managing GRC activities. Only 8% of respondents take a siloed approach to risk management, where individual teams or business units manage risks.

The high adoption of centralized GRC teams indicates a strong trend toward integration in the market, as most organizations recognize the importance of taking a unified approach to risk and compliance management. However, those 8% of organizations still operating in silos face significant challenges, including inconsistent risk mitigation practices and inefficiencies, which we will discuss later in this chapter.

Does your organization have a centralized governance, risk, and compliance program that works across business units and geographies?



2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

Centralization does not mean a shared responsibility across all elements of GRC

In fact, 43% of organizations still view compliance primarily as the function responsible for enforcing regulations and industry standards. This is similar to last year's results, where 45% of respondents chose this option. Another 36% see compliance as a tool to mitigate risks, although they acknowledge that risk management and compliance activities are often conducted independently in response to specific events.

However, a new and integrated approach is emerging, with 22% of organizations choosing to align risk and compliance activities, a 55% increase year-over-year. One example of this kind of approach is connecting controls to risks, which means when addressing an issue on a control, the risk associated with that control would be reduced.

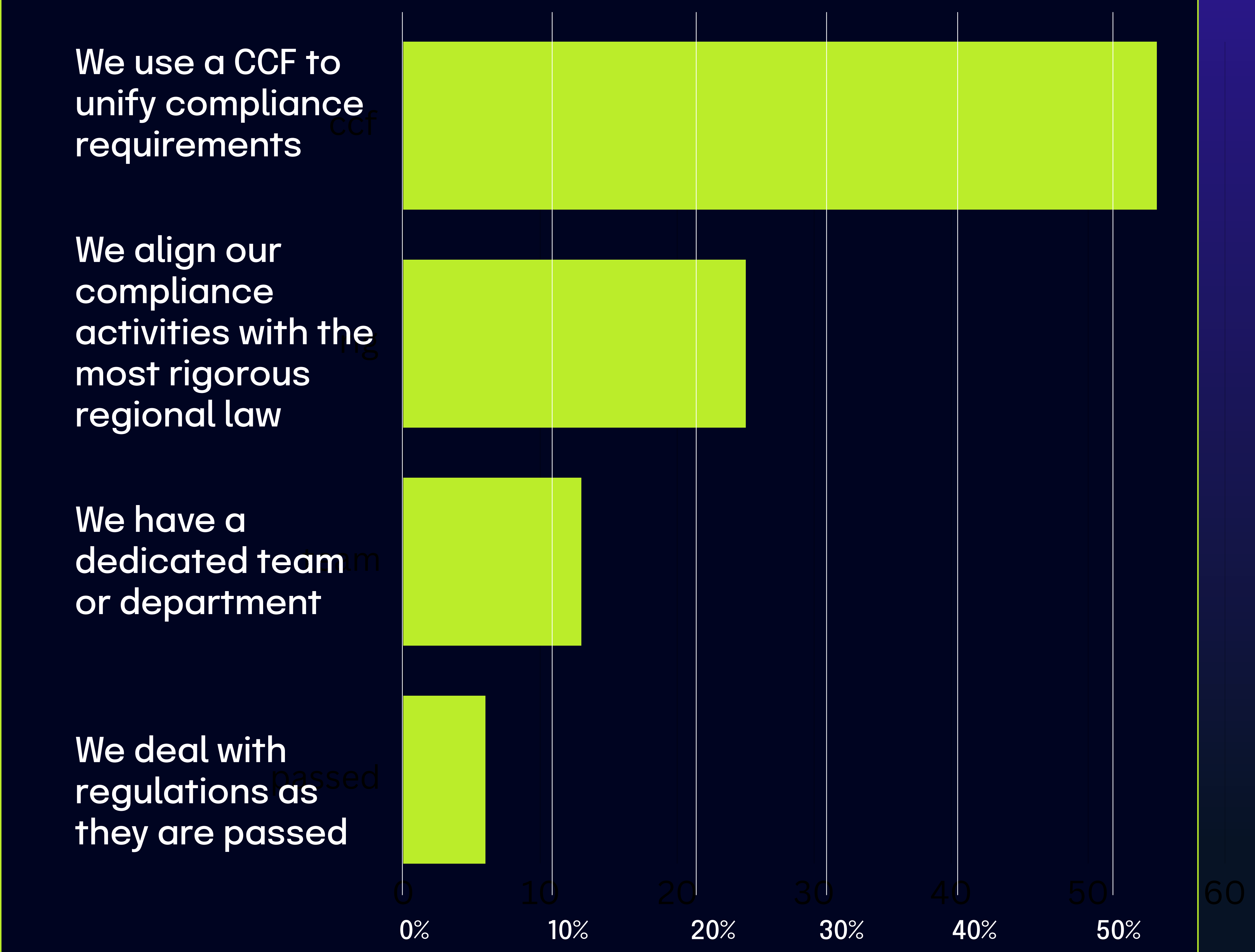
	Approach to managing IT risks				
	Ad-hoc or when a negative event happens	In siloed departments, processes, and tools	An integrated tool and it's mostly manual	An integrated tool and it's mostly automated	Our MSSP manages our IT risks
Compliance is responsible for enforcing regulations / industry standards	65%	41%	30%	35%	61%
Risk management and compliance activities are typically conducted in response to separate events	29%	52%	48%	30%	17%
Our risk and compliance activities are integrated	5%	6%	22%	35%	22%

STRATEGY 2:

Leveraging a common controls framework

55% of respondents said they utilize a common controls framework (CCF) that aggregates and rationalizes regulations to boost efficiency when addressing rules and requirements across different frameworks. This represents a 10% increase year-over-year, showcasing that this was not a short-term trend. The remaining organizations were split in how they adapted to new regulations, with 25% choosing to align to the most regional laws while 6% maintain a reactive approach of responding to individual changes as they happen. This segmentation highlights the various levels of maturity across organizations. Mature organizations choose to look ahead and streamline their processes, while others remain siloed in their approach to GRC.

How does your organization adapt its cybersecurity and compliance controls to manage regional variances in data security and privacy regulations?

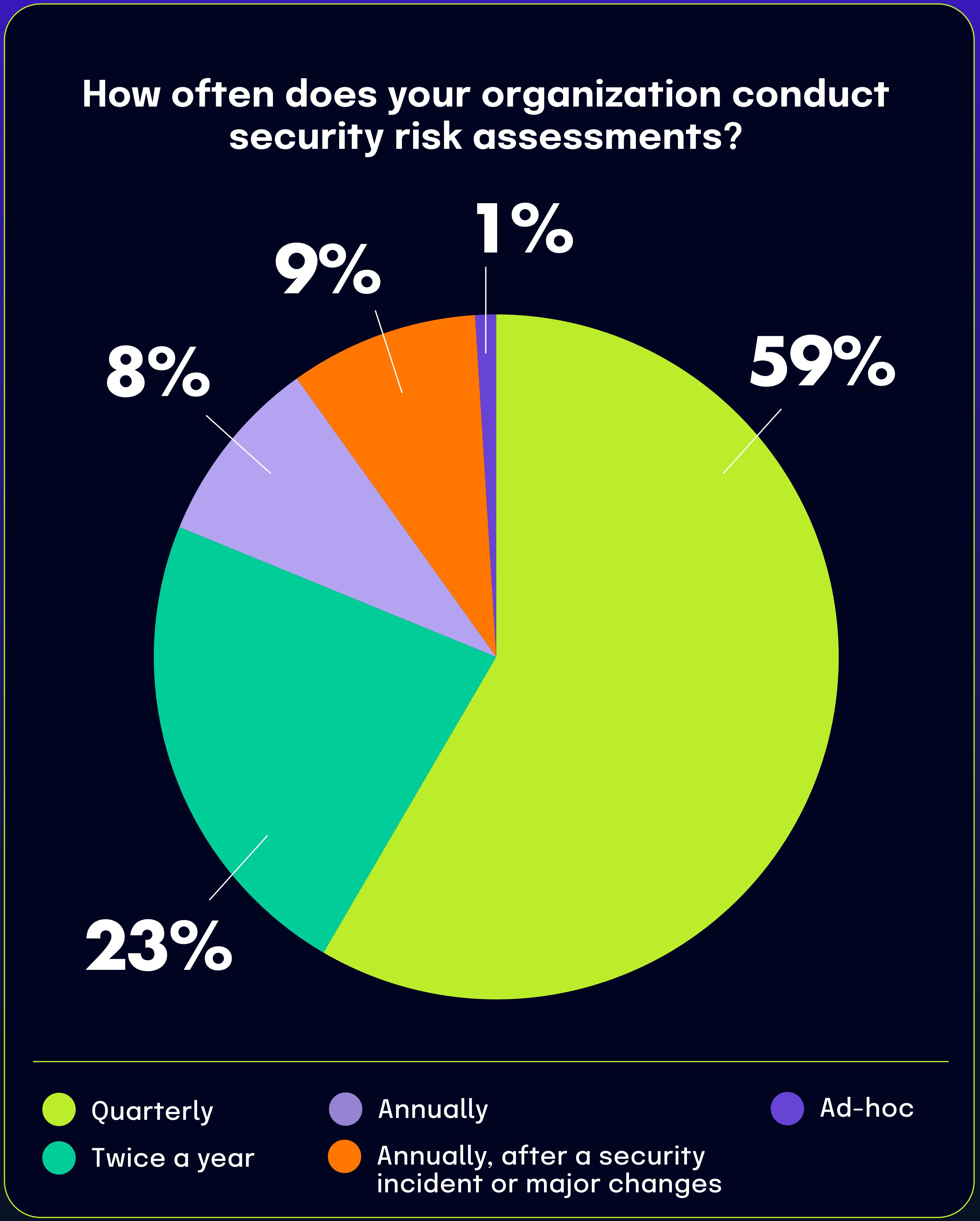


2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

STRATEGY 3:

Conducting quarterly risk assessments

The frequency of risk assessments saw the largest shift year-over-year, with 59% of respondents stating they conducted quarterly assessments as opposed to annually, compared to 45% last year. One reason for this shift is the continued adoption of risk management technology, which has reduced the burden associated with conducting these assessments, and companies have realized the value of having real-time visibility of their risk postures.



How often does your organization conduct security risk assessments?

2025 IT and Risk Compliance Benchmark Report

hyperproof.io/it-compliance-benchmarks

STRATEGY 3:

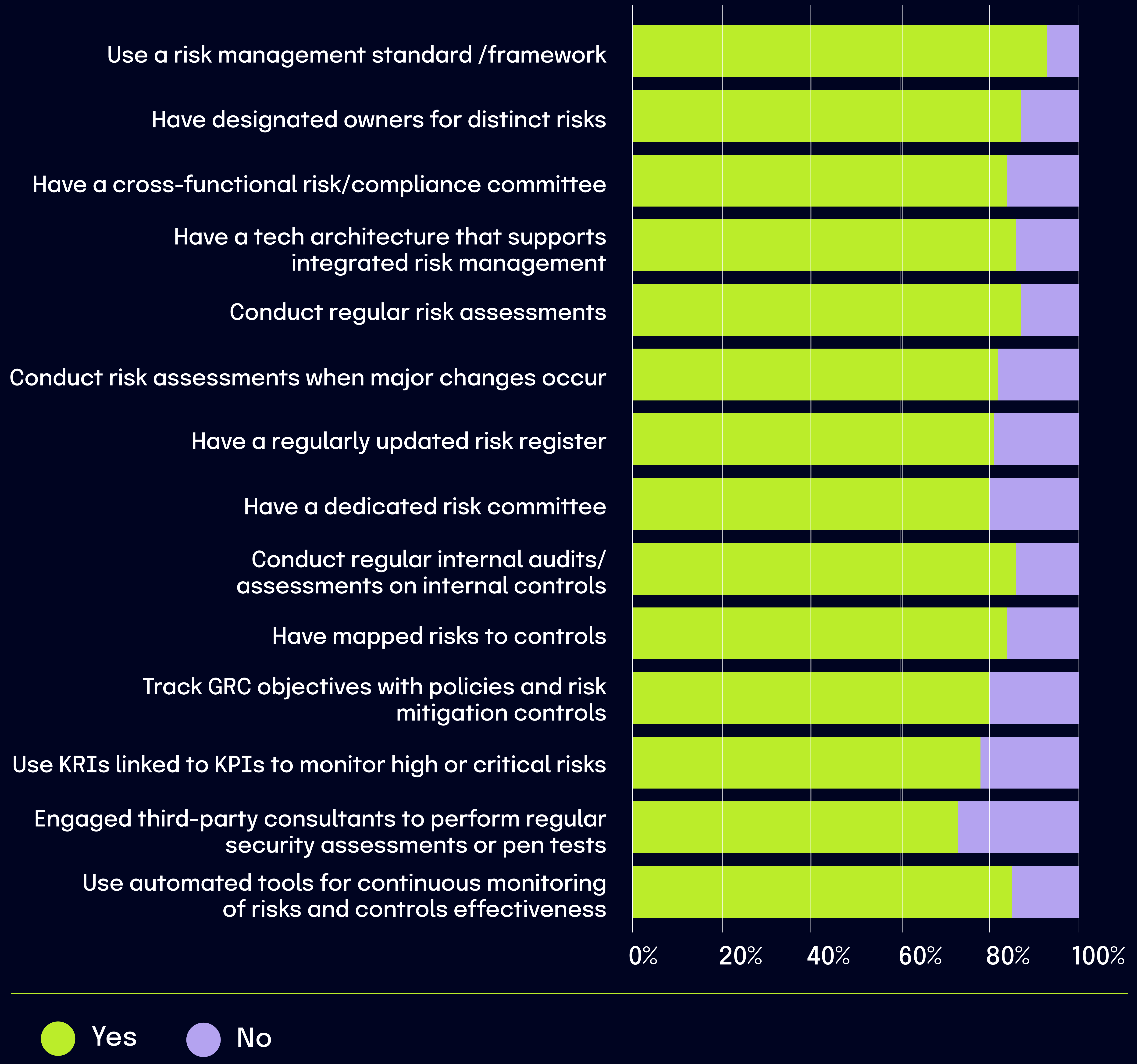
Conducting quarterly risk assessments (cont.)

Many organizations also recognize the value of engaging with third party consultants to find system gaps. 73% of respondents have engaged with third-party consultants to perform regular security assessments or penetration tests. It's important to note that frameworks like PCI DSS require penetration testing, and DORA will require red-teaming. 13% of respondents adhere to PCI DSS, and 10% adhere to DORA.

FRESH FACT

73% have engaged with third-party consultants to perform regular security assessments or penetration tests

Have you taken the following actions to formalize your commitment to risk management?



2025 IT and Risk Compliance Benchmark Report

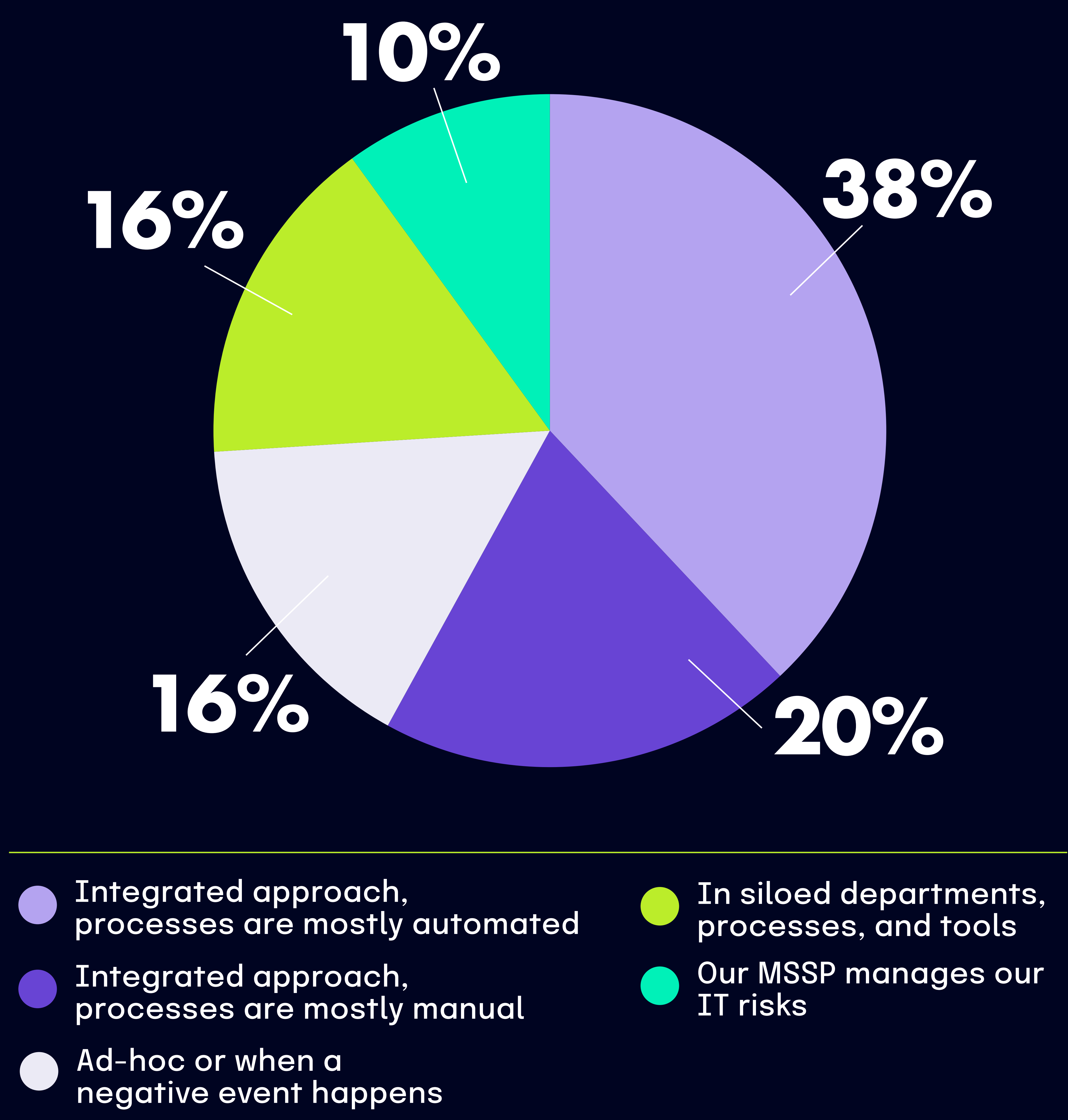
hyperproof.io/it-compliance-benchmarks

STRATEGY 4:

Adopting comprehensive risk management programs with people, processes, and technology

Over half (58%) of all respondents recognize that IT risk management requires integrated efforts across roles and teams. Many organizations have streamlined their approaches: 38% of all respondents have automated most of their IT risk management procedures. The number of organizations that continue to manage IT risk in silos has continued to decline year-over-year. Last year, 19% of organizations said they manage IT risks in silos, compared to 16% this year.

Which of the following statements is the closest reflection of how your organization manages IT risks?



2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

CHAPTER 2

Framework Adoption Trends

This year's survey reveals an important shift: **organizations are moving from reactive, checklist-driven approaches toward proactive, integrated strategies that align risk and compliance management with their broader business goals**. Companies are also adopting frameworks and tools that reduce inefficiencies and improve consistency to streamline operations. The majority of respondents (64%) use dedicated risk management software, and 72% of organizations use software that monitors their security controls and provides compliance posture reporting. This trend reflects a growing recognition that fragmented, manual processes hinder performance and scalability.

FRESH FACT

72%

of organizations use software that monitors their security controls and provides compliance posture reporting

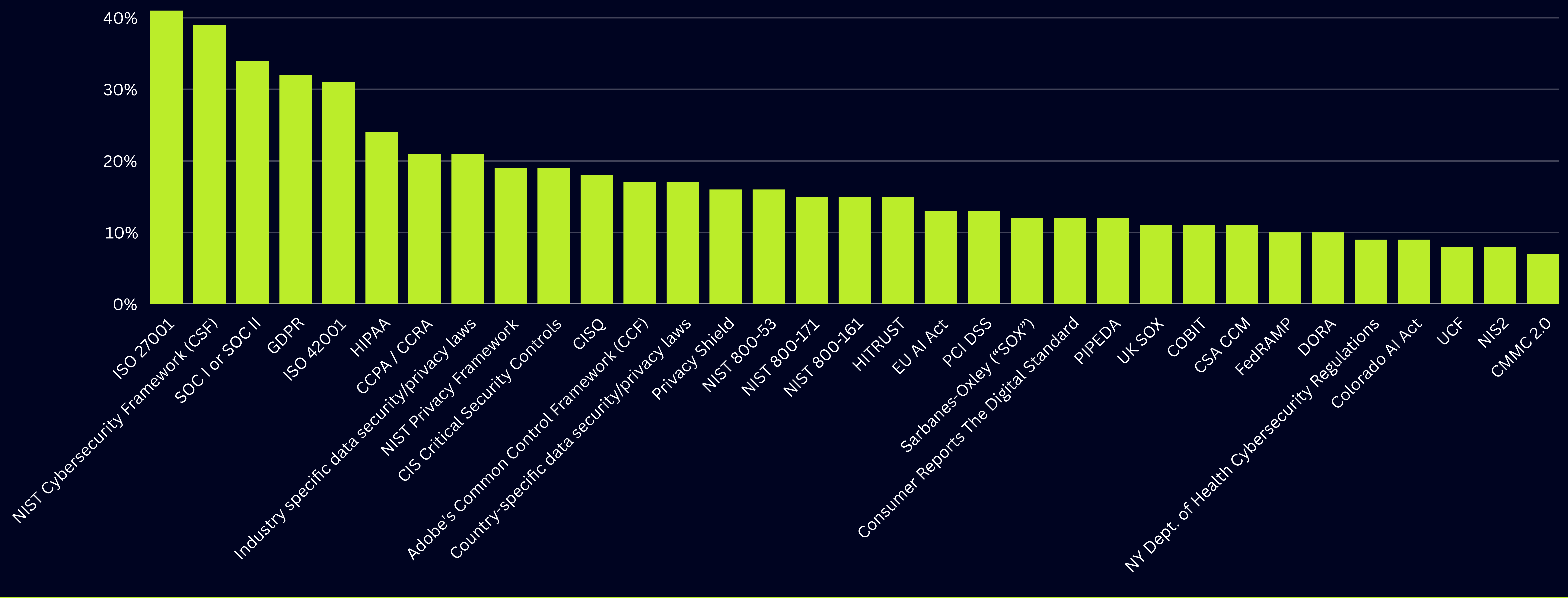
Cybersecurity and data privacy framework usage

Cybersecurity and data privacy framework usage remains relatively steady year-over-year. **ISO 27001 leads adoption with 41% adherence, reflecting its global recognition for information security management.** NIST CSF follows closely, with 39% of organizations leveraging its guidance to manage and reduce cybersecurity risks effectively. SOC I and SOC II are also widely implemented at 34%.

Regional regulations like GDPR are prioritized by 32% of organizations, underscoring the importance of data protection and privacy in EU markets, which we will discuss in detail later in this chapter. Similarly, CCPA has gained traction, with 21% adherence, reflecting growing attention to U.S. state-level privacy laws.

As organizations seek to align their practices with both global and regional compliance requirements, they tend to prefer widely recognized standards and frameworks with controls they can repurpose for additional frameworks as they add them. Organizations are now taking a proactive approach to managing security and privacy because they need to support business expansion and pursuit of new markets, especially in the EU.

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



2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

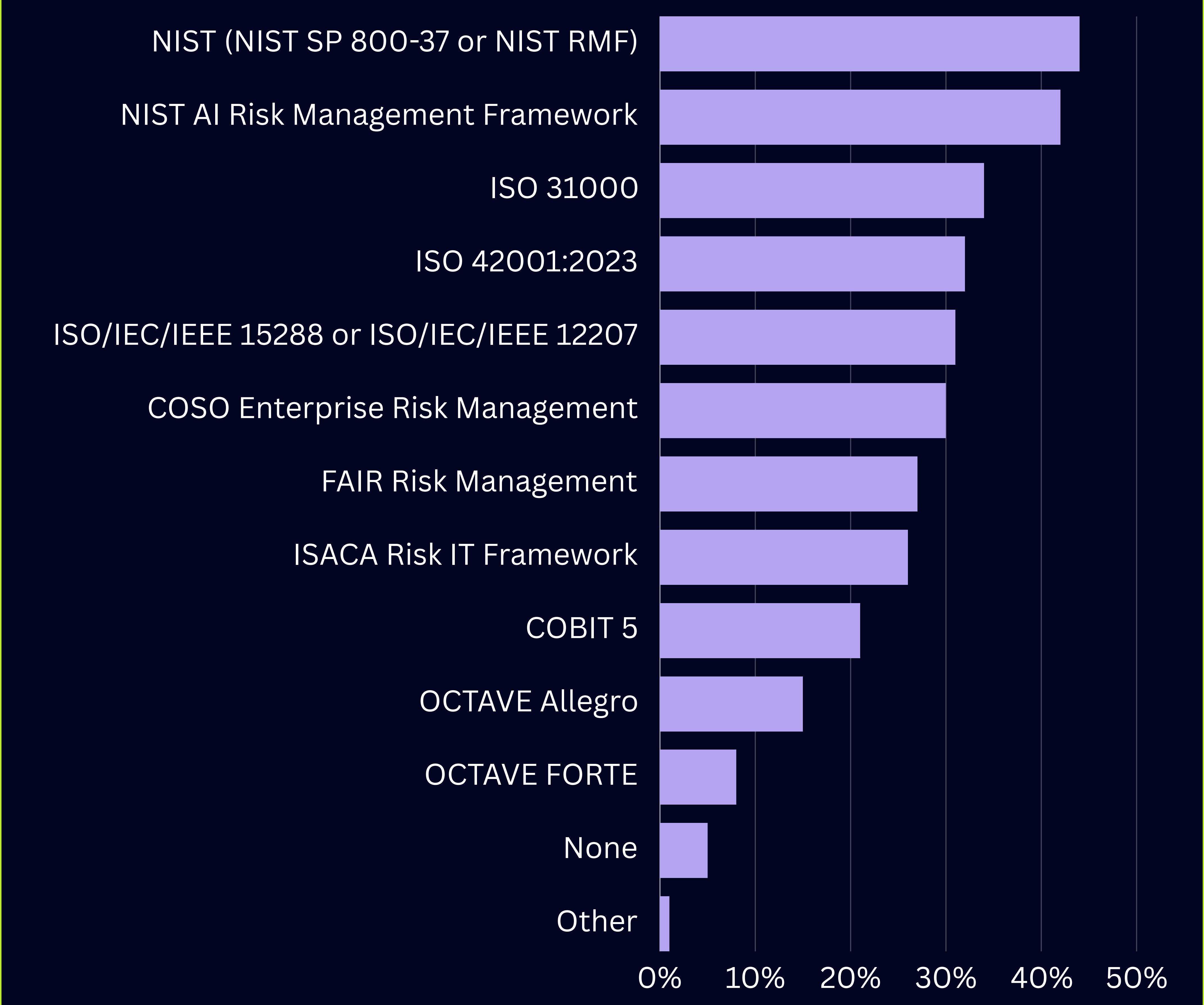
IT risk management framework usage

Among the most widely used frameworks, NIST SP 800-37 leads with 44% adoption, signaling its usefulness in guiding organizations to assess, respond to, and monitor IT risks. Close behind is the NIST AI RMF, adopted by 42% of respondents, highlighting the growing focus on managing risks specific to AI systems.

Global standards like ISO 31000 (34%) and ISO 42001:2023 (32%) are also popular, demonstrating their value in offering comprehensive approaches to risk management – including guidelines for AI risk – across diverse industries. Additionally, 31% of organizations use ISO/IEC/IEEE 15288 or ISO/IEC/IEEE 12207, frameworks designed for managing systems and software engineering life cycles.

Other notable frameworks include the COSO Enterprise Risk Management framework (30%), reflecting its relevance for integrating IT risk into overall enterprise risk strategies, and the FAIR Risk Management model (27%), which is widely recognized for its quantitative approach to risk assessment. Meanwhile, 5% of organizations surveyed reported using no formal IT risk management framework, indicating potential gaps in their approach to managing IT vulnerabilities.

Which of the following IT risk management frameworks does your organization use?



2025 IT and Risk Compliance Benchmark Report

hyperproof.io/it-compliance-benchmarks

Preparing for AI regulations

Organizations aren't just implementing more AI-related controls because they are wary of the risks introduced by increased AI tools usage; regulatory bodies are requiring them to do so. While a majority of companies are proactively addressing AI-related risks in line with forthcoming EU regulations, a significant portion remains in transition. Our findings underscore the importance of continued efforts to fully implement robust risk management systems, ensuring compliance and fostering trustworthy AI practices across markets.

FRESH FACT

59% have implemented a risk management framework due to the EU AI Act

Organizations aren't just implementing more AI-related controls because they are wary of the risks introduced by increased AI tools usage; regulatory bodies are requiring them to do so.

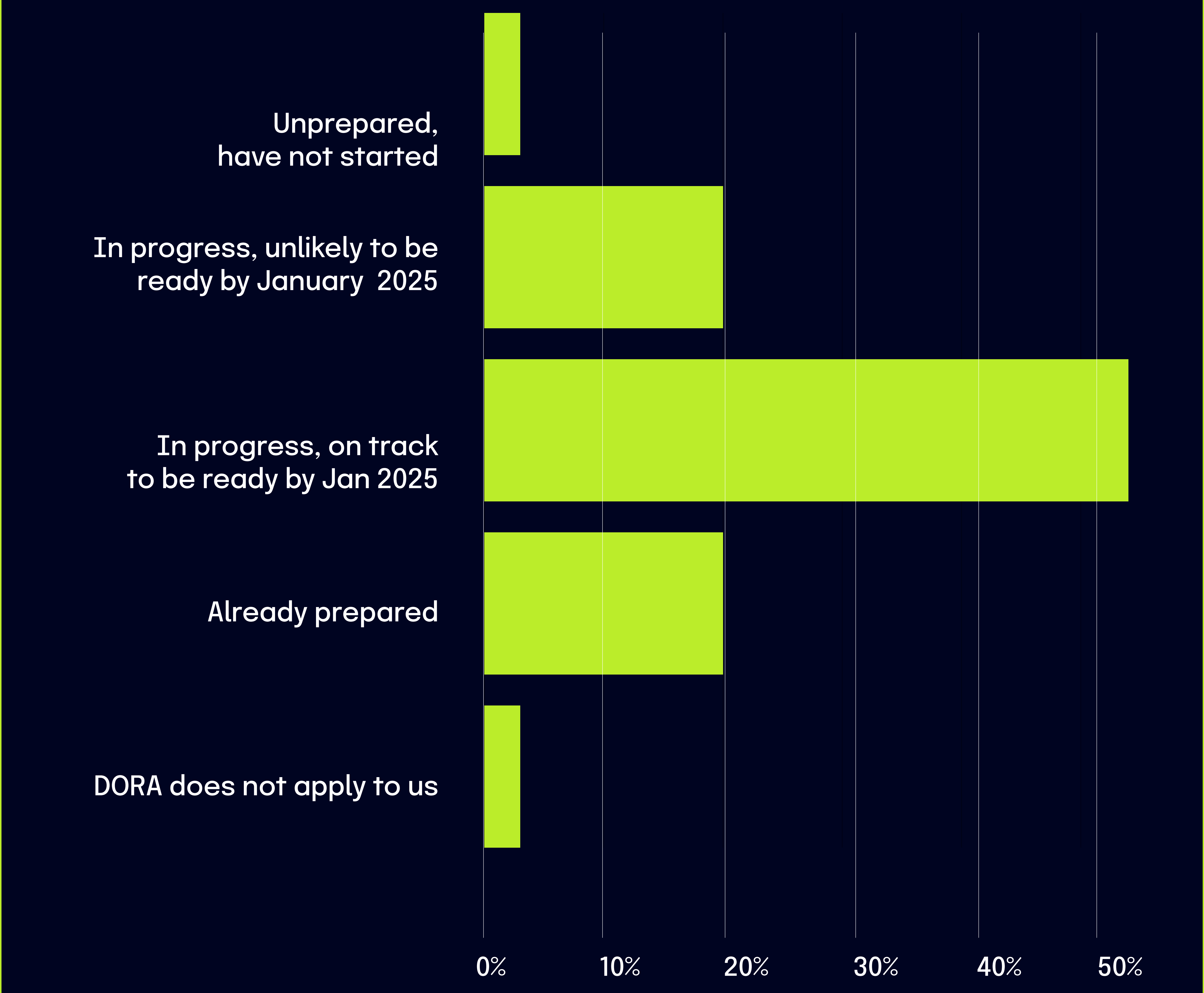
The Digital Operational Resilience Act (DORA)

All financial institutions in the EU and ICT vendors of financial institutions must comply with DORA, a European Union regulation aimed at bolstering the financial sector's ability to withstand and recover from digital disruptions and cyber threats. Adopted on November 28, 2022, DORA entered into force on January 16, 2023, with enforcement beginning on January 17, 2025.

While DORA does not explicitly address artificial intelligence (AI) systems, its comprehensive ICT risk management framework encompasses AI technologies utilized within financial operations. Financial institutions employing AI for functions like fraud detection or credit scoring must ensure these systems adhere to DORA's standards for operational resilience.

We asked respondents how far along their organization is preparing for DORA enforcement in January 2025. **We found that over 90% of organizations have already started preparing for DORA.**

How far along is your organization in preparing for Digital Operation Resilience Act's (DORA) enforcement in January 2025?



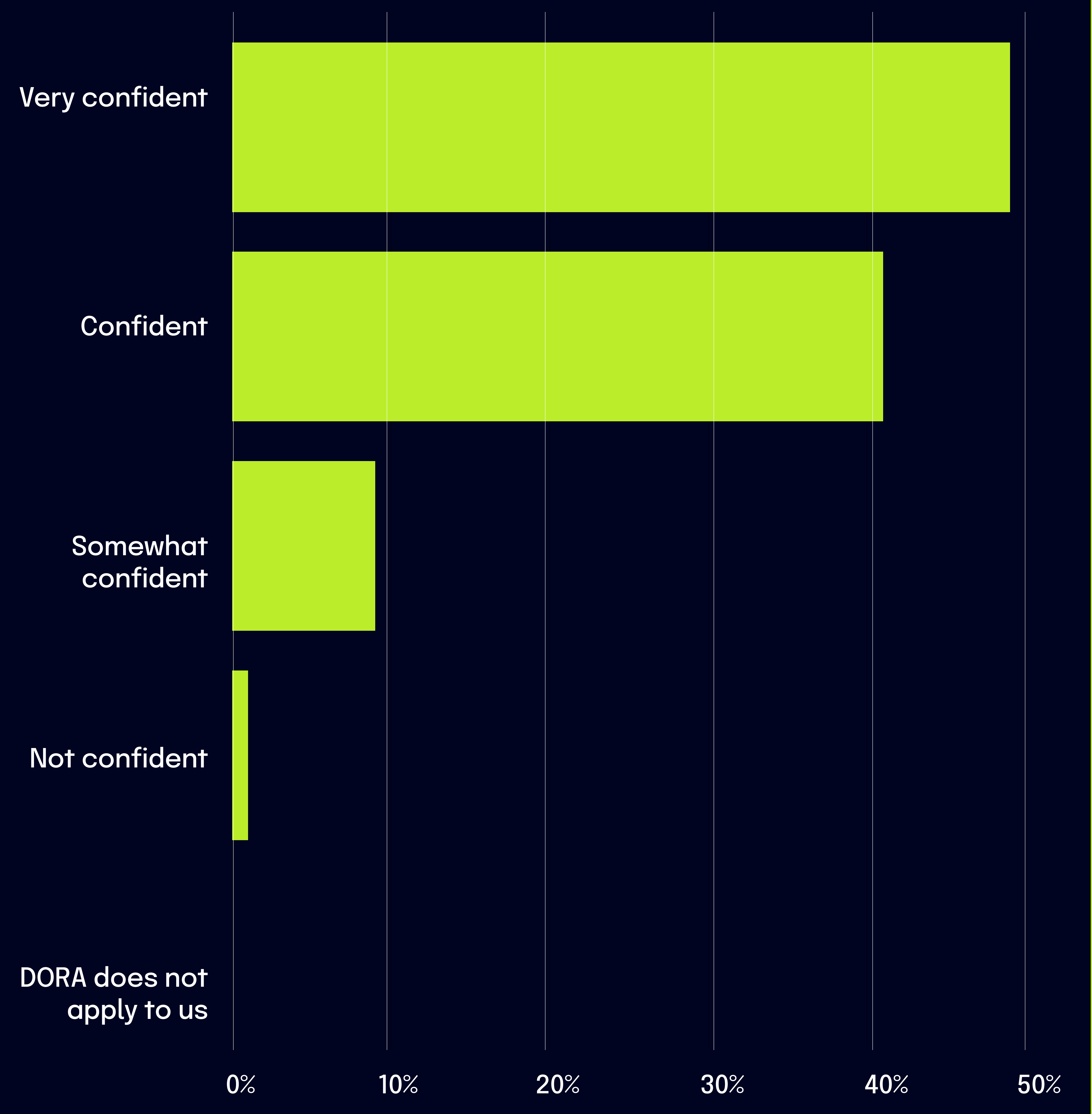
2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

We also asked organizations to rate their confidence in their ICT providers' readiness to meet DORA's stringent requirements. 49% are "very confident" in their providers' preparedness, citing regular audits and ongoing communication as key compliance indicators. An additional 41% express confidence, noting observable progress in aligning operations with DORA standards.

However, 9% of respondents are only "somewhat confident," indicating that while their providers know DORA, a comprehensive assessment of readiness is still pending. A small fraction (1%) lack confidence, expressing concerns about their providers' understanding and capability to comply with DORA's mandates. Notably, nearly all organizations recognize the applicability of DORA, with only 0.1% stating it does not apply to them.

These findings underscore a general sense of assurance among organizations regarding their ICT providers' compliance with DORA. Nonetheless, uncertainty among some organizations highlights the need for continued diligence in evaluating and ensuring provider readiness as the enforcement date nears.

What is your level of confidence that your ICT providers will comply with DORA's stringent requirements?



2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

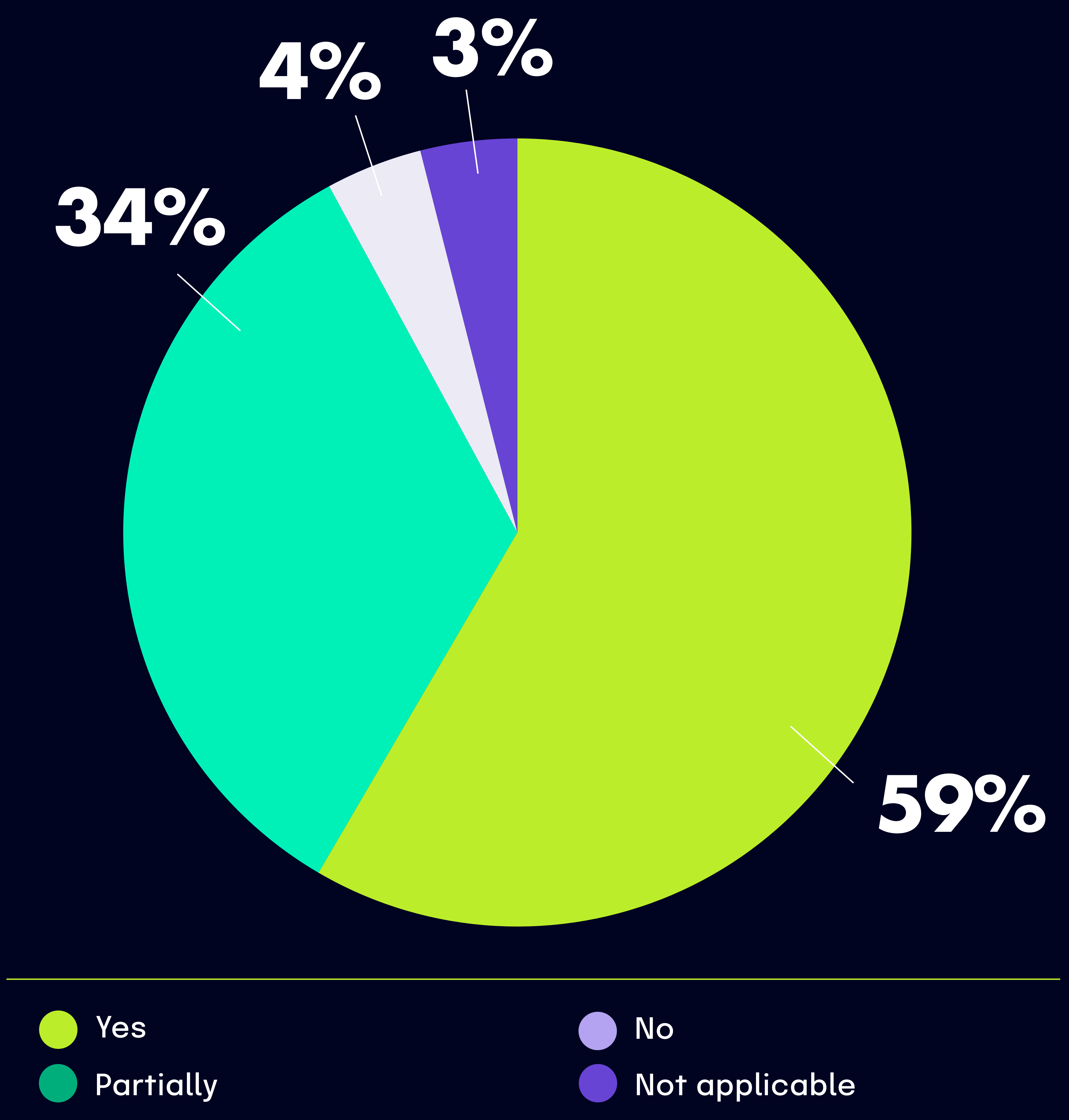
The European Union's Artificial Intelligence Act (AI Act)

In addition to DORA, EU regulators are actively developing regulatory frameworks to govern AI applications and systems. The European Union's Artificial Intelligence Act (AI Act), adopted in May 2024, establishes a comprehensive framework to regulate AI systems to ensure their safe and ethical deployment across various sectors.

We asked respondents whether their organization has implemented risk management frameworks to address AI risks and comply with the EU AI Act. The results reveal varied stages of readiness in implementing comprehensive risk management frameworks to address AI-related risks.

Notably, 59% of respondents report fully establishing such frameworks, aligning with the AI Act's stringent requirements. An additional 34% have initiated the process but have yet to fully comply. Meanwhile, 4% are in the preliminary stages, currently assessing the Act's mandates and planning future framework development. Another 4% consider the AI Act inapplicable to their operations, likely due to their AI system usage.

Has your company implemented a comprehensive risk management framework to address risks associated with the use of AI under the EU AI Act?



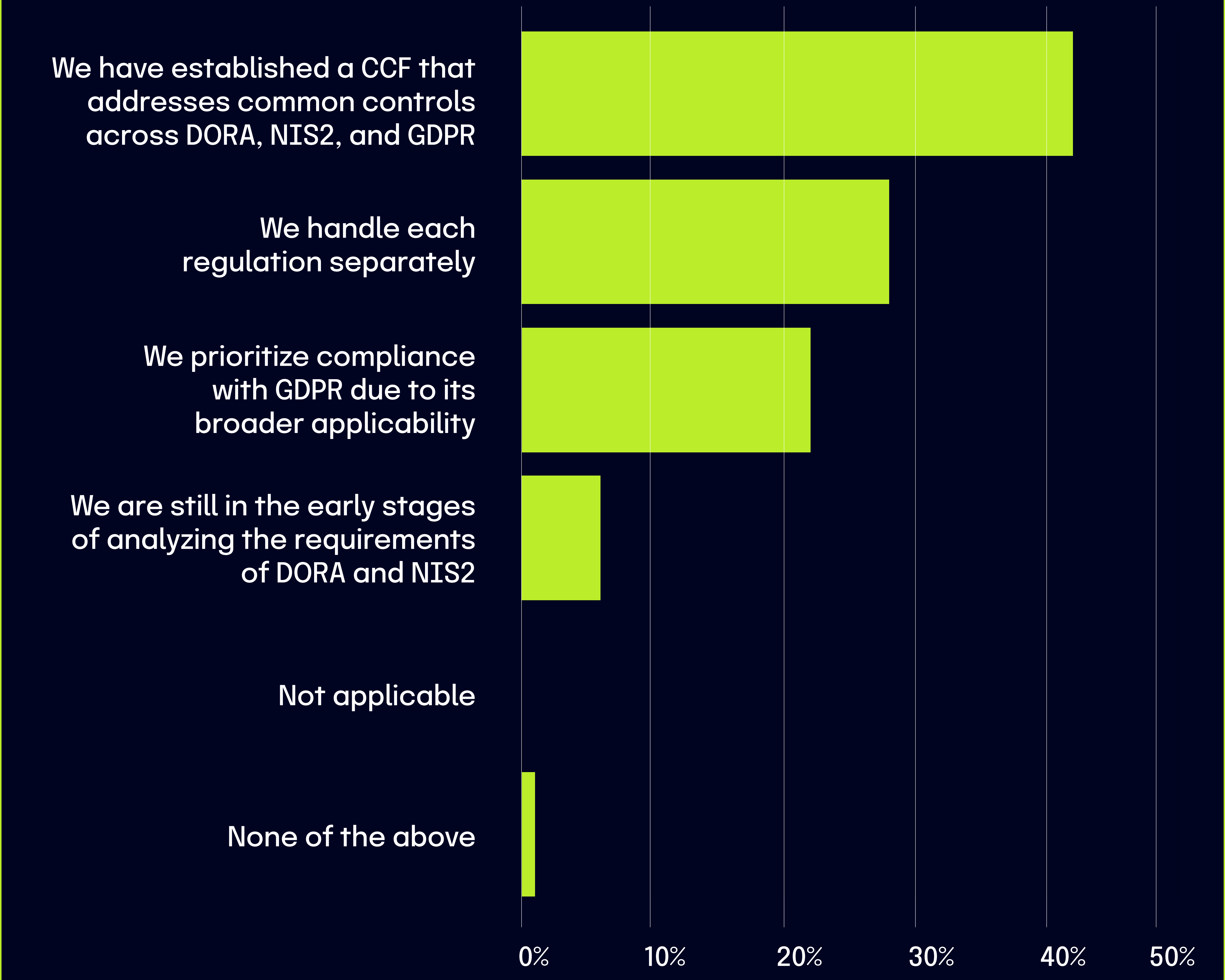
2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

These findings are consistent with the results from a related question, where we asked respondents how their organization handles the overlapping compliance requirements between DORA, NIS2, and GDPR. For that question, 42% of respondents report establishing a common control framework that addresses common controls across DORA, NIS2, and GDPR, ensuring consistent compliance management.

FRESH FACT

59% have implemented a risk management framework due to the EU AI Act

How is your organization handling the overlapping compliance requirements between DORA, NIS2, and GDPR?



2025 IT and Risk Compliance Benchmark Report

hyperproof.io/it-compliance-benchmarks

CHAPTER 3

How Organizations Address GRC Tasks

Respondents are transitioning from fragmented, reactive GRC task management to a more mature and proactive approach, enabling them to manage risks more effectively. This evolution underscores the importance of GRC maturity as a critical driver of operational security and organizational success. Our survey has shown a clear correlation between IT risk management approaches and the likelihood of experiencing a security breach involving sensitive data for three consecutive years. **Organizations managing IT risk reactively or in siloed environments consistently report higher breach rates than those using integrated, automated tools.** In 2022, 77% of respondents who managed IT risk ad-hoc experienced a breach, compared to 57% of those using automated GRC solutions.

By 2024, this trend continued, with companies managing their IT risks ad-hoc having a 25% higher chance of experiencing a breach than those that take an integrated approach. **This data highlights a crucial trend: as organizations adopt more mature and integrated GRC practices, they significantly reduce the likelihood of experiencing a data breach.** The steady decline in breach rates among organizations using integrated and automated tools reflects a broader shift toward proactive risk management and more sophisticated evidence collection, control monitoring, and compliance processes.

Confidence in the ability to identify risks is high, but control management remains more difficult

We found a spectrum of responses when we asked respondents to self-assess how well their organizations performed risk management tasks. **Notably, 97% of respondents believe they meet their objectives in identifying and assessing risks,** indicating strong capabilities in this foundational area. However, performance declines in other areas: 88% report success in identifying controls, 84% in validating these controls against standard compliance frameworks, and 83% in aligning controls with identified risks.

FRESH FACT

97% believe they meet their objectives in identifying and assessing risks

The data shows that certain actions are harder to do well. For example:

19% feel they are not effectively monitoring and conducting automated control testing.

23% are not confident in their processes for flagging exceptions, reviewing, and remediating issues.

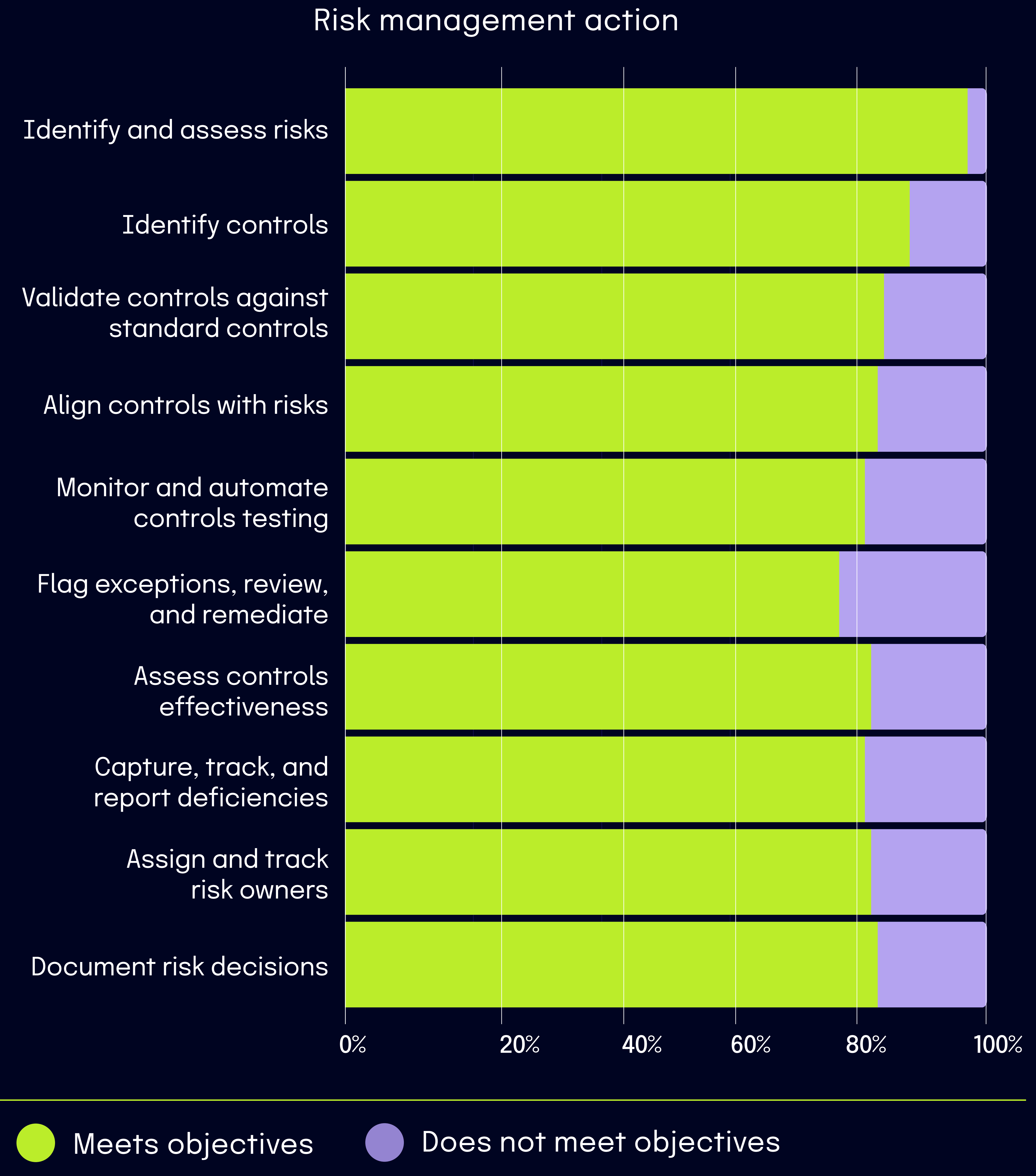
19% are not fully satisfied with their process for assessing controls' effectiveness and capturing, tracking, and reporting deficiencies.

18% report they have room for improvement in assigning and tracking risk owners.

17% said they're not meeting objectives when documenting risk decisions.

While companies are proficient in initial risk identification and assessment, there is room for improvement when implementing and monitoring controls, documenting controls, and remediating controls.

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



2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

Using integrated tools to manage IT risks may reduce the likelihood of a data breach

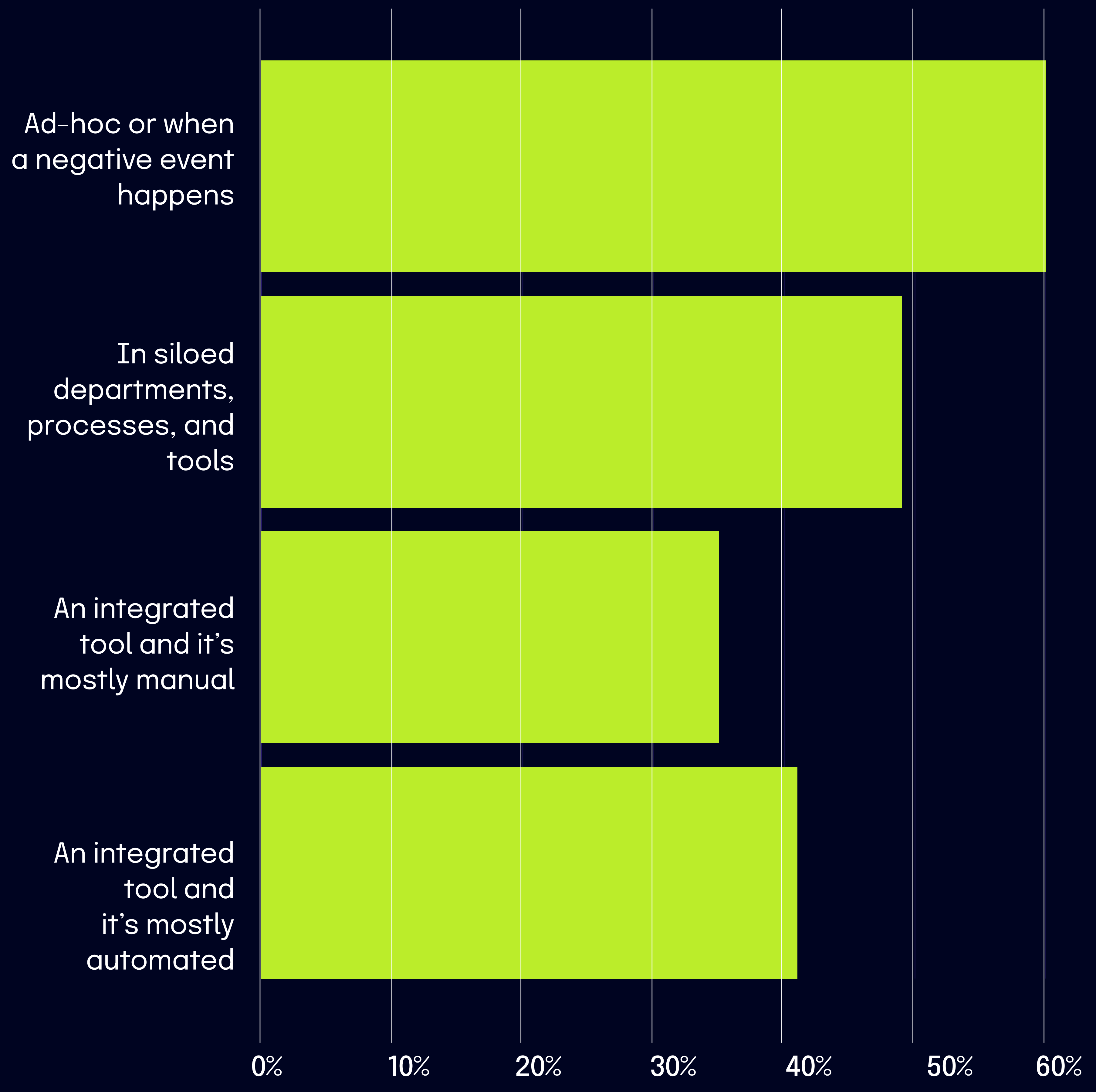
Organizations using integrated tools to manage IT risk are less likely to experience data breaches. In 2024, 60% of organizations managing IT risk ad-hoc or when a negative event happens experienced a data breach, compared to only 35% using an integrated, mostly manual tool and 41% using an integrated, automated tool.

FRESH FACT

60% of organizations managing IT risk ad-hoc or when a negative event happens experienced a data breach in 2024

Has your organization experienced a data or privacy breach in the last year?

A: Yes
By IT risk management approach



2025 IT and Risk Compliance Benchmark Report

hyperproof.io/it-compliance-benchmarks

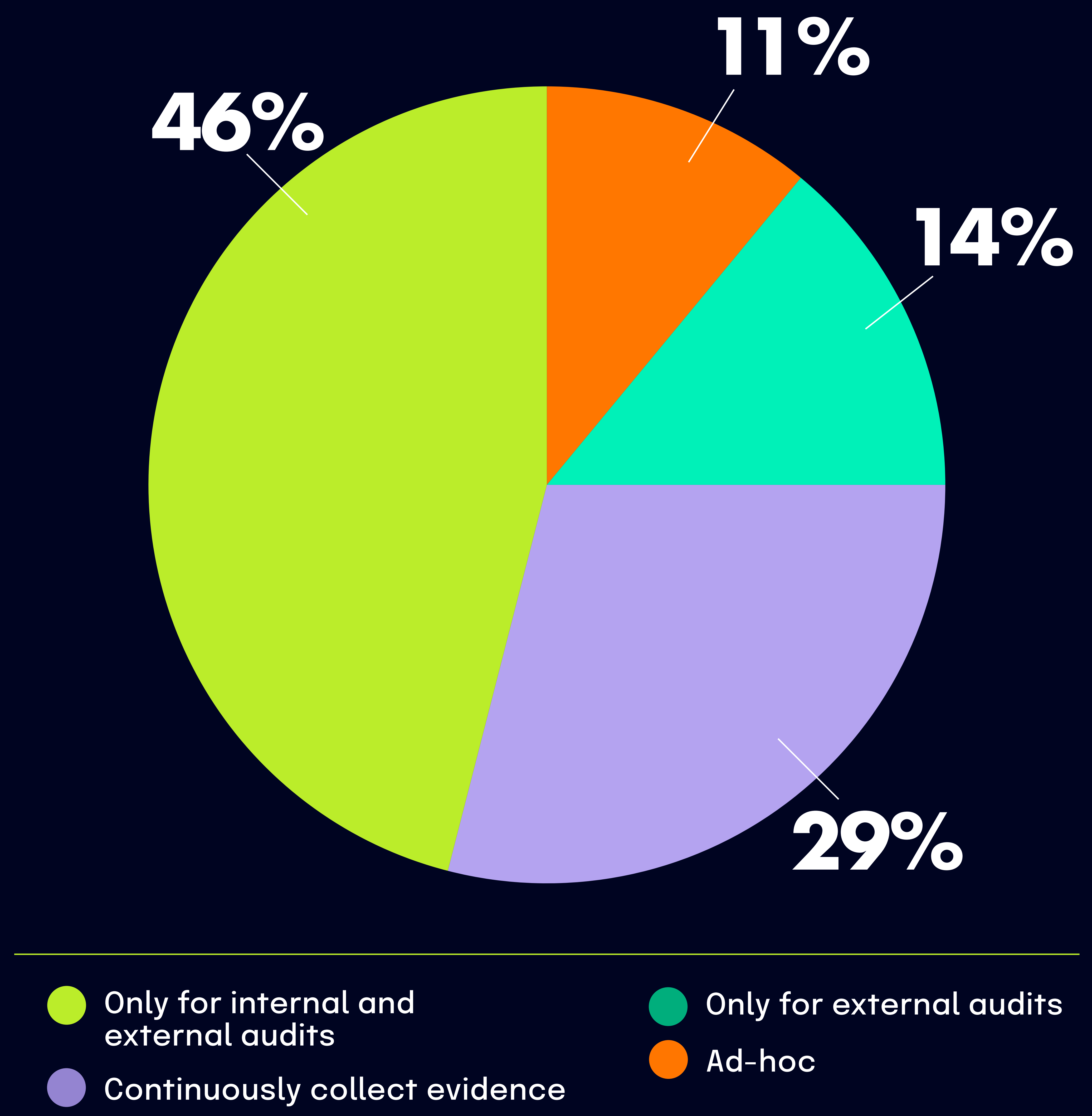
Evidence collection habits

A surprising majority of companies (71%) still take a reactive approach to evidence collection, gathering evidence ad-hoc or only for audits. This approach can have long-term efficiency impacts, due to teams spending the majority of their time on menial tasks instead of strategic work.

FRESH FACT

71% still take a reactive approach to evidence collection, gathering evidence ad-hoc or only for audits

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



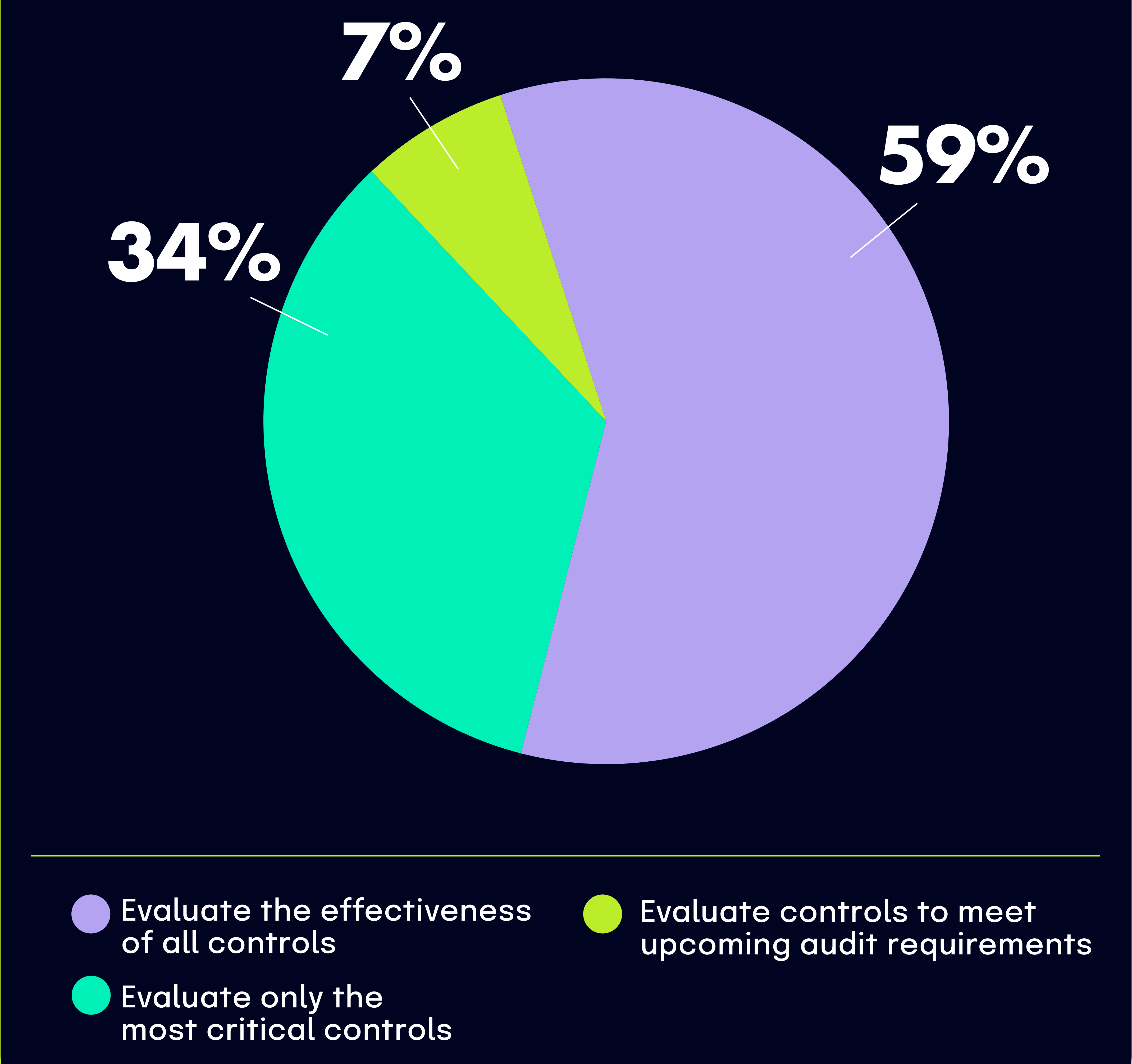
2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

Control testing and monitoring trends

Another example of the push to greater maturity is the shift from testing only a subset of controls to testing all of their controls. **This year, 59% of respondents reported that they test all controls instead of only the most critical controls, an increase of 26% year-over-year.** Several factors could be contributing to this shift, including:

- The fact that mature organizations recognize that vulnerabilities can exist in any part of their control environment, not just in critical areas
- Mature organizations are more likely to prioritize continuous monitoring and regular testing
- The increased adoption of a common control framework (CCF), which limits the number of controls needed to be tested
- The increased adoption of technology that reduces the overall control testing burden

What best describes your organization's approach to evaluating the effectiveness of security and compliance controls?

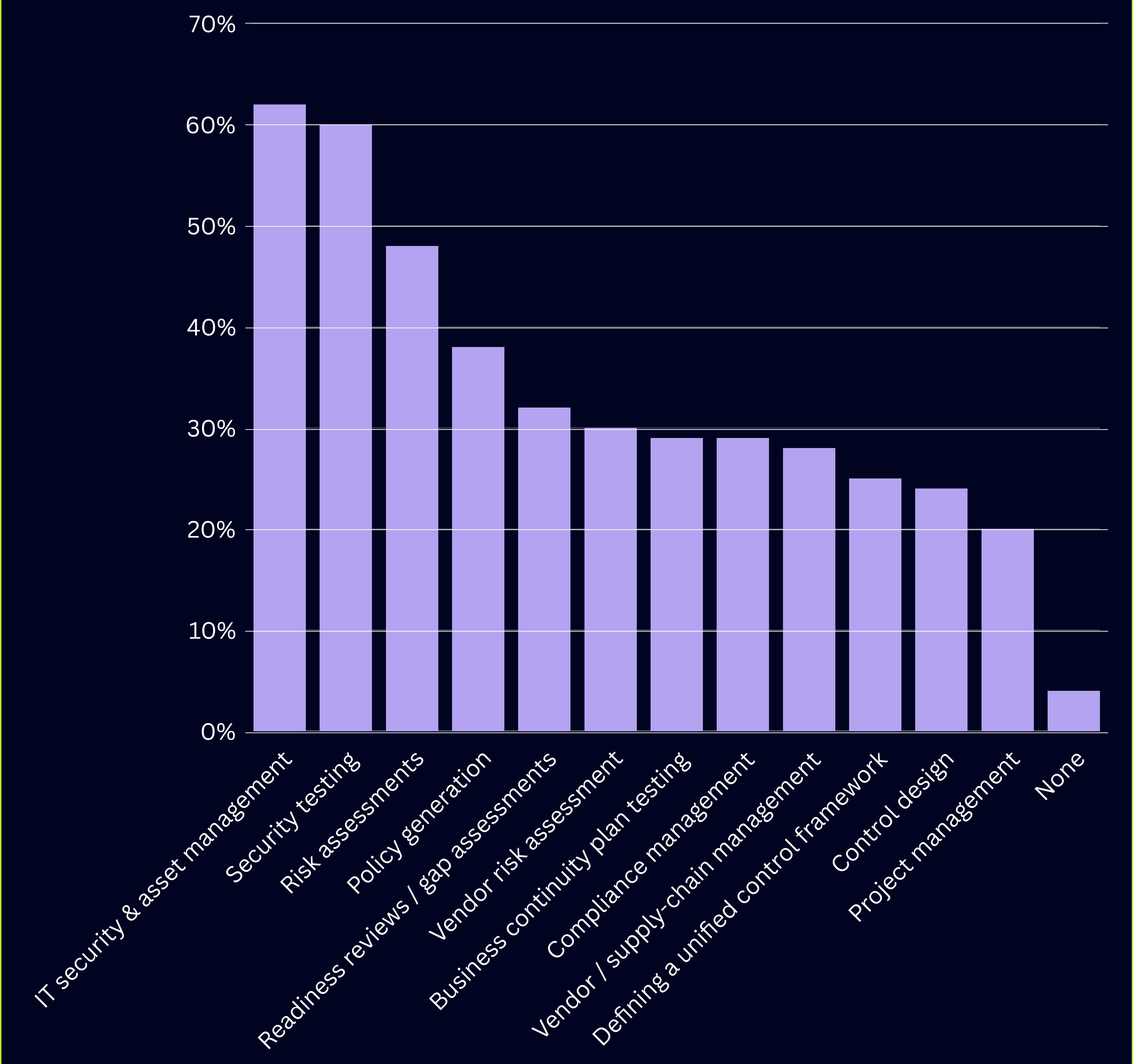


2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

Risk and compliance services outsourced

While organizations surveyed spend most of their budgets on building internal capabilities, they recognize the strategic value external specialists can provide. Organizations will most likely outsource IT security, asset management, and risk assessments to strengthen cybersecurity resilience in response to growing threats. Many also turn to consulting firms for policy generation and compliance management to navigate the complexities of evolving regulatory frameworks, likely because they balance compliance and risk management needs with internal capacity limitations. The GRC space also faced hiring freezes in 2024, which could have led to increased reliance on outsourcing. Additionally, the industry experienced a shortage of IT professionals last year, which could drive the need to outsource. *ISC2's 2024 Cybersecurity Workforce Study* found that the size of the active cybersecurity workforce only grew 0.1% in 2024, compared to 8.7% the previous year.

What services do you outsource to consulting/security and compliance advisory firms?

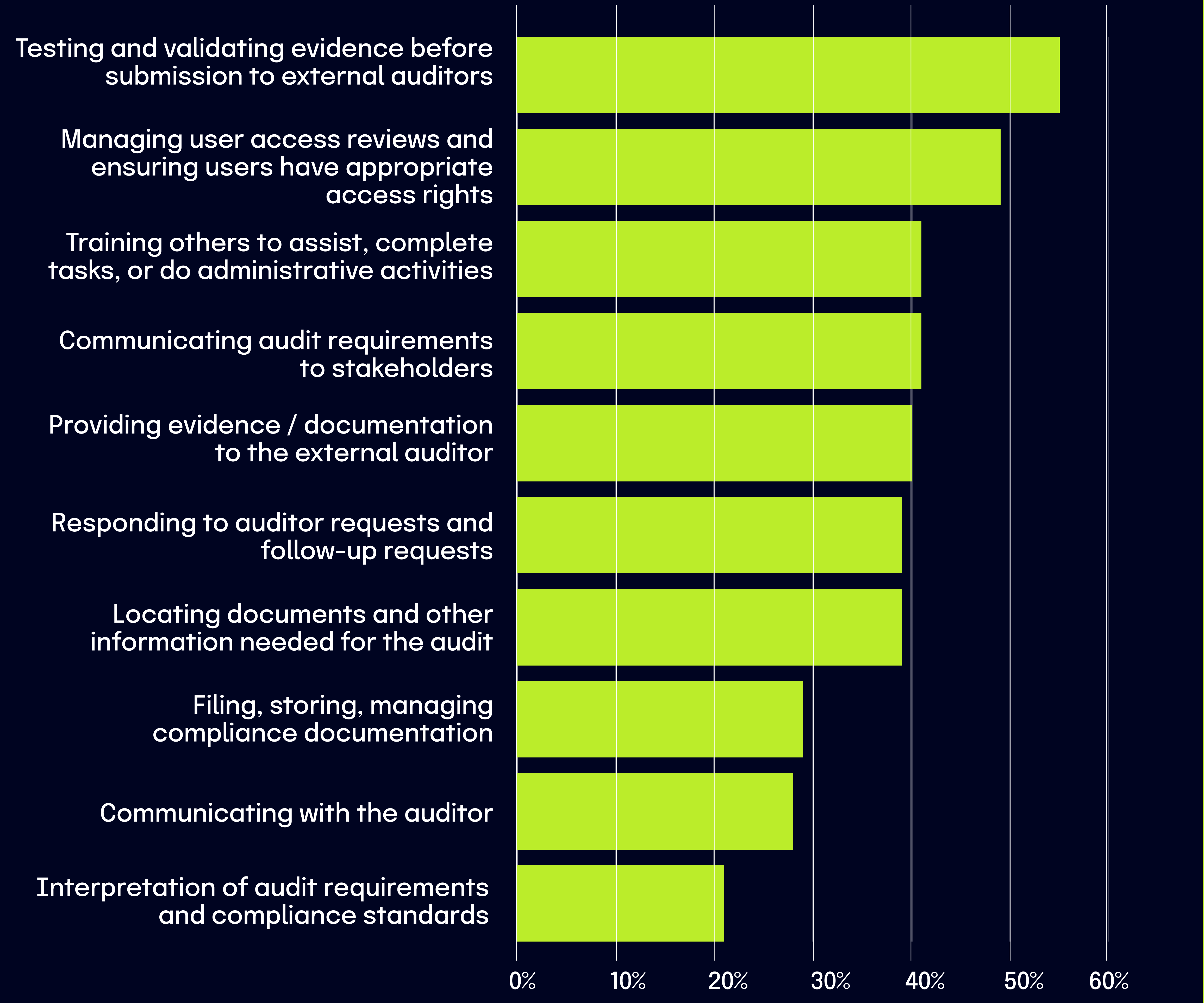


2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

Audit challenges

The greatest burden on passing audits and verifying compliance is related to evidence validation, user access, communication, and document management. These challenges highlight the complexities of audits and their strain on teams: they are all time-consuming, resource-intensive processes that reflect GRC teams' ongoing challenges.

When it comes to preparing for and executing audits, what tasks do you find to be tedious or take longer than you'd like?

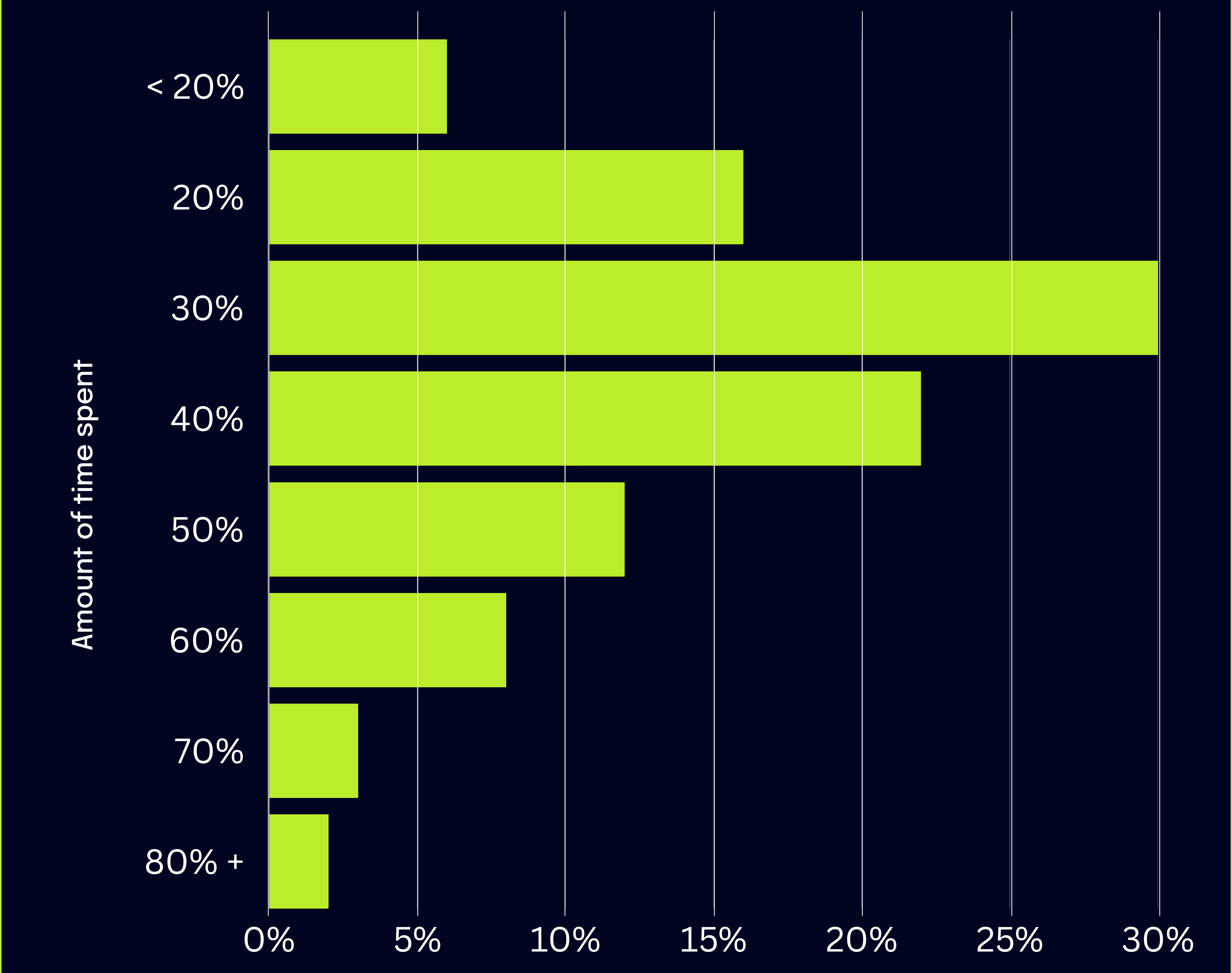


2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

Administrative work and repetitive tasks

For many organizations, administrative work remains a significant burden, with 52% of respondents estimating their teams spend between 30% and 50% of their time on these tasks. This suggests substantial opportunities for efficiency gains through automation or process improvements exist.

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



2025 IT and Risk Compliance Benchmark Report

hyperproof.io/it-compliance-benchmarks

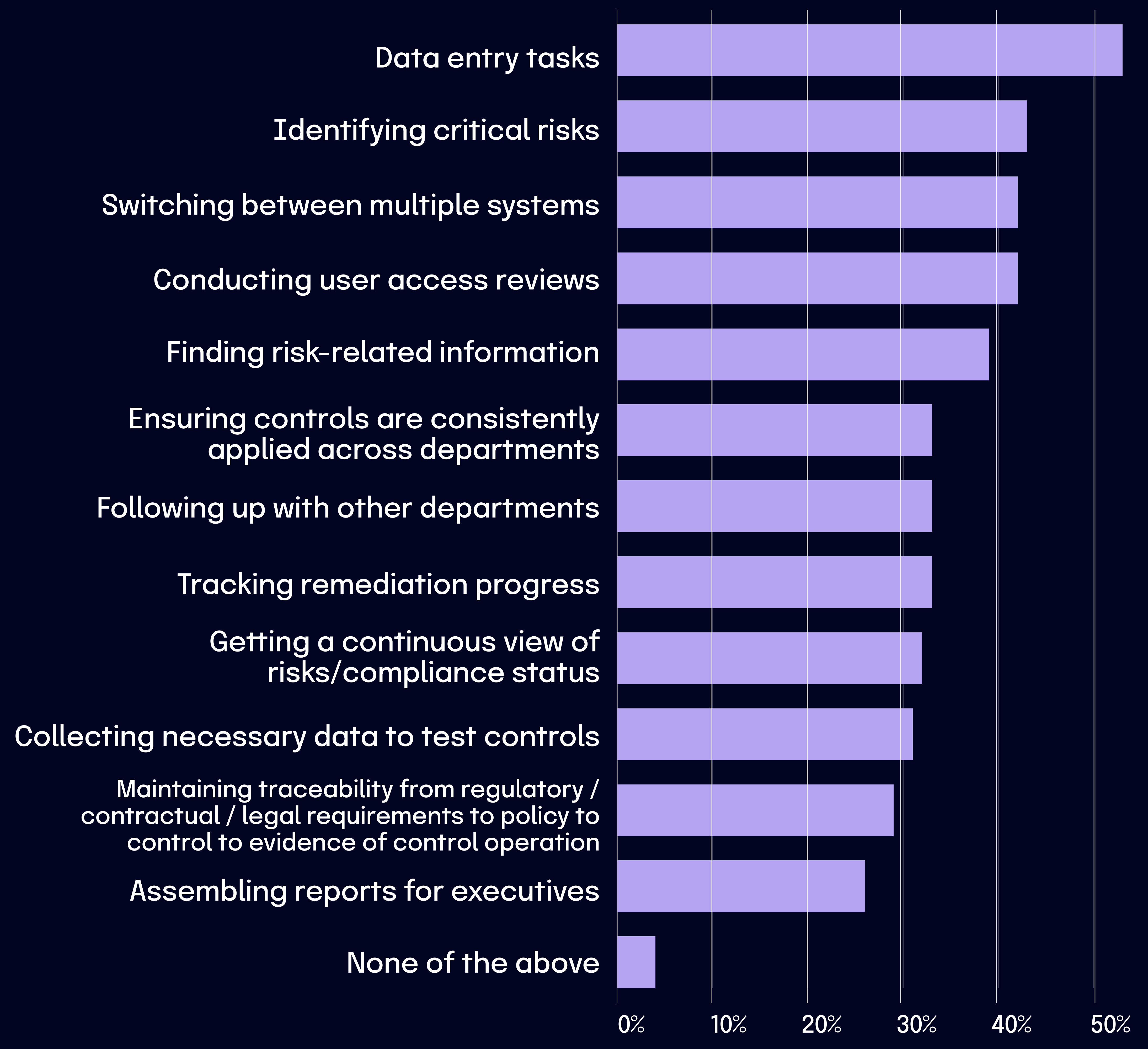
Hidden inefficiencies of GRC

Despite efforts by GRC teams to streamline workflows, adopt new processes, and better integrate their work, our respondents stated that their work is still burdensome and certain tasks are too laborious.

The most challenging and tedious risk-related work items can be categorized under four themes:

- Data entry, including tracking risk decisions or entering the status of a risk item
- Having to switch between too many systems to complete a single process
- Making sense of disparate data sources and systems to identify where the critical risks are and what caused the risk
- Managing user permissions and conducting user access reviews

What recurring or time-consuming tasks do you struggle with when managing security and data privacy risks?



2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

IT risk management and compliance tools

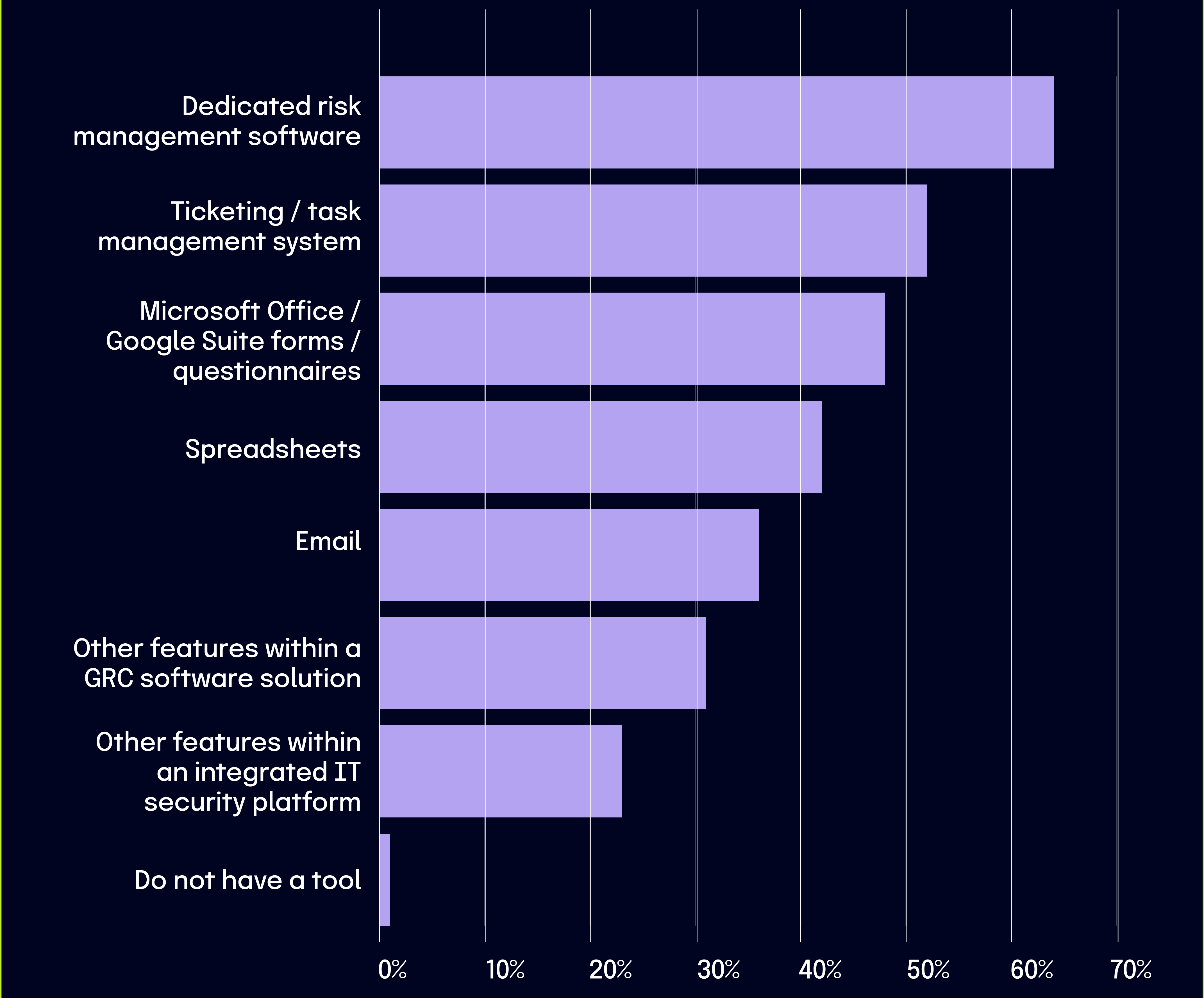
GRC teams are leaning toward using integrated, automated tools for risk tracking, decision-making, validating controls, testing evidence, and much more. **This year, there is a notable preference for dedicated or integrated software solutions, including the automation features respondents need to operationalize their processes over manual or legacy methods**. This push toward operationalization indicates that respondents use technology to strategically address areas of GRC that have traditionally been managed via ad-hoc manual processes.

> This year, there is a notable preference for dedicated or integrated software solutions, including automation features respondents need to operationalize their processes.

Types of tools adopted by GRC teams

The most commonly used tools include dedicated risk management software (64%), ticketing/task management systems (52%), and forms or questionnaires created in office productivity suites like Microsoft Office or Google Suite (48%). Spreadsheets are still widely used by 42%, while email is used by 36%. Only 1% reported not using any tool for this purpose.

What tools are you using to track risk owners?



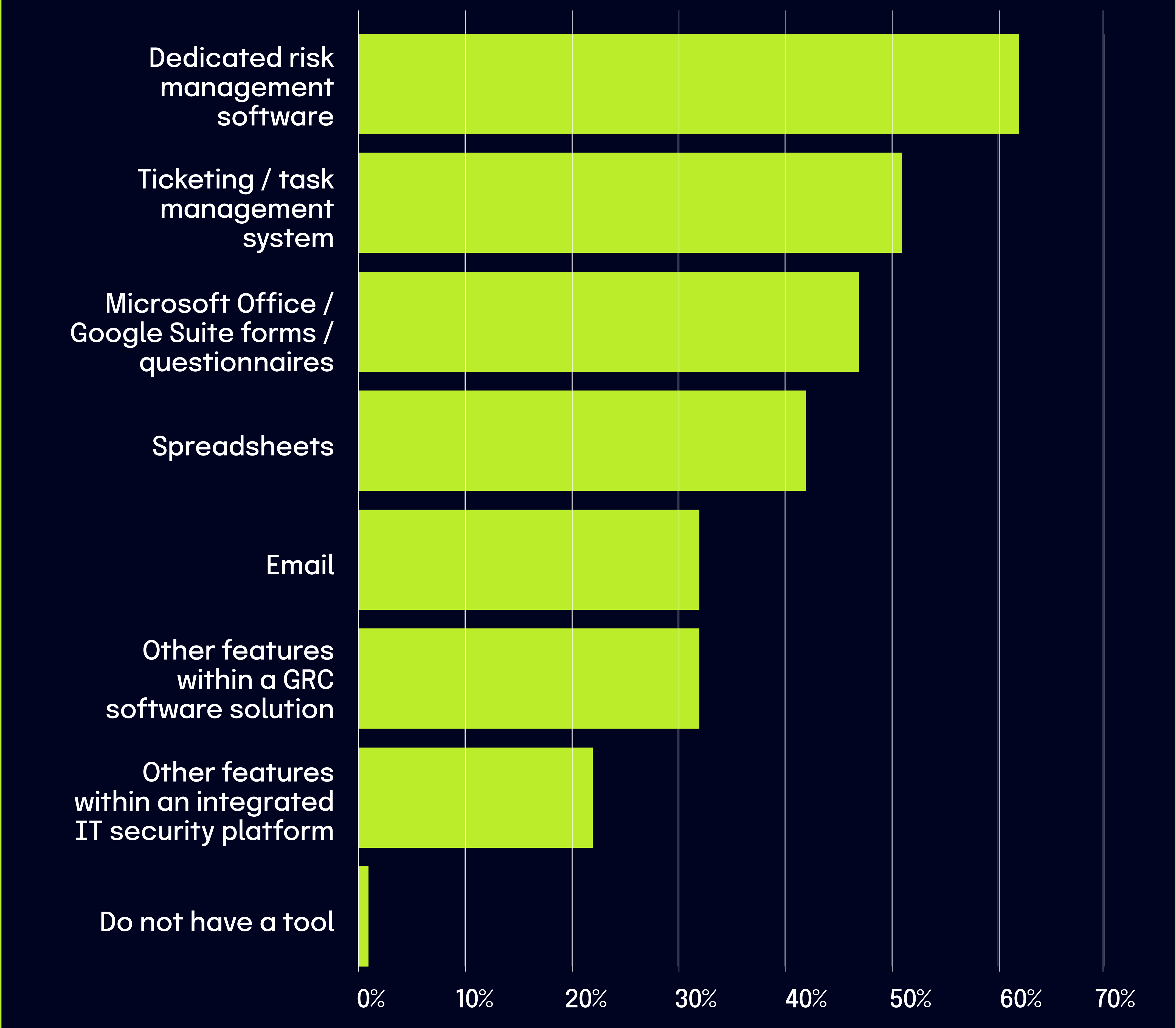
2025 IT and Risk Compliance Benchmark Report

hyperproof.io/it-compliance-benchmarks

Risk decision-tracking tools

When documenting decisions such as accepting, mitigating, transferring, or ignoring risks, 62% of organizations rely on dedicated risk management software. Ticketing/task management systems (51%) and forms/questionnaires (47%) also see frequent use. Spreadsheets remain common at 42%, while 32% use email and 1% do not use any tools for this task.

What tools are you using to track decisions based on risks, such as acceptance, mitigate, transfer, or ignore?



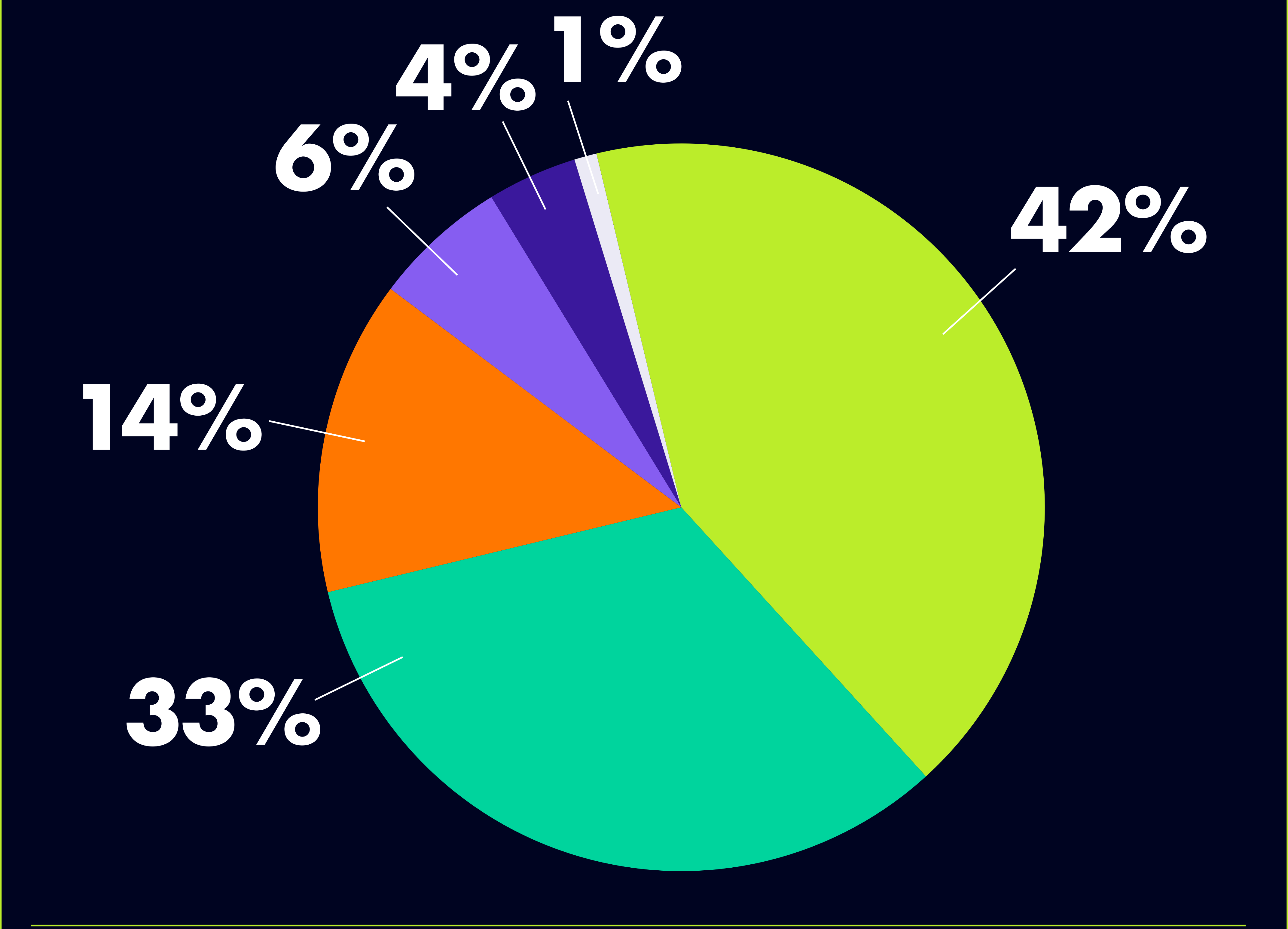
2025 IT and Risk Compliance Benchmark Report

hyperproof.io/it-compliance-benchmarks

IT compliance management tools

For tasks such as completing security audits and monitoring controls, 42% use a compliance module within cloud-based GRC software, and 33% rely on purpose-built software for managing IT compliance operations. Spreadsheets and file storage systems are less prevalent, used by only 14%. On-premises GRC software (6%) and custom-built software (4%) see limited use, with 1% reporting no tool usage.

What tools are you using to manage your IT compliance effort (e.g. completing security audits for certifications like SOC 2, ISO 27001, PCI, etc., testing and monitoring controls)?



- ● Compliance module in a cloud-based GRC software
- ● Purpose-built software for managing compliance
- ● Spreadsheets, Word docs, and/or file storage systems
- ● Compliance module in an on-prem GRC software
- ● Custom-built software
- ○ Do not have a tool

2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

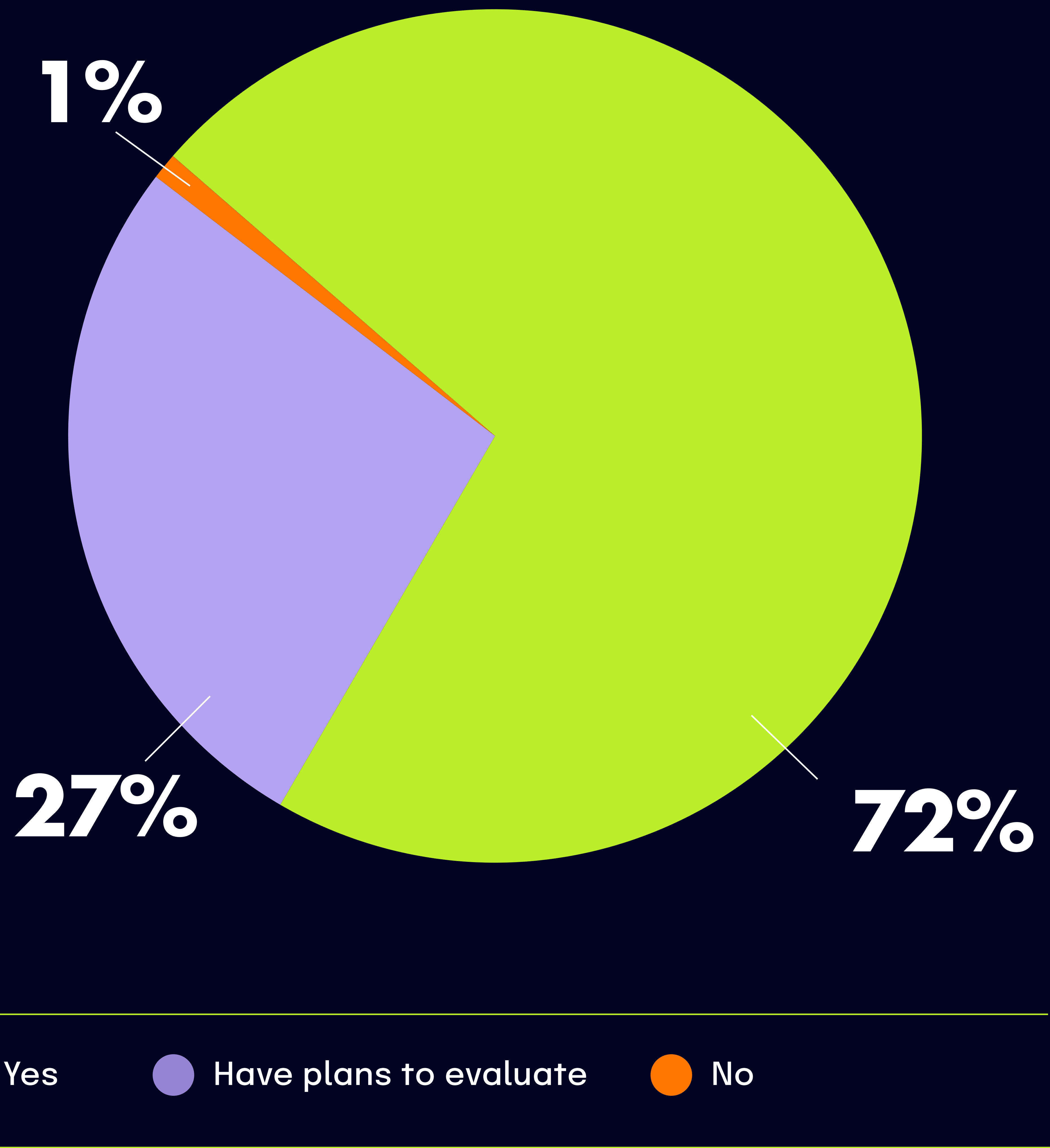
Continuous control monitoring tools

Our respondents reported widespread adoption and growing interest in continuous controls monitoring software, which automatically evaluates the effectiveness of security controls and compliance status across an organization's assets and attack surface. 72% of organizations report using software that monitors security controls and provides compliance posture reporting. This high adoption rate reflects the growing reliance on automated solutions to streamline compliance efforts and reduce cyber risks.

FRESH FACT

72% of organizations report using software that monitors security controls and provides compliance posture reporting

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



2025 IT and Risk Compliance Benchmark Report

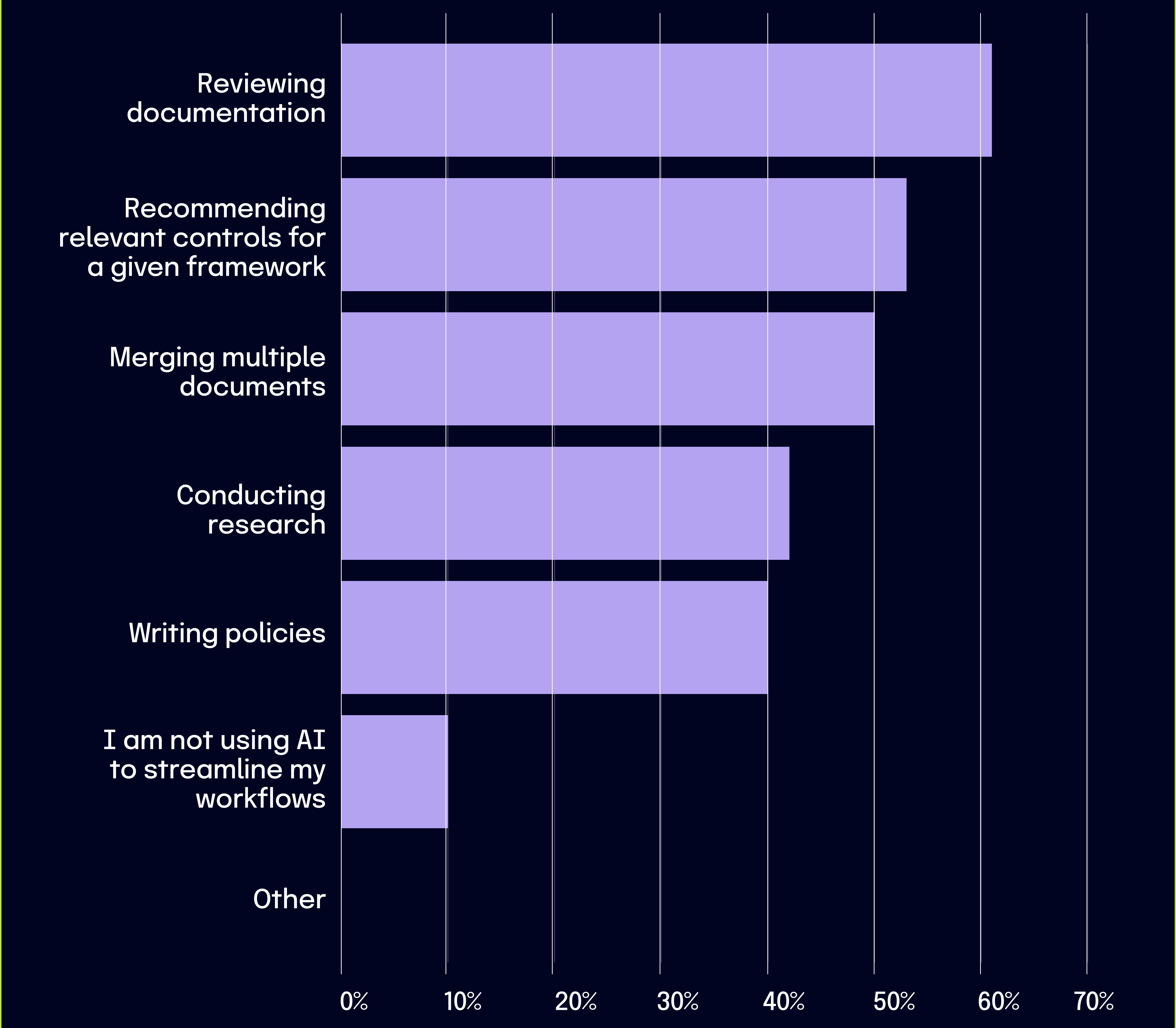
hyperproof.io/it-compliance-benchmarks

AI risk: an emerging concern and a force accelerator

Use cases for generative AI tools in GRC

90% of respondents use generative AI (genAI) tools in one or numerous ways to boost productivity, reduce manual processes, and streamline workflows. The most widely adopted use of AI is in reviewing documentation (61%), followed by recommending relevant controls for frameworks (53%), merging multiple documents (50%), conducting research (42%), and writing policies (40%). These applications demonstrate AI's ability to automate tasks such as generating policy drafts, ensuring consistency, and providing contextual recommendations, significantly reducing effort and enhancing efficiency. For example, AI expedites policy creation by analyzing regulatory frameworks and organizational needs to produce robust and tailored policies while freeing time to focus on strategic tasks like stakeholder alignment and risk mitigation. **Only 10% of respondents are not using AI to streamline their workflows**, emphasizing AI's growing role as a transformative enabler in GRC processes.

Are you using AI to streamline any of the following workflows?

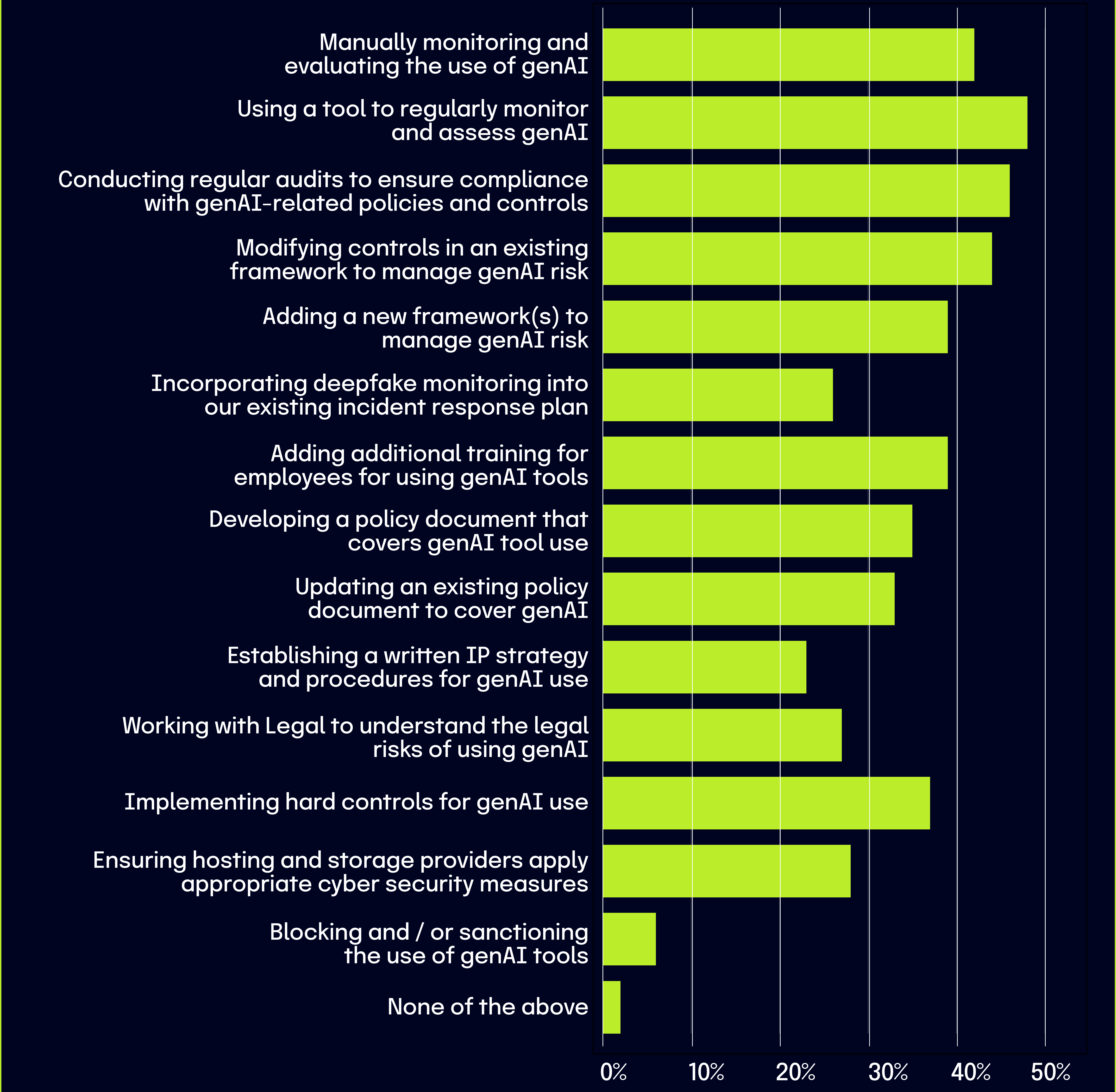


2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

Keeping AI risk management top-of-mind

While respondents recognize the benefits of using AI tools, they're also keeping risks in mind. This year, we saw organizations' understanding of AI risks maturing, evidenced by many implementing sophisticated practices to monitor and mitigate AI risks. A significant portion of organizations plan to actively monitor AI usage, with 42% manually monitoring and 48% using tools to automate this process. This indicates a dual approach, balancing human oversight with technology-driven solutions. 46% plan regular audits to ensure compliance, showcasing a strong emphasis on governance and accountability. Only 39% reported adding additional training for employees on the responsible use of generative AI tools in 2024, which is low considering that the EU AI Act mandates that companies train their employees on the risks of AI from February 2nd, 2025, and onward.

What policies or procedures do you plan on putting in place to mitigate business risk associated with AI and genAI tools in 2025?



2025 IT and Risk Compliance Benchmark Report

hyperproof.io/it-compliance-benchmarks

CHAPTER 4

Third-Party Risk: The Ever-Expanding Threat Vector

Managing third-party risks has become a cornerstone of effective GRC programs as organizations expand their tech stacks and increasingly rely on external vendors, suppliers, and partners to drive innovation. While many have adopted best practices, including those outlined by NIST CSF, significant vulnerabilities remain. This year's survey revealed that **only one in five organizations have yet to fully implement these practices**, showcasing that the majority are taking this risk seriously. However, the data also shows that while these practices reduce your risk level, they do not entirely prevent the risk, with 55% of those who adopted these best practices suffering supply chain issues and 46% experiencing a breach.

As you explore this section of the report, consider the dual realities it reveals: the progress made in aligning with leading frameworks like NIST CSF and the critical gaps that remain. Addressing third-party risks requires more than adopting best practices – **it demands consistent execution, vigilant oversight, adoption of new technologies, and a commitment to continuous improvement**. The third-party risk landscape is only growing, and organizations must redouble their efforts to safeguard their supply chains, protect sensitive data, and ensure compliance across their extended networks.

Addressing third-party risks requires more than adopting best practices – it demands consistent execution, vigilant oversight, adoption of new technologies, and a commitment to continuous improvement.

Approaches to managing third-party risk

To find out what organizations do tactically to address third-party risks, we asked respondents whether they are following best practices for managing cyber risks using best practices outlined by NIST CSF for managing cyber risks from suppliers and third-party partners.

We saw year-over-year improvements across all areas of third-party risk management, reflecting a maturing landscape where organizations progressively close gaps in their supply chain security practices.

There are several reasons why respondents reported such significant improvements to third-party risk management. →

Growing awareness: Organizations increasingly recognize third-party risks' interconnected nature within their supply chains.

Standardization of practices: Organizations are moving from conceptual understanding to actionable, integrated implementation of GRC strategies.

Enhanced collaboration: The increased response and recovery planning underscores the importance of shared responsibility and coordinated efforts with suppliers.

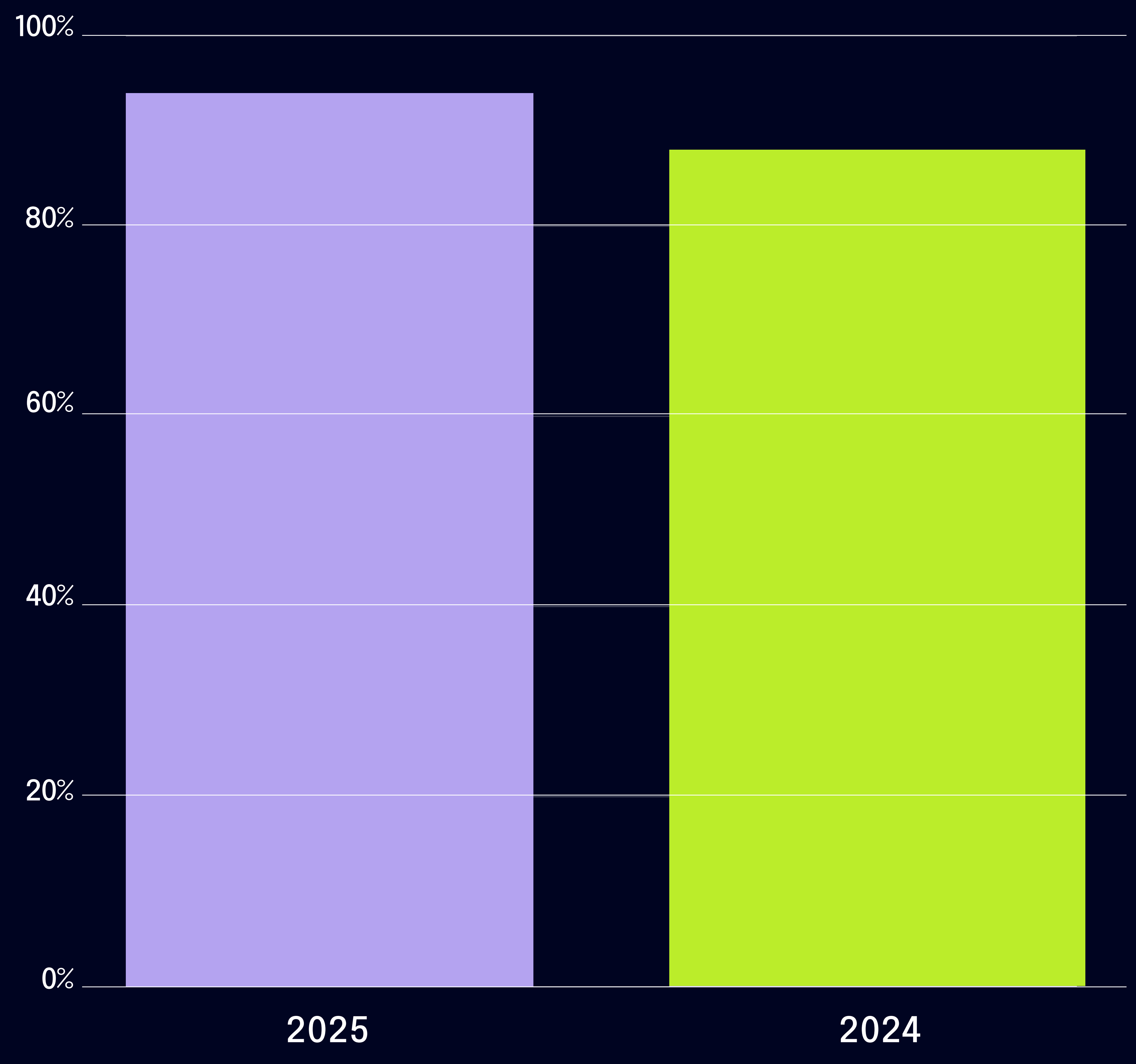
Year-over-year, the proportion of organizations aligning stakeholders in their supply chain risk management processes rose from 88% to 94%. This reflects a continued commitment to collaboration and strategic planning, signaling that organizations are continuing to see the benefits of a unified approach to cybersecurity risk challenges.

FRESH FACT

94% of organizations report aligning stakeholders in their supply chain risk management

Does your organization identify, establish, assess, and manage supply chain risk management processes to ensure stakeholders agree?

A: Yes



2025 IT and Risk Compliance Benchmark Report

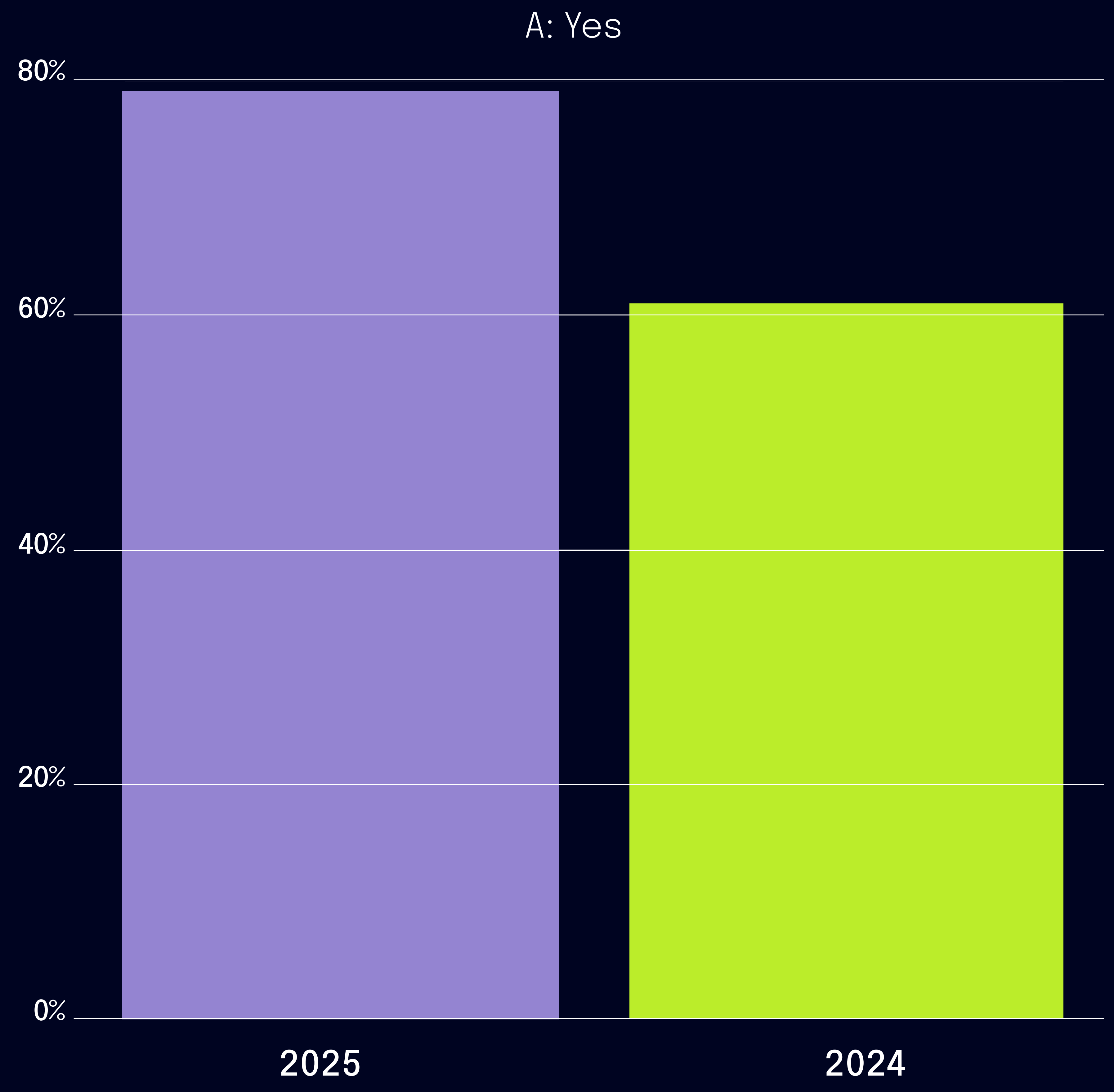
hyperproof.io/it-compliance-benchmarks

We also saw a notable increase in the use of cyber supply chain risk assessments, which grew from 61% to 79% year-over-year. This significant improvement suggests that organizations are not only recognizing the importance of assessing their suppliers but are also operationalizing these assessments more effectively.

FRESH FACT

26% year-over-year increase in the number of respondents using a cyber supply chain risk management process

Does your organization identify, prioritize, and assess suppliers and third-party partners of systems, components, and services using a cyber supply chain risk assessment process?



2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

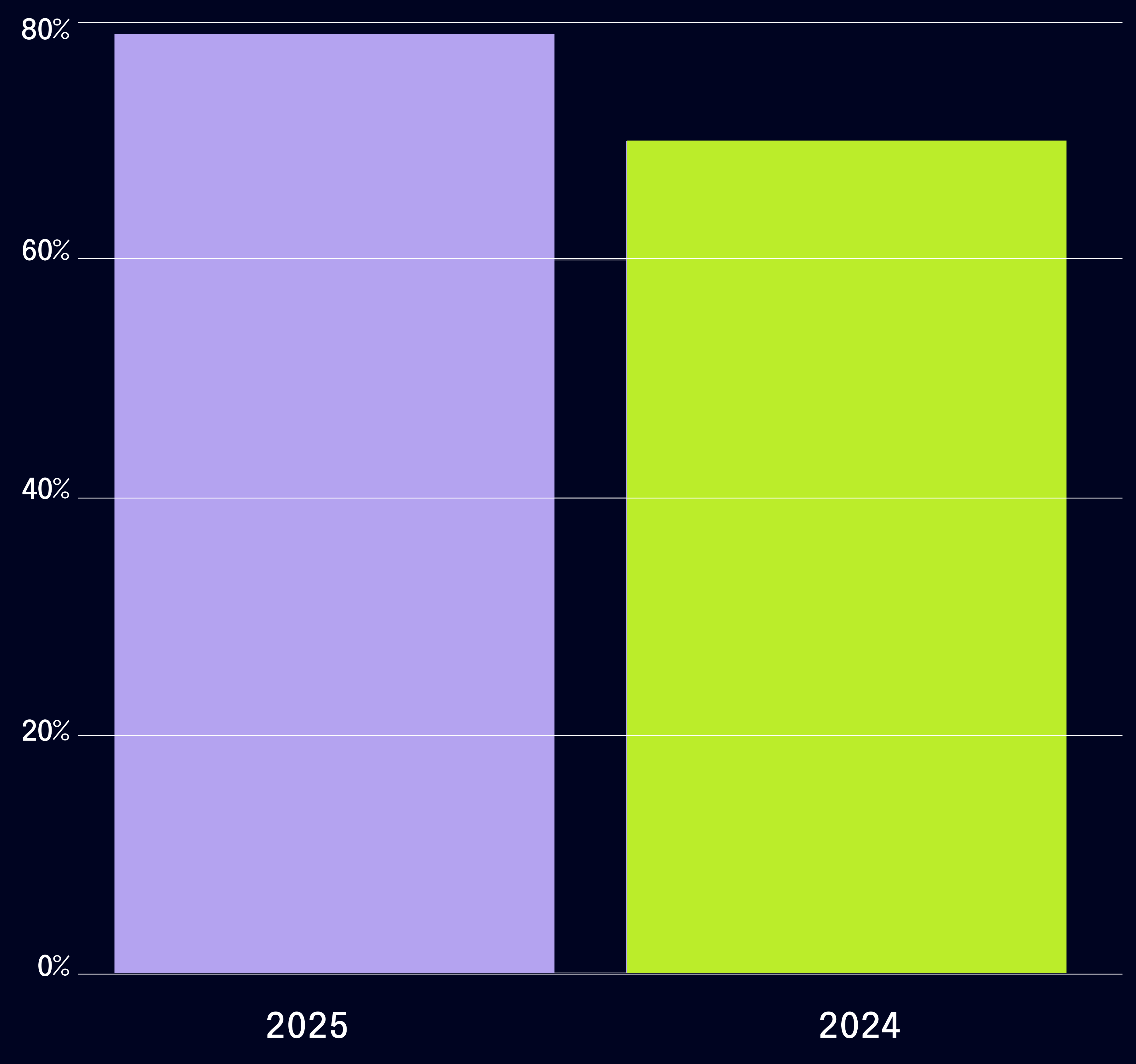
The percentage of organizations implementing cybersecurity measures in third-party contracts also climbed from 70% to 78%, signifying a stronger focus on ensuring that cybersecurity expectations are clearly enforced through formal agreements. Routine assessments of suppliers and third-party partners increased from 70% to 77% as well, highlighting a growing emphasis on continuous monitoring and accountability.

FRESH FACT

78% of organizations report implementing cybersecurity measure in third-party contracts

Does your organization implement measures in third-party partner contracts to meet cybersecurity program objectives?

A: Yes



2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

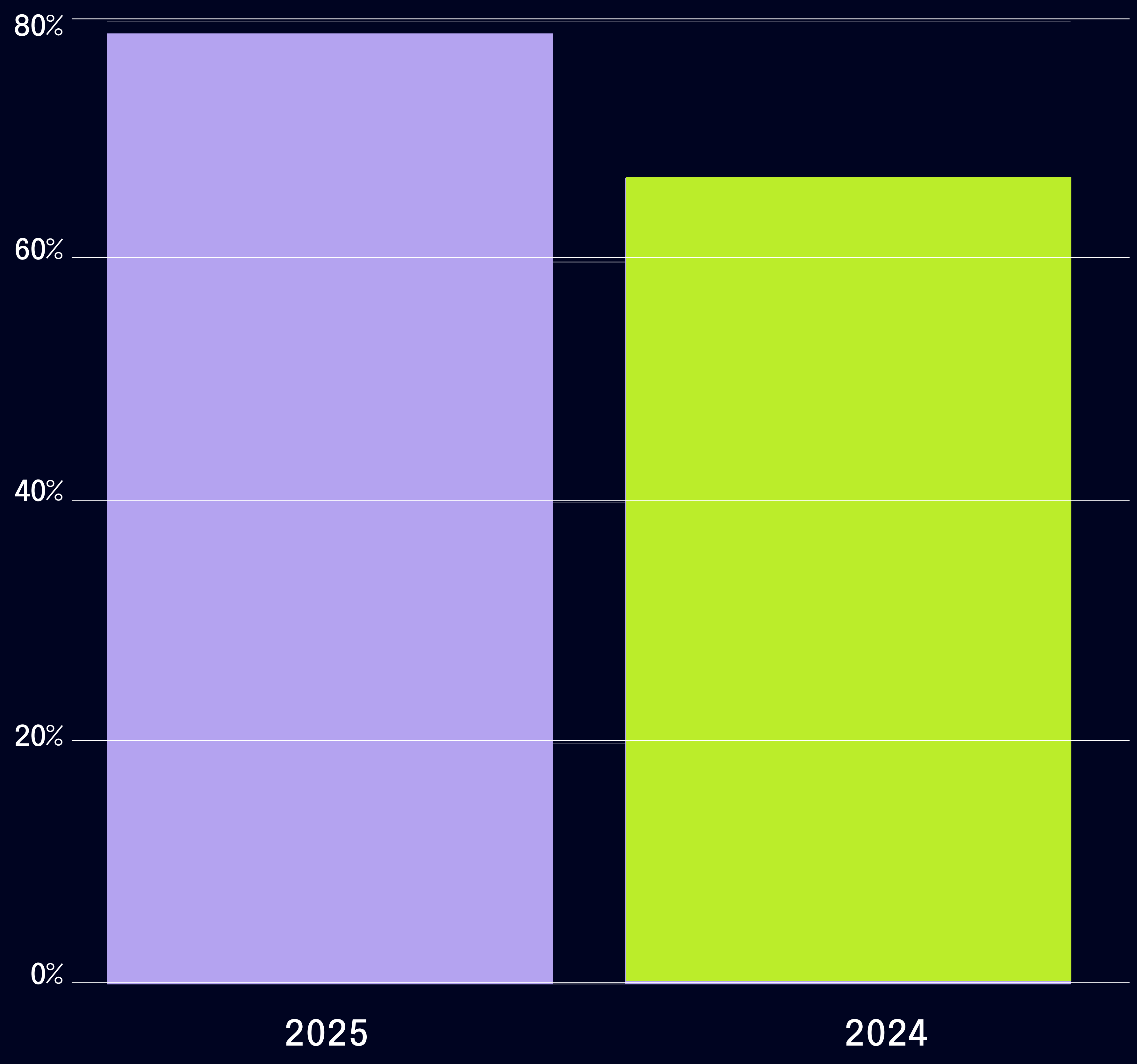
The percentage of organizations conducting response and recovery planning/testing with their suppliers jumped from 67% to 79%, indicating that organizations are more focused on preparedness and resilience in their supply chains, enhancing their ability to respond effectively to incidents.

FRESH FACT

16% year-over-year increase in the number of respondents conducting response and recovery planning and testing

Does your organization conduct response and recovery planning and testing with suppliers and third-party providers?

A: Yes



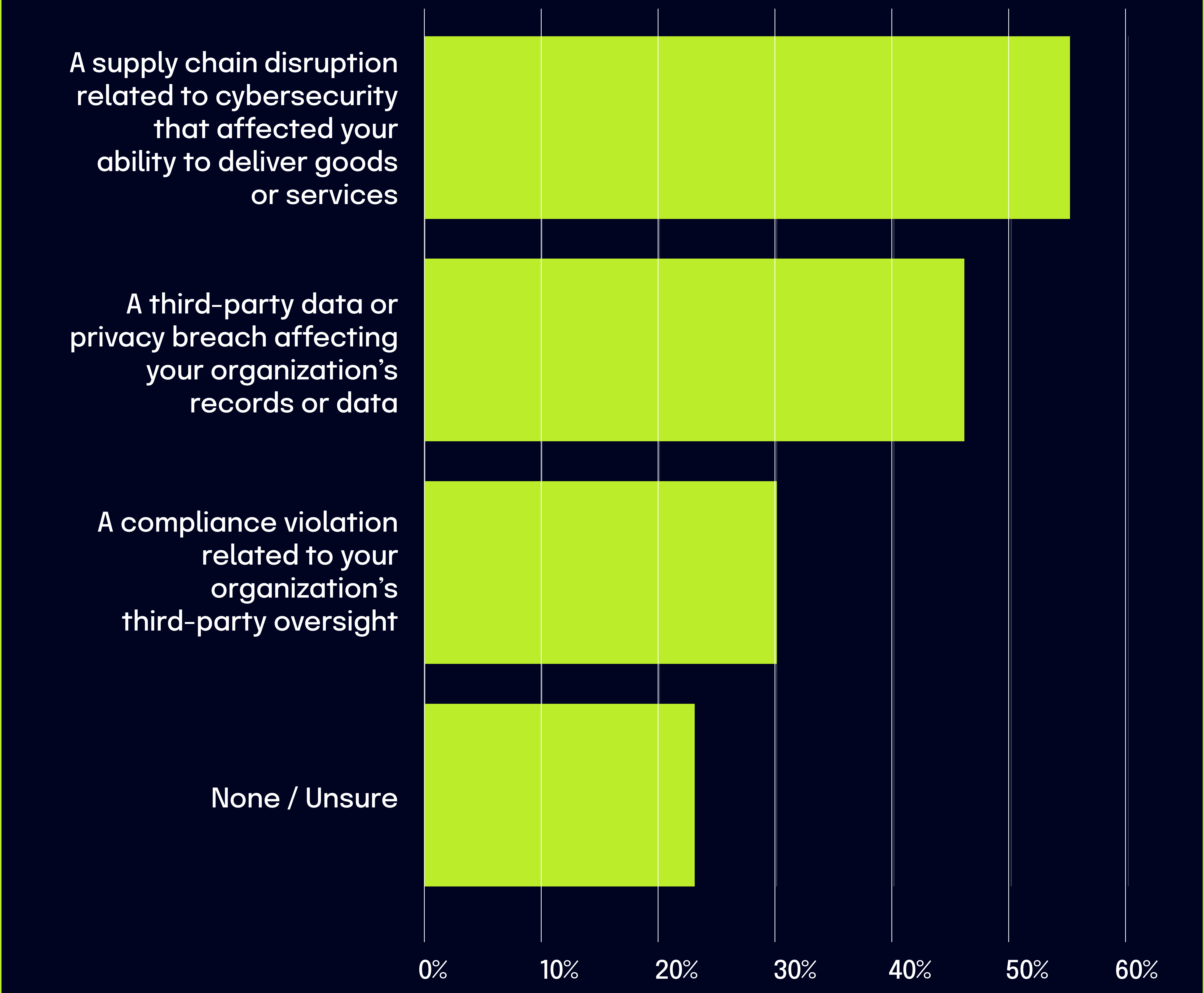
2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

Impact of third-party cyber incidents

Similar to the last couple of years, surveyed organizations in 2024 were significantly impacted by third-party cyber incidents over the past year. Notably, 55% experienced supply chain disruptions due to cybersecurity issues, affecting their ability to deliver goods or services. Additionally, 46% reported data or privacy breaches from third-party vendors, compromising their records or data. Compliance violations related to third-party oversight were noted by 30% of respondents. Conversely, 23% indicated they were either unaffected by such events or uncertain about any impacts.

To enhance resilience against such risks, all organizations must implement comprehensive supply chain risk management processes, prioritize and assess third-party risks, enforce contractual cybersecurity measures, conduct regular compliance evaluations, and collaborate on response and recovery planning with their suppliers and partners. Adopting these practices can significantly strengthen an organization's defense against cyber threats within the supply chain.

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



2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

Third-party risk management tools

Organizations use various automated and manual tools and tactics to identify and manage IT risks from third-party relationships, with the vast majority including:

78% rely on specialized VRM tools to assess, monitor, and manage these risks. Integrating third-party risk management into existing GRC platforms offers a more cohesive approach, streamlining processes and improving oversight.

49% use productivity suite forms or questionnaires to gather risk information.

42% rely on spreadsheets for tracking, reflecting a significant dependence on manual methods.

37% use ticketing and task management systems to handle third-party risk-related tasks.

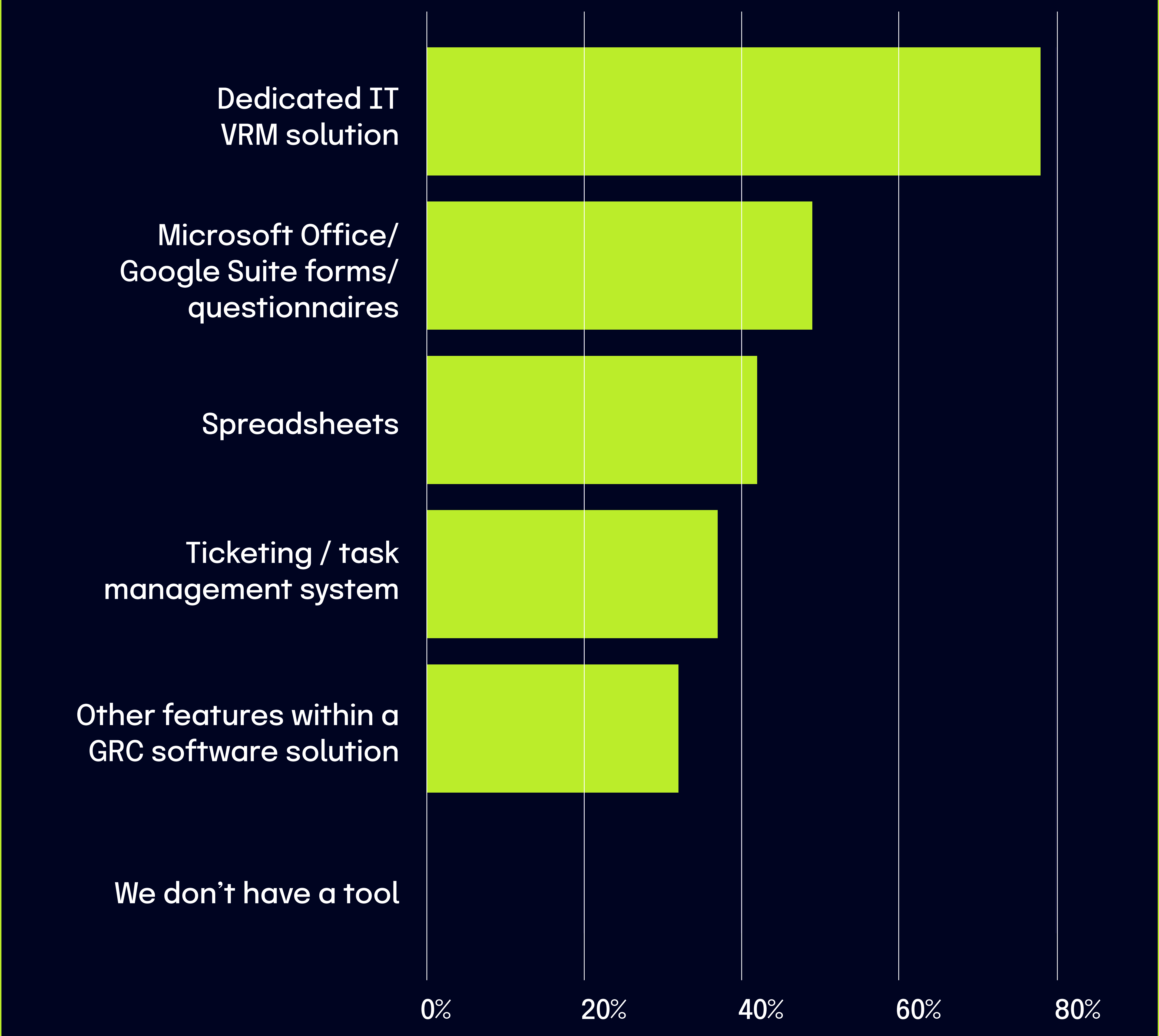
32% leverage features within broader GRC platforms to integrate these efforts into their overall strategies.

1% of respondents report not using any tools for third-party IT risk management.

The wide variety of responses showcases that third-party risk management has the greatest potential for maturity, as there is yet to be one agreed-upon response. There is also a high tax of manual efforts still associated with managing this kind of work. To enhance efficiency and scalability, organizations should adopt integrated platforms that reduce reliance on manual tools, minimize errors, and provide a comprehensive, real-time view of the risk landscape.

> To enhance efficiency and scalability, organizations should adopt integrated platforms that reduce reliance on manual tools.

What tools are you using to identify and manage IT risks arising from your third parties?



2025 IT and Risk Compliance Benchmark Report

hyperproof.io/it-compliance-benchmarks

CHAPTER 5

Budgeting: How Much Are Companies Investing in GRC and Security?

GRC and Security programs have historically been viewed as cost centers – essential, yet often begrudgingly funded. However, a paradigm shift occurred in 2024: **organizations increasingly recognize the strategic value of GRC and Security, not just as a safeguard against risks and regulatory penalties but as a key enabler of growth and market expansion**. This shift is clearly reflected in this year's survey findings, which reveal significant increases in GRC and Security budgets and a growing emphasis on technology-driven and internal capability-focused strategies.

To get the clearest picture of respondents' budgets for 2025, we asked about GRC and Security budgets separately. These two initiatives are often deeply connected but have different objectives and scope. To provide you with the most granular view of the data, you will see two sections in this chapter: one for GRC budgets and one for Security budgets.

A paradigm shift occurred in 2024: organizations increasingly recognize the strategic value of GRC and Security, not just as a safeguard against risks and regulatory penalties but as a key enabler of growth and market expansion.

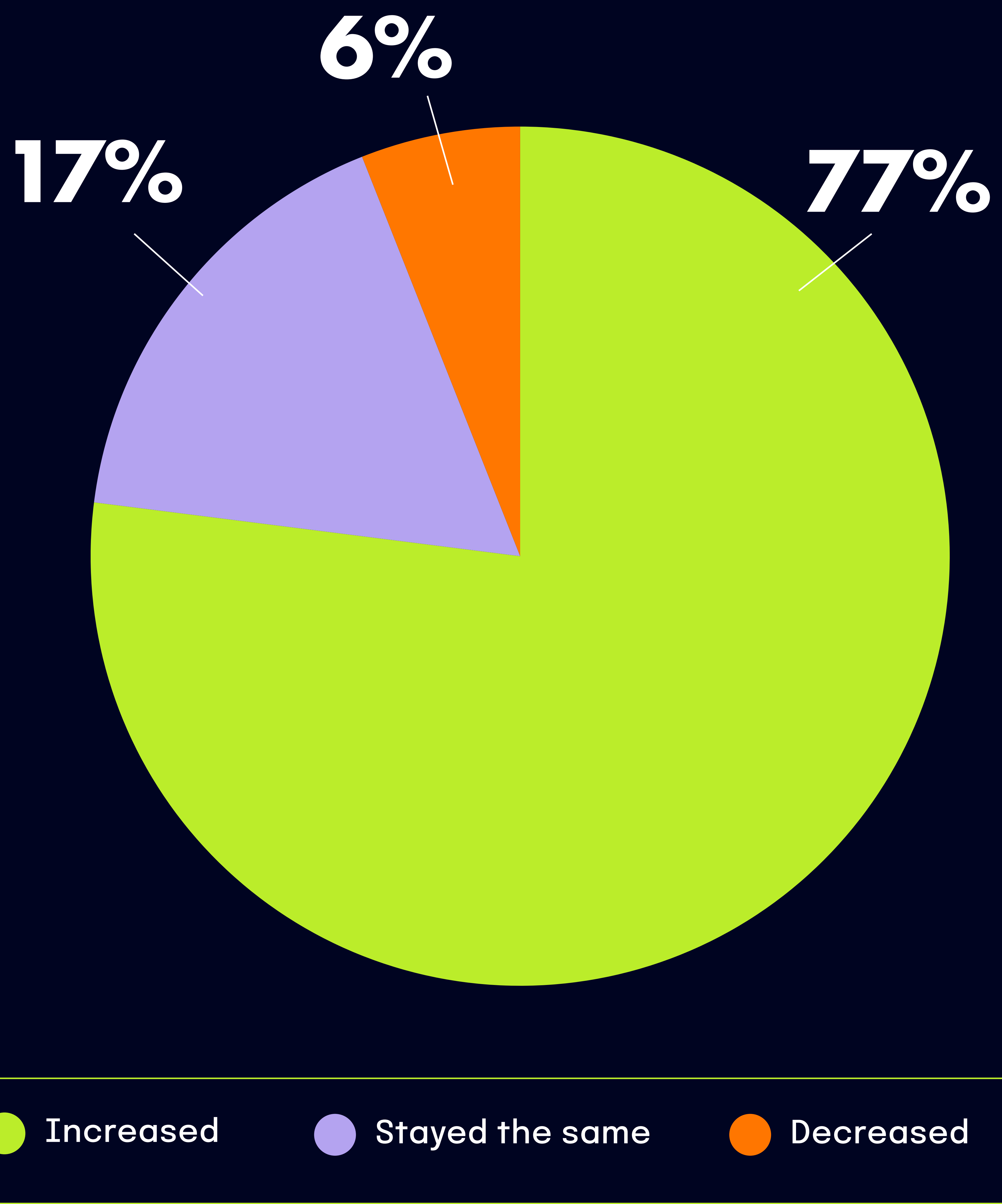
GRC Budgets in 2024

The vast majority of respondents reported that their GRC budgets increased by 77% in 2024, reflecting the ongoing shift in the way organizations view GRC. Compliance activities have traditionally been seen as a cost center, but more businesses view them as a force accelerator to unlock new markets and expand existing opportunities.

Drivers for GRC budget increases in 2024

The top driver for increased GRC budgets is revenue growth, cited by 62% of respondents. As organizations expand, their operational scale and associated risks grow, necessitating enhanced GRC investments to safeguard their business operations and maintain compliance. Growth in cloud footprint was reported by 47% of respondents as another key factor. This aligns with the increasing reliance on cloud technologies, which, while enabling agility and scalability, also introduce new risk vectors that require robust GRC oversight.

In 2024, did your GRC budget increase, decrease, or stay the same vs. 2023?



2025 IT and Risk Compliance Benchmark Report

hyperproof.io/it-compliance-benchmarks

Organizations are also grappling with a more complex and demanding regulatory environment:

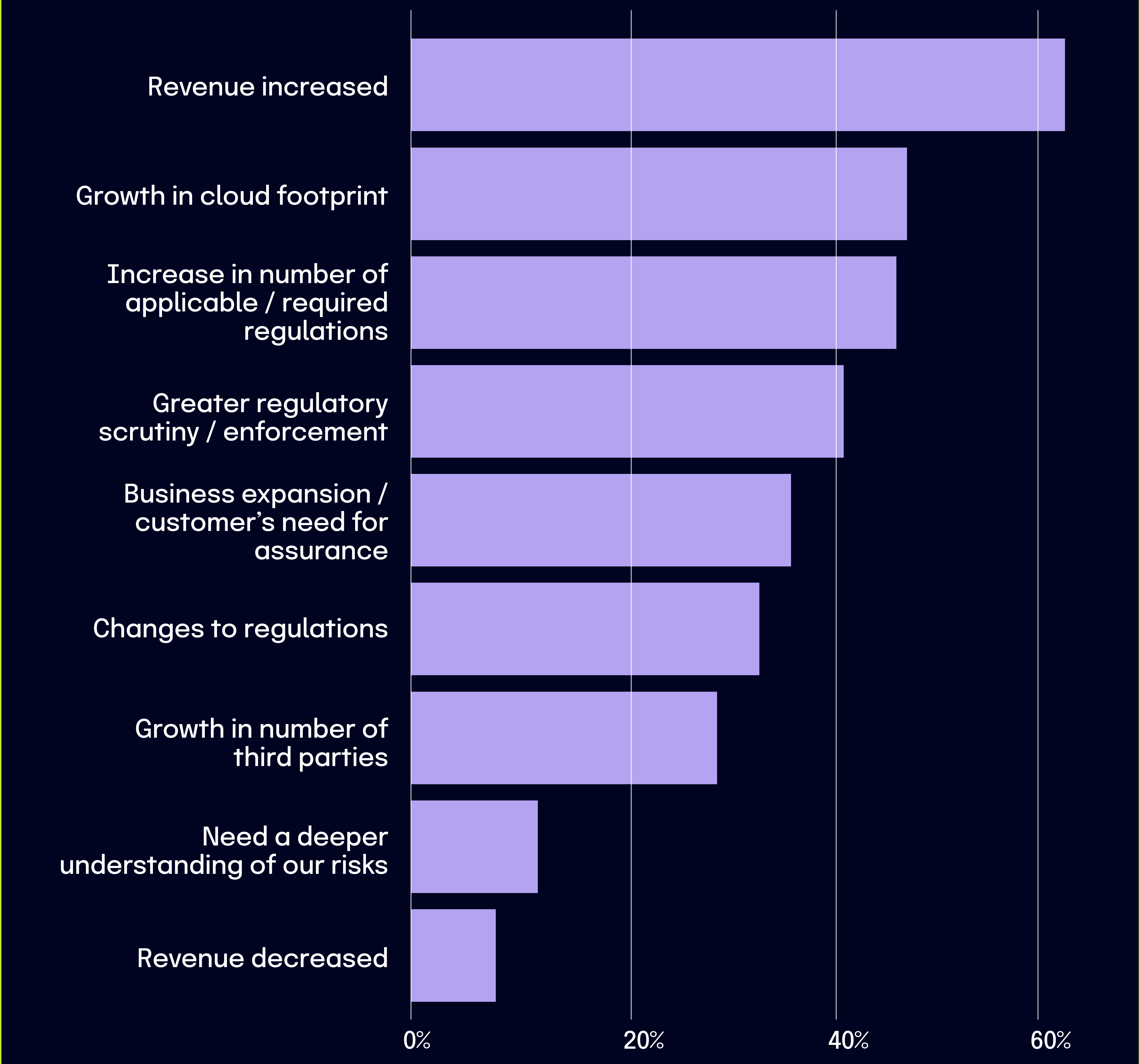
46% reported an increase in applicable or required regulations, reflecting the broadening scope of compliance obligations.

41% pointed to greater regulatory scrutiny or enforcement, underscoring the heightened vigilance of regulators.

33% cited changes to regulations (regulatory volatility), emphasizing the need to adapt to evolving compliance requirements.

Regulatory changes and enforcement pressures are compelling organizations to allocate more resources to GRC programs. These drivers illustrate a dual focus on supporting growth and adapting to external pressures.

What drivers caused your GRC budget to change in 2024?



2025 IT and Risk Compliance Benchmark Report

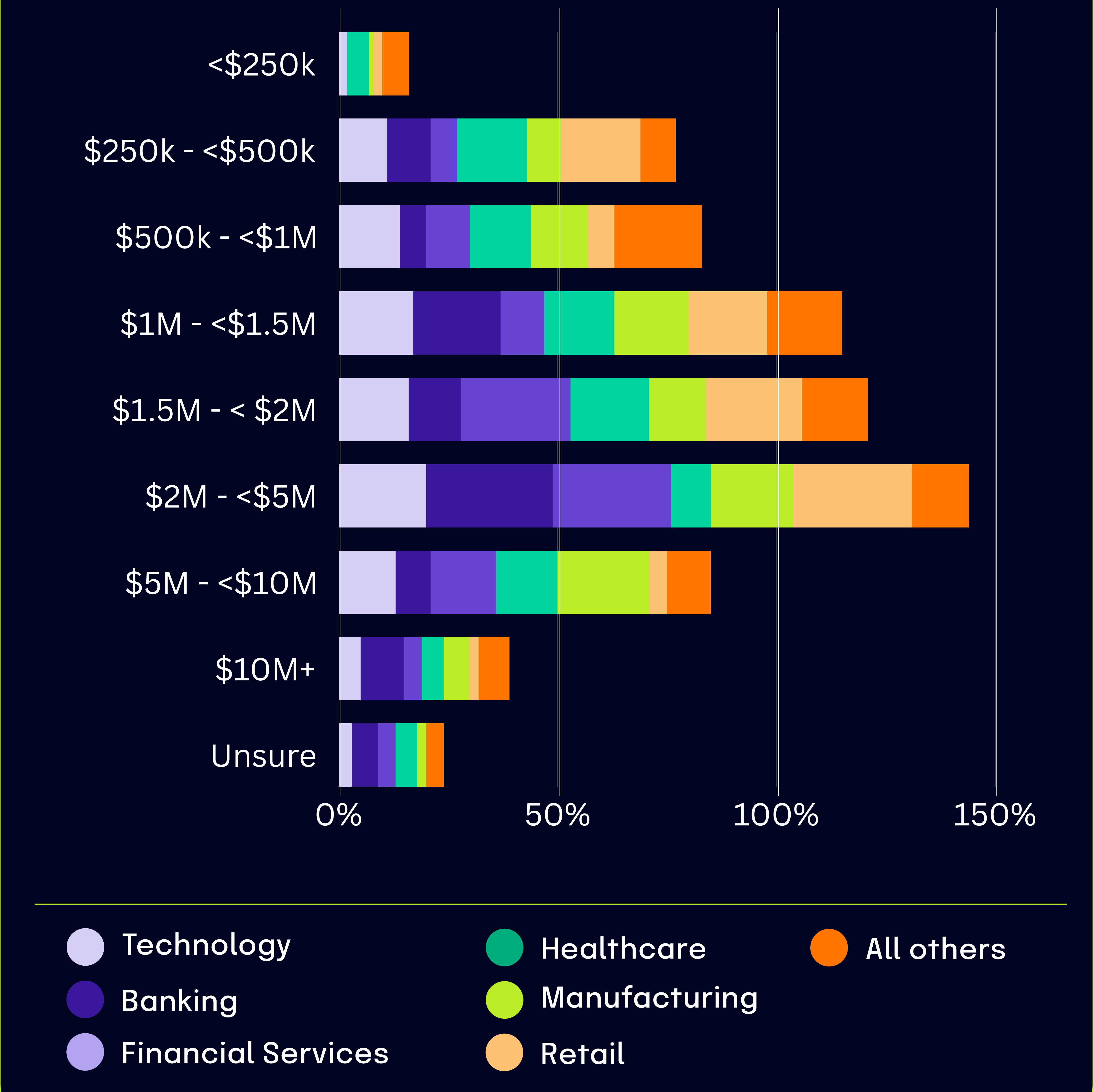
hyperproof.io/it-compliance-benchmarks

GRC budgets by industry

Respondents from the Banking and Financial Services sectors reported the highest GRC budgets, predominantly in the $2 million+ and $5 million+ ranges, reflecting their significant compliance and risk management needs. Retail and Healthcare industries displayed mixed budget patterns; Retail companies generally allocated mid-level budgets ($250,000 to $5 million), with few reaching the highest tiers. Similarly, Healthcare organizations, often under-investing in GRC, are likely to boost their budgets in 2025 following major data breaches, like the Change Healthcare incident that impacted over 100 million individuals, underscoring the need for robust GRC measures to protect sensitive data.

In contrast, Technology companies maintained moderate GRC budgets, aligning with mid-level spending. The "All Others" category, encompassing companies from various other industries, showed the broadest range of budgets from less than $250,000 to over $2 million, indicating diverse GRC approaches across sectors. This variability highlights different industry priorities and the potential impact of underinvestment in comprehensive risk and compliance strategies.

What is your GRC budget (including staffing, software, and external services such as auditing) for 2025?



2025 IT and Risk Compliance Benchmark Report

hyperproof.io/it-compliance-benchmarks

GRC budget increases by industry

Technology and Financial Services companies predict a balanced mix of moderate and significant budget increases, reflecting steady growth. The Banking industry shows conservative growth with the highest concentration in the 1%-10% range. Healthcare and Manufacturing industries have taken the lead in significant budget increases (25%-50%), reflecting targeted investments to scale GRC efforts. Retail anticipates making moderate increases, with limited projections for higher-tier growth.

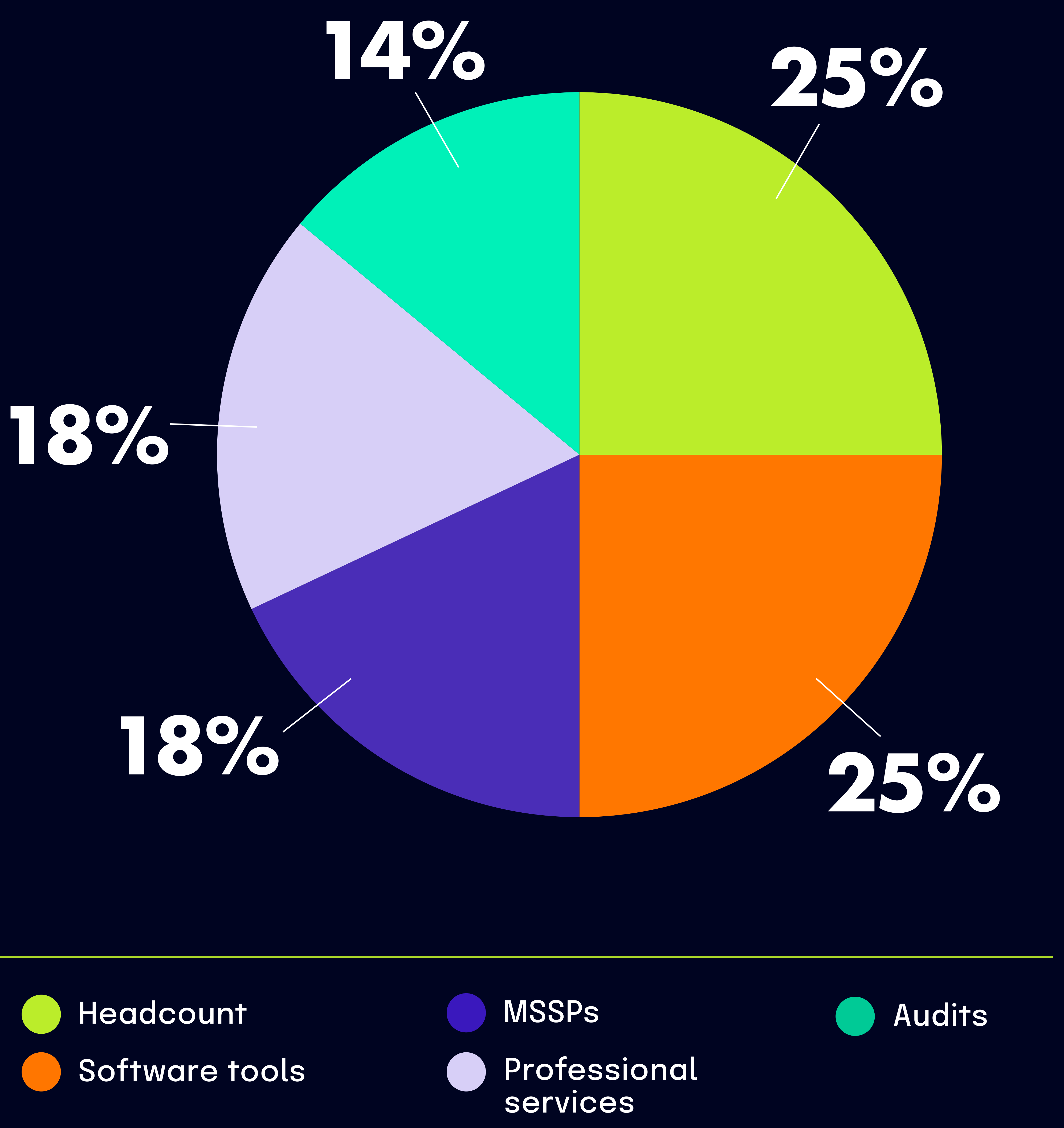
	Industry							
Budget Increase Range	Aggregate	Technology	Banking	Financial Services	Healthcare	Manufacturing	Retail	All others
1% to 10% increase	30%	27%	48%	21%	35%	30%	26%	37%
10% to 25% increase	38%	38%	33%	39%	35%	33%	52%	42%
25% to 50% increase	21%	24%	12%	30%	10%	23%	7%	14%
50% to 100% increase	10%	10%	6%	9%	20%	14%	7%	7%
More than 100% increase	1%	1%	0%	0%	0%	0%	7%	0%

GRC budget allocations in 2024

We asked respondents how they allocated their GRC budgets. Overall, the data reveals that headcount and software tools were the primary areas of budget allocation in 2024, with MSSPs, professional services, and audits receiving smaller shares. With almost 40% spent on consultation services, it's clear that expert knowledge and support is still a pervasive need in this space.

> Headcount and software tools were the primary areas of budget allocation in 2024.

What percentage of your budget allocation goes to the following areas?

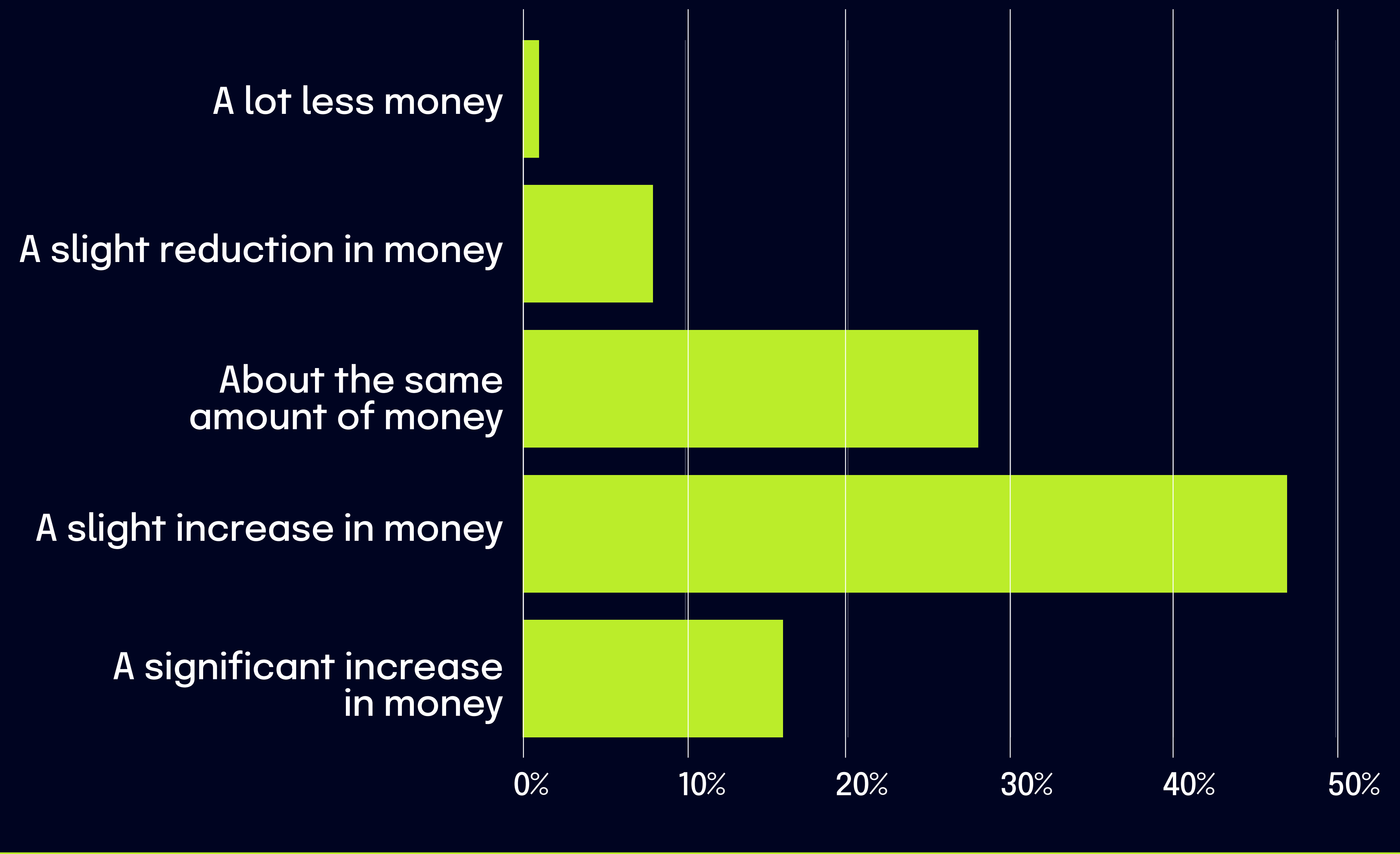


2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

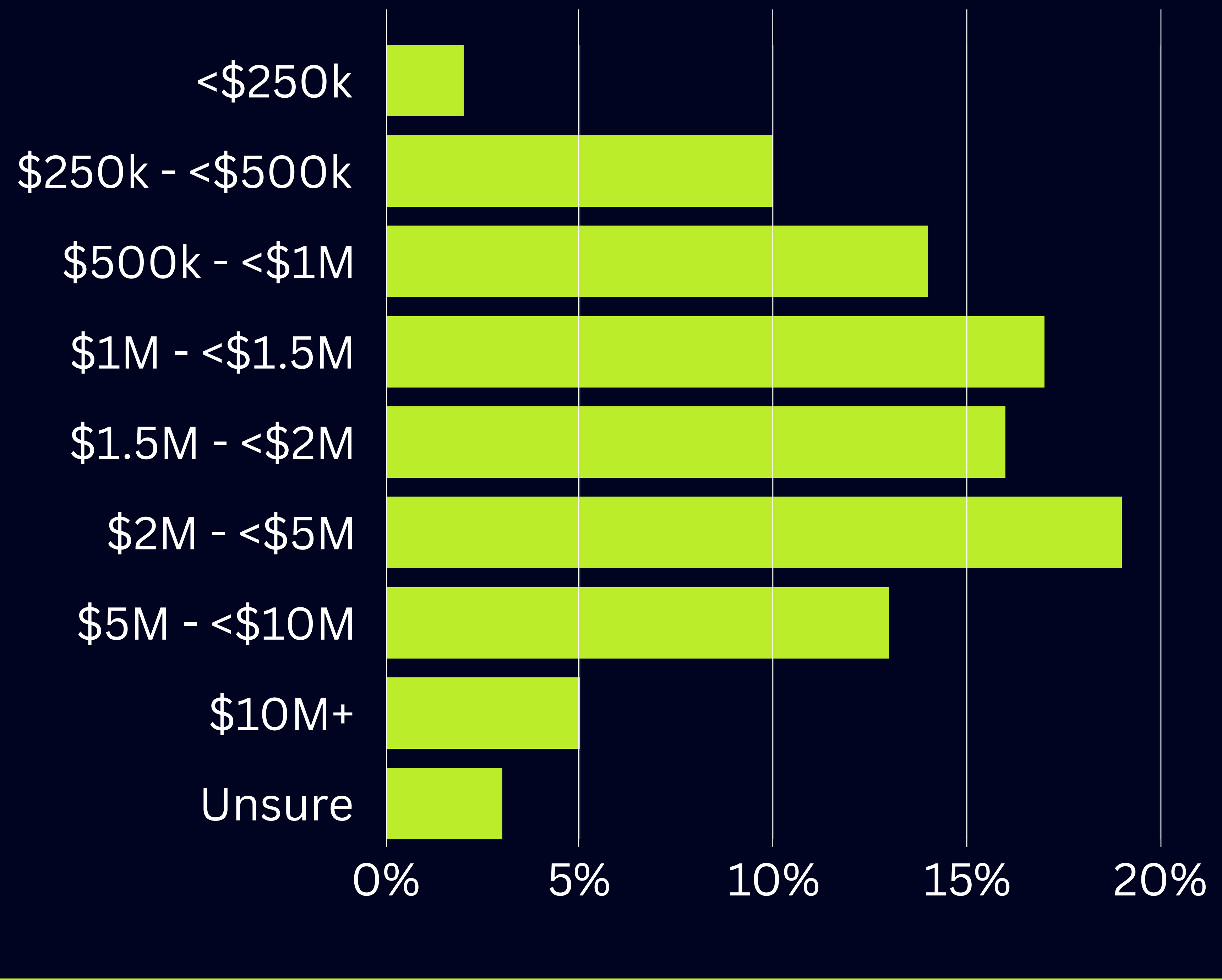
GRC budget allocations in 2025

Surprisingly, most respondents expect their GRC budgets to increase for the second consecutive year. We then asked about what the GRC budgets were for 2025. Over half of the respondents (52%) say that their GRC budgets for 2025 are between $1 million and $5 million, with an additional 18% projecting budgets exceeding $5 million.

Do you anticipate that your organization will spend more, less or about the same amount of money on IT risk management and compliance in 2025 vs. 2024?



What is your GRC budget for 2025?



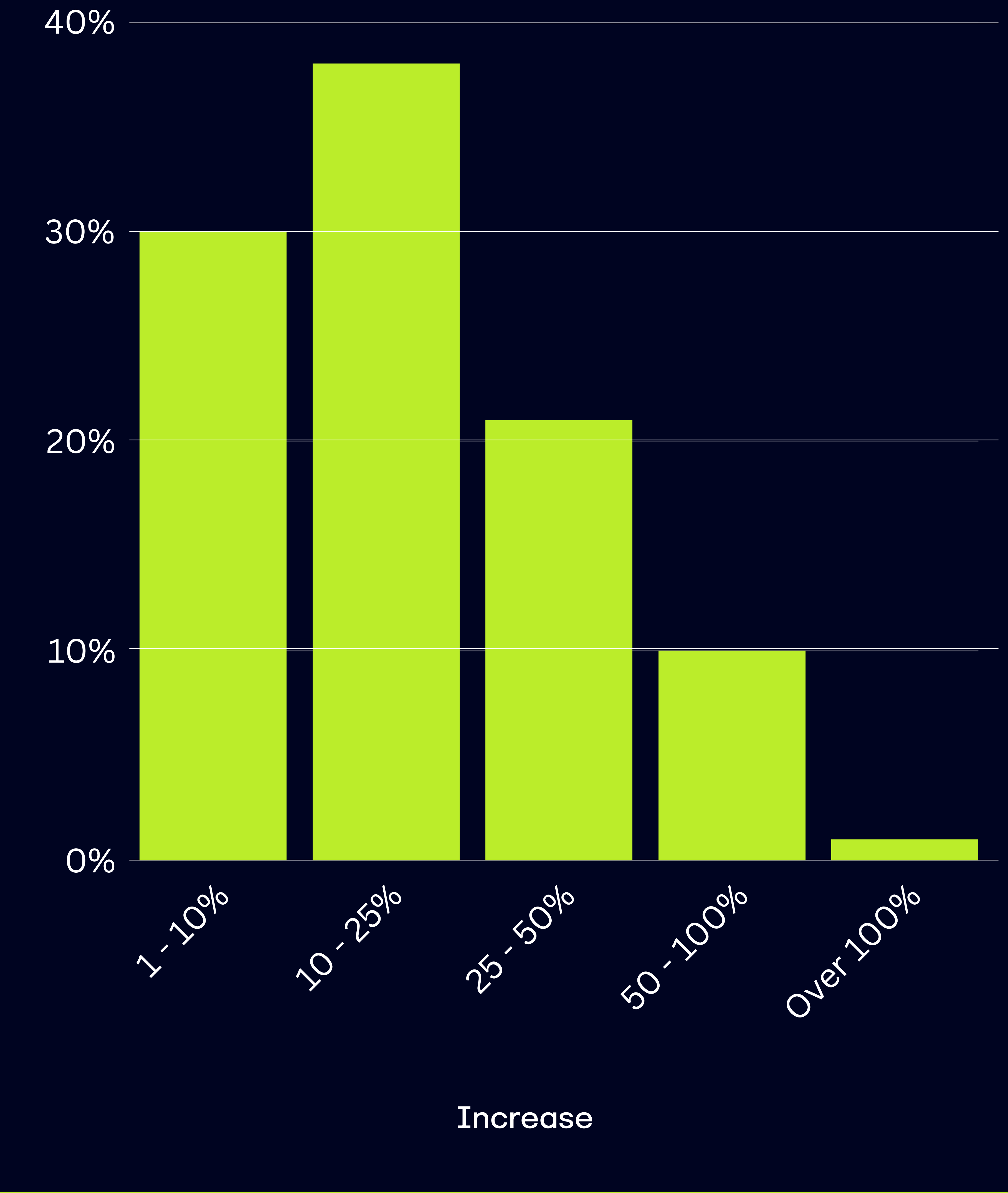
Expected GRC budget increases for 2025

We asked respondents about the extent of their budget increases and their responses varied: 30% indicated a small increase (under 10%), while the largest group, 38%, projected a moderate increase (between 10% and 25%). Additionally, 21% of respondents expected a generous increase in their budget, ranging between 25% and 50%. Notably, 11% anticipated their budget would grow by more than 50%.

FRESH FACT

11% anticipate their GRC budget would grow by more than 50% in the next 12-24 months

What is the expected or planned increase in your GRC budget in the next 12-24 months?



2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

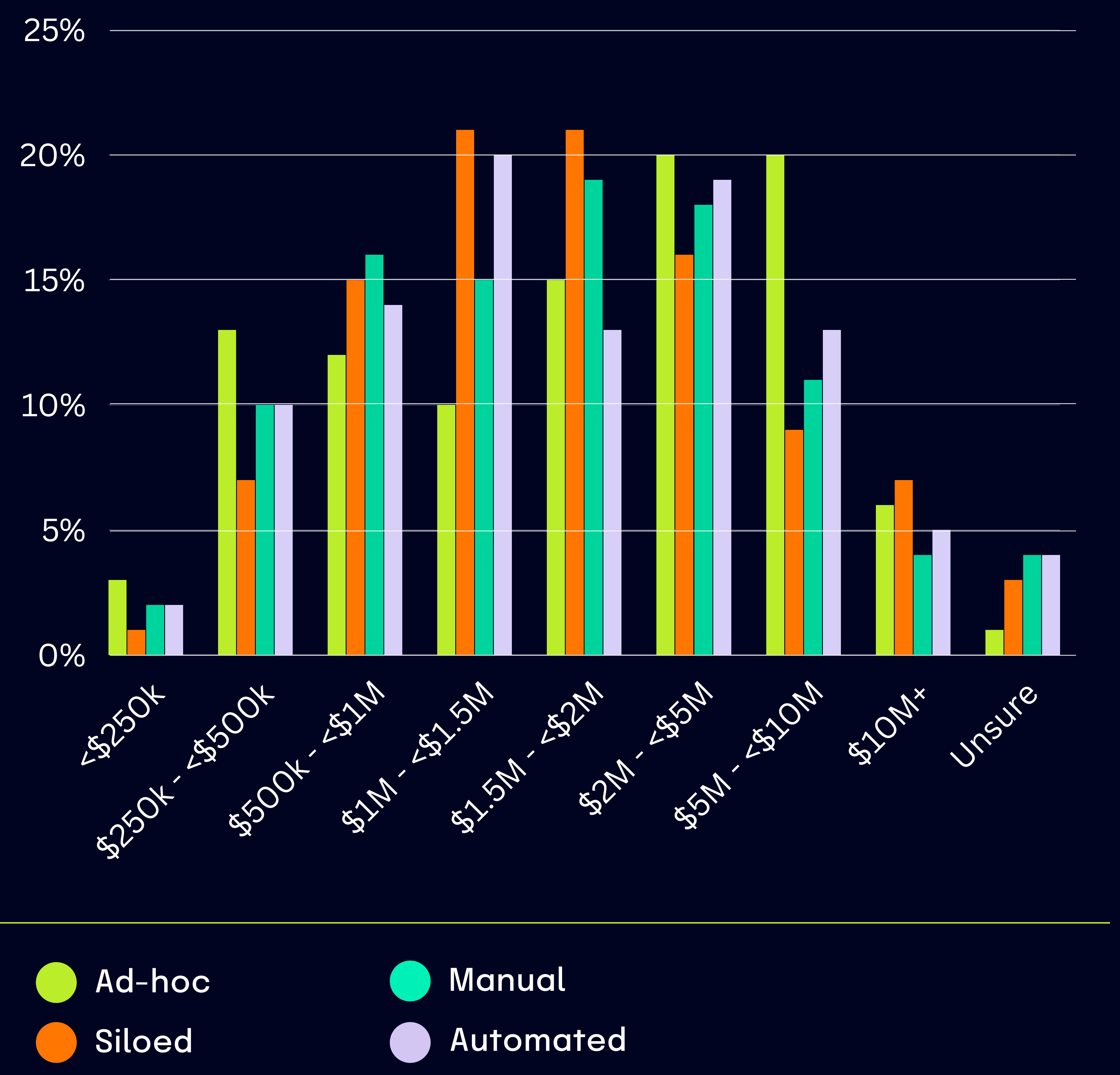
GRC budgets by approach to risk management

Those managing IT risk ad-hoc or in siloes tend to have smaller GRC budgets. The data reveals that budget distribution broadens and becomes more consistent across all tiers as IT risk management maturity increases – from ad-hoc and siloed to integrated and automated approaches. The notable outlier is MSSP-managed organizations, which cluster at the highest budget levels due to this model's significant costs and comprehensive coverage. These findings underscore the critical link between risk management maturity and the ability to effectively secure and allocate GRC funding.

> Those managing IT risk ad-hoc or in siloes tend to have smaller GRC budgets.

What is your GRC budget (including staffing, software, and external services such as auditing) for 2025?

By IT risk management approach



2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

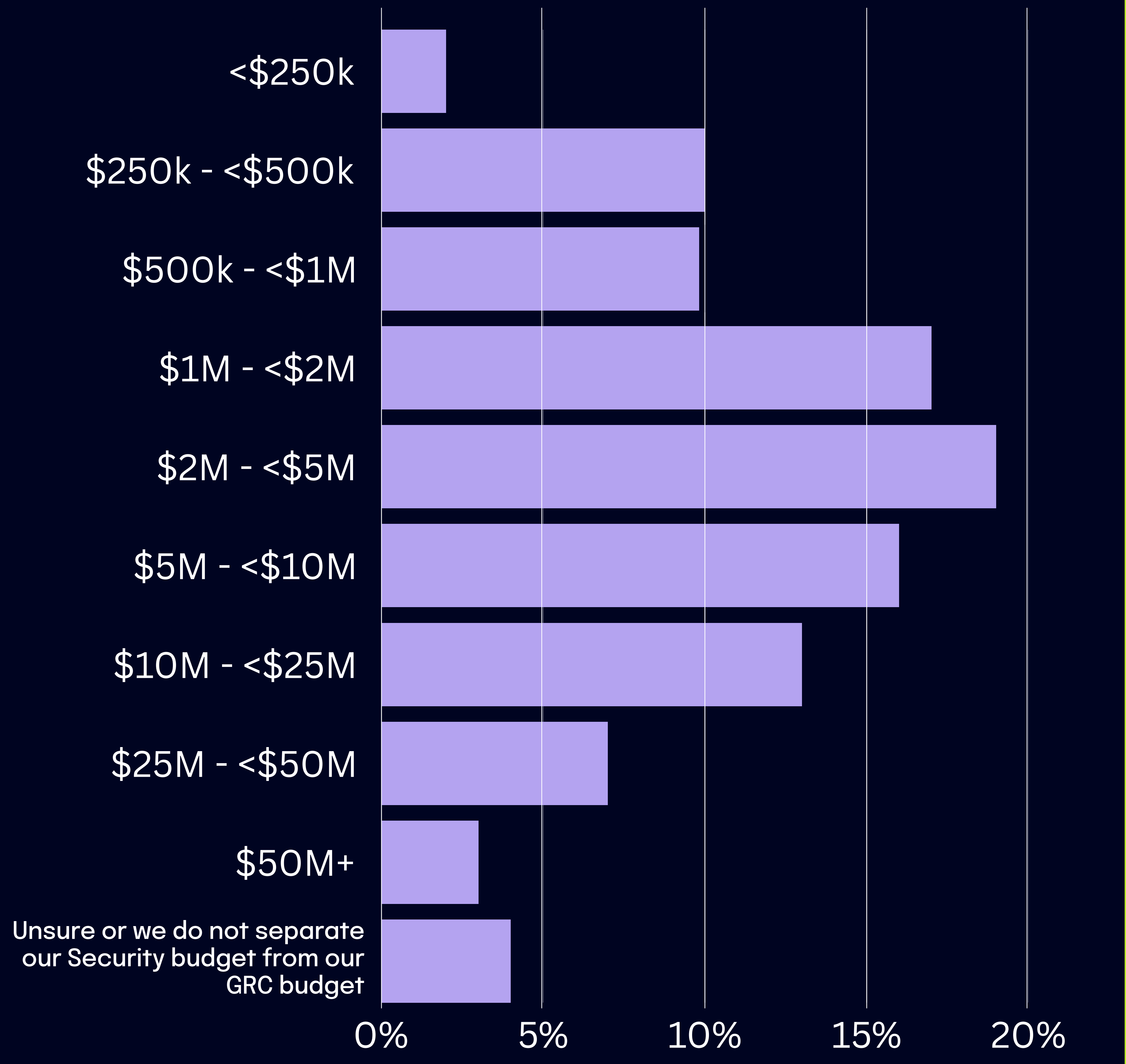
Security budgets in 2025

Over half of the surveyed organizations (52%) will allocate between $1 million and $10 million to Security in 2025. Smaller budgets (less than $500,000) represent 12%, while the highest tiers ($10 million and above) account for 23% of respondents, underscoring the scalability of security spending as organizational needs grow. A small portion of respondents (4%) either are unsure or do not separate their Security budgets from their GRC budgets.

FRESH FACT

52% of organizations will allocate between $1M and $10M to Security in 2025

What is your Security budget for 2025?



2025 IT and Risk Compliance Benchmark Report

hyperproof.io/it-compliance-benchmarks

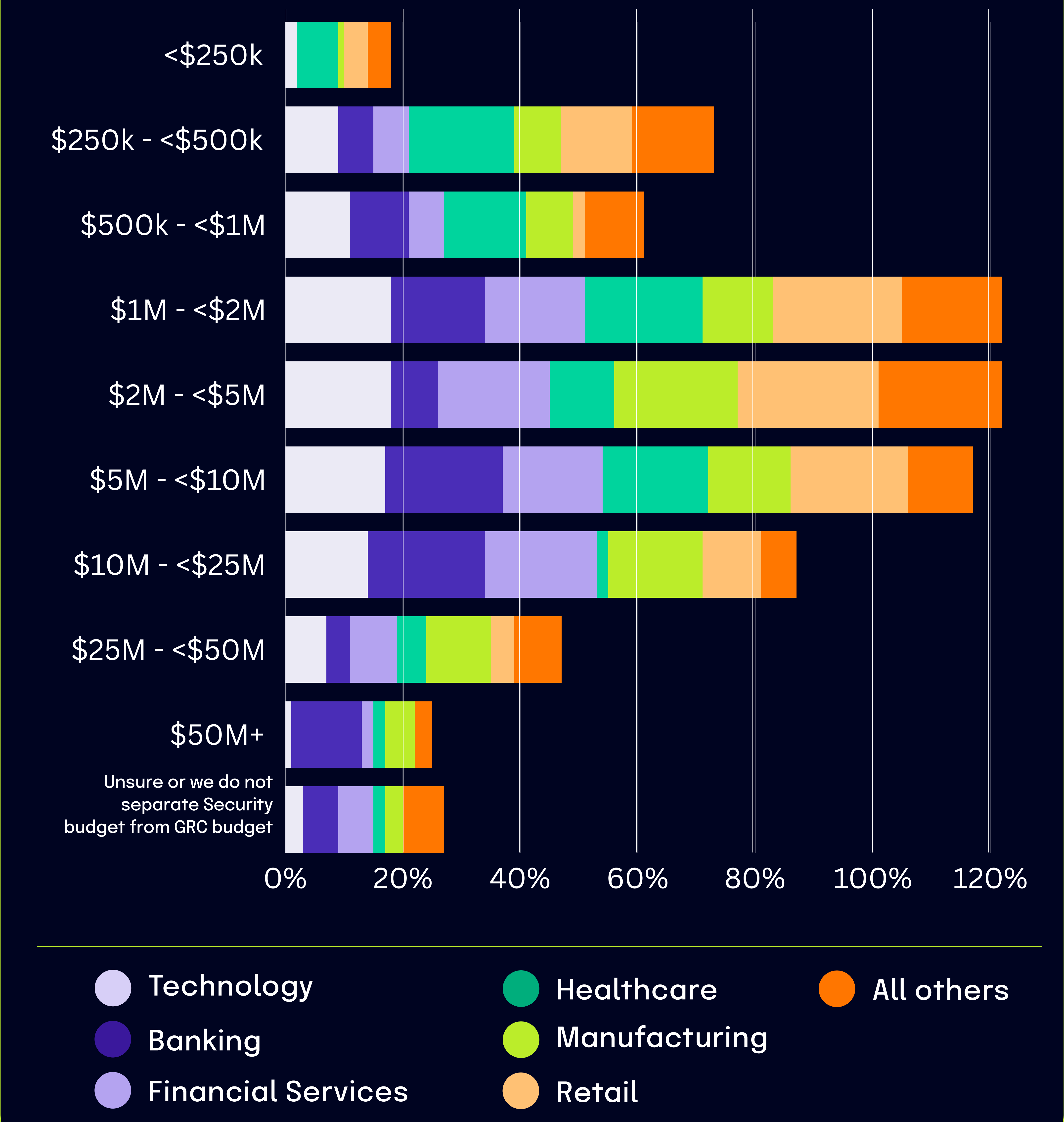
Security budgets by industry

In the technology sector, companies typically have medium to large budgets, with 35% allocating between $2 million and $10 million, though only 1% spend over $50 million. Banking leads with the largest security budgets, where 20% of banks spend between $10 million and $25 million, 12% exceed $50 million, and only 6% have budgets under $500,000. Financial Services also show large budgets, similar to Banking, with 19% spending $10 million to $25 million and 36% having mid-level budgets ranging from $1 million to $5 million.

Conversely, Healthcare entities generally have smaller budgets, with 18% spending between $250,000 to $500,000 and 14% between $500,000 to $1 million, rarely allocating over $10 million. The Manufacturing industry displays a broad budget spectrum, with 21% in the $2 million to $5 million bracket and 11% allocating $25 million to $50 million. In contrast, Retail indicates higher spending, with 46% of respondents allocating $1 million to $5 million and 30% between $10 million and $50 million, demonstrating diverse budget allocations across different industries.

What is your Security budget for 2025?

By industry



2025 IT and Risk Compliance Benchmark Report

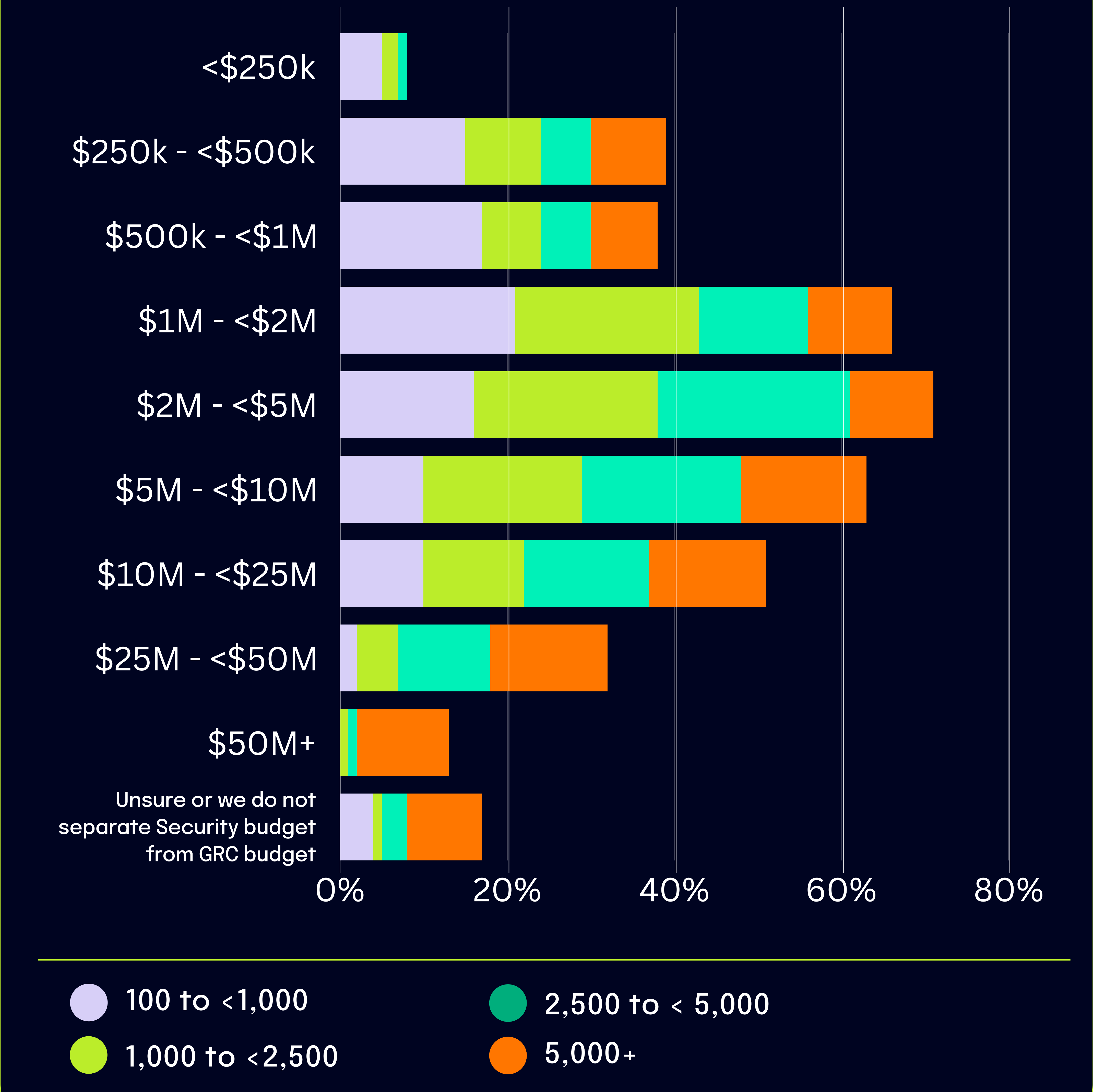
hyperproof.io/it-compliance-benchmarks

Security budgets by company size

Smaller companies (100 to <1,000 employees) often have limited resources for their security programs, with 36% reporting budgets under $1 million. Midsized companies (1,000 to <5,000 employees) typically allocate mid-range budgets between $2 million and $10 million. Large companies (5,000+) and the largest firms (over 5,000 employees) lead in high-budget allocations, with 40% spending $10 million or more, reflecting their more complex security needs. Additionally, the largest companies frequently report being unsure or not separating their security budgets from their GRC budgets, indicating a different approach to financial allocation for security measures.

What is your Security budget for 2025?

By company size



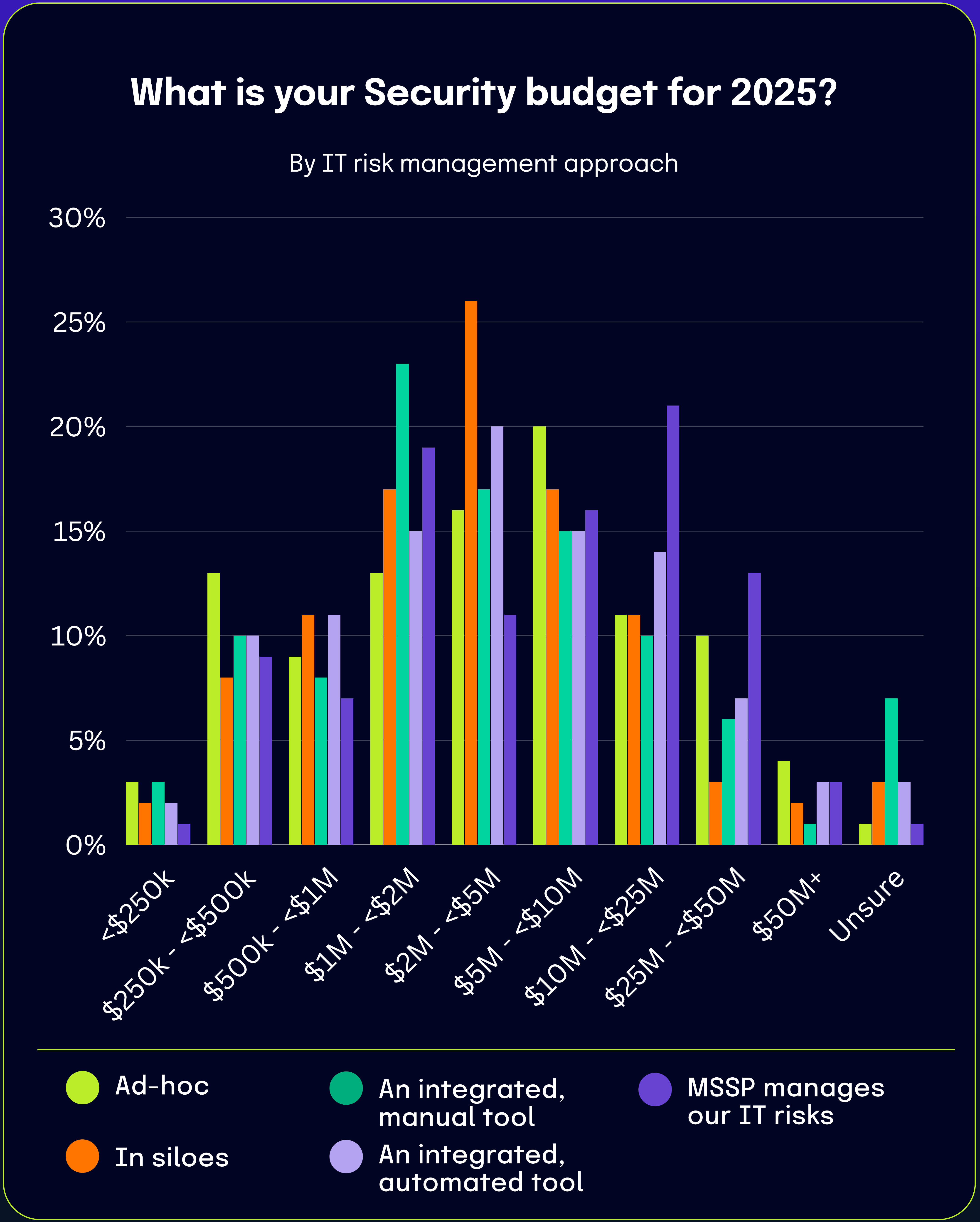
2025 IT and Risk Compliance Benchmark Report

hyperproof.io/it-compliance-benchmarks

Security budgets by approach to IT risk management

We found that organizational maturity dictates security budget scalability and distribution. Organizations' approaches to IT risk management significantly influence their security budget allocations, with clear patterns emerging based on maturity and reliance on internal or external strategies. The data illustrates a clear relationship between the maturity of IT risk management approaches and budget allocations:

- Reactive and siloed strategies constrain budgets, limiting organizations to lower or mid-level tiers
- Integrated, automated approaches improve budget scalability, particularly when leveraging automation
- MSSP outsourcing leads to dominant representation in high-budget tiers, reflecting the cost of outsourcing critical risk management responsibilities



2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

Addressing third-party risks requires more than adopting best practices – it demands consistent execution, vigilant oversight, adoption of new technologies, and a commitment to continuous improvement.

CHAPTER 6

Who Is Responsible for GRC?

GRC functions are steadily becoming more central to business strategy, and this year's data indicated a shift toward shared responsibility models and collaborative decision-making. The shared responsibility model is gaining traction, driven by mounting pressures for CISOs. 2024's high-profile legal actions against CISOs have highlighted the risks of centralized accountability, leading to a push for distributing responsibility for business risks across roles within an organization. Effective GRC requires a collective effort, with compliance embedded across teams and functions.

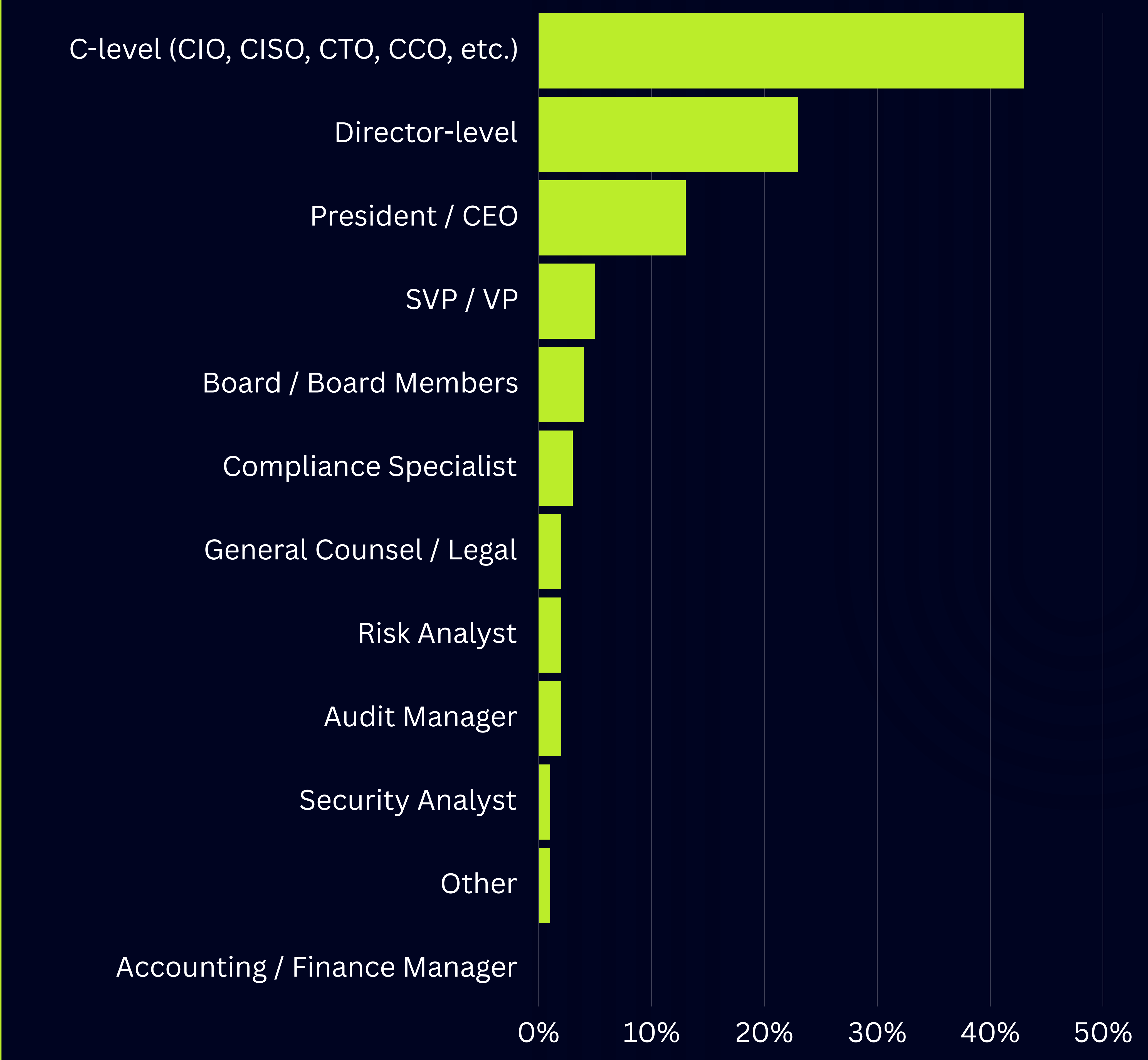
We found that decision-making around compliance technology also highlights the collaborative nature of modern GRC. Compliance, security, and risk leaders frequently champion or influence technology adoption, working alongside legal, financial, and executive stakeholders – a cross-functional approach ensuring that GRC strategies align with organizational priorities, balancing operational needs, regulatory requirements, and budget considerations.

Who oversees compliance

This year, we found that while compliance is often anchored at the executive level, it is also distributed across a range of leadership positions, depending on organizational structure and priorities. The diversity of roles reflects the varying degrees of emphasis on compliance as a strategic, legal, or operational function.

The most common oversight comes from C-level executives (e.g., CIO, CISO, CTO, CCO), with 43% of respondents indicating these leaders are responsible for compliance. This highlights the importance of compliance at the executive level, where it is often integrated into broader strategic and operational planning. In 13% of organizations, the President or CEO directly oversees compliance, signaling its significance as a top-level priority. Directors also play a significant role in overseeing compliance in 23% of organizations, suggesting a more operational or departmental approach to compliance management. It is far less common for the General Counsel or legal professionals, SVPs or Vice Presidents, Audit Managers, Compliance Specialists, or Board members to oversee compliance.

What is the highest level position or title overseeing compliance?



2025 IT and Risk Compliance Benchmark Report

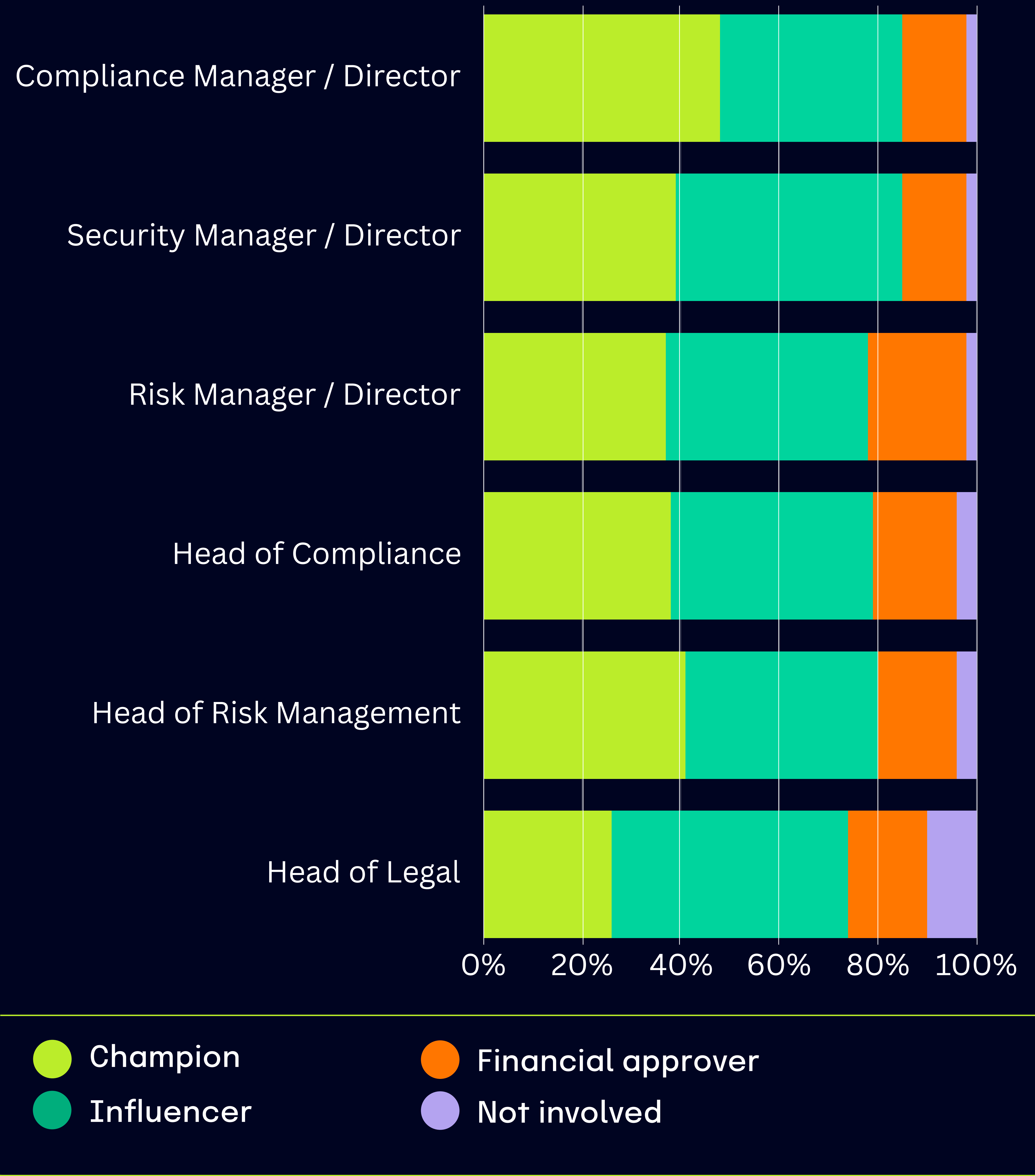
hyperproof.io/it-compliance-benchmarks

Leading decision-makers involved when buying compliance or risk technology

Multiple roles and titles are involved in purchasing compliance or risk technology, showcasing the importance of cross-functional collaboration. Notably, compliance, security, and risk leaders take on the most active roles, reflecting their close connection to the operational and regulatory challenges that drive technology adoption.

Nearly half (48%) of organizations identify the compliance manager/director as the champion driving the decision to adopt compliance or risk technology. A significant portion (37%) see them as influencers, with only 13% serving as financial approvers. Security leaders play a dual role, with 39% acting as champions and 46% serving as influencers. Their involvement underscores the overlap between cybersecurity and compliance in risk management technology adoption. Risk leaders are involved in varied capacities, with 37% as champions and 41% as influencers. Notably, 20% of risk managers also serve as financial approvers, highlighting their role in balancing technology needs with budget considerations.

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



2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

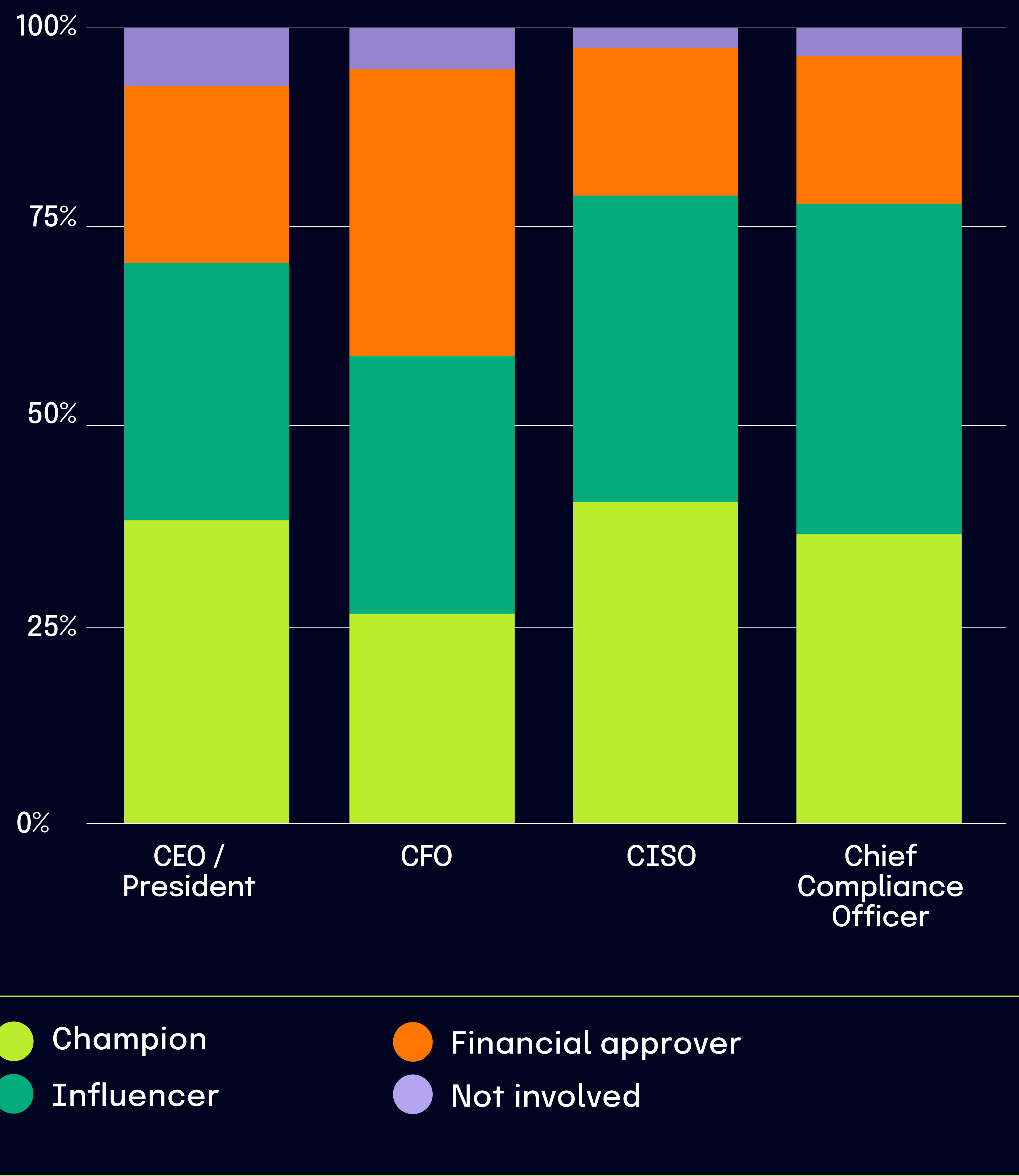
Roles the C-suite plays in decision-making

The CCO is seen as a champion in 37% of organizations and as an influencer in 41%, with 18% acting as financial approvers. Chief Information Security Officers (CISOs) often drive decisions as champions (41%) or serve as influencers (38%), reflecting their integral role in aligning compliance technology with cybersecurity needs.

The CFO is predominantly a financial approver (36%) but also acts as a champion (27%) and influencer (32%), showing their oversight of cost considerations. CEOs are champions in 39% of organizations and financial approvers in 22%, indicating their strategic interest in compliance technology decisions. Legal leaders play a strong influencer role (48%), with 26% acting as champions. This reflects the importance of legal perspectives in ensuring compliance technology aligns with regulatory requirements.

Across all roles, the data shows a collaborative approach to purchasing compliance and risk technology, with champions, influencers, and financial approvers in the C-suite working together to align organizational needs with strategic priorities.

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



2025 IT and Risk Compliance Benchmark Report

hyperproof.io/it-compliance-benchmarks

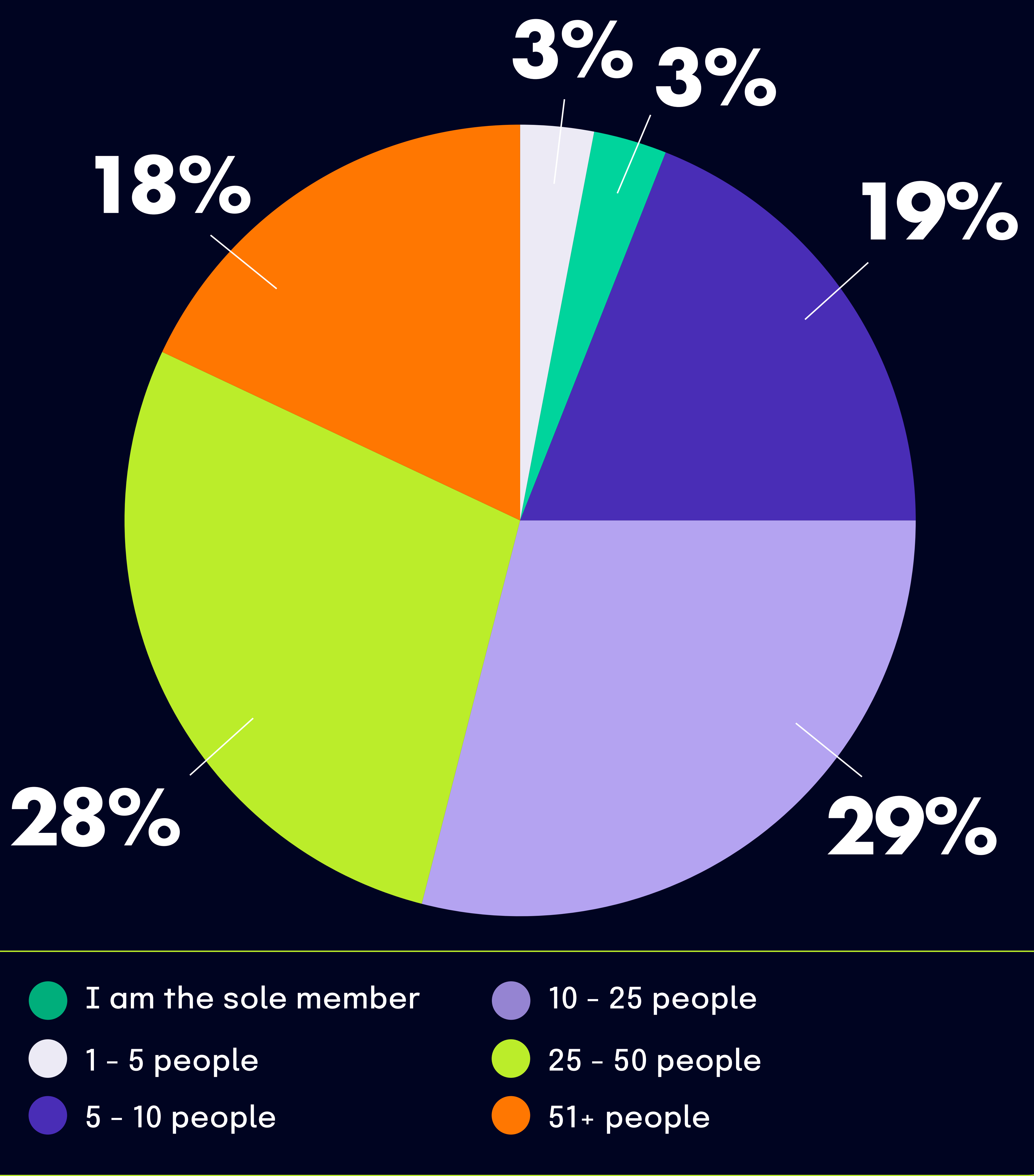
Compliance and risk management team sizes in 2024

Most organizations maintain midsized compliance teams, with 33% employing 5 to less than 10 staff members, and 30% employing 10 to less than 25 staff members. Most organizations recognize the importance of a dedicated infosec/cybersecurity compliance team but may scale their resources proportionally to their size, complexity, or risk exposure.

Smaller teams are common, but less dominant: organizations with 1 to 4 staff members account for only 17% of the total. The GRC space is trending away from minimal investment in cybersecurity compliance, even among smaller organizations.

A significant proportion of organizations report larger compliance teams, with 14% employing 25 to less than 50 staff members, and 6% employing 50+ staff members. These larger teams are concentrated in industries with high regulatory demands or large enterprises where complex operations require substantial resources dedicated to infosec and cybersecurity compliance.

What is the size of your compliance management and/or risk management team?



2025 IT and Risk Compliance Benchmark Report

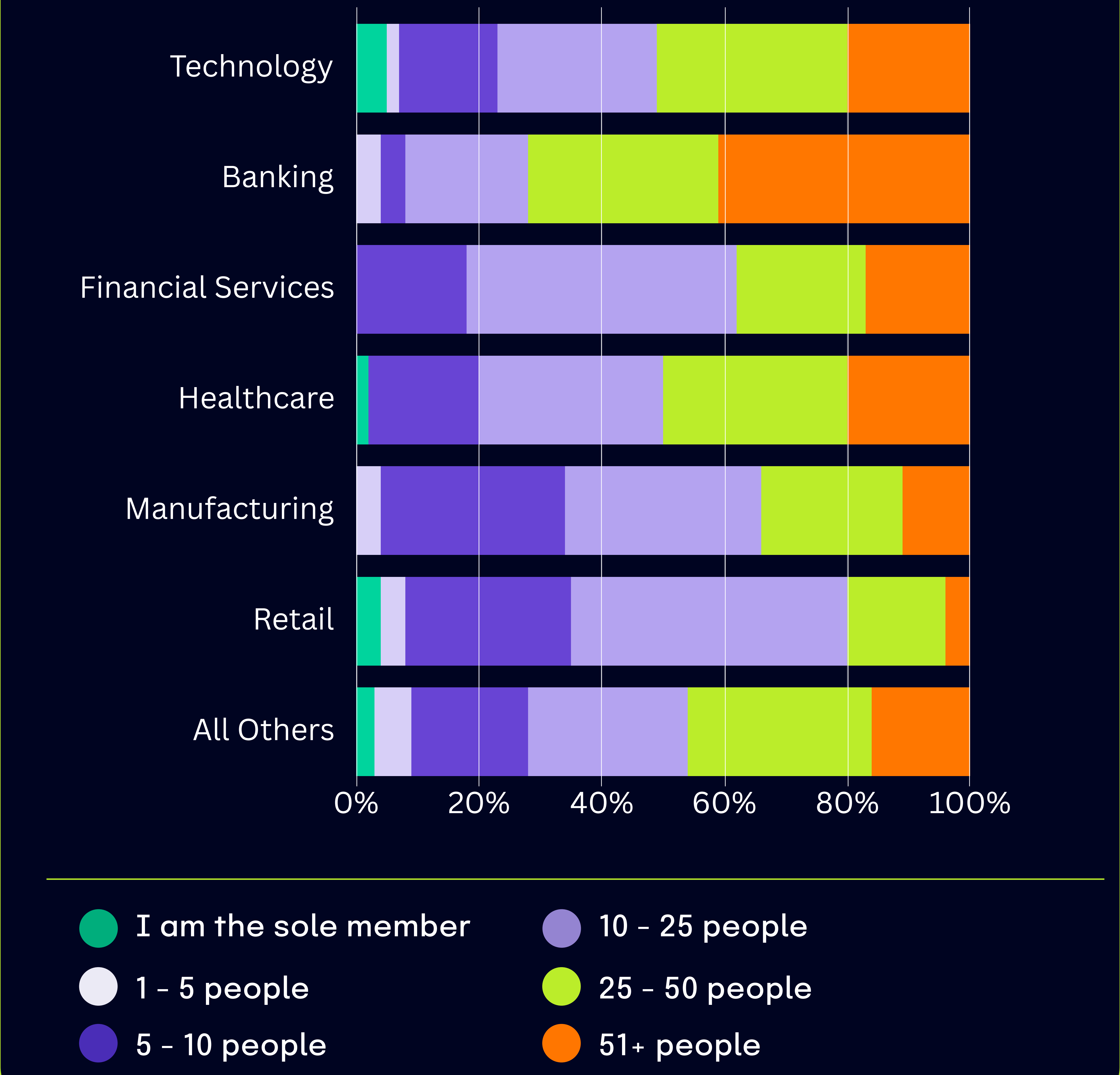
hyperproof.io/it-compliance-benchmarks

Compliance and risk management team sizes by industry

Midsized teams are common across all sectors. Across industries, 5 to less than 10 staff members is the most common team size, balancing resource allocation and operational demands. Larger teams concentrated in highly regulated sectors (e.g., Banking or Health Tech) will likely allocate larger teams (25+ staff), underscoring the additional resources needed to meet complex compliance obligations. Smaller teams are more prevalent in manufacturing and small organizations. These organizations exhibit a higher proportion of lean teams, likely due to fewer compliance mandates or resource constraints.

What is the size of your compliance management and/or risk management team?

By industry



2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

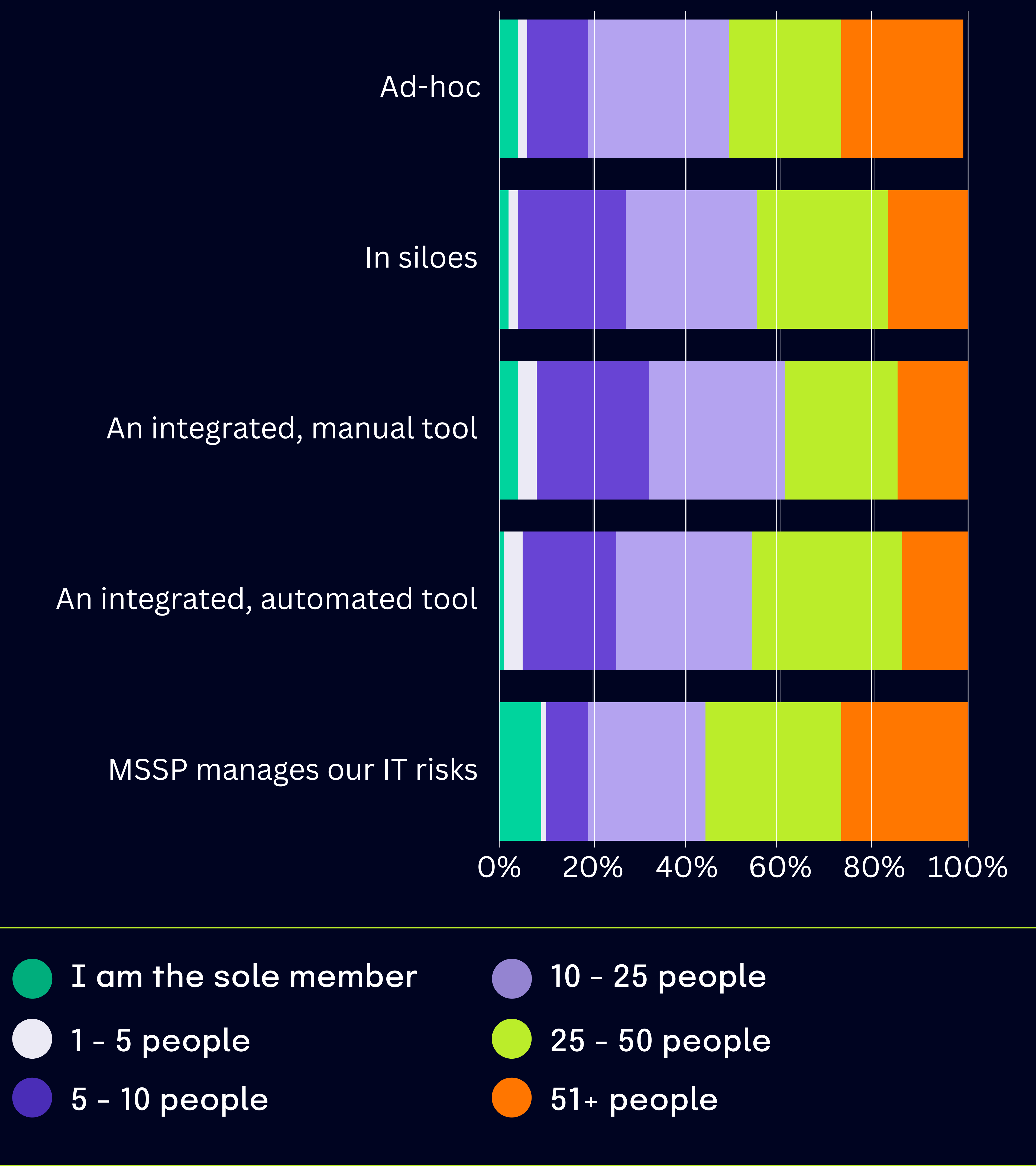
Compliance and risk management team sizes by approach to managing IT risks

Overall, organizations with mature, integrated, and automated IT risk management approaches can manage scale with smaller teams than those who take an ad-hoc approach. This trend persists for both companies using an integrated manual or automated tool.

Midsized teams were the most common across most approaches. 5 to less than 10 staff was the most frequently reported team size, reflecting a standard investment level for infosec compliance. Integrated and automated approaches consistently show the broadest budget and team size distribution, demonstrating their capacity to scale efficiently. Conversely, ad-hoc and siloed approaches constrain growth. These methods focus heavily on midsized teams, with limited representation in larger team sizes, highlighting the challenges of scaling without integration or strategic frameworks. Lastly, organizations outsourcing to MSSPs allocate larger teams to manage the complexities of external partnerships.

What is the size of your compliance management and/or risk management team?

By IT risk management approach



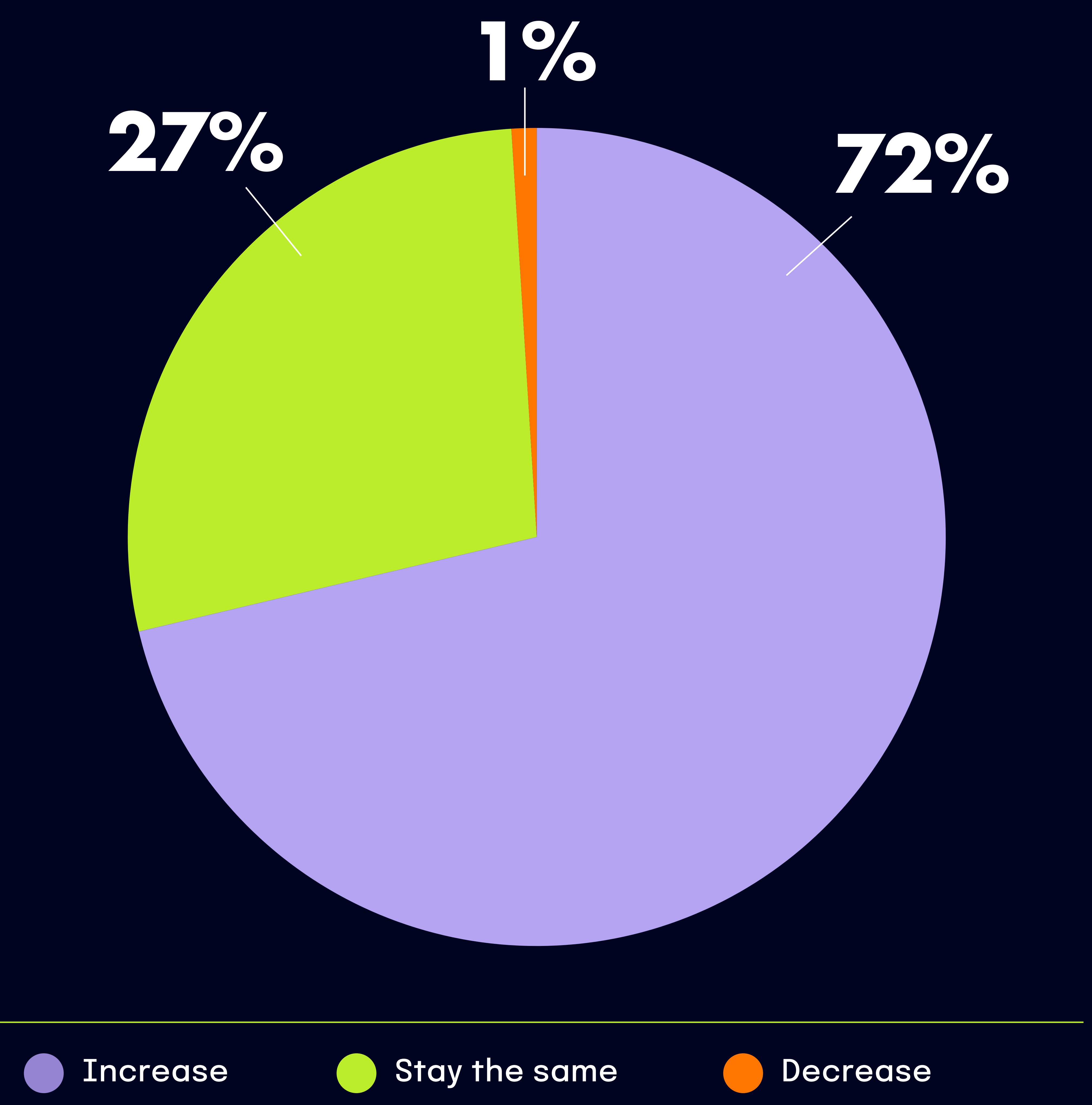
2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

Compliance team growth in the next two years

72% of all respondents plan to grow their company's compliance team's personnel over the next two years, and only 27% of respondents said their team size will stay the same. These organizations may already have mature compliance functions or face resource constraints that limit their ability to scale further. However, their decision to maintain team size suggests recognizing the critical nature of compliance, even without immediate expansion.

Only 1% of respondents said their team's size will decrease within the next two years, underscoring the enduring importance of compliance functions. Organizations have shifted away from viewing these teams as expendable because reducing them can lead to significant organizational vulnerabilities.

In the next two years, will your company's compliance team headcount grow, stay the same, or decrease?



2025 IT and Risk Compliance Benchmark Report

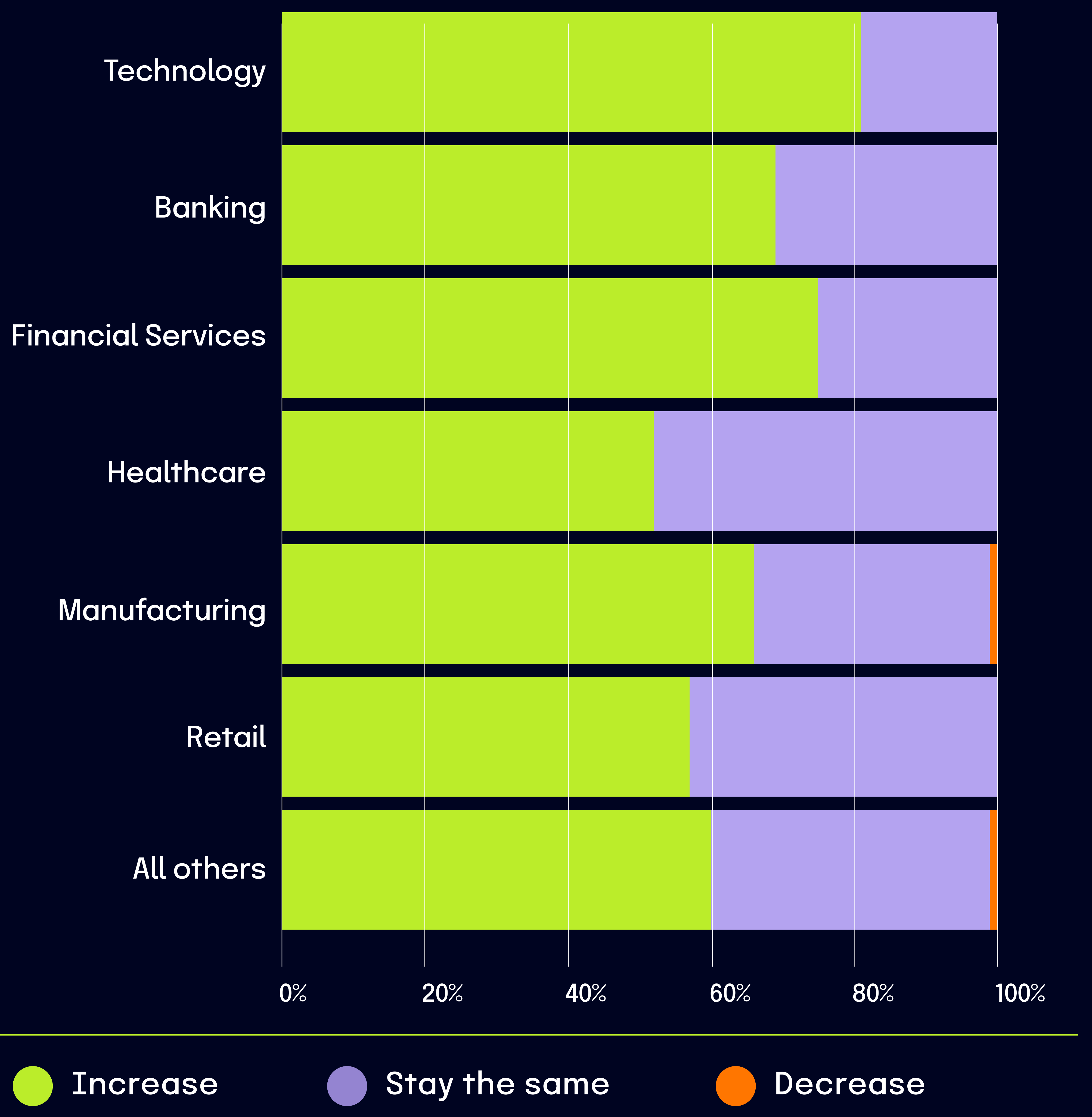
hyperproof.io/it-compliance-benchmarks

Compliance team growth by industry

Technology leads with 81% of companies planning to increase compliance team size, significantly higher than the aggregate of 72%. The Financial Services and Banking verticals show strong growth, with 69% of Banking companies surveyed and 75% of Financial Services companies planning to continue hiring. Manufacturing and Retail show more conservative trends. 66% of Manufacturing companies surveyed said they will grow their team, with 1% potentially shrinking staff. For Retail, 57% of the respondents said they would grow their team, with 43% maintaining their current team size. Healthcare stands out as the most conservative industry in hiring; only 52% plan to increase the size of their compliance team; 48% will keep team size the same, and none plan to reduce staff.

In the next two years, will your company's compliance team headcount grow, stay the same, or decrease?

By industry



2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

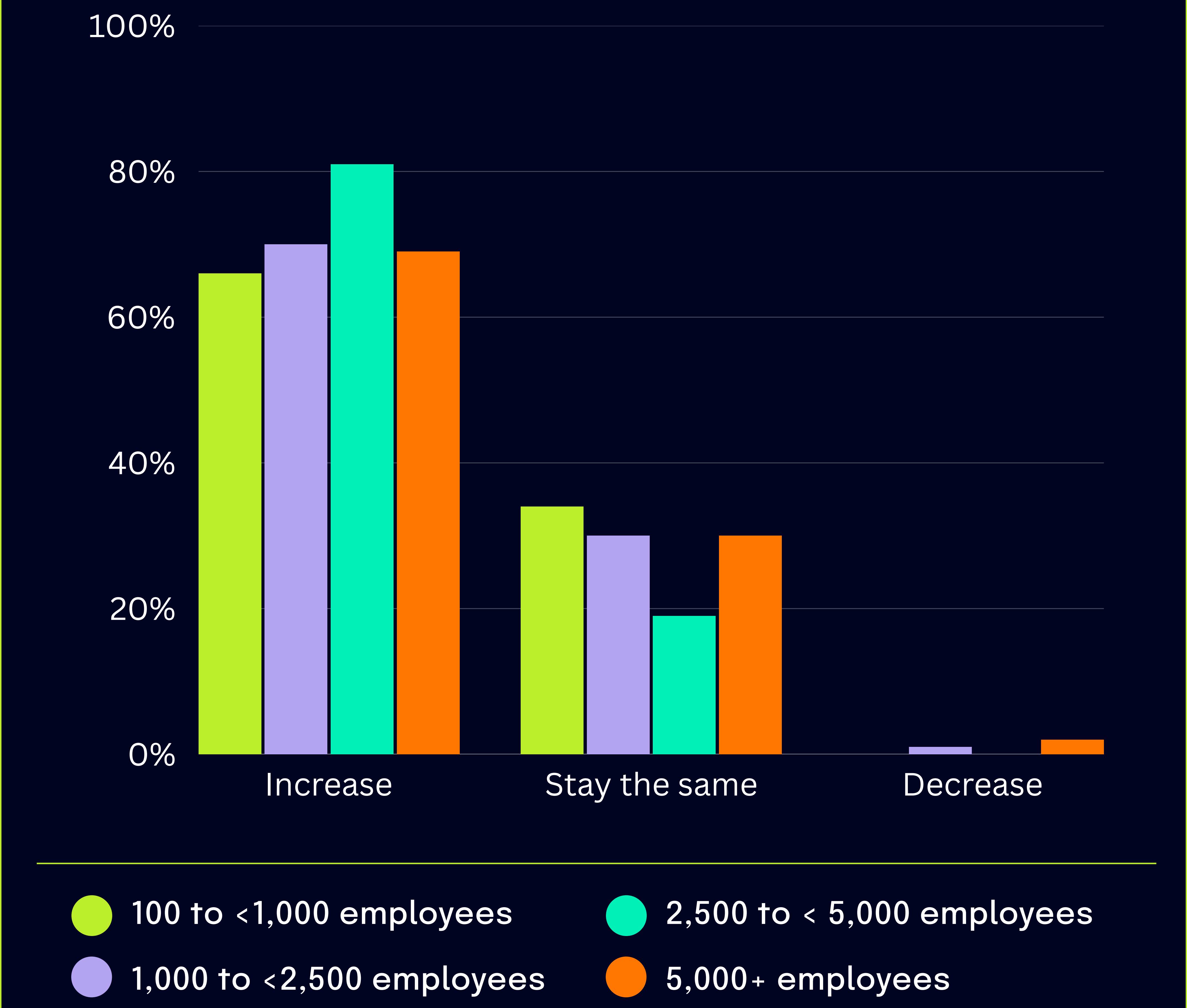
Compliance team growth by company size

Organizations of varying sizes expect different levels of growth for their compliance teams focusing on information security and data privacy, reflecting their unique capacities and priorities. While most organizations anticipate growth in compliance teams, the scale and pace of this expansion vary by company size, with larger midsized organizations driving the most significant increases.

Small enterprises (2,500 to <5,000 employees) will likely grow their compliance team at 81%, reflecting their scaling needs and heightened focus on compliance. Small and midsize organizations (100 to <2,500 employees) show steady growth expectations, with 66–70% planning to increase their compliance teams and minimal reductions. Large organizations (5,000+ employees) tend to be just as aggressive in their hiring plans as small and midsize organizations, with 69% planning expansion.

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?

By company size



2025 IT and Risk Compliance Benchmark Report

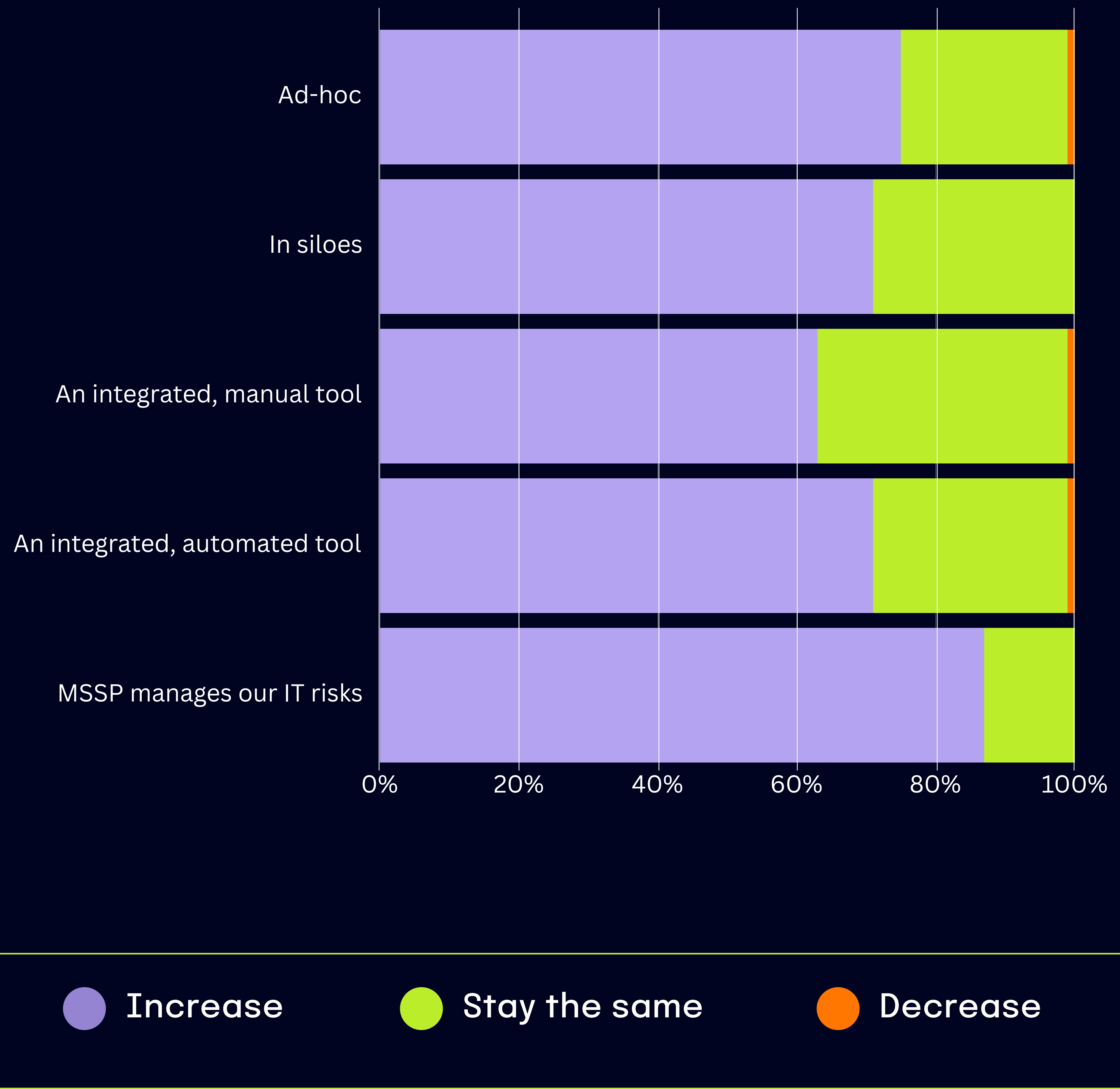
hyperproof.io/it-compliance-benchmarks

Compliance team growth by IT risk management approach

Organizations' approaches to managing IT risks significantly influence their plans for growing compliance teams focusing on information security and data privacy. Organizations that rely on MSSPs to manage their IT risks as a group lead in compliance team growth, with 87% planning expansions. Meanwhile, organizations that take an integrated approach but use mostly manual processes exhibit the lowest growth expectations (63%) and are most likely to say their team size will remain stable (36%). Across all approaches, very few organizations anticipate personnel reductions, signaling broad confidence in maintaining or growing compliance teams.

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?

By approach to managing IT risk



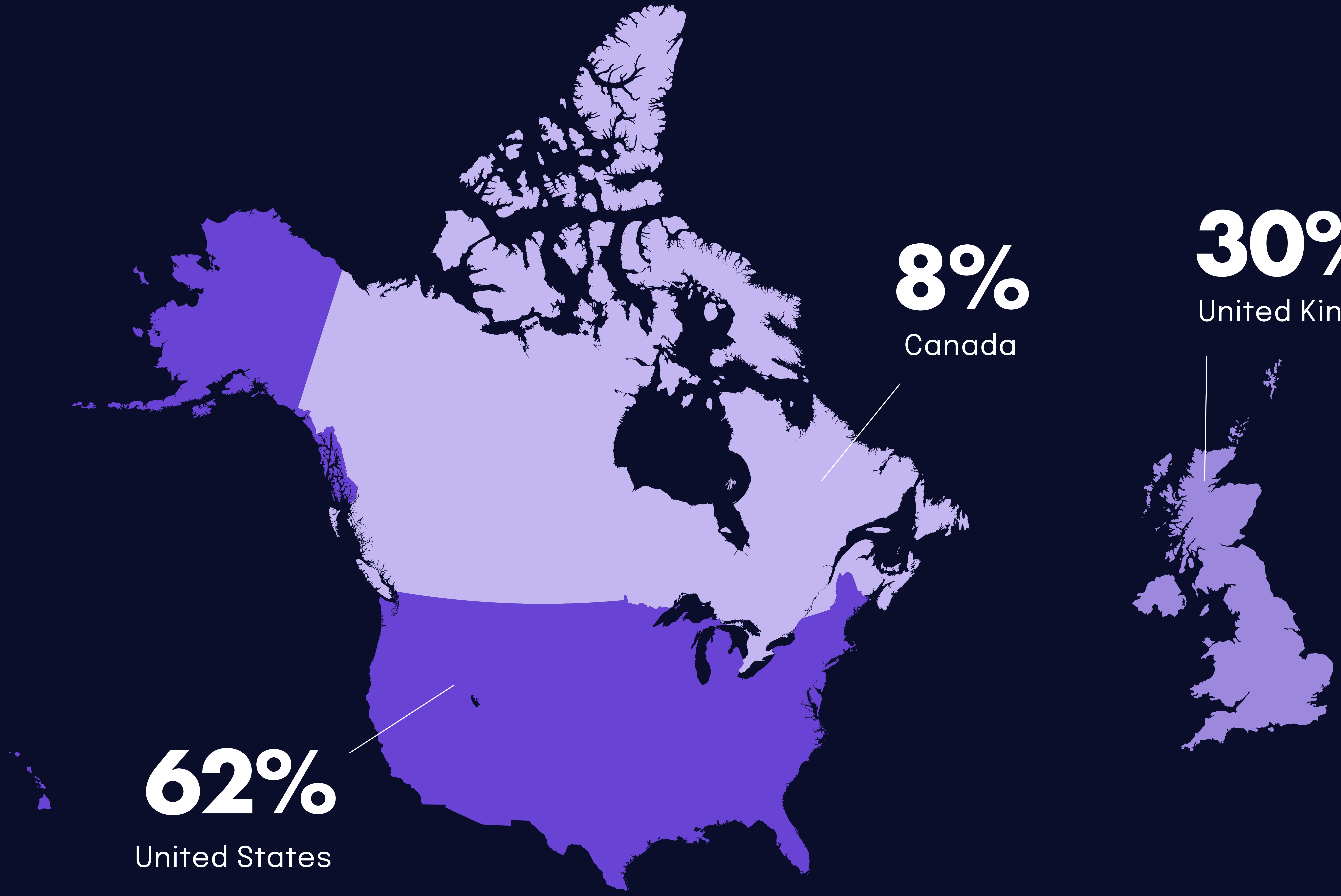
2025 IT and Risk Compliance Benchmark Report hyperproof.io/it-compliance-benchmarks

2025

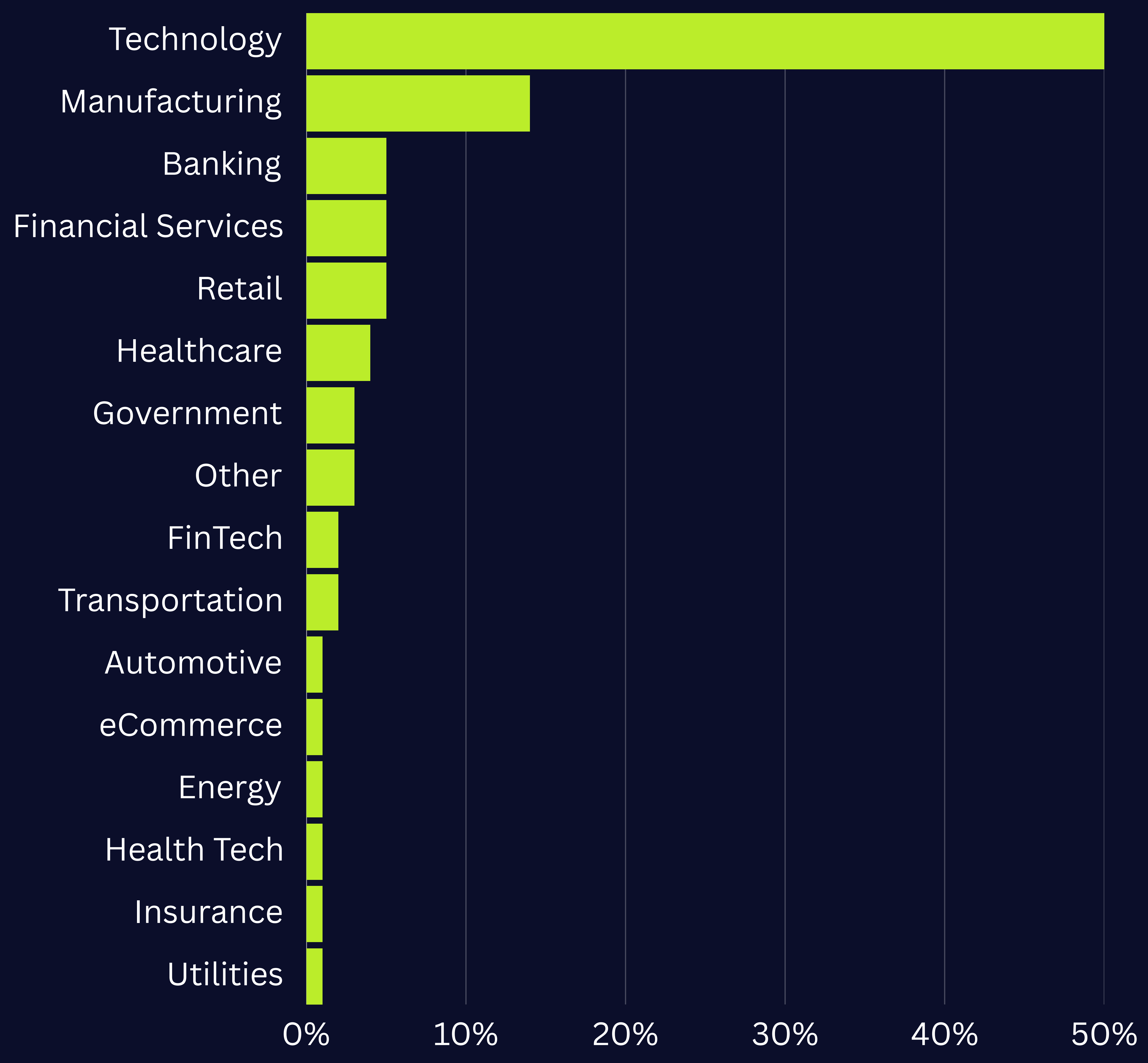
Survey Methodology

The 2025 IT Risk and Compliance Benchmark Survey gathered **1,000 responses during November 2024.**

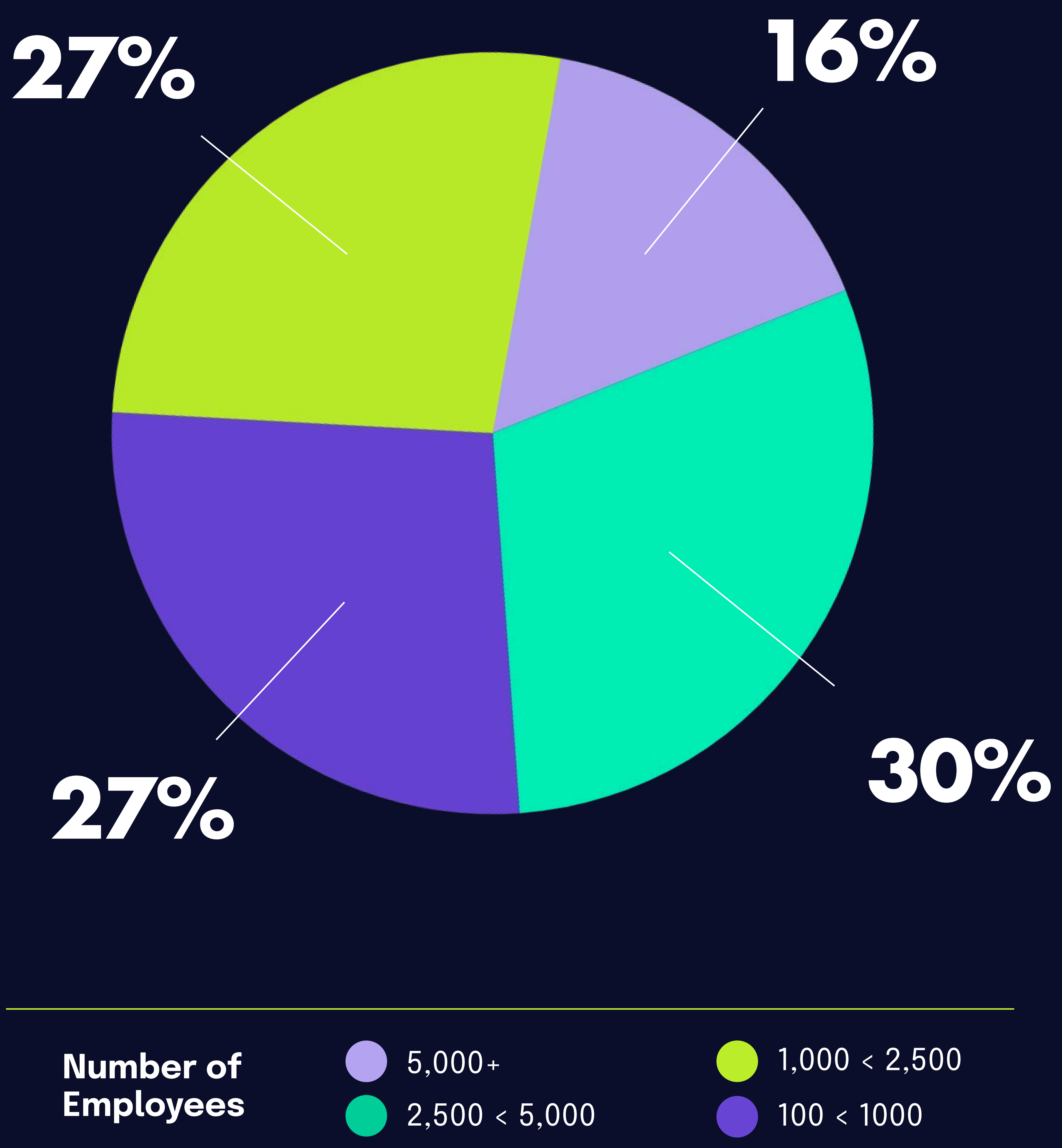
Location



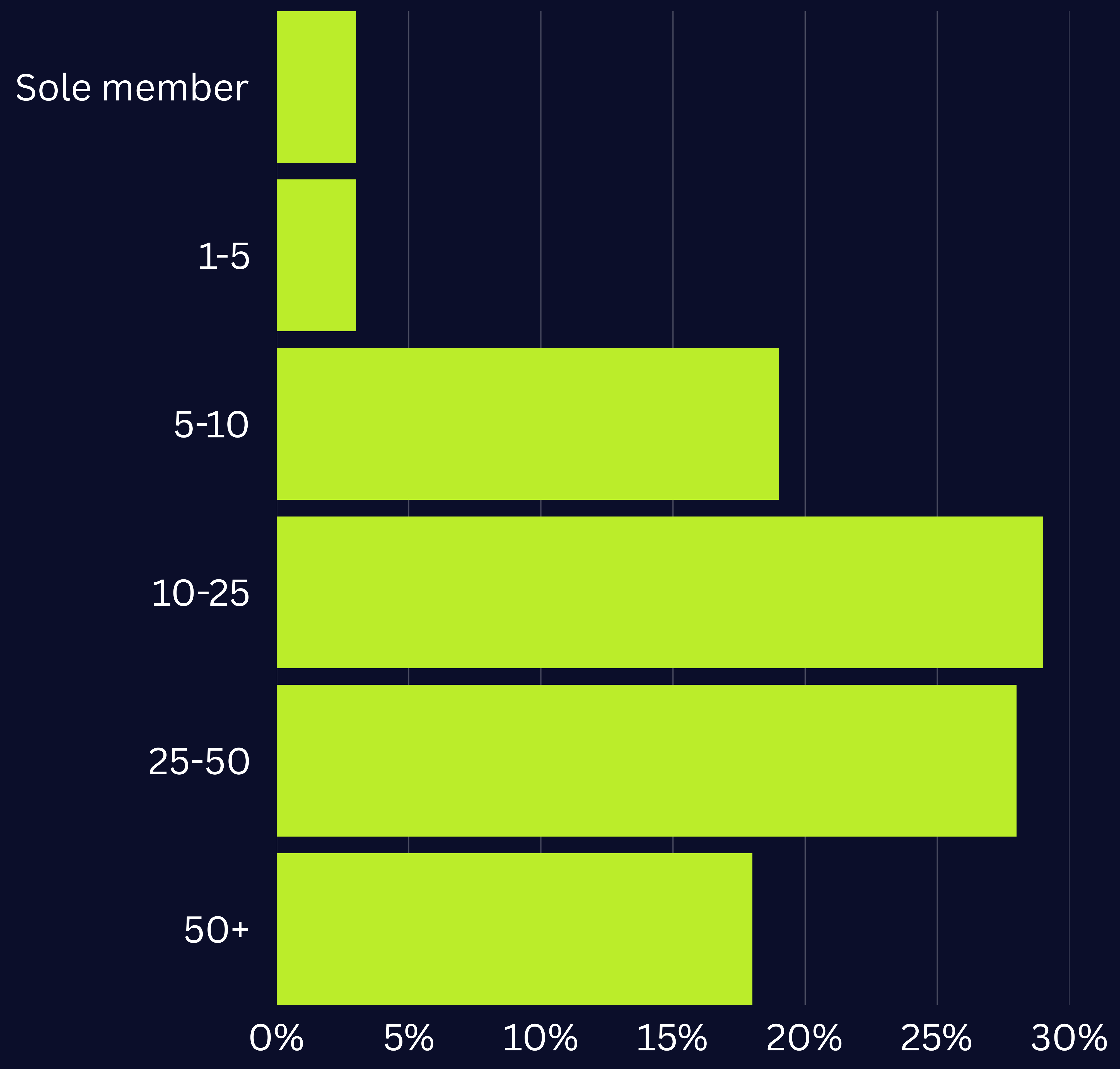
Industries surveyed



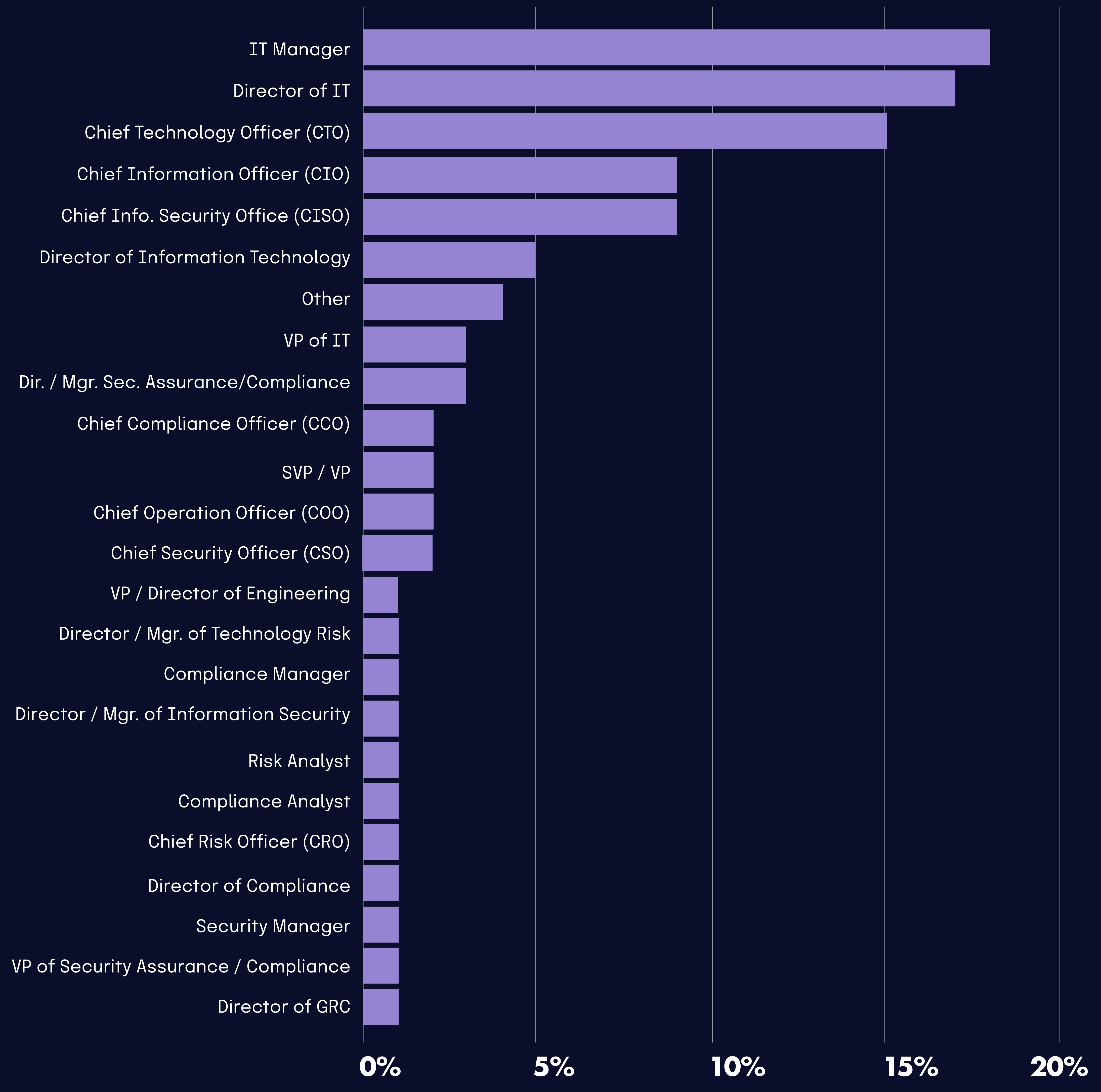
Organization size



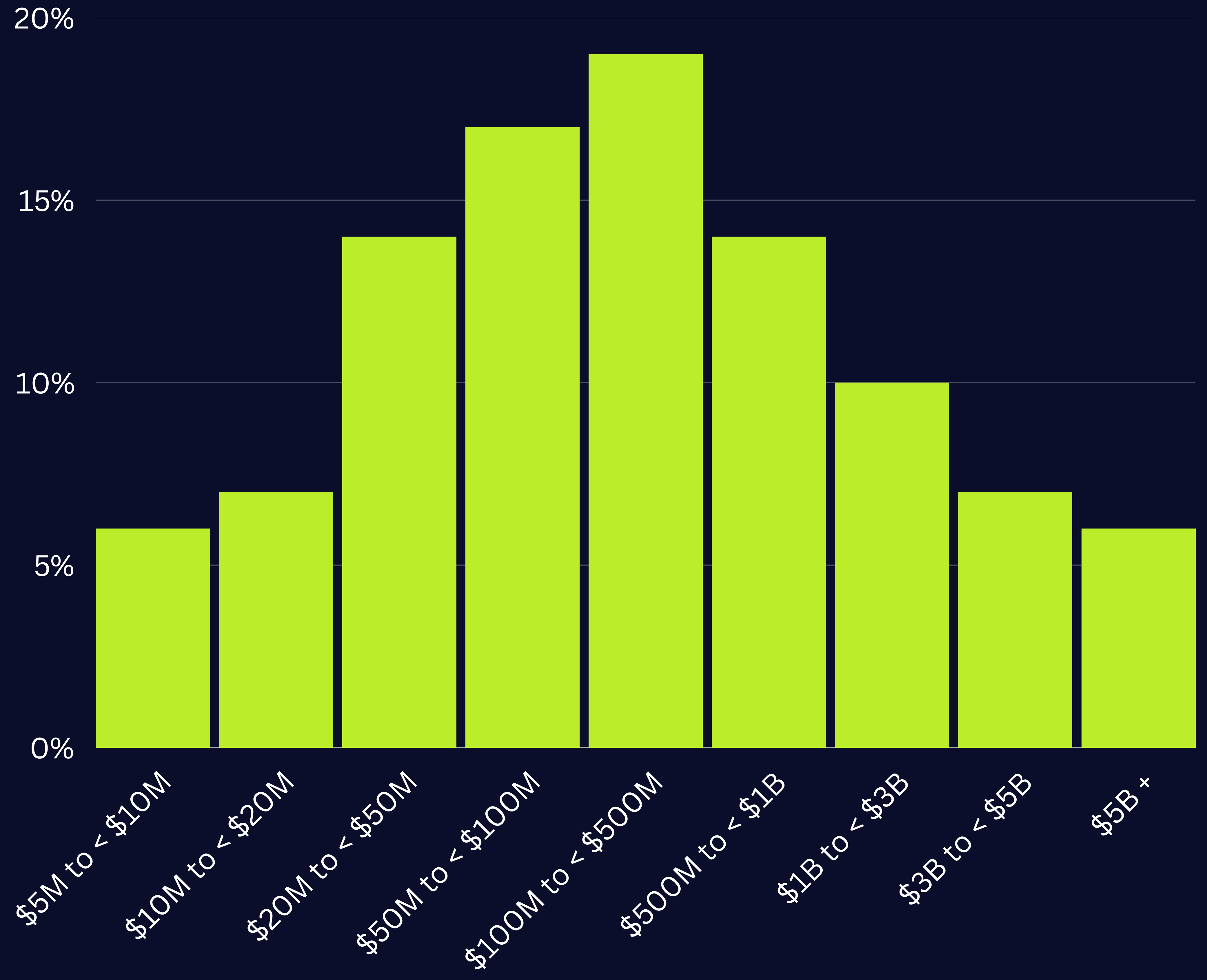
Team size



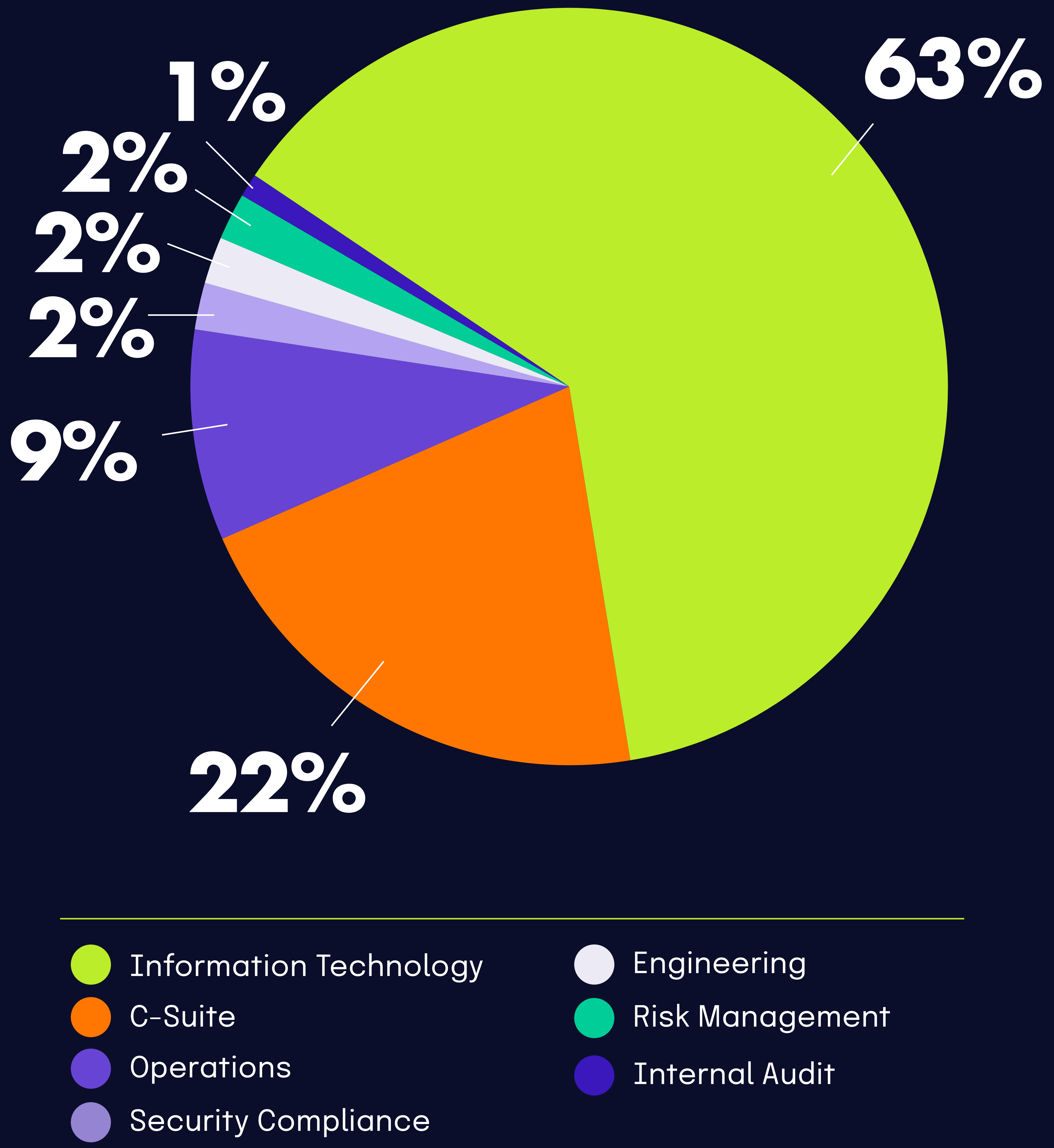
Job Titles



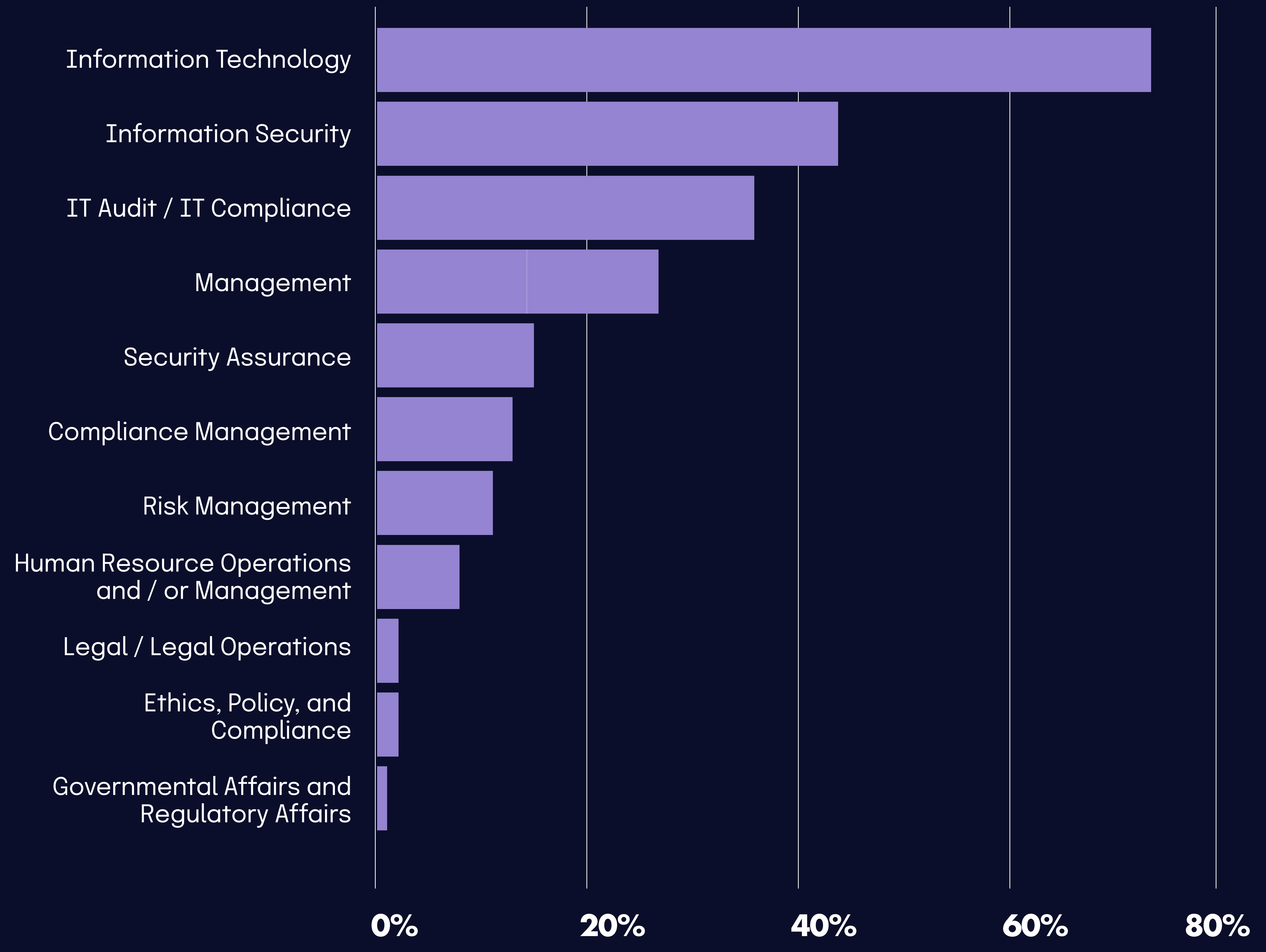
Revenue



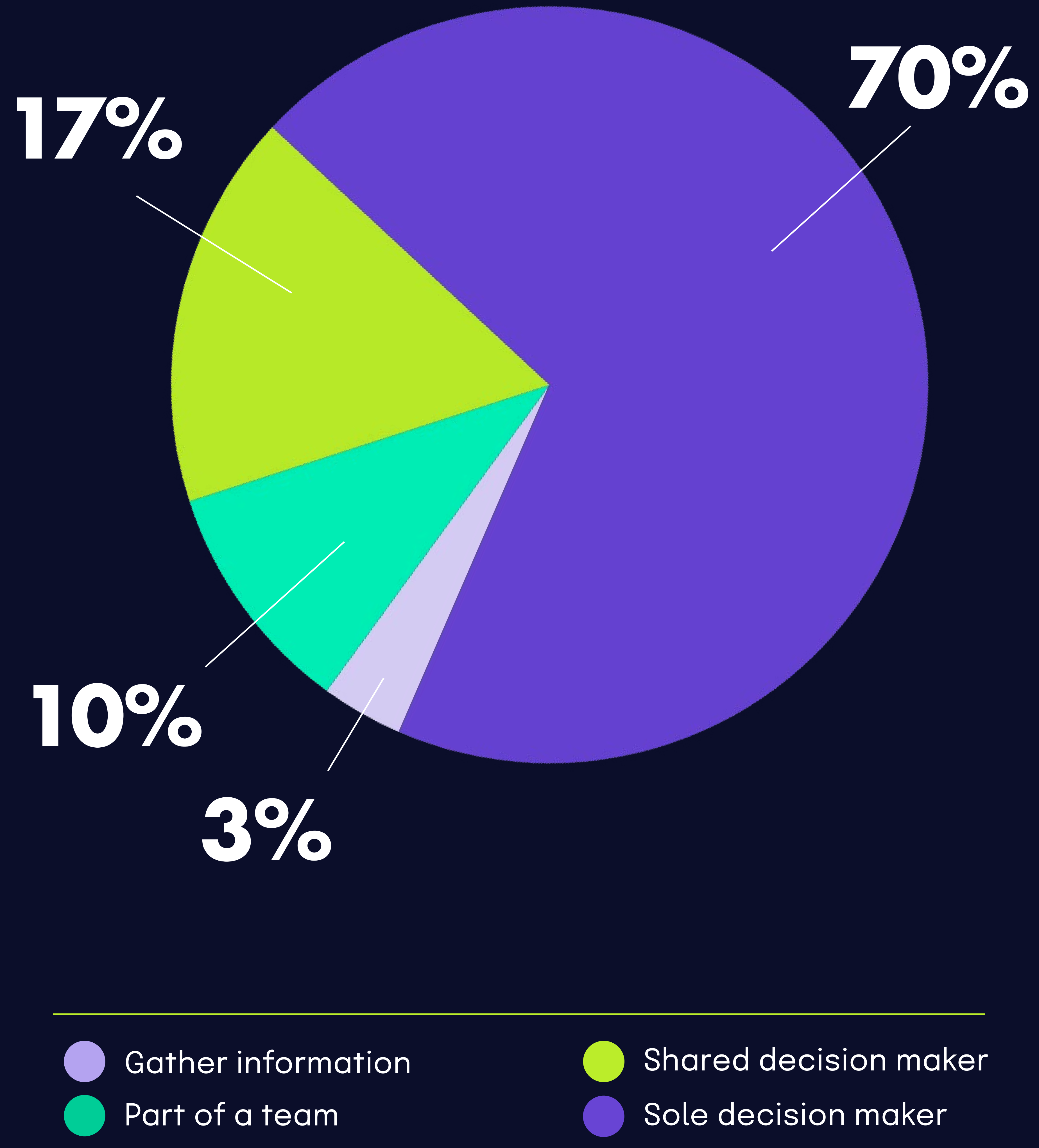
Department



Job function



Decision-making capabilities



hyperproof

About 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, Appian, Outreach, and Thales.

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

Get a Demo

2025 IT and Compliance Benchmark Report

The Reader's Digest Issue