hyperproof

2023 IT COMPLIANCE AND RISK BENCHMARK REPORT

2022'S GAME-CHANGERS AND THE OUTLOOK ON 2023

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

TABLE OF CONTENTS

FOREWORD

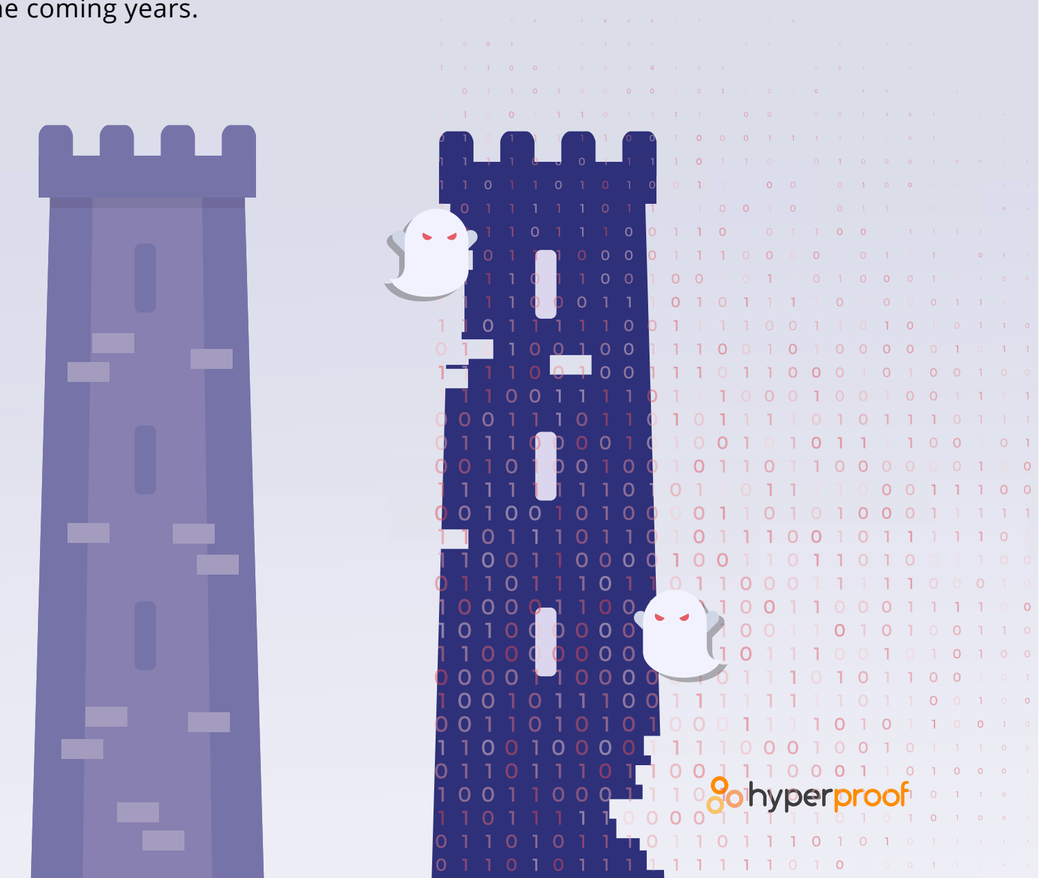
COMPANIES ARE LEVELING UP IN RESPONSE TO RISK

Hyperproof conducts an annual survey to uncover the top challenges IT compliance professionals face and what issues they are focused on in the coming year. We've asked over 1,000 survey respondents about their pain points, IT risk and compliance budgets, staffing, risk management best practices, and much more to provide an in-depth view of the market's current state and what to prepare for this year.

2022 provided highly publicized security breaches that had C-Suites across the country pivot their attention to governance, risk, and compliance. That theme carries through in our data: **security and compliance professionals are facing the pressure to level up their risk responses to avoid becoming a breaking news story about another security breach**. In 2022, regulator responses to security breaches rapidly increased (along with public scrutiny), and new regulations have required companies to quickly adapt, including having a new game plan for communicating risk to their C-Suites, the board members, and employees. Despite a looming recession, security and compliance is one area where spending continues to remain high, and companies are turning their attention toward making compliance operations a regular best practice across all facets of their organizations.

Surprisingly, more companies than expected are reporting that they still struggle with manual processes and tasks despite only 10% reporting that they use spreadsheets to manage compliance operations and risk, and 89% reported using a GRC software to manage compliance operations and risk. This could be due to the fact that the majority of respondents report handling risk and compliance in silos, which we will investigate throughout this report.

In 2022, **1 in 2 companies with 1,000-5,000 employees** suffered a security breach, indicating that threat actors are as motivated as ever to gain access to lucrative and corporate data. **57% of surveyed organizations expect to spend more time on risk compliance management in 2023**, as opposed to last year's 35%. Additionally, **63% of survey respondents expect to spend more money on IT compliance and risk management**, an increase from 45% in 2022. With security breaches on the rise and greater attention from the C-Suite and board on how to prevent them, companies are poised and ready to level up their risk and compliance management processes in the coming years.



OUTLOOK FOR 2023

The Western economy is bracing for an increase in turmoil — including a cocktail of highly-publicized security breaches, rising inflation, continued supply chain disruptions, volatile interest rates, and an anticipated recession — while, at the same time, compliance professionals and attorneys are preparing for even more regulatory changes (some of which we will cover later). These preparations include planning to expand their teams, outsourcing more work, and maintaining their budgets, all discussed throughout this report. But first, let's dive into what is driving security, compliance, and risk management professionals to increase their capacity.

REGULATORS ARE CRACKING DOWN

In 2022, regulators and legislators at both the federal- and state-level moved forward with efforts to curb a sharp rise in data collection and retention that has heightened the risks and costs of breaches. Congress did not succeed in enacting a federal privacy law, but they did initiate a proposal to move forward on these topics pursuant to existing statutory authorities. Several states enacted new comprehensive state privacy legislation, and others enacted issue-specific laws focused on topics including children's and employees' privacy, while state regulators in California, Colorado, and elsewhere took critical steps toward implementing their own privacy laws.

Russia's invasion of Ukraine also brought increased attention from both public and private sectors around the importance of robust cybersecurity strategies and tactics. The federal government continues to move forward with policies designed to encourage continued vigilance, like the Cyber Incident Reporting for Critical Infrastructure Act of 2022 and the President's Cybersecurity Executive Order.

Cybersecurity laws continued to evolve outside of the US as well. Regulators at both the UK and the EU grappled with the fallout from Schrems II, pushing companies to do more to keep personal data in Europe. However, the introduction of the Trans-Atlantic Data Privacy Framework provided a possible compromise to allow personal data to flow across the Atlantic. Regulators in Ireland issued over $600 million in fines against Meta for several alleged violations of the General Data Protection Regulation (GDPR), and Argentina proposed new legislation designed to bring their cybersecurity laws more in line with GDPR. Australia became the target of massive ransomware attacks and quickly enacted legislation that would significantly increase penalties for data breaches to a minimum of AU $50 million.

INDIVIDUAL ACCOUNTABILITY HAS CISOs DIVIDED

As anxiety around cybersecurity increased, along with the amount of legislation in response, security breaches became hot topics in the news. Regulatory bodies increased their emphasis on individual accountability, especially for senior corporate officers and other prominent organizational figureheads like Drizly CEO James Cory Rellas. Notably, the FTC specifically named and sanctioned Rellas — a new move for the governing body. This change in posture, combined with the results of our survey, indicate a larger shift towards enforcement, particularly for organizations that don't have adequate controls around the protection and disposition of consumer data.

Joe Sullivan, Uber's former CISO, attempted a cover up of an incident where hackers stole the personal details of 57 million customers and the personal information of 600,000 Uber drivers, which led to a media firestorm. His subsequent conviction — one that held him personally accountable but did not directly impact Uber as a company — had a massive and divisive impact on the security community. The conviction could have wide-ranging consequences for CISOs — some argue that the case will prompt more whistleblowers in the future, and some assert that security chiefs should be prepared to be held personally accountable for incidents they are involved in. This discourse continues into 2023 as more companies are taking an eagle-eyed approach to managing security compliance to avoid becoming another news story and facing the subsequent reputational damage.

DATA BREACHES ARE IN THE NEWS

As we discussed earlier, data breaches were a hot news topic in 2022, which begs the question: are breaches actually increasing, or are we simply more focused on them?

The answer is nuanced: while bad news generates more public interest and a splashy headline attracts more attention than the fine print in a legal document, security breaches have, in fact, legitimately impacted more organizations in the last three years than the 10 years prior. As more companies leverage new technology, including social media, their exposure to cyber attacks increases. Consumers are also becoming more aware of the vulnerabilities of their online data, and companies are wary of the reputational damage that can ensue when a breach occurs.

Take, for example, Aerojet Rocketdyne, who settled for $9 million to resolve allegations that the company violated the False Claims Act (FCA) by misrepresenting their compliance with cybersecurity requirements in certain federal government contracts. These FCA violations with the DOJ are illustrative of the sorts of risks DoD contractors face in their attestations. CISOs are now laser-focused on tightening their security and compliance programs to avoid becoming another news story, which is having an impact on every facet of the InfoSec space.

SECURITY, COMPLIANCE, AND RISK PROFESSIONALS ARE PREPARING FOR REGULATORY CHANGES

All of this pressure has InfoSec professionals bracing for regulatory changes, many of which either went into effect on January 1, 2023 or will go into effect this year. Some of the highest-impact regulatory changes are outlined below:

DATA PRIVACY IN THE US

The year 2023 will go down in history as marking the beginning of a profound shift in the philosophy underlying data privacy laws in the United States. US data privacy laws have historically been reactive, as opposed to the EU's GDPR, which enables individuals to effectively own their personal data and arms them with the legal right to control it. In 2023, nearly 30 states have some form of privacy protection law in place or in draft for debate and passage. Five states already have comprehensive policies in place: California, Utah, Colorado, Connecticut, and Virginia. California has already implemented GDPR-inspired standards statutes, and Colorado, Connecticut, Utah, and Virginia are following close behind. Additionally, California, Colorado, and Virginia are set to make important updates in 2023 that are shifting the underlying philosophical framework regarding data privacy protection.

First, let's start with California and the changes to the California Privacy Right Act (CPRA). On January 1, 2023, an amendment to the California Consumer Privacy Act (CCPA) went into effect that provides consumers the right to correct inaccurate personal information that businesses have about them and the right to limit the use and disclosure of sensitive personal data collected about them. This amendment affects for-profit businesses that conduct operations in California and either have gross revenues over $25 million, buy, sell, and/or share personal information of 100,000+ consumers, or derive more than 50% of their revenue from personal information. The CPRA also establishes the California Privacy Protection Agency (CPPA), which investigates and enforces violations of privacy laws, including the power to impose fines on organizations that violate these laws. The CPRA also works to educate consumers and businesses about privacy rights and responsibilities and provides guidance on how to comply with privacy laws.

The Virginia Consumer Data Protection Act (CDPA) also went into effect on January 1, 2023. Data collectors must now obtain explicit consent for collecting or using sensitive data or for collecting or using minors' personal data. The changes also include the assessments of vendors' privacy and security posture, including their ability to delete or return data at the end of a contract.

Lastly, on July 1, 2023, changes to the Colorado Privacy Act (CPA) will go into effect. Like the CDPA, the updates will require new data privacy and security assessments for high-risk processing and assessments of vendors' privacy and security posture, including their ability to delete or return data at the end of a contract. The updates also include universal opt-out by 2024 and a ban on dark patterns. Affected organizations include companies that do business in Colorado or target Colorado residents and either process the personal information of 100,000+ residents or process the personal information of more than 25,000 Colorado residents and profit from the sale of personal information. Violations incur a $2,000 fine (up to $500,000 total).

PRIVACY REGULATIONS IN CHINA

China's Personal Information Protection Law (PIPL), which took effect in November 2021, has had a ripple effect across global industries. It somewhat aligns with GDPR and other global privacy regulations, including that the data subject has the right to access, right to withdrawal, and the right to deletion. However, it vastly differs in key areas: the state-based agency, The Cyberspace Administration of China (CAC), will oversee PIPL compliance, departing from the global norm of independently operated agencies who oversee compliance. It's not clear what the precise terms of applicability are yet, but it's reasonable to assume many mid-to-large-sized entities will need to comply with PIPL. Additionally, as other neighboring countries draft their own privacy laws, there's a chance PIPL may carry significant influence over the future of regulation in parts of Asia.

POTENTIAL UPDATES TO NIST CYBERSECURITY FRAMEWORK

In January 2023, the National Institute of Standards and Technology (NIST) announced its intent to make new revisions to its Cybersecurity Framework (CSF) document, with an emphasis on cyberdefense inclusivity across all economic sectors. The new CSF could see protocols surrounding increasing international collaboration in cybersecurity efforts while still retaining the level of detail within the existing standards and guidelines to ensure the framework is scalable and useful for as many organizations as possible. Current recommendations for updates include a request for the new CSF to more clearly relate to other NIST frameworks, making improvements to the CSF's website, and expanding coverage and governance outcomes to supply chains.

UPDATES TO NIST CYBERSECURITY FRAMEWORK'S TREATMENT OF PNT SERVICES

In January 2023, NIST released NIST IR 8323 Revision 1, which established guidelines for applying the cybersecurity framework to responsible use of Positioning, Navigation, and Timing (PNT) services. The Foundational PNT Profile was created by applying the NIST CSF to help organizations identify systems dependent on PNT, identify appropriate PNT sources, detect disturbances and manipulation of PNT services, and manage the risk to these systems. Organizations may use this profile as a starting point to apply their own unique mission, business environment, and technologies to create or refine a security program that will include the responsible use of PNT services.

NEW DIRECTIVES FROM THE EU

The EU Data Governance Act (DGA) will become applicable in late 2023 and will facilitate data access and sharing with the public sector, adding another layer of complexity as organizations try to understand what it takes to facilitate compliant data transfers. The DGA will establish robust procedures to facilitate the reuse of certain protected public sector data and foster data altruism across the EU. It will define a new business model for data intermediation services that would serve as trusted environments for organizations or individuals to share data, support voluntary data sharing between companies, facilitate the fulfillment of data sharing obligation set by law, enable individuals to exercise their rights under GDPR, and enable individuals to gain control over their data and share it with trusted companies.

SO, WHAT WILL THE IMPACT BE IN 2023?

This brings us to 2023: as a result, anxiety around cyber threats is high, and the need to quickly adapt to changing regulation is looming. As regulators pile on the pressure, organizations are pushed to respond by increasing headcount, tech stacks, usage of cloud-based software, and the amount of work they are willing to outsource to mitigate new and mounting compliance burdens.

First, let's discuss security, compliance, and risk management professionals' capacity to respond: with massive layoffs and The Great Resignation impacting organizations across the globe, companies are in dire need of more cybersecurity personnel to fill key roles. **ISACA's State of Cybersecurity Report 2022** reported the highest retention difficulties in the security and compliance industry in years. 60% of those surveyed reported difficulty in retaining qualified cybersecurity professionals, up from 53% in 2021. Cybersecurity professionals are leaving their positions in droves due to poor financial incentives, being recruited by other companies, limited opportunities for career advancement, high work stress levels, and lack of support from management.

As a result, turnover is high and companies are responding by broadening their searches to include candidates without traditional degrees, offering more flexible schedules to attract and retain qualified talent, and providing more support and training for InfoSec employees. Both technical and soft skills gaps are becoming more pervasive in the current hiring market, and organizations are weighing their options between increasing their use of contractors and consultants and increasing their in-house team size.

This critical resource shortage is colliding with the ever-expanding landscape of the Cloud and an increase in the usage of technology platforms to store and manage data. The pandemic and subsequent migration to the Cloud had unintended compliance-related consequences: businesses (especially those in the Technology sector) now deal with under-protected cloud data. As traditionally in-office companies attempted to transition overnight to virtual workplaces, many prioritized speed over security and, subsequently, left data exposed — while potentially putting themselves out of compliance. Today, many organizations are still catching up on ensuring that their cloud processes comply with data privacy regulations — regulations that, which we established above, are constantly changing.

This presents a circuitous problem for InfoSec professionals: the more digital tools they use to get work done, the more third-party risk they expose themselves to, but these tools have become integral in their response to the pandemic and the subsequent economic turmoil that has ensued. In 2023, initiatives have slightly shifted: now that InfoSec professionals are leveraging Cloud data and digital platforms to manage risk and compliance, they must find ways to consolidate these platforms to both reduce their vulnerabilities and get a holistic view of their compliance posture.

Survey respondents clearly understand the need to level up operational compliance, but risks have overwhelmed their capacity to respond. Our survey results also revealed that **organizations are still struggling to connect the dots between compliance and risk — a key strategy to responding to increased regulatory scrutiny**. While more companies than ever are adopting new technologies to manage compliance and risk, the two are still operating in silos, creating unexpected and additional manual processes and preventing InfoSec professionals from getting the full view of their risk and compliance posture. The colliding impacts of geopolitical, economic, and climate concerns require more integrated and agile risk management and compliance operations paradigms to help companies stabilize, and potentially even grow, during a challenging business environment.

TOP 5 KEY THEMES FROM THIS YEAR'S SURVEY

1. THE RELATIONSHIP BETWEEN THE C-SUITE AND INFOSEC PROFESSIONALS IS CHANGING

In October, 2022, Joe Sullivan, the former Uber security chief, was found guilty of one count of obstructing the FTC's investigation of a breach of customer and driver records and failing to report this breach to government regulators. He was also found guilty of one count of misprision, or acting to conceal a felony from authorities. 33% of respondents said that in the wake of the Joe Sullivan/Uber case verdict, their company has made changes to how the Legal team works with their CISO to protect the company. Additionally, the data shows that CFOs are becoming more present when it comes to decisions about investing in risk and compliance efforts. As more stakeholders look to get involved to avoid a security disaster, InfoSec professionals should anticipate a sharp increase in requests for reports, presentations, and communication on their security, risk, and compliance postures.

2. CHANGES IN THE MARKET ARE RESULTING IN NEW PURCHASE PATTERNS AND A SURPRISING INCREASE IN BUDGET

Even with a recession looming, security and compliance is one area where spend continues to remain high. Regulator response has been rapidly increasing, and new regulations are forcing companies to quickly adapt and expand their teams to meet new regulatory demands. 29% of respondents said that they allocate most of their annual governance, risk, and compliance (GRC) budgets to GRC tools, as opposed to compliance audits (25%), outsourcing/consultant work (22%), and staff (24%). This aligns with 2022's findings as well: the highest ranked category of where spend was allocated was GRC compliance tools at 28%.

3. THIRD-PARTY RISK REMAINS A MAJOR CHALLENGE

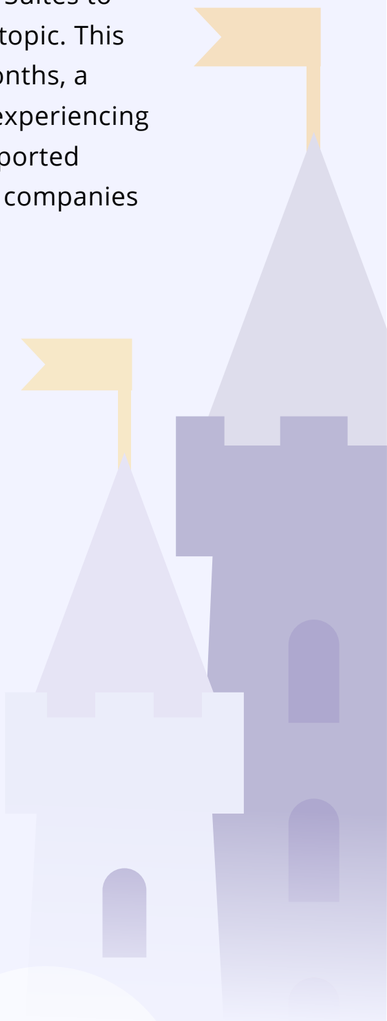
74% of surveyed companies have experienced an audit finding that they couldn't promptly resolve related to third-party risk management. Third-party risk remains a challenge that isn't adequately handled, and surveyees are continuing to expand their network of third-party partners. As a result, third-party risk is influencing supply chain decision-making — the third-party risk landscape has expanded to the point where a vendor's security and compliance posture may now be a deciding factor in business partnerships.

4. THE STRUGGLE TO UNIFY RISK AND COMPLIANCE MANAGEMENT PERSISTS

Companies clearly see the importance of unifying operational compliance and risk management. In a summary of actions taken, 73% of respondents have aligned their risk management with compliance efforts, and 57% of respondents believe that having a solid compliance program helps mitigate risks. However, 31% of respondents are still managing risk and compliance in silos, which results in additional manual processes, an increased workload, more stress, and less visibility into risk and compliance posture.

5. THE IMPACT OF DATA BREACHES REMAINS HIGH

News coverage of data breaches is relentless, and all eyes are on C-Suites to prevent their companies from becoming another trending security topic. This year, 42% of those surveyed experienced a breach in the last 24 months, a reduction from 2022's report where 63% of respondents reported experiencing a breach. However, the cost of data breaches remains high: 39% reported losing $1M-$5M on data breaches compared to 2022 where 44% of companies reported breaches costing between $1M-5M.



TOP FINDINGS IN NUMBERS

In this year's survey, we found eight key statistics that indicated that companies are leveling up their response to risk and looking for ways to streamline compliance operations. Here are the top findings in numbers:

85%

of respondents say their company has a board member with cybersecurity expertise

As the board takes a magnifying glass to cybersecurity, compliance operations, and risk management, security and compliance professionals will need to brace themselves for a barrage of requests for detailed reporting, more internal assessments, and more frequent communication with the board around cybersecurity risk.

33%

of respondents made changes to how Legal teams work with CISOs because of the Joe Sullivan/Uber verdict

As a direct result from media coverage after the Joe Sullivan/Uber case, which we will discuss more in chapter 3, executive teams are paying more attention than ever to how their company is staying secure, meaning risk and compliance finally has a seat at the table. This has both its benefits and challenges for security, IT, compliance operations, and risk management professionals that they need to start preparing for well in advance. InfoSec professionals are going to need to level up their workflows to coordinate with more members across their organizations to maintain compliance.

51%

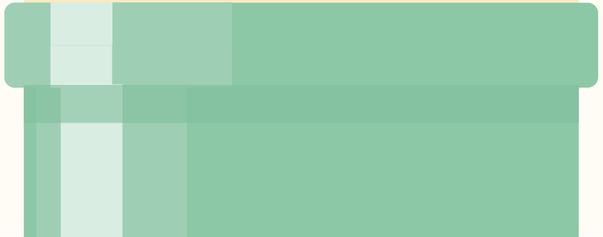
of respondents struggle with identifying critical risks to prioritize remediations

Although respondents were highly confident in their abilities to address risk, surveyees also noted that they are still struggling to identify and prioritize risks. This means that while respondents felt they were doing an adequate job of addressing risk, they still struggle with finding risk related information when they need it and must switch between multiple systems throughout the risk management process. While risk management is improving for many organizations, there are opportunities for further improvement.

ONLY 10%

of respondents use spreadsheets to manage their IT compliance efforts in 2023, vs. 43% in 2022

GRC software usage for risk tracking, risk management, IT compliance management and third-party risk management has increased year-over-year, while use of spreadsheets has declined. This is a huge shift from 2022's benchmark data, indicating that the market is quickly adapting GRC tools to operationalize compliance and risk workflows.



57%

of respondents believe that having a solid compliance program helps mitigate risks

Over half of survey respondents agree that unifying risk and compliance helps mitigate risk in the long-run, but many in the industry are still struggling to do so. Connecting the dots between compliance and risk is still a challenge even though the majority of respondents know it's a high priority and leads to a long-term reduction in risk.

ONLY 10%

of respondents have an integrated view of risks and have aligned risk and compliance activities

Despite only 10% of respondents reporting that they still use spreadsheets to manage their IT compliance efforts, this data point indicates that the overwhelming majority of surveyees still struggle to align risk and compliance activities, even with a tool in place.

57%

of all respondents anticipate spending more time on IT risk management and compliance in 2023

32% of respondents said they would postpone adding additional compliance frameworks and/or certifications due to lack of capacity to take on new work and to mitigate stress in the coming months, but this can only happen for so long. With security breaches on the rise and increasing pressure to keep companies safe, compliance managers will need to find ways to reduce their manual administrative tasks to better focus on IT risk management.

70%

of respondents plan to grow their compliance team over the next two years

In a volatile economy, spending on compliance operations and risk management is still expected to increase, as all eyes are on CISOs to prevent data breaches. This willingness to invest in risk management is in sharp contrast to other categories of corporate spending in the current down economy. Yet, this trend to hire more staff is logical, given that 32% of respondents said they had to postpone the pursuit of new compliance frameworks/certifications due to insufficient resources.

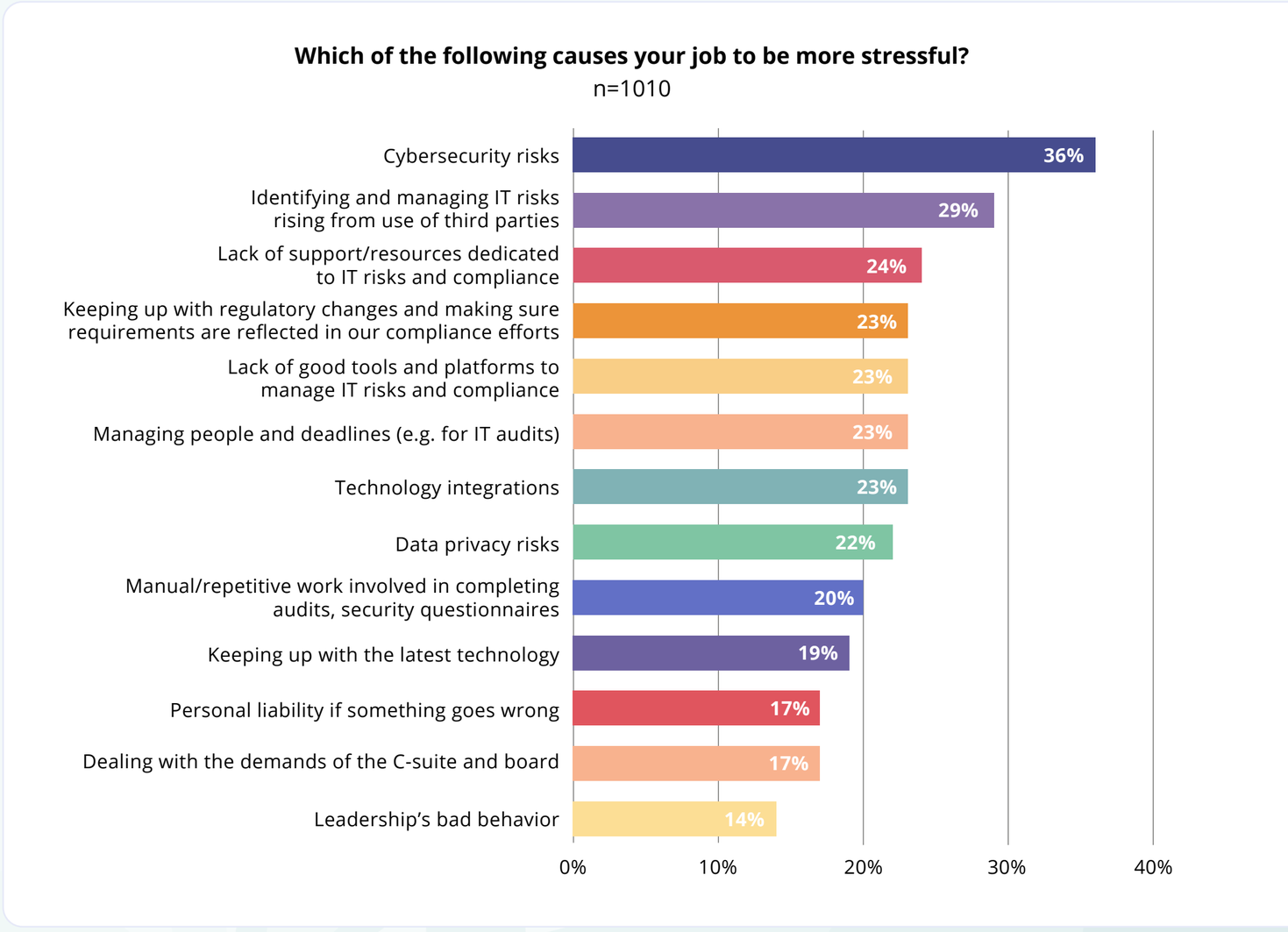
CHAPTER 1

STILL GRINDING: ATTEMPTING TO OPERATIONALIZE COMPLIANCE AND RISK

SEEING THE FOREST THROUGH THE TREES

This year, we found that security, compliance, and risk management professionals were more concerned with short-term, immediate threats as opposed to handling larger scale decisions like long-term security issues. Respondents reported that their **number one source of stress was cybersecurity risks (36%), followed by third-party risk (29%)**.

Respondents are focusing on tactical problems rather than the bigger, more long-term challenges, which could be a result of the burden of manual processes. Although **58% of respondents are reducing their manual processes with GRC platforms**, they still aren't able to be as strategic about risk and compliance as they would like — they are struggling to see the forest through the trees. The reason? Compliance professionals are still burdened with administrative tasks: we found that **the average respondent spends 38% of their time at work on manual tasks**. This is an interesting turn of events, considering that increased regulatory scrutiny is going to require security, compliance, and risk professionals to approach their job functions with more long-term strategy.



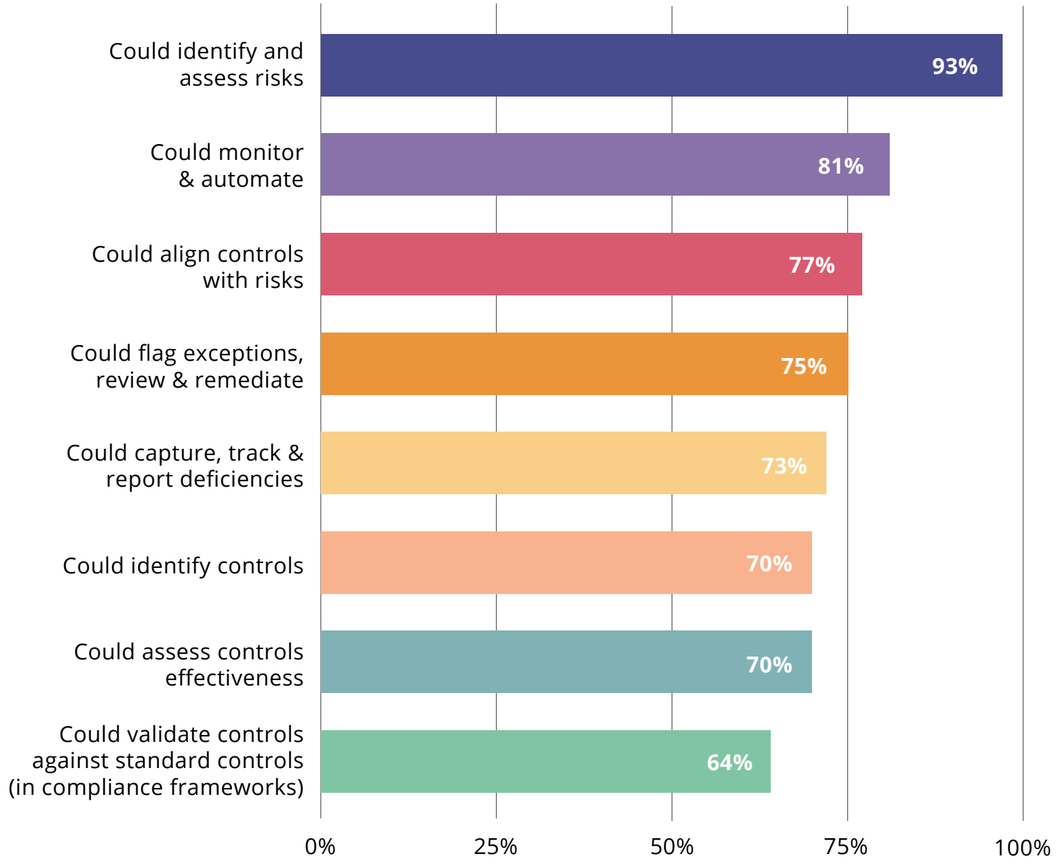
RISK MANAGEMENT CONFIDENCE REMAINS HIGH, BUT DATA SILOS PERSIST

Risk Management is taken seriously by respondents as a central part of business initiatives and top-of-mind for surveyees, with **93% of respondents feeling that they've done well in identifying and assessing risks**.

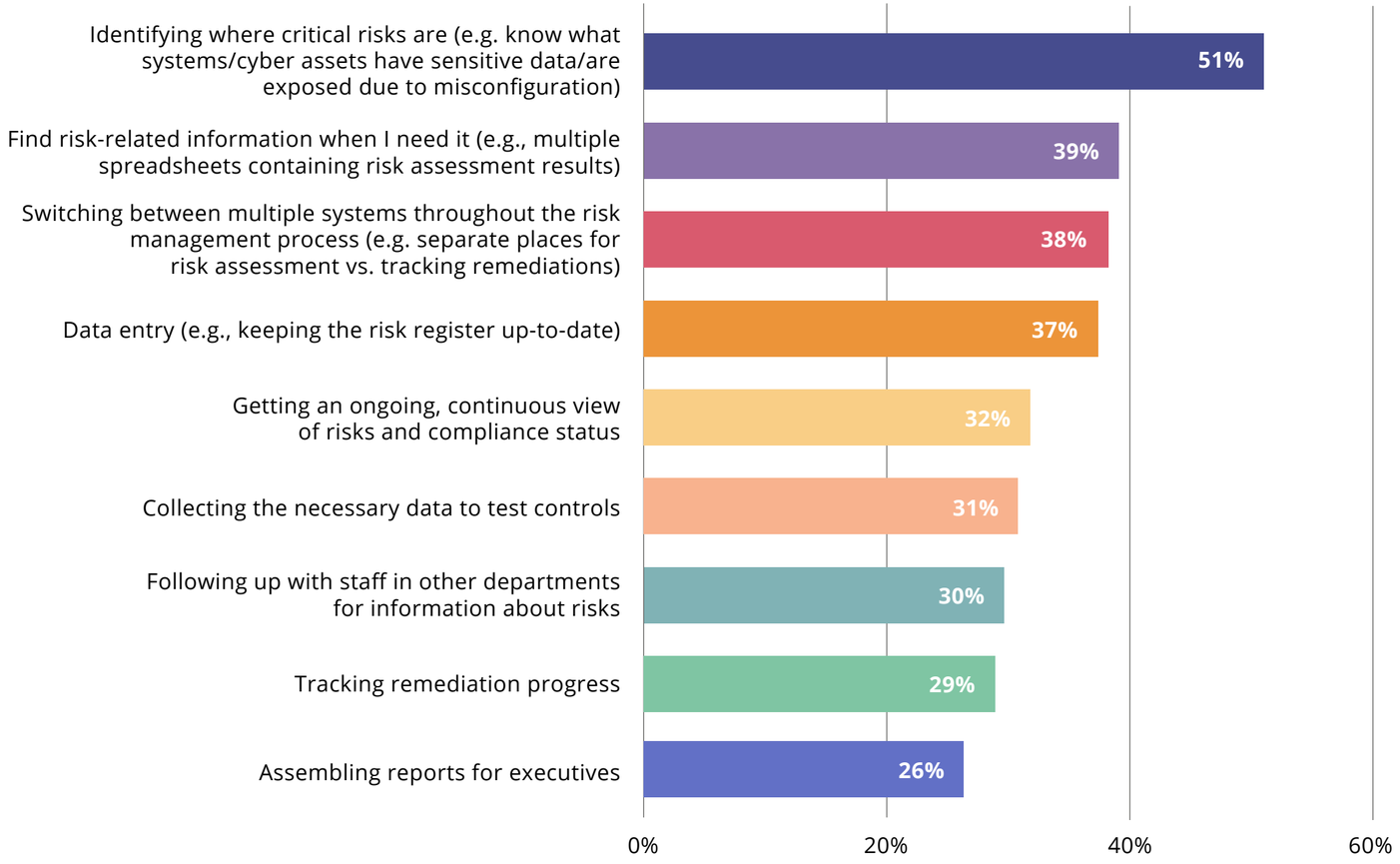
IT risk assessments also continue to be a high priority. **56% of InfoSec professionals are conducting annual security risk assessments**, and **27% are conducting biannual assessments**. Unsurprisingly, mature companies that had more employees and a longer business tenure were prone to conduct assessments twice a year, likely due to the size and complexity of their security compliance programs.

Although respondents grasp the importance of risk management, processes for managing IT risks lag behind their intentions. Despite this overwhelming confidence respondents have about identifying and assessing risks, **51% say they struggle with identifying where the critical risks are** to assess what remediations to prioritize. **30% of respondents** said their process to identify controls that can mitigate risks **does not meet their company's objectives** and **39% of all respondents said they struggle with finding risk-related information** when they need it.

In your opinion, how well is your company doing in performing each of the following risk management actions?
n=1010



What recurring or time-consuming tasks do you struggle with when managing security and data privacy risks in your internal environment?
n=1010



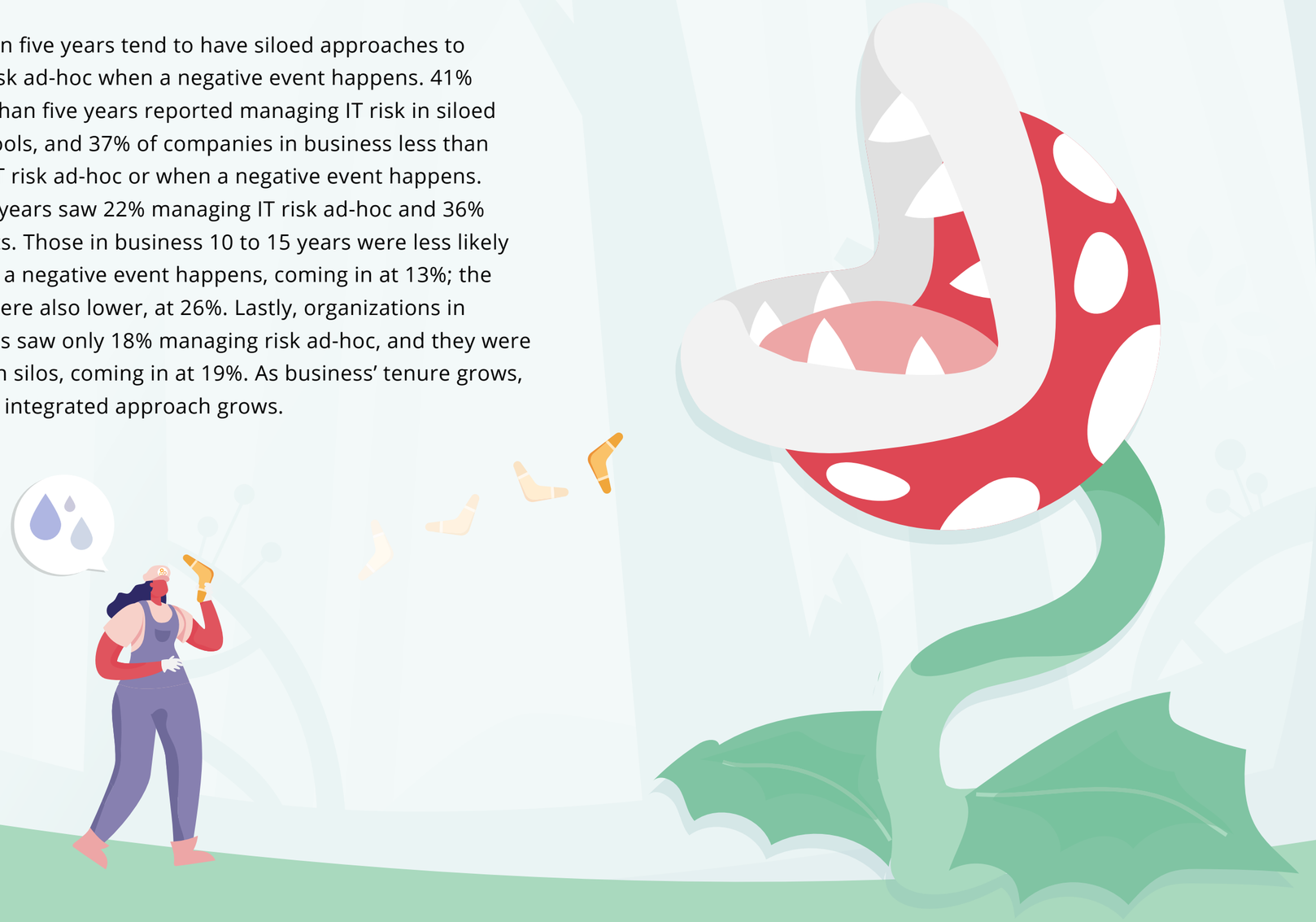
So, why are surveyees so confident in their ability to address risks but still struggling to identify risk-related critical tasks? Identifying and prioritizing critical risks is, by far, considered the most time-consuming activity related to managing security and data privacy risks. This problem is at least partially caused by respondents not having the right data at their fingertips. Additionally, **38% of respondents admitted that they switch between multiple systems throughout the risk management process** and that they have separate places for risk assessments vs. tracking remediation efforts, such as multiple spreadsheets containing risk assessment results or multiple platforms tracking risk.

THE KEY TAKEAWAY

Because risk management and compliance operations activities are still operating in silos, organizations are struggling to unify compliance and risk. In fact, 90% of surveyed organizations are managing risks and their compliance program in silos, which we will discuss more in detail in chapter 5.

SEGMENT DIFFERENCES: DOES COMPANY SIZE PLAY A FACTOR?

Companies in business less than five years tend to have siloed approaches to risk management or manage risk ad-hoc when a negative event happens. 41% of companies in business less than five years reported managing IT risk in siloed departments, processes, and tools, and 37% of companies in business less than five years reported managing IT risk ad-hoc or when a negative event happens. Companies in business 5 to 10 years saw 22% managing IT risk ad-hoc and 36% managing in siloed departments. Those in business 10 to 15 years were less likely to manage risk ad-hoc or when a negative event happens, coming in at 13%; the siloed efforts in this segment were also lower, at 26%. Lastly, organizations in business for more than 15 years saw only 18% managing risk ad-hoc, and they were also less likely to manage risk in silos, coming in at 19%. As business' tenure grows, the likelihood of them using an integrated approach grows.



OPERATIONALIZING COMPLIANCE REMAINS A TOP PRIORITY

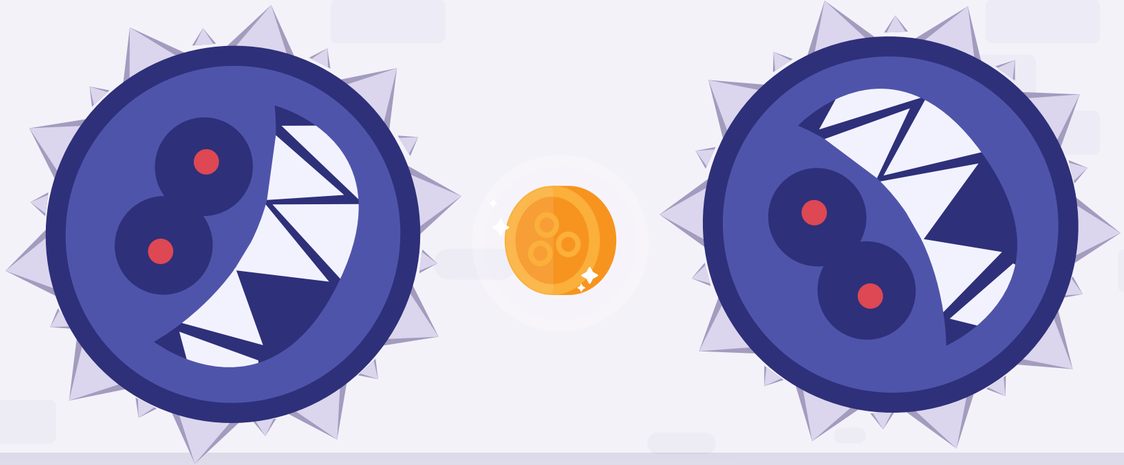
ONLY 10% **of respondents use spreadsheets to manage their IT Compliance efforts in 2023, vs. 43% in 2022**

There were several compelling trends we found while digging into the survey data on compliance operations. First, the vast majority of organizations consider control testing to be an important aspect of their security and infosec compliance program but are heavily taxed by the burden of manual testing. **52% of organizations test all of their controls, while 41% only test the most critical controls to mitigate risk**. On the other hand, only 9% of surveyed said they only test the controls needed for their next audit.

81% of respondents say they are meeting their company objectives when it comes to control testing, however **43% of respondents say their internal team still conducts manual control reviews** and testing to ensure those security controls are still operational. 4/10 respondents feel that control testing ("testing and validating the evidence before it's sent to external auditors") is a very time-consuming task. One thing to note is that some controls will always require manual testing — this is an inevitability due to some business processes, however, respondents are looking for ways to reduce unnecessary manual control testing where possible.

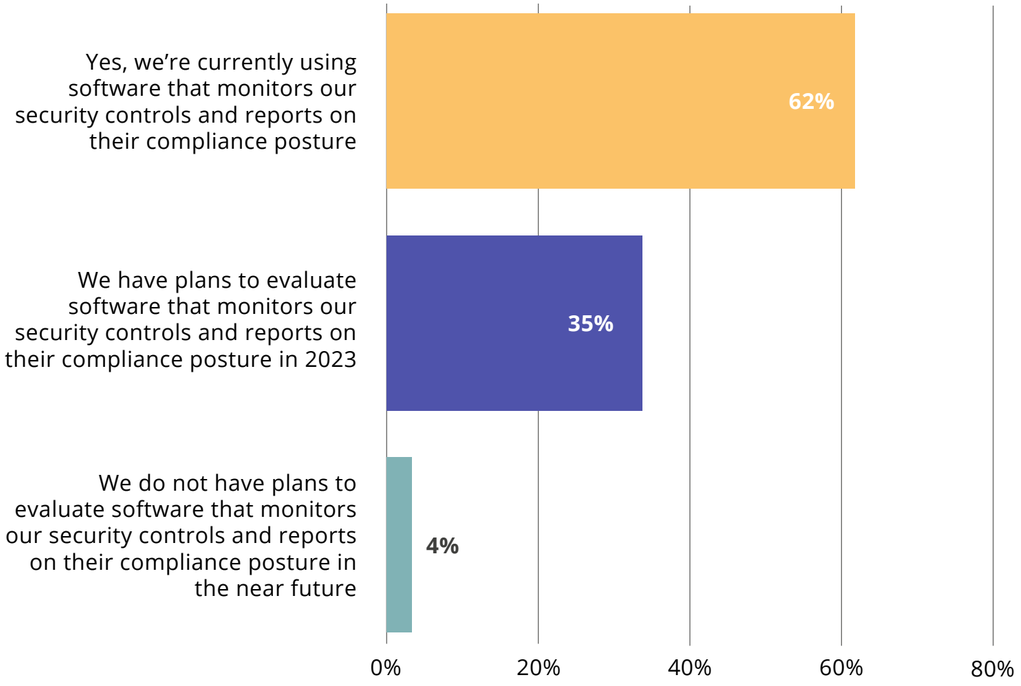
CONTROLS TESTING AND MONITORING AUTOMATION TRENDS

62% of respondents currently use software that monitors their security controls and reports on their compliance posture, while an additional **35% have plans to evaluate this type of software in 2023**. Only 4% do not have plans to deploy this type of software in the coming year. This finding is much higher than Gartner's prediction in March of 2022: they hypothesize that by 2026, 20% of companies will have more than 95% visibility of all their assets, which will be prioritized by risk and control coverage by implementing cyber asset attack surface management functionality, up from less than 1% in 2022. Clearly, a software-based approach to controls testing and monitoring is on the rise at a higher rate than Gartner's initial prediction, and security, compliance, and risk managers are much more aware of their need to automate as much of these processes as possible.



To save time, optimize your organization's existing resources and reduce cyber risk, 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?

n=1010



We also asked respondents how they would describe the actual testing of the effectiveness of controls within their organization around security and compliance. **93% said they either test all controls or test the most critical controls according to risk**, signifying that companies are taking a risks-focused approach to control monitoring, as opposed to an audit-focused approach.

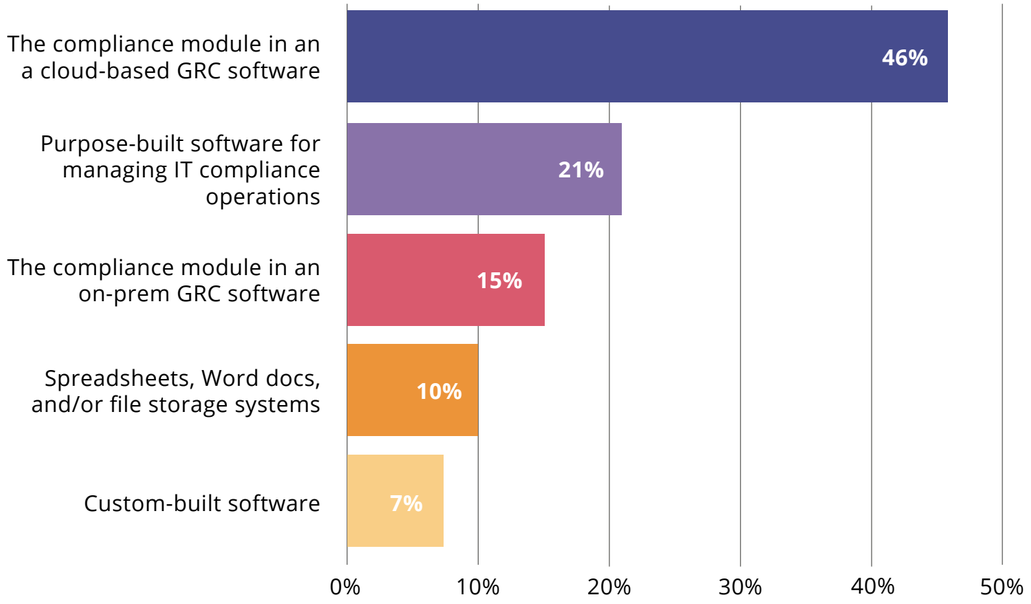
One tool to help facilitate this approach is continuous controls monitoring (CCM), which puts compliance teams on the same page as security teams and allows both to work in parallel to protect their organization. CCM helps compliance professionals serve as an extra set of eyes and ears to spot security weaknesses while helping to reduce the workload of an overburdened security team. An effective CCM system captures and analyzes data about preventative and detective controls (e.g., access, MFA, encryption, firewall, endpoint protection, deployment approval policy) from a security tech stack. Users are also able to set up tests to automatically detect when preventative controls aren't operational, which risks have increased, and when a company is out of compliance.

TECHNOLOGY: THE TOOL MOST USED TO HELP

How can compliance operations professionals solve these manual processes? **42% of respondents reported that they use a compliance module in a cloud-based GRC software**, which has been long-touted as the quickest and easiest way to reduce manual processes.

Strikingly, **only 10% of respondents use spreadsheets to manage their IT Compliance effort in 2023, vs. 43% in 2022**. InfoSec professionals are leaning in to adopting new technologies and cloud-based software to alleviate the burdens of compliance operations, an indicator that spreadsheet usage is not scalable for the long-term.

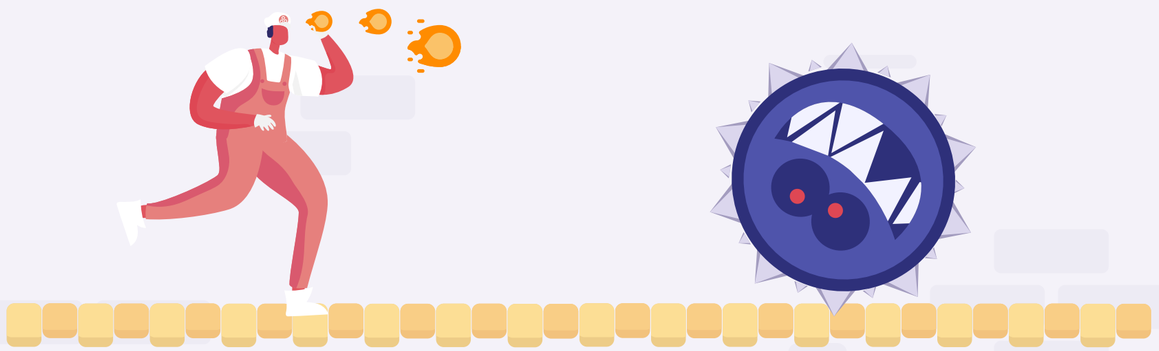
What tools are you using to manage your IT compliance effort (e.g. completing security audits for certifications like SOC II, ISO 27001, PCI, etc., testing and monitoring controls)?
n=1010



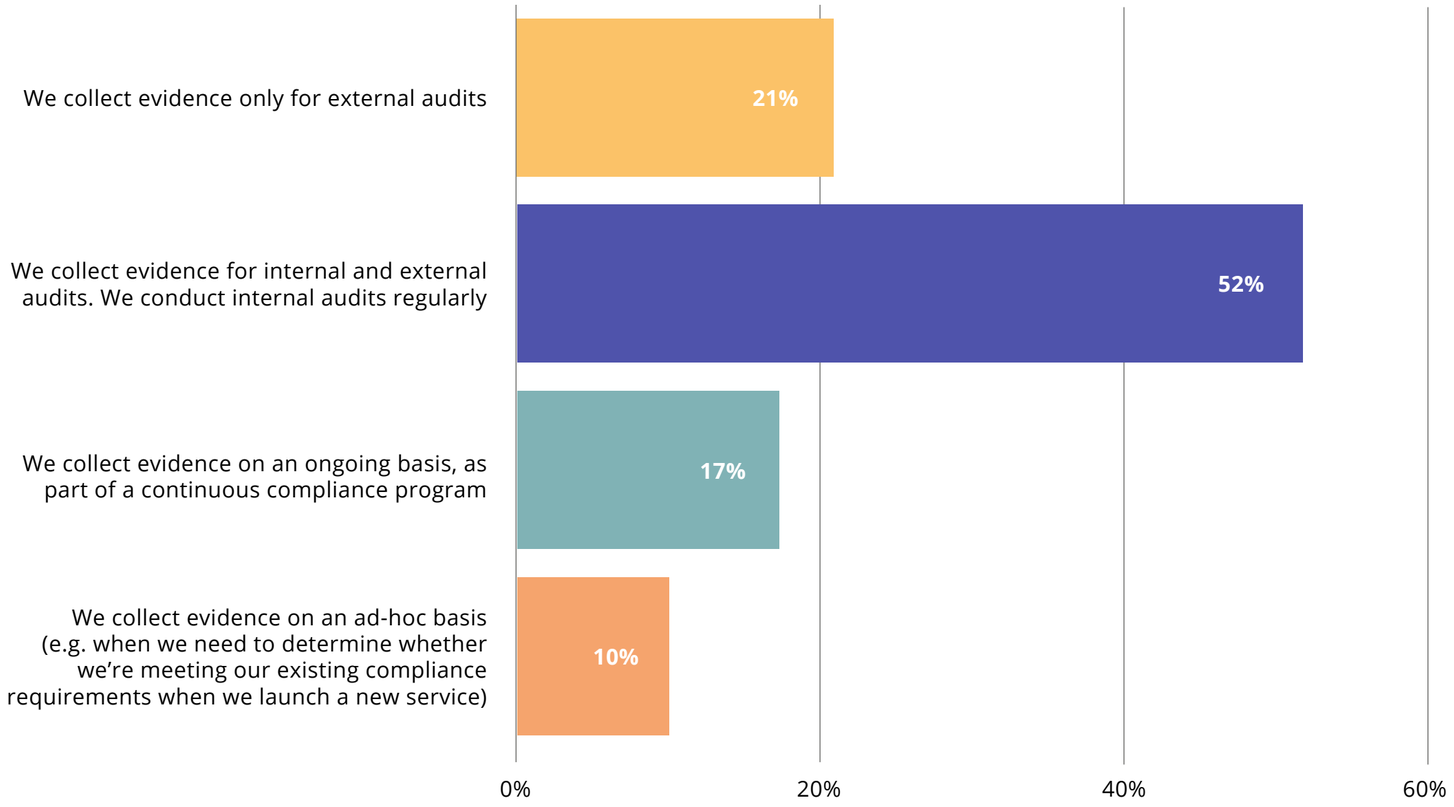
65% of respondents say they use the risk management module in a cloud-based GRC software to document and track risks. Additionally, over **70% of respondents have taken extensive actions that demonstrate their commitment to risk management.**

THE GOOD NEWS

Many companies have truly operationalized compliance — meaning they devote ongoing attention to ensuring that controls are operationally effective and not just written on paper. **69% of companies surveyed either conduct internal audits regularly or collect evidence on an ongoing basis, as part of a continuous compliance program**. Likewise, 89% of respondents use some type of software to manage their IT compliance efforts, as opposed to spreadsheets and Word documents, demonstrating the operationalization of compliance efforts by the majority of those surveyed.

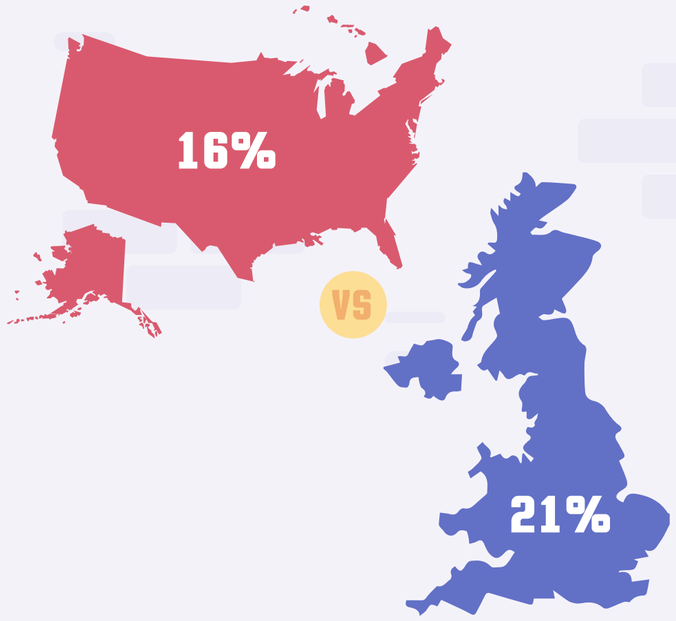


Choose the statement that most accurately reflects how your organization approaches evidence collection (to verify that controls are operating effectively):
n=1010



SEGMENT DIFFERENCES IN THE US VS. UK

In the United States, organizations were less likely to collect evidence on an ongoing basis, with only 16% doing so vs. 21% of UK organizations that do so. This difference between the countries is statistically significant.



MOST COMMONLY USED FRAMEWORKS

Managing multiple frameworks often means time-consuming, repetitive tasks (e.g. gathering evidence of a control's effectiveness multiple times) — but technology is opening doors for larger companies. Technology allows management of multiple frameworks to be more streamlined and simplified, resulting in these companies being able to further operationalize risk and compliance.

The patterns on usage of particular frameworks shows that companies are trying to mature their compliance operations, and that there is a desire to use frameworks that are well-trusted and well-vetted by outside organizations.

The more common frameworks used for compliance are more prescriptive and detailed, with ISO 27001 serving as a good example — as opposed to other frameworks, like SOC 2, which is a highly discussed framework among companies for business reasons (i.e. securing deals and checking off the very basics of security compliance). However, in 2023, we saw in this year's data that companies are shifting their attention to truly and strategically improving their security postures.

It comes as no surprise that the most common frameworks surveyees reported adhering to in the next 12 months are NIST Cybersecurity Framework, followed by ISO 27001. By using these more in-depth and holistic frameworks, companies are able to more clearly see how their current security compliance posture stacks up against the recommended baseline.

In the chart below, you'll notice that nearly all respondents manage multiple frameworks, which means they have additional processes to manage when testing controls and assessing risks.

COMPLIANCE FRAMEWORKS

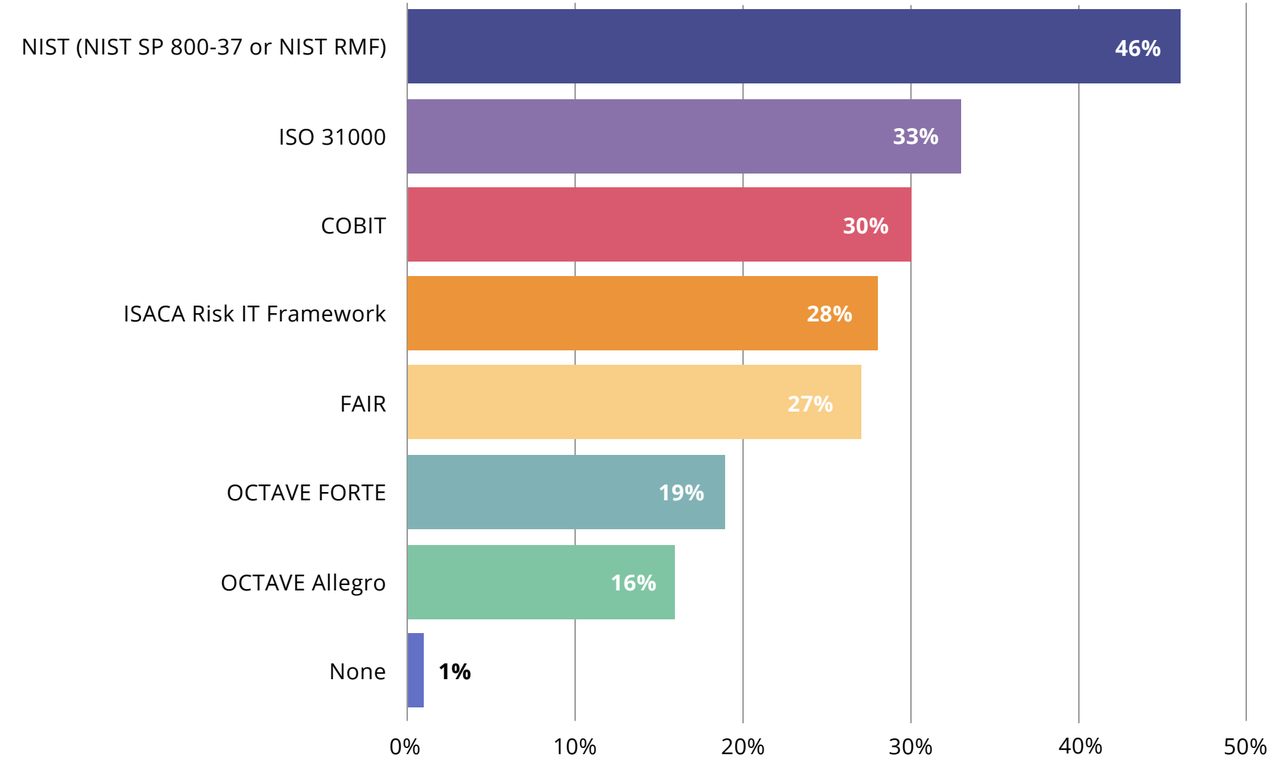
NIST Cybersecurity Framework (CSF)	30%	**CCPA / CCRA**	10%
ISO 27001	26%	**CSA CCM**	8%
COBIT	22%	**SOC I or SOC II**	8%
NIST Privacy Framework	17%	**HITRUST**	8%
Adobe's Common Control Framework (CCF)	17%	**HIPAA**	8%
Industry specific data security/privacy laws	16%	**PCI DSS**	8%
CIS Critical Security Controls	16%	**Consumer Reports The Digital Standard**	7%
CISQ	15%	**UK SOX**	7%
GDPR	14%	**FedRAMP**	6%
NIST 800-171	13%	**CMMC 2.0**	6%
Country-specific data security/privacy laws	13%	**Sarbanes-Oxley (SOX)**	6%
NIST 800-161	12%	**PIPEDA**	5%
Privacy Shield	11%	**UCF**	4%
NIST 800-53	11%		

n=1010

RISK MANAGEMENT FRAMEWORKS

When asked which of the following IT risk management frameworks are preferred to identify and manage IT risks, respondents ranked NIST (NIST SP 800-37 or NIST RMF) as the most common framework, followed by ISO 31000 and then COBIT. FAIR, surprisingly, came in at the fourth most common. FAIR is a more complex framework to adhere to due to the granular data needed to make calculations, but newer companies are adopting it more frequently. We found that **33% of companies in business less than 10 years use FAIR** — the largest usage of FAIR by company tenure. Newer companies are also less likely to use a software automation tool to manage IT risk and compliance.

Does your organization use any of the following IT risk management frameworks to identify and manage IT risks?
n=1010



SEGMENT DIFFERENCES

BY REGION

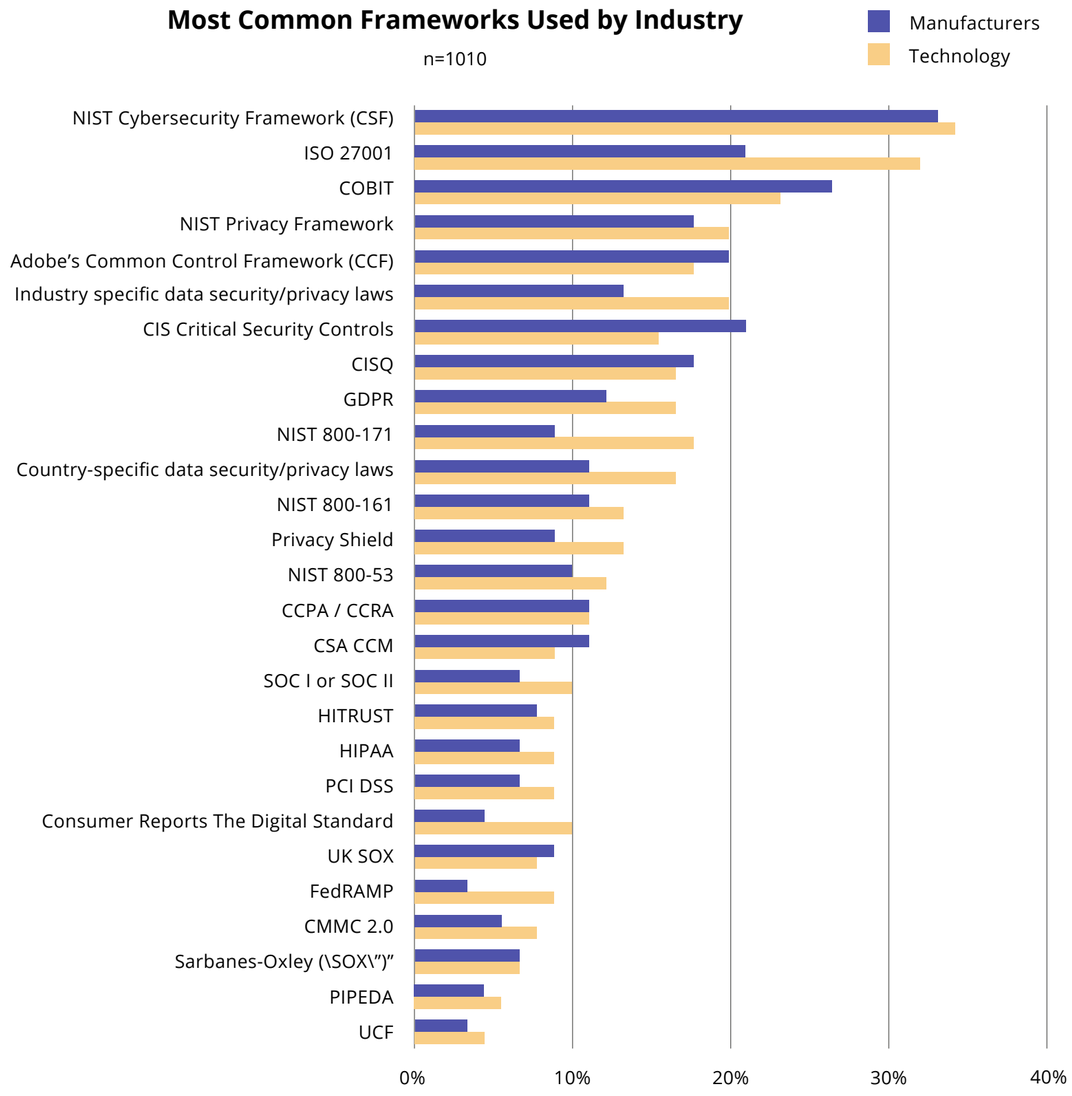
This year, the proportion of UK respondents using NIST frameworks closed in on ISO frameworks, with **43% using NIST frameworks and 44% using ISO frameworks**. The usage of NIST frameworks was much higher in the UK this year, an interesting change from previous years since ISO frameworks tend to be the most ubiquitous in the UK. The UK is clearly adopting more NIST frameworks, but this pattern does not run in the opposite direction — usage of NIST frameworks still dominates for US-based companies.

BY INDUSTRY

We also found that manufacturers, who historically have preferred to use ISO frameworks, reported that they are now using NIST frameworks the most. Across industries surveyed, NIST and ISO were still the leading frameworks adopted, followed by COBIT, NIST Privacy Framework, and Adobe's Common Control Framework (CCF).

BY REVENUE

Both companies with less than $10M in revenue and with 500M+ in revenue used NIST Cybersecurity Framework the most. Additionally, discussion about SOC I and SOC II has been a hot topic in the last few years, **but only 8% of respondents reported adhering to SOC I or SOC II in the next 12 months.**



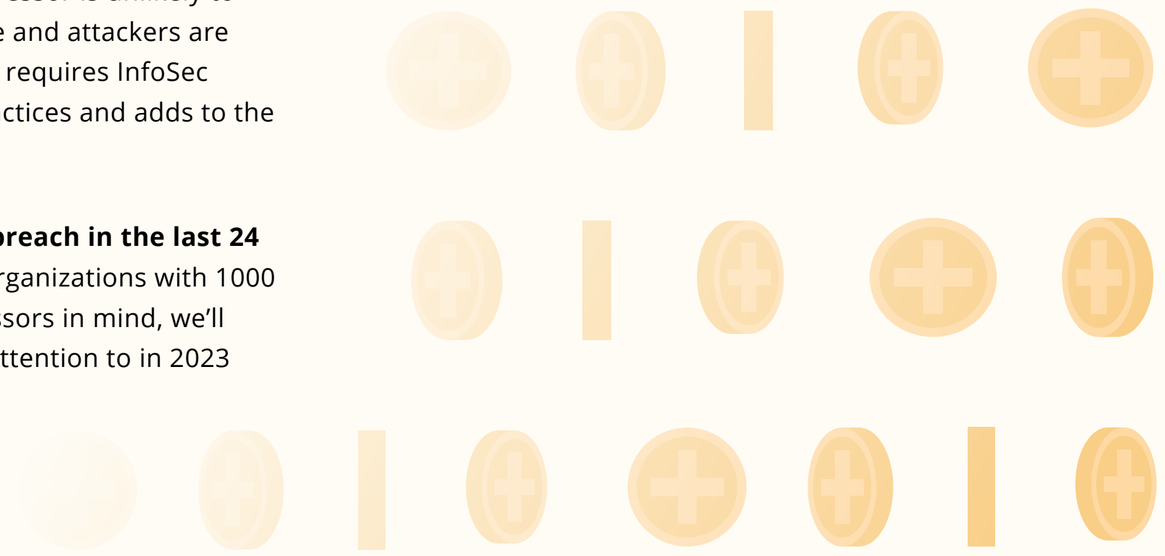
CHAPTER 2

1UP: A SURPRISING INCREASE IN BUDGET PRIORITIZATION AND ALLOCATION

EXPANSION PACKS FOR BUDGETS ARE COMING SOON

We saw significant changes from last year's report regarding budget and priorities: namely, that even though most Western companies are preparing for a recession, **most security, compliance, and risk management departments are actually planning to level up their efforts** and expand their budgets in 2023. This is likely due to mounting stress over cybersecurity risks, which was the **largest stressor reported for InfoSec professionals at 36**%. Notably, cybersecurity risks were also the highest reported cause of stress in 2022. This stressor is unlikely to change in the future, as cyber attacks are on the rise and attackers are becoming more creative with their approaches. This requires InfoSec professionals to stay up-to-date on security best practices and adds to the already growing pressure of preventing an attack.

Speaking of, **57% of organizations experienced a breach in the last 24 months**, with the largest percentile being midsize organizations with 1000 to less than 2500 employees. With these major stressors in mind, we'll cover which areas organizations want to pay more attention to in 2023 and how they plan on allocating their budgets.



ANTICIPATED TIME AND BUDGET SPENT ON IT RISK AND COMPLIANCE EFFORTS

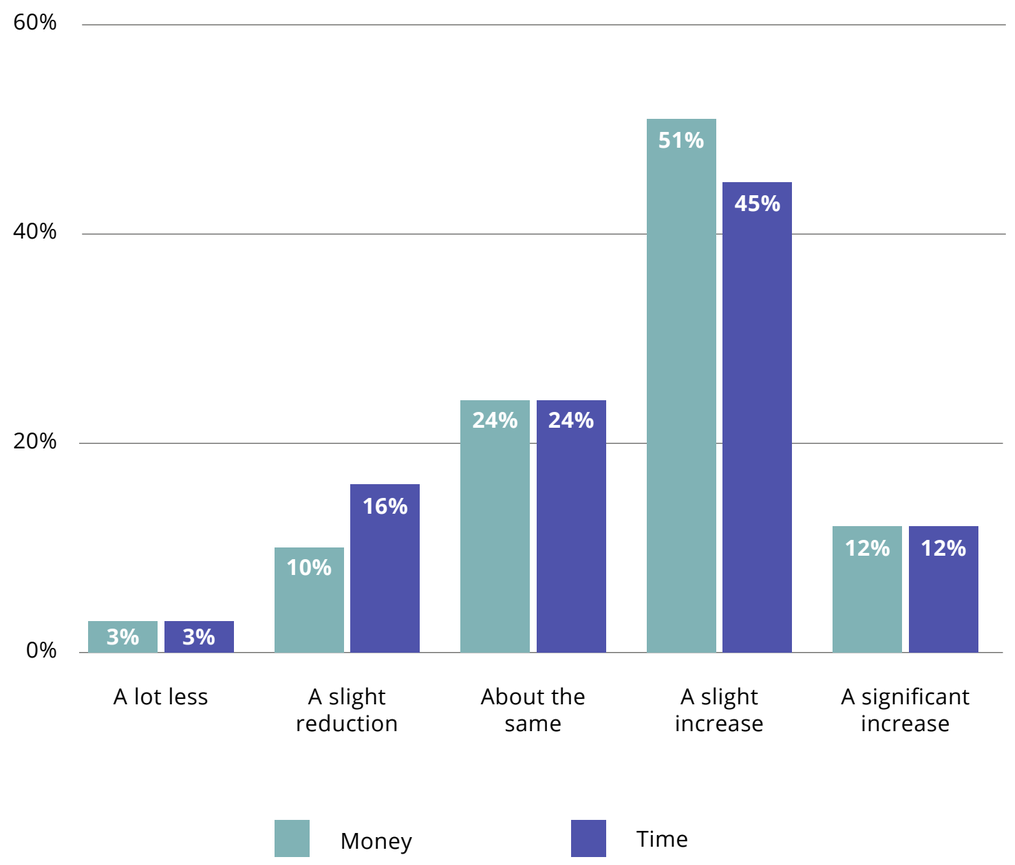
57% **of all respondents anticipate spending more time on IT risk management and compliance in 2023 vs. 2022**

All eyes are on risk management and compliance operations. **63% of companies** are planning to spend more money on compliance and risk in 2023 (vs. 45% in 2022), with an **average estimated percent increase in GRC budget in the next 12 to 24 months of 25%**. Of the respondents increasing their budgets, **76% expect to increase spend by at least 10%**. Only **13% said they will reduce spending, and 3% said they will spend "a lot less money"** on IT risk management and compliance operations in 2023.

Further, **57% of respondents said they would spend more time on IT risk management and compliance** in 2023, whereas in the prior year only 35% expected to spend more time on IT risk management. The change this year indicates a major shift in the market's perspective of how important it is to properly allocate their time and money toward IT risk management and compliance operations.

We found that the anticipated increase in both the amount of time and money spent on these efforts is nearly identical, indicating that InfoSec professionals and company leaders are feeling the pressure of regulatory scrutiny and are quickly expanding their capabilities and capacity in response.

Do you anticipate that your organization will spend more, less, or about the same amount of time/money on IT risk management in 2023 vs. 2022?
n=1010



HOW COMPANIES ARE ALLOCATING BUDGET TO REDUCE STRESS

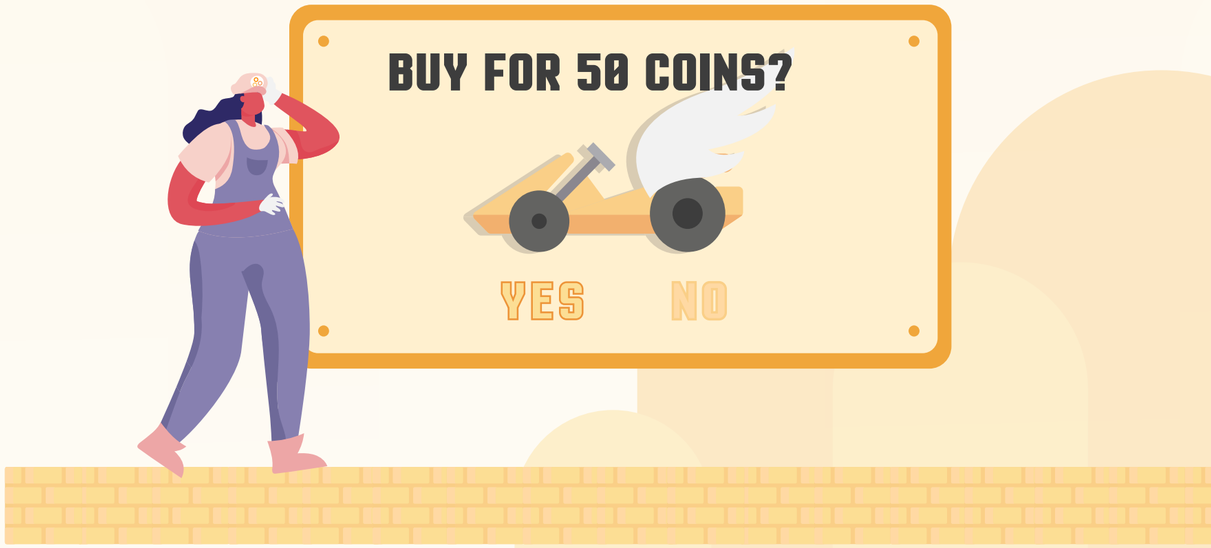
In chapter 1, we covered the top stressors for security, risk, and compliance professionals. Now, we'll discuss where those companies are allocating their budgets to alleviate stress when burnout is at an all time high for compliance professionals.

As discussed in chapter 1, technology is the primary relief for overburdened compliance professionals, with **58% of respondents saying they use GRC software to automate work** around evidence collection, issue tracking, remediation, control monitoring and/or reporting of risks and compliance activities. Hiring outside expertise is another relatively common solution. 35% of respondents hired a managed security service firm/consultancy to take on the work.

Surprisingly, all of these measures aren't enough for some organizations: nearly one-third of respondents **(32%) said they had to postpone the pursuit of new compliance frameworks/certifications** due to insufficient resources.

The second largest stressor was third-party risk, which we'll go into greater detail in chapter 4. This is unsurprising since in 2022, 51% of respondents said their third-party risk management program was expanding. The stresses of identifying and managing IT risks rises as a company's cloud landscape broadens.

While assessing the risk of company-built tools has been a longstanding priority for many organizations, companies haven't historically applied the same level of scrutiny to their third-parties. **But the pattern has clearly shifted** — companies of all sizes are beginning to seek out more information on their vendors' security programs, including understanding key vendors' risk management processes and controls to ensure that they're only using software and services from trustworthy vendors.



FREQUENCY AND COST OF DATA BREACHES

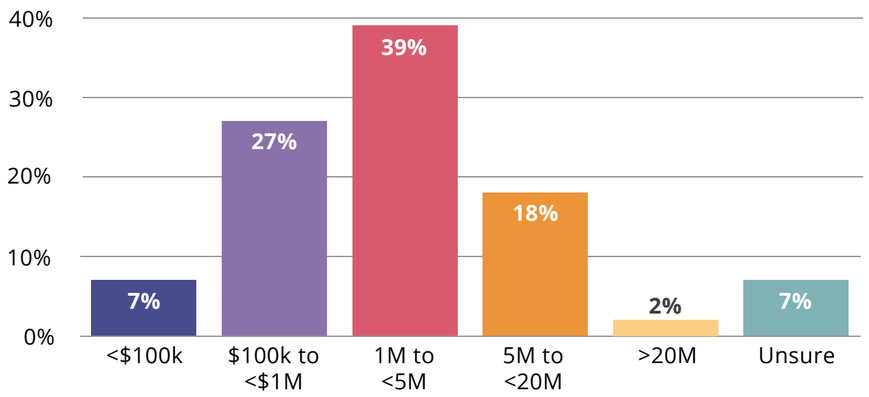
This year, only **42% of those surveyed experienced a breach in the last 24 months**, a significant reduction from the previous year where 63% of respondents reported experiencing a breach. Notably, those who tied their risk and compliance activities together did not experience the same frequency of breaches than those who did not. However, the cost of data breaches remains high.

In the last 24 months, has your organization experienced a security breach (not merely an incident) that led to the disclosure of regulated data such as personally identifiable information (PII), protected health information (PHI), or other sensitive data?

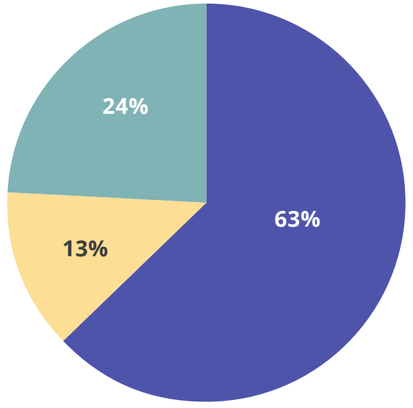
n=1010

In 2022 and 2023, $1M-$5M was the most frequently reported amount of money lost via a data breach. Diving deeper, we can see trends in cost of data breaches by company size. Companies with greater than 2,500 employees were more likely to incur $5M-$20M in money lost via data breaches, whereas smaller companies with less than 2,500 employees were more likely to incur $100k-$1M.

Cost of Data Breaches
n=423

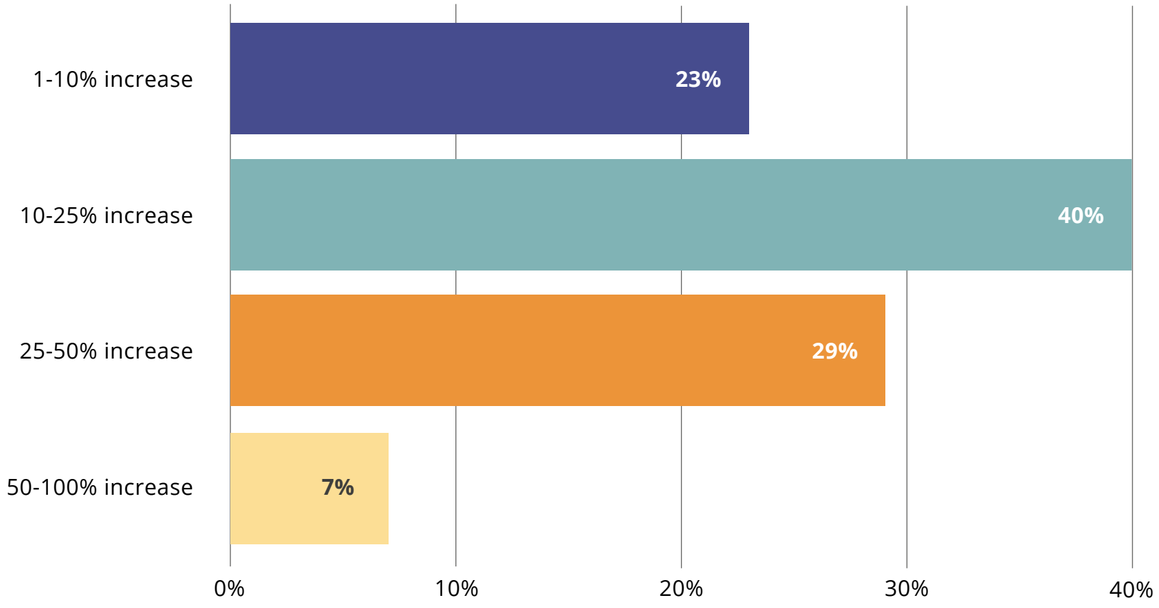


Do you anticipate that your organization will spend more, less, or about the same amount of money on IT risk management in 2023 vs. 2022?
n=1010



For an average organization from our dataset, spending on technology represents a greater proportion of their organization's GRC spend than any other category (compliance audits, staff, and outsourced expertise). The greater emphasis on technology shows that organizations are attempting to gain efficiencies in managing risks and compliance processes.

What is the expected or planned increase in your GRC budget in the next 12 to 24 months?
n=1010



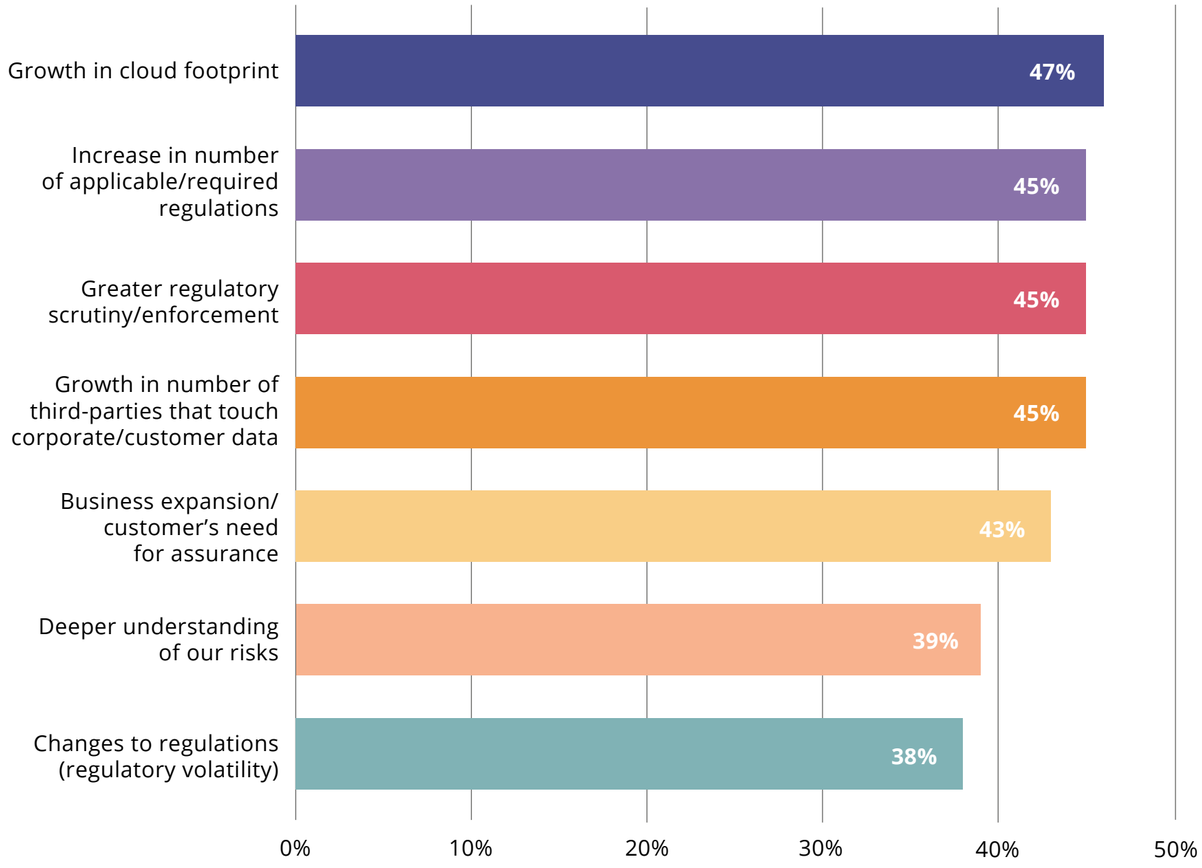
DRIVERS OF SPEND INCREASE

The number of respondents who said they will spend more money on IT risk management **increased 18%** year-over-year from 2022 to 2023, showing an upward trajectory of annual spend on IT risk management.

Multiple factors are driving the increase in GRC spend for organizations. The most commonly selected factor was growth in cloud footprint, which is often caused by growing use of third-party software, mentioned above as the second biggest stressor for respondents. According to the survey, increasing regulatory scrutiny and enforcement, increasing numbers of required regulations, and increasing need from customers for assurance are key drivers closely following cloud footprint growth.

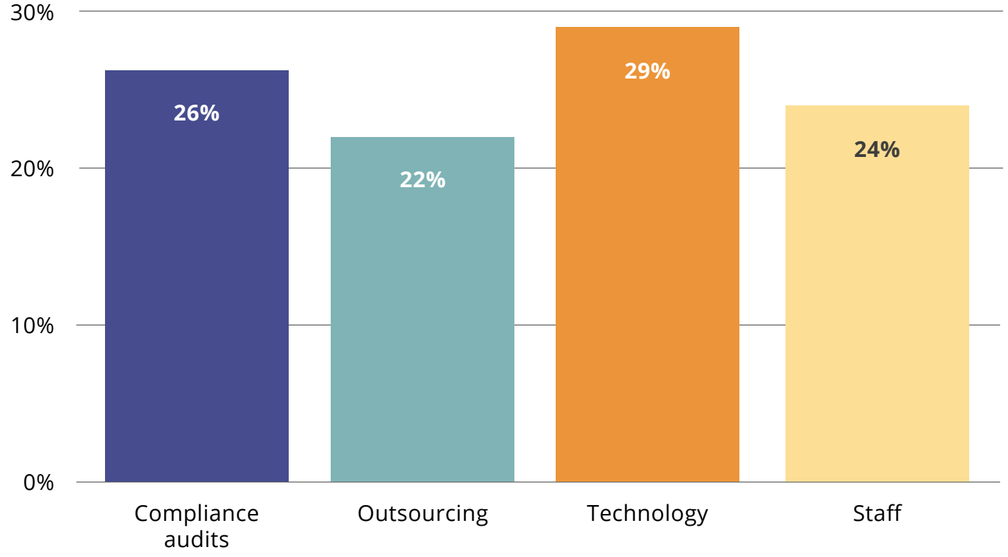
Growth in cloud footprint was also the leading cause of spend increase last year at 47%. Year-over-year, the percentile hasn't changed much, as companies are continuing to find new technologies to add to their tech stacks to scale their businesses and solve for their manual processes.

What are the top factors driving your IT risk/compliance spend increase?
n=1010



CURRENT ALLOCATION OF FUNDS IN COMPLIANCE

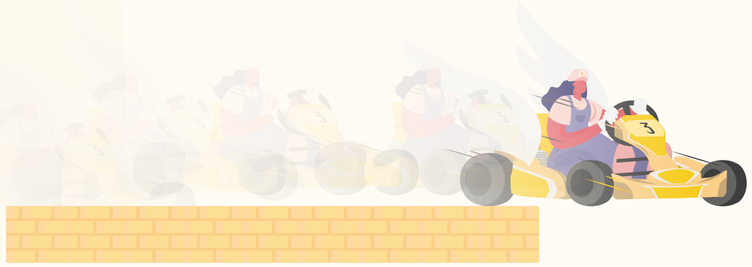
On average, spend on audits and on staff to operate the GRC program are about the same, with the mean of audit spending coming in at 25% of total GRC program budget, and staffing spending coming in at 24% of budget. But technology spend is even greater — coming in at an average of 29% of budget. Outsourcing, on the other hand, only accounts for 22% of total GRC spend.



Like last year's survey, technology (governance, risk, and compliance tools, 28%) is ranked first, but this year compliance audits is ranked second. Last year, staff (management and training programs, 26%) was ranked second. In the last year, priorities have shifted slightly with compliance audits just barely overtaking staffing, a key difference.

Until this year, reported spend on staff has increased significantly year-over-year. Companies should be prepared to invest budget into both growing their compliance program capabilities and investing in management and training programs, so their staff is prepared to handle new and emerging threats.

Where necessary, organizations are using outsourced experts to fill in the gaps. **The top three services companies outsourced were IT security and asset management (57%), security testing (vulnerability scans/pen testing) (40%), and risk assessments (30%)**. But is using outsourcing as a staff augmentation strategy enough? Despite organizations' plans to increase their capacity to respond to risks and compliance requirements, these activities are there to help organizations stay afloat but aren't sufficient. **Nearly one-third of respondents (32%) said they had to postpone the pursuit of new compliance frameworks/ certifications due to insufficient resources for compliance**.

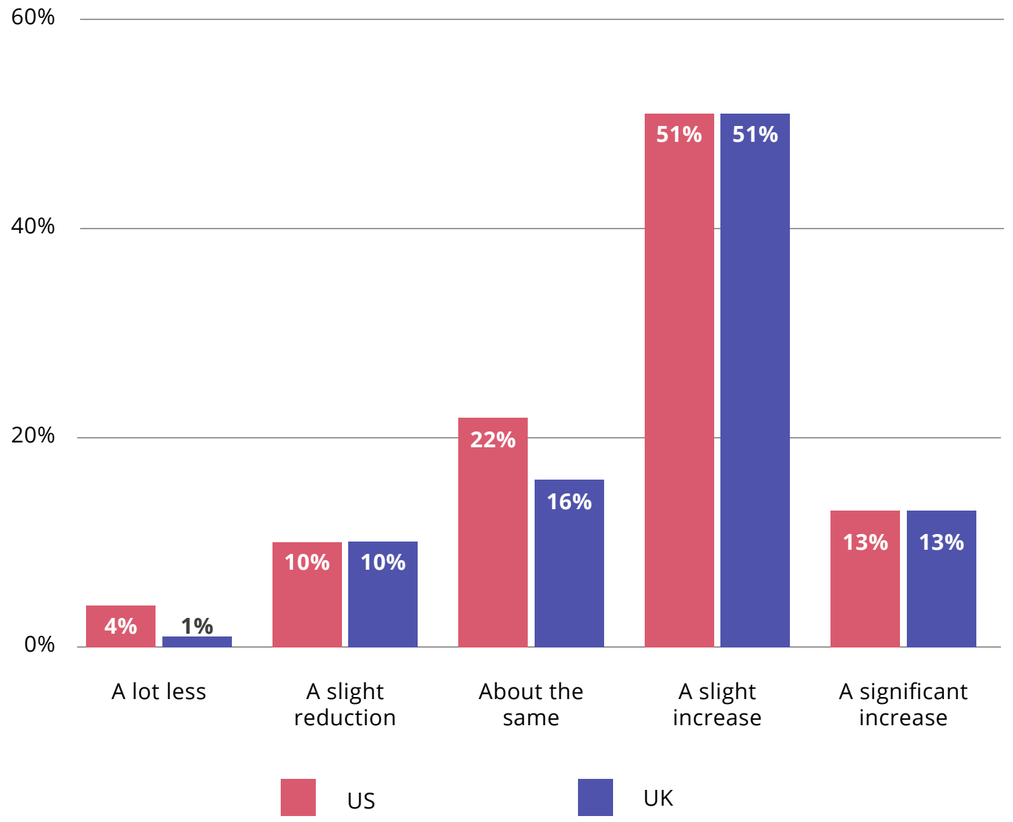


SEGMENT DIFFERENCES

When breaking down US versus UK anticipated 2023 spending, we did not see major differences, meaning the US and UK are relatively aligned on where they plan on prioritizing risk and compliance issues and allocating budget.

The one key difference is that **4% of US respondents said they *would spend a lot less money* on IT risk management in 2023 compared to 2022,** whereas **only 1% of UK organizations said the same thing. 10% of both categories of respondents** said they would spend a slight reduction in money. 22% of US respondents anticipate spending about the same amount of money, while 16% of UK respondents answered as such. 51% of both US and UK respondents anticipate a slight increase in spending. Directionally, we see the trend of an increase in spend in both regions. The UK has recently strengthened their regulation and cybersecurity requirements, which is a notable driver for the slight increase in spend in the region. Finally, **13% of US organizations expect to spend significantly more, whereas 12% of UK respondents expect to spend significantly more.**

Do you anticipate that your organization will spend more, less, or about the same amount of money on IT risk management in 2023 vs. 2022?
n=1010



CHAPTER 3

NEW PLAYERS HAVE ENTERED THE GAME: HOW THE C-SUITE AND BOARD ARE GETTING INVOLVED

LEGAL TEAMS, BOARD MEMBERS, AND SECURITY/IT PROFESSIONALS ARE INCREASING COMMUNICATION WITH EACH OTHER

85% **of respondents say their company has a board member with cybersecurity expertise**

In today's environment, regulatory enforcement and scrutiny around companies' security programs and other types of compliance programs (e.g. anti-money laundering; knowing your customers) has intensified. Directionally, we see a trend of companies tightening governance over matters of cyber risk and focusing on more transparency and communication around compliance and risk throughout their organizations. CISOs are visibly held accountable in headline-making legal matters, and they are worried. Several companies made headlines in 2022 for security breaches, failures, and regulatory violations, including Joe Sullivan/Uber, Aerojet Rocketdyne, Drizly, and FTX.

In response, the way cybersecurity experts are communicating with the C-Suite is changing. We asked respondents about how they communicate with the board, their stakeholders, their Legal teams, and more to understand how the market is shifting to adapt to increased regulatory scrutiny.

RESPONSE TO THE JOE SULLIVAN VERDICT

33% **of respondents said that their companies have made changes to how legal teams work with CISOs in the wake of the Joe Sullivan/Uber case verdict**

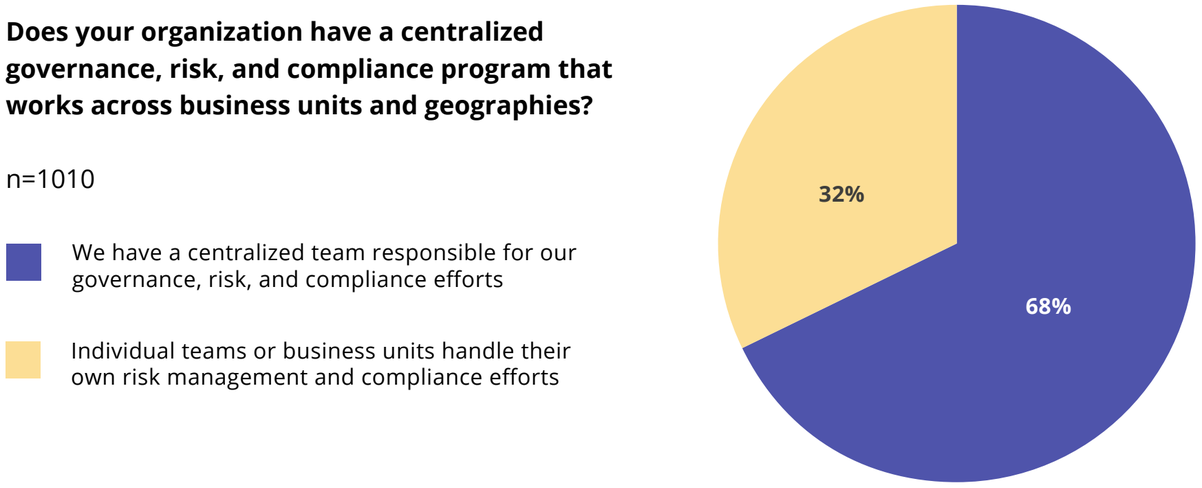
In October 2022, Joe Sullivan, the former Uber security chief, was found guilty of one count of obstructing the FTC's investigation of a breach of customer and driver records and failing to report this breach to government regulators. He was also found guilty of one count of misprision, or acting to conceal a felony from authorities. **33% of respondents said that in the wake of the Joe Sullivan/Uber case verdict, their company has made changes to how the legal team works with their CISO to protect the company and its CISO.** Companies are paying attention to these highly-publicized news stories and are anxious about what they can do to avoid becoming one. Breaking down the long-standing silo between IT/Security and Legal teams is top-of-mind for many respondents.

RELATIONSHIPS WITH THE BOARD

Additionally, **85% of respondents say their company has a board member with cybersecurity expertise**. An additional 14% say they plan to make sure that their board has cybersecurity expertise in 2023. This number surprised us as historically CISOs have not had a seat at the table in the boardroom. These changes indicate a larger market shift to more strategic thinking about risk and compliance.
We also asked respondents if they have a centralized governance, risk, and compliance program. **68% of respondents said yes, they have a centralized team, while 32% said that individual teams or business units handle their own risk management and compliance efforts**.

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

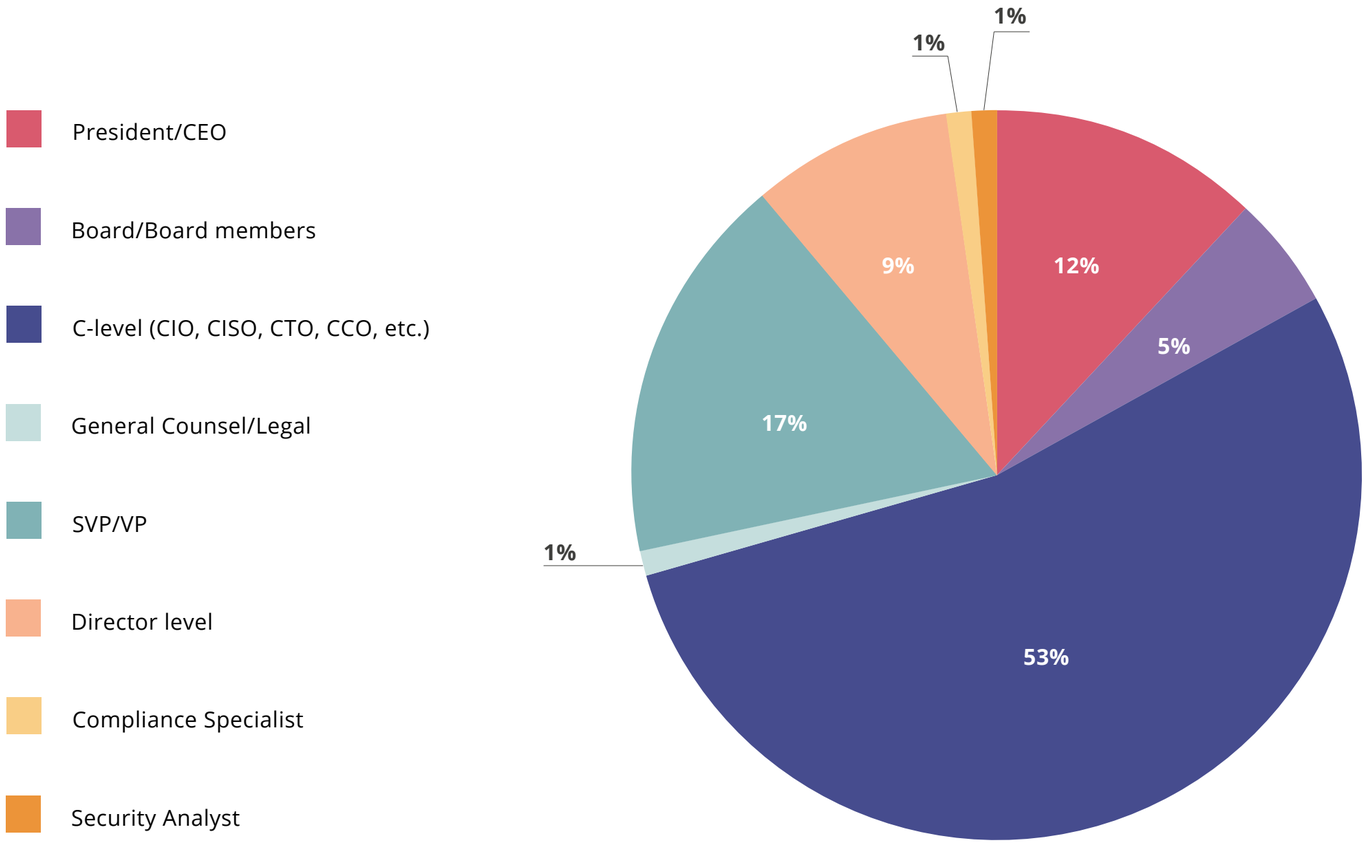
n=1010



WHO IS RESPONSIBLE FOR RISK AND COMPLIANCE?

The highest level of positions or titles overseeing compliance were **most likely to be a non-CEO C-level executive (CIO, CISO, CTO, CCO, etc.), coming in at 53%**. The closest following were SVP/VPs at 17%, then President/CEO at 12%. The least likely level/roles to oversee compliance were Security Analysts (1%) and General Counsel/Legal (1%). Director-level positions, which included compliance specialists, risk architects, audit managers, and accounting and finance managers, came in at 9%.

What is the highest level position or title overseeing compliance?
n=1010

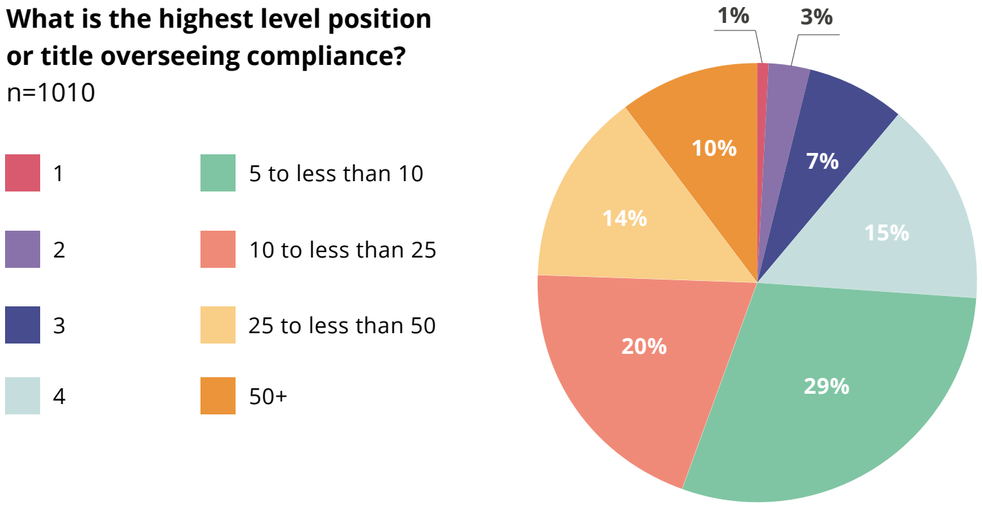


STAFF SIZE

Surveyees reported having an average number of 17 employees dedicated to infosec/cybersecurity compliance. 29% of respondents had 5 to less than 10 employees, followed closely by 10 to less than 25 employees at 20%. 15% said they had 4 dedicated employees, 14.% said they had 25 to less than 50 dedicated employees, and 10% said they had 50+ dedicated employees.

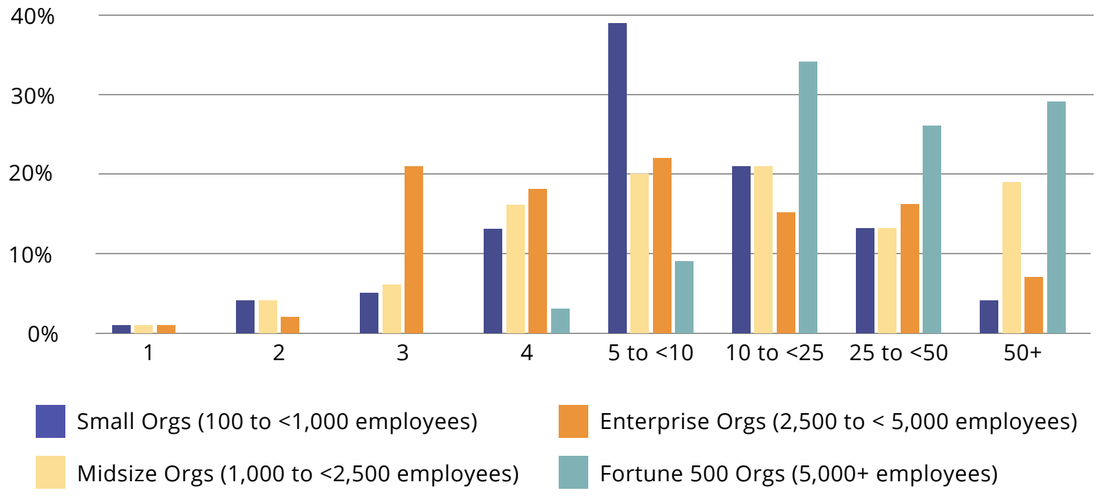
TOTAL AGGREGATE REPORTED

What is the highest level position or title overseeing compliance?
n=1010



STAFF SIZE BY ORGANIZATION SIZE

How many full time staff are dedicated to the infosec/cybersecurity compliance function at your organization?
n=1010



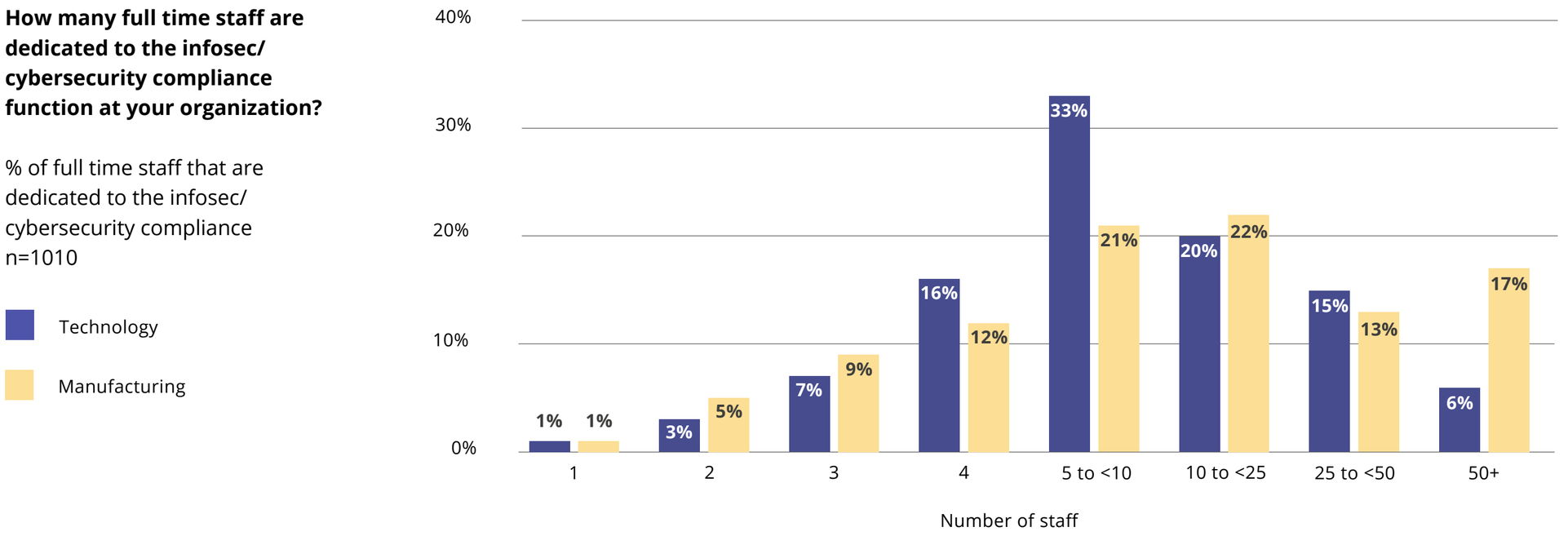
Notably, smaller organizations with 100 to less than 1,000 employees tended to have 5 to less than 10 team members dedicated to infosec and/or cybersecurity. Fortune 500 organizations reported having 10 to less than 25 dedicated employees, followed by 50+ dedicated employees. As organizations grow, the need to scale teams to meet new demands grows with them.

SEGMENT DIFFERENCES

When comparing manufacturing vs. the technology industry, on the aggregate, those in the manufacturing industry were more likely to have over 50 employees dedicated to infosec/cybersecurity compliance. Technology companies tend to have much smaller compliance teams, and the biggest proportion of tech companies have 5 to less than 10 dedicated employees. Companies with annual revenue over $500M were the most likely to have 50+ employees compared to companies with less than $500M revenue. 25% of organizations in business for 15 years had at least 50 employees dedicated to infosec/cybersecurity compliance.

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

% of full time staff that are dedicated to the infosec/ cybersecurity compliance
n=1010



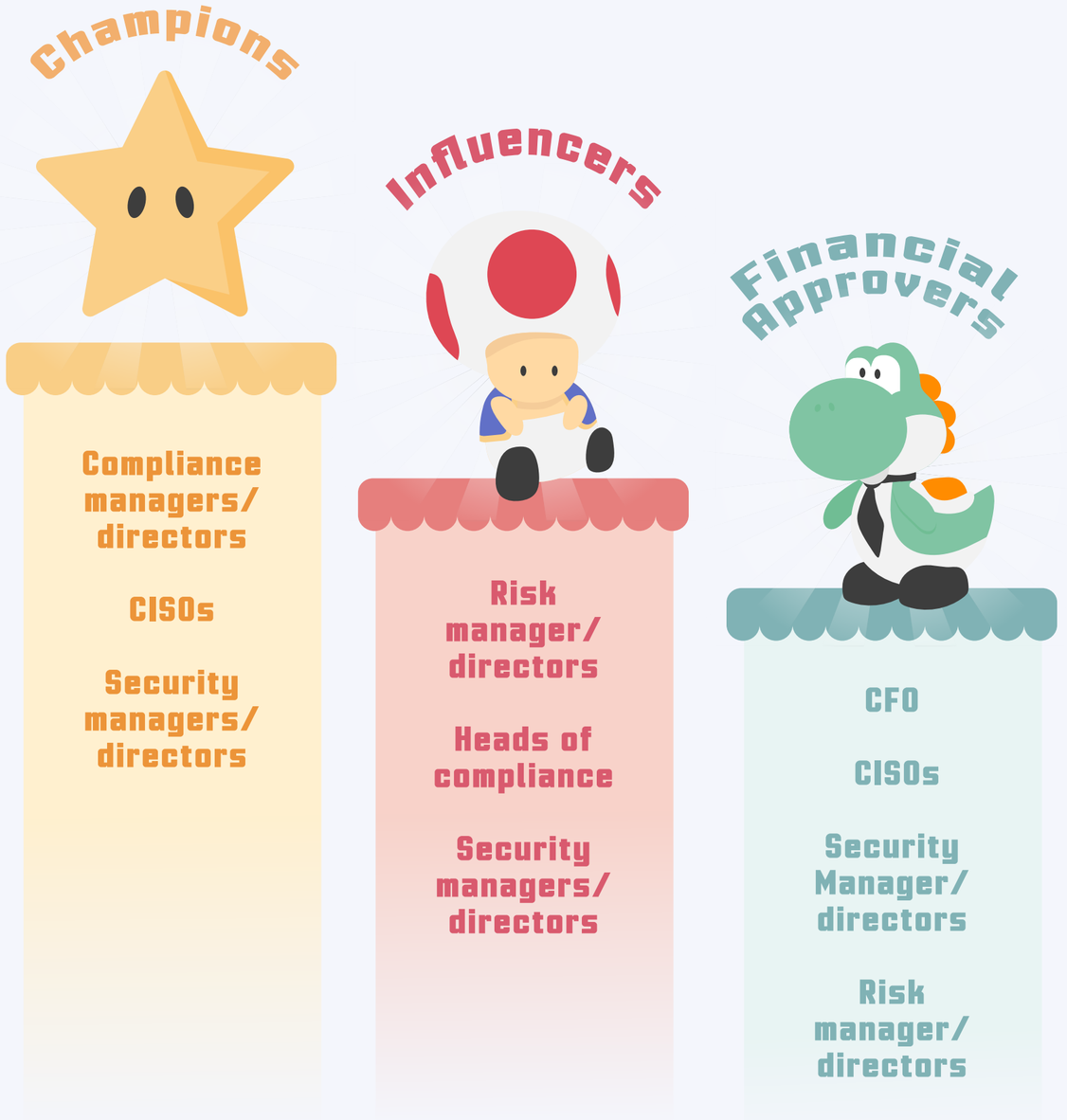
ORGANIZATIONAL STRUCTURE FOR RISK MANAGEMENT AND COMPLIANCE OPERATIONS

46% said that risk management was a distinct and separate function from the compliance function, with their own distinct staff members. 52% said the functions are integrated, with risk responsibilities rolling up into compliance personnel's jobs. 2% said it varies by business function and location.

Over 70% of respondents have taken extensive actions that demonstrate their commitment to risk management, with an additional 14% saying they plan to make sure their board has cybersecurity expertise in 2023. **This aligns with our findings that 57% of all respondents anticipate spending more time on IT risk management and compliance in 2023.**

DECISION MAKERS

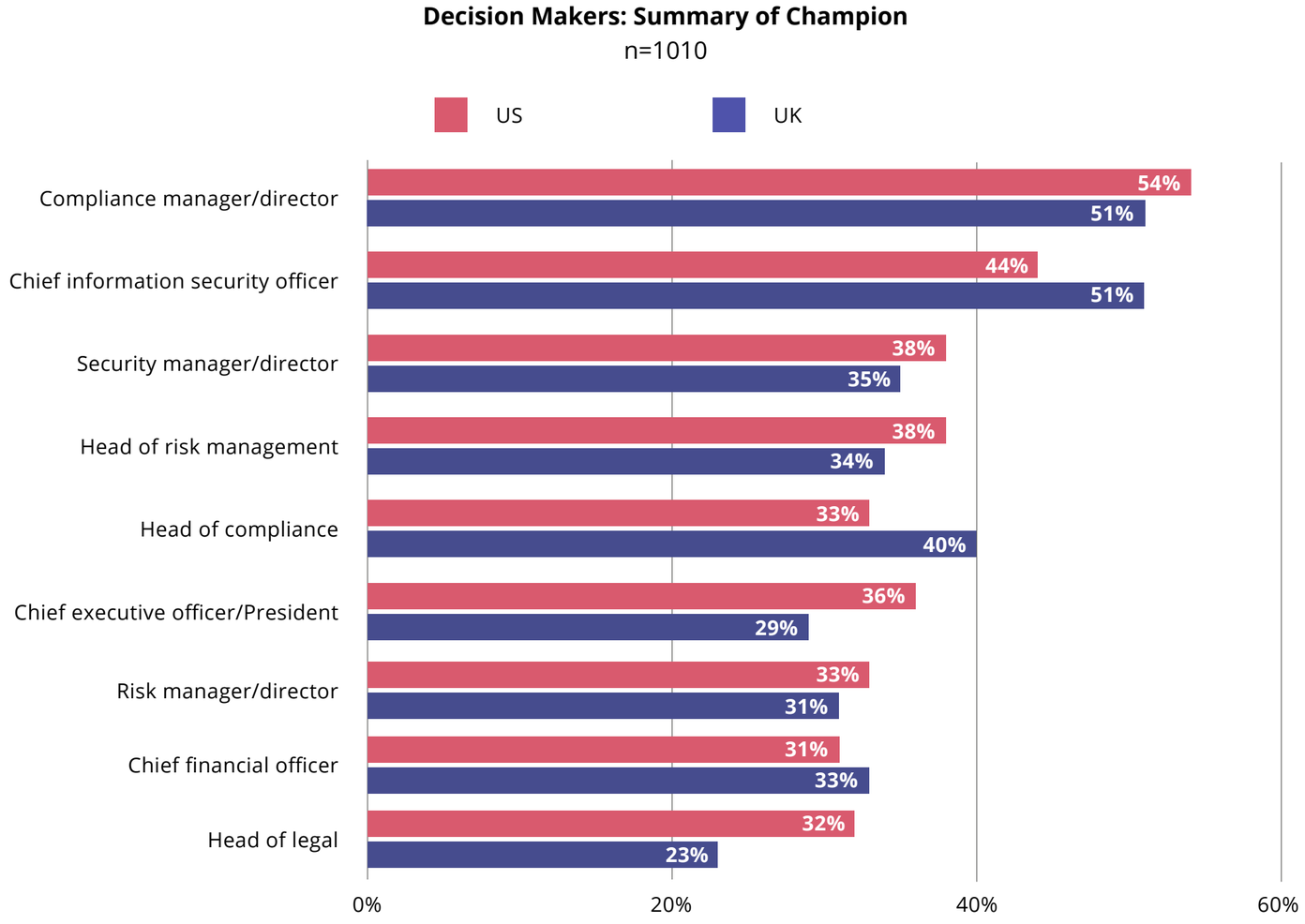
We asked respondents to tell us who are the decision-makers when their organization makes risk or compliance technology purchase decisions. We categorized stakeholders as champions, influencers, and financial approvers. On the aggregate, champions were most likely to be compliance managers/directors, CISOs, or security managers/directors. Influencers were most likely to be risk manager/directors, heads of compliance, and security manager/directors. Financial approvers were most likely to be CFOs, CISOs, security manager/directors, and risk manager/directors.



SEGMENT DIFFERENCES

Between the UK and the US, there were the following differences:

- CEO/presidents were more likely to be a champion in the US, as well as the head of legal
- CISOs were more likely to be champions in the UK
- CEO/presidents were more likely to be influencers in the UK
- CISOs were more likely to be the financial approver in the US



CHAPTER 4

THIRD-PARTY RISK'S DIFFICULTY RATING: VERY HARD

THE THIRD-PARTY RISK LANDSCAPE IS GROWING

As seen in our previous benchmark reports, the pandemic has accelerated the usage of digital third-party platforms, including cloud-based technology, to get work done remotely. The expansion of digital services have forced compliance and risk managers to reckon with increased exposure to risks while concurrently updating their processes to support the increased speed, complexity, and scale of these new platforms.

Globalization and the increasing complexity of supply chains have made it difficult for organizations to understand and manage all of the risks associated with their third-party relationships. Companies often work with a large number of third-party suppliers, vendors, and service providers, making it difficult to monitor and manage risks associated with all of them. Supply chains have become more complex with the integration of multiple stages and partners across various geographic locations, making it challenging for organizations to have visibility and control over their third-party partners. With so many third-party partners, it can be difficult to implement standard processes and procedures for managing risk. This can lead to inconsistent risk management practices, increasing the likelihood of issues slipping through the cracks.

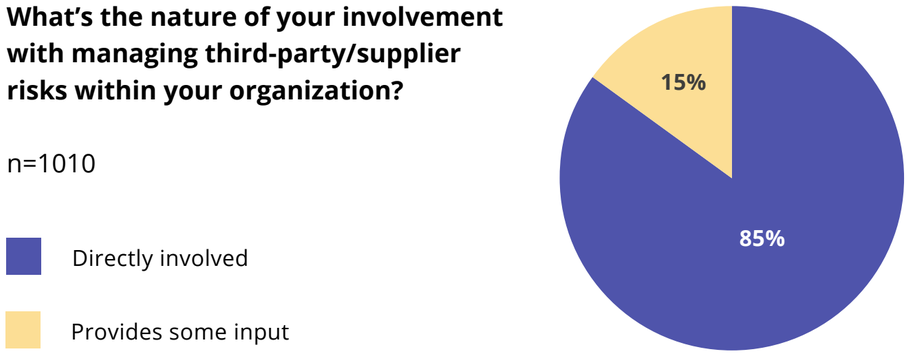
Keeping up with third-party risk due diligence is difficult, and the data from third-party risk profiles — like security questionnaires — takes a long time to parse. All the while, regulations that require companies and public-entities to have sufficient oversight over their third-parties have increased. Organizations are now responding by using vendor risk management tools, however, these tools are not fully addressing their third-party risk needs, which we will discuss in detail in this chapter.

HOW INVOLVED RESPONDENTS WERE WITH HANDLING THIRD-PARTY RISK

We found that the overwhelming majority of respondents were directly involved with addressing third-party risk. 85% of respondents reported being involved with regularly identifying, managing and/or monitoring third-party risks, and 15% provided some input to help colleagues identify, manage, and/or monitor third-party risks. Notably, all surveyees were involved in some capacity with third-party risk management at their organizations. Third-party risk remains top-of-mind for InfoSec professionals across all demographics, from company size, revenue, business tenure, and headquarter location.

What's the nature of your involvement with managing third-party/supplier risks within your organization?

n=1010

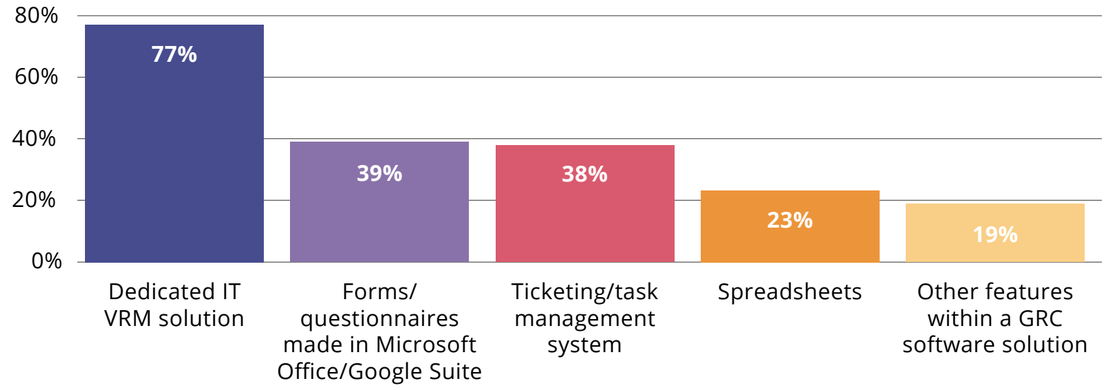


TOOLS USED TO MANAGE THIRD-PARTY RISK

When asked what tools they are using to identify and manage IT risks rising from third parties **77% of respondents reported using dedicated IT vendor risk management (VRM) solutions**. These tools support enterprises that have to assess, monitor and manage their exposure to risks arising from their use of third parties that provide IT products or services or that have access to their information. 39% reported using forms and/or questionnaires made in Microsoft Office or Google Suite, and 38% reported using a ticketing or task management system. 23% reported using spreadsheets, and 19% reported leveraging other features within a GRC software solution.

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

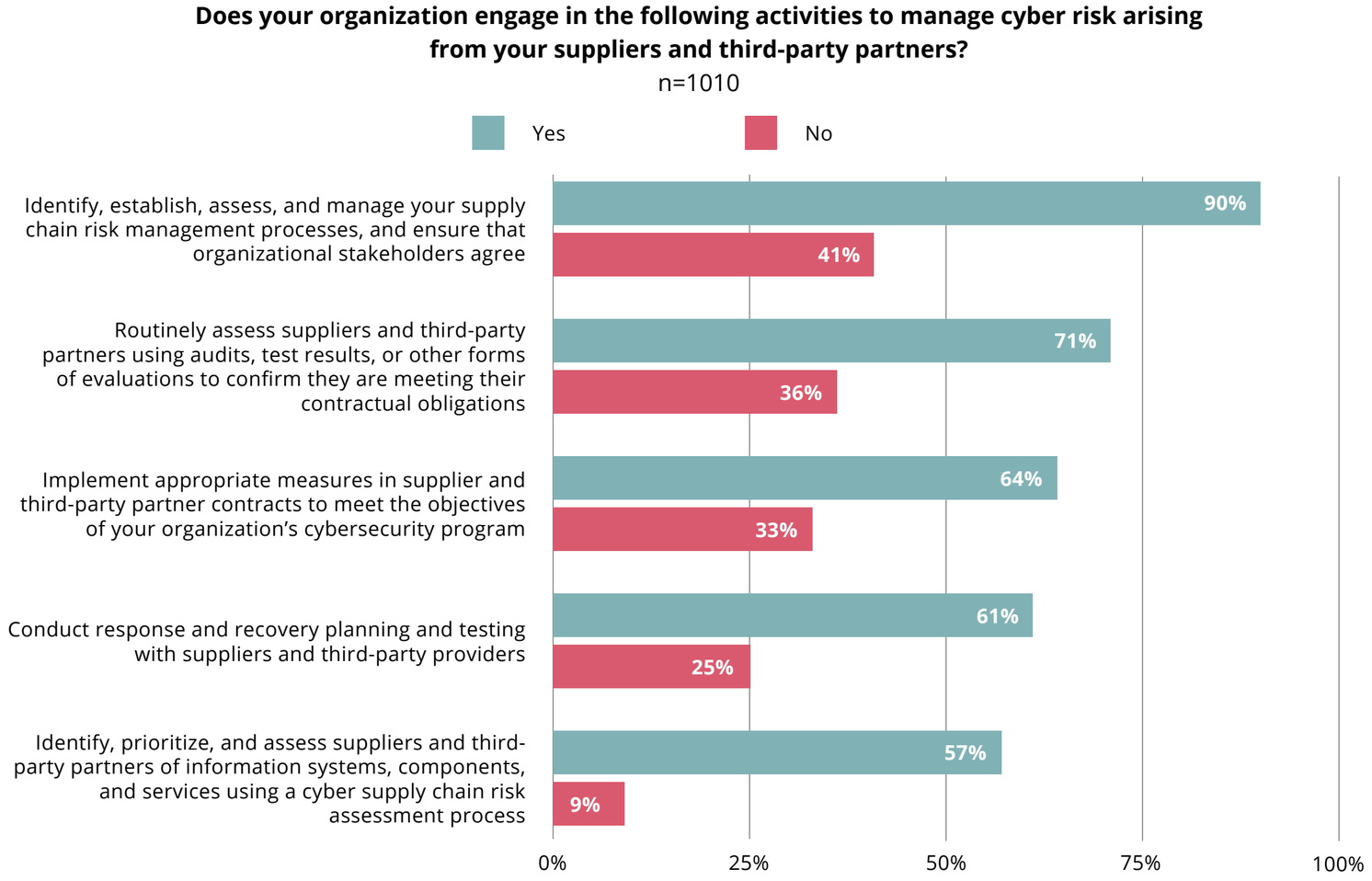
n=1010



HOW RESPONDENTS ARE ADDRESSING THIRD-PARTY RISK

When asked what their organizations do to manage cyber risk arising from suppliers and third-party partners, we received a mix of responses.

As seen in the chart to the right, organizations have clear processes in place for managing third-party risk. For instance, **identifying, establishing, assessing, and managing supply chain risk management processes to ensure that all stakeholders agree is a common practice among respondents, with 90% reporting that they engage in this activity to manage third-party risk**. However, while respondents established that they have comprehensive plans and processes in place to address third-party risk, they



are still struggling with frequent breaches and an inability to address audit findings due to third-party risk (both discussed in more detail later in this chapter). We see a conflict here: the confidence to address third-party risk is high, but respondents have trouble prioritizing which third parties to address. This is often because aggregating third-party risk data is difficult, which disrupts their ability to properly prioritize which third-parties are most critical.

Third-party risk management is an area with many opportunities for improvement. Not all organizations have implemented critical activities to manage cyber risk arising from their third-parties. While assessing the risk of company-built tools has been a longstanding priority for many organizations, third-party risk management hasn't historically received as much attention from risk and compliance professionals. But the pattern has clearly shifted — companies of all sizes are beginning to seek out more information on their vendors' security programs, including understanding key vendors' risk management processes and controls to ensure that they're only using software and services from trustworthy vendors. 85% of all respondents are involved regularly in identifying, managing and/or monitoring third-party risks.

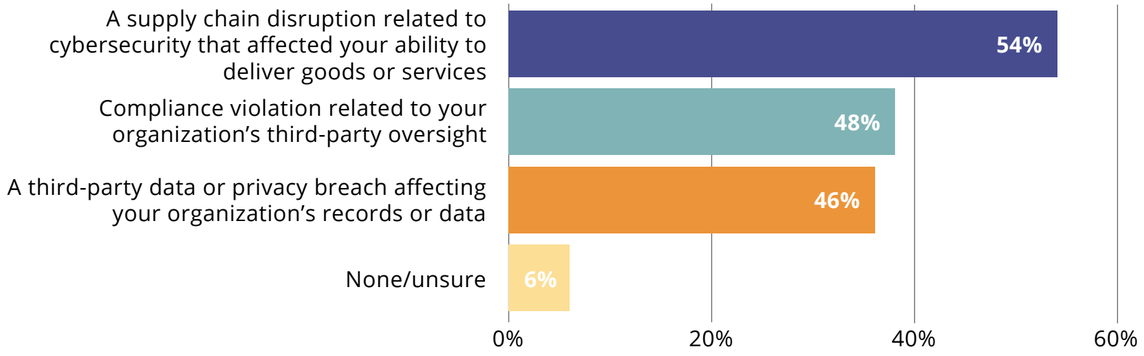
Additionally, more InfoSec professionals are spending money on and leveraging cloud technology for their risk and compliance efforts. In 2023, respondents are planning to allocate the highest percentage (29%) of their budgets to spend on new technology, and the biggest driver of spend increase is growth in the cloud footprint (46%), in other words, use of SaaS tools.

THIRD-PARTY EVENTS EXPERIENCED

With all these processes in place, one would expect a minimal amount of third-party events experienced in 2022. However, this was not the case. We asked respondents if their organization had been impacted by any of the following events in the last year: supply chain disruption, compliance violations, and/or a third-party data or privacy breach. **54% reported experiencing a supply chain disruption related to cybersecurity that affected their ability to deliver goods or services**. 48% reported experiencing a compliance violation related to their organization's third-party oversight. 38% reported experiencing a third-party data or privacy breach affecting their organization's records or data, and 6% reported that they either did not experience a third-party disruption or were unsure if they did.

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

n=1010



AUDIT FINDINGS: THE PRIMARY THIRD-PARTY RISK CHALLENGE

As discussed above, respondents have many processes in place to address third-party risk. However, these processes are not optimal; they do not deliver the results one would expect, especially when looking at the data around their ability to address third-party risk audit findings.

74% of respondents have experienced (or are expecting) an audit finding that they cannot promptly resolve related to third-party risk management. This number is staggering – managing third-party risk is clearly still incredibly difficult for companies, and InfoSec professionals are worried about both bandwidth and budget to address these issues.

In our 2022 survey, 51% of respondents said their third-party risk management program was expanding. Clearly, the platforms they adopted to mitigate third-party risk management are not fully addressing their needs. Additionally, companies may have trouble fully utilizing their tools because they don't have the right processes in place or the right risk data that would help them determine which of their vendors to prioritize. Vendor prioritization will continue to be challenging because threat actors are aware of how easy it is to target a company via a third-party vendor and will continue to become more creative with their methods. Until organizations can comprehensively consolidate, organize, and view their third-party risk data to fully address this challenge, this problem will persist.

CHAPTER 5

POWER UP FOR THE ENDGAME WITH UNIFIED RISK MANAGEMENT AND COMPLIANCE OPERATIONS

COMPLIANCE TECHNOLOGY IS NOT JUST A SIDEQUEST ANYMORE

70% **of respondents said that their compliance and risk team will grow in size over the next two years**

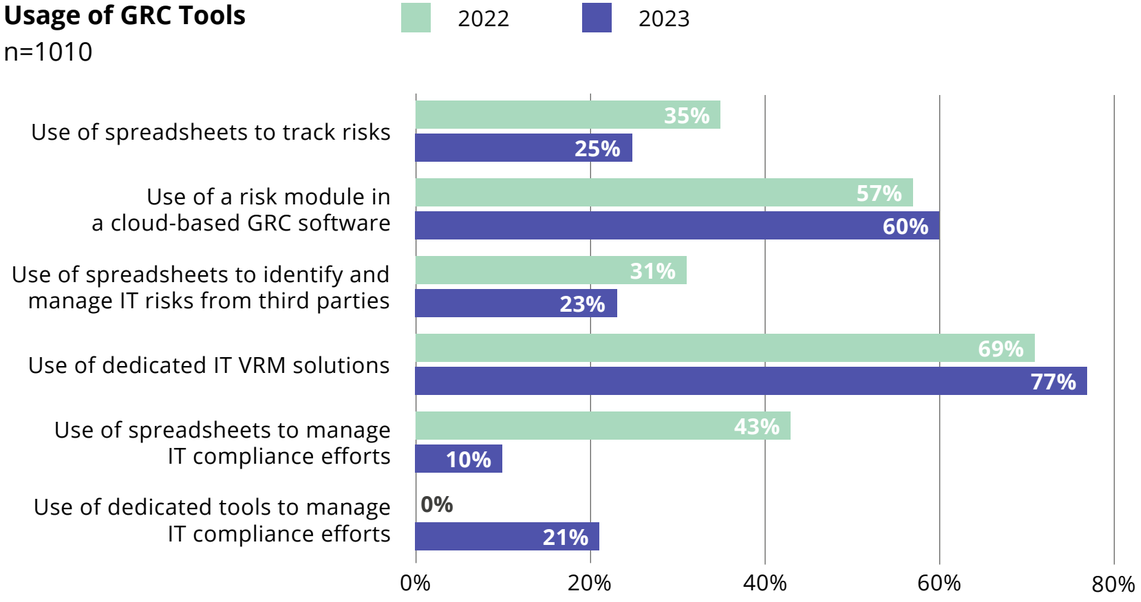
Compliance tools usage has grown in the last year, with 65% in 2023 using integrated risk management solutions compared to 57% in 2022. The usage of tools is no longer a nice-to-have but a need-to-have as the landscape has changed drastically with the advent of newer, more powerful technology tools — both for companies and threat actors alike.

Respondents are aware that tools are a need-to-have, yet 38% said most of their time is spent on manual and/or administrative tasks. Simply having tools doesn't equate to realized efficiency; the right tools — which are integrated and intuitive — unify compliance and risk to actually solve the data silo problem. One of the reasons security, risk, and compliance managers are still spending time on manual tasks is the fact that they are using clunky and unintuitive GRC tools that take away time from truly operationalizing compliance and risk.

USAGE OF GRC TOOLS

In 2023, 25% of all respondents use spreadsheets to track risks versus 35% in 2022. Use of the risk module in a cloud-based GRC software has slightly increased from 57% last year to 60% this year. In 2023, **23% of all respondents use spreadsheets to identify and manage IT risks from third parties versus 31% in 2022. Use of dedicated IT VRM solutions increased from 69% last year to 77% this year**. Only 10% of respondents use spreadsheets to manage their IT compliance efforts in 2023, versus 43% in 2022.

Usage of GRC Tools
n=1010



This adoption of new tools aligns with the Technology sector's rapid increase in digital platform usage and Cloud technologies in response to the pandemic, and, as a result, this new mix of GRC tools has helped operationalize compliance efforts and adapt to new compliance requirements. However, the usage of Cloud technology has its downsides: third-party risk vulnerabilities (discussed in chapter 4), siloed views of risk and compliance (discussed in chapter 1), and fractured reporting across multiple solutions.

With acute skills shortage in the cybersecurity and compliance domains, technology should be a part of the solution to keep up with risks and a growing compliance burden. However, the right platforms will provide holistic views of a company's compliance, security, and risk posture while having the ability to link risks to controls. Technology helps to increase visibility by:

- Enabling professionals to see which risks are critical to prioritize
- Increasing accountability by providing transparency and mechanisms to track who is responsible for tasks
- Enabling professionals to quickly identify common controls and map them to risks and regulatory requirements
- Increasing efficiency in key risk management tasks, such as control testing
- Reducing time spent on administrative tasks, such as communicating audit requests to stakeholders and gathering evidence for audits

SEGMENT DIFFERENCES BY COMPANY SIZE

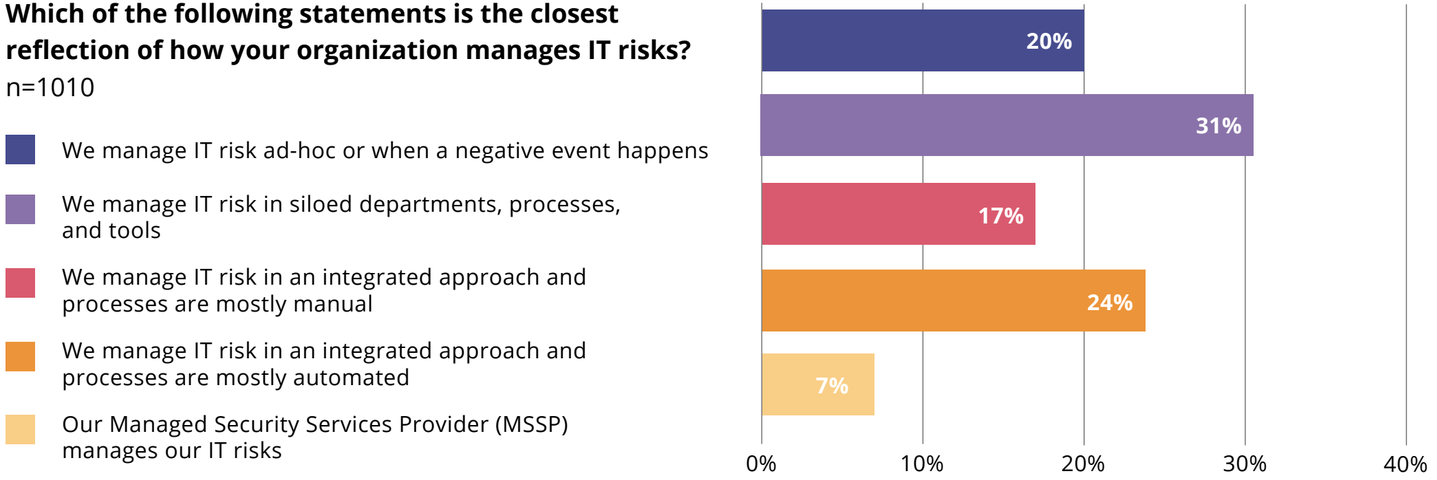
Companies with 2,500 to less than 5,000 employees were more likely to have plans to evaluate software to monitor their security controls and reports on their compliance posture in 2023 (76%). Likewise, companies with 5,000+ employees also came in at 71%, the second highest. Organizations with 100 to less than 1,000 employees and 1,000 to less than 2,500 employees came in respectively at 57% and 60%. This demonstrates that at least half of organizations of all sizes are seeking to evaluate software as an option to augment their security and compliance efforts in 2023.

UNIFYING RISK AND COMPLIANCE IS STILL A NEED

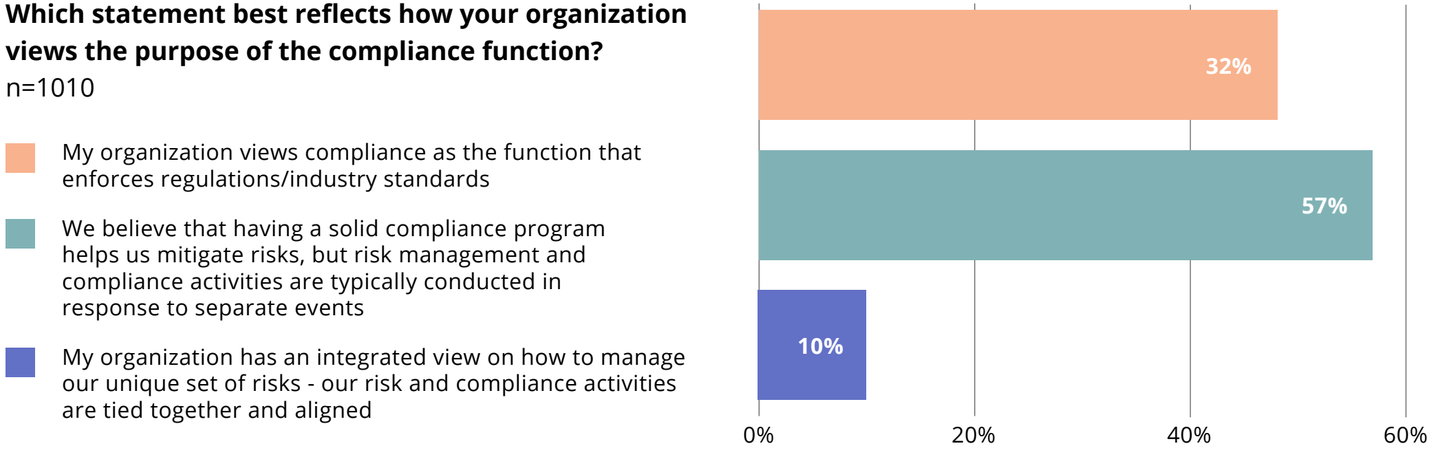
SILOS LED TO MORE BREACHES

Although risk and compliance continues to operate in silos, respondents recognize the benefits of changing this reality with **57% saying that having a solid compliance program helps them mitigate risks**, even though risk management and compliance activities are typically **conducted in response to separate events. Only 10% of respondents have an integrated view on how to manage their unique set of risks and have aligned their risk and compliance activities**, and organizations that managed risk in an ad-hoc manner or only when a negative event happened were more likely to experience a breach.

Which of the following statements is the closest reflection of how your organization manages IT risks?
n=1010



Which statement best reflects how your organization views the purpose of the compliance function?
n=1010



Managing risk ad-hoc or in siloed departments had negative impacts on those surveyed: **1 in 2 companies managing risk ad-hoc or in siloed departments experienced a breach in 2022**. 61% of companies that characterized their risk management approach as "ad-hoc" experienced a breach, and 46% of those managing risk in siloed departments experienced a breach.

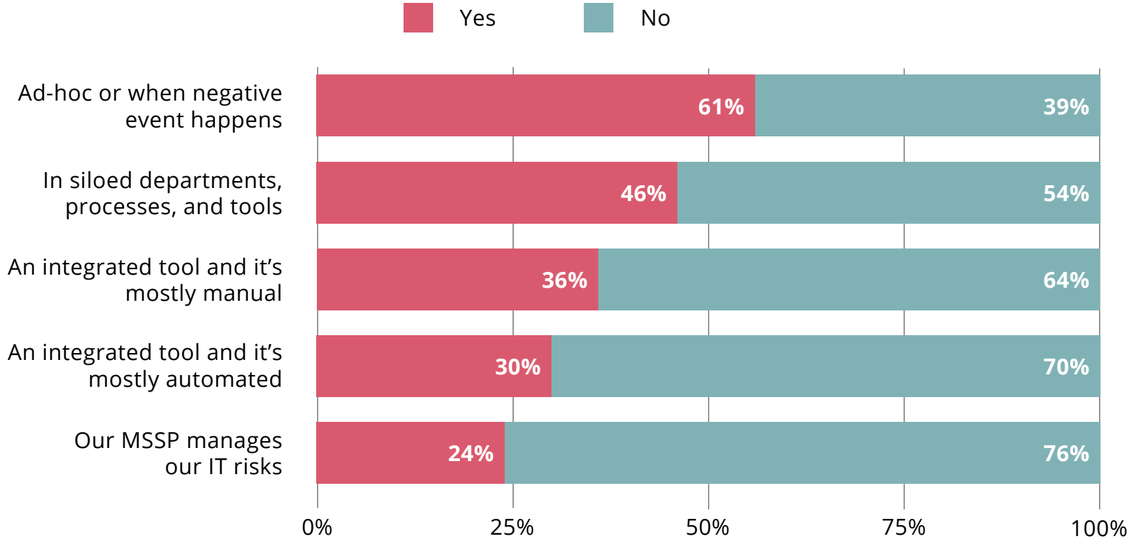
In contrast, only 36% of companies with an integrated approach and manual tools and 30% of companies with an integrated approach and automated tools experienced breaches. Companies that unified their risk and compliance operations did not suffer the same frequency of breaches, indicating that operating in silos opens companies up to vulnerabilities.

KRIS AND KPIS WERE HARDER TO ESTABLISH

Notably, **29% of respondents do not have established KRIs linked to their KPIs for any identified high or critical risks**, indicating that risk and compliance could still be operating in silos, or respondents haven't figured out how to measure meaningful changes to risk level. Unifying risk and compliance efforts can help solve each of these pervasive challenges. **68% of respondents using integrated tools with both manual and automated processes did not experience a breach in 2022, and 72% of respondents who have tied their risk and compliance activities together did not experience a breach.**

In the last 24 months, has your organization experienced a security breach (not merely an incident) that led to the disclosure of regulated data such as personally identifiable information (PII), protected health information (PHI), or other sensitive data?

n=1010

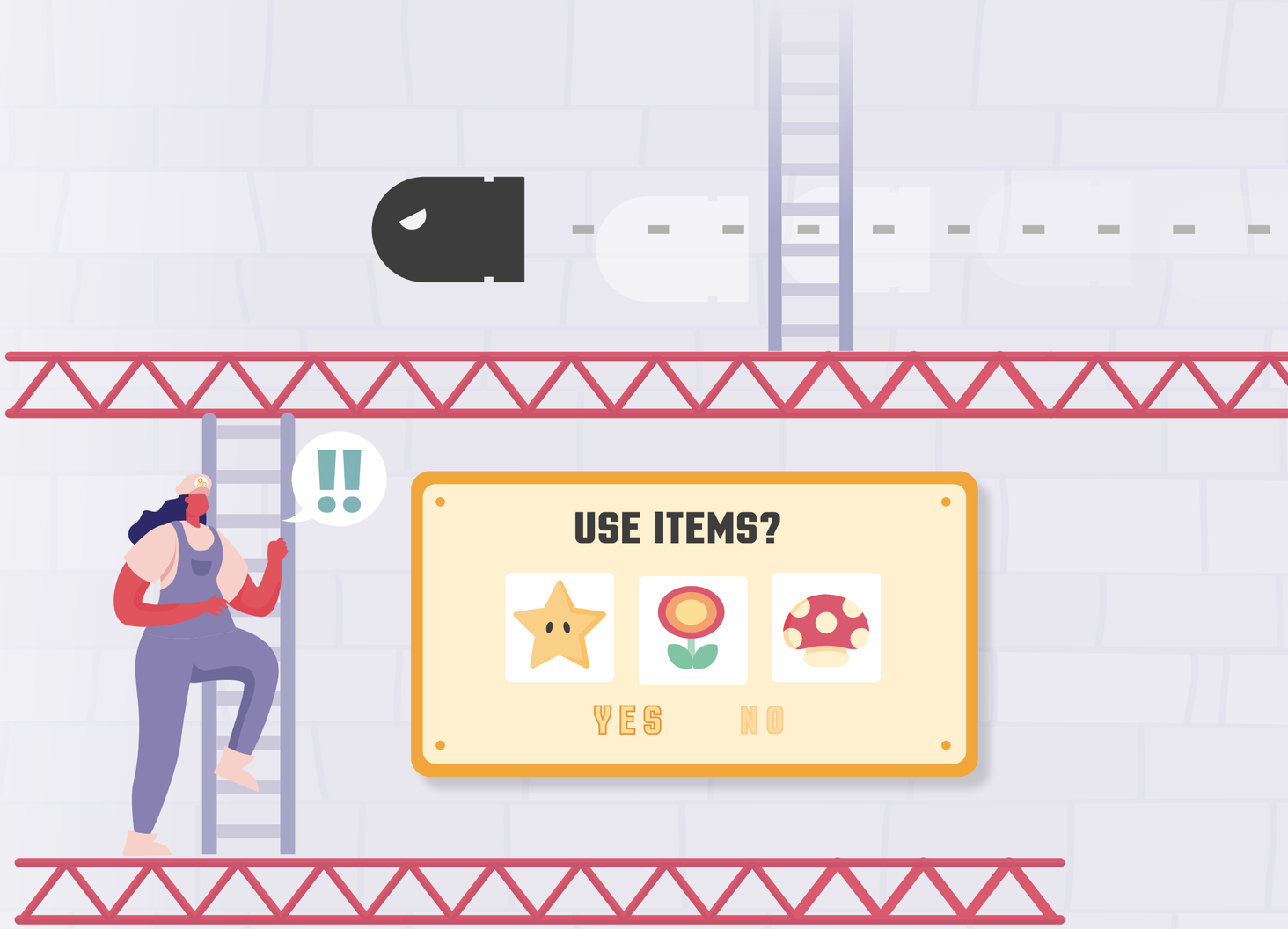


31% of respondents said they manage IT risk in siloed departments, processes, and tools, followed by **24% that manage IT risk in an integrated approach** where their processes are mostly automated. These numbers are striking; while respondents clearly see the value in unifying risk management and compliance operations, the overwhelming majority of those surveyed aren't following this best practice. Even the most powerful IT risk management tools can under-deliver when key processes haven't been established.

AN INCREASE IN TIME-CONSUMING MANUAL PROCESSES

Managing risk and compliance in silos was time-consuming for respondents. We asked "What portion of your risk and compliance management team's time is spent on administrative tasks?" **The average respondent said 38% of time is spent on administrative tasks.** This is about the same as last year, where the mean was 39%. **85% of all respondents said their risk and compliance management team spends at least 1/3 or more of their time at work on repetitive tasks.** Automating administrative tasks could reduce the burden of manual processes for security, compliance, and risk managers.

So, how could companies go about addressing risk management and compliance operations more holistically? Namely, they could reimagine the process by focusing more on macro strategies by identifying the overlaps between their risk management and compliance activities to streamline their processes.



THE BENEFITS OF UNIFYING RISK AND COMPLIANCE TECHNOLOGY

Taking an integrated approach to risk and compliance operations allows organizations to focus on their unique set of risks while avoiding duplicate activities across their risk and compliance management processes. Organizations that take this approach typically start the risk management process with conducting a risk assessment. From there, they create security policies and implement internal controls tailored to the results of their risk assessment. This allows for greater alignment throughout the organization by allowing for input from all stakeholders, not just a select few. And, it helps create a compliance program that integrates directly with risk operations.

In this study, we wanted to see whether companies that take an integrated approach to GRC achieved significantly better outcomes from a security standpoint and business performance perspective compared to organizations that still view compliance as a separate, policing function. We found strong evidence that organizations taking an integrated approach have better security posture than their counterparts who view compliance solely as the function that enforces rules and regulations:

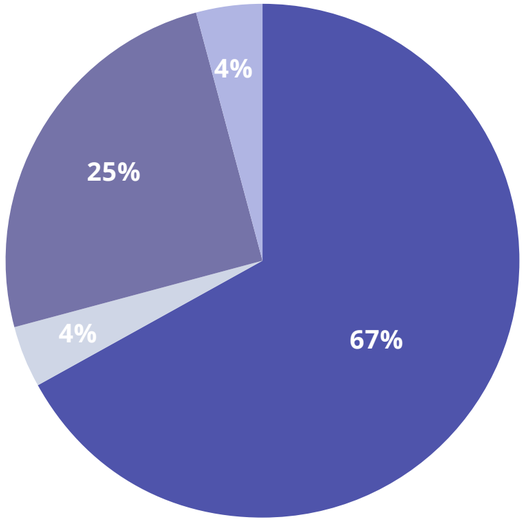
- On average, organizations that take an integrated approach to risk management experienced security breaches less often than those who view their compliance function as the enforcer of rules.
- As a group, organizations that take an integrated approach spend less time on repetitive and administrative tasks compared to those who believe the compliance function's purpose is to enforce the rules.

SURVEY METHODOLOGY

The 2023 IT Compliance and Risk Benchmark Survey gathered 1,010 responses during December 2022 and January 2023. All organizations come from the following industries:

INDUSTRIES SURVEYED

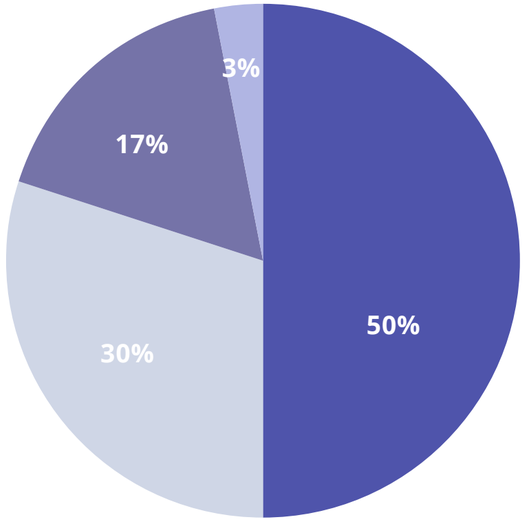
n= 1010



- Technology
- Automotive
- Tech-Forward Manufacturers
- HealthTech

ORGANIZATION SIZE AND MAKEUP

n= 1010

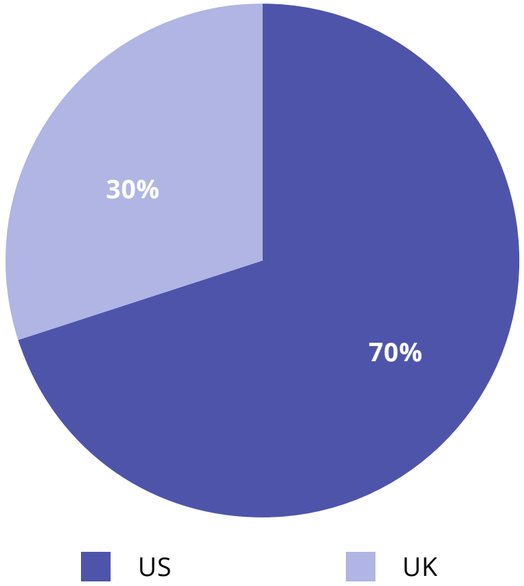


- Small Organizations (100-1,000 employees)
- Midsize Organizations (1,000-2500 employees)
- Small Enterprise Organizations (2500-5000 employees)
- Large Enterprise Organizations (5,000+ employees)

The average organizational size of respondents was 1,664 employees.

LOCATION

n= 1010

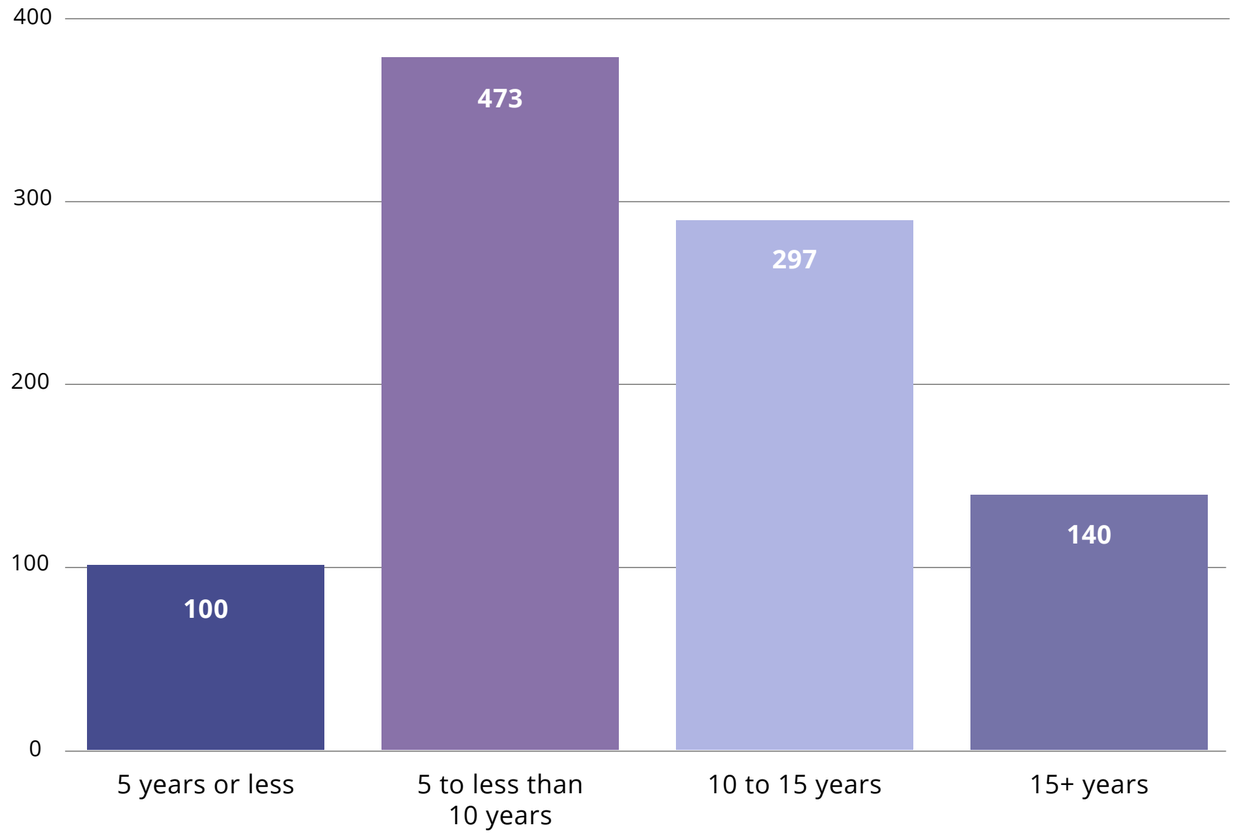


Respondents came from organizations that have U.S.-based headquarters and U.K.-based headquarters. 70% of respondents come from companies with headquarters in the US. 30% of respondents come from companies with headquarters in the U.K. Organizations with single and multiple locations were included.

BUSINESS TENURE

n= 1010

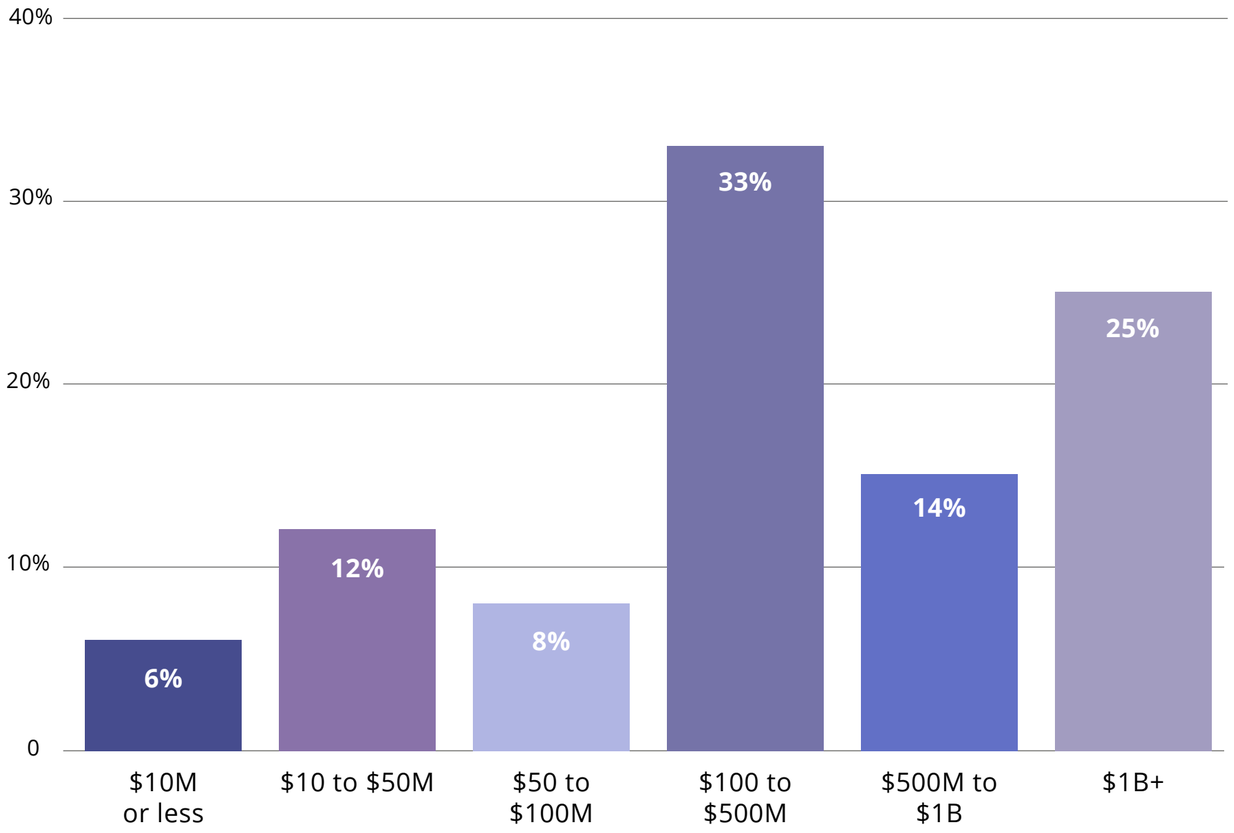
We surveyed a variety of companies with the following business tenures:



REVENUE

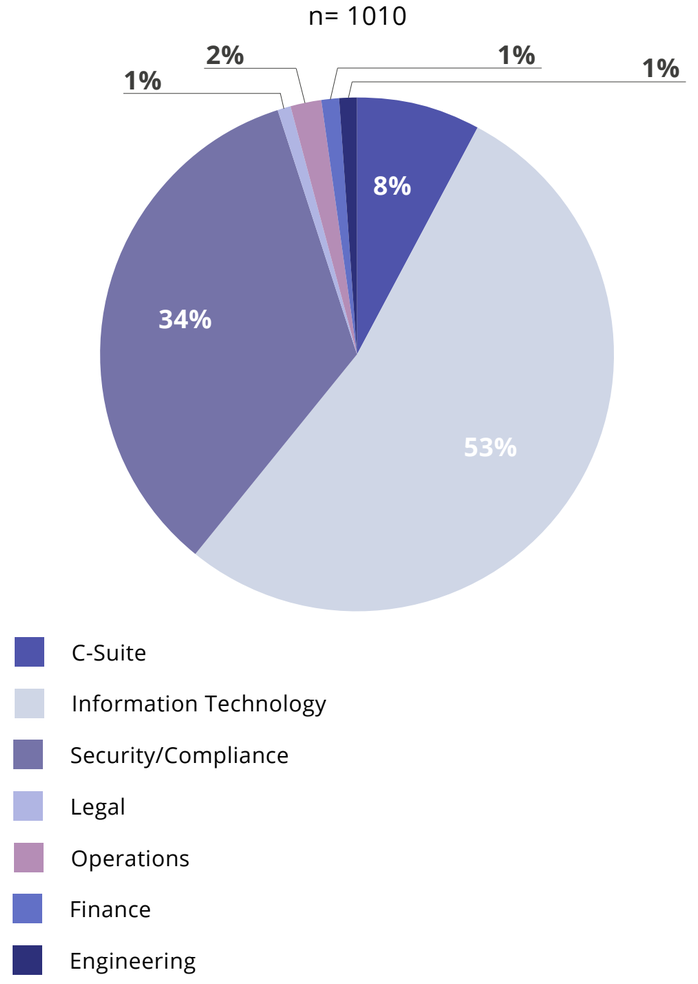
n= 1010

Respondents work for companies that generated the following revenue in 2022:



DEPARTMENT

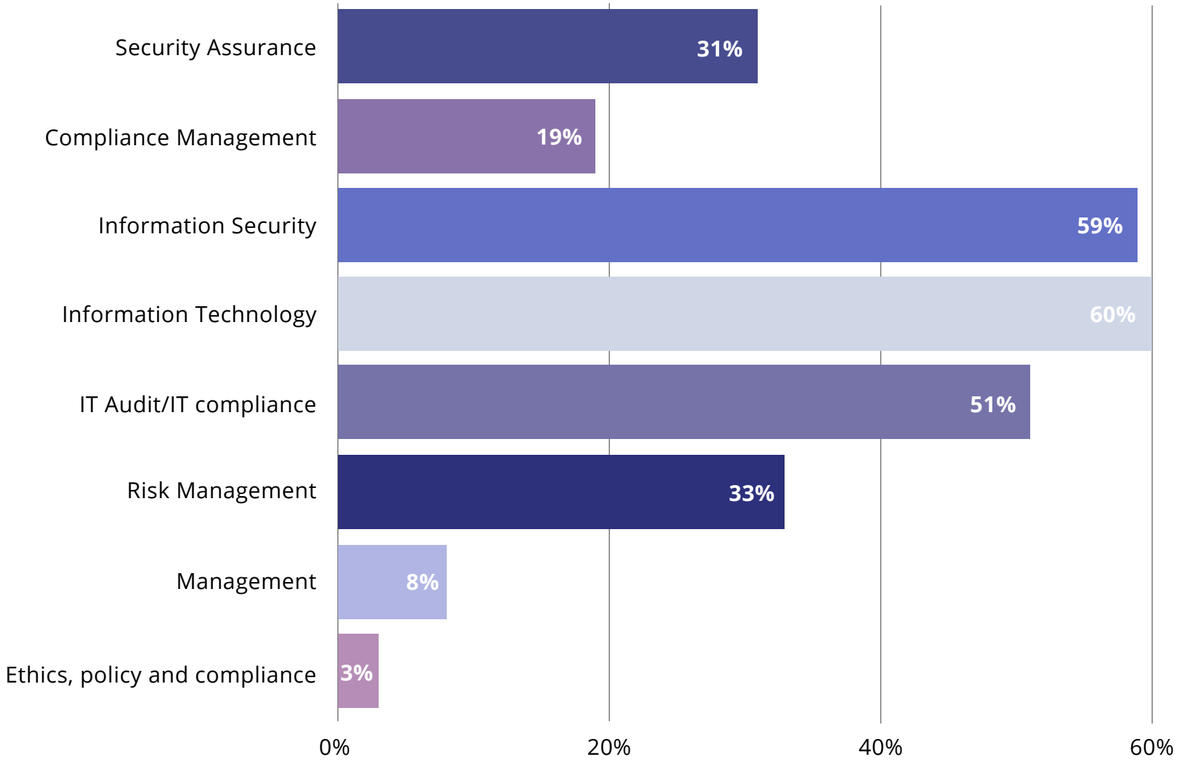
n= 1010



JOB FUNCTION

n= 1010

We asked respondents to tell us their primary job function
(they could select up to three job functions)



DECISION MAKING CAPABILITIES

83% of all respondents said they are directly involved in decisions regarding cybersecurity and data privacy risks for their organizations. 16% percent said they're knowledgeable enough to understand the requirements and needs regarding cybersecurity and data privacy for their organization. **1% said** they do not make decisions but are involved in maintaining IT security and data privacy for their company.

81% of respondents said they are the sole decision-maker in decisions regarding data security and data privacy compliance for their organization. **16% said** they are one of the decision-makers within their organization; **2% said** they are part of a team or committee, and **1%** said they gather information and provide research regarding data security and data privacy compliance.

ABOUT HYPERPROOF

Hyperproof is a security compliance management software company focused on bringing trust to life for its customers. The Hyperproof platform empowers compliance, risk, and security teams to stay on top of all compliance work and manage organizational risks (including vendor risks) continuously. Hyperproof is disrupting the GRC space by tackling a pressing problem ignored by others: helping compliance pros gain control over and effectively manage their ever-growing compliance workload. Industry-leading companies like Motorola, Instacart, 3M, Outreach, Nutanix, and Fortinet trust Hyperproof to help them manage their security and compliance efforts. To learn more about Hyperproof, visit **hyperproof.io**