hyperproof

2022 IT Compliance Benchmark Report

A look at how companies manage IT risks and compliance efforts in a time when requirements are increasing in complexity

hyperproof

Table of Contents

OPENING

03 **Foreword:** The State of Security Assurance in 2021 and Outlook on 2022

08 **2022 Survey Result Highlights**

CHAPTERS

15 **Chapter 1:** Priorities and Budget Allocation for 2022

22 **Chapter 2:** Governance and Staffing

27 **Special Segment:** The Benefits of Taking an Integrated Approach to IT Risk Management

34 **Chapter 3:** IT Risk Management — Perceptions, Approaches, and Key Activities

43 **Chapter 4:** Challenges with Risk Management Processes

48 **Chapter 5:** IT Security Assurance and Compliance Practices

53 **Chapter 6:** Tools For Managing Risks and Compliance Processes

APPENDIX

58 **Survey Methodology**

61 **About Hyperproof**

hyperproof

FOREWORD

The State of Security Assurance in 2021 and Outlook on 2022

Foreword: The State of Security Assurance in 2021 and Outlook on 2022

This is the third year that Hyperproof has conducted our annual ***IT Compliance Benchmark Survey***, a comprehensive survey which includes responses from over 1,000 participants and more than 50 benchmarks on how private-sector companies are managing IT risks and their compliance programs. To help our readers understand the benchmarks and statistics in this report in their proper context, we felt it necessary to create a short foreword that complements the report. The foreword summarizes what we believe to be the most important issues security assurance, compliance, and risk management professionals must grapple with at this moment in time.

With so much happening in the security and compliance industry each year, it's difficult to choose just one theme to discuss. But if we were to select just one theme to encapsulate 2021, it would be this: **Expectations on an organization's cyber hygiene and the maturity of their compliance program have ratcheted way up.** After companies and government agencies have suffered numerous devastating attacks for years — including major attacks on the nation's critical infrastructure sectors in 2021 (e.g., oil pipeline, financial, food, and transportation sectors were all affected), organizations have finally begun to step up their own cyber defenses and their oversight of vendors and suppliers.

As a SaaS provider, Hyperproof saw this trend of heightened scrutiny play out in our own sales cycle. In the past, potential customers asked us just a few security questions during the security review process. Now, many potential customers want to see a lot of detailed information to validate that our service is able to meet their security and privacy requirements. They are conducting detailed reviews of our SOC 2 report and asking a number of follow-up questions. We've also seen more instances of customers asking us to make contractual commitments to meet specific security requirements because they must meet certain contractual obligations themselves. Many of Hyperproof's customers — both Fortune500 and privately held companies — are in a similar situation and facing an increasing barrage of security questions from their customers.

REGULATIONS WITH SUPPLY CHAIN RISK MANAGEMENT REQUIREMENTS

The notion that supply chain risk management needs to become programmatic (vs. ad-hoc) has made its way into a number of regulations and industry standards in the last few years. Here are just a few of the more prominent regulations and standards organizations should pay attention to:

EU's General Data Protection Regulation (GDPR)

GDPR's scope includes all European Union organizations that collect, store, or process the personal data of any person residing within the EU, as well as any non-EU organizations that offer goods and services to European residents or non-EU organizations that process personally identifiable data. The European Union expects data processors — including managed service providers (MSPs) and SaaS providers — throughout the world to become compliant with GDPR legislation. EU organizations (data controllers) that leverage non-EU data processors must make sure their data processing vendors are following GDPR guidelines.

Under GDPR guidelines, data processors have a duty to protect data in a manner that ensures the security of all personal data, including protecting against unauthorized or unlawful processing, as well as against accidental loss and damage. Administrative, physical, and technical safeguards must be put in place, as EU law puts equal liability on data controllers and data processors.

California's Consumer Privacy Rights Act (CPRA)

The CPRA, which will go into full effect on January 1 2023, imposes a similar set of requirements on data processors — those who process personal data on behalf of another company — as GDPR. It obligates organizations that collect data (e.g., any company with consumers who reside in California) to hold their service providers accountable for protecting data in a manner that ensures the security of all personal data.

NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations

Any organization that handles federal information is required to implement NIST SP 800-53 controls and prove their compliance posture in order to maintain the relationship with their government customer.

NIST SP 800-53 got a major update in September 2020 that added a new control family on Supply Chain Risk Management. Based on its language, it's clear that NIST wants organizations to put risk at the heart of supply chain management. This control family emphasized several key points:

- All agencies and contractors are required to have formal risk policies and procedures to identify and manage supply chain risk.
- All agencies and contractors need to be aware of the origins and components of systems they use to ensure that changes upstream are assessed and documented.
- All agencies and contractors must assess suppliers based on identified risks, and agreed contractual or terms and conditions.
- All agencies and contractors must identify key supply chain information related to sensitive operations and systems; identify security controls to countermeasure third-party risks associated with the operations and systems.
- Third-party agreements or contracts should clearly underline any privacy-related controls that third-parties should adhere to as part of development of supply of systems and services.
- There must be notification agreements established to ensure third-parties know when and how to alert organizations in the event of issues.

In other words, NIST is saying that if your company is considered a "supplier" of a government contractor, you will need to implement the security controls your customer expects you to have and attest that you have them in your contractual agreement with the government agency. If you are using a third-party component in your own application, you will need to assess the risks posed by using that third-party component and verify that the third-party has adequate data protection safeguards in place to neutralize risks.

CMMC 2.0

The Cybersecurity Maturity Model Certification (CMMC) program was created in 2020 by the Department of Defense to verify that all companies in the Defense Industrial Base (DIB) — both contractors and subcontractors — have sufficient security and privacy safeguards in place to protect federal information (specifically, controlled unclassified information) within their care. The original version set five levels and required all contractors and subcontractors — regardless of whether they handle sensitive data or not — to go through a third-party certification assessment to verify their security controls and compliance posture.

In November 2021, the Department of Defense revamped the program (CMMC 2.0) to three levels and canceled the third-party certification requirement from companies in level 1 — those who do not handle controlled unclassified information. However, all level 1 companies (mostly small businesses) must perform an annual self-assessment and a company officer or executive will need to **affirm** that the answers provided in the annual self-assessment are accurate and complete.

To make sure that no one makes false claims in their security self-assessment, the Department of Justice has the legal power to investigate government contractors who allegedly submitted "false claims" regarding their cybersecurity practices under the False Claims Act (FCA). The DOJ can impose hefty fines on entities and individuals who are found guilty of fraud.

The DOJ said the following types of situations may trigger an investigation into an organization or an individual:

- Knowingly providing deficient cybersecurity products or services
- Knowingly misrepresenting their cybersecurity practices or protocols
- Knowingly violating obligations to monitor and report cybersecurity incidents and breaches

Under the FCA, a person acts *knowingly* when the person 1) has actual knowledge of the information, 2) acts in deliberate ignorance of the truth or falsity of the information, or 3) acts in reckless regard of the information. Further, the person need not have any specific intent to defraud the government.

Thus, as it relates to the CMMC 2.0's self-assessment affirmation, if the affirmation is incorrect, the DIB company could be liable under the FCA even though its leadership did not intend to defraud the government and did not have actual knowledge that its affirmation was incorrect. The DIB company could be found "in reckless disregard of the truth" by failing to conduct a sufficient due diligence of its cybersecurity practices and procedures prior to its affirmation. This subjects the company to damages and monetary penalties.

Here's the key takeaway from all these regulations: When organizations fail to put sufficient focus on their compliance program (including failing to conduct sufficient due diligence on their own and their third-parties' cybersecurity practices and procedures), they can lose customers and face significant legal liability. Executives overseeing company operations can also face personal liability under certain regulations like CMMC 2.0.

THE CHALLENGE FOR 2022: OPERATING UNDER A CONTINUOUS ASSURANCE MODEL

To reduce this potential liability, it's important for organizations to fully understand the requirements they're asked to meet and implement the controls necessary to meet those legal and contractual requirements. Organizations should test their controls and collect evidence on an ongoing basis to show customers (and regulators) that they are meeting their contractual obligations throughout the duration of the contract.

In addition to legal risk mitigation, continuous review and management of controls is critical for maintaining resilience. Cyber attack schemes are evolving quickly. New security and compliance risks can be introduced through routine business decisions, such as when employees start using a new cloud service to boost operational efficiency or when a division decides to launch a new product.

At this junction, organizations must rise to a new challenge. They need to build the capabilities necessary to operate under a **continuous assurance model**. This includes finding a way to scale the activity of implementing controls — activities undertaken to meet legal requirements, mitigate security and privacy risks, and improve operational efficiency. Organizations will need to stand up a **structured, repeatable, continuous approach** for training the right people on controls, assigning ownership of controls, assessing compliance to controls, and remediating gaps.

To be successful in operating in a continuous assurance model, organizations will need to use technology to centrally manage their compliance program and distribute responsibility of operating controls and managing risk to people within multiple business functions. Technology will empower people to perform control activities properly, on time, and efficiently — so that assurance work becomes a business enabler, not something that slows down the business too much.

This model of continuous assurance is a big departure from the audit-centric model of yesterday, where organizations relied on point-time audits to measure their security posture and determine what remediations are needed. Those who rise to the challenge of operating in a continuous assurance model will be the organizations who are trusted and beloved by their customers.

2022 IT Compliance Benchmark Report Authors:

JINGCONG ZHAO
Senior Director, Market Strategy & Product Marketing, Hyperproof

CAT HAUSLER
Content Marketing Manager, Hyperproof

hyperproof

HIGHLIGHTS

2022 Survey Result Highlights

2022 Survey Result Highlights

In November and December 2021, we surveyed 1,014 professionals in the Technology industry who are responsible for security assurance, IT compliance, information security, IT audits, and IT risk management within their organizations. 700 respondents work for companies headquartered in the US and 314 respondents work for companies headquartered in the UK. Respondents come from organizations as small as 50 employees and as large as 10,000+ employees. All respondents are directly involved in making decisions regarding security assurance, IT compliance, information security, IT audits, and IT risk management within their organizations.

HERE ARE THE TOP RESULTS FROM THIS YEAR'S SURVEY

1

Many intend to expand the scope of their third-party risk management programs in 2022.

Half of all surveyed organizations — 51% in total — are planning to expand their third-party risk management program in 2022.

Many organizations have become keenly aware that they need to get better at managing IT risks arising from the use of third-parties. In fact, greater awareness of third-party risk is one of the top reasons organizations have chosen to increase their overall IT risk and compliance management budget in 2022.

Three-quarters of all surveyed organizations said they have a process in place today to identify, treat and monitor third-party risks — but their processes aren't working well. 90% of all survey respondents reported being negatively affected by a third-party incident in the past year.

Of all respondents that experienced a third-party incident, 69% said a supply chain disruption affected their ability to deliver goods and services. 63% said they faced a third-party data breach that affected their organization's records or data. 28% said they experienced a compliance violation related to their organization's third-party oversight.

Many organizations in the survey admitted to struggling with managing the risks associated with third-parties and/or suppliers. We presented respondents with a number of vendor risk management challenges and asked them which ones they struggle with most. The top challenge — selected by 33% of survey respondents —is that **collecting risk information on third-parties is too manual and time-consuming.** Respondents also struggle with inefficiencies in orchestrating the vendor risk assessment/remediation process.

2 Data breaches continue to plague organizations.

We've all heard the saying it's not a matter of if, but when, when discussing the topic of data breaches. This saying is popular because it's true. In our latest survey, 63% of respondents reported that they experienced a data breach that led to the disclosure of regulated data — such as protected health information or other sensitive data — in the last 24 months. These data breaches typically cost an organization losses in the seven-figure range. Among respondents who had knowledge of data breaches within their organization, the biggest proportion — 44% of respondents — reported that they lost between $1M-5M. These organizations incurred costs including business disruption, productivity loss, revenue loss, legal fines, penalties, and the costs of remedies.

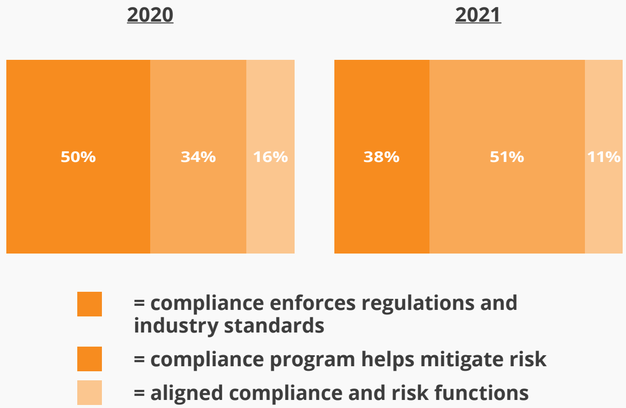
3 Many organizations have evolved beyond taking a "check the box" approach to compliance.

This year and last year, we asked respondents to share how they view the purpose of their compliance function. Is it the function that enforces regulations and industry standards? Or does their organization take an integrated view of how they manage their risks and align their risk and compliance activities whenever possible? Or, are they somewhere in between the two ends of the spectrum — where they recognize that a solid compliance program helps them mitigate risks, but risk and compliance activities are conducted separately?

Last year, 50% of all respondents said they view compliance as the function that enforces regulations and industry standards. This year, the proportion of respondents who answered this way dropped to 38%. Meanwhile, the proportion of those who said they believe that a solid compliance program helps them mitigate risks rose to 51%, from 34% last year. Interestly, the proportion of respondents reporting that their firm takes an integrated approach and have aligned their risk and compliance functions fell from 16% in 2020 to 11% this year.

The trend reveals that more organizations have decided that compliance isn't something that's done on the side. Instead, maintaining an effective compliance program is critical to managing risks well. It is encouraging to see organizations moving beyond a "check the box" approach to compliance. However, many organizations still have a ways to go in unifying their risk management and compliance effort. As this space continues to grow in complexity, more organizations will need to integrate compliance and risk in order to adequately meet all requirements and proactively deal with potential risk incidents.

Q: Question: Which statement best reflects how your organization views the purpose of the compliance function?



4 The status of the compliance function and its perceived importance within an organization continues to rise.

For the third year in a row, the majority of survey respondents reported that they plan to spend more money on compliance in the next 12 months. Forty-five percent of surveyed organizations — the biggest group — said they intend to spend more money on IT risk management and compliance in 2022 vs. 2021. A key factor for this budget increase is due to the US Government's new "zero trust" approach to managing cybersecurity. **Ninety percent of US-based respondents** whose organizations generate significant revenue from government contracts said that the government's move to overhaul how it manages cybersecurity is factored into their own security and compliance management plan in 2022.

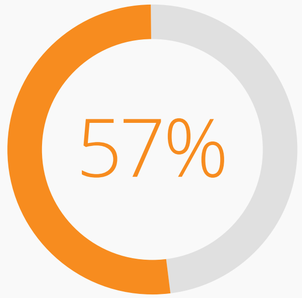
The majority of surveyed organizations have also made some commitments to manage their IT risks in a formal, disciplined approach. The further investment of resources (financial and otherwise) indicates that organizations are dedicated to the future of their IT risk management and compliance programs.

Going into 2022, the majority (63%) of survey respondents plan to add staff to their compliance team. Respondents also said that compared to a year ago, the head of the compliance function is now more likely to report to a C-level executive vs. a lower level position (e.g., director) in their organization. In addition to this, 74% percent of all respondents said their organization has identified clear roles and responsibilities and owners for various risks. These three data points show that organizations have become increasingly aware of the strategic importance of an effective compliance program and hiring a dedicated team.

5 A sharper focus on controls and effective compliance operations.

As the compliance function has been elevated in status, compliance and security assurance teams have also become more sophisticated in how they operate to meet compliance and security objectives. For example, many organizations have realized that controls are the key to cybersecurity management success. These organizations have identified appropriate controls by using industry frameworks as a reference and by understanding their risks. They are avoiding duplicating effort by implementing common controls frameworks that aggregates and rationalizes compliance requirements from different laws and regulations. They are assessing their security controls and the controls of key third-parties on a more frequent basis than in the past.

In fact, the use of a *common controls framework (CCF)* has become a mainstream practice. When asked "How does your organization deal with regional variances in data security and privacy regulations?"



of all respondents said they utilize a CCF that aggregates and rationalizes compliance requirements from different laws and regulations to organize their security and privacy risk management practices

This practice exceeded the two alternatives by quite a stretch. In fact, only 37% of organizations said they identify the most stringent/comprehensive law they must comply with and structure their compliance and risk management activities to meet that law. Just 5% said they deal with new privacy and data security regulations one at a time, as they are passed.

We saw that many organizations are referencing a number of IT risk/security/compliance frameworks to ensure they have a good set of controls to safeguard information. The most referenced frameworks among survey respondents are CIS Security Controls (50%), NIST Frameworks (e.g. NIST CSF, NIST SP 800-53; 49%), and ISACA IT Risk Framework (47%).

This year, we saw more organizations using the practice of regular internal audits (in addition to external audits) to ensure that their controls over information security and data privacy are operating effectively. Half of all respondents said their organization expects them to test all controls in their organization — not just the ones for their next audit or the top ones according to their risk assessment result. 56% of all respondents said they test all controls.

This year, 48% of all organizations said they collect evidence for internal and external audits and that internal audits are done regularly. Last year, only 27% of respondents answered this way. In addition, one in five (21%) respondents this year said they are collecting evidence on an ongoing basis, as part of a continuous compliance program.

Collectively, these findings indicate that organizations are getting more rigorous around managing their controls. The level of maturity is higher than we'd expected and we're encouraged to see these results. With more threats, more systems to protect, more tools to deploy, and more people to manage, organizations face constant pressure to move faster and keep up with the ever-changing risk landscape. We believe that there is a strong need for organizations to have proper controls in place to manage cybersecurity threats and risks across applications, systems, facilities, and third-parties.

6 Risk and compliance management tools proliferate but efficiency gains haven't been realized.

The use of dedicated GRC tools to manage IT risks and compliance programs has increased YoY. For instance, 57% of respondents this year said they use the risk module in a cloud-based GRC software to document and track their risks (compared to 41% last year). Fifty-five percent of this year's respondents said they use the compliance module in a cloud-based GRC software to manage their IT compliance effort (compared to 20% last year). Fifty-five percent of this year's respondents said they are using software purpose built for managing IT compliance operations (compared to 45% last year).

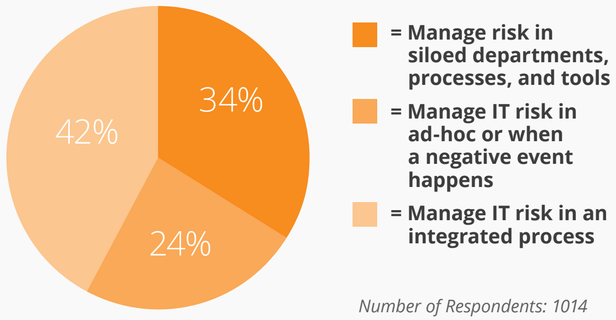
However, time spent on routine, repetitive, administrative tasks has not decreased correspondingly. The typical respondent said their compliance function still spends about 40% of their time at work on tasks that are administrative in nature, which aren't a good use of a skilled professional's time. It is possible that some organizations adopted new tools shortly before taking the survey, and thus haven't fully implemented the tools to receive value. But on the whole, the data suggests that GRC tools have not delivered the efficiencies organizations are looking for.

Why is this the case? We see two likely scenarios. One, we found that organizations' GRC tools may not be integrated with the other apps their employees are already using. In fact, while many organizations have some type of GRC software, they still manage portions of their compliance program in numerous other places.

For instance, we found that 45% of respondents store some compliance documents in cloud-based file storage systems such as Box, Google Drive, OneDrive and SharePoint. Email is still a popular tool for coordinating compliance projects, and another sizable chunk of compliance information resides in cloud infrastructure services such as Azure, AWS, and Google Cloud.

If GRC tools aren't easily integrated into an organization's broader tech stack to allow people to pull in compliance data automatically and work where they prefer, their value is limited. In fact, over 85% of all respondents are still planning to evaluate new tools next year with the goal of streamlining and automating their compliance processes.

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



Number of Respondents: 1014

Further, 58% of all respondents admitted that their organization manages IT risk in a way that lacks sufficient planning and coordination between the various parties that need to be involved. When we asked respondents "What of the following statements is the closest to how your organization manages IT risks?", the results break down as follows:

- Thirty-four percent of all respondents said they manage IT risks in siloed departments, processes and tools.
- Twenty-four percent said they manage IT risk in ad-hoc or when a negative event happens.
- The remaining respondents said they manage IT risk in an integrated process.

Even the most powerful IT risk management tools can under-deliver when key processes haven't been established. Our survey results point to the possibility that a lack of process and coordination between the key stakeholders involved in IT risk is hindering organizations from making the most out of the tools they already have. When different teams use different tools, the organization cannot easily gain an accurate, complete picture of their compliance posture.

7 Taking an integrated approach to risk and compliance management is a key practice for lowering organizations' security risk and increasing resilience.

In this survey, we asked respondents "Which statement best reflects how your organization views the purpose of the compliance function? They could choose from one of three options:

1. My organization views compliance as the function that enforces regulations/industry standards.
2. We believe that having a solid compliance program helps us mitigate risks; but risk management and compliance activities are typically conducted separately, in response to separate events.
3. My organization has an integrated view on how to manage our unique set of risks - our risk and compliance activities are tied together and aligned.

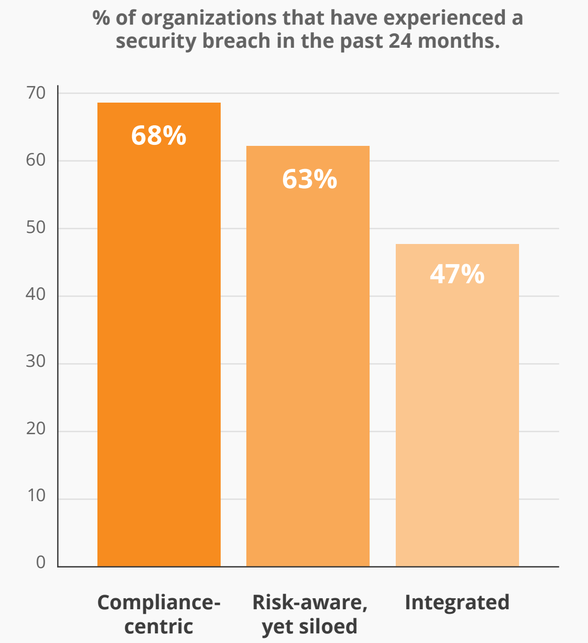
For the purpose of this analysis, we call the first cohort the “compliance-centric” cohort. 38% of all respondents self-reported into this cohort. We call the second cohort the “risk-aware yet siloed” cohort. 51% of respondents self-reported into this cohort. We call the third cohort the “integrated” cohort; just 11% of all respondents self-reported into this cohort.
We found strong evidence that the organizations that take an integrated approach have better security posture and face a lower level of risk compared to organizations who view their compliance function strictly as the function that enforces rules and regulations.

While 63% of survey respondents overall reported that their organization has experienced a security breach in the past 24 months, only 47% of those who take an integrated approach to risk management and compliance activities experienced a security breach. This is a statistically significant result from the other two cohorts. Meanwhile, 68% of all respondents in the “compliance-centric” cohort experienced a security breach in the past two years. Of those who believe that compliance programs help mitigate risk but still manage activities in silos, 63% reported a compliance violation.

Further, organizations that take an integrated approach spent less time on repetitive/ administrative tasks compared to the other two cohorts. The average organization that takes an integrated approach said their compliance team spent 31% of their total time on administrative tasks that aren’t a good use of time, while the average compliance-centric organization reported that their compliance team spent 42% of their total time on administrative tasks!

Why are organizations in the integrated cohort less prone to falling victim to data breaches and more efficient in managing their compliance program? We found that these integrated organizations are more likely to pay close attention to the controls they’ve put in place to ensure that information security objectives are met. They are better at identifying controls to treat specific risks and making sure controls are remediated if they’re tested and are deficient. Further, they are more likely than other organizations to collect evidence on an ongoing basis to verify the effectiveness of controls.

Q: Has Your organization experienced a security breach in the past 24 months?



Number of Respondents: 1014

hyperproof

CHAPTER 1

Priorities and Budget Allocation for 2022

01 | Priorities and Budget Allocation for 2022

In chapter one, we will report on the key risks organizations faced in 2021, which risk management program areas organizations want to pay greater attention to going forward, their compliance budget allocations, and 2022 budgeting plans.

TOP-OF-MIND RISKS FOR SURVEYED ORGANIZATIONS

Cybersecurity attacks are not only at an all time high, but attackers' tactics are getting more and more creative. With this in mind, it's no surprise that the top response of organizations when asked "Which of the following causes your job to be more stressful?" was **cybersecurity risks**. This was the first-ranked answer in our 2020 survey as well, and unfortunately, it is not likely to change moving forward.

Many organizations suffered from data breaches in 2021. In fact, **63% of respondents reported that they experienced a data breach that led to the disclosure of regulated data** — such as protected health information or other sensitive data — in the last 24 months. Of those respondents, small/mid-sized companies (250 to less than 1,000 employees), enterprise companies (5000+), and those who have been in business less than five years reported the highest percentage of data breaches in 2021. These data breaches proved costly for most organizations — **44% of companies who reported a data breach said they lost between $1M-5M.**

Data privacy risks were a primary stressor for our respondents as well. This also isn't shocking considering that most surveyed organizations need to comply with multiple, disparate data privacy regulations — some of which apply broadly to businesses (including organization's suppliers and vendors) and to many kinds of data. For instance, GDPR and other major data privacy laws like CPRA (California), CPA (Colorado), VCDPA (Virginia) not only hold organizations ("data collectors") accountable

63%

experienced a data breach that led to disclosure of regulated data

44%

reported a data breach that cost them between $1M—$5M

hyperproof

for meeting privacy and security principles, but also require organizations ("data collectors") to hold their service providers ("data processors") accountable to meeting the same privacy and security principles. As such, organizations can easily step outside the bounds of privacy laws if they're not careful.

In 2021, widely-used social media companies Meta (Facebook) and LinkedIn faced allegations of violating users' privacy. In addition to concerns around data privacy incidents, there's an increasing number of information security and privacy regulations and standards that companies must conform to in order to do business with their target customers.

An issue that's having more of an impact on our respondents this year is **identifying and managing IT risks rising from use of 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 importance. But the pattern is starting to shift — 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.

Considering this, we asked, "Heading into 2022, which phrase best describes your third-party risk management program?"

- Fifty-one percent of respondents labeled their third-party risk management program as "expanding".
- Forty-seven percent said they'll keep their programs in a "steady state".
- Only three percent reported a reduction in their third-party risk management program.

Third-party risk management is receiving greater organizational focus because the majority of surveyed organizations experienced adverse events due to a third-party in 2021. When asked to specify the type of event(s) experienced in 2021, respondents reported the following:

62%
organization was impacted by a supply chain disruption that affected their ability to deliver goods or services.

57%
experienced a third-party data or privacy breach that affected their organization's records or data

25%
reported a compliance violation related to their organization's third-party oversight

10%
did not experience any third-party incidents

Segment Differences

US vs. UK: The primary and most significant difference between events experienced by US vs. UK companies was regarding supply chain disruption. Organizations in the UK were significantly more impacted by these types of events (71% vs. 58%).

Time in business: Supply chain disruptions also had the biggest impact on companies in business for five years to less than 10 years. Seventy-one percent of organizations this size reported a disruption in supply chain vs. 59% of companies in business for 10+ years, and 52% percent in business for less than five years.

How organizations view the purpose of their compliance function: Organizations who see compliance as helping to mitigate risks, but with risk and compliance activities being conducted separately, experienced significantly more supply chain disruptions. In comparison, companies who view risk and compliance activities as being tied together and aligned reported significantly more compliance violations related to their organization's third-party oversight.

Perception on Spending Level

Knowing that compliance is top of mind for many respondents, we wanted to better understand how organizations view compliance management spend and how they plan to allocate dollars moving forward.

Sixty-eight percent of organizations believe they are currently devoting the right amount of resources to risk and compliance management. Companies in the UK reported significantly higher in terms of this than US companies did (73% vs. 66%).

Current Allocation of Funds Within Compliance

Although spending varies from one organization to the next, when we aggregated the responses, we saw the average (or mean) organization chose to allocate their compliance spend in the following way:

- 28%: Technology (governance, risk and compliance tools)
- 26%: Staff (management and training programs)
- 24%: Compliance Audits (attestations, enforcements, monitoring and forensics)
- 22%: Outsourcing (consultants to address risks, etc.)

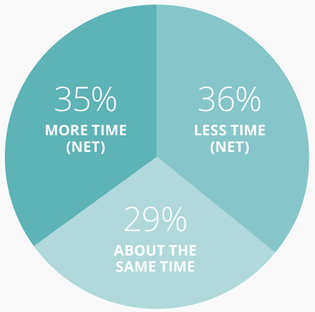
Governance, risk, and compliance tools were at the top of this list for respondents in last year's report as well. This would indicate that this type of technology is still important to compliance and security professionals.

Reported spend on staff increased significantly year-over-year (YOY) — 26% in 2021 vs. 23% in 2020. As compliance needs continue to grow, companies of all sizes should expect to allocate more funds to management and training programs.

Anticipated Spending for 2022

When asked "Heading into 2022, do you anticipate that your organization will spend more, less or about the same amount of time on IT risk management and compliance overall?" there was a close split in answers. Here is the breakdown of responses:

Q: Heading into 2022, do you anticipate that your organization will spend more, less or about the same amount of time on IT risk management and compliance overall?

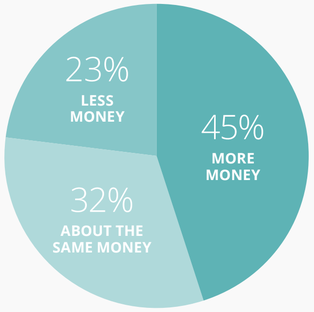


Number of Respondents: 1014

Despite the ongoing need for IT risk management and compliance, most respondents do not anticipate spending significantly more or significantly less time on this area in 2022. However, it is interesting to note how close the percentages are for slightly more anticipated time spent and slightly less anticipated time spent (29% vs. 30%).

While results were relatively split on anticipated time spent on IT risk management and compliance, respondents were more aligned in terms of anticipated financial contribution. **Forty-five percent of organizations — the biggest group — said they intend to spend more money on IT risk management and compliance in 2022 vs. 2021.** Thirty-two percent of respondents said they will keep spending the same year over year. Twenty-three percent said they plan to spend less in 2022.

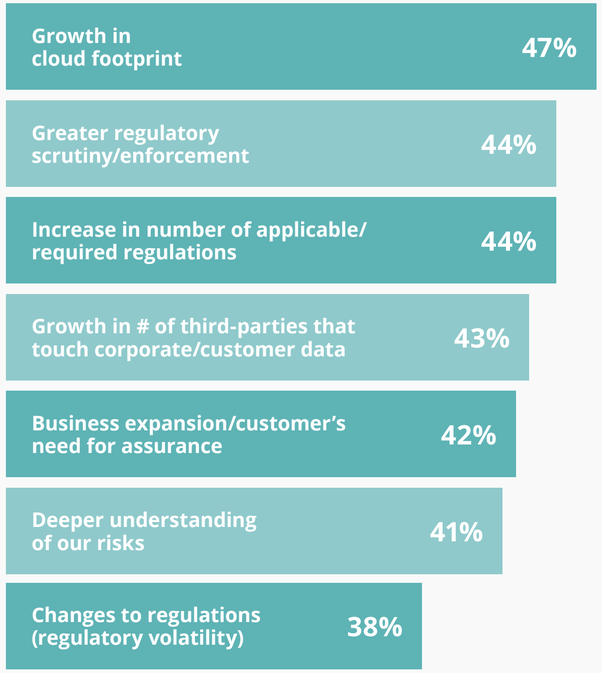
Q: Heading into 2022, do you anticipate that your organization will spend more, less or about the same amount of money on IT risk management and compliance overall?



Number of Respondents: 1014

Organizations who expect to increase spending on IT risk management and compliance in 2022 reported the following as the top factors that will drive higher spend:

Q: What are the top factors driving your IT risk/ compliance spend increase?
Summary of Ranked top 3.



Number of Respondents: 454

These responses vary quite a bit from what organizations reported in 2020:

- **The top answer to this question in 2020 was changes to regulations (regulatory volatility),** with 55%.
- "Growth in cloud footprint" grew in importance year-over-year (YOY) — 29% in 2020 to 47% in 2021.
- On the other hand, "changes to regulations" dropped from the top spot to the bottom of the list.
- "Business expansion/customer's need for assurance" also saw a greater percentage YOY, growing from 35% to 42%.

There have been some significant changes to the US government's management of cybersecurity in 2021. These changes have exerted downward pressure on private sector organizations to put more rigor into their compliance program.

In 2021, the Biden Administration announced ambitious plans to improve cybersecurity across the federal government. The federal government is overhauling how it manages cybersecurity; it intends to pursue a "zero trust" strategy focusing security on users, assets, and resources, and authenticating them all the time. For contractors and IT providers, it means that they should integrate those big objectives into their security plans and routine operations sooner rather than later. For instance, contractors may start by self-assessing their readiness to meet requirements set out in NIST SP 800-53 (Moderate Impact) and NIST 800-171 to ensure they're prepared to meet security requirements that will come up in the contracting process.

In this survey, we asked US respondents whose organizations generate significant revenue from government contracts *whether the government's move to overhaul how it manages cybersecurity factored into their own security and compliance management plan in 2022.* **Ninety percent of US-based respondents replied "yes".**

Additionally, the Department of Justice introduced the Civil Cyber-Fraud Initiative, in the fall of 2021 to prompt government contractors and grant recipients to improve their security practices in order to limit future cybersecurity incidents. The federal government is planning to use the False Claims Act — which imposes hefty fines on entities who are found guilty of purposely submitting "false claims" to the government — to push organizations to maintain effective compliance programs and avoid misrepresenting their cybersecurity practices or protocols.

With these factors in mind, it's not surprising that the *increase in the number of applicable/required regulations* and *greater regulatory scrutiny/enforcement* are some of the top ranked reasons why organizations are increasing their 2022 IT compliance program budget.

Q: Did you factor the U.S. government's cybersecurity overhaul into your own 2022 compliance budget?

90%

Responded 'yes'

How Much Are The Planned Budget Increases?

Of the respondents who said that they expect to increase their spend on IT risk and compliance, **45% reported that they plan to spend 10-25% more in 2022.** This is less of an anticipated financial increase compared to 2020 when the majority of organizations said they expected to raise spend on IT risk and compliance by 25-50% in 2021.

Q: What is the expected or planned increase in your compliance budget in the next 12 to 24 months?

		Company HQ		Time in Business		
	Total	**US**	**UK**	**< 5 years**	**5–10 years**	**10–15 years**
	454	307	147	71	192	126
1% to 10% increase	18%	15%	22%	13%	13%	21%
10% to 25% increase	45%	46%	44%	46%	49%	42%
25% to 50% increase	30%	31%	30%	35%	28%	32%
50% to 100% increase	6%	7%	4%	6%	8%	5%
More than a 100% increase	1%	1%	—	—	2%	—

Number of Respondents: 454

hyperproof

CHAPTER 2

Governance and Staffing

02 | Governance and Staffing

In the last chapter, we reported on the key risks organizations faced in 2021, risk management program areas organizations want to pay greater attention to going forward, their compliance budget allocations, and 2022 budgeting plans. In this chapter, we will reveal organizations' structures for managing IT compliance programs, staffing/personnel levels, and staffing growth plans. We'll also report on the GRC activities organizations tend to outsource.

ORG STRUCTURES FOR MANAGING GRC PROGRAMS

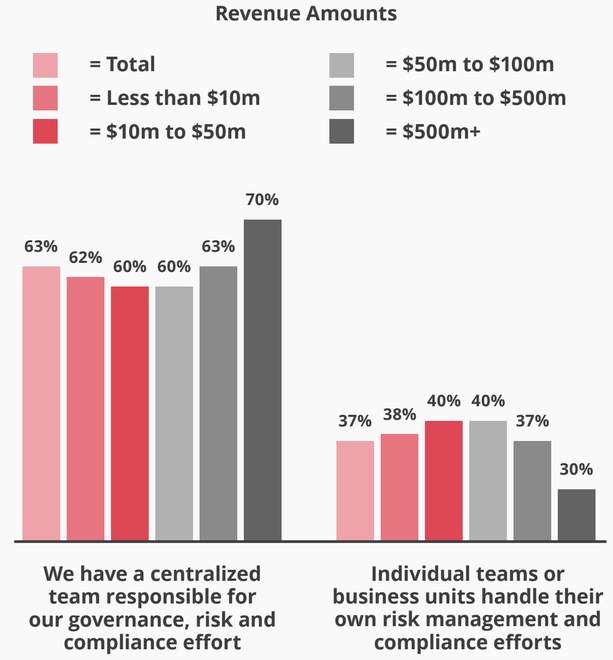
Sixty-three percent of all respondents reported that their organization has a centralized governance, risk, and compliance program that cuts across business units and geographies, while just 37% of all respondents said individual teams are responsible for their own risk management and compliance efforts.

When we compared US and UK companies, we didn't find meaningful differences in how these respondents structured their risk and compliance programs. However, very large organizations — those that made more than $500 million in 2021 — were significantly more likely to have a central team (70%) vs. smaller organizations (those that made less than $500M).

We also asked respondents a related question: **"Is the risk function a distinct, separate function from the compliance function? Or are risk responsibilities rolled into the compliance personnel's jobs?"**

- Forty-eight percent of respondents have separate risk and compliance functions — each with their own staff.
- Forty-six percent said their organization has an integrated function, and risk responsibilities are rolled into compliance personnel's jobs.
- The remaining proportion (6%) said the arrangement varies by business function/and or location.

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



Number of Respondents: 821

Segment Differences

US vs. UK: US companies are significantly more likely to keep risk and compliance as separate functions compared to UK companies (50% vs. 43%).

Time in business: Organizations that have been in business for 10 years or longer are significantly more likely to integrate their risk and compliance activities into a single function compared to their companies that have been in business for less than five years (54% vs. 37%).

We could not find meaningful differences in how companies structure their risk management function when we reviewed the data by company revenue and employee count.

Personnel Plans

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

The mean (or average) organization in the survey set said they have 21 full time staff dedicated to the compliance function. However, there is significant variability among those who answered the question. Here's the breakdown of staffing.

Q: How many full time staff are dedicated to the compliance function at your organization?

	Company Size					
	Total	50 – 250	250 – 1,000	1,000 – 2,500	2,500 – 5,000	5,000+
# of Staff	1014	196	341	184	127	166
1	1%	5%	1%	—	—	1%
2	4%	7%	4%	4%	2%	1%
3	9%	16%	11%	10%	5%	1%
4	12%	14%	13%	14%	12%	5%
5-10	23%	33%	21%	26%	17%	14%
10-25	19%	9%	21%	20%	22%	22%
25-50	15%	3%	19%	15%	22%	18%
50+	17%	13%	11%	12%	20%	37%
Mean	21	14	18	18	26	33

Number of Respondents: 1014

The size of the compliance team correlates positively with the size of the organization. Large organizations generally have more staff dedicated to the compliance function compared to smaller organizations.

WILL COMPLIANCE TEAMS GROW IN 2022?

Going into 2022, the majority (63%) of survey respondents plan to add staff to their compliance team. Thirty-seven percent said that their compliance team will stay the same. Just 1% said they expect their compliance team to shrink. These results remained consistent from last year to this year.

We did not see significantly different results in this question when we compared US respondents to UK respondents.

We did not see significantly different results when we compared companies based on how long they've been in business or how much revenue they generated in 2021.

Segment Differences

How organizations view the purpose of their compliance function: Those who view compliance function as the function that enforces regulations are significantly more likely to add staff to their compliance team compared to those organizations whose risk and compliance activities are integrated (65% vs. 54%). This result isn't surprising; when organizations align their risk and compliance activities, synergies and efficiencies are created and duplicative efforts can be eliminated. Thus, the need to add additional staff is reduced in such organizations.

WHAT IS THE HIGHEST LEVEL POSITION OR TITLE OVERSEEING COMPLIANCE?

Overall, those in charge of security, IT risk, and compliance decisions have high standing within their organization as well as significant formal authority:

- Eleven percent of respondents said their company's board of directors are directly overseeing the compliance function.
- Seventeen percent of respondents said their compliance function reports to the company's president or CEO .
- Nearly half (46%) of all respondents said their compliance function reports to a member of the C-suite staff that's not the CEO, such as CIO, CISO, CTO, COO, etc.
- Thirteen percent of all respondents said the most senior person in charge of compliance is a director-level individual.

Compared to a year ago, the head of the compliance function is now more likely to report to a C-level executive vs. a lower level position (e.g., director) in their organization. This is a sign that more organizations have become aware of the strategic importance of an effective compliance program over time.

Segment Differences

US vs. UK: A greater proportion of UK companies tend to view their compliance function as a highly strategic function compared to US companies. Respondents in UK- based companies are also more likely to have their Board overseeing their compliance function vs. US respondents (14% vs. 9%). Respondents in US-based companies are more likely than their UK counterparts to report that the highest level position overseeing the compliance function is a C-suite executive (48% vs. 40%).

Company age: Younger companies (those in business for less than five years) are much more likely to have their CEO/president overseeing the compliance function vs. companies in business for longer than five years. Meanwhile, companies that have been in business for five years or more are more likely to shift this responsibility to someone in the C-suite other than the CEO/president.

WHAT RISK MANAGEMENT AND COMPLIANCE ACTIVITIES GET OUTSOURCED?

It is difficult for organizations to hire enough staff to fully address all their risk management, security, and compliance program's needs. GRC expertise is relatively scarce and talent is expensive. The vast majority (98%) of all surveyed respondents outsource one or more IT compliance activity to third-party advisory firms.

98%

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

In terms of types of activities outsourced, it turns out that organizations are outsourcing a variety of tasks. The most commonly outsourced activity is **IT security and asset management.** In second place is **risk assessments.** Vendor management and project management were the least outsourced activities.

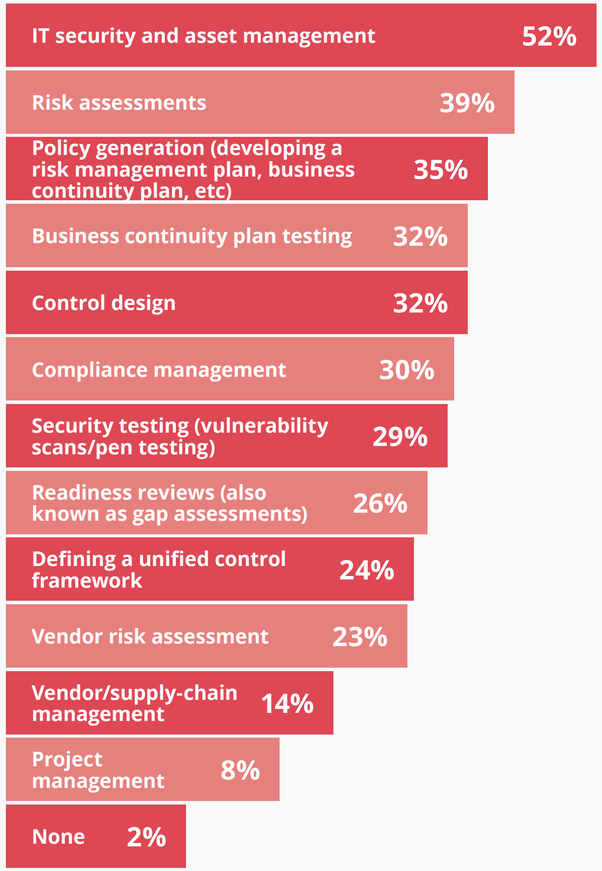
Segment Differences

US vs. UK: UK companies are far more likely to outsource **IT security and asset management** compared to US companies (58% vs. 49%). UK companies are also more likely to outsource the **management of their compliance program** (36% vs. 28%).

Company age: Organizations that have been in business for 5-10 years are significantly more likely to outsource **IT security and asset management** to a third-party compared to organizations that have been around for less than five years (52% vs. 41%). Organizations that have been around for longer than 10 years are even more likely to outsource **IT security and asset management** (63% of them outsource this activity).

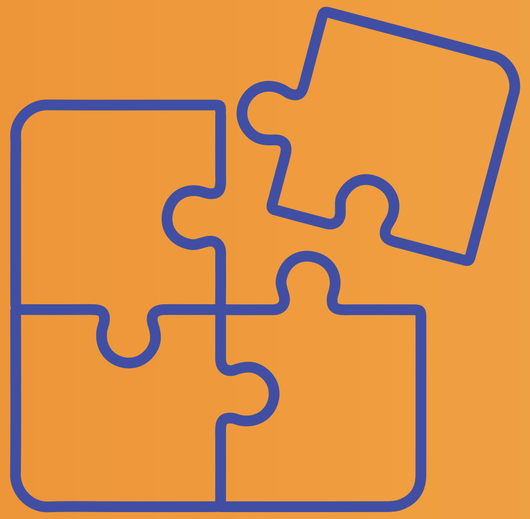
Younger organizations are more likely to seek assistance on **control design** from a third-party compared to older companies. Thirty-seven percent of companies that have been in business for less than 5 years have outsourced **control design**, compared to just 26% of companies that have been around for 10 to 15 years.

Q: What risk management and compliance activities get outsourced?



Number of Respondents: 454

hyperproof



SPECIAL SEGMENT

The Benefits of Taking an Integrated Approach to IT Risk Management

2a | The Benefits of Taking an Integrated Approach to IT Risk Management

In the past several years, industry analyst firms like Gartner, as well as various GRC vendors, have championed the value of taking an integrated approach to risk management and compliance (also known as a "risk-first" approach). This represents a departure from a compliance-first approach — which is when an organization opts to define its security policies and internal controls based on regulatory requirements (i.e., either laws or infosec frameworks/standards).

Arguments against using the compliance-centric approach are two-fold: first, organizations often get a false sense of security once their auditor says they've met certain regulatory requirements and standards (e.g., an organization receives their SOC 2 type II report). Second, as organizations expand and their regulatory obligations grow (and risks evolve), they end up spending more time and money than necessary on infosec compliance. Why? Because when a firm tries to adhere to multiple compliance frameworks and mitigate multiple risks while treating each as a separate project, they end up duplicating work and repeating the same (or highly similar) activities.

On the other hand, organizations that take an integrated approach choose to focus first on their unique set of risks, and addressing compliance requirements becomes just a portion of a holistic risk management approach. These organizations start the risk management process by conducting a risk assessment. They create security policies and implement internal controls tailored to the results of their risk assessment. (A control is a specific action, process, or protocol designed to mitigate a specific risk or neutralize a specific threat.) Those controls are mapped to "standard" controls in IT compliance frameworks and regulatory requirements to minimize duplicative efforts. The compliance team's focus is then ensuring that key controls are evaluated for proper functionality so that material risks are mitigated, not simply ticking off boxes outlined in regulations.

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 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:**

- As a group, organizations who take an integrated approach do a much better job at avoiding data breaches and security incidents than those who believe the compliance function's purpose is to enforce rules.
- When organizations experience a security breach, on average, organizations that take an integrated approach to risk management (aligning risk and compliance activities) lose less money than organizations who view their compliance function as the enforcer of rules (and manage risk and compliance activities separately).
- 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.

KEY FINDINGS

In this survey, we asked respondents to select one statement from the set below that best reflects how their organization views the purpose of the compliance function:

- My organization views compliance as the function that enforces regulations/industry standards.
- We believe that having a solid compliance program helps us mitigate risks; but risk management and compliance activities are typically conducted separately, in response to separate events.
- My organization has an integrated view on how to manage our unique set of risks - our risk and compliance activities are tied together and aligned.

Here's the breakdown of responses:

- Just over half (51%) of all organizations said they believe that having a solid compliance program helps them mitigate risks. But risk management and compliance activities are still conducted separately, in response to separate events.
- 38% said their organization views compliance as the function that enforces regulatory/industry standards; in other words, compliance is a separate function from the risk management function.
- 11% of all respondents said their organization has an integrated view on how to manage their unique set of risks.

Segment Differences

US vs. UK: Companies in the US are significantly more likely to view compliance as the function that enforces regulations than UK-based companies (41% vs. 30%). UK companies are significantly more likely to take an integrated approach on how they manage their risks (15% vs. 10%).

Employee size: The largest companies (those with more 5,000 employees) are significantly more likely to take an integrated risk management approach compared to mid-size companies (those with 250 to less than 1000 employees and those with between 1000 and 2,500 employees).

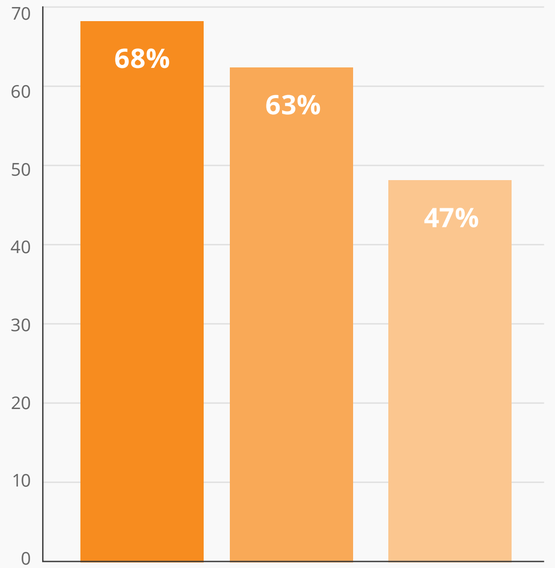
We found that organizations' perspective on the purpose of their compliance function is not correlated with their longevity. Companies that have been around for 15 years are no more likely to take an integrated view on risk management than companies that have been around for 3, 5, or 10 years. Further, companies' perspective didn't correlate with how much revenue they generated.

As a group, organizations who take an integrated approach do a much better job at avoiding data breaches and security incidents than 1) those who believe the compliance function's purpose is to enforce rules and 2) those who believe that their compliance program helps with risk mitigation but conduct risk and compliance activities in silos. The differences we found are statistically significant.

While 63% of survey respondents overall reported their organization has experienced a security breach in the past 24 months, only 47% of those who take an integrated view of risk management and compliance activities experienced a security breach. On the other hand, 68% of all respondents who view the compliance function as the enforcer of rules have experienced a security breach in the past two years. Of those who believe that compliance programs help mitigate risk but still manage activities in silos, 63% reported a compliance violation.

When organizations experience a security breach, on average, organizations that take an integrated approach to risk management (aligning risk and compliance activities) lose less money than organizations who view their compliance function as the enforcer of rules (and manage risk and compliance activities separately). While the average organization that views the compliance function as the enforcer of regulations lost $4.43 million in an incident, the average organization that takes an integrated approach lost $3.46 million; that's almost a million-dollar difference.

Q: Percentage of organizations that experienced a security breach In the past 24 months:



= My organization views compliance as the function that enforces regulations

= Having a solid compliance program helps us mitigate risks, but risk management & compliance activities are typically siloed

= My organization has an integrated view on how we manage our unique set of risks – our risks and compliance activities are aligned

Number of Respondents: 638

Further, we found that **organizations that take an integrated approach spent less time on repetitive/ administrative tasks.** The average organization that takes an integrated approach spent 31% of their total time on administrative tasks; while the average organization that viewed compliance as the policing function spent 42% of their total time on administrative tasks!

Average Time Compliance Pros Spend on Admin Tasks (as a % of total time at work)

31%

Orgs that take an integrated approach to risk and compliance management

42%

Orgs that view compliance as the policing function

Why are organizations in the integrated cohort less prone to data breaches and more efficient in managing their compliance program? We found that these integrated organizations are more likely to pay close attention to the **controls** they've put in place to ensure that information security objectives are met.

Organizations in the integrated cohort are better at **identifying controls** for risk mitigation, **flagging control deficiencies**, and **remediating issues** than organizations in the other two cohorts. Organizations in the integrated cohort are significantly more likely to say that they are successful at the following risk management activities compared to organizations in the two other cohorts:

- **Identify controls:** Eighty-one percent of respondents in the integrated cohort said they have identified specific controls needed to treat specific risks. Seventy-two percent of respondents in the compliance-centric cohort responded this way. Sixty-five percent of respondents in the "risk-aware but siloed" cohort responded this way.
- **Flag exceptions, review, and remediate:** Seventy-two percent of respondents in the integrated cohort said they are reviewing control test results and doing a good job at remediating controls when necessary. Sixty-six percent of respondents in the compliance-centric cohort responded this way. Sixty-one percent of respondents in the "risk-aware but siloed" cohort responded this way.

Q: In your opinion, how well is your company doing in performing each of the following risk management actions? Summary Of Meets Our Company's Objectives

	How Org Views Purpose of Compliance Function		
	Function that enforces regulations/industry standards	**Helps us mitigate risks; but risk and compliance activities are conducted separately**	**Our risk and compliance activities are tied together and aligned**
Respondents	383	518	113
Identify & assess risks	92%	91%	96%
Assess controls effectiveness	78%	71%	80%
Capture, track & report deficiencies	74%	72%	78%
Align controls with risks	72%	71%	76%
Identify controls	72%	65%	81%
Validate controls against standard controls	69%	68%	70%
Monitor & automate controls testing	68%	66%	73%
Flag exceptions, review & remediate	66%	61%	72%

Number of Respondents: 1014

What enables those in the integrated cohort to manage controls more effectively than the other two cohorts? **We found it's because these organizations, compared to the other two cohorts, are more digilent in collecting evidence needed to verify that controls are operating effectively.** In fact, they're far more likely than other organizations to collect evidence on an ongoing basis as part of a continuous compliance program.

We asked all respondents to "choose the statement that most accurately reflects how your organization approaches evidence collection to verify that controls are operating effectively". Answer choices are the following:

- We collect evidence only for external audits.
- We collect evidence on an ad-hoc basis (e.g., when we need to determine whether we're meeting our existing compliance requirements when we launch a new service).
- We collect evidence for internal and external audits. We conduct internal audits regularly .
- We collect evidence on an ongoing basis, as part of a continuous compliance program.

We found organizations in the integrated cohort are far less likely to say that they only collect evidence for external audits compared to organizations in the compliance-centric cohort. Only 8% of those in the integrated group selected this response compared to 43% of all respondents in the compliance-centric cohort.

Meanwhile, organizations in the integrated cohort are significantly more likely to collect evidence on an ongoing basis as part of a continuous compliance program. 39% of integrated organizations selected this response compared to just 13% of all respondents in the compliance-centric cohort.

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

	How Org Views Purpose of Compliance Function		
	Function that enforces regulations/industry standards	**Helps us mitigate risks; but risk and compliance activities are conducted separately**	**Our risk and compliance activities are tied together and aligned**
Respondents	383	518	113
We collect evidence for internal and external audits. We conduct internal audits regularly	41%	55%	38%
We collect evidence only for external audits	43%	17%	8%
We collect evidence on an ongoing basis, as part of a continuous compliance program	13%	22%	39%
We collect evidence on an ad-hoc basis (e.g. when we need to determine whether we're meeting our existing compliance requirements when we launch a new service)	4%	6%	15%

Number of Respondents: 1014

hyperproof

CHAPTER 3

IT Risk Management — Perceptions, Approaches, and Key Activities

03 | IT Risk Management: Perceptions, Approaches, and Key Activities

Chapter 2 of this report reviewed organizations' structures for managing IT compliance programs, staffing/personnel levels, staffing growth plans, and the GRC activities organizations tend to outsource. In this chapter we will examine the major risk management processes organizations have implemented, including: the data protection compliance frameworks they adhere to, how they deal with regional variances in regulations, and how they identify, manage, and treat risks, including third-party risks.

IT RISK MANAGEMENT AND COMPLIANCE PROGRAM MANAGEMENT

With the knowledge that most organizations either already are or will be adhering to some type of cybersecurity and/or data privacy compliance framework in 2022, we wanted to better understand how compliance programs are managed — both in theory and actuality. For instance, what activities have companies taken to formalize their commitment to managing IT risks? What's the expectation that's placed upon the compliance function around testing of controls related to security and compliance? When do organizations collect evidence to verify that controls are operating effectively? Do they collect evidence just when an external auditor asks them for evidence, or do compliance teams collect evidence as part of a continuous compliance program?

Risk Identification Process

We wanted a full understanding of how organizations are identifying risk today.

When asked "What is your organization's process for identifying risks within your organization?", we saw the following results:

- Sixty-six percent of organizations said that they "meet with and/or survey key leaders on a regular basis".
- Eighteen percent responded that "risk identification is ad-hoc".
- Sixteen percent of companies "use an existing risk template as the starting point for risk identification".

Segment Differences

Company age: Younger companies (in business five years or less) are significantly more likely to meet with and/or survey key leaders on a regular basis in order to identify risk.

Q: Is your organization tracking the following types of risks?

Number of Respondents: 1014

Which Risks are Being Tracked?

In addition to knowing how organizations are dealing with risk, it is interesting to understand what risks are being tracked. The top three risks that are being tracked according to our respondents are: cybersecurity, privacy, and quality (product quality). See the chart to the left for a full breakdown of risks tracked.

It is interesting to find that the majority of surveyed organizations (60%) are currently tracking corporate social responsibility risks. Over half (53%) are also tracking environmental risks and 55% already track labor standards risk. With the rise in discussion around environmental, social, and governance (ESG) issues, organizations will likely need to focus more time on environmental risk in upcoming years. Moving forward, companies can expect to feel the pressure to step up their ESG tracking and reporting from all sides — including regulatory bodies such as the SEC, investors, and customers.

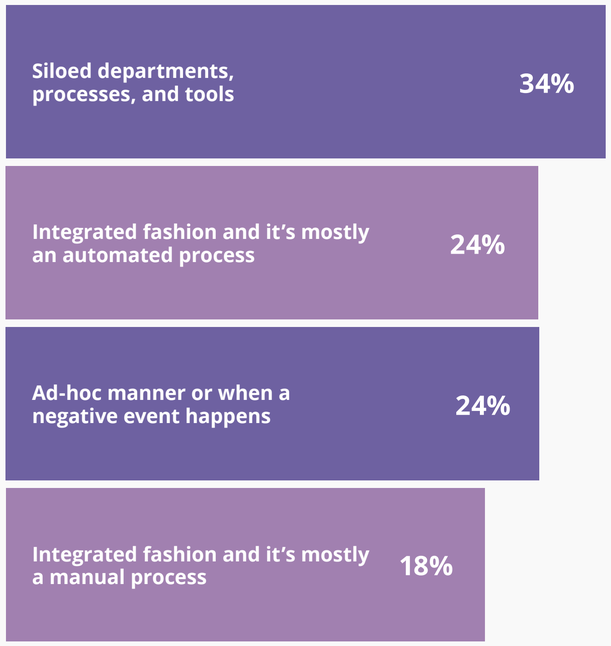
As important as it is to know what risks organizations are currently tracking, reviewing which risks are less likely to be tracked is vital as well. **Close to half of organizations (40%) said they do not need to track geo-political risks.** Human rights and labor standards were also reported as risks that are less likely to be tracked — thirty-five percent of organizations said they don't track human rights, trafficking, and slavery risks, while 33% answered that they don't track risks tied to labor standards.

Despite this response, there are some risks that organizations noted they aren't currently tracking but that they think should be tracked. **Companies identified the following as the top risks that should be tracked:** environmental, geo-political, human rights, employee retention, conduct and ethics, and labor standards. As mentioned above, it makes sense that environmental risk would be top of mind for respondents. It will be interesting to note how these tracked vs. untracked risks change over 2022.

RISK MANAGEMENT APPROACHES

We asked "Which of the following statements is the closest reflection of how your organization manages IT risks?" Here's what we found:

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



Number of Respondents: 1014

It is interesting to note that while organizations seem to be using various tools to manage IT risks, the process is still siloed for most respondents. This could be due to the fact that the various tools do not connect to one another, so respondents cannot get comprehensive visibility into all the steps in their risk management process.

Tactics Taken to Manage Risks

Based on forensic analysis and extensive research, cybersecurity and risk management experts from NIST, ISO, and other organizations have determined a set of key actions organizations can take to ensure data security, confidentiality, and integrity. These best practices include:

1. Using an IT risk management framework to identify and manage IT risks
2. Identifying clear roles and responsibilities and owners for various risks
3. Creating a cross-functional risk/compliance committee that meets regularly to execute risk management tasks
4. Putting together a technology architecture that supports integrated risk management
5. Conducting risk assessments on a cadence
6. Re-assessing risks whenever major changes (e.g. global events, new technology purchased, personnel changes, etc.) occur
7. Maintaining a risk register: A repository of risk information that contains a description of a particular risk, the likelihood of it happening, its potential impact, how it ranks in priority relative to other risks, the planned response, and who owns the risk
8. Conducting internal audits/assessments on controls
9. Aligning risk management and compliance efforts
10. Having ongoing monitoring processes, e.g., establishing Key Risk Indicators, teaching employees about the types of cybersecurity risk issues most likely to occur within the organization

In this survey, we asked respondents "Which of the following best represents the actions you've taken to formalize your commitment to risk management? Select all that apply". We offered these 10 best practices as answer options. We found that **the majority of surveyed organizations have made some commitments to manage their IT risks in a formal, disciplined approach.**

Here's the breakdown of results:

- Seventy percent of respondents use a risk management standard/framework such as ones developed by NIST and ISO.
- Seventy-four percent said they have identified clear roles and responsibilities and owners for various risks.
- Seventy-two percent said they have a cross-functional risk/compliance committee that meets on a regular basis and executes on their risk management plan.
- Seventy-four percent said they have a technology architecture that supports integrated risk management.
- Seventy-five percent said they conduct risk assessments on a regular cadence (e.g. annually or quarterly).
- Seventy-two percent said they conduct risk assessments outside of scheduled risk assessments whenever major changes occur that may change our risk profile and re-prioritize risks.
- Seventy-four percent said they maintain a risk register and they generally keep it up-to-date.
- Seventy-seven percent said they conduct internal audits/assessments on internal controls on a regular basis.
- Seventy-four percent said they have aligned their risk management with their compliance efforts.
- Seventy-two percent said they implemented processes that methodically track governance objectives, risk/ownership/accountability and compliance with policies and risk mitigation controls.
- Seventy-one percent have established KRIs and/or KPIs for any identified high or critical risks.

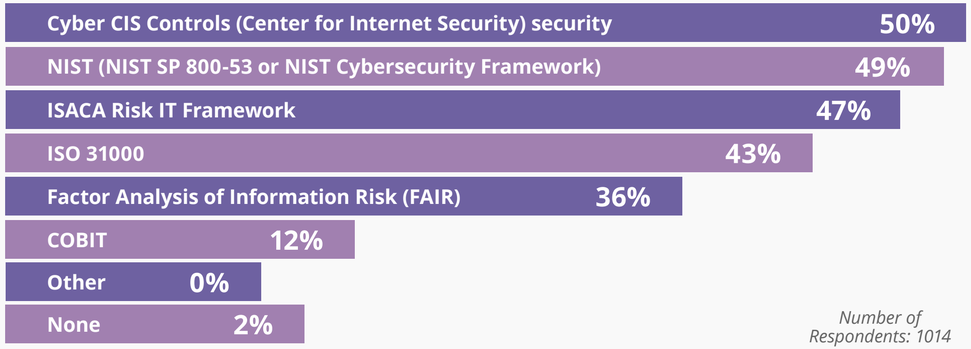
DETAILED FINDINGS AND KEY DIFFERENCES BETWEEN SEGMENTS

IT Risk Management Frameworks

IT risk management frameworks help organizations manage IT risks in a systematic way. In this survey, **70% of all respondents reported that their organization is using an IT risk management framework/standard.** Upon taking a deeper look at the data, we found that UK-based companies had a higher likelihood of leveraging an IT risk management framework/standard such as the ones developed by ISO or NIST (74% vs. 68% of US-based organizations).

What Specific IT Risk Management Frameworks Are Organizations Using?
When asked "Does your organization use any IT risk management framework to identify and manage IT risks? NIST, ISO, CIS, ISACA are just a few organizations that provide IT risk management frameworks.", here is how organizations responded:

Frameworks Organizations Are Using



Number of Respondents: 1014

GOVERNANCE AND ACCOUNTABILITY

Most survey respondents view strong governance as a critical factor in their IT risk management program.

Risk management in the modern enterprise is a team sport. There are multiple individuals in an organization that address cybersecurity and compliance in one way or another. Clearly defining those roles and responsibilities is crucial, because without that clarity, your business can run into one of two big mistakes:

1. You might have multiple roles focused on the same task — this breeds confusion, wastes resources, provokes office turf wars, and hampers efficiency.
2. You might have **no role** focused on certain tasks—which can leave risks unaddressed, until a crisis emerges.

In our survey, on average, 74% percent of all respondents said their organization has identified clear roles and responsibilities and owners for various risks. We found that companies in business for 10-15 years were most likely to have clear roles, responsibilities, and risk owners identified. This isn't surprising seeing that it takes time for an organization to mature their risk management organization — knowing that roles, responsibilities, and owners need to be assigned comes with experience in and a complete understanding of the compliance space.

Seventy-two percent of survey respondents said their organization has a cross-functional risk/compliance committee that meets on a regular basis and executes on their risk management plan.

Risk Assessments

Risk assessments are a crucial part of any IT risk management program or integrated risk management program. Risk assessments help security assurance and compliance teams get clear on where gaps exist so they can focus their efforts on risks that are most significant or most likely to occur within their business. Additionally, many security compliance frameworks require risk assessments to be an ongoing part of an organization's infosec management process.

In this survey, we found that:

- **Seventy-five percent of all survey respondents conduct risk assessments on a regular basis** (e.g. annually or quarterly) while 25% don't follow this practice.
- Seventy-two percent of survey respondents' organizations conduct risk assessments outside of scheduled risk assessments whenever major changes occur; 28% don't follow this practice.

Usage of Risk Register

As defined by the Office of Management and Budget, a risk register is a "repository of risk information" that contains a description of a particular risk, the likelihood of it happening, its potential impact from a cost standpoint, how it ranks overall in priority relevant to all other risks, the response, and who owns the risk.

Risk registers are useful information gathering constructs: they help an organization effectively integrate cybersecurity risk management into an overall enterprise risk management program. A risk register can be integrated into any risk management methodology your organization uses.

74%

of organizations use a risk register

74%

of organizations have identified owners for various risks

ALIGNING RISK MANAGEMENT TO COMPLIANCE EFFORT

For a sizable organization that has hundreds of IT systems and adheres to multiple information security and data privacy frameworks, it's easy to become "over-controlled". When organizations don't take the time to map controls back to the risks and the compliance requirements they address, it's easy to create duplicative controls unintentionally.

In this study, **74% of all respondents said that they have aligned their risk management with their compliance efforts.**

Internal Audits and Assessments

When an organization's technology environment changes fast, controls set up just a few months ago may be obsolete today. To ensure that internal controls built to mitigate key risks and satisfy regulatory requirements are actually working to maintain an acceptable risk level, organizations need to audit their internal controls on a regular basis. For instance, an IT audit might include a review of your company's maintenance of IT assets, its security patch management, or its procedures to evaluate the security risks posed by new technology.

In our survey, **77% of all respondents said they conduct internal audits and assessments on internal controls on a regular basis.**

Continuous Monitoring

Risks and threat vectors can change in a matter of minutes. Security-conscious organizations know how important it is to have a continuous monitoring system in place. Monitoring isn't just about setting up dashboards with key indicators of risks (e.g., number of critical business systems that include strong authentication protections). Monitoring can include employee education and conducting risk response exercises to train employees in recognizing, reporting, and responding to cybersecurity incidents

In this survey, we found that **72% of all respondents have implemented processes to methodically track governance objectives, risk/ownership/ accountability, and compliance with policies and risk mitigation controls.** However, we found that the methods of monitoring vary from quite rudimentary (e.g., using only external audits to verify compliance posture) to fairly sophisticated (e.g., using internal audits, external audits, and monitoring software).

Key Risk Indicators

Seventy-one percent of all respondents have established Key Risk Indicators for identified "high" or "critical" risks. Companies who have been in business for five years or longer are more likely to have established Key Risk Indicators than organizations who are younger (less than 5 years in business).

77% conduct internal audits and assessments on internal controls on a regular basis

72% have implemented processes to methodically track governance objectives, risk/ownership/ accountability, and compliance with policies and risk mitigation controls

ORGANIZATIONS' PERCEPTIONS ON HOW WELL THEY THINK THEY'RE MANAGING RISKS

Standard-setting bodies ranging from NIST to ISO have recommended that organizations take a risk-based approach to meeting their information security and compliance objectives. This means going through these steps in sequence (and repeating the process any time changes occur):

1. Identify and assess risks
2. Identify existing controls
3. Validate controls against standard controls published in compliance frameworks
4. Align controls with risks
5. Test controls to ensure effectiveness
6. Flag issues and exceptions; Review and remediate
7. Once controls have been deployed, assess their effectiveness on a cadence
8. Capture and track deficiencies and remediate

Even though the majority of organizations have taken measures to formalize their commitment to risk management, we found that some respondents still **struggle with some of the key steps outlined above.**

When we asked "In your opinion, how well is your company doing in performing each of the following risk management actions?", we found that more than a quarter of organizations said the way they're performing risk management tasks **does not meet their company's objective.** Organizations tend to struggle with the following tasks:

- Assessing controls' effectiveness (25% of respondents selected "does not meet our company's objective")
- Capture, track, and report deficiencies (27% of respondents selected "does not meet our company's objective")
- Align controls with risks (28% of respondents selected "does not meet our company's objective")
- Identify controls (31% of respondents selected "does not meet our company's objectives")
- Validate controls against standard controls (in compliance frameworks) (32% of respondents selected "does not meet our company's objectives")
- Monitor and automate controls testing (32% of respondents selected "does not meet our company's objectives")
- Flag exceptions, review and remediate (36% of respondents selected "does not meet our company's objectives")

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

	Does not meet our company's objective	Meets our company's objective
Identify & assess risks	8%	92%
Assess controls effectiveness	25%	75%
Capture, track & report deficiencies	27%	73%
Align controls with risks	28%	72%
Identify controls	31%	69%
Validate controls against standard controls (in compliance frameworks)	32%	68%
Monitor & automate controls testing	32%	68%
Flag exceptions, review & remediate	36%	64%

Number of Respondents: 1014

DO ORGANIZATIONS INCLUDE THEIR THIRD PARTIES IN THEIR RISK MANAGEMENT PROGRAM?

As a reminder, **57% of organizations said that they experienced a third-party data or privacy breach** that affected their organization's records or data in 2021. Considering this, we wanted to learn more about how respondents are assessing third-party risk.

When asked "What prompts you to assess your third-parties/vendors/suppliers?", respondents replied in the following way:

- Fifty-five percent are required to assess third-parties in order to adhere to specific regulatory, industry, or data privacy requirements.
- Forty-five percent said they must ensure that third parties do not introduce risks into business that could negatively impact them.
- Just 1% of companies reported that they do not assess third-parties from a risk standpoint.

As a follow up to the previous question, we asked, "Are you tracking security and privacy risks in your third-party providers/vendors/suppliers?".

The large majority of respondents (74%) told us that they are indeed tracking third-party risks. Twenty-five percent of organizations said that they don't currently track third-party risk, but plan to in 2022. It's interesting to note that a quarter of all respondents did not track third-party risk in 2021 — especially when more than half of all surveyed respondents experienced a third-party data or privacy breach in 2021.

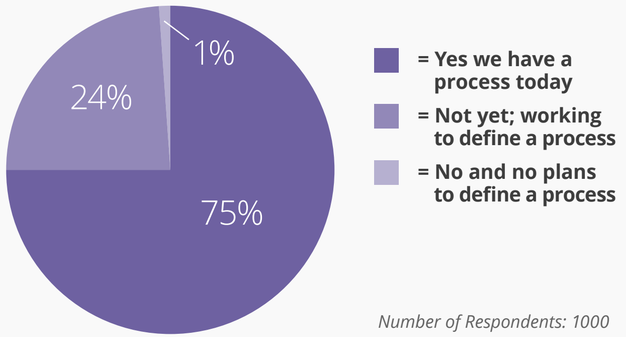
In this survey, we also asked respondents whether they have a process in place to identify, treat, and monitor third-party and/or supply chain risks.

Most organizations (75%) also reported that they currently have a process in place to identify, treat, and monitor third-party and/or supply chain risks. In comparison, 24% of respondents said that they don't have a process yet, but are working to develop one. Only 1% of organizations answered that they don't have a process and have no plans to create one.

Segment Differences

- US-based companies are more likely to have a third-party/supply chain risk monitoring process in place — 77% as opposed to 71% of their UK-based counterparts.
- Organizations who view compliance as a function that enforces regulations also reported higher numbers on this topic (84%). Vs. the following:
  - 68%: organizations who view compliance as a function that helps mitigate risks; but risk and compliance activities are conducted separately
  - 75%: organizations who view risk and compliance activities as tied together and aligned

Q: Do you have a process in place to identify, treat and monitor third party and/or supply chain risks?



Number of Respondents: 1000

hyperproof

CHAPTER 4

Challenges with Risk Management Processes

04 | Challenges with Risk Management Processes

The previous chapter of this report highlighted the importance of risk management to our respondents. It also shined a light on the processes organizations utilize to manage risks and how organizations perceive their own risk management practices. In this chapter, we will delve into the pain points companies encounter when it comes to managing IT risks.

STRUGGLES WITH VENDOR RISK MANAGEMENT

Throughout this report, we've discussed third-party risk and its growing importance to compliance programs in recent years. We now know that most organizations (75%) currently have a process in place to identify, treat, and monitor third-party and/or supply chain risks. But how effective is that process? With this question in mind, we wanted to understand the potential struggles of third-party risk management.

We asked: "What are your top challenges or struggles when managing the risk associated with third-parties and/or suppliers?". Here are some notes of interest based on responses:

- The top challenge noted by our respondents is that **collecting risk information on third parties is manual and time-consuming.** Thirty-three percent of organizations called this out as their biggest struggle when managing third-party risk.
- In our 2020 survey, this response came in as the second biggest challenge for companies. In 2022, organizations will face increasing compliance requirements to get a better handle on their vendors. They'll need to find tools that help them gather third-party risk information more efficiently. Compliance operations platforms like Hyperproof's will help in this regard.
- The other top struggles reported by organizations were: 1. vendor assessments and vendor remediation taking place in different tools which creates inefficiencies (32%), and 2. managing remediation projects is manual and time-consuming (31%).
- On the other hand, the lowest reported challenge was organizations feeling that they can't trust that third parties are doing what they say they're doing. Eighteen percent of respondents said that this is a top struggle in regards to third-party risk.

TAKE CONTROL OF YOUR THIRD-PARTY RISK MANAGEMENT NOW

This is a full breakdown of respondents' top third-party risk management challenges :

Q: What are your top challenges or struggles when managing the risk associated with third-parties and/or suppliers?

Number of Respondents: 1000

WHAT IS TAKING UP RESPONDENTS' TIME?

As noted in the section above, companies struggle with how time consuming third-party risk management is — so we wanted to dig into the specific tasks that were causing issues with third-party risk management. We were also interested in what other compliance and risk management tasks are taking up time that could be better spent elsewhere.

Third-party and/or Supplier Risks

To get a full picture of the types of tasks that organizations think are taking up too much employee time we also asked: "When it comes to managing third party and/or supplier risks, what tasks do you find to be tedious/take way longer than you'd like?"

Forty percent of respondents expressed frustration with putting together reports to communicate what they're doing from a vendor risk management perspective to their leadership team. Thirty-nine percent of companies said that collecting risk information from vendors is tedious or takes too much time.

Here are other tasks that respondents reported being tedious/ or taking longer than they'd like:

- Understanding which vendors they need to worry about/investigate further from a risk perspective (36%)
- Evaluating reports provided by third-parties (35%)
- Tracking statuses of vendor management tasks across the vendor lifecycle (35%)
- Going back and forth with vendors to clarify questions from questionnaire/assessments (34%)
- Identifying and classifying vendors according to risk (34%)
- Maintaining an up-to-date list of all vendors (33%)

Segment Differences

Time in business: Organizations in business for 10-15 years were significantly more likely to report having issues with understanding which vendors they need to worry about/investigate further from a risk perspective. This might be due to the fact that more tenured companies are leveraging a greater number of vendors than younger companies.

STRUGGLES WITH MANAGING RISKS FROM ORGANIZATION'S INTERNAL ENVIRONMENT

When asked "when it comes to managing security and data privacy risks arising from your internal environment, what tasks do you find to be tedious/ takes way longer than you'd like?", organizations reported the following:

- Forty-eight percent — the largest group — reported that having to switch back and forth between multiple systems through the risk management process is a task they think takes too long.
- Forty-three percent have trouble finding risk-related information when they need it (e.g., multiple spreadsheets containing risk assessment results).
- Forty-three percent of respondents find data entry too time consuming.
- Forty-three percent of organizations also believe they spend too much time putting together reports for executives to communicate the work being done from a risk perspective.
- Forty percent of all respondents said they find collecting the necessary data to test controls tedious and/or too time consuming.
- Thirty-seven percent of companies surveyed find being able to get an ongoing, continuous view of risks and compliance status tedious and/or too time consuming.
- Thirty-five percent of respondents reported that tracking remediation progress takes way longer than they'd like.

Unfortunately, the top two tasks reported on this list are all too familiar to compliance and security professionals. Many people in this industry still work from outdated and isolated tools (spreadsheets, Google docs, etc.) that make it difficult for employees to easily collaborate and gather evidence for risk management.

Segment Differences

How organizations view the purpose of their compliance function: Organizations who view risk and compliance as tied together and aligned are more likely to struggle with having to switch back and forth between multiple systems through the risk management process. This challenge is likely top of mind for this segment because companies that consciously try to align their risk and compliance functions together are more cognizant of the reality that they're using disparate systems.

CHALLENGES AROUND PREPARING FOR EXTERNAL AUDITS

It is also interesting to note what tasks are taking up too much time when it comes to audits. When asked "when it comes to preparing for and executing audits, what tasks do you find to be tedious/takes way longer than you'd like?", **almost half of respondents (42%)** said that testing and validating evidence before it's sent to an external auditor takes too much time. Thirty-nine percent of organizations indicated that responding to auditor requests and follow-up requests is tedious/takes more time than they'd like.

Here are other tasks that respondents reported being tedious/take longer than they'd like:

- Providing evidence/documentation to the external auditor (38%)
- Filing, storing, and managing compliance documentation (37%)
- Training others to assist, complete tasks or do administrative activities (37%)
- Communicating audit requirements to stakeholders in their organization (36%)
- Locating documents and other information needed for the audit (35%)
- Communicating with the auditor (31%)

IS TIME BEING SPENT ON WORTHWHILE TASKS?

It's clear that respondents view a plethora of tasks as being tedious/taking more time than they'd like. To better understand how much time organizations actually think employees are spending on these tasks we asked, "Think about the people who are responsible/accountable for risk and compliance management in your company. What portion of this team's time is spent on repetitive/administrative tasks that aren't a good use of their time?".

Most respondents (59% of total) said that their compliance team is spending at least forty percent of their time on repetitive/administrative tasks that aren't a good use of their time.

This response indicates that for many organizations today, preparing for audits still involves too many manual steps. In the future, companies who hope to fix this will need to look for solutions that will support their employees on this front, such as automating various tasks and parts of the evidence collection. Respondents to this survey seem to be aligned with this view — **85% of organizations noted that they have plans to evaluate/purchase tools to streamline and automate their risk management and compliance processes in 2022.**

59%

said their compliance team is spending at least 40% of their time on repetitive/administrative tasks

85%

plan to evaluate/purchase tools to streamline and automate risk management and compliance in 2022

hyperproof

CHAPTER 5

IT Security Assurance and Compliance Practices

05 | IT Security Assurance and Compliance Practices

Now that many organizations have lived through data breaches — including those caused by their IT system vendors — merely claiming that you're secure (and compliant) isn't enough for stakeholders and customers. Businesses must continually prove that their security controls are functioning properly and that contractual and regulatory requirements are being met.

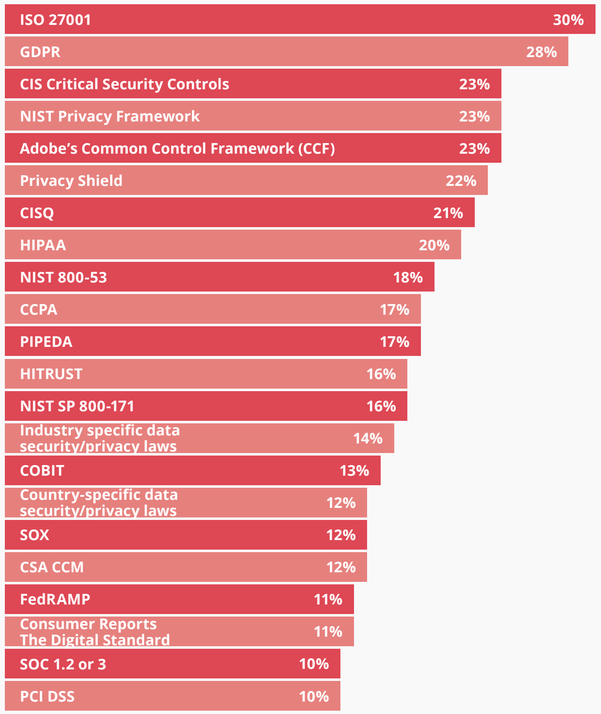
According to NIST SP 800-53 (Security and Privacy Controls for Information Systems and Organizations), security assurance is "the measure of confidence that the security functionality is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system". Assurance comes from the demonstrated ability to meet security objectives, evidenced by the results of control tests, assessments and/or audits. In this survey, we sought to understand how organizations are managing their security assurance and IT compliance efforts at a tactical level.

USE OF FRAMEWORK(S)

While some compliance frameworks are very industry-specific, others are helpful general-purpose data protection frameworks that can aid organizations in mitigating the risk of security breaches and privacy violations. With this in mind, we were interested to understand which frameworks companies are already adhering to or are planning to complete in 2022. We asked, "Which cybersecurity and/or data privacy compliance frameworks does your organization adhere to or plan to adhere to in the next 12 months?"

While respondents were fairly split on this topic (see results below), two frameworks rose to the top. **Thirty percent of respondents reported that they'd be adhering to the information security standard ISO 27001.** Just behind ISO 27001 was GDPR (28%), the regulatory standard required for any organization that does business in the European Union (EU) or touches the data of EU citizens. Not surprisingly, we found that significantly more UK-based organizations plan to adhere to GDPR than US-based companies in 2022 (35% of UK companies vs. 25% of US-based companies).

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



Number of Respondents: 1014

APPROACHES TO ADDRESSING REGIONAL VARIANCES IN REGULATIONS

No matter where a company is physically based, its customers are likely spread out across multiple regions. The United States does not have a federal data privacy law such as the EU's GDPR. Thus, most companies are likely to encounter regional state-level variances in data privacy regulations. These variances can be hard to track for organizations that have a footprint in many states. Because of this we asked, "How does your organization deal with regional variances in data security and privacy regulations?"

At a high level, the results would indicate that most respondents are looking at the full picture of data security and privacy regulations, instead of in geographic silos.

More than half of respondents (57%) said that they utilize a common controls framework that aggregates and rationalizes compliance requirements from different laws and regulations. Thirty-seven percent of organizations reported that they identify the most stringent and comprehensive law that must be complied with and then structure their compliance and risk management activities to meet that law. Only 5% of respondents told us that they deal with new data privacy and security regulations one at a time, as they are passed.

HOW DO ORGANIZATIONS ENSURE THAT THEIR CONTROLS ARE OPERATING EFFECTIVELY?

First we asked: "What is the expectation that's placed upon the compliance function around testing of controls related to security and compliance?"

- **Fifty percent of organizations said that they're expected to test all controls.**
- Forty-six percent of respondents answered that they're expected to test most critical controls.
- Only four percent of organizations told us that they're expected to test only controls needed for the next audit.

Segment Differences

Company age: Younger companies (in business for five years or less) were significantly more likely to report having to test all controls vs. companies who have been in business for five to ten years and those who have been in business for ten to fifteen years (58% vs. 47% and 48%).

How organizations view the purpose of their compliance function: Those who view compliance as the function that enforces regulations also reported significantly higher in regards to having to test all controls as opposed to other groups in this segment.

We also asked respondents: "How would you describe the actual testing of controls within your organization around security and compliance? Select the statement that most accurately describes your approach." These responses only varied slightly from the previous question:

- 56%: We test all controls
- 39%: We test only the most critical controls according to risk
- 4%: We test only those controls needed for the next audit

When looked at in conjunction, the responses to the previous two questions suggest that the majority of companies are both expected to and actually do proactively test their controls, as opposed to only doing the minimum needed for their next audit.

Responses we got about evidence collection supported a move away from the ad-hoc approach to compliance as well. We asked: "Choose the statement that most accurately reflects how your organization approaches evidence collection (to verify that controls are operating effectively)". Here's how respondents answered:

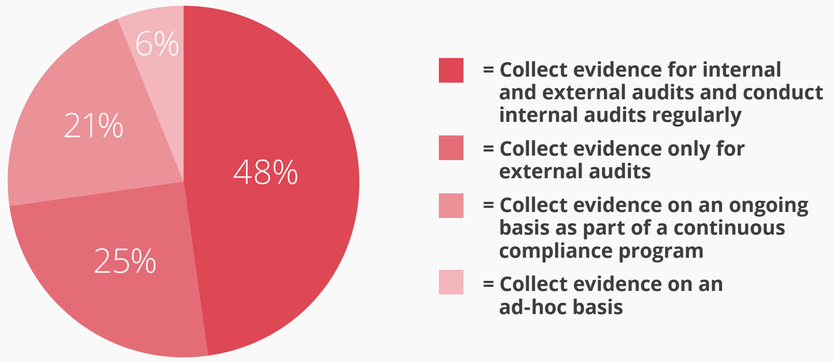
- **Forty-eight percent of organizations said that they collect evidence for internal and external audits and conduct internal audits regularly.**
- Twenty-five percent reported that they collect evidence only for external audits.
- Twenty-one percent responded that they collect evidence on an ongoing basis as part of a continuous compliance program.
- **Only six percent said that they collect evidence on an ad-hoc basis.**

Segment Differences

Company age: Older companies (ten years in business or more) are more likely than younger companies to collect evidence for internal and external audits and conduct internal audits regularly.

How organizations view the purpose of their compliance function: Unsurprisingly, organizations who view risk and compliance activities as tied together and aligned are more likely to collect evidence on an ongoing basis as part of a continuous compliance program.

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



Number of Respondents: 1014

APPROACHES TO MONITORING VARY SIGNIFICANTLY

Monitoring is an important part of security assurance: a properly designed monitoring program should trigger early warning indicators that something is happening in the business that could cause a security incident and/or a compliance failure. Organizations may deploy one or multiple approaches to monitoring controls meant to mitigate IT risks, including formal external audits, internal audits, and through software applications.

To better understand how organizations are gauging the effectiveness of their controls, we asked: "Which of the following best characterizes your organization's approach to monitoring the efficacy of internal controls designed to mitigate IT risks?" Here is a breakdown of the responses:

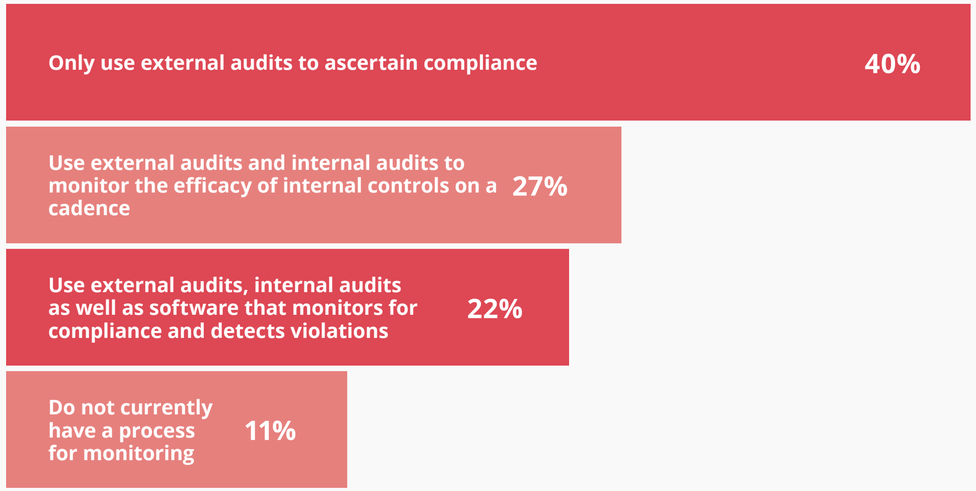
- **Forty percent, the biggest cohort of respondents, reported they only use external audits to ascertain compliance.** In other words, these organizations' primary focus is on proving compliance rather than ensuring a continuously secure environment.
    - This response is a bit of a surprise because it contradicts the previous finding that 48% of organizations collect evidence for internal and external audits and conduct internal audits regularly. A likely reason for this is that respondents understand how involved monitoring is and all of the pieces that go into monitoring to make it effective.
- Twenty-seven percent of respondents said they use external audits and internal audits to monitor the efficacy of internal controls on a cadence.
- Twenty-two percent of respondents said they use external audits, internal audits as well as software that monitors for compliance and detects violations.
- Eleven percent of respondents said they do not currently have a process for monitoring.

Segment Differences

Time in business: Established companies, in business for 10+ years, reported that they are more likely than younger companies to use external audits, internal audits as well as software that monitors for compliance and detects violations.

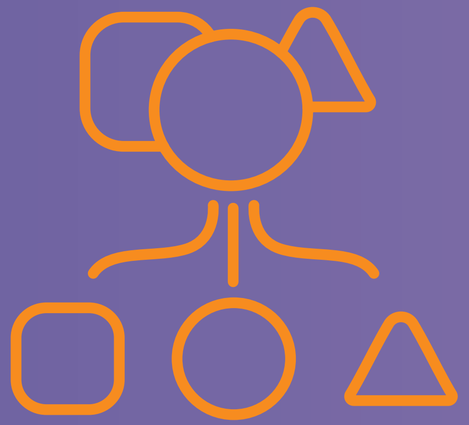
How organizations view the purpose of their compliance function: Organizations whose risk and compliance activities are aligned are significantly more likely to use external audits and internal audits on a regular cadence

Q: Which of the following best characterizes your organization's approach to monitoring the efficacy of internal controls?



Number of Respondents: 1014

hyperproof



CHAPTER 6

Tools For Managing Risks and Compliance Processes

06 | Tools For Managing Risks and Compliance Processes

As compliance work continues to grow in importance and complexity, the need for tools to properly manage compliance and risk operations has become increasingly apparent. Each year brings new, more sophisticated tools to this space, and yet, in our 2020 survey we found that almost half (48%) of all respondents were still using spreadsheets to document and track risks. Further, the typical respondents said their compliance function still spends about 40% of their time at work on tasks that are administrative in nature, tasks that aren't a good use of their time. We were interested to see if and how organizations are using different tools and whether there have been major changes year over year (YoY).

WHAT TOOLS ARE COMPANIES USING?

Tracking Internal Risk

When asked: "What tools are you using to document and track your risks?," **57% (the largest cohort) of respondents said that they utilize the risk management module in a cloud-based GRC software.** In contrast, spreadsheets fell to the bottom of the list with 32% of organizations noting that they use this tool. Here is a full breakdown of YoY results:

Q: What tools are you using to document and track your risks?

	Total 2020	Total 2021
All Respondents	1029	1014
The risk management module in a cloud-based GRC software (also known as integrated risk management solutions)	41%	57%
The risk management module in an on-prem GRC software	30%	48%
Standalone risk management software	34%	42%
Custom-built software	38%	38%
Spreadsheets	48%	32%
We don't have a tool	4%	1%

Number of Respondents: 1014

The use of dedicated GRC tools to manage IT risks and compliance programs has increased YoY. For instance, 57% of respondents this year said they use the risk module in a cloud-based GRC software to document and track their risks, compared to 41% last year. Respondents also reported a higher usage of the risk management module in an on-prem GRC software — 48% in 2021 vs. 30% in 2020. The use of standalone risk management software increased as well, with 42% of organizations reporting utilizing this kind of software in 2021 compared with 34% in 2020. Spreadsheets appear to be decreasing in popularity — 32% of respondents said they use spreadsheets in 2021 vs. 48% in 2020.

Segment Differences

How organizations view the purpose of their compliance function: Companies who view risk and compliance as tied together and aligned reported a higher use of the risk management module in a cloud-based GRC software compared to companies who view the compliance function as the function that enforces laws and standards and companies who conduct risk and compliance activities separately. Here is the breakdown of responses by group:

- Sixty-six percent of companies who view risk and compliance as tied together and aligned reported using the risk management module in a cloud-based GRC software.
- Fifty-five percent of companies who view the compliance function as the function that enforces laws and standards reported using the risk management module in a cloud-based GRC software.
- Fifty-six percent of companies who conduct risk and compliance activities separately reported using the risk management module in a cloud-based GRC software.

TRACKING THIRD-PARTY RISK

We've put a lot of focus on **third-party risk** in this survey, and the answers from respondents indicate that they see it as an increasingly important topic as well. Considering this, we were curious about what tools are being used to identify and manage third-party risk.

The large majority of organizations **(69%) told us that they use a dedicated IT vendor risk management (VRM) solution** to identify and manage third-party risk. Here is a look at the rest of the responses:

- Forty-four percent of respondents use forms/questionnaires made in Microsoft Office/Google Suite
- Thirty-eight percent of respondents use a ticketing/task management system
- Thirty-one percent of respondents use spreadsheets
- Thirty percent of respondents use other features within a GRC software solution
- Just 1% of respondents said they don't have a tool

The use of a dedicated IT VRM solution was the top answer to this question in 2020 as well. However, the percentage of respondents who utilize this type of solution went up significantly — 69% in 2021 vs. 58% in 2020. The number of respondents who use a ticketing/task management system increased YoY as well, from 28% in 2020 to 38% in 2021. The use of spreadsheets, on the other hand, fell from 44% in 2020 to 31% in 2021.

Segment Differences

US vs. UK: UK-based companies reported a higher likelihood of using spreadsheets to manage and identify third-party risk compared to their US based counterparts. Thirty-five percent of UK-based companies used spreadsheets vs. 29% of US-based companies.

MANAGING IT COMPLIANCE EFFORTS

When asked "what tools are you using to manage your IT compliance effort?", more than half of respondents **(55%) said that they use the compliance module in a cloud-based GRC software.** An equal proportion of organizations **(55%) reported they utilize software that's purpose-built for managing IT compliance operations.** These are the other tools companies are using:

- Forty-two percent of respondents said they use spreadsheets, Word docs, and/or file storage systems.
- Thirty-nine percent of organizations responded that the compliance module in an on-prem GRC software helps them to manage their IT compliance effort.
- Thirty percent reported utilizing a custom-built software.
- Only 1% of respondents said that they don't have a tool.

This year, we saw a significant increase in organizations using tools built specifically for managing IT compliance processes. In 2020, just 20% of respondents reported using the compliance module in a cloud-based GRC software to manage their IT compliance effort; 45% of respondents reported using software purpose built for managing IT compliance operations.

INTEGRATIONS BETWEEN SYSTEMS TO OPTIMIZE RISK AND COMPLIANCE MANAGEMENT PROCESSES

As a reminder, **48% of respondents expressed that they find it tedious or time consuming to switch back and forth between multiple systems** throughout the risk management process. Keeping this number in mind, along with the fact that the majority of respondents already use some type of compliance and risk software, we get the picture that the **GRC softwares being used aren't working or aren't as effective as they could be.** To get more value from GRC tools, these tools need to be properly integrated with the existing productivity apps organizations are already using.

To better understand which integrations would be most beneficial to organizations, we asked: "Which of the following tools would you like your risk management and compliance management solution to work with/integrate with?"

We found that although many organizations have GRC software, they still manage a portion of compliance programs in numerous other places. For instance, **45% of respondents store some compliance documents in cloud-based file storage systems** such as Box, Google Drive, SharePoint and OneDrive.

Email is still a popular tool for coordinating compliance projects. Another sizable chunk of organizations' compliance information resides in cloud infrastructure platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud (GCP).

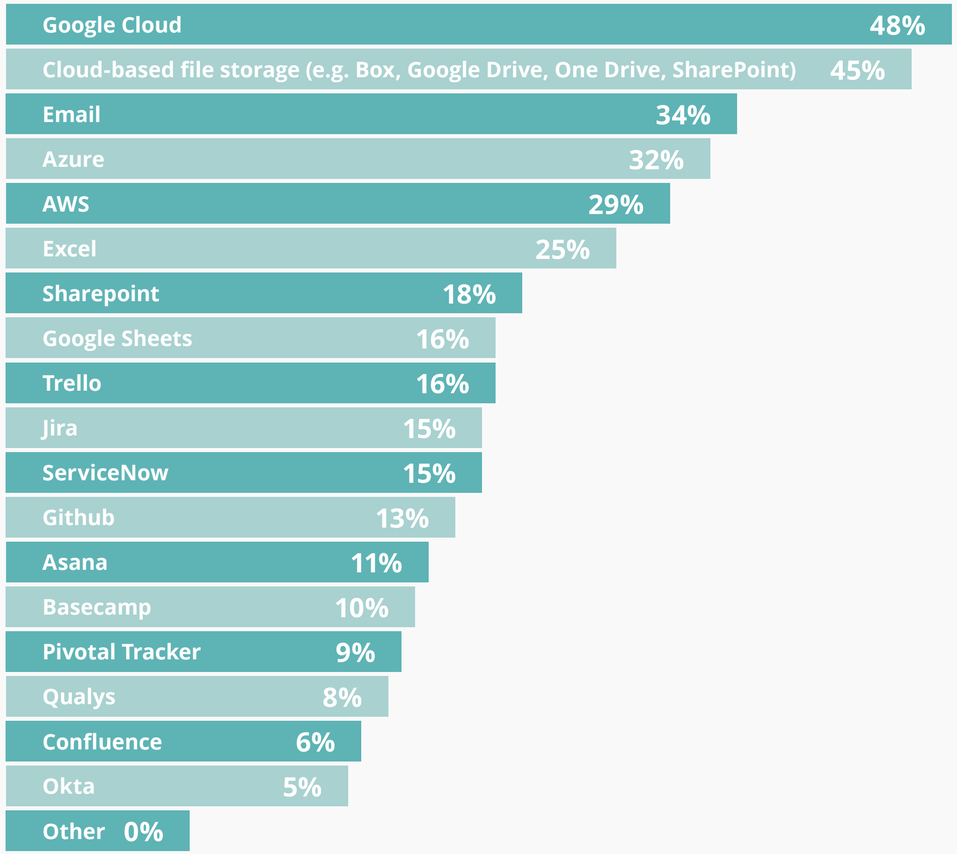
If GRC tools aren't easily integrated into an organization's broader tech stack to allow people to pull in compliance data automatically and work where they prefer, their value is limited. In fact, over 85% of all respondents are still planning to evaluate new tools next year in 2022 with the goal of **streamlining and automating their compliance processes.**

85%

respondents are planning to evaluate new tools in 2022 with the goal of streamlining and automating their compliance processes

Here's exactly how companies responded:

Q: Which of the following tools would you like your risk management and compliance management solution to work with/integrate with?



Number of Respondents: 1014

Segment Differences

US vs. UK: The most significant discrepancy between US and UK-based companies was about the workflow platform Service Now. UK-based companies expressed more interest in having their risk management and compliance management solution integrated with ServiceNow.

Time in business: Companies in business for 10+ years expressed significantly more interest than their younger counterparts in integrations for the following tools: Cloud-based file storage, Azure, Service Now, and Github.

hyperproof

APPENDIX

Survey Methodology

A | Survey Methodology

The 2022 IT Risk Management and Compliance Survey gathered 1,014 responses during November and December 2021. All organizations come from the Technology industry.

Organization Size

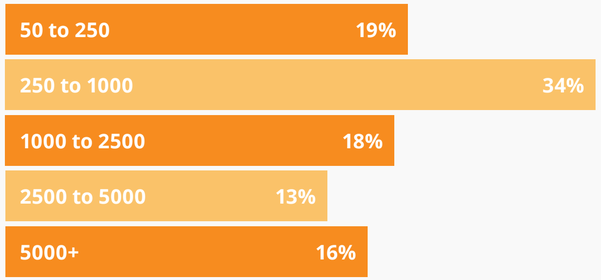
We defined organizational sizes for comparison as follows:

- **Small** (50 to less than 250 employees),
- **Midsize** (250 to less than 1,000 employees),
- **Large** (1,000 to less than 2,500 employees),
- **Small-Enterprise** (2,500 to less than 5,000) and,
- **Large-Enterprise** (5,000+).

We deliberately excluded organizations with less than 50 employees because we felt that respondents from the smallest organizations would not be as knowledgeable about IT risk management as respondents from larger organizations, simply because organizations generally wait to invest in IT risk management until they've become viable businesses.

19% of all respondents are from Small organizations, 34% of respondents are from Midsize organizations, 18% are from Large organizations, 13% of respondents are from Small-Enterprise organizations, and 16% of respondents are from Large-Enterprise organizations. The mean (or average organization) in the survey has 1,968 employees.

Q: How many employees are employed by your organization worldwide?



Number of Respondents: 1014

Location

Respondents came from organizations that have US-based headquarters and UK-based headquarters. 700 respondents come from companies with headquarters in the US. 314 respondents come from companies with headquarters in the UK. Organizations with single and multiple locations were included.

Tenure Of Businesses

- 21% of respondents work for companies that have been around for 5 years or less.
- 44% of respondents work for companies that have been around between 5 to less than ten years (38% of total).
- 22% of respondents work for firms that are between 10 and 15 years old.
- 12% of respondents work for firms that have been around for 15 years or longer.

Revenue

- 21% of respondents work for companies that generated $10 million or less in 2021 annual revenue.
- 26% of respondents work for companies that generated between $10 million and $50 million in 2021 annual revenue.
- 14% of respondents work for companies that generated between $50 million and $100 million in 2021 annual revenue.
- 15% of respondents work for companies that generated between $100 million and $500 million in 2021 annual revenue.
- 25% of respondents work for companies that generated $500 million or more in 2021 annual revenue.

Department

- 14% of respondents are in the C-suite.
- 64% of respondents are in Information Technology (IT).
- 15% of respondents are in SecurityCompliance.
- 5% of respondents are in Operations.
- 1% of respondents are in Engineering.
- Other departments including Legal and Finance — were not selected by the respondents.

Job Function

We asked respondents to tell us their primary job function (they could select up to 3 job functions).

- 62% of all respondents selected Information Technology as their primary Job Function.
- 51% of all respondents selected IT audit/IT compliance as their primary job function.
- 48% of all respondents selected Information Security as their primary job function.
- 24% of all respondents selected Risk Management as their primary job function.
- 23% of all respondents selected Security Assurance/ Compliance as their primary job function.
- 15% of all respondents selected Management as their primary job function.
- 7% of all respondents selected Human Resource Operations and/or Management as their primary job function

We have a few additional respondents in functions such as Ethics, Policy and Compliance and Governmental affairs.

Job Level

The vast majority of respondents are Manager level or above.

Q: What's your primary job function?

Number of Respondents: 1014

Decision-Making Regarding Data Security and Data Privacy Compliance

Eighty-six percent of all respondents said they are directly involved in decisions regarding cybersecurity and data privacy risks for their organizations. Twelve percent said they're knowledgeable enough to understand the requirements and needs regarding cybersecurity and data privacy for their organization. Just 2% said they do not make decisions but are involved in maintaining IT security and data privacy for their company.

Roles In Security, Privacy, and Compliance

Eighty percent of respondents said they are the sole decision-maker in decisions regarding data security and data privacy compliance for their organization. Fifteen percent said they are one of the decision-makers within their organization; 4% 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.

hyperproof

ABOUT HYPERPROOF

Hyperproof is a software company focused on creating revolutionary software that brings trust to life. To date, Hyperproof has delivered an innovative SaaS compliance operations platform that empower compliance, risk and security teams to stay on top of all compliance work and manage organizational risks (including vendor risks) on a continuous basis. Hyperproof has disrupted the GRC space by tackling a pressing problem ignored by others: helping compliance pros gain control over and effectively manage their ever-growing workload. Hyperproof is used by market leaders in security tech, enterprise software, fintech, healthcare tech, and data communications, including Sophos, ForgeRock, 3M, Outreach, and Motorola Solutions. To learn more about Hyperproof, visit hyperproof.io or follow Hyperproof on LinkedIn.