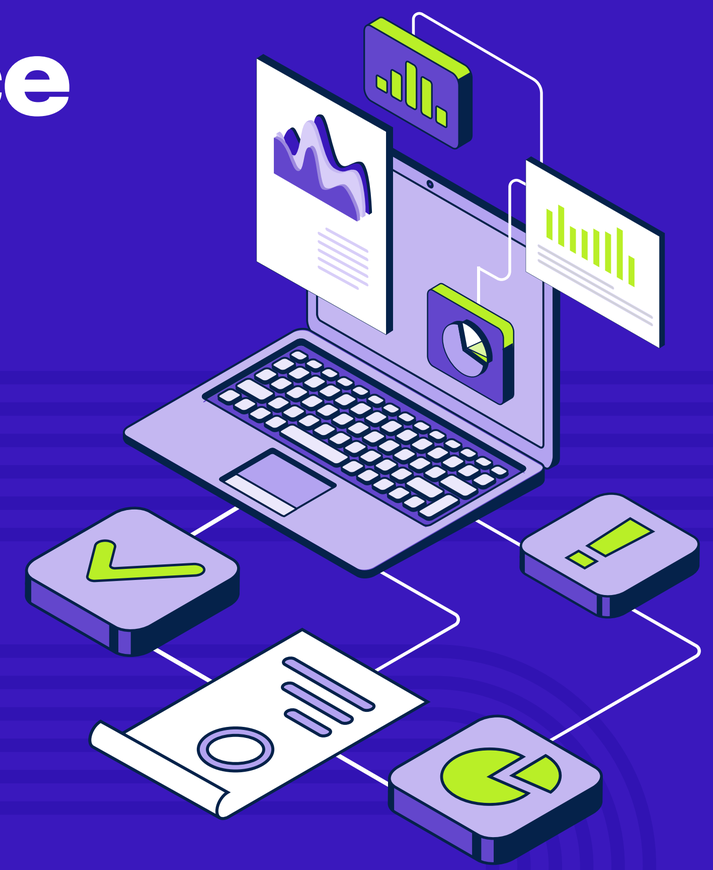
SUMMER 2025

2025 IT Risk and Compliance Benchmark Report

Beyond the Benchmark: How Does Our Report Compare?



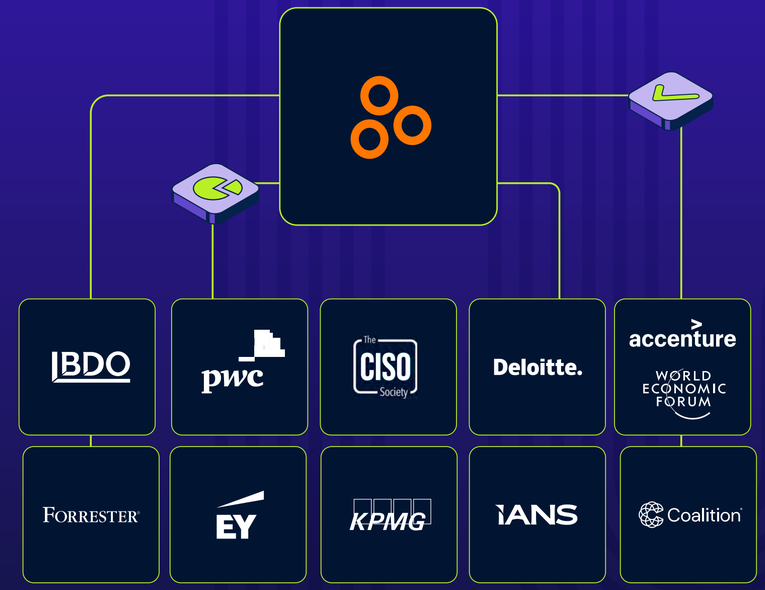
A PUBLICATION BY hyperproof

Foreword

What do Chief Information Security Officers (CISOs) think about? For most, it's not the latest zero-day vulnerability or sophisticated nation-state attack. Instead, it's the gnawing uncertainty about whether their governance, risk, and compliance programs will withstand the next audit, regulatory inspection, or board inquiry.

Every year, we release our annual benchmark report, which takes a deep dive into market trends in the risk and compliance landscape to help you prepare for the year ahead. **This year, we expanded our efforts even further by asking a critical question: how does our report compare to others released around the same time?**

We reviewed 10 reports to see how our data compared and contrasted to give you even more insights into industry trends. We selected these reports based on the credibility of the organizations that produced each report, the time frame of each report, and the uniquely different perspectives created by surveying similar but different audiences who participated in *The 2025 IT Risk and Compliance Benchmark Report*. The exclusive research that follows is limited to only those statistics and findings where we saw a strong relationship between our data and the external report's findings.



> How does our report compare to others released around the same time?

In the course of creating this report, we looked at the following for insights related to our own findings:

FORRESTER®

2025 Budget Planning Guide: Security And Risk

Includes increasing cybersecurity budgets, driven by regulatory pressures and customer expectations

REPORT →

pwc

The 2024 Global Digital Trust Insights Report

Shows rising breach costs, with cloud security being a major concern, yet many organizations lack adequate risk management plans

REPORT →

BDO

The 2024 BDO Board Survey

Shows how cybersecurity remains a significant concern, prompting boards to shift responsibility from IT to a company-wide approach

REPORT →

Deloitte.

2025 Audit Committee Practices Report

Addresses key priorities for audit committees, emphasizing cybersecurity, enterprise risk management (ERM), and finance/internal audit talent

REPORT →

accenture

WORLD ECONOMIC FORUM

The Global Cybersecurity Outlook 2025

Covers challenges like supply chain vulnerabilities, a growing skills gap, and fragmented regulatory landscapes

REPORT →

The State of Continuous Controls Monitoring Report

Addresses some of the challenges CISOs face in aligning security and compliance, with less than half reporting harmonized efforts

REPORT →

What Audit Committees Should Prioritize in 2025

Encourages audit committees to reassess risk management frameworks, enhance scenario planning, and ensure effective compliance strategies amid changing economic and regulatory landscapes

REPORT →

On The 2025 Audit Committee Agenda

Covers the need for robust oversight in financial reporting, compliance, and risk management during global challenges

REPORT →

2024 Cyber Claims Report

Emphasizes the importance of strong cyber hygiene and active partnerships with insurance providers to mitigate risks

REPORT →

2024 Security Budget Benchmark Report

Emphasizes the importance of visibility and credibility for CISOs in gaining and maintaining budgets

REPORT →

Table of Contents

CHAPTER 1

Regulatory Chaos: Security's Tough Reality

Organizations today face an increasingly splintered regulatory landscape that challenges even the most sophisticated compliance programs. The data in this chapter reveals a stark reality: **over three-quarters of CISOs report that regulatory fragmentation across jurisdictions significantly hampers their compliance efforts**. This widespread challenge forces security and compliance teams to navigate a patchwork of requirements varying by industry, geography, and data type, often with conflicting or overlapping mandates that strain existing governance frameworks.

The financial implications of this fragmented environment are substantial. According to *The 2025 IT Risk and Compliance Benchmark Report*, 41% of organizations have adjusted their GRC budgets in response to heightened regulatory scrutiny and enforcement. This reallocation of resources demonstrates how regulatory pressure directly influences organizational priorities and investment decisions. For GRC professionals, this means continuously justifying and optimizing compliance expenditures while maintaining effective protection in a shifting regulatory landscape.

Most concerning is the compliance gap uncovered in this research: despite the proliferation of country-specific data security and privacy laws, only 17% of organizations (according to *The 2025 IT Risk and Compliance Benchmark Report*) currently adhere to or plan to adopt these requirements. This statistic signals a significant disconnect between regulatory expectations and organizational capabilities, exposing companies to substantial compliance risk across multiple jurisdictions. This gap exists partly because nearly half of organizations struggle to keep pace with the speed and volume of regulatory changes, creating an environment where compliance teams must constantly prioritize which requirements demand immediate attention.

The following chapters examine these trends in greater detail, showing how organizations are responding to these challenges through various structural approaches. From sequential handling of new regulations to establishing dedicated regional compliance teams, GRC and cybersecurity professionals are developing diverse strategies to address the fragmentation defining today's regulatory landscape. The statistics presented offer insight into both the scale of current challenges and emerging practices that may help organizations build more resilient compliance functions capable of adapting to tomorrow's regulatory requirements.

76% of CISOs report regulatory fragmentation significantly impacts compliance efforts

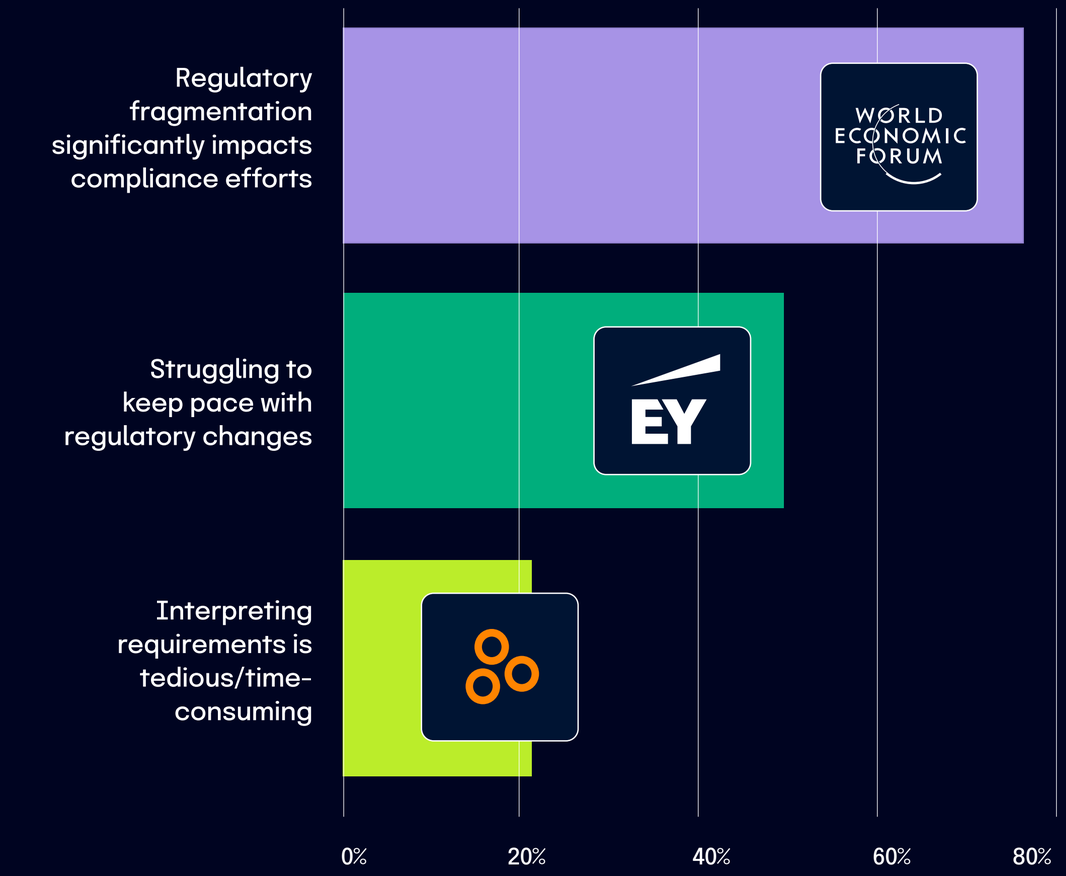
The Global Cybersecurity Outlook 2025 Insight Report shows that over three-quarters of CISOs find that regulatory fragmentation across jurisdictions significantly impairs their organizations' ability to maintain compliance. This widespread challenge creates a complex regulatory landscape that demands substantial resources to navigate effectively.

This regulatory complexity is further emphasized in the *What Audit Committees Should Prioritize in 2025 Report*, which shows 49% of global respondents are struggling to keep pace with the speed and volume of regulatory changes.

These findings provide important context for data from *The 2025 IT Risk and Compliance Benchmark Report*, which indicates that 21% of respondents find interpreting audit requirements and compliance standards to be tedious or more time-consuming than anticipated. This percentage reflects the downstream impact of the broader regulatory challenges identified in the other reports.

Together, these statistics illustrate organizations battling a constantly shifting and geographically fragmented compliance environment. Regulatory fragmentation and rapid changes create practical interpretation challenges for compliance teams. When organizations must understand and apply inconsistent or conflicting requirements across multiple jurisdictions, requirements that may be constantly evolving, the interpretation task inevitably becomes more complex and time-intensive.

Regulatory fragmentation impact across jurisdictions



hyperproof.io/it-compliance-benchmarks

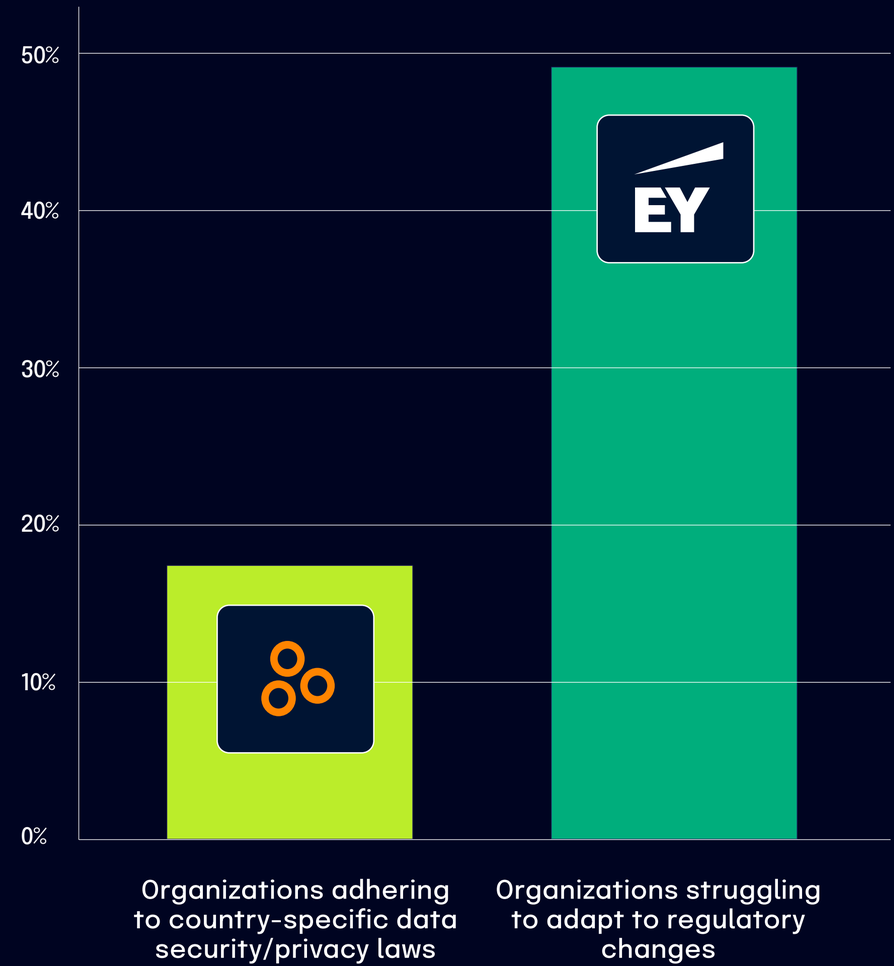
Only 17% of organizations adhere to country-specific data security/privacy laws despite their growing prevalence

17% of respondents in the *The 2025 IT Risk and Compliance Benchmark Report* said that their organization currently adheres to or plans to adhere to country-specific data security and privacy laws. This alarmingly low adoption rate comes at a time when countries worldwide increasingly implement their own unique regulatory frameworks for data protection.

This limited compliance with country-specific regulations makes more sense when considered alongside findings from the *What Audit Committees Should Prioritize In 2025 Report*, which highlights that 49% of organizations struggle to adapt to the speed and volume of regulatory changes. Nearly half of all organizations simply cannot keep pace with the rapidly changing regulatory landscape.

The connection between these statistics points to a significant compliance challenge: as countries continue to implement individualized approaches to data security and privacy regulation, organizations face mounting complexity in tracking, interpreting, and implementing these varied requirements. The substantial gap between the proliferation of country-specific regulations and the relatively low organizational adoption rate reflects the practical difficulties in managing compliance across multiple jurisdictions with different, sometimes conflicting requirements. This relationship between regulatory complexity and compliance rates explains why many organizations prioritize international frameworks or industry standards over country-specific requirements, despite their legal obligations to follow local laws.

Organizational compliance with security and privacy laws



hyperproof.io/it-compliance-benchmarks

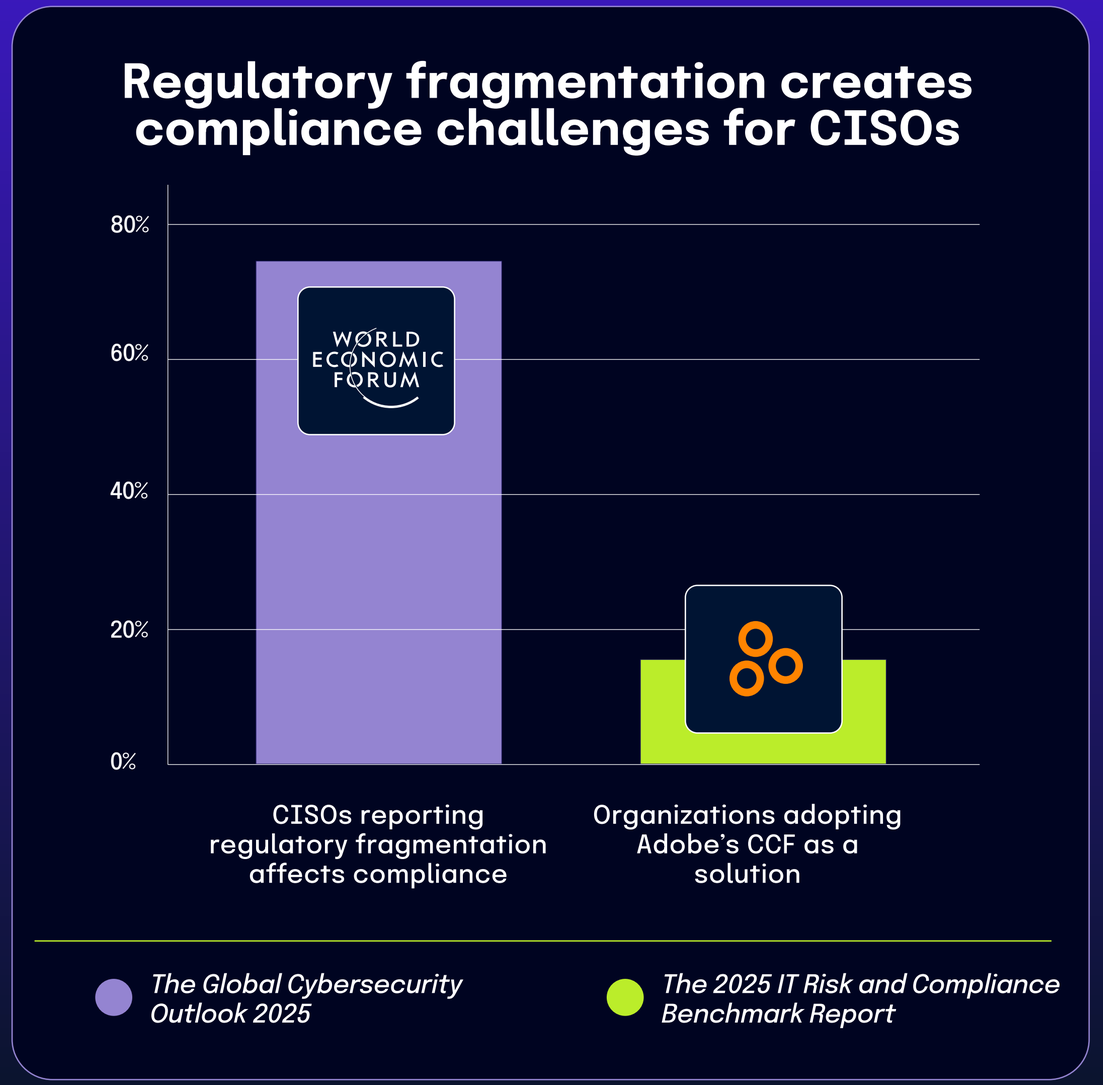
76% of CISOs report regulatory fragmentation affects compliance, with 17% turning to Adobe's CCF as a potential solution

According to *The Global Cybersecurity Outlook 2025 Report*, 76% of Chief Information Security Officers struggle with regulatory fragmentation significantly impacting their compliance efforts. This widespread challenge creates complexity as organizations attempt to navigate overlapping and sometimes conflicting regulatory requirements across different jurisdictions and industries.

In response to this fragmentation, *The 2025 IT Risk and Compliance Benchmark Report* shows that 17% of surveyed organizations have adopted or plan to implement Adobe's Common Control Framework (CCF). This framework offers a unified approach to compliance by mapping controls across multiple regulations and standards, potentially simplifying compliance efforts for organizations.

The connection between these statistics becomes clearer when considering the populations surveyed. *The World Economic Forum Report* focuses specifically on C-level executives, while Hyperproof's benchmark report showcases data from a broader range of roles. The 17% adoption rate of CCF represents organizations that have identified a specific solution to address the regulatory complexity experienced by the larger percentage of CISOs.

This relationship suggests that **as regulatory environments continue to evolve with increasing complexity, frameworks like CCF that consolidate compliance requirements are becoming a strategic choice for organizations looking to streamline their compliance programs across multiple regulations**. When organizations manage compliance in silos, they often miss critical security gaps between regulatory frameworks, leaving vulnerabilities that sophisticated threat actors can exploit. The 17% adoption rate of unified frameworks like CCF suggests an competitive advantage for these organizations through reduced compliance costs, more efficient resource allocation, and potentially stronger security postures.



Regulatory scrutiny is driving significant changes in corporate compliance budgets

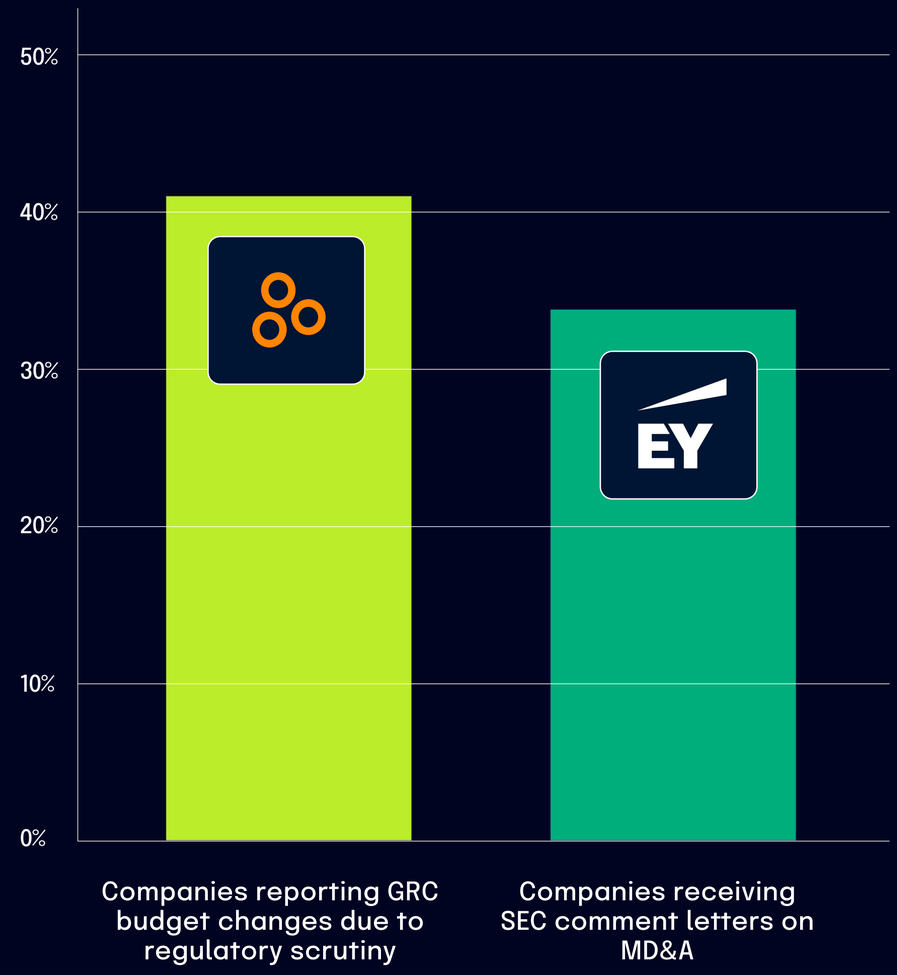
According to *What Audit Committees Should Prioritize in 2025*, 34% of registrants received comment letters on Management's Discussion and Analysis (MD&A) sections of their financial filings. These formal communications from the Securities and Exchange Commission directly show the increased regulatory oversight that organizations must address.

2024			
Comment area	Ranking 12 months ended June 30*	Comment area received as a percentage of registrants receiving comment letters	Average letters per registrant**
MD&A**	1	34%	1.2
Non-GAAP financial measures	2	32%	1.3
Segment reporting	3	15%	1.3
Revenue recognition	4	13%	1.2
Goodwill and intangible assets	5	7%	1.2
Business combinations	6	6%	1.1

SOURCE: *What Audit Committees Should Prioritize in 2025*

*These rankings are based on topics assigned by research firm Audit Analytics (AA) for SEC comment letters issued to registrants with a market capitalization of $75M or more

SEC scrutiny drives changes to compliance budgets



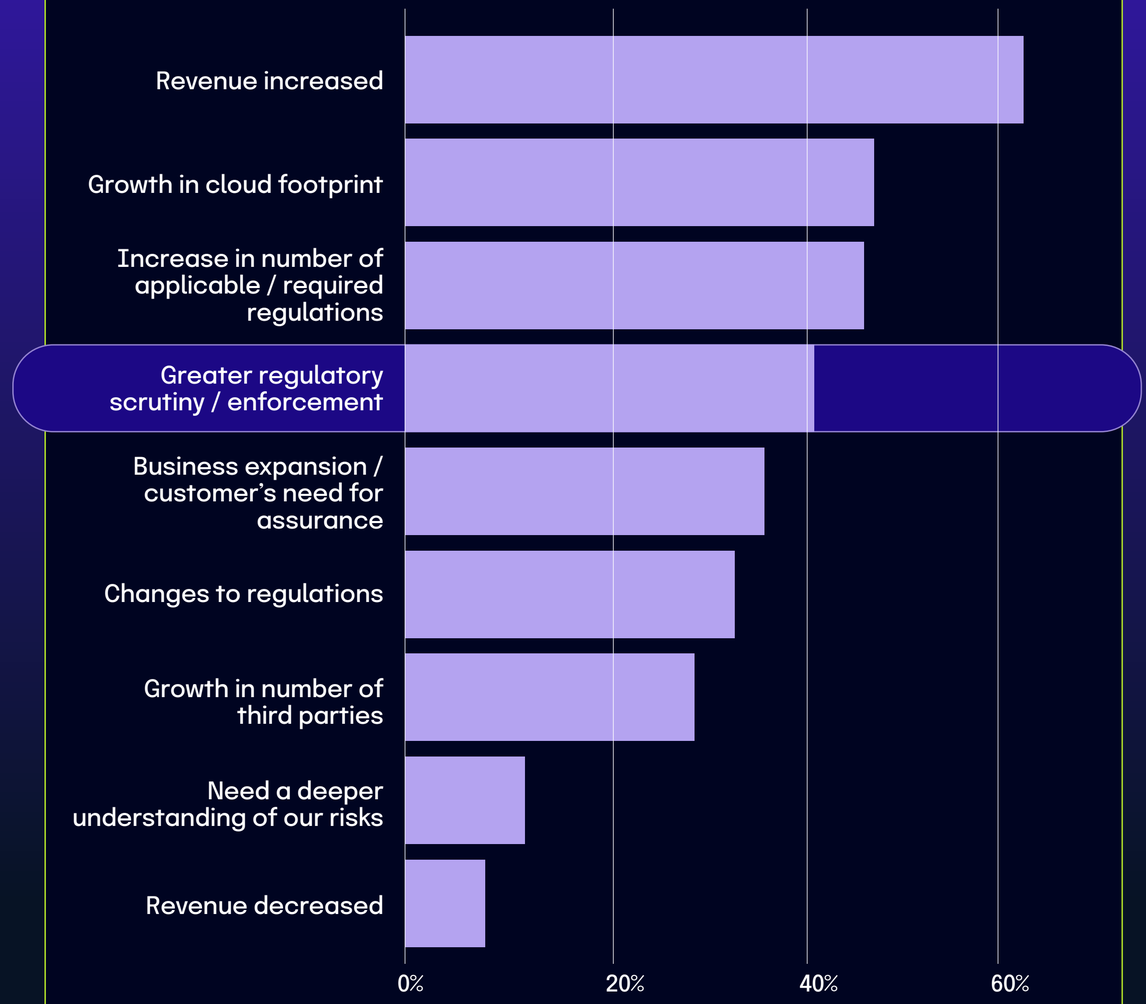
This heightened scrutiny appears to be having direct financial impacts. 41% of respondents in *The 2025 IT Risk and Compliance Benchmark Report* stated that their GRC budget changed in 2024 due to greater regulatory scrutiny and enforcement. This connection clearly shows how regulatory actions translate into organizational resource allocation decisions.

The relationship between these statistics tells an important story about cause and effect in today's compliance landscape. When companies receive SEC comment letters asking for clarification, additional disclosures, or changes to their MD&A sections in financial filings like 10-K or 10-Q reports, they typically must allocate more resources to address these regulatory concerns.

Increased regulatory engagement is reshaping organizational priorities and spending. As regulatory bodies become more assertive in their oversight, companies are responding by adjusting their GRC investments to meet evolving compliance expectations and avoid potential penalties or reputational damage.

> As regulatory bodies become more assertive in their oversight, companies are responding by adjusting their GRC investments to meet evolving compliance expectations and avoid potential penalties or reputational damage.

What drivers caused your GRC budget to change in 2024?



SOURCE: *The 2025 IT Risk and Compliance Benchmark Report*

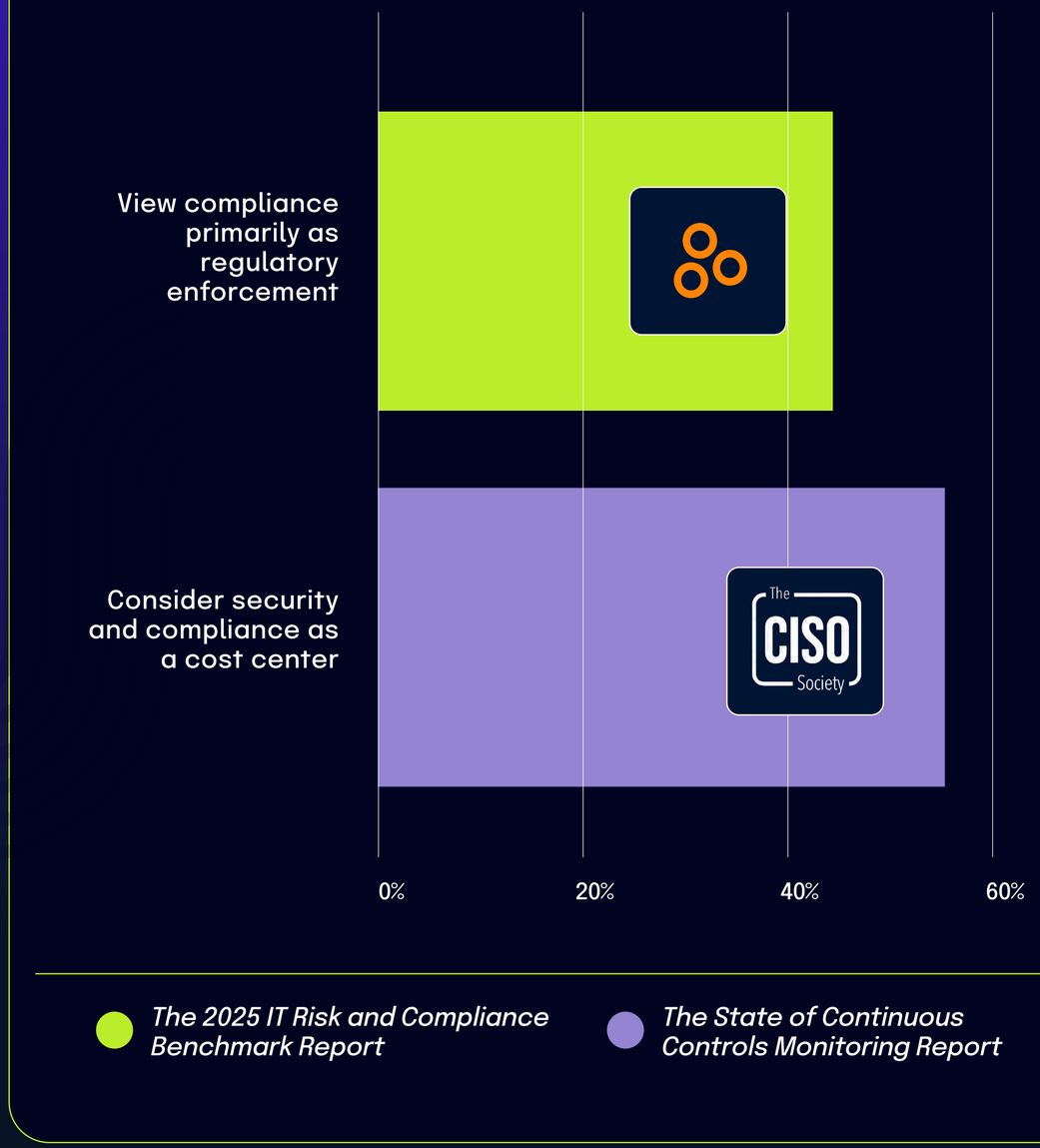
hyperproof.io/it-compliance-benchmarks

43% of organizations view compliance primarily as a regulatory enforcement function

The 2025 IT Risk and Compliance Benchmark Report indicates that 43% of respondents view their compliance function primarily as the enforcer of regulations and industry standards. This perception positions compliance as a necessary, but potentially restrictive, organizational component that focuses mainly on maintaining adherence to external requirements.

> Viewing GRC is a cost center limits compliance's organizational influence to an enforcement role instead of positioning it as a valuable partner in business growth and innovation.

Organizations view as regulatory enforcer, not enabler



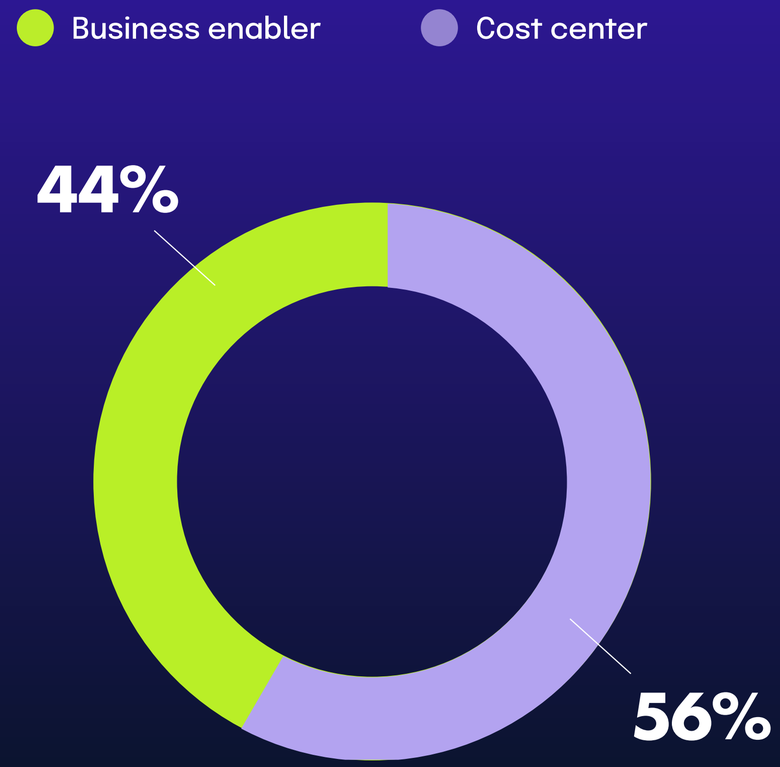
hyperproof.io/it-compliance-benchmarks

This finding gains additional context when paired with data from *The State of Continuous Controls Monitoring Report*, which found that 55.8% of CISOs consider security and compliance to be a cost center rather than a business enabler. Together, these statistics suggest a clear connection between how organizations perceive compliance financially and how they define its functional role.

When organizations view compliance primarily as a cost center, they tend to focus on its mandatory aspects, specifically the enforcement of necessary regulations, rather than its potential strategic benefits. This narrow perception often limits compliance's organizational influence to an enforcement role instead of positioning it as a valuable partner in business growth and innovation.

Financial perceptions directly shape functional definitions within organizations. Companies that see compliance primarily as a financial burden typically limit its scope to regulatory enforcement, while those viewing it as a value-adding function are more likely to embrace a broader, more strategic role for their compliance teams.

Does your organization consider security and compliance as a business enabler or a cost of doing business?

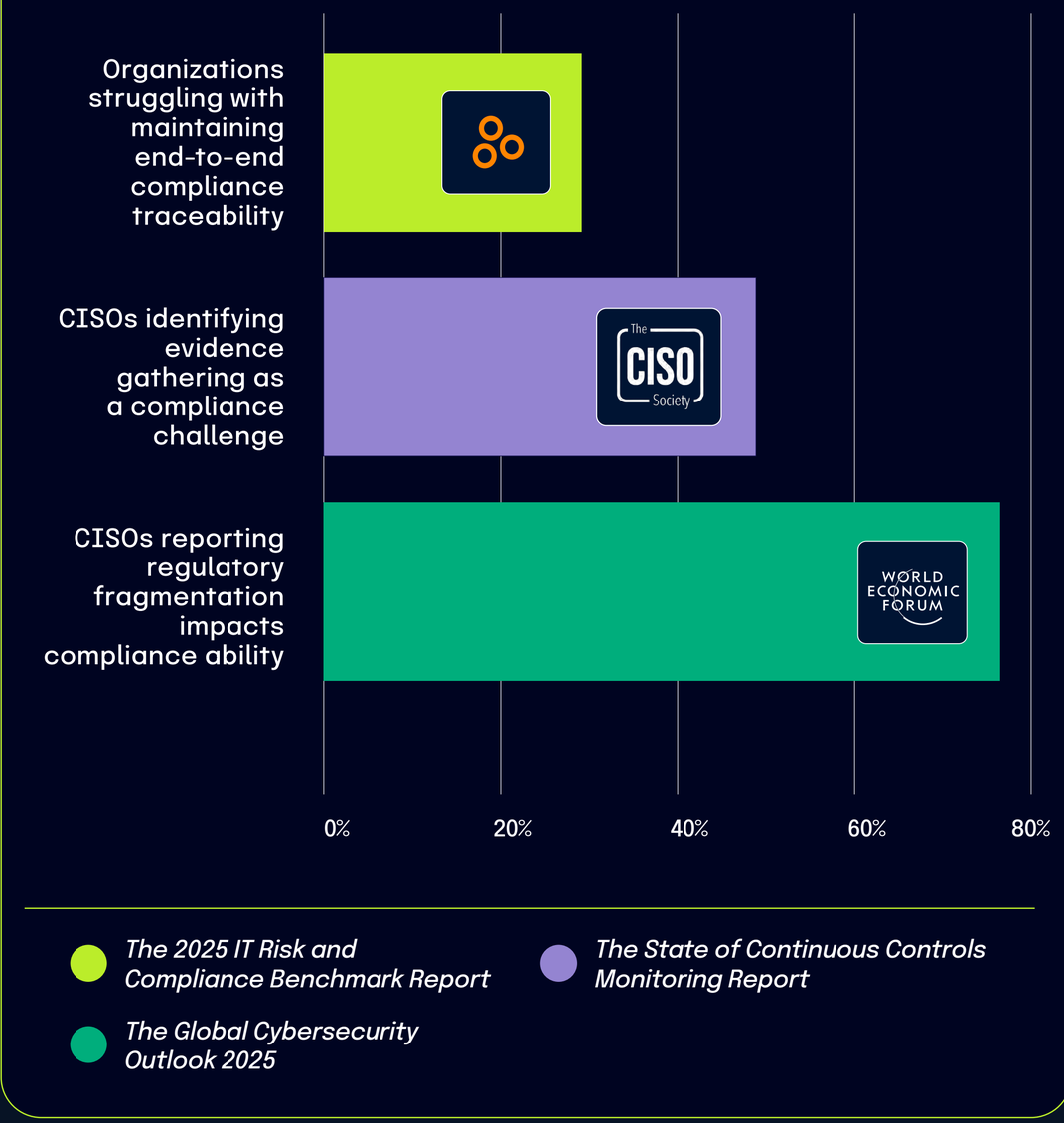


SOURCE: *The State of Continuous Controls Monitoring Report*

Nearly 3 in 10 organizations struggle with maintaining end-to-end compliance traceability

According to *The 2025 IT Risk and Compliance Benchmark Report*, 29% of respondents struggle with maintaining traceability from regulatory, contractual, and legal requirements through policy and controls to adequate evidence of control operation. This challenge creates a significant gap in many organizations' compliance frameworks.

Regulatory traceability remains a compliance gap



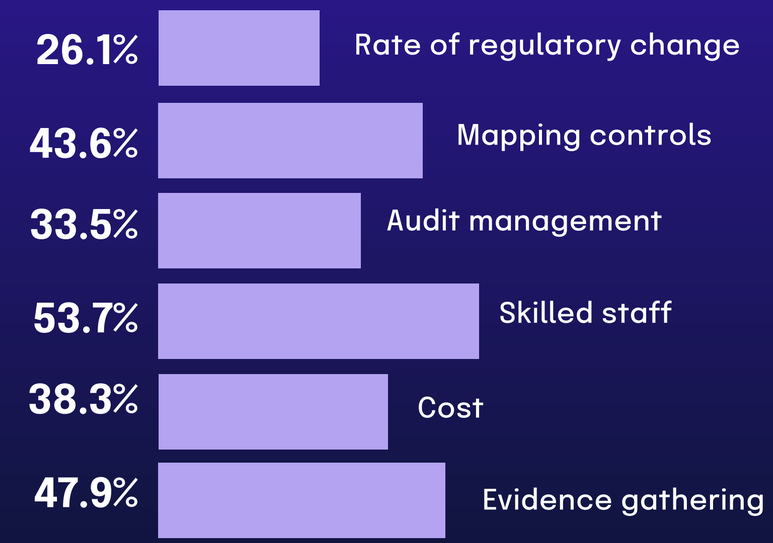
hyperproof.io/it-compliance-benchmarks

This finding gains additional context when paired with *The State of Continuous Controls Monitoring Report*, where 47.9% of CISOs specifically identified evidence gathering as a challenge. This statistic directly connects to the "evidence of control operation" component in the traceability chain, highlighting a key breakdown point in the compliance process.

The complexity of maintaining traceability becomes even more complex due to regulatory fragmentation, as highlighted in *The Global Cybersecurity Outlook 2025 Report*. The report found that 76% of CISOs indicate that fragmentation of regulations across jurisdictions significantly impacts their organizations' ability to maintain compliance. This higher percentage reflects the specific challenges faced by CISOs in multi-jurisdictional organizations who must navigate numerous requirements across contracts, jurisdictional boundaries, and local laws.

Together, these statistics demonstrate how maintaining end-to-end compliance traceability involves multiple interconnected challenges, from managing diverse regulatory requirements at the start of the process to collecting adequate and sufficient evidence at the end.

What are your greatest challenges in implementing new or outdated frameworks?



SOURCE: *The State of Continuous Controls Monitoring Report*

CHAPTER 2

Governance Without Systems Creates Dangerous Gaps

The integration of risk management into organizational governance presents a complex picture of progress and persistent challenges. While a majority of organizations have adopted regular risk assessment cadences – 87% conduct assessments on a set schedule, according to *The 2025 IT Risk and Compliance Benchmark Report* – significant disconnects remain between governance goals and operational execution. Many organizations still lack centralized systems for managing risk and compliance data, with over 40% from *The State of Continuous Controls Monitoring Report* reporting this critical infrastructure gap. Additionally, based on *The 2025 IT Risk and Compliance Benchmark Report*, 82% of teams believe they effectively assess control effectiveness, but 45% of board directors from the *2024 BDO Board Survey* seek external validation, a confidence gap that hinders governance assurance. This misalignment between operational self-assessment and board expectations underscores the need for better translation of day-to-day risk activities into executive-level visibility and trust.

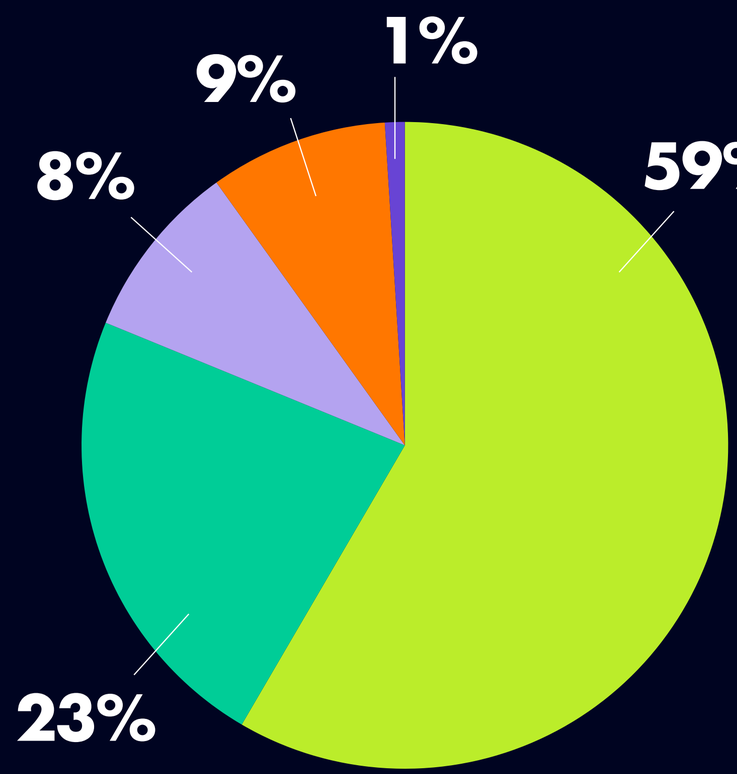
For GRC and cybersecurity professionals, these findings highlight the importance of aligning governance structures with practical implementation. The prevalence of quarterly security risk assessments (59%, based on *The 2025 IT Risk and Compliance Benchmark Report*) mirrors the frequency with which cybersecurity appears on audit committee agendas (71% of respondents of *The Audit Committee Practices Report 2025*), illustrating how governance mandates increasingly dictate operational rhythms.

However, the perception of security as a cost center by 55.8% of CISOs, according to *The State of Continuous Controls Monitoring Report*, continues to constrain teams' ability to secure necessary resources, despite growing expectations. As organizations navigate these competing pressures, the need for improved integration, communication, and strategic investment becomes clear. The following sections explore these dynamics in greater depth, offering insights into prevailing practices, evolving market trends, and actionable opportunities to enhance risk governance maturity.

87% of organizations formalize risk management through regular assessment cadences

The 2025 IT Risk and Compliance Benchmark Report highlights that 87% of surveyed organizations conduct risk assessments on a regular cadence to formalize their commitment to risk management. This high percentage demonstrates that structured, scheduled risk assessment has become a standard practice across most organizations, regardless of their specific frequency.

How often does your organization conduct security risk assessments?



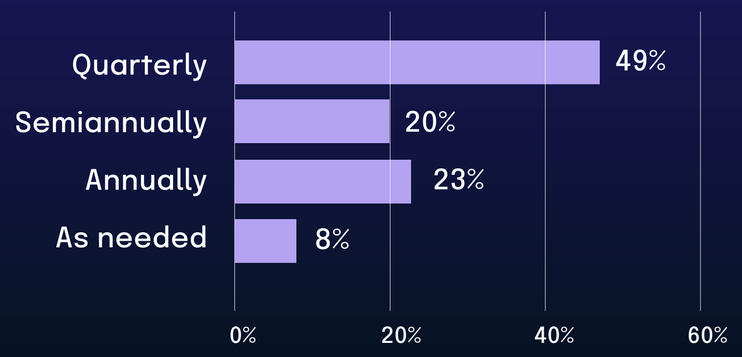
SOURCE: *The 2025 IT Risk and Compliance Benchmark Report*

hyperproof.io/it-compliance-benchmarks

This finding gains additional context when compared with *The Audit Committee Practices Report 2025*, which found that 49% of respondents discuss enterprise risk management (ERM) quarterly at the audit committee level. The difference between these percentages highlights important nuances in how organizations approach risk management practices across different organizational contexts.

While nearly half of audit committees specifically address risk quarterly, the broader 87% figure from the benchmark report includes organizations following various schedules, including annual, semi-annual, and quarterly assessments. This distinction shows how organizations tailor their risk management approaches to their specific governance structures, industry requirements, and risk profiles.

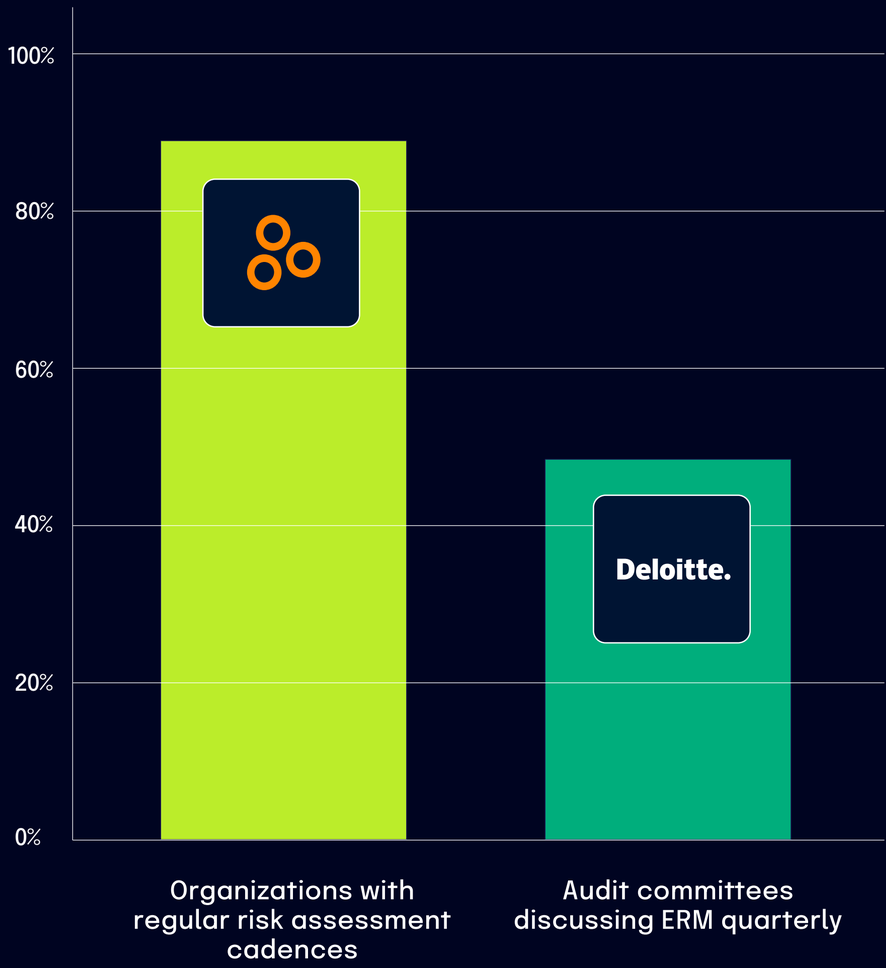
How frequently is [cybersecurity] discussed by the audit committee?



Deloitte.

SOURCE: *The Audit Committee Practices Report 2025*

Regular risk assessments now standard practice across organizations



Nearly 60% of organizations conduct quarterly security risk assessments, aligned with audit committee practices

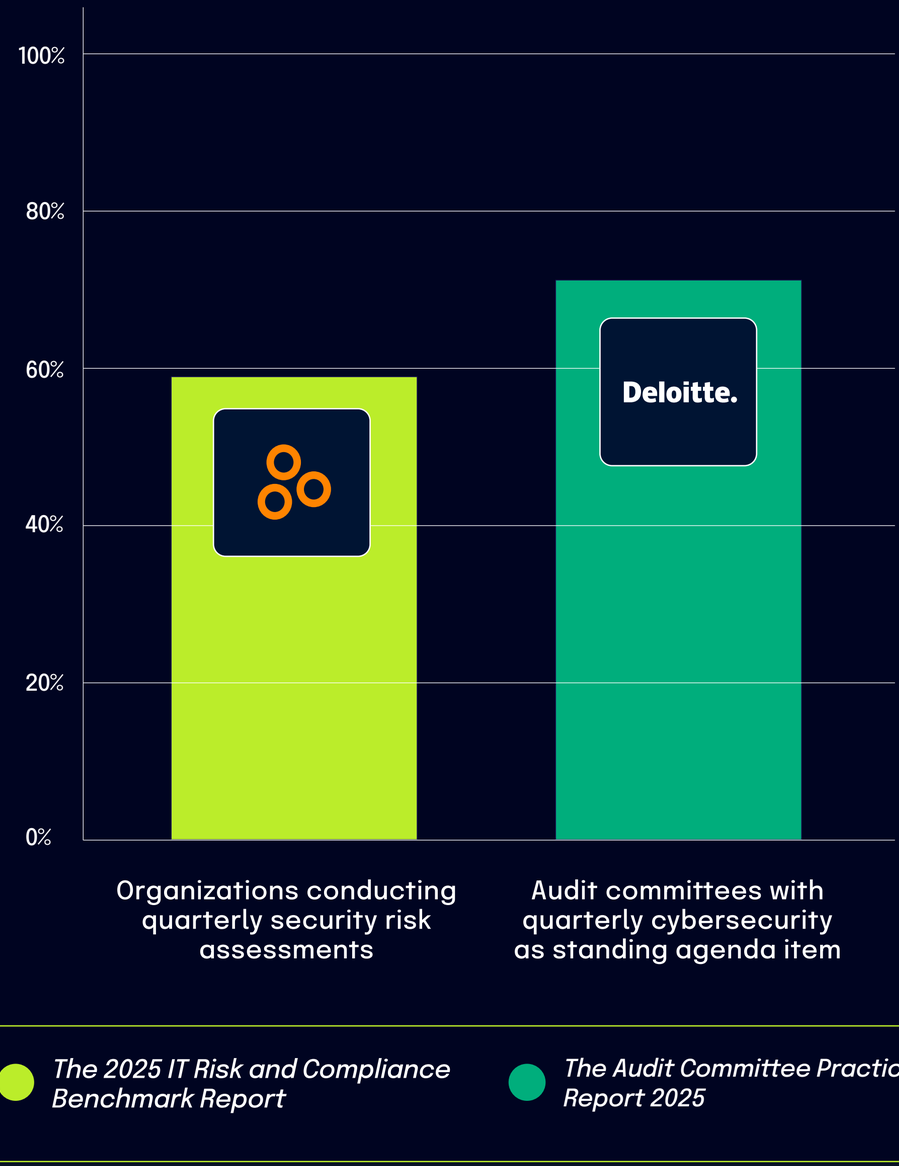
The 2025 IT Risk and Compliance Benchmark Report found that 59% of organizations conduct security risk assessments quarterly, establishing this as the predominant cadence for evaluating cybersecurity risks across surveyed organizations. This quarterly rhythm has become standard practice for most security teams.

This finding gains additional context when compared with *The Audit Committee Practices Report 2025*, which shows that 71% of respondents include cybersecurity as a standing item on their audit committee agenda quarterly. The alignment between these statistics uncovered an important governance relationship: as cybersecurity becomes a regular focus at the audit committee level, organizations are adjusting their assessment practices to provide timely information to these oversight bodies.

The clear connection between these statistics suggests that governance requirements are directly driving operational security practices. When audit committees expect quarterly updates on cybersecurity posture, security teams respond by conducting risk assessments at the same frequency to ensure current information is available for review. This governance-driven approach to risk assessment timing shows how board-level oversight is actively shaping security operations in many organizations.

This relationship highlights the growing integration of cybersecurity into corporate governance structures, with assessment practices being specifically designed to meet the oversight needs of senior leadership and board committees.

Quarterly security risk assessments align with governance expectations



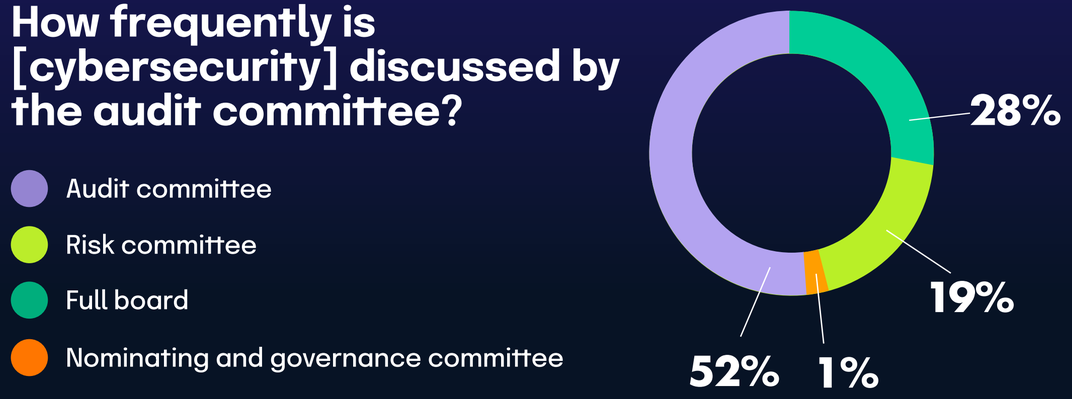
hyperproof.io/it-compliance-benchmarks

52% of audit committees have primary ERM oversight, while over 40% of organizations lack centralized systems for risk management

The Audit Committee Practices Report 2025 states that 52% of audit committees now have primary oversight of enterprise risk management (ERM), establishing a formal governance structure for risk oversight in many organizations. At the same time, *The State of Continuous Controls Monitoring Report* identifies that 40.4% of organizations lack a centralized system for managing their risk and compliance information.

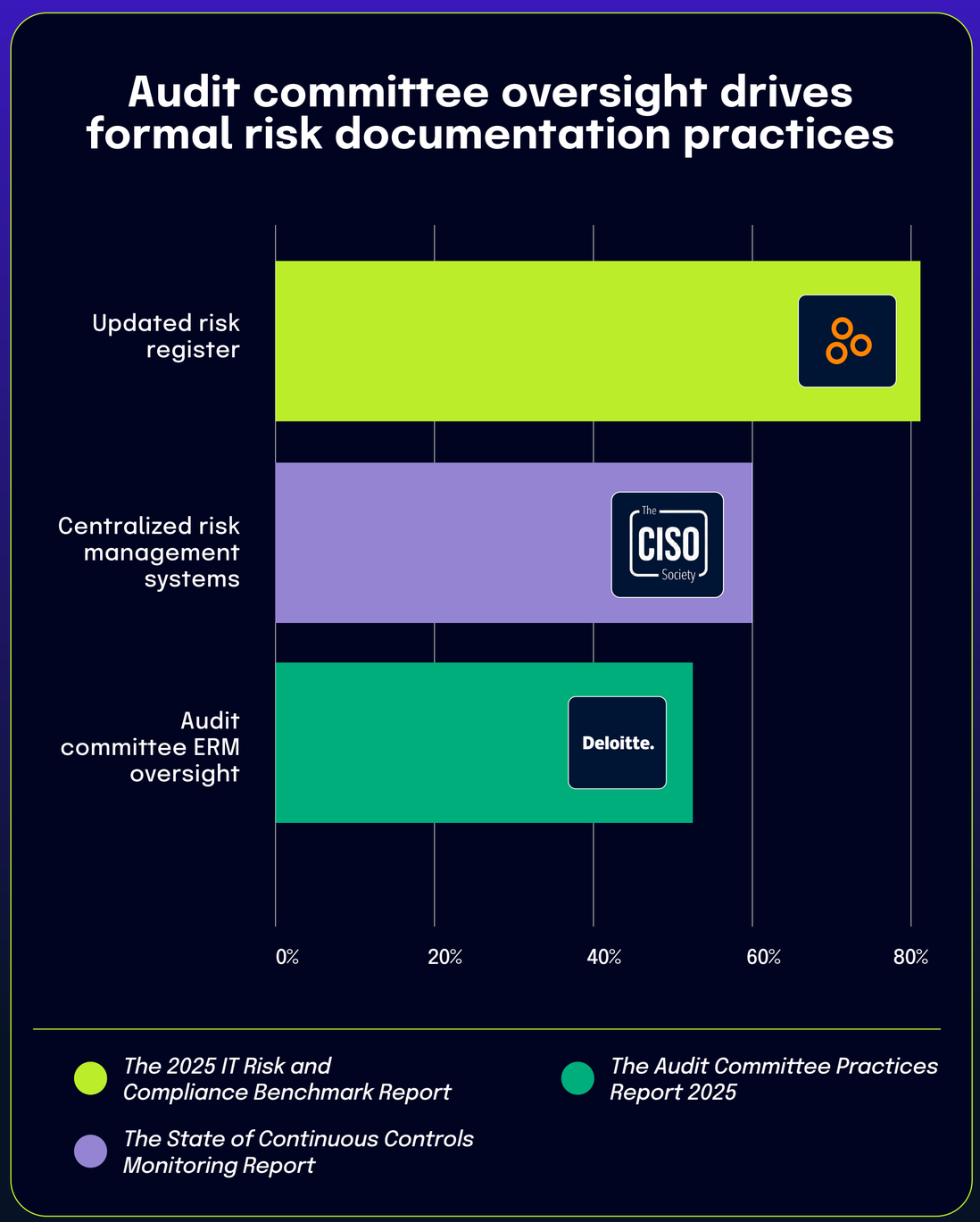
These governance and system realities provide important context for findings in *The 2025 IT Risk and Compliance Benchmark Report*, which shows that 81% of organizations maintain an updated risk register serving as a single repository for all identified risks. These registers typically include comprehensive information about each risk, such as a description of the risk, reference, owner, and mitigation controls. Meanwhile, 19% of organizations report not having an updated risk register.

How frequently is [cybersecurity] discussed by the audit committee?



SOURCE: *The Audit Committee Practices Report 2025*

Audit committee oversight drives formal risk documentation practices



hyperproof.io/it-compliance-benchmarks

Governance structures likely influence risk documentation practices. Organizations where audit committees have formal ERM oversight responsibility typically demand structured documentation and regular reporting, potentially explaining the high percentage of maintained risk registers. The formal governance mechanism creates accountability that drives documentation discipline.

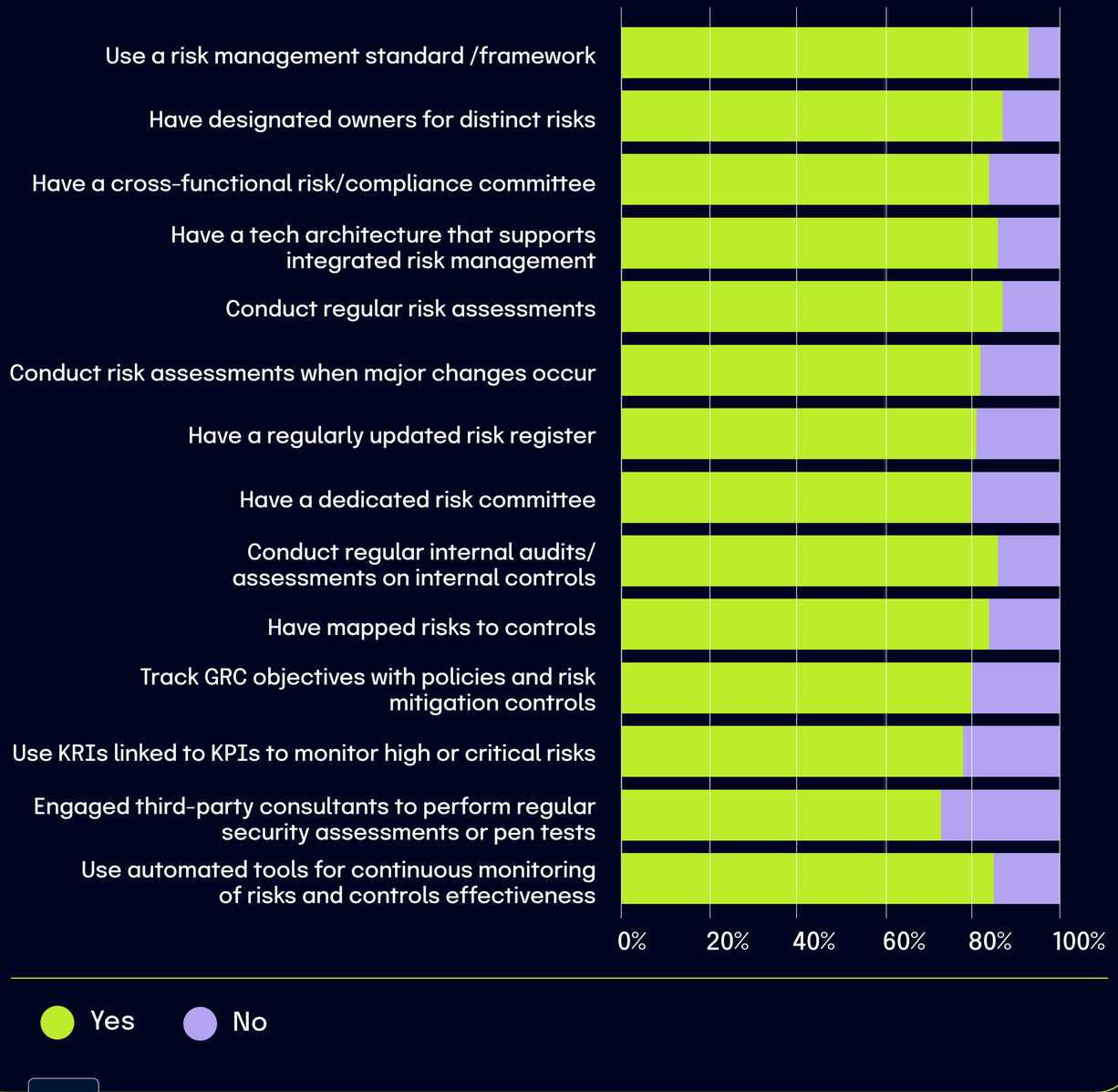
Similarly, the relationship between system infrastructure and risk documentation is clear. The significant percentage of organizations lacking centralized systems aligns with the portion that doesn't maintain comprehensive risk registers. Without integrated technology infrastructure, organizations struggle to document, update, and report on risks across the enterprise.

These findings collectively demonstrate how governance arrangements and technological capabilities shape risk management practices. While we can't definitively establish the exact statistical correlation between audit committee oversight and risk register maintenance, the logical relationship between governance structures, systems infrastructure, and risk documentation practices offers valuable insight into organizational risk management maturity across industries.

FRESH FACT

19% of organizations report not having an updated risk register

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



SOURCE: *The 2025 IT Risk and Compliance Benchmark Report*

hyperproof.io/it-compliance-benchmarks

18% of organizations fail to effectively assign and track risk owners, reflecting broader security governance challenges

According to *The 2025 IT Risk and Compliance Benchmark Report*, 18% of organizations are not meeting their objectives in assigning and tracking risk owners. This significant gap in risk governance exposes a fundamental weakness in how organizations structure accountability for managing security and compliance risks.

The perception of security and compliance as a cost center – shared by 55.8% of CISOs, according to *The State of Continuous Controls Monitoring Report* – has significant implications for risk governance. When security is viewed primarily as an operational expense rather than a strategic investment, organizations are less likely to allocate sufficient resources to build robust governance structures. This often leads to underinvestment in the systems and processes needed to establish clear risk ownership, weakening the foundation for effective risk management.

As a result, many organizations adopt oversimplified ownership models in which all security and compliance responsibilities fall to the CISO or security team, rather than being distributed across relevant business units. This centralized accountability model is often unsustainable, placing undue pressure on technical teams to manage risks they cannot fully control without broader organizational involvement. Ultimately, **the way an organization values its security function directly impacts its ability to implement effective governance practices and ensure shared accountability for risk across the enterprise.**

Inadequate risk ownership undermines security governance effectiveness

hyperproof.io/it-compliance-benchmarks

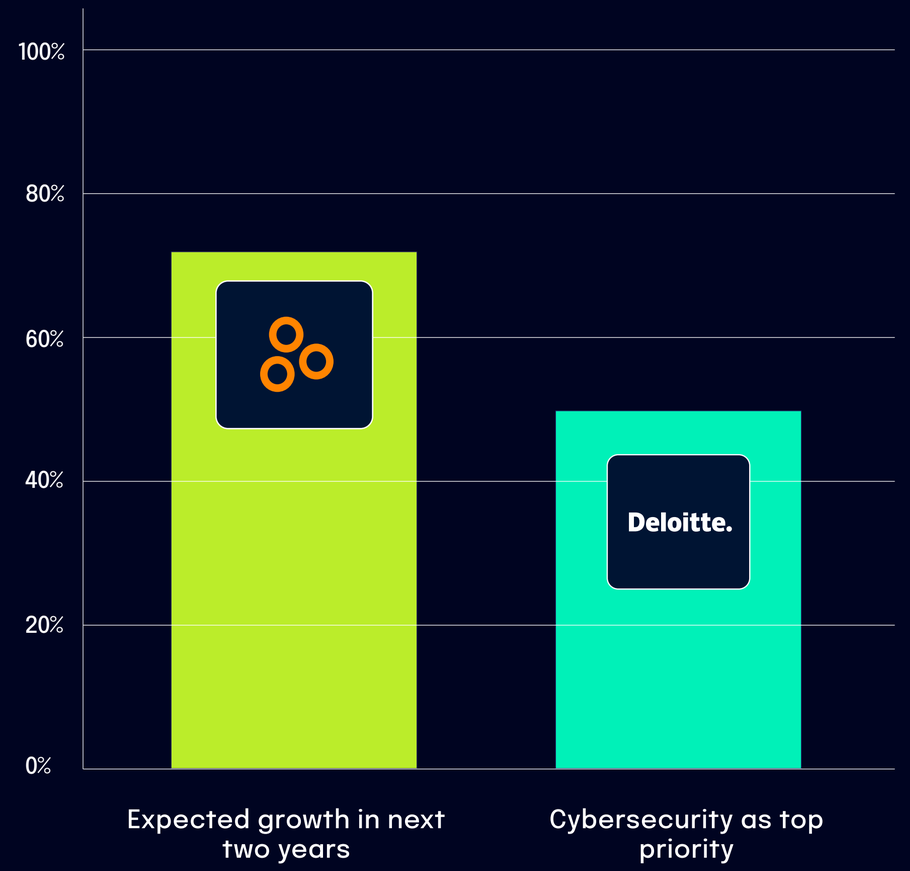
Cybersecurity tops audit committee priorities, driving compliance team growth

According to *The Audit Committee Practices Report 2025*, 50% of respondents ranked cybersecurity as the number-one area of focus for their audit committee over the next 12 months. This significant governance attention directly connects to a key finding from *The 2025 IT Risk and Compliance Benchmark Report*, which found that 72% of respondents expect their information security and data privacy compliance teams to grow over the next two years.

FRESH FACT

50% of respondents ranked cybersecurity as the number-one area of focus for their audit committee over the next 12 months

Audit committee priorities drive security compliance team growth

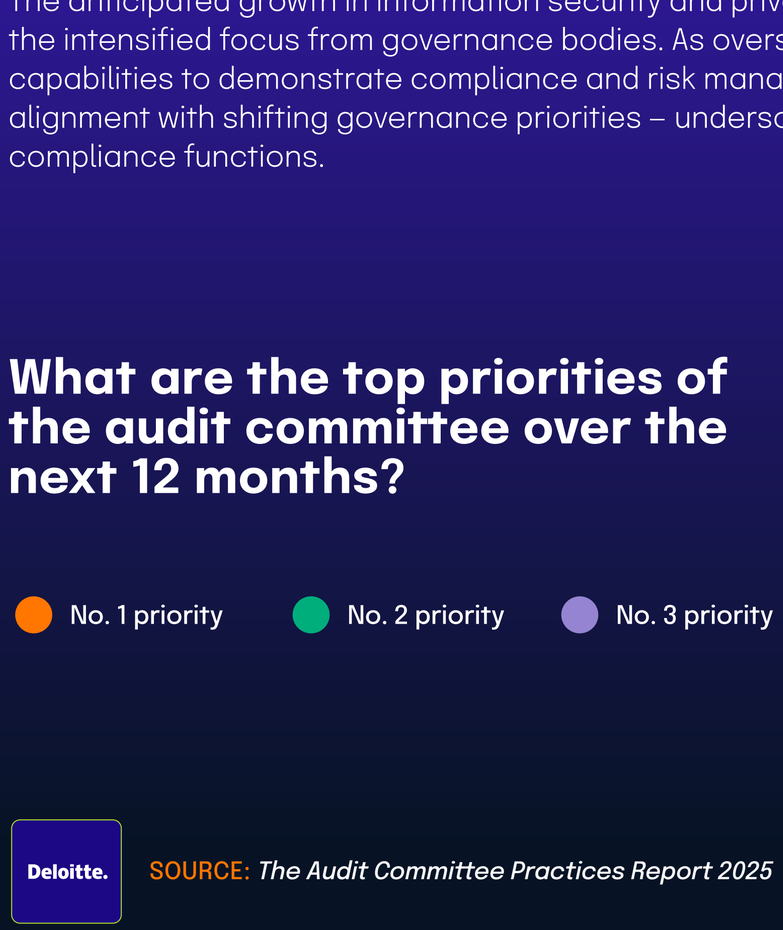


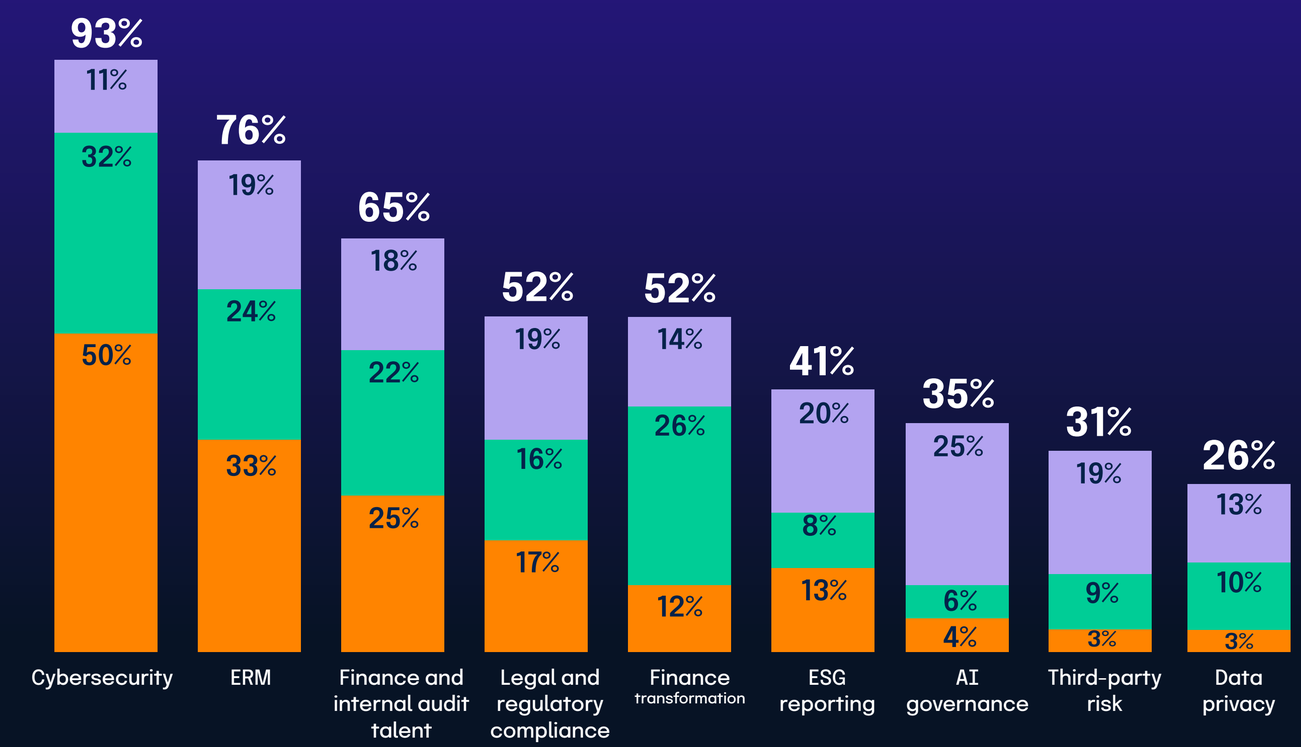
hyperproof.io/it-compliance-benchmarks

These findings illustrate how **board-level priorities directly influence organizational resource allocation, particularly in areas like cybersecurity and privacy.** When half of audit committees rank cybersecurity as a top agenda item, they create accountability pressure that cascades through the organization, prompting increased staffing for compliance and security teams. This governance-driven demand for assurance fuels operational changes, with teams tasked with measuring, monitoring, and reporting on security controls becoming essential to meeting board expectations.

The anticipated growth in information security and privacy compliance teams reflects both the rising complexity of regulatory environments and the intensified focus from governance bodies. As oversight becomes more rigorous, organizations are responding by bolstering their internal capabilities to demonstrate compliance and risk management maturity. This staffing trend is not just a response to operational needs but a strategic alignment with shifting governance priorities – underscoring how top-level oversight increasingly shapes day-to-day decision-making across risk and compliance functions.

What are the top priorities of the audit committee over the next 12 months?





Deloitte.

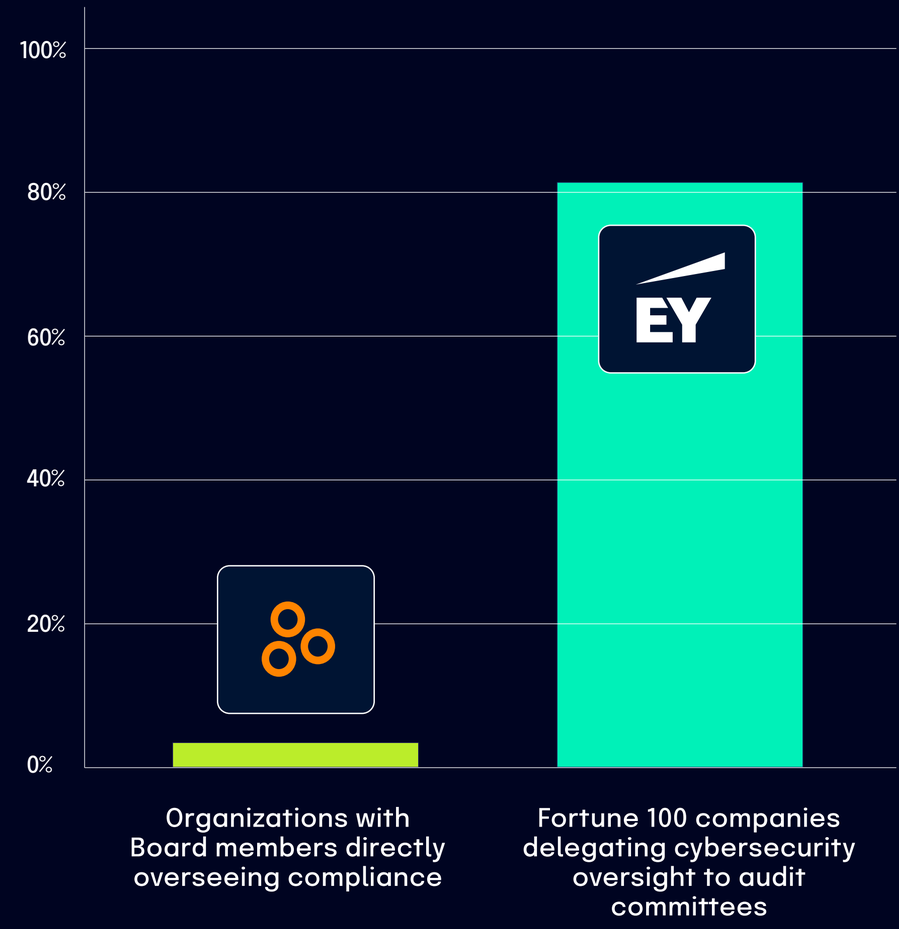
SOURCE: *The Audit Committee Practices Report 2025*

Only 4% of organizations have Board members directly overseeing compliance functions

The 2025 IT Risk and Compliance Benchmark Report shows that only 4% of organizations have Board members directly overseeing compliance, highlighting how rare direct Board involvement remains in most governance structures. This aligns with findings from the *What Audit Committees Should Prioritize in 2025 Report*, which notes that 81% of Fortune 100 companies delegate cybersecurity oversight to their audit committees. These statistics reflect a broader trend: organizations commonly rely on specialized committees to manage complex compliance responsibilities rather than assigning them to the full Board.

This delegation model allows Boards to maintain strategic focus while ensuring that compliance and cybersecurity receive the necessary attention from experts within audit committees. By entrusting these responsibilities to dedicated subgroups, organizations create more efficient governance frameworks capable of handling regulatory complexity and operational nuance. While compliance continues to grow in importance, this structure helps explain why direct Board oversight remains relatively uncommon – it's not a sign of neglect, but of specialization and strategic division of responsibility.

Specialized committees handle compliance oversight



hyperproof.io/it-compliance-benchmarks

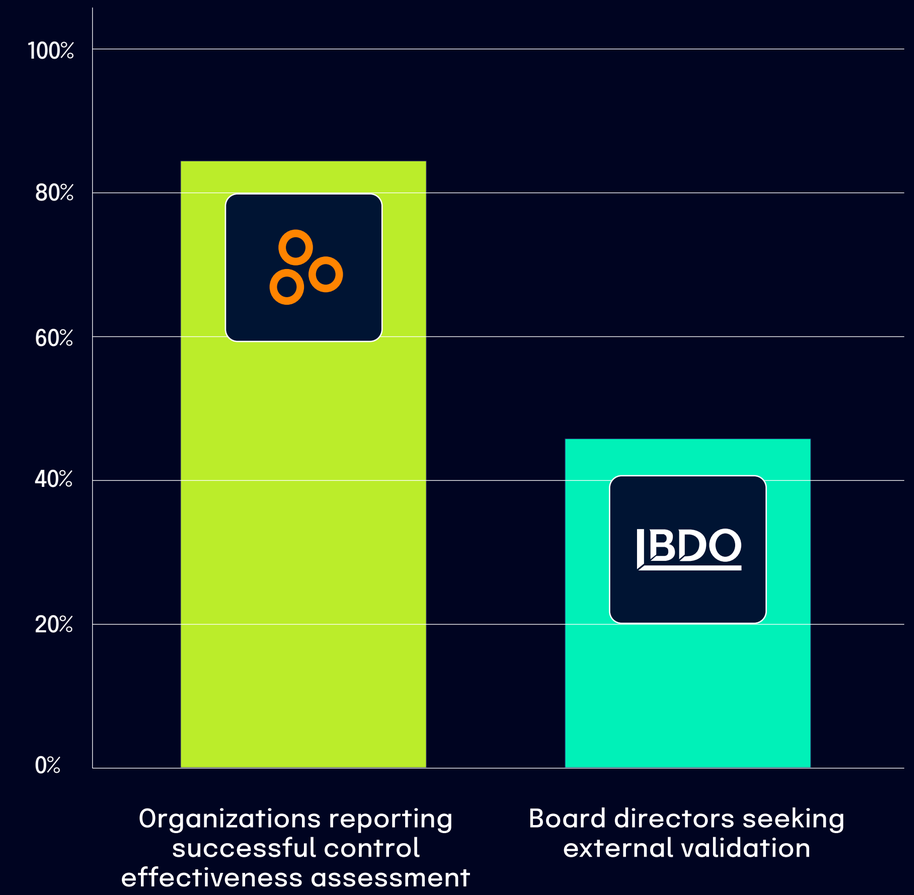
82% of organizations report meeting control effectiveness objectives, yet 45% of Board directors still seek external validation

According to *The 2025 IT Risk and Compliance Benchmark Report*, 82% of organizations believe they are successfully meeting their objectives in assessing control effectiveness. This high self-reported success rate demonstrates widespread confidence in internal control assessment processes. However, *The 2024 BDO Board Survey* contains a compelling counterpoint: 45% of directors indicate they are looking to external assessments for control validation. This significant disconnect highlights a potential gap between operational confidence and governance assurance requirements.

The relationship between these statistics suggests several possibilities. First, while internal teams may believe they're effectively assessing controls, this confidence might not be adequately communicated to board-level stakeholders. Second, even when internal assessments are rigorous and well-communicated, many directors still prefer independent validation due to their fiduciary responsibilities and audit committee independence requirements.

This dynamic reflects the different perspectives within organizational hierarchies. Operational teams focus on implementing and testing controls based on defined objectives, while boards must maintain skepticism and independence in their oversight role. The gap between operational self-assessment (82%) and board comfort level (with 45% seeking external validation) illustrates the complex nature of governance relationships in risk management and the persistent tension between internal assurance activities and external validation requirements.

Control assessment confidence gap between operations and board



hyperproof.io/it-compliance-benchmarks

CHAPTER 3

Beyond Talk: Technology Actions Matter Most

Organizations are under growing pressure to implement effective technology solutions to manage expanding risk and compliance obligations. As regulatory demands increase and threat landscapes reflect changing attacker priorities and tactics, the tools organizations choose – or neglect – to adopt play a critical role in shaping their security posture. Despite broad recognition among security leaders of the need for advanced technology, major implementation gaps remain. For example, while 54% of organizations cite cloud environments as their top cybersecurity risk, only 11% have adopted or plan to adopt the Cloud Security Alliance Cloud Controls Matrix. This disconnect between risk awareness and framework adoption underscores the ongoing struggle to align identified threats with appropriate technical controls, uncovering both a challenge and an opportunity for GRC professionals to drive change.

The divide between belief in and execution of automation further illustrates this gap. A striking 94.2% of CISOs agree that continuous controls monitoring improves security and compliance, yet only 72% have implemented such tools – and over half still report a lack of compliance integration within development pipelines. This tension between aspiration and execution is often fueled by technical debt, limited resources, and shifting priorities, leaving organizations vulnerable in fast-paced software environments. As this chapter explores, understanding where technology adoption succeeds or falters provides GRC and cybersecurity professionals with critical benchmarks to evaluate their own programs. The findings highlight the need for strategic investments and cross-functional alignment to bridge the gap between risk recognition and effective technology-driven governance.

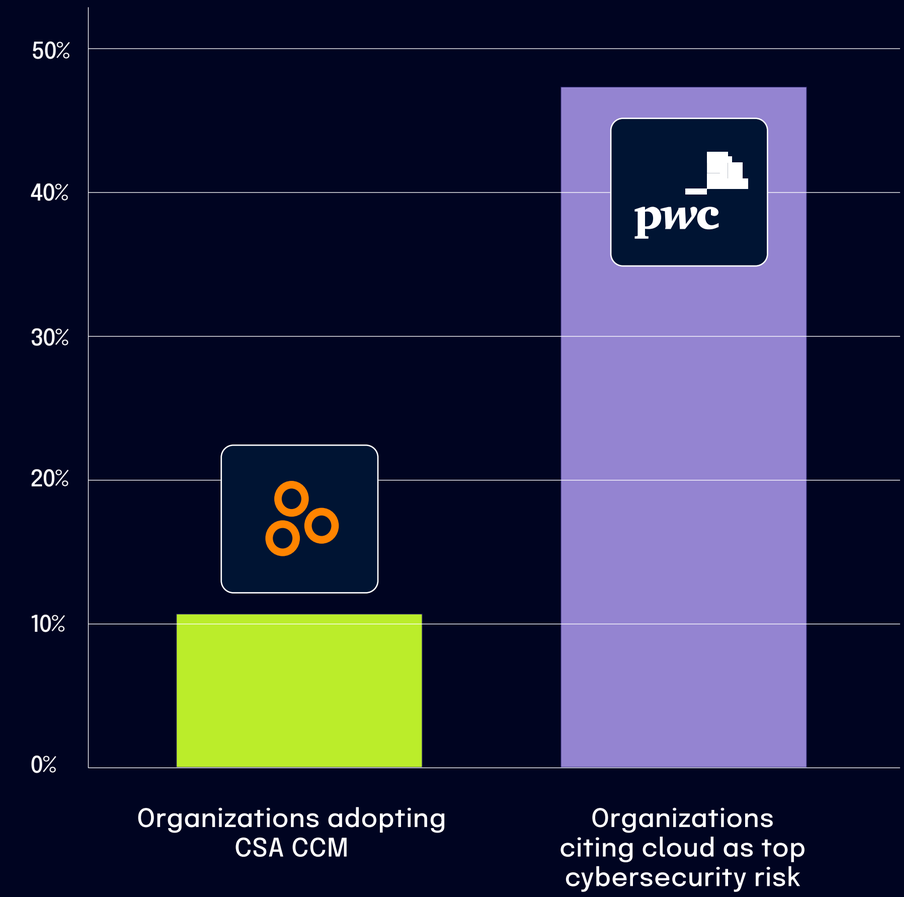
47% of organizations cite cloud as their most pressing cybersecurity risk, yet only 11% adopt CSA CCM

According to *The 2024 Global Digital Trust Insights Report*, nearly half of surveyed organizations (47%) identify cloud environments as their most pressing cybersecurity risk. This concern spans across industries as businesses increasingly migrate critical operations to cloud platforms.

Despite these widespread concerns, *The 2025 IT Risk and Compliance Benchmark Report* found that only 11% of organizations currently adhere to or plan to implement the Cloud Security Alliance Cloud Controls Matrix (CSA CCM), a framework specifically designed to address cloud security risks.

This apparent disconnect can be partially explained by the different populations surveyed in each report. Organizations worried about cloud security may be addressing these risks through alternative frameworks or custom controls rather than specifically adopting CSA CCM. Additionally, while many organizations recognize cloud risks, they may lack awareness of specialized frameworks like CSA CCM or struggle with implementation due to resource constraints.

Cloud environments remain top cybersecurity risk for organizations

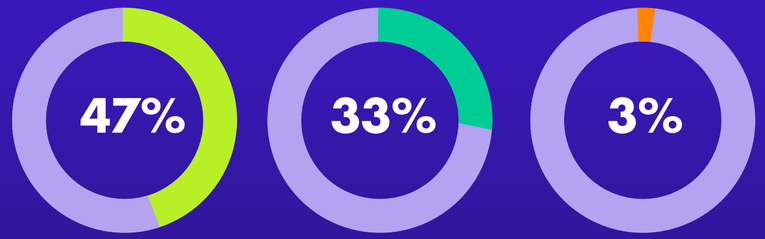


hyperproof.io/it-compliance-benchmarks

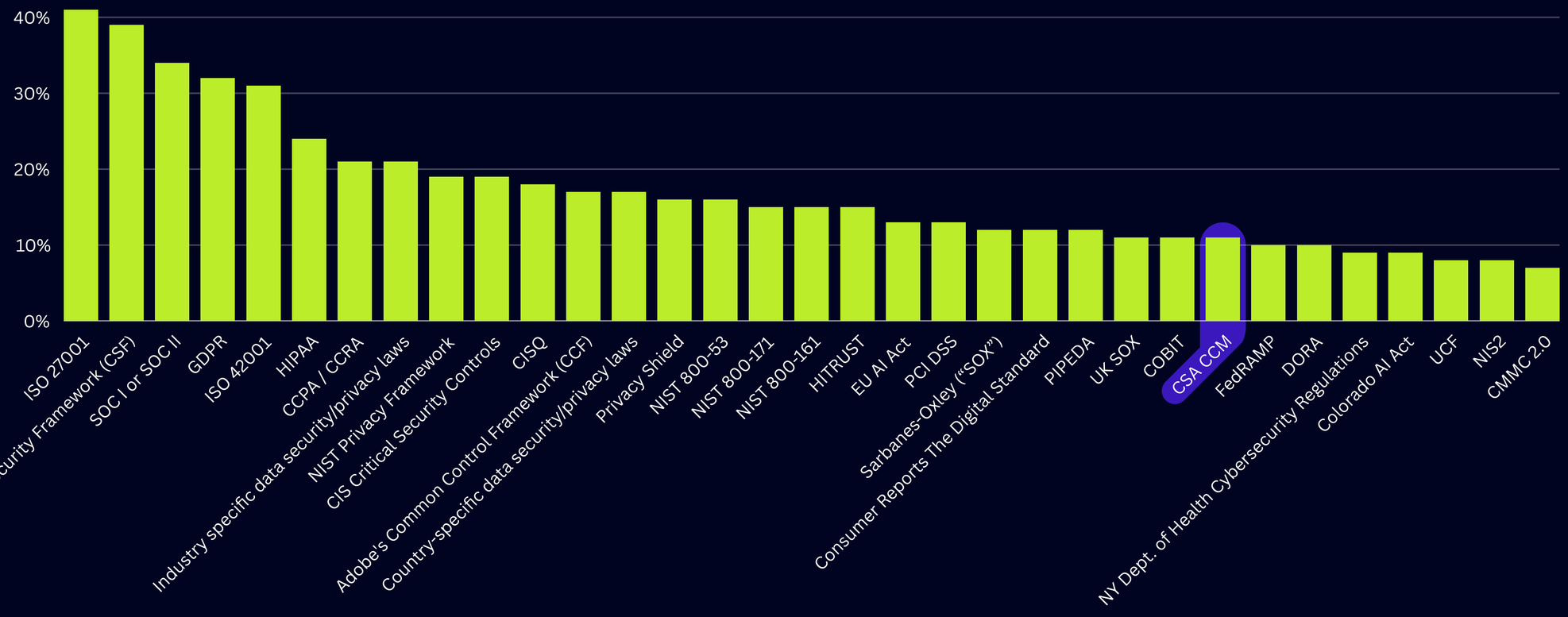
The significant gap between recognized cloud security risks (47%) and CSA CCM adoption (11%) suggests that although cloud security remains a priority for most organizations, there is considerable variation in how they choose to address these concerns within their security programs. This highlights how organizations often take diverse approaches when managing similar risk profiles, even when facing comparable security challenges.

Cloud security: top threat, top investment – yet, poorly managed

SOURCE: *The 2024 Global Digital Trust Insights Report*



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



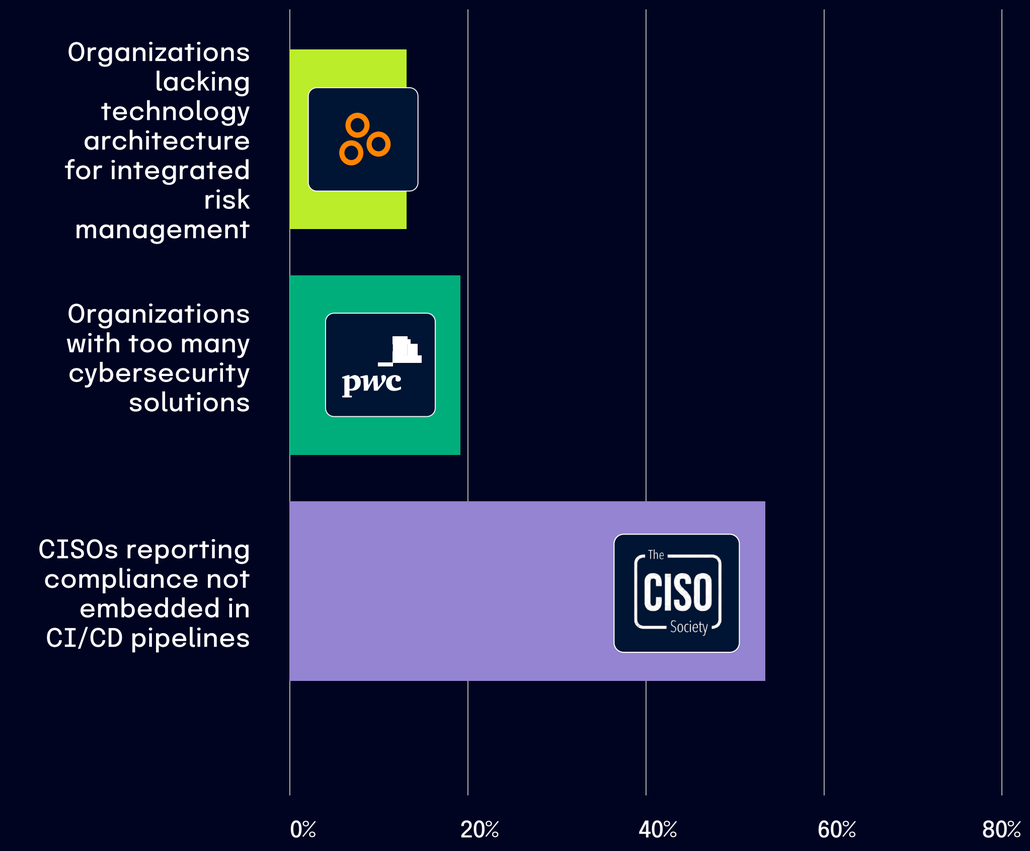
SOURCE: *The 2025 IT Risk and Compliance Benchmark Report*

14% of organizations lack technology architecture for integrated risk management, driven by solution sprawl and development pipeline gaps

The 2025 IT Risk and Compliance Benchmark Report shows 14% of organizations lack a technology architecture that effectively supports integrated risk management. *The 2024 Global Digital Trust Insights Report* indicates that 19% of organizations have too many cybersecurity solutions, creating a fragmented technology environment. *The State of Continuous Controls Monitoring Report* found that 53.7% of CISOs report compliance is not embedded in their CI/CD pipelines.

These findings show how **technology fragmentation and implementation gaps combine to create architectural environments that cannot effectively support integrated risk management**. Integrated risk management faces both technical and procedural obstacles, with solution sprawl and development pipeline limitations being key contributors to the architectural inadequacies.

Technology architecture gaps limit integrated risk management



hyperproof.io/it-compliance-benchmarks

53.7% of CISOs report compliance is not embedded in development pipelines, while 15% of organizations lack any automated risk monitoring tools

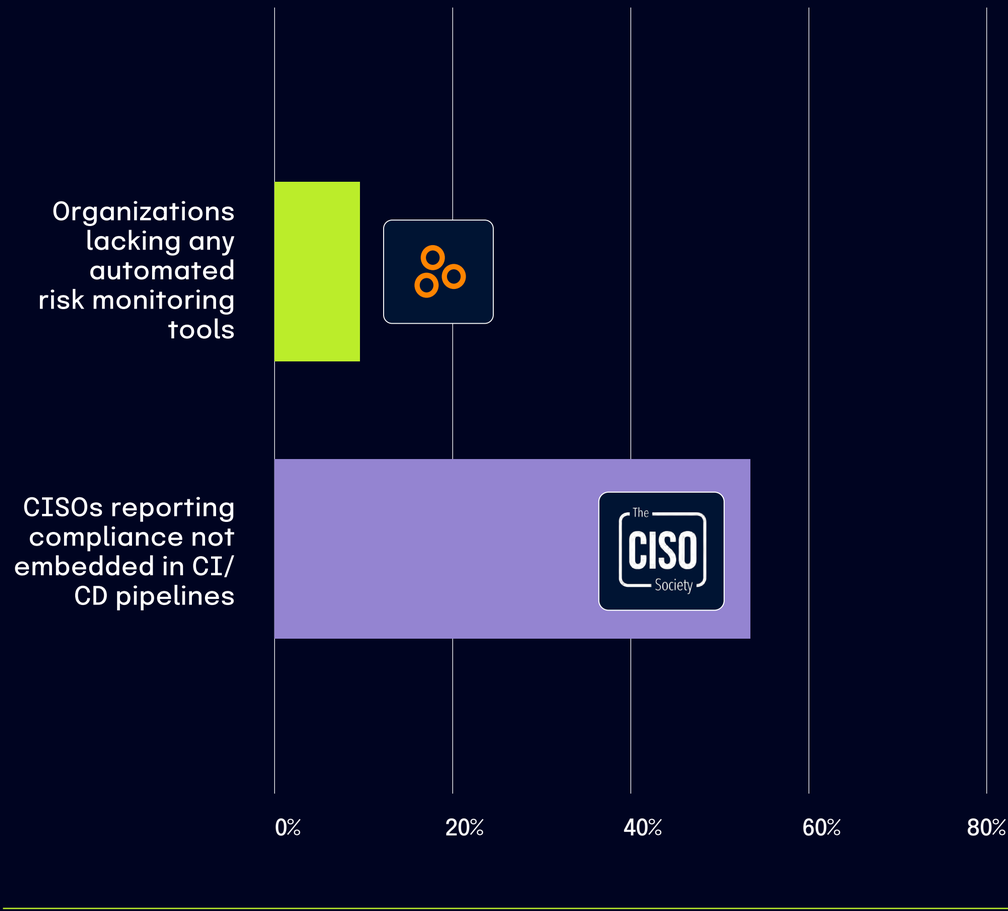
According to *The State of Continuous Controls Monitoring Report*, more than half of Chief Information Security Officers (53.7%) state that compliance is not embedded in their CI/CD pipelines. This significant gap in development automation highlights a specific, yet critical shortcoming in how organizations integrate security and compliance into their technology delivery processes.

This finding provides valuable context for understanding *The 2025 IT Risk and Compliance Benchmark Report* statistic that 15% of organizations do not utilize any automated tools for continuous monitoring of risks and controls' effectiveness. The relationship between these statistics suggests that pipeline automation represents just one component of the broader automation landscape, with some organizations lacking even fundamental monitoring tools.

The gap between these percentages (53.7% vs. 15%) demonstrates different levels of automation maturity. While most organizations have implemented some form of basic risk monitoring automation, specific advanced implementations like CI/CD pipeline integration remain challenging for many. This creates a spectrum where a smaller percentage completely lack automation tools, while a larger group has basic automation but struggles with more sophisticated implementations.

These interconnected findings demonstrate how automation adoption varies significantly across different security and compliance functions, with development pipeline integration presenting a particular challenge even for organizations that have implemented other forms of monitoring automation.

Compliance integration lags in development pipeline automation



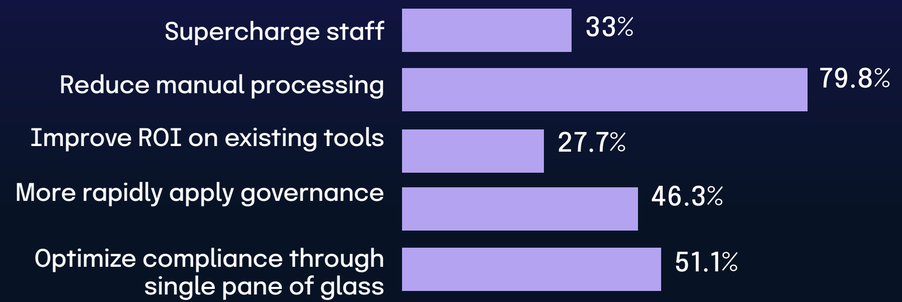
hyperproof.io/it-compliance-benchmarks

20% of organizations have integrated IT risk management but rely on manual processes, confirming industry-wide automation needs

According to *The 2025 IT Risk and Compliance Benchmark Report*, 20% of organizations have successfully implemented integrated approaches to IT risk management but still rely primarily on manual processes for execution. This insight provides valuable context for understanding the industry's broader prioritization of automation initiatives.

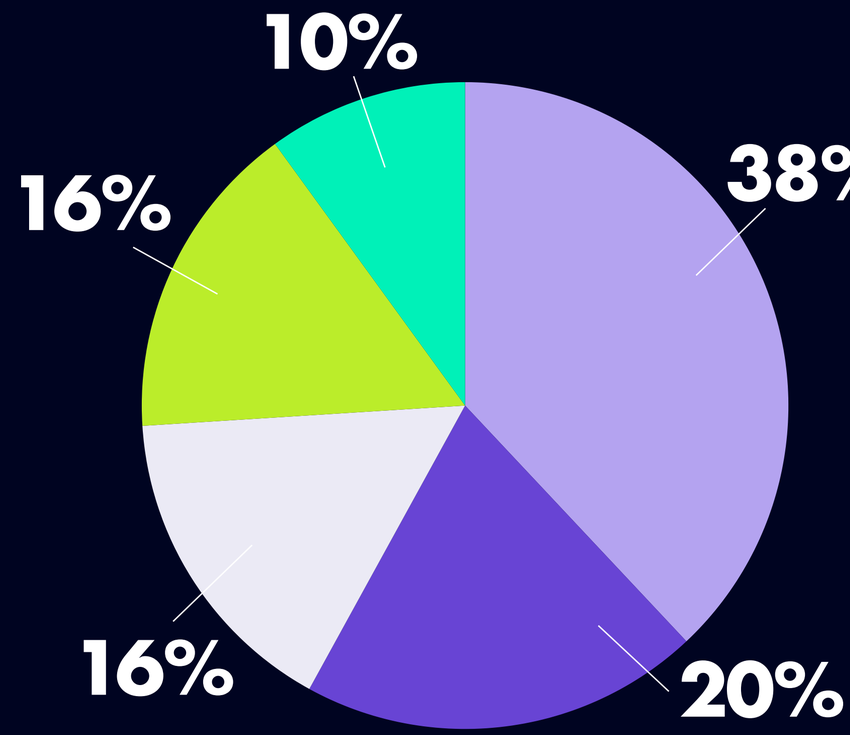
This statistic directly aligns with *The State of Continuous Controls Monitoring Report*, which found that 79.8% of CISOs believe reducing manual processing represents their biggest automation opportunity. When nearly one-fifth of organizations have achieved integration but remain burdened by manual processes, it's clear why so many security leaders identify manual processing as the critical bottleneck.

Where do you see the biggest opportunity for adding automation in your compliance and risk management programs?



SOURCE: *The State of Continuous Controls Monitoring Report*

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



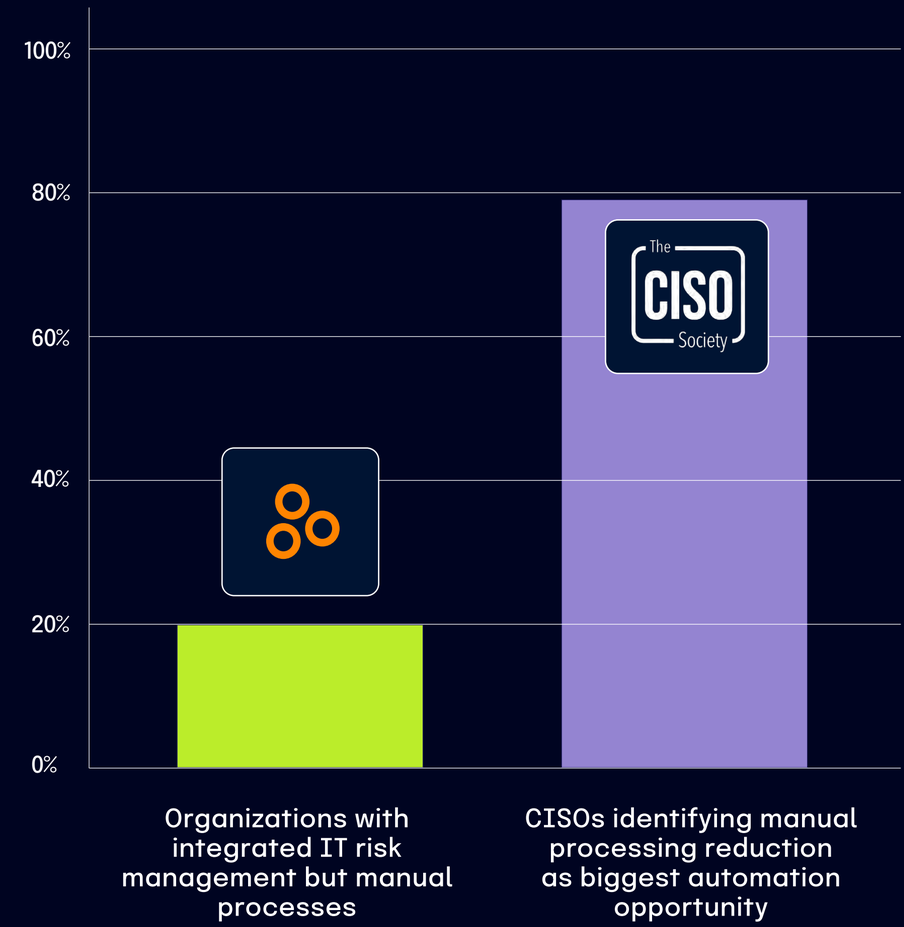
SOURCE: *The 2025 IT Risk and Compliance Benchmark Report*

hyperproof.io/it-compliance-benchmarks

These organizations have overcome the significant hurdle of breaking down departmental silos to create unified risk management approaches, but their progress is hampered by the inefficiency and error potential of manual workflows. The relationship between these findings suggests a common maturity pattern in risk management evolution: organizations first integrate their approach conceptually and organizationally, but achieving full technological integration through automation emerges as a separate, subsequent challenge.

The widespread recognition among CISOs about the importance of reducing manual processes reflects this reality that many organizations have achieved strategic alignment in risk management but continue to struggle with operational efficiency in execution.

Manual processes continue despite integrated risk management



hyperproof.io/it-compliance-benchmarks

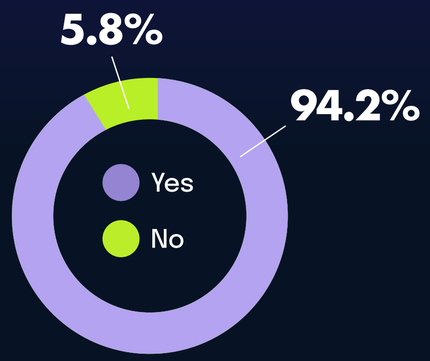
The vast majority of CISOs believe in continuous monitoring, while most organizations have already implemented related solutions

According to *The State of Continuous Controls Monitoring Report*, 94.2% of CISOs believe that continuous controls monitoring will improve both compliance and security.

The 2025 IT Risk and Compliance Benchmark Report indicates that 72% of respondents use software that monitors their security controls and reports on their compliance posture. 58% of respondents use software to continuously monitor and detect issues with security controls and the systems they use.

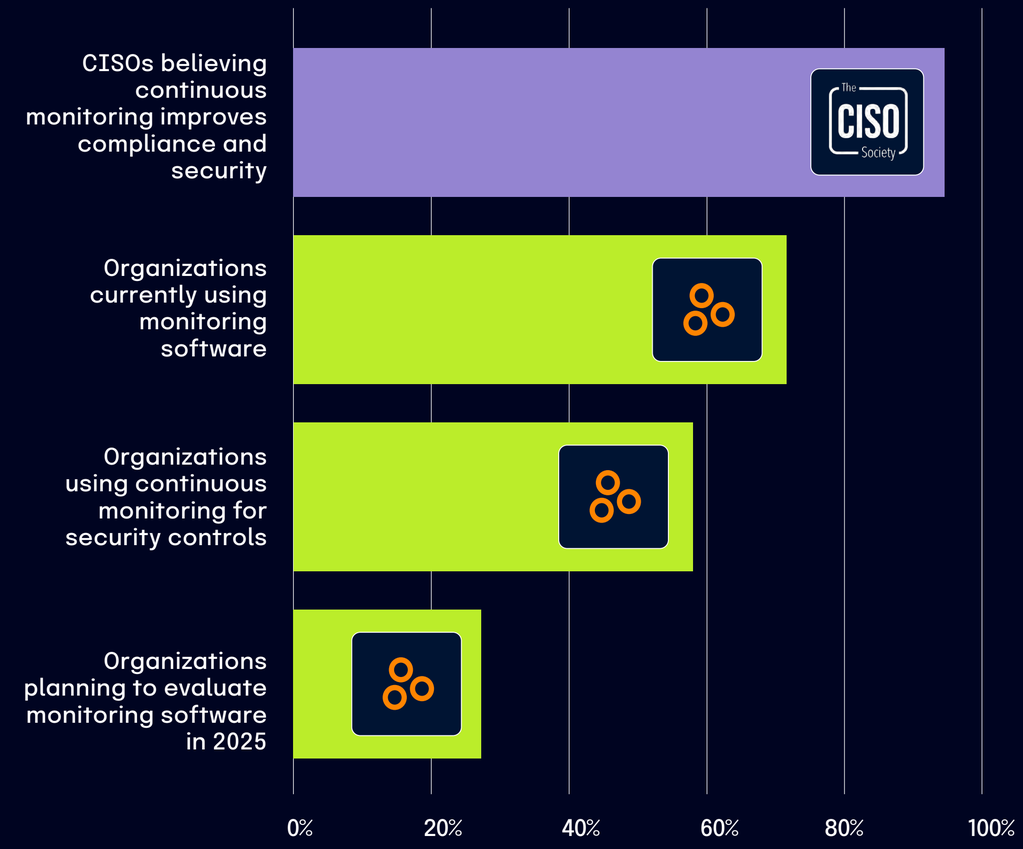
The benchmark report also found that 27% of respondents plan to evaluate these solutions in 2025. The strong belief among CISOs in the value of continuous monitoring (94.2%) is driving substantial current adoption (72%), with continued growth on the horizon as more organizations plan evaluations. While a gap remains between CISO beliefs and actual implementation, the trend clearly shows movement toward alignment between security leaders' perspectives and organizational practices in continuous controls monitoring.

Do you see continuous monitoring as improving both compliance and security?



SOURCE: *The State of Continuous Controls Monitoring Report*

Security leaders drive adoption of continuous controls monitoring



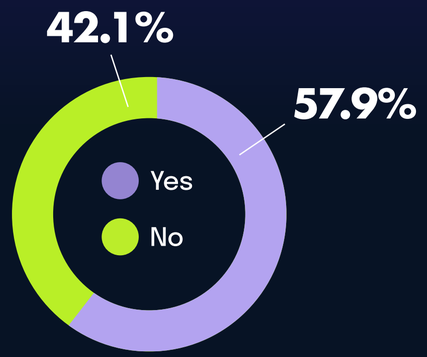
hyperproof.io/it-compliance-benchmarks

Cloud-based GRC solutions becoming standard for compliance management

According to *The 2025 IT Risk and Compliance Benchmark Report,* 42% of organizations use the compliance module within cloud-based GRC software – also known as integrated risk management solutions – to manage their IT compliance efforts. This growing adoption underscores a broader shift toward specialized cloud platforms that offer centralized governance capabilities. Complementing this trend, *The State of Continuous Controls Monitoring Report* shows that 57.9% of organizations use GRC tools to collect and maintain compliance evidence, reinforcing the increasing reliance on purpose-built technology to manage compliance complexity.

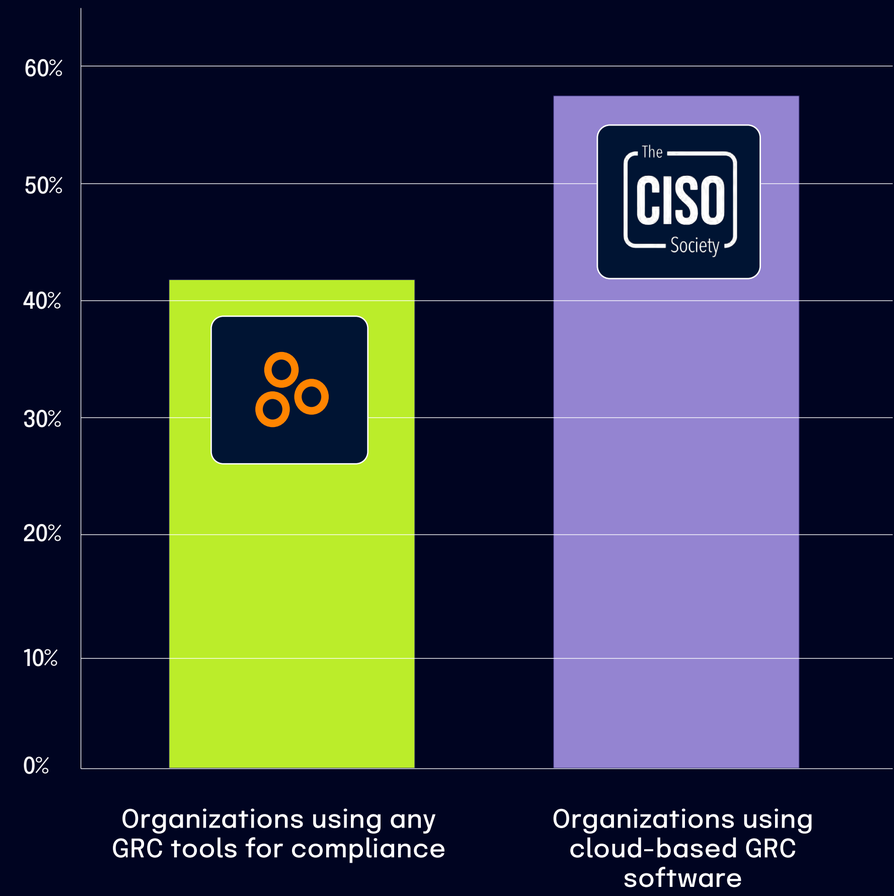
Cloud-based compliance modules now represent a substantial portion of the GRC technology landscape. While nearly 58% of organizations use GRC tools for evidence management, 42% specifically rely on cloud deployments – indicating a strong preference for scalable, accessible solutions. As compliance demands continue to evolve, organizations are moving away from general-purpose tools in favor of platforms designed to streamline and automate compliance workflows. These solutions offer key advantages such as centralized oversight, real-time updates, and easier collaboration for distributed teams, making them an increasingly essential part of modern compliance strategies.

Are you using GRC tool(s) to collect and maintain compliance evidence?



SOURCE: *The State of Continuous Controls Monitoring Report*

Cloud-based GRC software gains momentum



hyperproof.io/it-compliance-benchmarks

Organizations increasingly leverage multiple features within their GRC platforms

According to *The 2025 IT Risk and Compliance Benchmark Report,* 32% of organizations use features within their GRC software to track decisions based on risk, highlighting how many are extending the value of their governance platforms beyond basic compliance. This trend aligns with findings from *The State of Continuous Controls Monitoring Report*, which shows that 57.9% of organizations use GRC tools to collect and maintain compliance evidence. Together, these statistics show a common adoption pattern: organizations often begin using GRC platforms for compliance documentation and later expand into more advanced risk management capabilities.

The gap between these two usage rates – 57.9% for compliance evidence versus 32% for risk-based decision tracking – suggests that **while GRC tools are widely adopted for foundational compliance tasks, a growing number of organizations are maturing in their use of platform features.** By leveraging multiple capabilities within a single solution, security and compliance teams can build more integrated processes that connect regulatory obligations with informed risk decisions. This progression signals an important shift from single-purpose implementations to more holistic governance strategies, maximizing the return on investment in GRC technology.

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

FRESH FACT

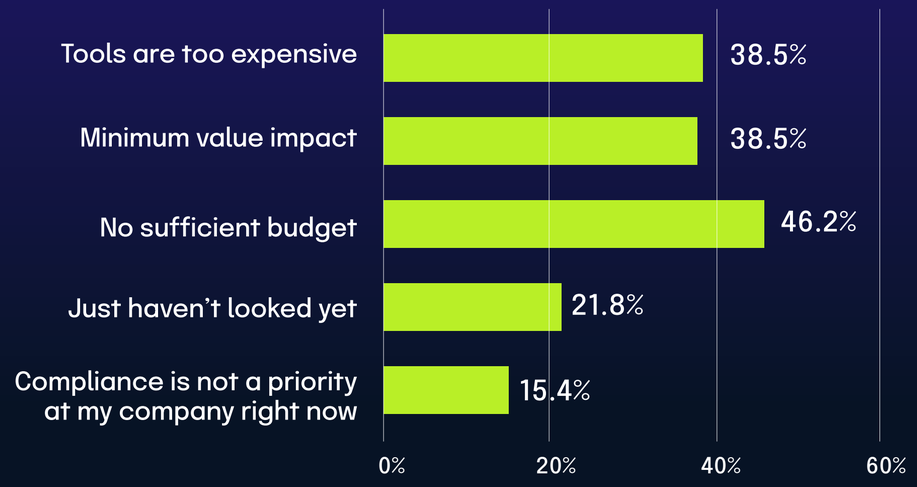
How respondents use GRC platforms

hyperproof.io/it-compliance-benchmarks

Budget constraints drive many organizations to forego dedicated GRC tools

According to *The State of Continuous Controls Monitoring Report*, 46.2% of organizations identify insufficient budget as the primary barrier to implementing dedicated GRC tools. This aligns with data from *The 2025 IT Risk and Compliance Benchmark Report*, where 14% of respondents still rely on basic productivity tools – such as spreadsheets, documents, and file storage systems – to manage IT compliance. Together, these findings demonstrate how financial constraints significantly shape the technology choices organizations make for compliance management.

What is preventing you from using GRC tools to collect and maintain compliance evidence?



SOURCE: *The State of Continuous Controls Monitoring Report*

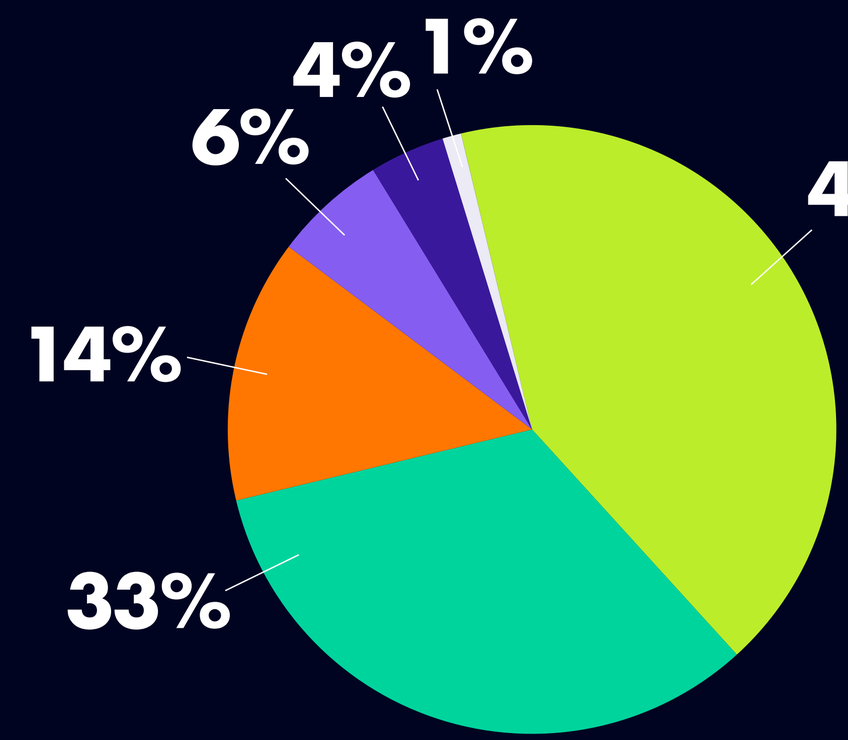
Budget constraints shape GRC technology

hyperproof.io/it-compliance-benchmarks

While basic office tools offer familiarity and no additional cost, they lack the advanced capabilities and scalability of purpose-built GRC platforms. The gap between the 46.2% facing budget limitations and the 14% using basic tools suggests that many organizations seek alternative solutions, such as open-source tools or features within existing security platforms, to meet compliance needs without incurring additional costs. These statistics underscore how economic pressures continue to influence compliance strategies, forcing organizations to carefully balance affordability with the need for effective, reliable governance technology.

> The gap between the 46.2% facing budget limitations and the 14% using basic tools suggests that many organizations seek alternative solutions, such as open-source tools or features within existing security platforms, to meet compliance needs without incurring additional costs.

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



SOURCE: *The 2025 IT Risk and Compliance Benchmark Report*

hyperproof.io/it-compliance-benchmarks

Cost considerations drive organizations to leverage existing IT security platforms for risk management

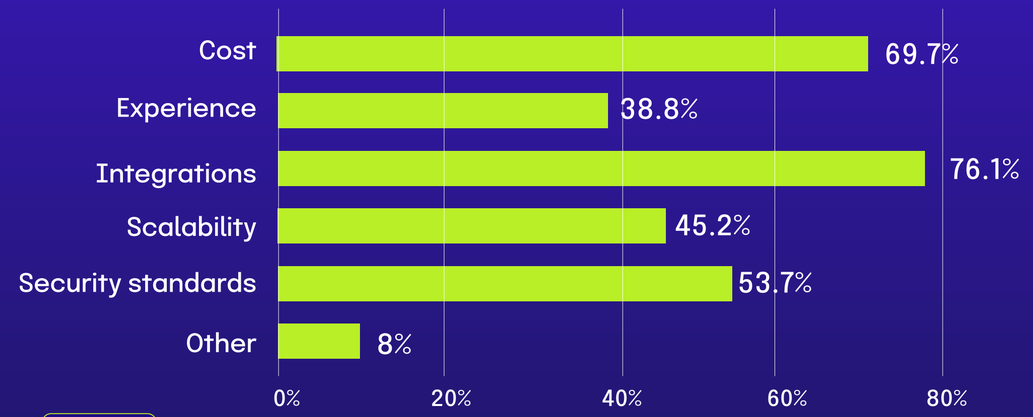
According to *The State of Continuous Controls Monitoring Report*, 69.7% of organizations prioritize cost as the most important factor when selecting security tools and vendors. This strong emphasis on financial efficiency directly connects to a key finding from *The 2025 IT Risk and Compliance Benchmark Report*: 23% of respondents use features within their existing integrated IT security platforms to track risk owners rather than implementing standalone solutions.

This correlation demonstrates how budget-conscious organizations are increasingly looking to maximize their return on technology investments. By using risk management capabilities embedded within platforms they've already purchased, these companies avoid the additional expenses of separate GRC tools while still effectively addressing their governance needs.

When organizations have already invested in comprehensive security platforms, they naturally prefer to use the tools at hand rather than introducing new systems. This strategy allows them to maintain cost discipline while establishing formal processes for risk ownership tracking.

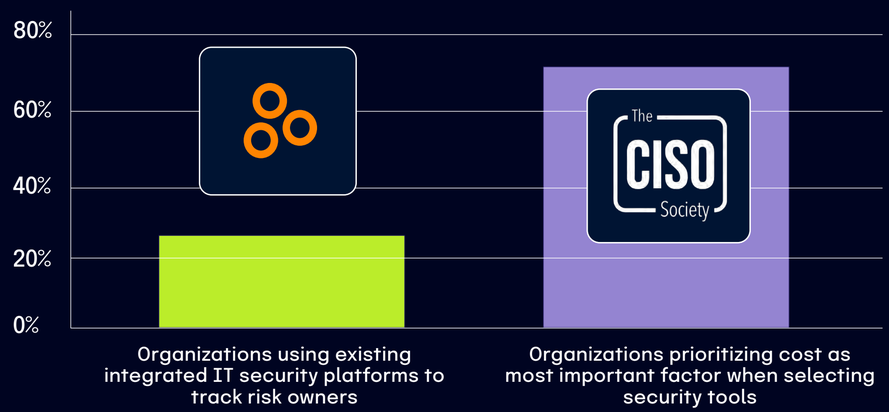
This practice represents a middle ground between basic spreadsheet-based approaches and dedicated GRC solutions, where organizations leverage existing investments to balance financial constraints with governance requirements. As integrated platforms continue expanding their feature sets, this pragmatic approach may become increasingly common for a subset of the market with less complex regulatory needs.

What features/services are most important when selecting tools/vendors to provide governance and continuous controls monitoring?



SOURCE: *The State of Continuous Controls Monitoring Report*

Cost-conscious organizations leverage existing security platforms for risk management



CHAPTER 4

Third-Party Failures Expose Compliance Gaps

Organizations today face growing pressure to secure not only their internal operations but also their broader ecosystems of vendors, partners, and service providers. The expanding attack surface introduced by third-party relationships poses complex challenges that require targeted risk management strategies. The data paints a clear picture: according to *The Global Cybersecurity Outlook 2025 Insight Report*, 54% of large organizations cite supply chain challenges as their biggest obstacle to cyber resilience, and 30% of respondents from *The 2025 IT Risk and Compliance Benchmark Report* cite compliance violations tied to third-party oversight. Even more concerning, 60% of respondents of *The 2025 IT Risk and Compliance Benchmark Report* say they were unable to resolve audit findings related to third-party risk management in a timely manner, underscoring the difficulty of managing risks beyond their direct control.

In response, many organizations are adopting specialized tools and governance practices to strengthen third-party risk management. A notable 78% of respondents to *The 2025 IT Risk and Compliance Benchmark Report* have implemented dedicated IT vendor risk management solutions, recognizing that general security controls are insufficient for addressing supply chain vulnerabilities. Additionally, third-party risk has gained increased attention at the governance level, with 23% of boards or audit committees now reviewing it as a quarterly agenda item, according to *The 2025 IT Risk and Compliance Benchmark Report*). These trends reflect a strategic shift: organizations are moving from reactive oversight to proactive risk mitigation, supported by purpose-built technology and stronger board engagement. The insights in this chapter help GRC and cybersecurity professionals benchmark their efforts and identify best practices for transforming third-party relationships into secure, compliant partnerships.

More than half of large organizations struggle with supply chain challenges while the vast majority implement specialized solutions for third-party risk management

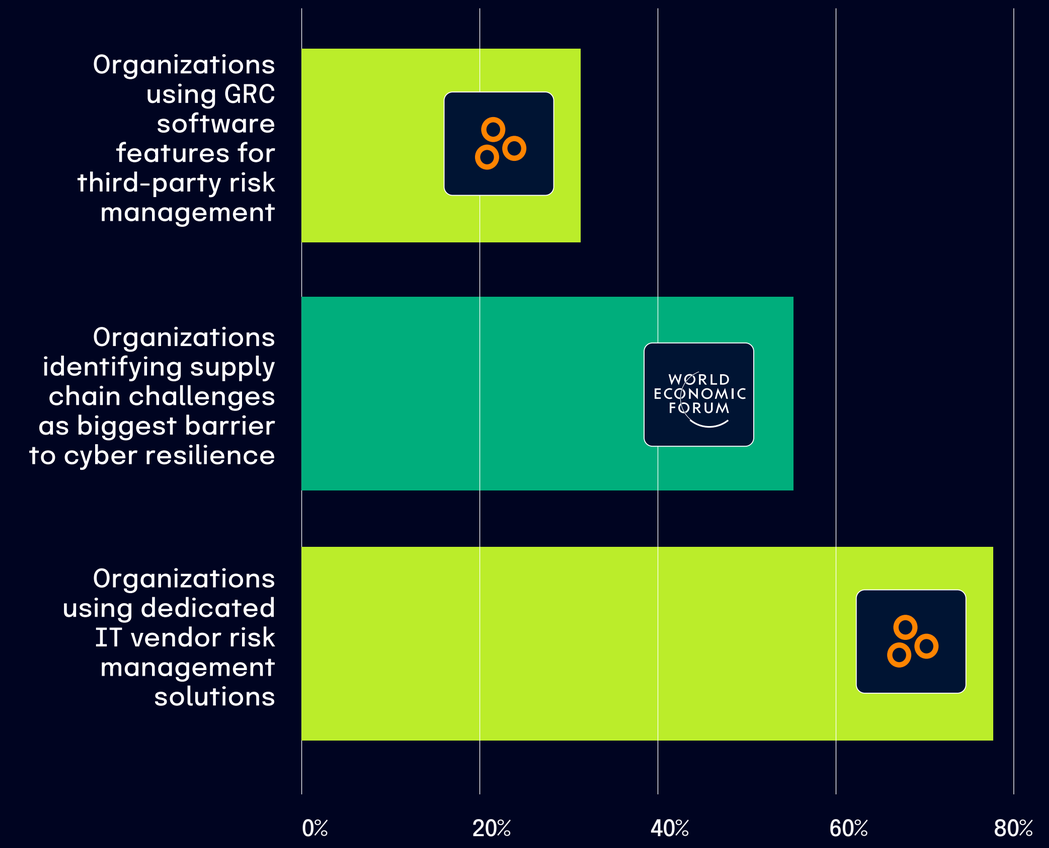
According to *The Global Cybersecurity Outlook 2025 Report*, 54% of large organizations identified supply chain challenges as the biggest barrier to achieving cyber resilience. This widespread concern about supply chain vulnerabilities appears to be driving significant investment in specialized risk management tools.

In response to these third-party risks, organizations are implementing various technology solutions, according to *The 2025 IT Risk and Compliance Benchmark Report*. The data shows that 78% of respondents use dedicated IT vendor risk management (VRM) solutions specifically designed to identify and manage IT risks from their third parties. Meanwhile, 32% of respondents rely on other features within GRC software solutions to address these same concerns.

As organizations recognize supply chain vulnerabilities as a major obstacle to cyber resilience, they're prioritizing specialized software solutions to manage third-party risk. The high adoption rate of dedicated IT VRM solutions (78%) suggests most organizations prefer purpose-built tools when tackling what the World Economic Forum identifies as their biggest security challenge.

The substantial difference between dedicated VRM adoption (78%) and the use of GRC software features (32%) shows that organizations generally prefer specialized tools over more generalized risk management solutions when addressing supply chain vulnerabilities. This preference likely reflects the complex and multifaceted nature of modern supply chain risks that demand focused attention and specialized capabilities.

Supply chain vulnerabilities drive risk management adoption



hyperproof.io/it-compliance-benchmarks

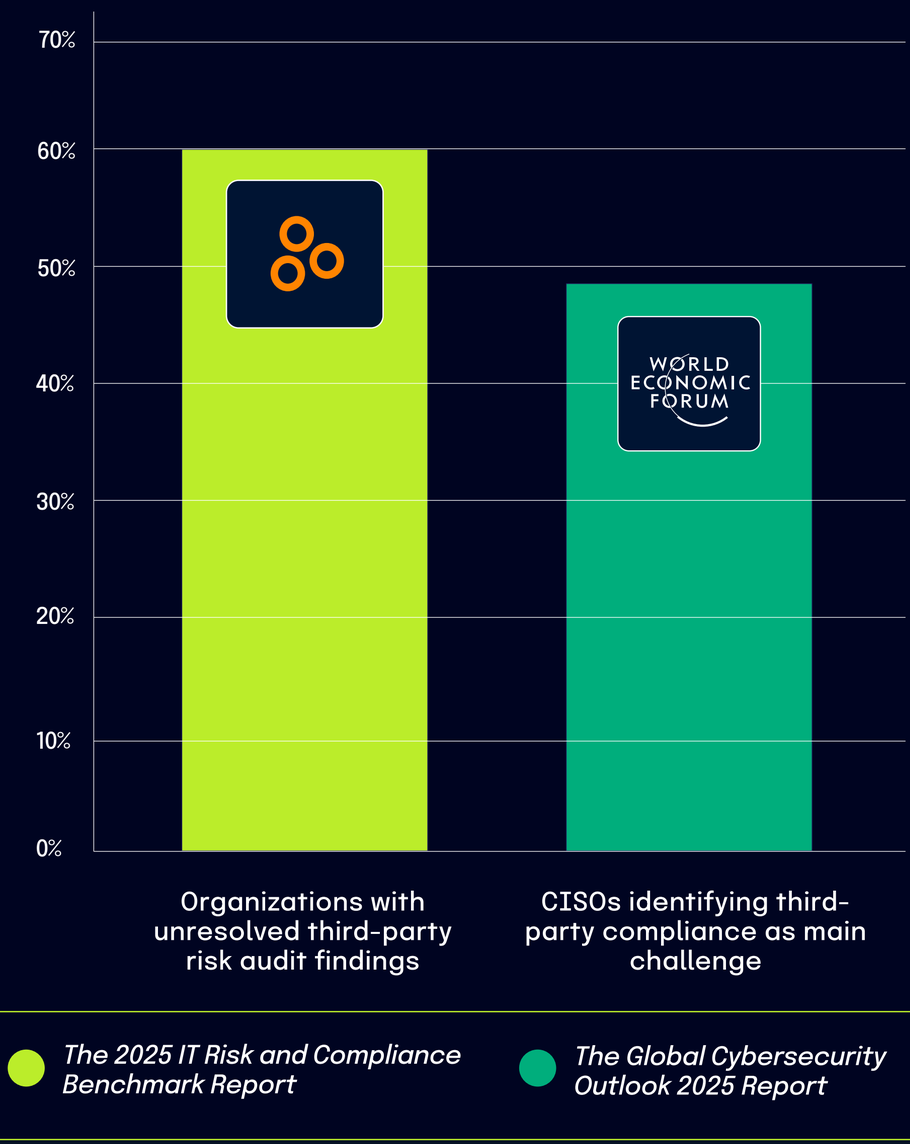
Unresolved third-party risk findings affect majority of organizations

According to *The 2025 IT Risk and Compliance Benchmark Report*, 60% of respondents have experienced an audit finding related to third-party risk management they couldn't promptly resolve. This widespread challenge highlights the persistent difficulties organizations face when addressing third-party risk gaps identified during audits.

The root cause of these unresolved findings becomes clearer when compared with data from *The Global Cybersecurity Outlook 2025 Insight Report*. According to this report, 48% of participating CISOs identify ensuring third-party compliance with security requirements as their main challenge in effectively implementing cyber regulations.

The connection between these statistics demonstrates why third-party risk management findings prove so difficult to remediate. When nearly half of security leaders struggle to enforce their security requirements with third parties, it naturally follows that a majority experience lingering audit issues in this area. This relationship illustrates how dependencies on external entities create unique governance challenges that differ significantly from internal control remediation.

Third-party compliance requirements limit audit finding resolution

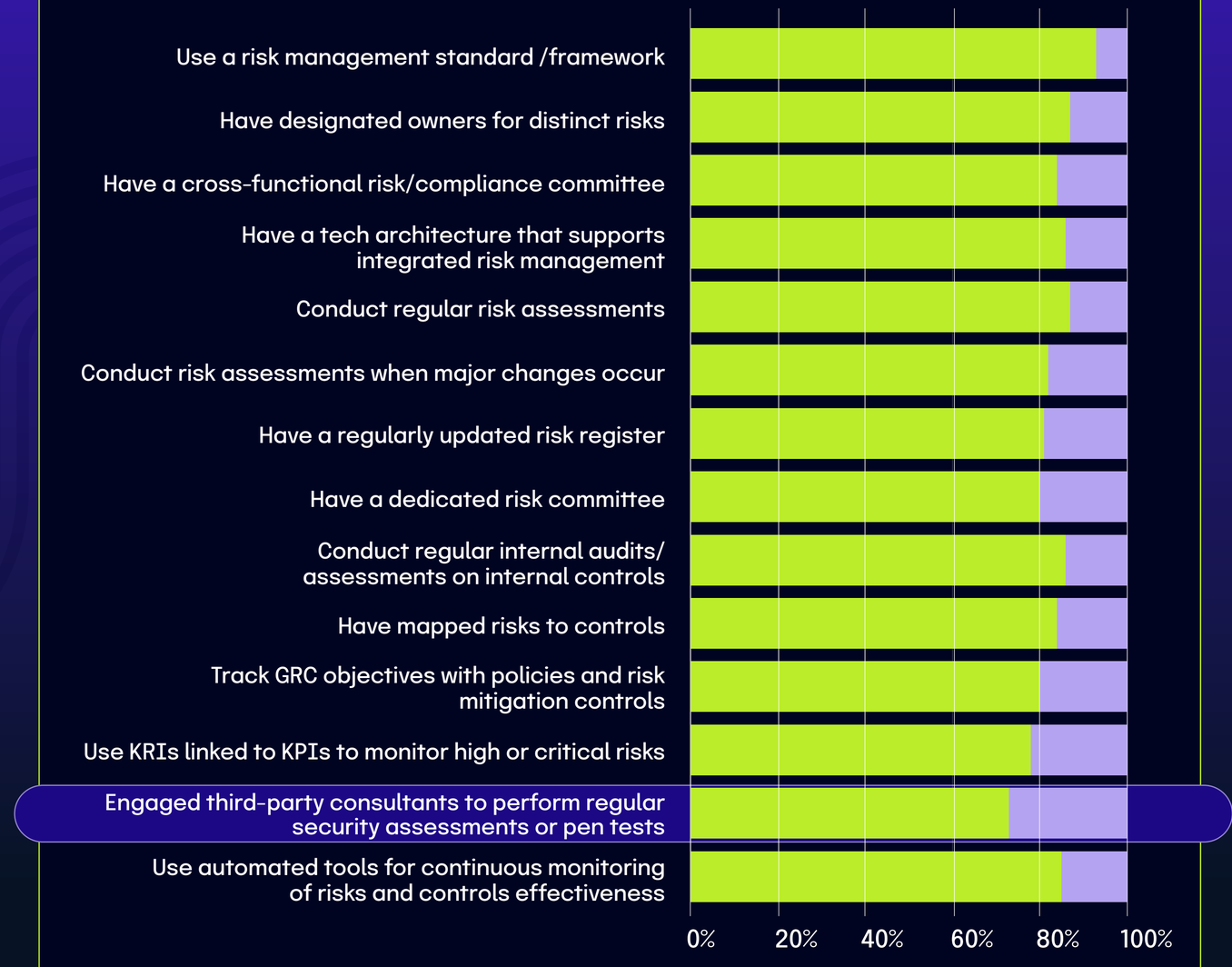


hyperproof.io/it-compliance-benchmarks

73% of organizations engage third-party security assessments, while 45% of board directors specifically seek external evaluations

The 2025 IT Risk and Compliance Benchmark Report found that 73% of surveyed organizations have engaged third-party consultants to perform regular security assessments or penetration tests. This high percentage demonstrates that external security validation has become a standard practice for most organizations seeking an objective evaluation of their security posture.

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



SOURCE: *The 2025 IT Risk and Compliance Benchmark Report*

hyperproof.io/it-compliance-benchmarks

This finding becomes more meaningful when compared with *The 2024 BDO Board Survey*, which found that 45% of directors specifically look to external assessments to evaluate their organization's security. The difference between these percentages reflects the distinct populations surveyed in each report.

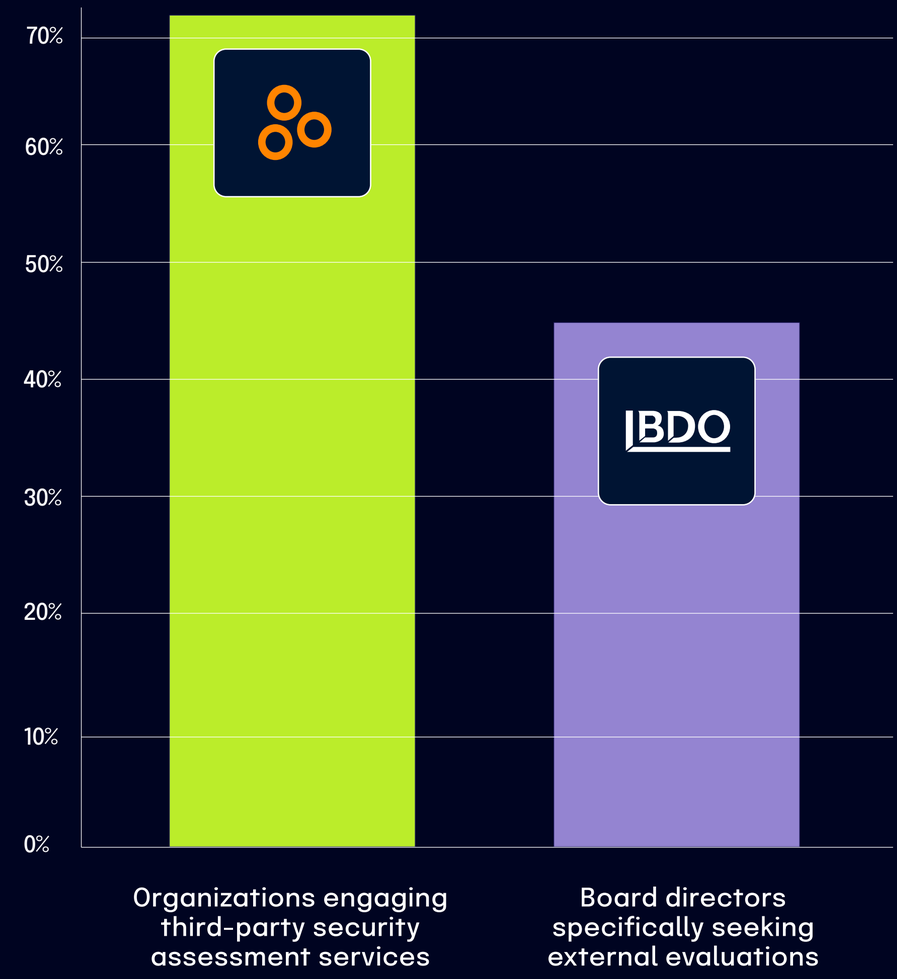
While nearly three-quarters of organizations have implemented third-party security assessments as an operational practice, the board-level perspective captured in the BDO survey shows that less than half of directors personally focus on these external evaluations. This distinction highlights the different priorities and visibility across organizational levels. Security and IT teams have typically already implemented these practices, while board attention spans numerous governance concerns.

Security practices often gain widespread adoption at operational levels before becoming a specific focus of board-level oversight. As cyber risks continue to escalate, the gap between organizational implementation (73%) and board-level focus (45%) will likely narrow as directors increasingly recognize the value of independent security validation.

FRESH FACT

45% of directors specifically look to external assessments to evaluate their organization's security

Organizations hiring external security assessment consultants



hyperproof.io/it-compliance-benchmarks

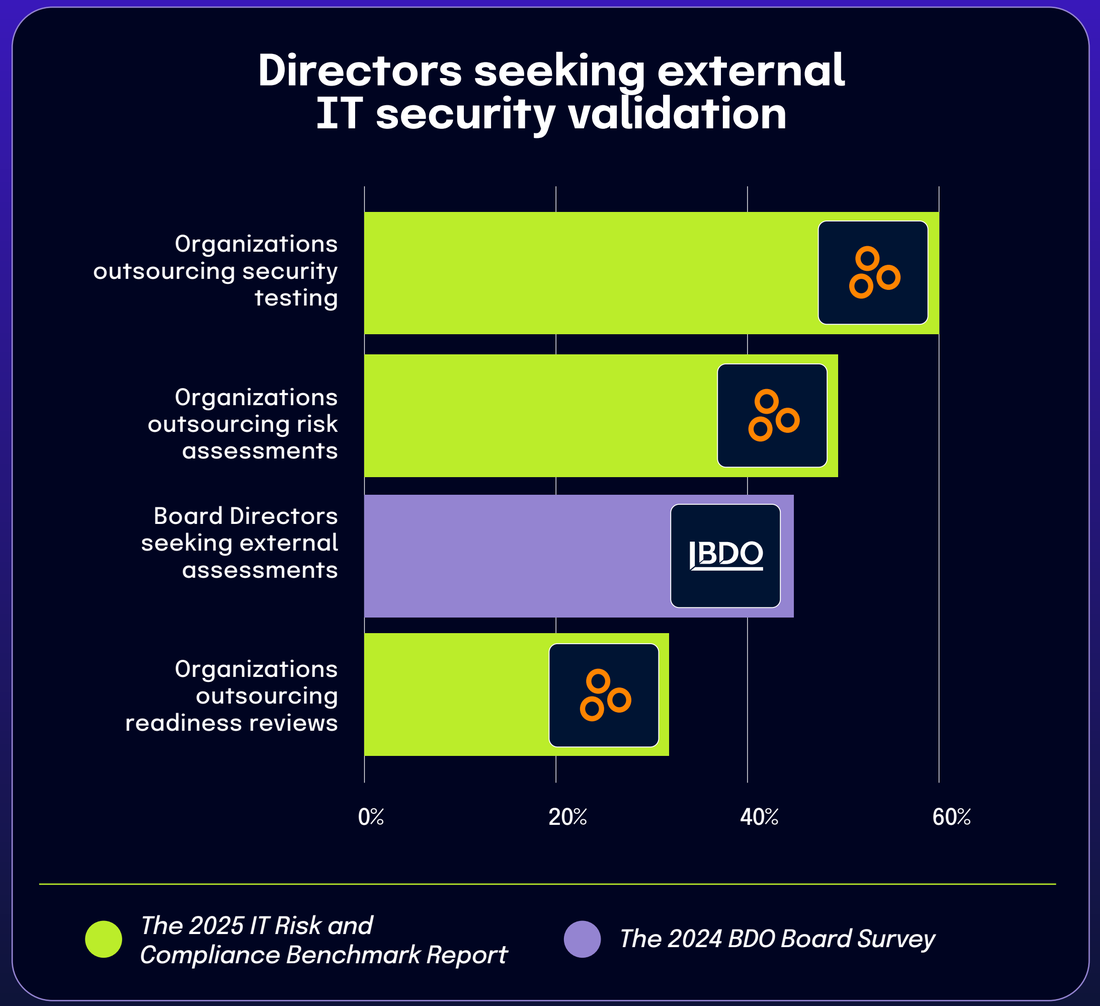
Nearly half of directors rely on external assessments while the majority of organizations outsource critical security functions

According to *The 2024 BDO Board Survey*, 45% of directors are seeking external assessments to ensure their IT systems and related controls can effectively protect against persistent cyber threats. This board-level priority appears to be directly influencing organizational behavior across multiple security and compliance functions.

The 2025 IT Risk and Compliance Benchmark Report captures how this governance focus translates into specific outsourcing practices. According to the data, 60% of respondents outsource security testing, including vulnerability scans and penetration testing, to consulting or security and compliance advisory firms. This represents the most commonly outsourced security function among those surveyed.

Additionally, 48% of respondents outsource risk assessments to external firms, according to *The 2025 IT Risk and Compliance Benchmark Report*. The close alignment between this figure and the 45% of directors seeking external assessments (from *The 2024 BDO Board Survey*) suggests a direct connection between board-level intentions and organizational actions. This correlation establishes a clear pattern where governance priorities directly drive specific security outsourcing decisions.

According to *The 2025 IT Risk and Compliance Benchmark Report*, 32% of organizations outsource readiness reviews (gap assessments) to consulting firms. While this represents a smaller percentage than other outsourced functions, it remains significant and aligns with the overall board-level interest in external validation.



Board governance concerns about cyber threats are manifesting in organizational practices. The substantial outsourcing rates across all three security functions, testing, risk assessment, and gap analysis reflect an increasing reliance on external expertise to address complex security challenges. This trend shows how board-level risk awareness drives operational decisions, with organizations seeking third-party validation at rates that closely mirror directors' stated priorities.

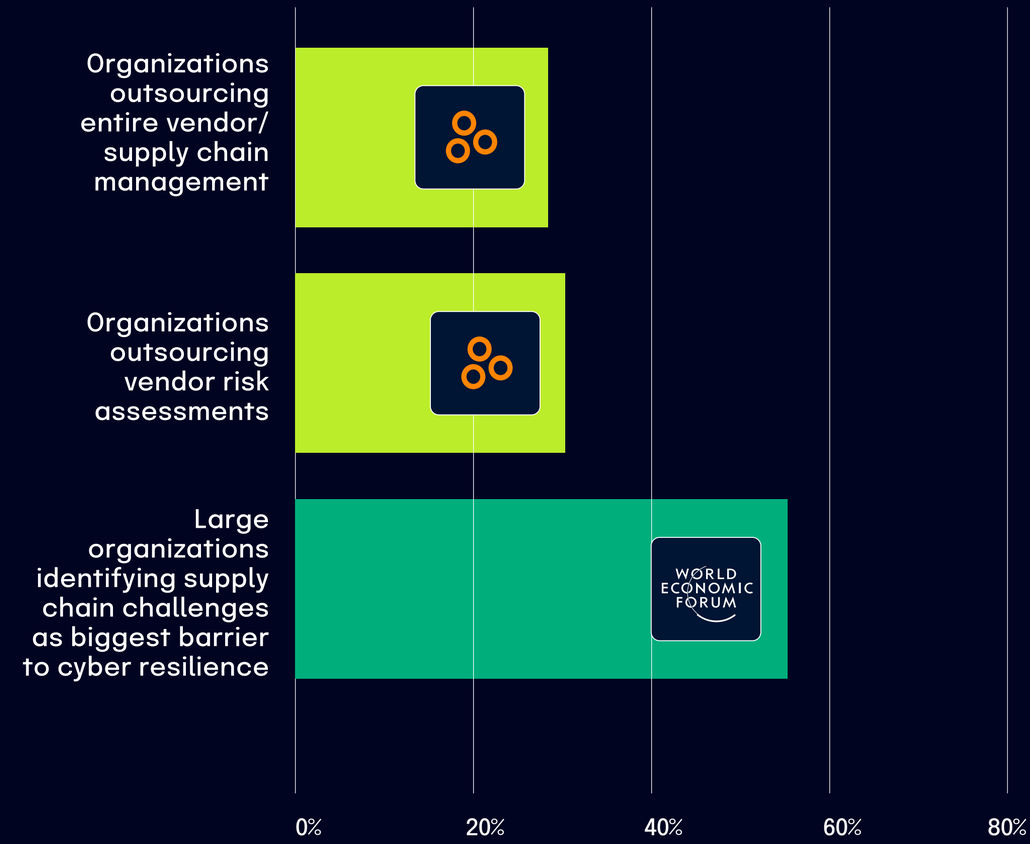
More than half of large organizations face significant supply chain challenges, while nearly a third outsource related risk management functions

According to *The Global Cybersecurity Outlook 2025 Report*, 54% of large organizations identified supply chain challenges as the biggest barrier to achieving cyber resilience. This widespread concern about third-party risk is driving organizations to outsource key management functions.

The 2025 IT Risk and Compliance Benchmark Report shows that 30% of respondents outsource vendor risk assessments to consulting, security, and compliance advisory firms. This represents a significant portion of organizations seeking external expertise specifically to evaluate their vendors' and supply chain partners' security postures.

Similarly, the benchmark report shows that 28% of organizations outsource their entire vendor/supply chain management function to external consulting and advisory firms. This closely related statistic demonstrates that organizations aren't just seeking help with assessing vendor risks but also with managing their overall supply chain security operations.

Supply chain challenges impacting organizational cyber resilience



hyperproof.io/it-compliance-benchmarks

As organizations grapple with what the World Economic Forum identifies as their biggest barrier to cyber resilience, approximately a third are turning to external expertise to manage these complex risks. The similar percentages between those outsourcing vendor risk assessments (30%) and those outsourcing broader supply chain management (28%) suggest a consistent approach to addressing these challenges.

These findings highlight how supply chain security concerns are driving significant changes in how organizations structure their risk management operations. Rather than building internal capabilities to address these complex challenges, a substantial minority are partnering with specialized consulting firms to leverage their expertise in assessing and managing third-party relationships.

FRESH FACT

54%

of large organizations highlight supply chain challenges as the greatest barrier to achieving cyber resilience

The main organizational challenges to cyber resilience

Small organizations	Medium organizations	Large organizations
01 Complex and evolving threat landscape	**01 Complex and evolving threat landscape**	01 Third-party risk management
02 Skills shortage	02 Third-party risk management	**02 Complex and evolving threat landscape**
03 Lack of incident response preparedness	03 Complexity of environments (e.g. IT, OT, IoT)	03 Complexity of environments (e.g. IT, OT, IoT)

SOURCE: *The Global Cybersecurity Outlook 2025 Report*

CHAPTER 5

Finding Risk Data Shouldn't Be So Hard

Enterprises rely on seamless information flow for informed risk decision-making, yet many organizations remain hampered by fragmented systems, siloed processes, and disconnected data sources. This lack of integration creates critical blind spots that weaken even the most carefully designed governance frameworks. According to *The State of Continuous Controls Monitoring Report*, 42% of organizations cite data and system silos as a significant challenge, and 39% report difficulty locating risk information when needed. These closely linked issues demonstrate how disjointed technical architectures directly hinder operational efficiency, forcing security and compliance teams to spend time tracking down data instead of proactively managing risk.

Resource limitations further intensify these challenges. With 44% of organizations, according to *The State of Continuous Controls Monitoring Report*, identifying budget and staffing constraints as their primary security operations hurdle, many teams are stuck in reactive cycles – highlighted by the 16% of respondents who manage IT risk only in response to negative events.

These statistics paint a picture of organizations struggling to balance short-term needs with the longer-term investments required to improve their risk management infrastructure. The connection between technical fragmentation and operational inefficiency emphasizes that architecture decisions are not just IT concerns – they're foundational to building mature, enterprise-wide risk capabilities. For GRC leaders, understanding and addressing these underlying barriers is key to moving from reactive risk management toward a more integrated, strategic approach.

42% of organizations struggle with data and system silos, creating fragmented risk management approaches

According to *The State of Continuous Controls Monitoring Report*, 42% of organizations face significant challenges due to data and system silos. This widespread technical and organizational fragmentation creates fundamental obstacles for integrated security and risk management approaches.

This broader system-level fragmentation directly impacts how organizations structure their risk management functions. According to *The 2025 IT Risk and Compliance Benchmark Report*, 16% of organizations manage IT risk through siloed departments, processes, and tools. The technical silos mentioned in *The State of Continuous Controls Monitoring Report* essentially create the conditions for the organizational silos observed in *The 2025 IT Risk and Compliance Benchmark Report*.

When critical systems and data exist in isolated environments that don't effectively communicate with each other, organizations naturally develop parallel risk management structures that mirror these technical divisions. This creates multiple disconnected approaches to risk across different business units instead of a cohesive, enterprise-wide strategy.

The relationship between these findings demonstrates how **technical architecture decisions shape organizational behavior and risk management practices.** While *The State of Continuous Controls Monitoring Report* identifies the broader challenge of system and data fragmentation, *The 2025 IT Risk and Compliance Benchmark Report* points to a related consequence: the development of disconnected risk management functions that independently address threats within their own domains without sufficient coordination across the enterprise.

Organizations managing IT risk through siloed departments

hyperproof.io/it-compliance-benchmarks

39% of organizations struggle to find risk information when needed, mirroring the 42% challenged by data silos

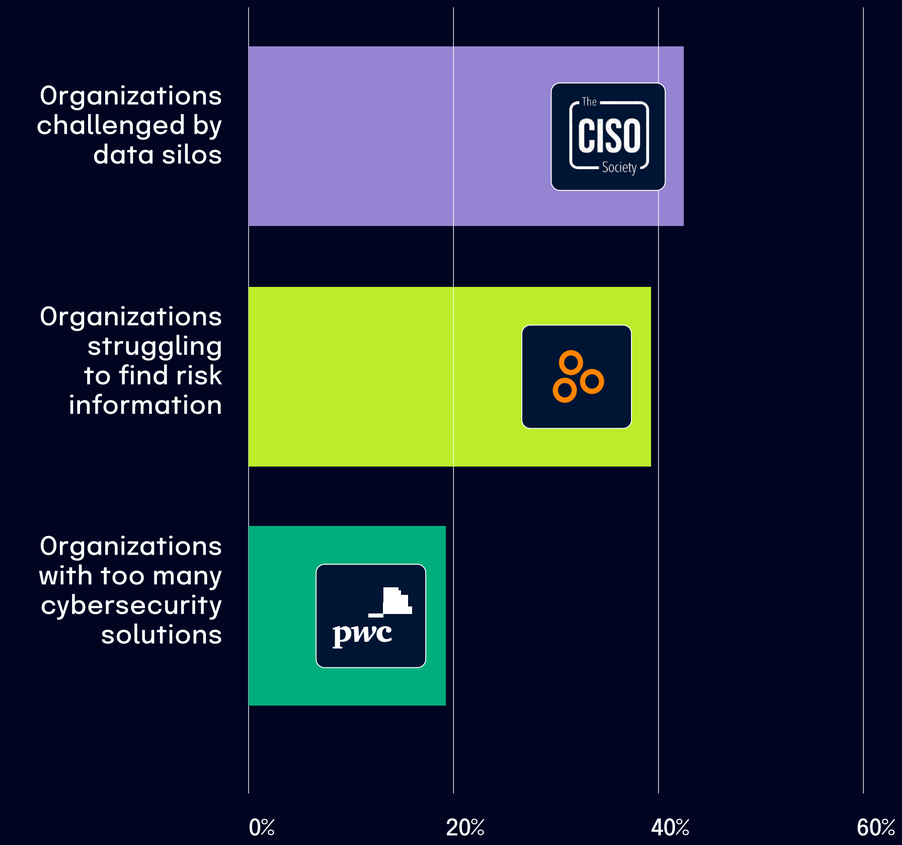
According to *The 2025 IT Risk and Compliance Benchmark Report*, 39% of organizations struggle to locate risk-related information when needed, primarily because data is scattered across multiple spreadsheets and systems. This statistic represents a significant operational challenge that hampers timely risk decision-making.

This difficulty in finding risk information closely aligns with *The State of Continuous Controls Monitoring Report,* where 42% of organizations face challenges from data and system silos. These nearly identical percentages likely represent two perspectives on the same fundamental problem: **fragmented information architecture creates persistent barriers to accessing critical risk data at the moment it's needed.**

Additionally, *The 2024 Global Digital Trust Report* states that 19% of organizations report having too many cybersecurity solutions. While this percentage is lower, it points to a key contributor to information fragmentation. Multiple security tools, each generating risk data in different formats and locations, naturally make consolidated risk information harder to locate.

The gap between organizations struggling to find information (39%) and those reporting too many tools (19%) suggests that tool proliferation is just one factor in a broader information management challenge. Organizations may face information retrieval difficulties even with a reasonable number of tools if those systems don't effectively integrate and share data.

Organizations struggling to access risk information when needed

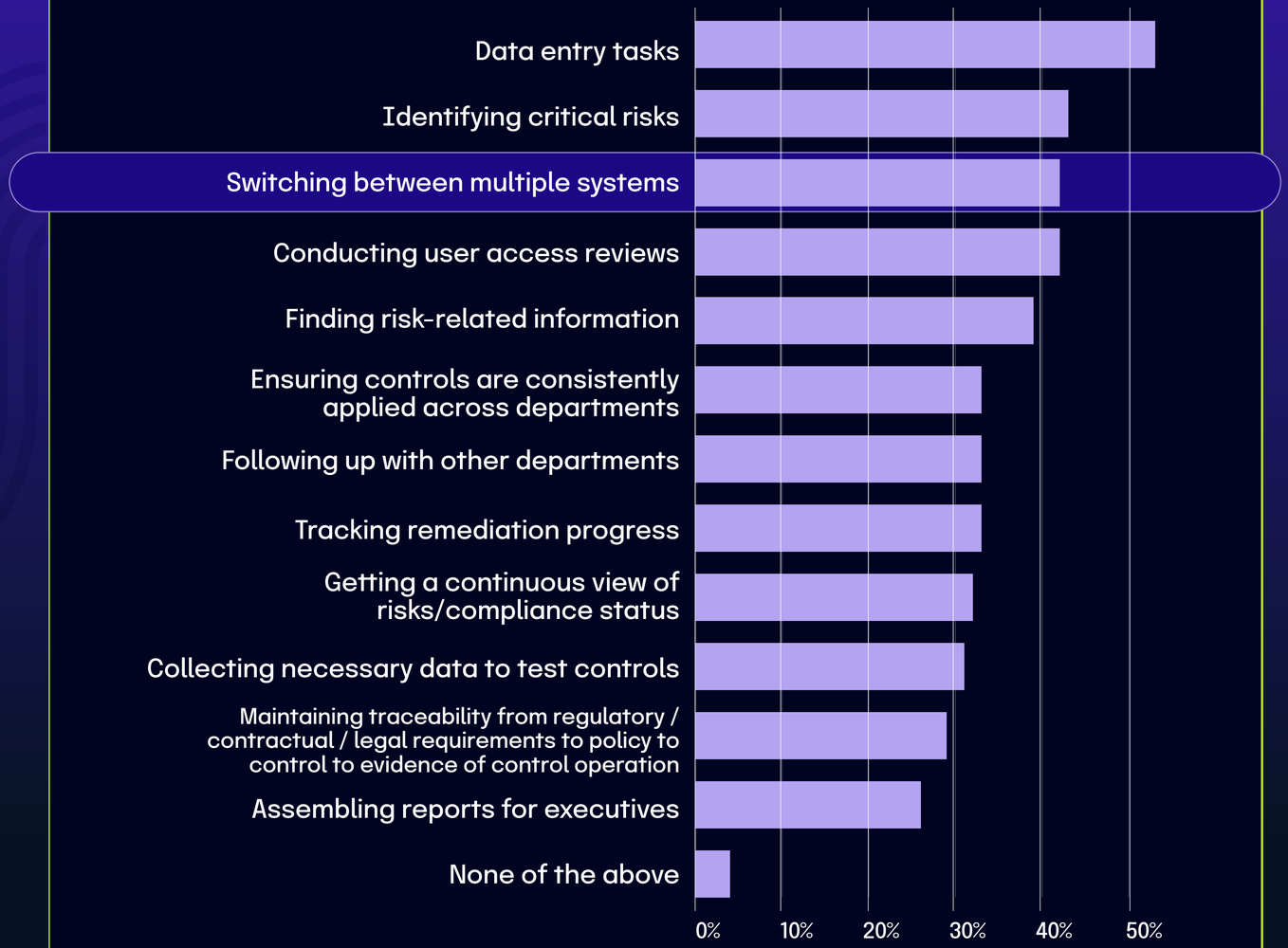


hyperproof.io/it-compliance-benchmarks

42% of organizations struggle with system switching during risk management processes, mirroring the 40.4% lacking centralized platforms

According to *The 2025 IT Risk and Compliance Benchmark Report*, 42% of organizations struggle significantly with switching between multiple systems throughout their risk management processes. This fragmentation creates operational friction as teams must navigate separate platforms for essential activities like risk assessment and remediation tracking.

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



SOURCE: *The 2025 IT Risk and Compliance Benchmark Report*

hyperproof.io/it-compliance-benchmarks

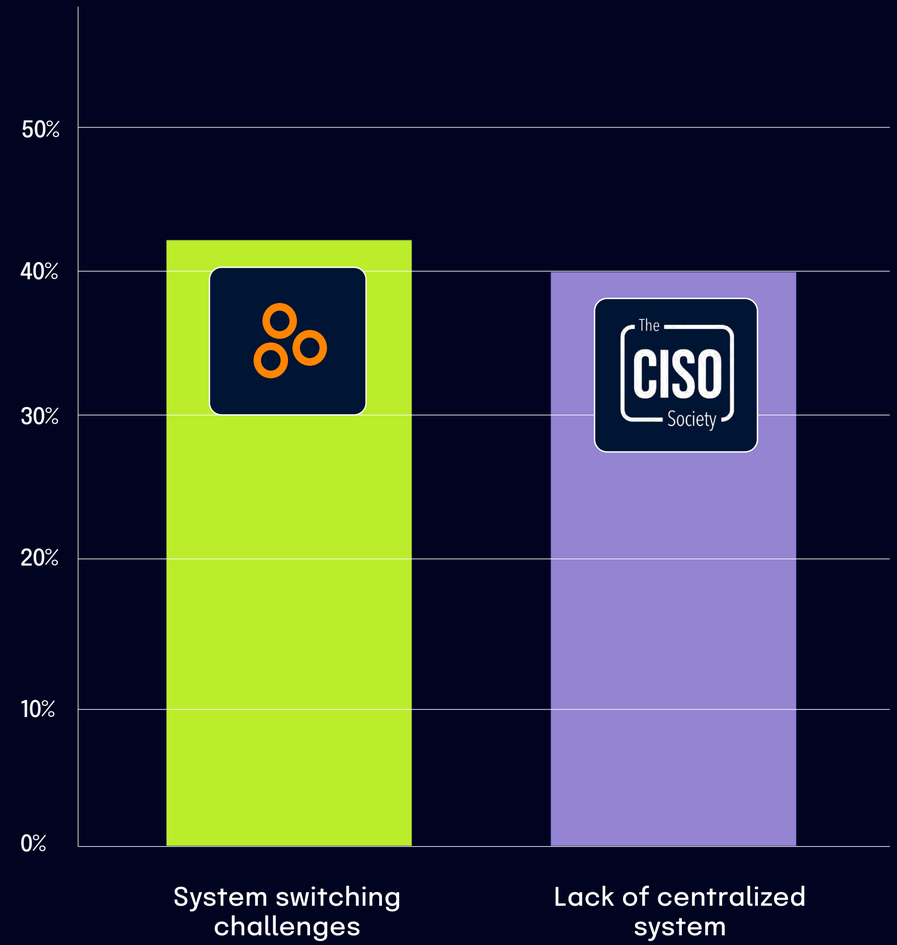
This finding closely aligns with *The State of Continuous Controls Monitoring Report*, which found that 40.4% of organizations are challenged by the lack of a centralized system for security and compliance management. These remarkably similar percentages suggest both reports are identifying the same fundamental problem from slightly different perspectives.

The connection between these statistics is straightforward: **without a centralized platform, organizations force their teams to switch between multiple disconnected systems to complete the risk management lifecycle.** This creates numerous inefficiencies, including duplicated efforts, inconsistent data, wasted time from context switching, and an increased likelihood of information slipping through the cracks.

FRESH FACT

40% of organizations are challenged by the lack of a centralized system for security and compliance management

Organizations switching between multiple risk management systems



hyperproof.io/it-compliance-benchmarks

33% of organizations struggle with cross-departmental risk information gathering, reflecting broader organizational silos

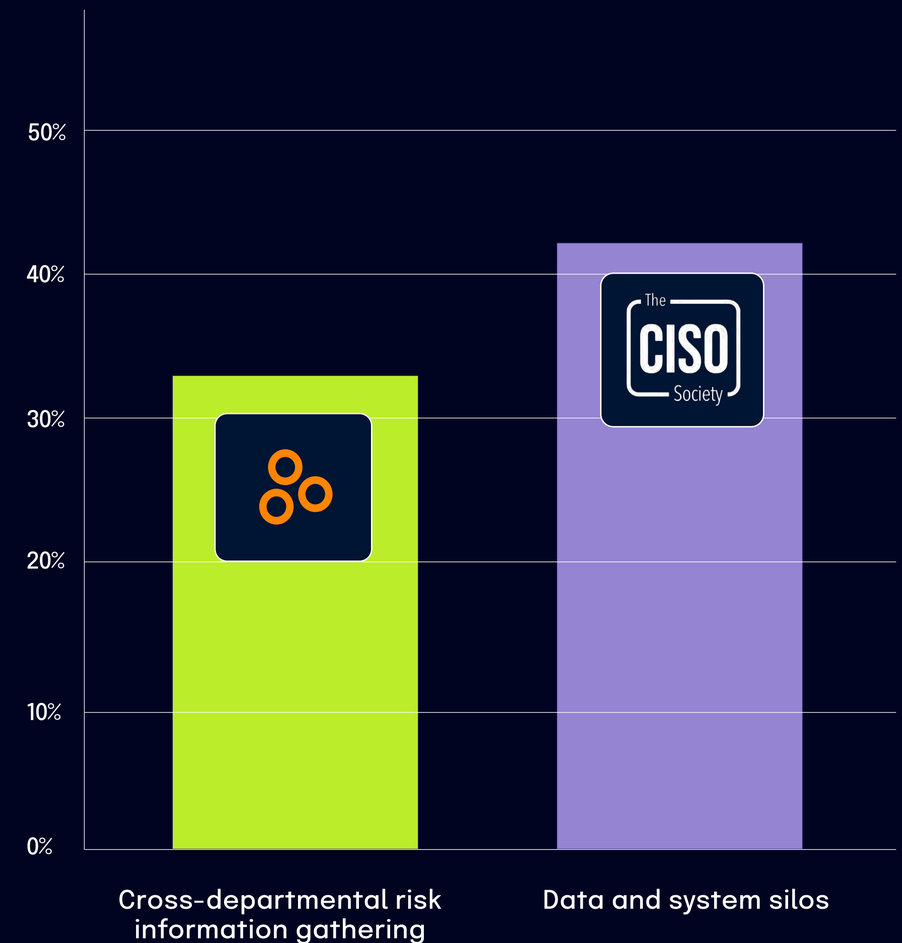
According to *The 2025 IT Risk and Compliance Benchmark Report*, 33% of organizations struggle significantly when following up with staff in other departments to gather risk information. This cross-functional collaboration challenge represents a fundamental obstacle to comprehensive risk management.

This finding aligns closely with *The State of Continuous Controls Monitoring Report*, where 42% of organizations struggle with data and system silos. The relationship between these statistics demonstrates how technical fragmentation often mirrors and reinforces organizational boundaries.

When information systems exist in silos, departments naturally develop isolated workflows and data management practices. The similar percentages between organizations reporting cross-departmental collaboration difficulties (33%) and those experiencing data silos (42%) suggest a strong correlation. Organizations with fragmented information architectures likely face greater friction in cross-functional risk management activities.

These findings illustrate how technology architecture decisions directly impact organizational behavior and risk management effectiveness. Technical silos don't just create data integration challenges, but they fundamentally shape how teams interact across departmental boundaries when managing enterprise risks.

Teams struggling to gather cross-departmental risk information



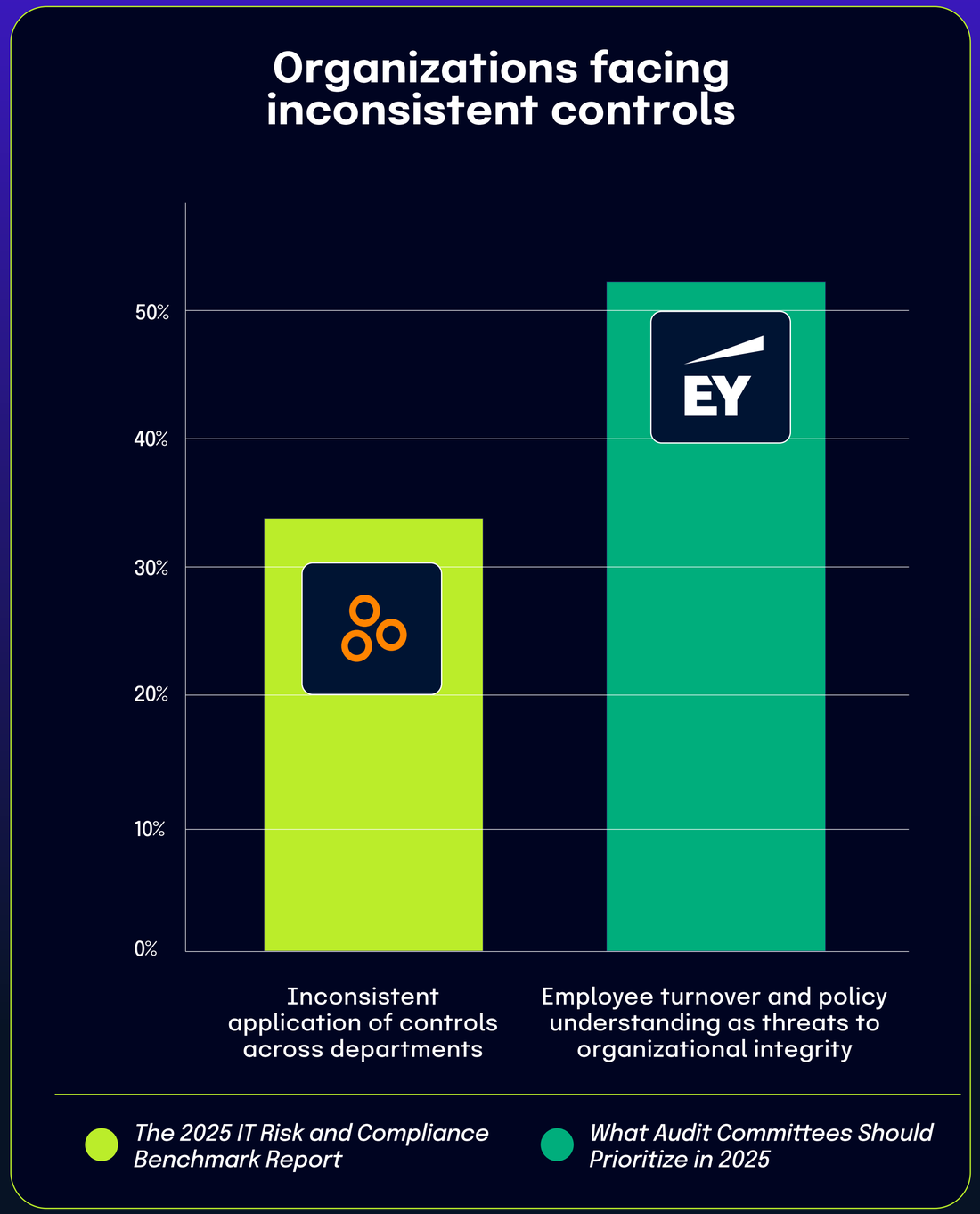
hyperproof.io/it-compliance-benchmarks

One-third of organizations struggle with consistent application of controls across departments

According to *The 2025 IT Risk and Compliance Benchmark Report*, 33% of respondents struggle with ensuring consistent application of controls across departments. This highlights a fundamental challenge in maintaining uniform risk management practices throughout organizations.

This finding becomes even more significant when paired with data from *What Audit Committees Should Prioritize In 2025*, which found that 53% of respondents identify employee turnover and policy understanding as major threats to organizational integrity. Though these statistics come from different populations, they expose a crucial connection: when employees don't fully grasp policies, inconsistent application of policy-based controls inevitably follows.

The link between staff turnover and control consistency involves multiple factors. Turnover alone doesn't necessarily cause inconsistent control application. However, when combined with inadequate procedural documentation or poor adherence to existing documentation, high turnover significantly disrupts consistent control implementation across departments. The data points to a chain reaction where staffing instability and knowledge gaps lead to inconsistent control application, undermining the organization's overall risk management effectiveness.

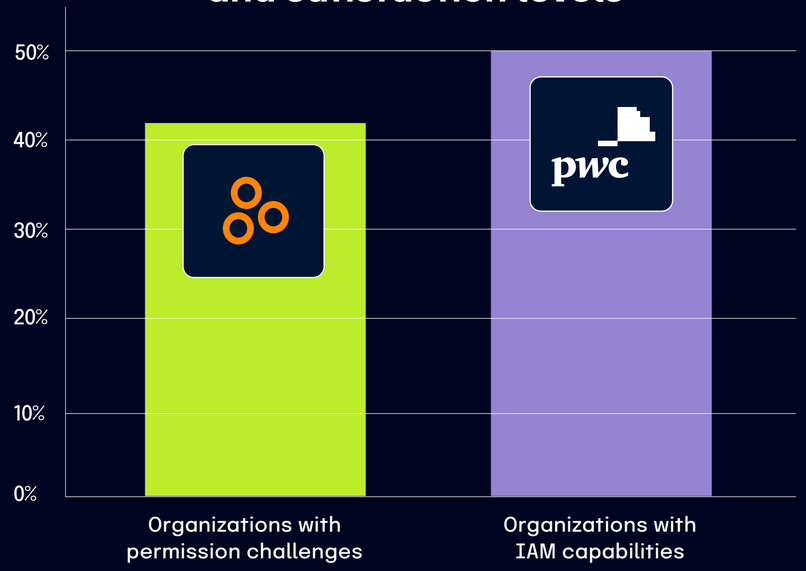


hyperproof.io/it-compliance-benchmarks

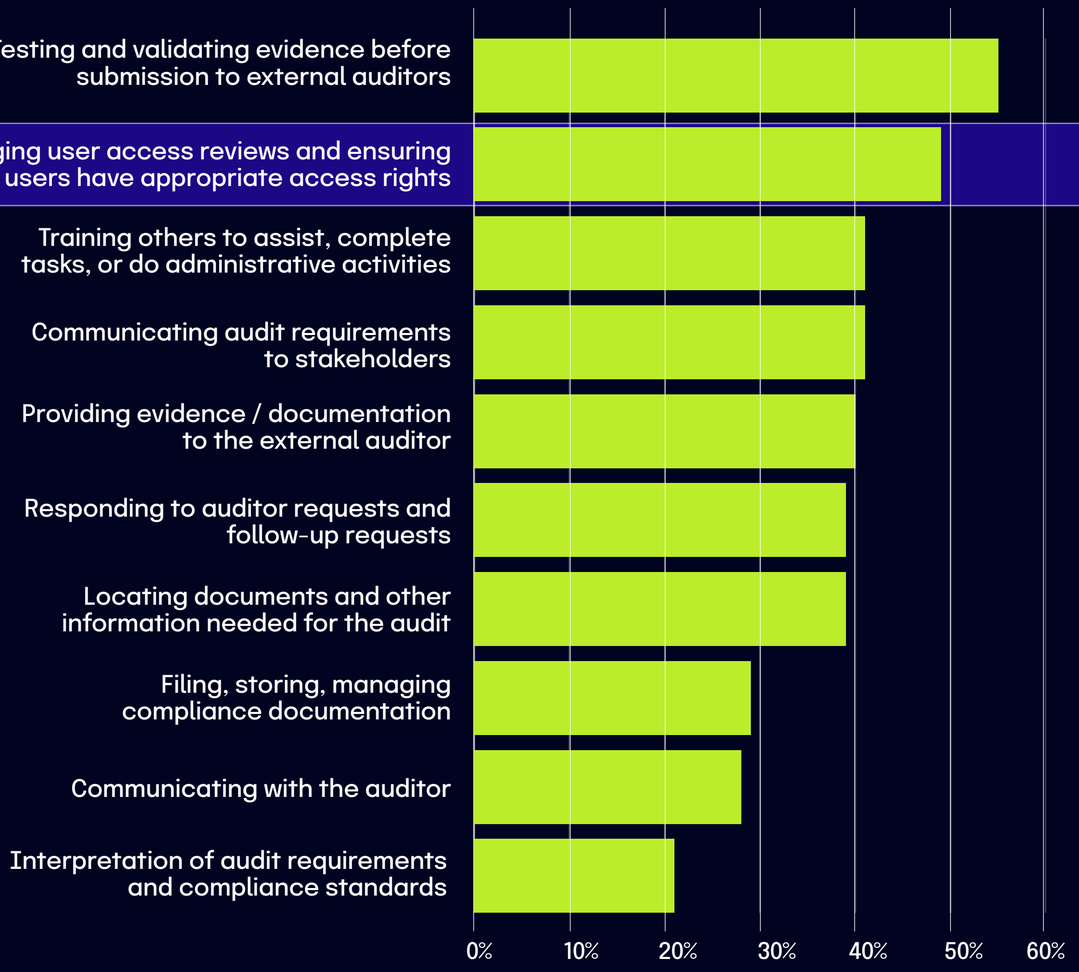
42% of organizations struggle with user permissions and access reviews, while only 50% express satisfaction with IAM capabilities

According to *The 2025 IT Risk and Compliance Benchmark Report*, 42% of organizations face significant challenges in managing user permissions and conducting user access reviews. This statistic underscores the widespread difficulties organizations encounter in maintaining appropriate access controls and governance processes.

User access management challenges and satisfaction levels



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



SOURCE: *The 2025 IT Risk and Compliance Benchmark Report*

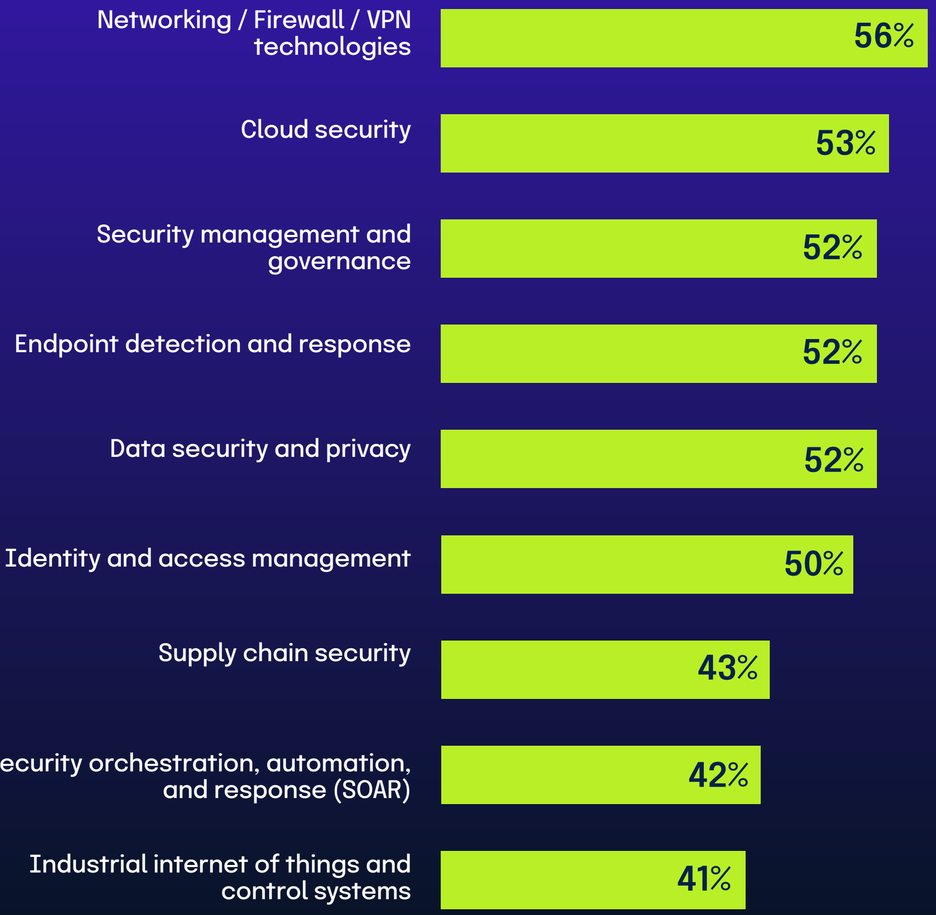
This finding aligns remarkably well with data from *The 2024 Global Digital Trust Insights Report*, which found that only 50% of security and IT respondents are satisfied with their identity and access management capabilities. The complementary nature of these findings creates a comprehensive picture of the IAM landscape across organizations.

These statistics illustrate a significant gap in identity governance maturity. With nearly half of organizations struggling with fundamental access management processes and a similar proportion expressing dissatisfaction with their IAM capabilities, it's clear that identity management remains a persistent challenge despite years of investment.

While some organizations have successfully implemented robust identity governance frameworks, a substantial portion continue to struggle with the basic mechanics of determining appropriate access rights and ensuring those rights remain suitable over time.

> **Only half of security and IT respondents are satisfied with their cybersecurity capabilities.**

Organization's technology capabilities in key cybersecurity areas



SOURCE: *The 2024 Global Digital Trust Insights Report*

44% of organizations struggle with resource constraints in IT security, leading to reactive risk management

According to *The State of Continuous Controls Monitoring Report*, 44% of organizations identified a lack of resources, budget, staffing, and personnel as their primary challenge in security operations. This resource shortage creates a significant ripple effect across IT governance structures. When teams are understaffed or underfunded, they're forced to make difficult prioritization decisions.

This resource constraint directly correlates with findings from *The 2025 IT Risk and Compliance Benchmark Report*, which noted that 16% of organizations manage IT risk on an ad-hoc basis or only in response to negative events. The connection becomes clear: insufficient resources make it extremely challenging to implement and maintain comprehensive, proactive risk management frameworks.

Organizations facing budget and staffing limitations must often focus their limited resources on immediate operational needs and active threat response rather than developing mature risk management processes. This creates a reactive cycle where teams can only address risks after they've manifested instead of proactively identifying and mitigating them. While most organizations understand the importance of structured risk management, resource limitations frequently force them into reactive postures.

Risk management at organizations struggling with IT security resource constraints

hyperproof.io/it-compliance-benchmarks

CHAPTER 6

Multi-Cloud Makes Evidence Collection Challenging

The operational burden of collecting, managing, and validating compliance evidence poses a major challenge for organizations – one that also presents a strategic opportunity for improvement. According to *The State of Continuous Controls Monitoring Report*, 47.9% of organizations cite struggles with basic evidence-gathering processes, creating a foundational weakness that affects everything from audit preparation to deficiency management. These inefficiencies not only slow operations but also shape overall risk posture, signaling a broader governance gap. For GRC professionals, the data underscores that evidence management is more than an administrative task – it's a critical function that impacts program effectiveness across the board.

This burden is especially visible in audit activities, where 55% of respondents in *The 2025 IT Risk and Compliance Benchmark Report* say that testing and validating evidence before submission is tedious or slower than expected – the most cited pain point in the compliance lifecycle. Additionally, 31% of respondents to *The 2025 IT Risk and Compliance Benchmark Report* face significant challenges collecting the data needed to test controls, while 42% operate in multi-cloud environments that complicate evidence collection, based on findings from *The 2024 Global Digital Trust Insights Report*.

Although 57.9% of respondents in *The State of Continuous Controls Monitoring Report* have adopted GRC tools for compliance evidence, 42% still rely on spreadsheets to track risk owners according to *The 2025 IT Risk and Compliance Benchmark Report* – a clear indicator of partial or stalled implementation. Budget constraints, cited by 46.2% of respondents to *The State of Continuous Controls Monitoring Report* as the main barrier to adopting advanced solutions, further exacerbate these issues.

These statistics point to a pressing need for investment in automation and process integration to reduce inefficiencies and enhance audit readiness. For security and compliance leaders, addressing these root causes is key to transforming compliance operations from reactive and manual to strategic and scalable.

Nearly half of organizations struggle with evidence gathering for compliance processes

The State of Continuous Controls Monitoring Report shows that 47.9% of organizations cite evidence gathering as a significant challenge in their compliance processes. This widespread difficulty collecting the necessary documentation represents the first step in what becomes a problematic workflow for many organizations.

This finding provides important context for data from *The 2025 IT Risk and Compliance Benchmark Report*, which shows that 29% of respondents find filing, storing, and managing compliance documentation to be tedious or more time-consuming than expected. These statistics highlight different points in the same operational chain: first gathering evidence, then managing that documentation.

Challenges in upstream activities inevitably cascade into downstream processes. When organizations struggle with efficient evidence gathering, those difficulties naturally extend to the subsequent tasks of organizing, storing, and maintaining that documentation. Evidence gathering and documentation management aren't isolated activities but parts of a continuous workflow. The high percentage of organizations struggling with both evidence collection and document management suggests that many compliance teams face workflow inefficiencies that impact their productivity and effectiveness across multiple stages of the compliance process.

Organizations struggling to gather evidence for compliance processes

hyperproof.io/it-compliance-benchmarks

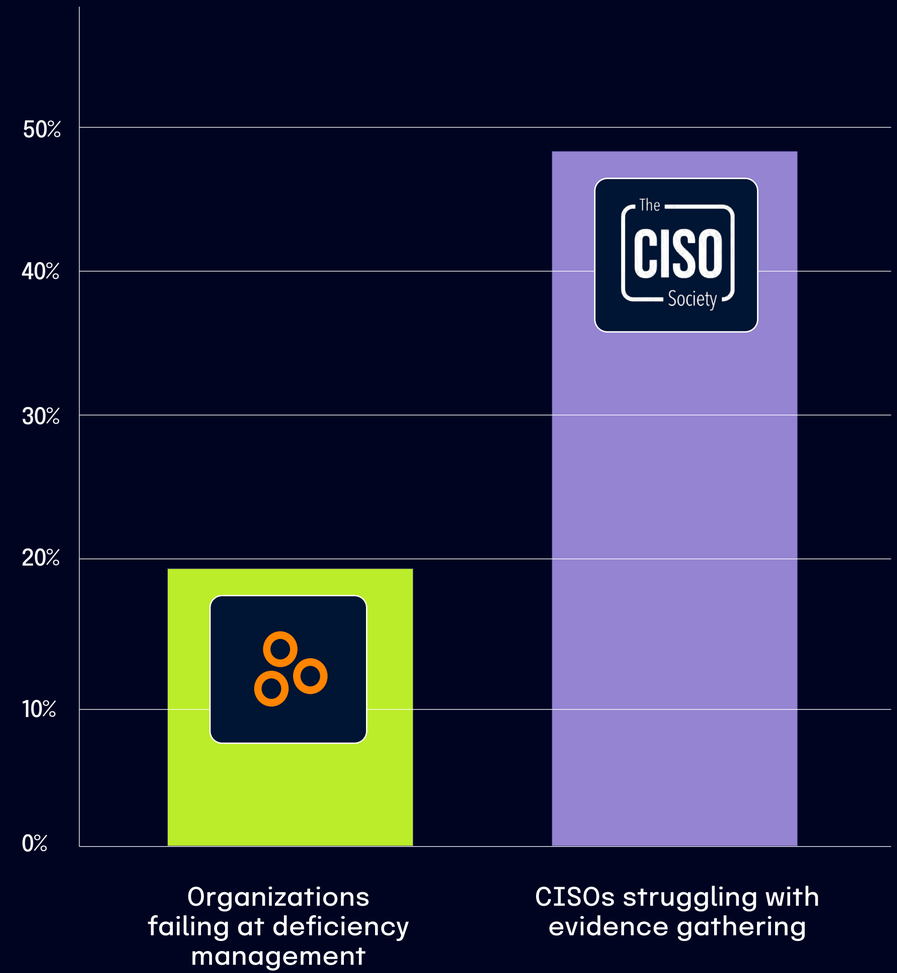
47.9% of CISOs struggle with evidence gathering, undermining deficiency management processes

According to *The State of Continuous Controls Monitoring Report*, nearly half (47.9%) of CISOs identify evidence gathering as one of their greatest operational challenges. This widespread difficulty in collecting and documenting control evidence creates significant upstream impacts on deficiency management processes across organizations.

19% of respondents are not fully satisfied with their process for assessing controls' effectiveness and capturing, tracking, and reporting deficiences

FRESH FACT

Evidence gathering impacts security control effectiveness



hyperproof.io/it-compliance-benchmarks

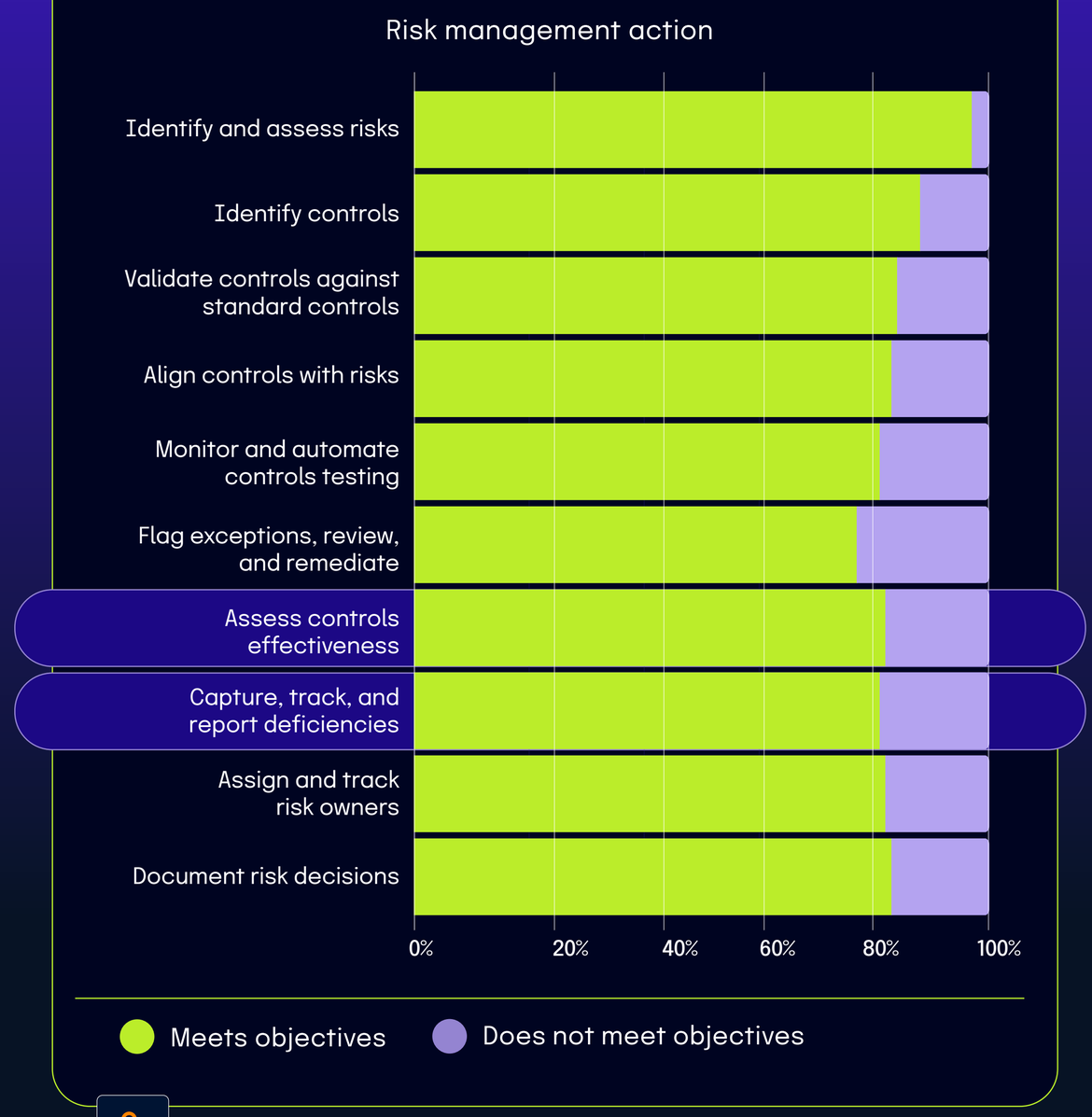
This evidence gathering challenge helps explain why *The 2025 IT Risk and Compliance Benchmark Report* found that 19% of organizations fail to meet their objectives in capturing, tracking, and reporting deficiencies. Without robust evidence collection processes, organizations simply cannot effectively identify and document control gaps.

When security teams struggle to gather appropriate evidence, they face several cascading problems: deficiencies remain undetected, those that are found may be incompletely documented, and the resulting reports lack the comprehensive information needed for effective remediation planning. The substantial gap between organizations experiencing evidence challenges (47.9%) and those explicitly failing at deficiency management (19%) suggests that many teams are implementing compensating processes despite their evidence difficulties.

This relationship highlights how fundamental evidence gathering capabilities are to the entire control effectiveness ecosystem. The challenges CISOs face when collecting evidence create ripple effects throughout the governance structure, ultimately compromising an organization's ability to identify and address control weaknesses.

> **Without robust evidence collection processes, organizations simply cannot effectively identify and document control gaps.**

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



SOURCE: *The 2025 IT Risk and Compliance Benchmark Report*

hyperproof.io/it-compliance-benchmarks

Nearly half of security leaders struggle with evidence gathering, potentially contributing to 14% of organizations skipping regular control audits

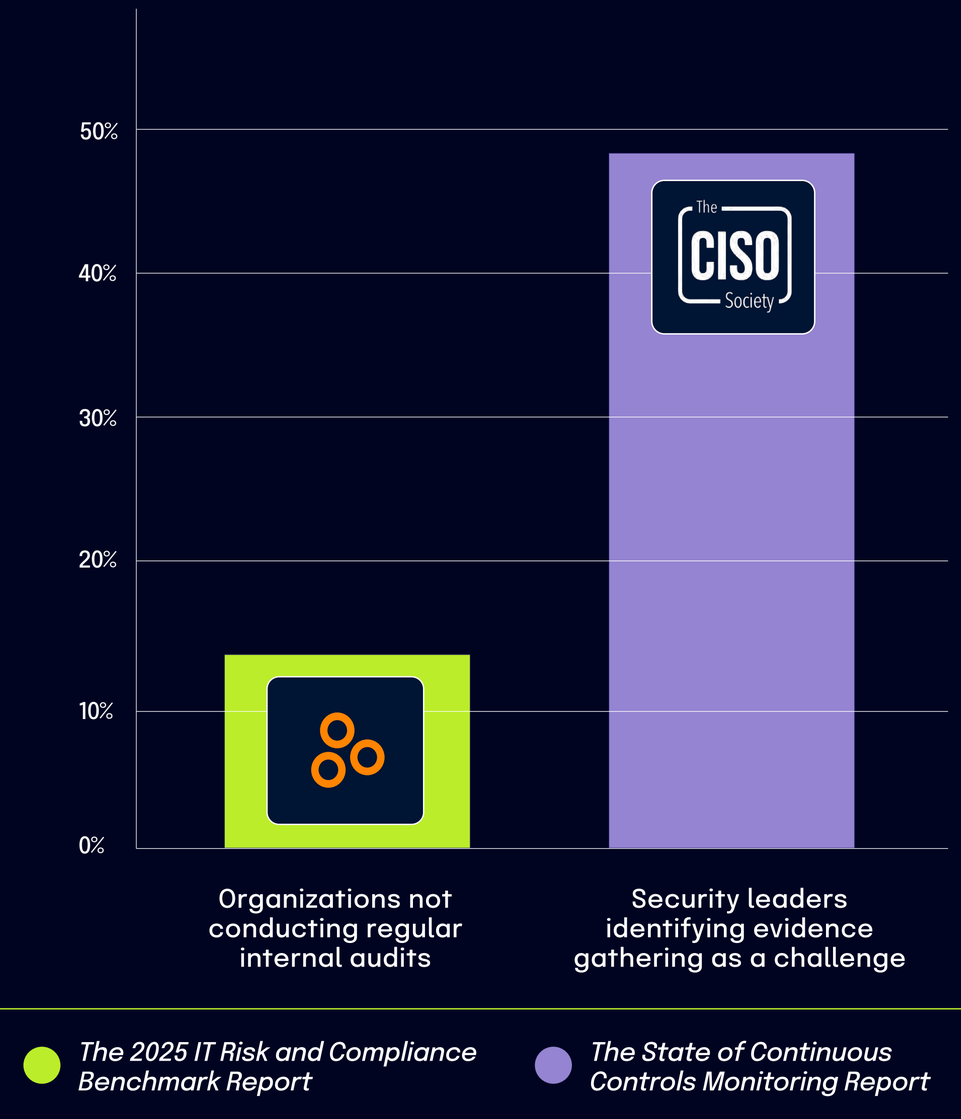
According to *The State of Continuous Controls Monitoring Report*, 47.9% of security leaders identify evidence gathering as a significant challenge in their controls assessment process. This widespread difficulty in collecting and documenting evidence creates a substantial operational burden for security and compliance teams.

This evidence collection challenge helps explain findings from *The 2025 IT Risk and Compliance Benchmark Report* that 14% of organizations don't conduct regular internal audits or assessments of their internal controls. The connection between these statistics suggests that for some organizations, the resource-intensive nature of evidence gathering may discourage or prevent them from implementing regular audit cycles.

While these statistics come from different survey populations, they suggest a plausible connection between operational challenges and governance practices. Organizations that find evidence collection particularly burdensome are likely more inclined to deprioritize or irregularly perform internal control assessments.

Practical implementation challenges directly impact governance activities. When fundamental tasks like evidence gathering become excessively difficult, they may undermine broader risk management processes, potentially causing some organizations to conduct control assessments on an ad-hoc basis rather than establishing consistent audit cycles.

Evidence gathering challenges reduce regular control audits



hyperproof.io/it-compliance-benchmarks

31% of organizations struggle to collect necessary control testing data, reflecting broader evidence gathering challenges

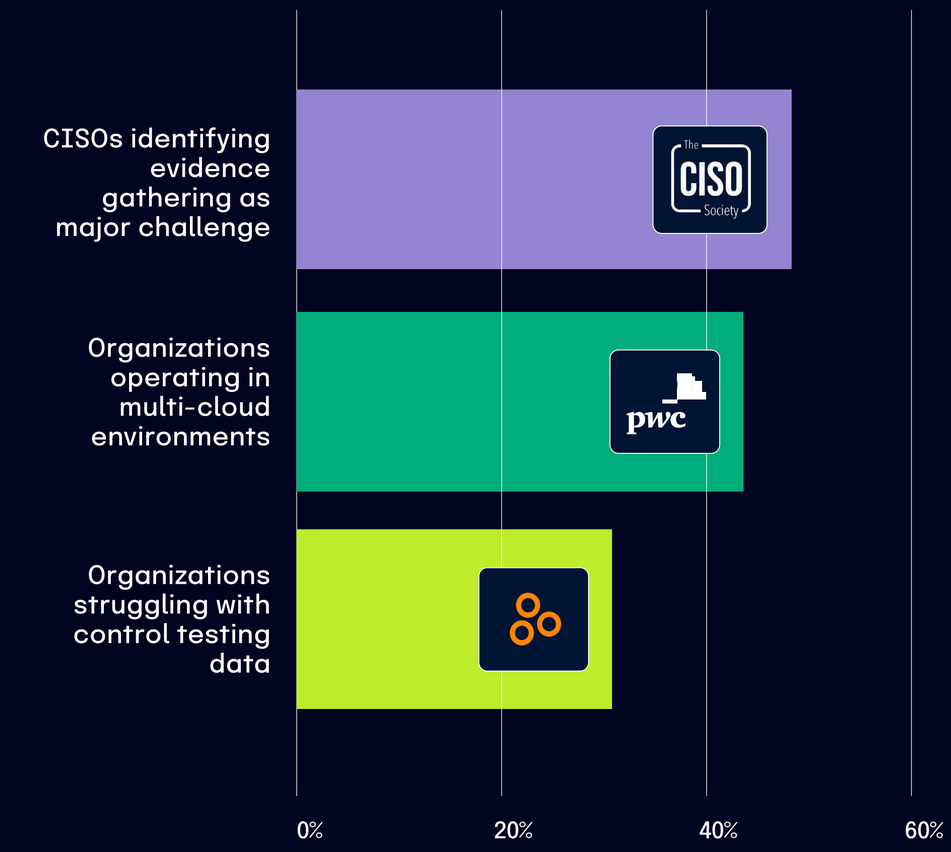
According to *The 2025 IT Risk and Compliance Benchmark Report*, 31% of organizations struggle to collect the necessary data to test controls effectively. This finding points to a fundamental operational obstacle that undermines control assurance efforts.

This challenge aligns with *The State of Continuous Controls Monitoring Report*, which found that 47.9% of CISOs identify evidence gathering as a major challenge. The connection between these statistics is apparent – collecting control testing data is essentially an evidence gathering activity – though the different percentages suggest varying difficulties across specific evidence collection scenarios.

Additionally, *The 2024 Global Digital Trust Insights Report* found that 42% of organizations operate in multi-cloud environments. This widespread architectural approach likely contributes to data collection challenges, as teams must navigate different platforms with inconsistent naming conventions, access mechanisms, and monitoring capabilities.

Collecting testing data across diverse cloud environments requires specialized knowledge of each platform's unique controls, administration interfaces, and logging mechanisms. Without standardized collection methods, organizations fail to obtain consistent evidence across their environments, particularly when teams lack expertise across all deployed cloud platforms. Together, these findings explain why nearly a third of organizations face testing data challenges – they operate in increasingly complex multi-cloud environments while lacking the streamlined evidence gathering capabilities needed for effective control validation.

Control testing struggles mirror evidence collection problems



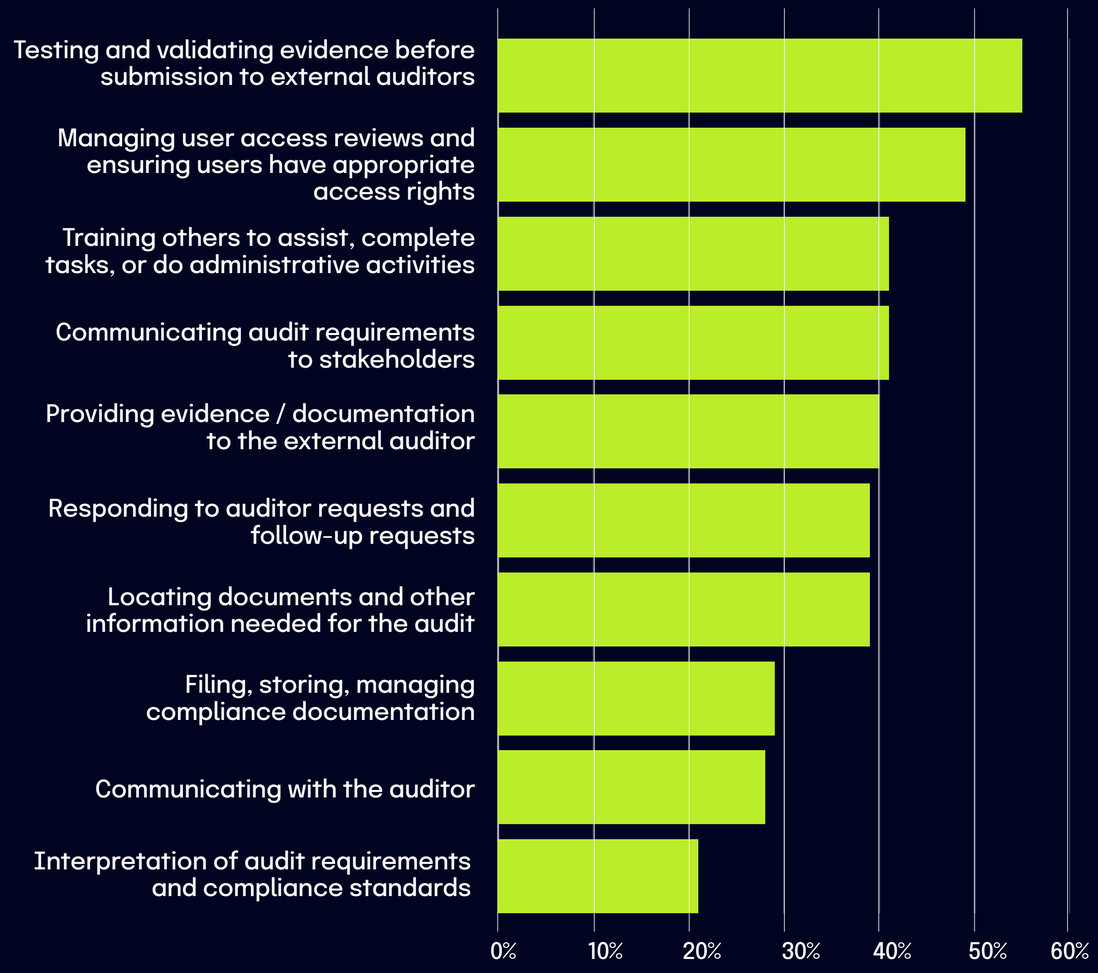
hyperproof.io/it-compliance-benchmarks

Nearly half of organizations struggle with evidence gathering, while a majority find audit-related tasks tedious and time-consuming

According to *The 2025 IT Risk and Compliance Benchmark Report*, 55% of respondents indicated that testing and validating evidence before submission to external auditors is tedious or takes longer than expected. This represents the most significant pain point in the audit process among those surveyed.

The report further found that 40% of respondents find the actual process of providing evidence and documentation to external auditors to be tedious or time-consuming. Similarly, 39% of respondents reported that responding to auditor requests and follow-up inquiries presents the same challenges. Another 39% indicated that simply locating documents and other information needed for audits is tedious or takes longer than expected.

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



SOURCE: *The 2025 IT Risk and Compliance Benchmark Report*

hyperproof.io/it-compliance-benchmarks

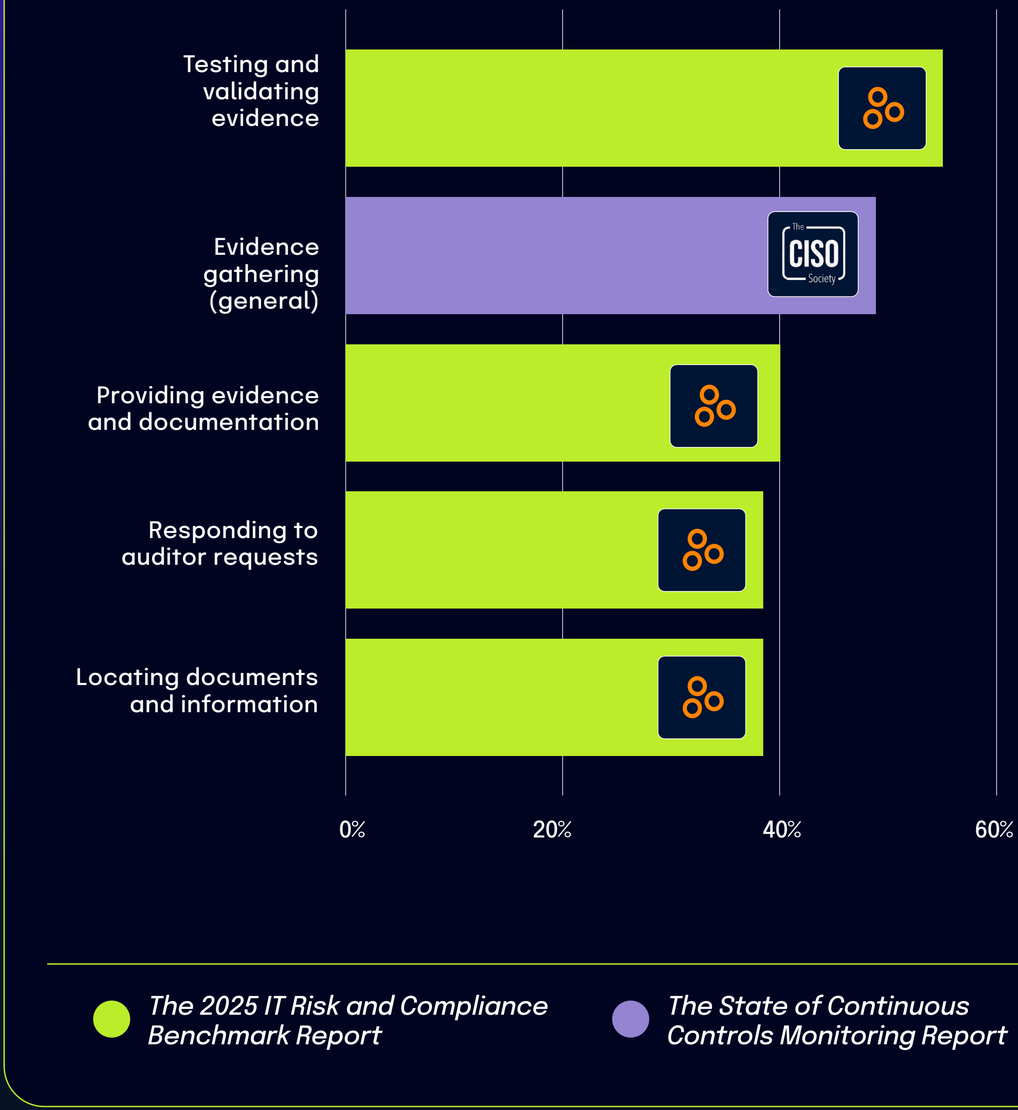
These findings closely align with data from *The State of Continuous Controls Monitoring Report*, which found that 47.9% of organizations cited evidence gathering as a challenge. The similarity between this figure and the percentages reporting specific audit-related difficulties suggests a direct connection between general evidence gathering challenges and the various tedious aspects of the audit process.

Organizations that struggle with fundamental evidence gathering are likely to experience difficulties throughout the entire audit lifecycle. The close alignment between those finding evidence gathering challenging (47.9%) and those reporting specific audit tasks as tedious (ranging from 39% to 55%) demonstrates how one core operational challenge manifests across multiple audit activities.

These findings highlight how evidence management challenges permeate the entire audit process. From initially locating necessary documents to responding to auditor requests, validating evidence before submission, and finally providing documentation to external auditors, each stage creates significant operational friction for about 40–55% of organizations. This consistent pattern suggests that an organization's fundamental evidence gathering capabilities strongly influence its overall audit experience.

> **Organizations that struggle with fundamental evidence gathering are likely to experience difficulties throughout the entire audit lifecycle.**

Evidence gathering can make audit tasks slow and tedious



hyperproof.io/it-compliance-benchmarks

Many organizations anticipate audit findings due to evidence-gathering challenges

According to *The 2025 IT Risk and Compliance Benchmark Report*, 24% of respondents indicated they have not yet experienced an audit finding but would not be surprised if they receive one soon. This significant percentage of organizations anticipating compliance issues reflects a growing awareness of potential gaps in their control environments.

This expectation of future audit findings appears closely connected to data from *The State of Continuous Controls Monitoring Report*, which found that 47.9% of organizations struggle with evidence gathering. The relationship between these statistics explains why many organizations feel vulnerable to potential audit findings despite having no current issues.

When nearly half of organizations cannot effectively collect and organize appropriate compliance documentation, it naturally creates uncertainty about audit readiness. Organizations unable to efficiently gather evidence demonstrating control effectiveness have valid reasons to anticipate future findings, even if they've avoided them so far.

Operational challenges in compliance processes directly influence risk perceptions. The substantial percentage struggling with evidence collection explains why a quarter of organizations expect audit findings on the horizon. This connection highlights how practical difficulties in day-to-day compliance activities translate into broader concerns about audit outcomes, leaving many compliance teams in a state of perpetual uncertainty.

Audit findings expected due to evidence collection issues

hyperproof.io/it-compliance-benchmarks

41% of organizations report that training team members takes longer than expected

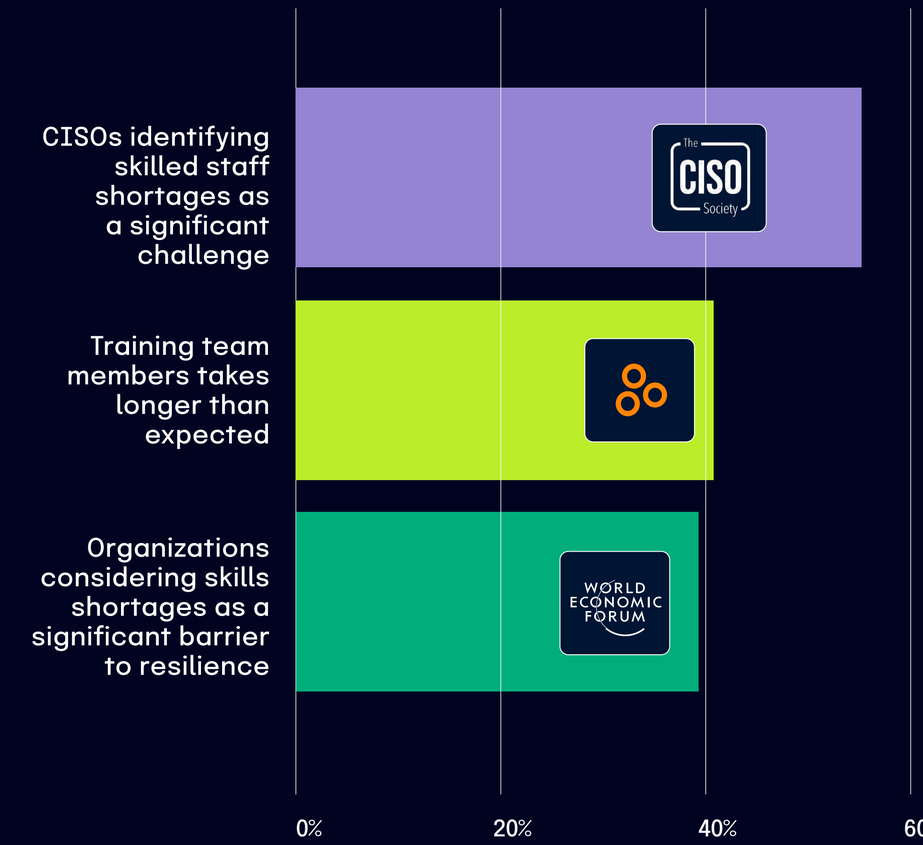
The 2025 IT Risk and Compliance Benchmark Report highlights that 41% of respondents find training others to assist with tasks or handle administrative activities to be tedious or more time-consuming than expected. This training challenge appears to be connected to broader industry-wide talent shortages.

The State of Continuous Controls Monitoring Report notes that 53.7% of CISOs identified skilled staff shortages as a significant challenge. When organizations lack personnel with the right baseline skills, training inevitably becomes more intensive and time-consuming. Instructors must build fundamental capabilities before they can address specialized tasks.

Similarly, *The Global Cybersecurity Outlook 2025 Insight Report* shows that 39% of organizations consider skills shortages a significant barrier to resilience. This widespread talent gap forces many organizations to work with team members who require extensive training to reach necessary competency levels.

An industry-wide skills shortage has directly impacted daily operations. Organizations facing a limited talent pool must invest substantially more time and resources in training to develop essential capabilities, explaining why so many find training processes to be unexpectedly burdensome and challenging.

Control testing struggles mirror evidence collection problems



hyperproof.io/it-compliance-benchmarks

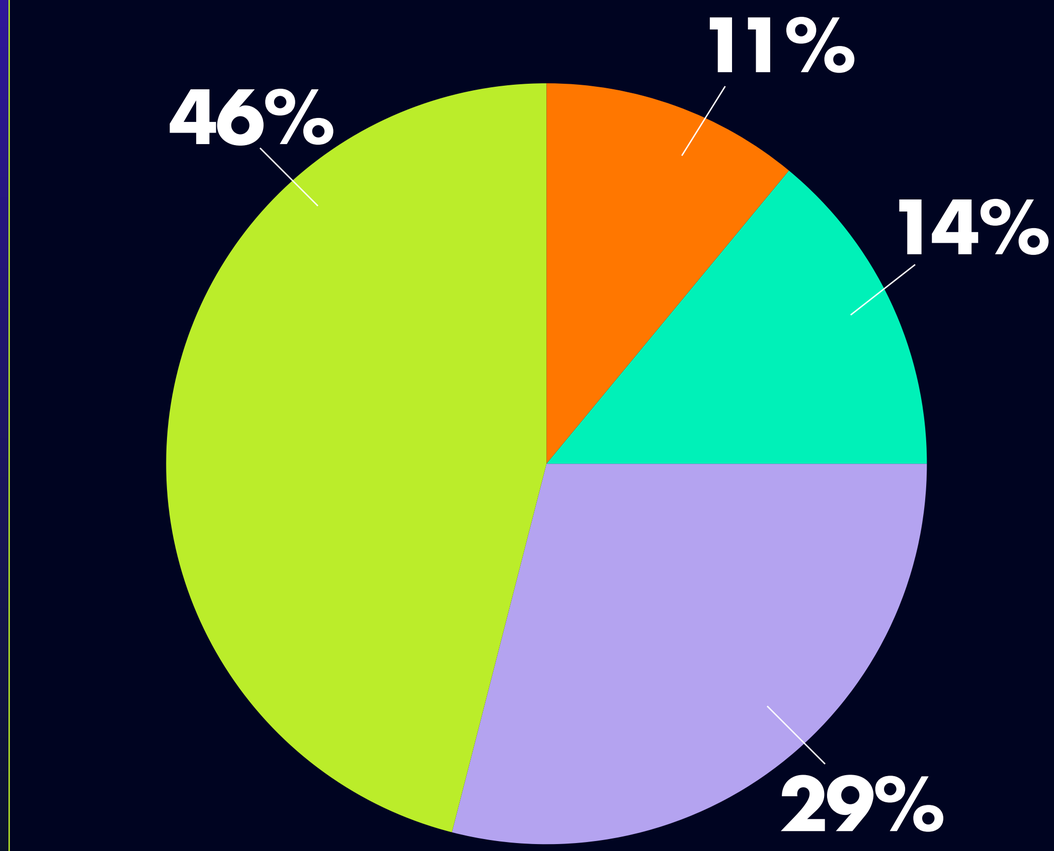
Nearly half of organizations conduct regular audits while a majority use specialized tools for compliance evidence management

According to *The 2025 IT Risk and Compliance Benchmark Report*, 46% of respondents indicated that their organization collects evidence for both internal and external audits and conducts internal audits regularly. This shows that many organizations have established structured audit processes as part of their governance framework.

However, the same report shows that only 29% of respondents indicated that their organization collects evidence on an ongoing basis as part of a continuous compliance program. This significant gap between periodic audit-based evidence collection and continuous monitoring suggests that while regular auditing is relatively common, continuous compliance remains a less widely adopted practice.

Technology use shows varied compliance program maturity

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



SOURCE: *The 2025 IT Risk and Compliance Benchmark Report*

hyperproof.io/it-compliance-benchmarks

These findings align with data from *The State of Continuous Controls Monitoring Report*, which found that 57.9% of organizations use GRC tools to collect and maintain compliance evidence. The widespread adoption of these specialized tools helps explain how organizations manage their audit processes, whether periodic or continuous.

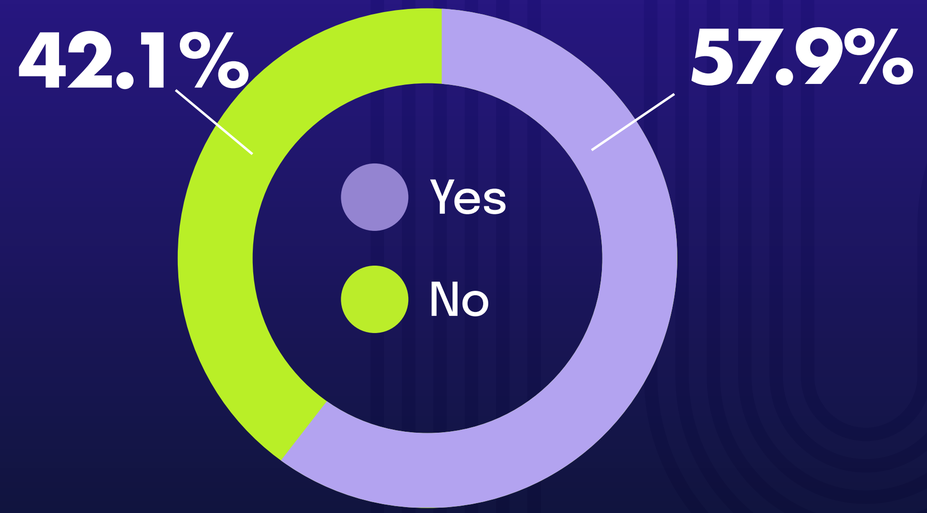
While most organizations (57.9%) have invested in the technological infrastructure to support systematic evidence collection through GRC tools, fewer have implemented regular audit processes (46%), and even fewer have established continuous compliance programs (29%).

While having the right tools is necessary for effective compliance management, technology alone doesn't drive continuous compliance adoption. Organizations appear to be at different stages of maturity in their compliance approaches, with most having acquired the enabling technology but fewer having fully implemented either regular or continuous monitoring practices.

29% of organizations have yet to establish continuous compliance programs

FRESH FACT

Are you using GRC tools to collect and maintain compliance evidence?



SOURCE: *The State of Continuous Controls Monitoring Report*

42% of organizations still rely on spreadsheets for tracking risk owners despite GRC tool availability

According to *The 2025 IT Risk and Compliance Benchmark Report*, 42% of respondents continue to use spreadsheets as their primary method for tracking risk owners within their organizations. This widespread reliance on basic tools for such an important governance function raises important questions about why dedicated GRC solutions haven't gained more traction.

The State of Continuous Controls Monitoring Report offers a potential explanation: 46.2% of organizations identify insufficient budget as the main barrier preventing them from implementing more sophisticated GRC tools. The striking similarity between these percentages suggests a direct correlation between budget constraints and continued spreadsheet dependency.

Nearly half of organizations find themselves caught in a difficult position – they recognize the need for structured risk ownership tracking but face financial limitations that keep them from moving beyond spreadsheet-based approaches. While spreadsheets offer flexibility and familiarity, they lack the automated workflows, comprehensive audit trails, and integrated risk visibility that purpose-built GRC solutions deliver. The alignment of these statistics from two independent reports underscores how budget considerations continue to shape technology decisions in risk management practices across industries, creating a persistent gap between best practices and operational reality.

Technology choices show budget constraints affect risk management

hyperproof.io/it-compliance-benchmarks

CHAPTER 7

Security and Compliance: Together, but Separate

Modern organizations are under increasing pressure to align security operations with compliance mandates while maintaining operational efficiency. As a result, integrating risk and compliance functions has become a strategic priority aimed at consolidating governance efforts, reducing redundancy, and presenting a unified defense against organizational threats. While progress is evident – 84% of organizations surveyed for *The 2025 IT Risk and Compliance Benchmark Report* say that they have aligned risk management with compliance – only 44.1% of respondents to *The State of Continuous Controls Monitoring Report* say these functions are "completely synchronized," a significant gap between alignment in principle and full integration in practice. Additionally, 51% of organizations surveyed for *The 2025 IT Risk and Compliance Benchmark Report* have formally assigned risk responsibilities to compliance personnel, signaling a shift toward unified governance structures (though implementation challenges remain).

This tension between awareness and action is also evident in responses to emerging threats. For example, while 55% of CISOs participating in *The Global Cybersecurity Outlook 2025 Insight Report* view deepfakes as a moderate to significant risk, only 26% of organizations plan to include deepfake monitoring in their incident response plans, based on data from *The 2025 IT Risk and Compliance Benchmark Report*. This pattern – recognizing risks before taking action – highlights the operational lag many security teams face when balancing known issues with evolving threats. Despite these challenges, commitment to compliance remains strong, with just 1% of organizations anticipating reductions in information security and privacy compliance teams over the next two years. For GRC and cybersecurity professionals, these findings underscore the importance of continued integration and investment, especially as governance frameworks evolve to meet rising regulatory expectations and increasingly sophisticated threat landscapes.

84% of organizations align risk management with compliance, though complete synchronization remains a challenge

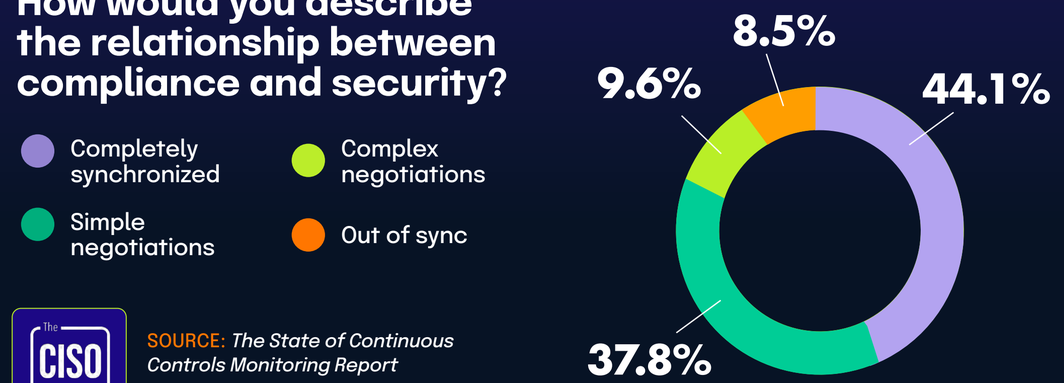
The 2025 IT Risk and Compliance Benchmark Report found that 84% of organizations have aligned their risk management with compliance efforts, specifically by mapping controls to the risks they're designed to mitigate. This high percentage demonstrates that most organizations recognize the value of connecting risk management and compliance activities rather than treating them as separate functions.

However, *The State of Continuous Controls Monitoring Report* adds an important nuance to this finding, with only 44.1% of respondents describing the relationship between compliance and security as completely synchronized. This significant gap between general alignment (84%) and complete synchronization (44.1%) highlights varying degrees of integration maturity across organizations.

This relationship between the statistics suggests that while most organizations have established basic alignment between risk and compliance activities, achieving deep functional integration remains challenging for many. Organizations appear to be at different stages of maturity: most have implemented fundamental mapping between controls and risks, but fewer have achieved the seamless synchronization that security leaders consider optimal for effective risk management.

Risk management and compliance show incomplete synchronization

How would you describe the relationship between compliance and security?



SOURCE: *The State of Continuous Controls Monitoring Report*

Over half of organizations integrate risk responsibilities into compliance roles

According to *The 2025 IT Risk and Compliance Benchmark Report*, 51% of respondents indicated that risk and compliance are integrated, with risk responsibilities rolled into compliance personnel's jobs. This organizational approach represents a significant trend toward unifying related governance functions under common management.

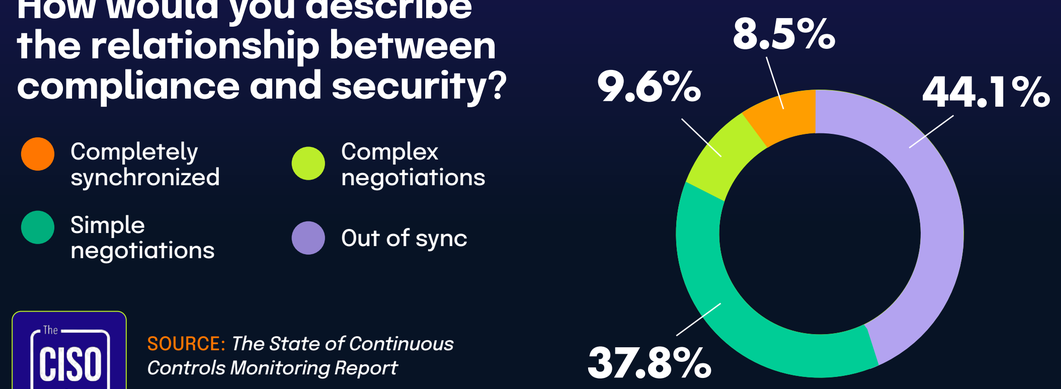
This integration is further supported by findings from *The State of Continuous Controls Monitoring Report*, which found that 44.1% of respondents described the relationship between compliance and security as "completely synchronized." The close alignment of these percentages from different surveys (51% integration and 44.1% synchronization) suggests a consistent trend toward consolidating related governance functions.

Organizations are actively breaking down traditional silos between risk, compliance, and security disciplines. When nearly half of organizations describe their compliance and security functions as completely synchronized, it reinforces the finding that a majority have formally integrated risk and compliance roles.

This connection highlights an important shift in organizational governance structures. Rather than maintaining separate teams for closely related disciplines, many companies now recognize the efficiencies gained through integration, creating roles that span multiple domains. This approach provides a more cohesive perspective on organizational risks and regulatory requirements, allowing personnel to address interconnected issues through a unified governance framework.

Risk and compliance roles increasingly merge

How would you describe the relationship between compliance and security?



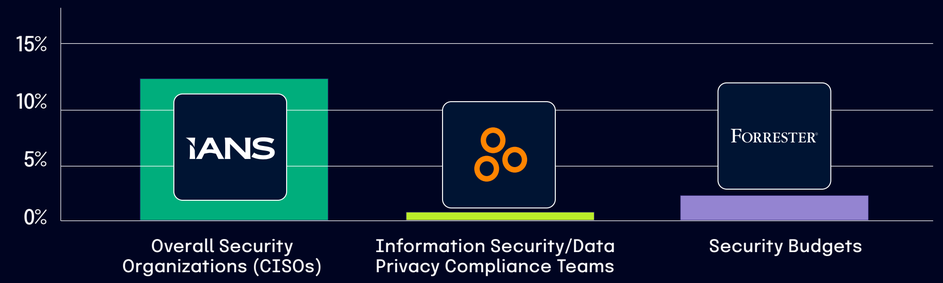
SOURCE: *The State of Continuous Controls Monitoring Report*

Only 1% of organizations expect to reduce information security/data privacy compliance teams in the next two years

Despite industry challenges, respondents to *The 2025 IT Risk and Compliance Benchmark Report* present remarkable stability in compliance team staffing plans. While just 1% of respondents expect their information security and data privacy compliance teams to decrease in personnel over the next two years, this finding becomes more significant when examined alongside other industry research.

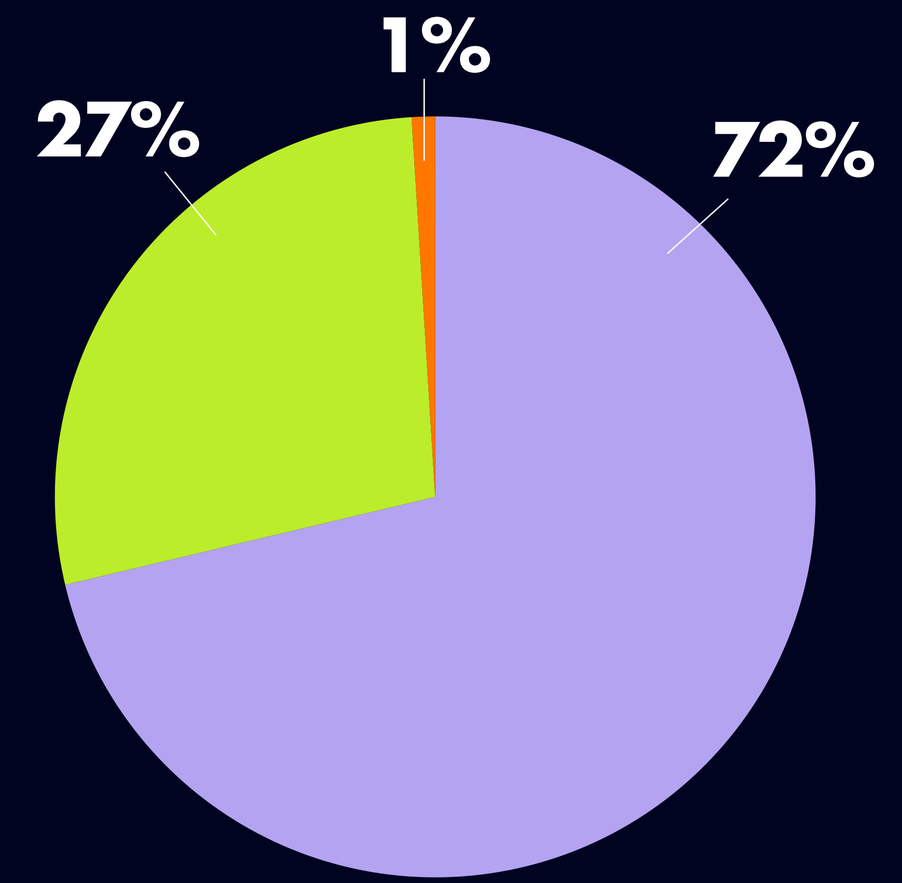
The 2024 Security Budget Benchmark Summary Report highlights a broader trend where 12% of CISOs are implementing headcount reductions across their security organizations. This suggests that compliance teams are being largely shielded from wider security staffing cuts, with organizations recognizing their essential value even during resource constraints.

Security budget allocation prioritizes compliance team stability



The 2025 IT Risk and Compliance Benchmark Report
2024 Security Budget Benchmark Summary Report
Budget Planning Guide 2025: Security And Risk

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



SOURCE: *The 2025 IT Risk and Compliance Benchmark Report*

hyperproof.io/it-compliance-benchmarks

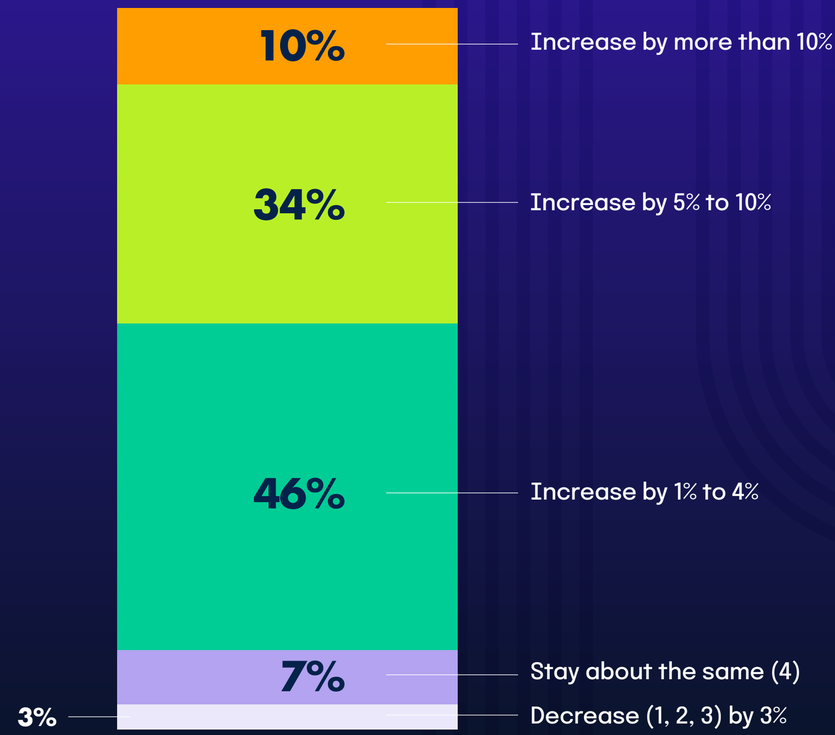
Additionally, *The 2025 Budget Planning Guide: Security And Risk* reports that 3% of organizations anticipate reduced security budgets in 2025. When compared with our finding that only 1% expect compliance team reductions, this indicates **organizations are prioritizing ways to maintain compliance capabilities even when facing financial limitations**.

Organizations are prioritizing their compliance functions during a period of selective resource optimization. While some security areas face personnel reductions, compliance teams focusing on information security and data privacy appear to maintain stable staffing levels, reflecting their ongoing importance in managing organizational risk.

FRESH FACT

Only
3%
of organizations anticipate reduced security budgets in 2025

Which of the following describes any planned/ anticipated change in your organizations budget for security in the next 12 months?



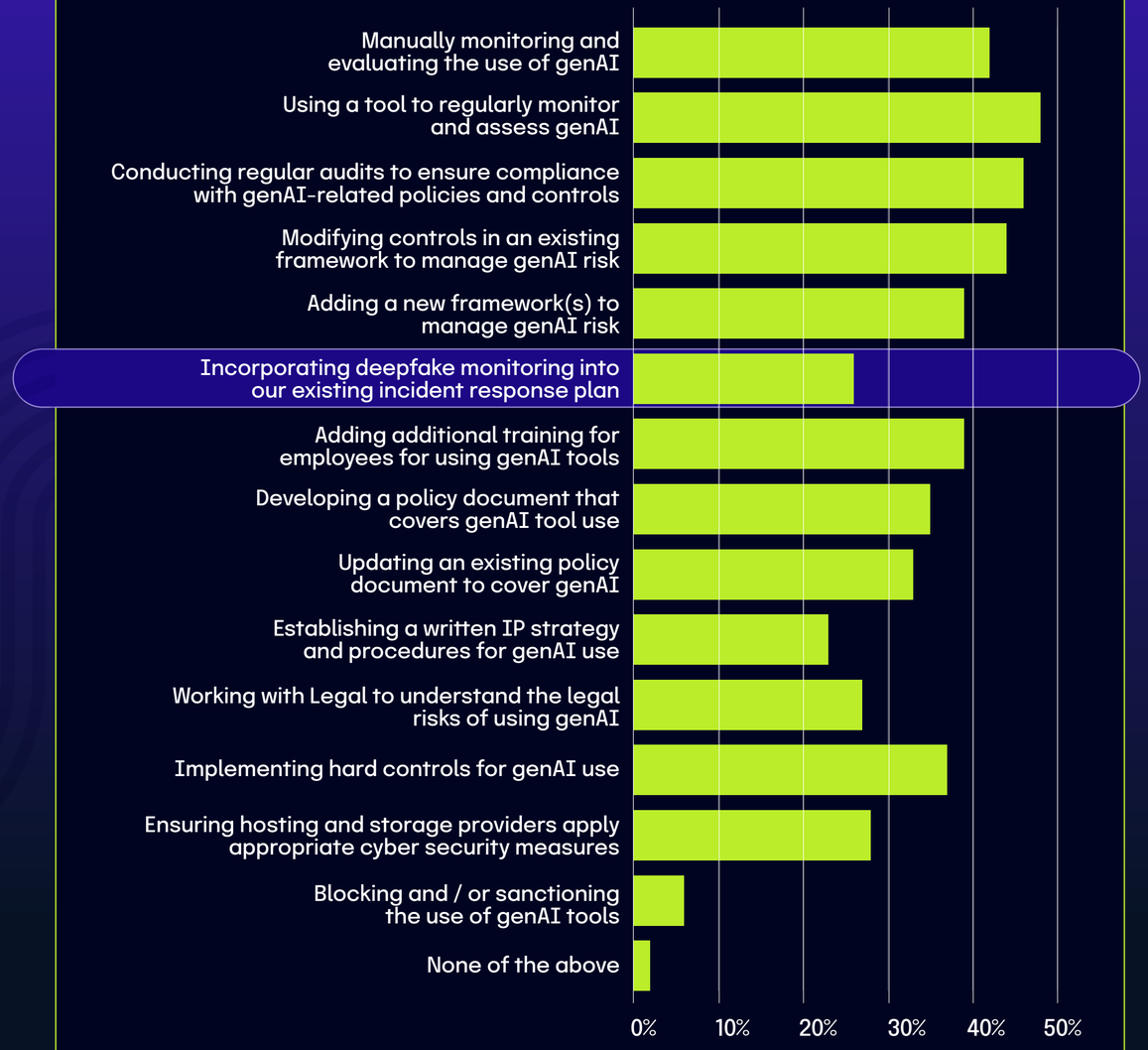
FORRESTER

SOURCE: *The 2025 Budget Planning Guide: Security and Risk*

26% of organizations plan to incorporate deepfake monitoring into incident response plans

The 2025 IT Risk and Compliance Benchmark Report found that just over a quarter of respondents (26%) are planning to incorporate deepfake monitoring capabilities into their existing incident response plans. This emerging focus on deepfake detection marks a significant shift in how organizations are preparing for modern digital threats.

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



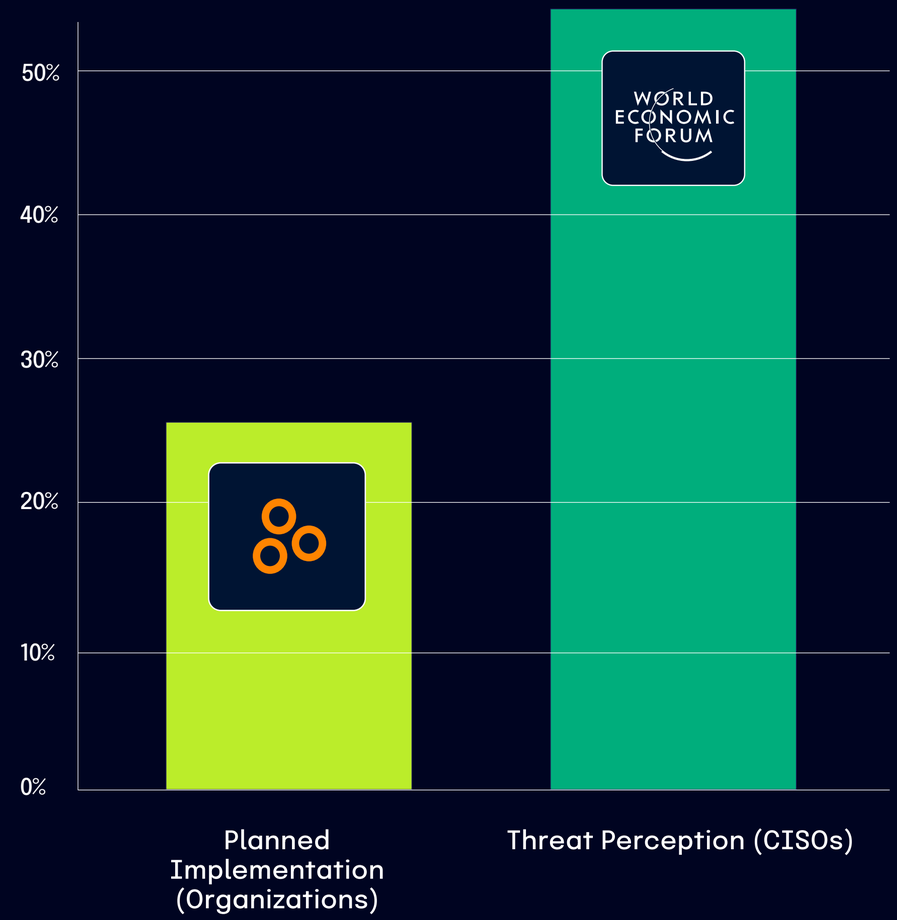
SOURCE: *The 2025 IT Risk and Compliance Benchmark Report*

hyperproof.io/it-compliance-benchmarks

This implementation trend gains greater context when viewed alongside *The Global Cybersecurity Outlook 2025 Insight Report*, which found that 55% of CISOs consider deepfakes a moderate-to-significant cyberthreat to their organizations. Threat perception is beginning to translate into concrete security planning, though not yet universally. The substantial gap between threat perception (55%) and planned implementation (26%) indicates that while many security leaders recognize the potential danger of deepfakes, fewer organizations have actually moved toward monitoring for them. This disparity likely stems from implementation costs, technical complexity, competing security priorities, or uncertainty about which detection methods would be most effective.

Together, these statistics demonstrate how emerging threats enter organizational security planning in phases, with recognition typically preceding the implementation of actual controls. As deepfake technology becomes more sophisticated and accessible, we'll likely see the percentage of organizations monitoring for these threats increase to better align with the perceived risk level.

Deepfake threats outpace security response planning



hyperproof.io/it-compliance-benchmarks

Conclusion

Although this report reflects a point in time of late 2024 and early 2025, we've identified a consistent theme: CISOs are concerned about whether or not their GRC programs will be able to adequately and sufficiently address their next audit, regulatory investigation, or board conversation.

We found a high degree of correlation between leading industry reports and *The 2025 IT Risk and Compliance Benchmark Report* that point to a clear trend: the confidence gap between operational teams and executive oversight. While 82% of organizations believe they effectively assess control effectiveness, 45% of board directors still seek external validation – highlighting a disconnect between technical execution and governance assurance.

Throughout this report, we've examined the root causes of such gaps, from regulatory fragmentation and underutilized GRC tools to resource constraints and inconsistent implementation. Despite widespread investment, such as the 84% of organizations aligning risk management with compliance, only 44.1% report full synchronization, illustrating the difference between alignment in theory and integration in practice.

The most forward-thinking organizations recognize that GRC is more than a regulatory obligation – it's a strategic enabler of business performance. Closing the gaps identified in this report requires more than new tools; it requires rethinking how security, compliance, and risk management work together to drive business value. Whether it's addressing the 47.9% struggling with evidence collection, bridging the 53.7% gap in integrating compliance into development pipelines, or enhancing third-party risk visibility to meet the 54% citing supply chain risk as a top concern, progress is possible with focused action.

As you move forward, consider the following steps:

1. Assess your GRC maturity using Hyperproof's GRC Maturity Model
2. Implement at least one improvement you've learned from this report in the next 90 days
3. Share key findings from this report with your leadership and Board

By doing so, your organization can transform GRC from a perceived cost center into a strategic asset – fueling resilience, agility, and competitive advantage in an increasingly complex landscape.

Remember, effective GRC isn't about perfect documentation or flawless audits. It's about making security an integral part of how your organization makes decisions, manages resources, and achieves its objectives. By applying the insights and tools from this benchmark report, you can transform your GRC program from a necessary cost into a competitive advantage.

The journey toward GRC maturity is ongoing, but with each step, your organization becomes more resilient, more agile, and better equipped to navigate the complex compliance landscape ahead. The future belongs to organizations that can turn compliance requirements into business opportunities and risk management into strategic advantage. With the right approach, your organization can be among them.

hyperproof

About Hyperproof

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

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

hyperproof

Get a Demo

2025 IT and Compliance Benchmark Report

Beyond the Benchmark: How Does Our Report Compare?