The CISO Society

2025

THE CISO SOCIETY **2025 STATE OF CONTINUOUS CONTROLS MONITORING REPORT**

WHERE WE ARE, WHERE WE'RE HEADED, AND THE ROLE OF NEW TECHNOLOGIES

SUPPORTED BY: RegScale

CONTENTS

ANALYST & AUTHOR

LOUIS BEDIGIAN

TASK FORCE

STEVE HINDLE
CISO-in-residence
The CISO Society

ANDREW PARISH
Sr Director of Global Information Security and Cybersecurity
Stack Infrastructure

QUYEN MCCARTHY
IT Security Ops Director
Jassby Inc.

JOSH ABLETT
vCISO
Adelia Risk

KAYLA WILLIAMS
CISO
Devo

DALE HOAK
Director of Information Security
RegScale

OPENING REMARKS

"What gets measured gets managed/done." It's a quote that we hear in the boardroom focused on increasing efficiency and performance and is often used by CISOs when focused on proving the value of their security programs. It's a fallacy – hear me out. In 1956, a paper was published with a significant body of evidence that countered this by highlighting that not everything that matters can be measured, and not everything that we can measure matters. When security aligns with both the business and technology teams on the implementation and measurement of security controls, it's often perceived as governance. But is it effective, and does it add value, or just additional burden and complexity across the organization? Does it honestly matter if it doesn't reflect the reality of the here and now state of security and compliance? In this new era of our Information Age, when automation and real-time data is paramount to delivering value and effectiveness while minimizing impact and loss, enters continuous controls monitoring. The fallacy of "more is better" has all but vanished, now CISOs and GRC leaders are tasked with delivering lean, effective, and continually managed programs – not by reporting what's already in the rear-view mirror.

STEVE HINDLE
CISO-in-residence,
The CISO Society

While all security teams want benefits like real-time insights, enhanced risk visibility, and improved efficiency, CISOs face significant challenges in operationalizing them. The research reveals a nuanced landscape: while less than half of organizations report a fully synchronized relationship between compliance and security teams, many CISOs are actively working to bridge the gaps. Unfortunately, they face significant hurdles in doing so. Over half of CISOs note that compliance is not embedded into their CI/ CD pipeline, and a staggering 80% admit to unnecessary duplication in their compliance efforts. The underlying truth is that even the most sophisticated GRC experts can be resistant to change, and organizational culture often presents the most formidable barrier. While establishing a Continuous Control Monitoring (CCM) framework might initially seem like a heavy lift, the long-term benefits of seamless security and compliance integration are undeniable: strategic alignment that ultimately strengthens an organization's entire security posture.

DALE HOAK
Director of Information Security,
RegScale

INTRODUCTION

APPROACHING THE COMPLIANCE CONUNDRUM

Thousands of rules and regulations have been implemented in the United States since the 1980s and 1990s[1], and thousands more are introduced every year. This is challenging enough for a business that only intends to operate domestically – for international organizations and organizations with global aspirations, the challenges are multiplied several times over.

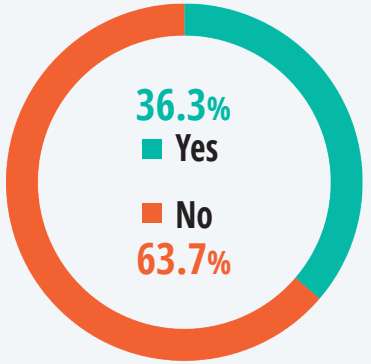
The evolving regulatory environment is just one of the topics The CISO Society looked at when building our 2025 State of Continuous Controls Monitoring Report. Almost 200 members participated in our survey to determine how much organizations spend to achieve compliance, their biggest hurdles to maintaining compliance, which technologies they use or plan to use to overcome their challenges, and more.

One of the key highlights is that only 5% of CISOs consider their compliance program to be optimized for efficiency and continuous improvement. But there is hope – in thinking about how technology will impact their business, nearly 95% of CISOs believe that continuous controls monitoring will improve both compliance and security.

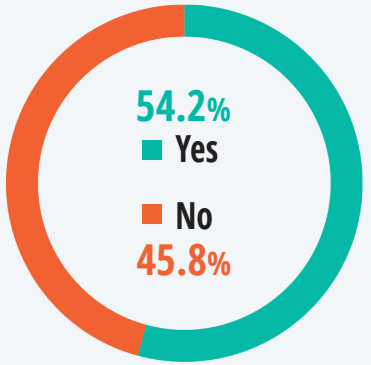
Read on as we take a closer look at how The CISO Society community members are tackling security and compliance amid a technological revolution.

1. https://regulatorystudies.columbian.gwu.edu/reg-stats

Does the burden of meeting new regulatory requirements slow your organizational growth?



Do you have the talent to meet future regulatory requirements?



BUSINESSES SPEND BIG ON COMPLIANCE AS TIGHT BUDGETS LIMIT GRC TOOL ADOPTION

Governance, Risk and Compliance (GRC) is an incredibly important part of doing business, but it has become more complex and more demanding as new regulations are introduced. Organizations are enduring a host of novel challenges as they attempt to remain compliant with overall and industry-specific requirements, and they're spending big to keep up.

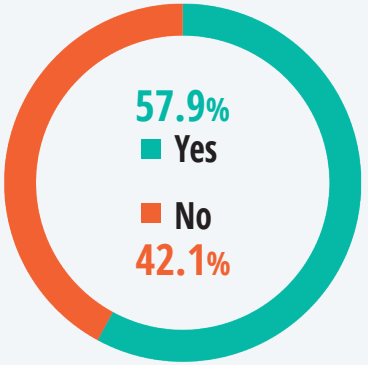
Fifty percent of CISOs said that, on an annual basis, they spend more than $200,000 worth of capital and dedicated staff resources to achieve and maintain compliance across their organization. Twenty percent spend between $100,000 and $200,000; the rest (30%) spend less than $100,000.

Not surprisingly, there is a noticeable divide between small and large organizations, the latter of which more frequently stated that their budget is in excess of $200,000. Many industries – education, finance, healthcare, manufacturing, public administration, retail and consumer goods, software and IT services, and transportation and logistics – had businesses that were evenly split on how much they spend.

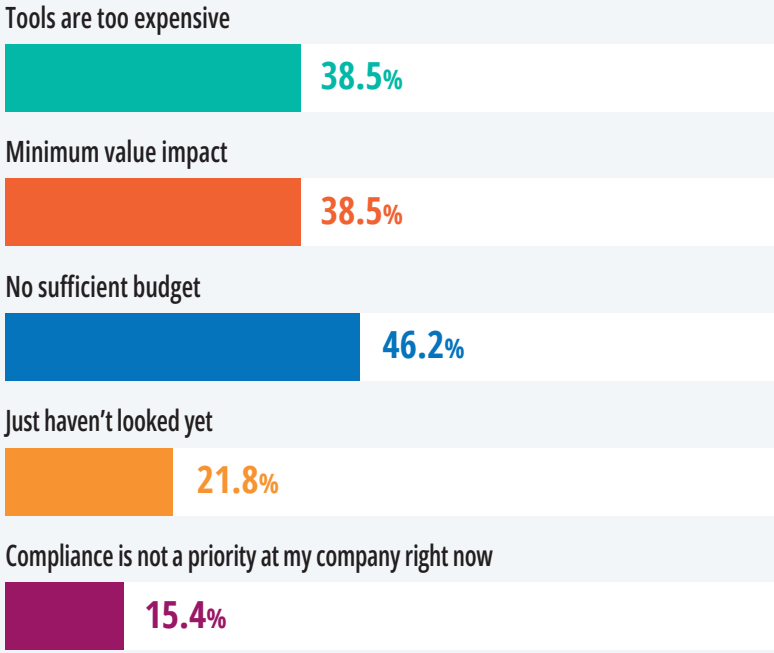
Most organizations (57.9%) spend at least some of their budget on GRC tools to collect and maintain compliance evidence. Among those who don't, 46.2% said they don't have a sufficient budget to invest in GRC tools. Seventy-one percent of manufacturers, 53% of both healthcare and software and IT services organizations, and 50% of education companies concur that their budgets are not sufficient.

Additionally, 38.5% said the tools are too expensive and believe the value impact is minimal. Nearly 22% said they just haven't looked yet while a smaller portion stated that compliance is not currently a priority at their organization. That latter reason was particularly prominent at entertainment and media businesses (66.7%) as well as manufacturers (42.9%).

Are you using Governance, Risk and Compliance (GRC) tool(s) to collect and maintain compliance evidence?



If NO, what is preventing you from doing so?



TOOLS, PROCESSES AND THE BUSINESS IMPACT

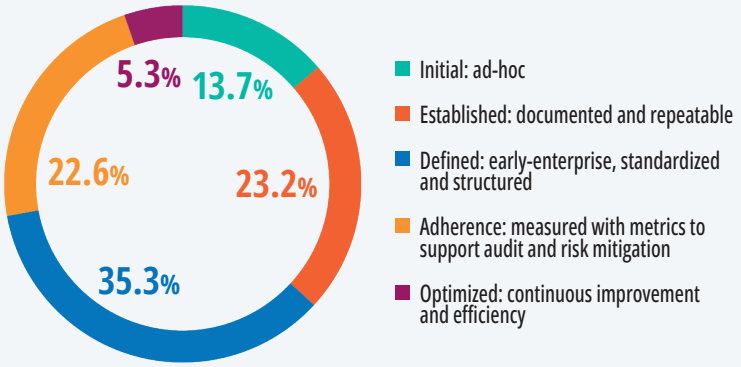
While their expenditures may be high, the way CISOs view their compliance program is not necessarily in line with the amount of money they spend in terms of maturity and the ability to stay ahead of regulatory obligations. Thirty-five percent of CISOs said that, on a scale of 1 to 5, they would rate their compliance program a 3 ("Defined: early-enterprise, standardized and structured").

Roughly one-fifth (22.6%) rate their program a 4 ("Adherence: measured with metrics to support audit and risk mitigation"), but only 5.3% believe their program is a 5 ("Optimized: continuous improvement and efficiency"). Twenty-three percent said their program is a 2 ("Established: documented and repeatable") and 13.7% said their program is a 1 ("Initial: ad-hoc").

CISOs that responded with a 1 or 2 were asked about the biggest challenge that is preventing their organization from maturing further. Almost half of the responders attributed their difficulties to a lack of personnel or resources.* ■

*Note: This data is based on an open-ended question in which respondents could manually write in their responses. The CISO Society asked survey participants, "On a scale of 1-5, how would you rate your compliance program?" – a multiple-choice question, and followed up with, "If you respond 1 or 2 above, what is the biggest challenge that is preventing you from maturing further?" – an open-ended question. Forty-four percent stated that their difficulties were due to a lack of resources, budget, staffing, manpower, personnel, and/or the size of their team. Many cited more than one of these difficulties.

On a scale of 1-5, how would you rate your compliance program?



Embedding "compliance as code" using AI, OSCAL, and OCSF creates a living, adaptive security framework that evolves with the business. This allows CISOs to maintain a more resilient security posture, decreasing the likelihood of breaches, data loss, or compliance violations. By shifting left in security, organizations identify and address security vulnerabilities earlier in the development lifecycle, resulting in fewer disruptions and reducing the potential financial impact of cybersecurity incidents. Additionally, by automating GRC programs, businesses can maintain continuous oversight of their control environments. This allows for a proactive response to evolving threats and changes within the enterprise, significantly reducing the chances of operational disruptions due to security or compliance issues. The real-time visibility offered by Dynamic Operational Control Assurance ensures that critical business processes are always aligned with the latest security protocols, minimizing downtime or vulnerabilities. Automating GRC tasks, no matter which route is taken, reduces manual oversight and the need for extensive human intervention. The optimization translates into significant cost savings, as fewer resources are required to manage compliance and risk mitigation processes.

KAYLA WILLIAMS
CISO, Devo

ORGANIZATIONS CHERRY-PICK WHERE, WHEN AND HOW COMPLIANCE IS EMBEDDED

Compliance remains elusive to many organizations with more than half of CISOs (53.7%) stating that it is not embedded into their CI/CD pipeline. Of the 46.3% that have embedded compliance, nearly one-third (32.1%) have done so in 1-25 percent of their pipeline. Just over a quarter (26.4%) said that compliance has been embedded into 26-50 percent of their pipeline while 27.4% have embedded compliance in as much as 75 percent. Less than one-sixth (14.2%) have embedded compliance into the majority (76-100 percent) of their pipeline. The latter poses an opportunity for organizations to integrate continuous controls monitoring into their CI/CD pipeline to improve GRC outcomes.

Less than half of the respondents (44.1%) described the relationship between compliance and security as completely synchronized, but more than a third (37.8%) said their relationship is in a phase of simple negotiations. Almost one in ten (9.6%) said their relationship is in a period of complex negotiations while 8.5% said their relationship is out of sync. Fifteen percent of CISOs blamed their challenges on management; 10% cited communication issues.*

These aren't the only challenges CISOs face. More than a quarter (26.3%) said they experience a moderate amount of duplication in considering or meeting the needs of multiple frameworks. Roughly one-sixth (15.8%) endure quite a bit of duplication and 37.4% have some duplication, but only a fifth (20.5%) said they have very little.

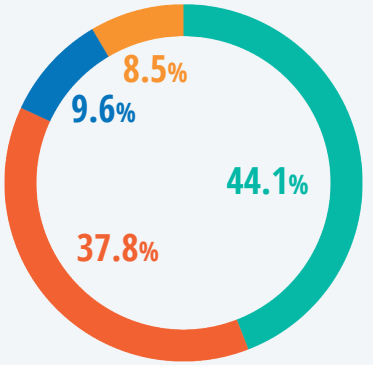
More than one-third of organizations (34.2%) hope to achieve their KPIs for compliance benchmarks by incentivizing (5.8%) success or by penalizing (9.5%) failure, or by implementing both incentives and penalties (18.9%). However, nearly two-thirds of organizations (65.8%) don't have any rewards or punishments in place.

LARGER ORGANIZATIONS TENDED TO BE PARTICULARLY CHALLENGED BY CONTROL MAPPING

Roughly half of CISOs (47.9%) cited evidence gathering as one of their greatest challenges in implementing new or updated frameworks. Even more (53.7%) pointed to skilled staff, followed by control mapping (43.6%), cost (38.3%), audit management (33.5%) and the rate of regulatory change (26.1%). Larger organizations (64.3% with 5,001-10,000 employees, 51.3% with 10,000+ employees, 59.1% with $501M-$1B in revenue and 51% with $1B+ in revenue) tended to be particularly challenged by control mapping. Most healthcare organizations (64.3%) faced this same challenge.

Larger, though not the largest organizations (71.4% with 5,001-10,000 employees and 68.2% with $501M-$1B in revenue), as well as education (66.7%) and entertainment and media (62.5%) companies, were most challenged when gathering evidence.

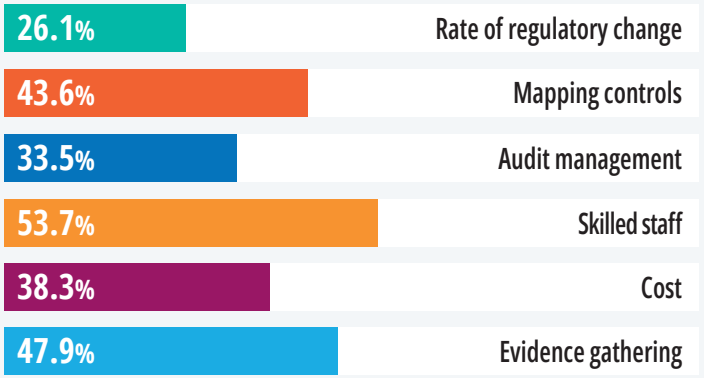
*Note: This data is based on an open-ended question in which respondents could manually write in their responses. The CISO Society asked survey participants, "How would you describe the relationship between compliance and security?" – a multiple-choice question, and followed up with, "If there are challenges, how could this be improved?" – an open-ended question.



How would you decribe the relationship between compliance and security?

- Completely synchronized
- Simple negotiations
- Complex negotiations
- Out of sync

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



I've been using GRC tools for over 20 years, and for most of that time they've been glorified spreadsheets that actually slow down my team's efforts to demonstrate compliance. Every little thing is click-click-click, and you spend as much time managing the tool as doing the work. As a vCISO, I'm incredibly excited about the promise of automated evidence collection and compliance-as-code. Maintaining compliance documentation across different frameworks across a dozen different clients is daunting. When GRC tools become an actual enabler and automation tool, they'll finally have delivered on their promise to simplify compliance.

JOSH ABLETT
CISO, Adelia Risk

COMPLIANCE AS CODE GAINS TRACTION BUT MANY CISOS ARE STILL NOT USING THE TECHNOLOGY

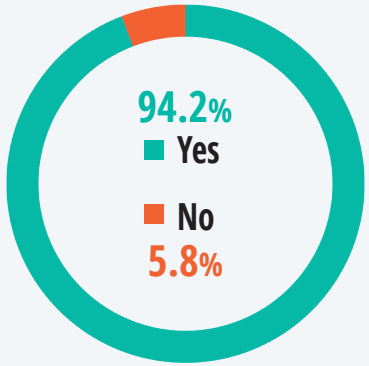
Regarding challenges that CISOs and/or their organization face in satisfying regulatory requirements, many (51.6%) were impacted by their maturing compliance program. Roughly two-fifths are challenged by evidence gathering (41.5%), data and system silos (42%), and the lack of a centralized system (40.4%). Others were challenged by regulatory change management (34.6%), audit readiness (33.5%) and control mapping (30.3%).

Regulatory change management proved to be the biggest sticking point for organizations with more than 10,000 employees (78.5%). On an industry basis, education businesses are equally challenged by audit readiness and their maturing compliance program (66.7%). Retail and consumer goods (75%) and entertainment and media (62.5%) corporations are coping with the lack of a centralized system, but retailers are also challenged by silos within their data (75%).

Just over 13% of CISOs are looking to technology to help solve their problems and have started to adopt or have plans to adopt Compliance as Code (OSCAL or OCSF). CISOs see a number of barriers to OSCAL adoption, including the belief that manual processes are easier (17.6%) and the assumption that current GRC processes are not broken (25.5%). More than one-third (37.2%) said that no platform has demonstrated its reliability and 41% said that OSCAL adoption is hindered by both a lack of usage and a difficulty in understanding its importance. That latter point resonated with retail and consumer goods companies, which said that OSCAL is still hard to understand. But for manufacturers (60%) and software and IT services companies (52.5%), the biggest barrier is that no one is using the technology.

If there's a silver lining here, it's that CISOs are interested in technology – they're just being very selective in which they choose. **Almost all (94.2%) believe that continuous controls monitoring will improve both compliance and security.** ■

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



As a seasoned security practitioner, I've seen firsthand how challenging it can be to truly align security, compliance, and risk. The research reveals a nuanced landscape: while less than half of organizations report a fully synchronized relationship between compliance and security teams, many CISOs are actively working to bridge the gaps. Unfortunately, they face significant hurdles in doing so. Over half of CISOs note that compliance is not embedded into their CI/ CD pipeline, and a staggering 80% admit to unnecessary duplication in their compliance efforts. The underlying truth is that even the most sophisticated GRC experts can be resistant to change, and organizational culture often presents the most formidable barrier. While establishing a Continuous Control Monitoring (CCM) framework might initially seem like a heavy lift, the long-term benefits of seamless security and compliance integration are undeniable: strategic alignment that ultimately strengthens an organization's entire security posture.

DALE HOAK
Sr. Director of Information Security, RegScale

MOST SECURITY LEADERS AREN'T SOLD ON GenAI JUST YET

Automation and Generative Artificial Intelligence (GenAI) continue to be two of the most talked about technologies. Approximately four out of five (79.8%) CISOs believe that a reduction in manual processing is the biggest opportunity to add automation to their compliance and risk management program. Roughly 50% expect automation to optimize compliance through a single pane of glass and nearly as many (46.3%) think the technology will allow them to more rapidly apply governance. One-third (33%) see an opportunity to supercharge staff while just over a quarter (27.7%) think that automation will improve the ROI on existing tools.

When asked which opportunity is their first priority, more than half (54.2%) of CISOs said they would prioritize a reduction in manual processing. Only 14.2% would prioritize the optimization of compliance through a single pane of glass and even fewer CISOs (12.1%) would prioritize the more rapid application of governance.

Automation may provide new opportunities to improve compliance and risk management, but that doesn't mean that CISOs are ready to universally adopt the technology or its AI companion. More than four-fifths (82.1%) of organizations are not currently using GenAI tools or functions within their compliance program and nearly one-third (33.2%) have incorporated automation without GenAI tools. Of those organizations, more than two-fifths (46.5%) are using automation to collect evidence or for control testing.*

Of those who do use GenAI, just under one-fifth (17.8%) deployed the technology to help with policy writing, policy review, policy updates and/or policy violations. Some (10.7%) rely on GenAI to assist in gathering and analyzing evidence while others (7%) use it to write regulatory submissions and to verify that controls meet regulatory requirements.**

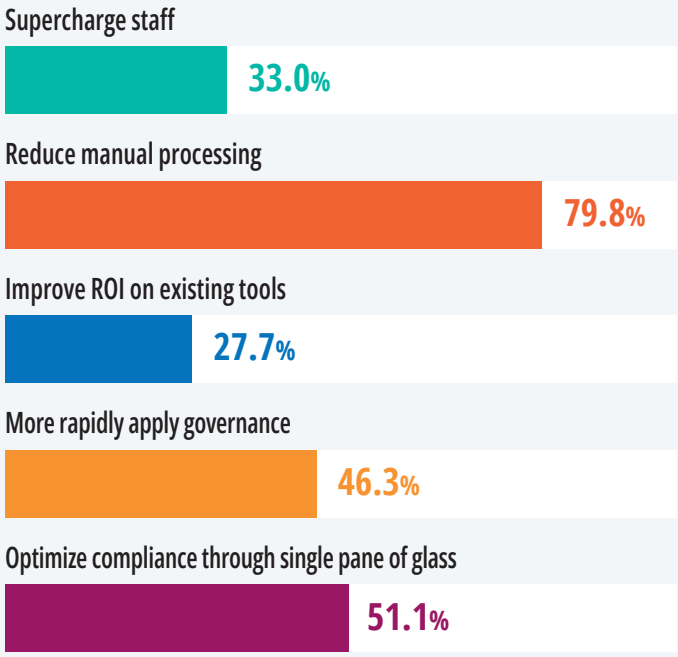
Small organizations (25% with 1-200 employees and 27.7% with less than $100M in revenue) were more likely to use GenAI. Small organizations (46.1% with 1-200 employees and 44.4% with less than $100M in revenue) were also more likely to incorporate automation in their compliance program without GenAI. However, most of the largest enterprises surveyed (89.7% with 10,000+ employees and 90.2% with $1B+ in revenue) have yet to deploy GenAI tools to support their compliance needs.

While GenAI adoption is minimal across all CISOs surveyed with just 17.9% using the technology within their compliance program, many appear to be preparing for its arrival. Nearly three-fourths (72.1%) have already developed policy and process language to ensure the tech is used responsibly, if and when it is actually deployed. ■

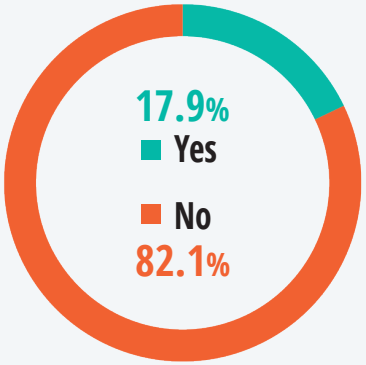
*Note: This data is based on an open-ended question in which respondents could manually write in their responses. The CISO Society asked survey participants, "Are you already incorporating automation in your compliance program that is not powered by GenAI tools?"– a yes/no question, and followed up with, "If yes, how?" – an open-ended question.

**Note: This data is based on an open-ended question in which respondents could manually write in their responses. The CISO Society asked survey participants, "Do you use GenAI tools or functions in your compliance program?" – a yes/no question, and followed up with, "If yes, how?" – an open-ended question.

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



Do you use GenAI tools or functions in your compliance program?



THE BOTTOM LINE IS THAT IT'S ALL ABOUT THE BOTTOM LINE

COST CONTINUES TO BE A TOP PRIORITY IN DETERMINING HOW COMPLIANCE IS MAINTAINED

Organizations of all types and sizes continue to be very budget-conscious about their compliance-related decisions. Almost one-third (31.1%) of CISOs believe that their company's resistance to change is primarily driven by financial matters. As expected, finances play a bigger role for small organizations (46.1% with 1-200 employees and 44.4% with less than $100M in revenue). Large enterprises (69.2% with 10,000+ employees and 70.5% with $1B+ in revenue) are more heavily influenced by company culture.

More than half of CISOs (55.8%) consider security and compliance to be a cost center versus a business enabler.

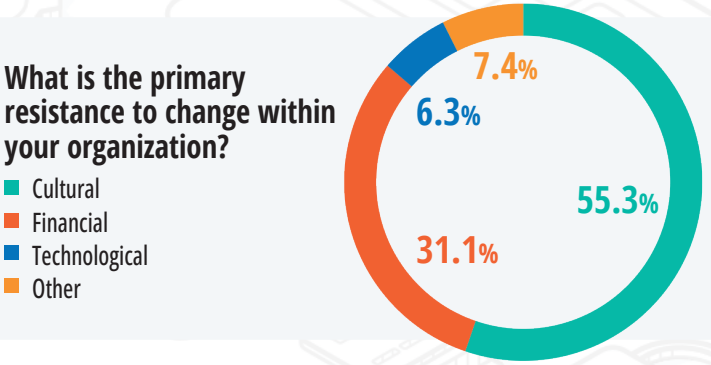
Large organizations (76.9% with 10,000+ employees and 70.5% with $1B+ in revenue) were more likely to hold this view. Comparatively, the smallest organizations surveyed (59.6% with 1-200 employees and 62.9% with less than $100M in revenue) consider security and compliance to be a business enabler.

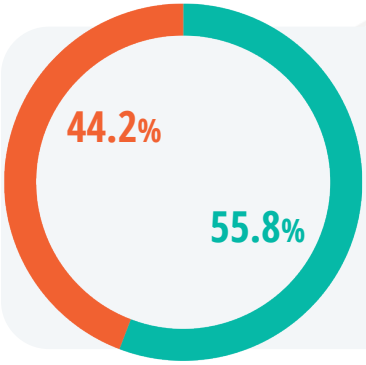
Monetary considerations are also on CISOs' minds when making decisions about company priorities. Nearly three-quarters (71.8%) said that their decisions are based on cost. Fifty-five percent are influenced by staffing and nearly as many (53.2%) take note of their organization's regulatory requirements. Only 19.7% said that their decisions are influenced by other things, including customer demands, ROI and strategic initiatives.

Company size (employees or revenue) did not significantly alter these results but there were notable differences across various industries. Cost proved to be a major priority for manufacturers (90%), healthcare providers (82.1%), entertainment and media companies (75%), and software and IT services companies (73.8%). Sixty-six percent of education businesses also considered the cost when making decisions, but they are more concerned about staffing (88.9%). Finance companies are most concerned about regulatory requirements (62.5%), but more than half (56.2%) also think about cost.

When asked which features/services are most important when selecting tools/vendors to provide governance and continuous controls monitoring, 69.7% said cost. This was second only to integrations (76.1%) but higher than security standards (53.7%), scalability (45.2%) and experience (38.8%).

What is the primary resistance to change within your organization?





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

- Cost Center
- Business enabler

We can't protect what we can't see. Security and compliance tools enable security teams to have better visibility into their environment. It is essential to identify, detect, and respond to incidents in a timely manner. These tools help reduce Mean Time to Detect (MTTD) and Mean Time to Resolve (MTTR). People are the first line of defense! An organization must foster a security-conscious culture, as security is the responsibility of every employee within their role.

QUYEN MCCARTHY
IT Security Ops Director, Jassby, Inc.

THE BOTTOM LINE IS THAT IT'S ALL ABOUT THE BOTTOM LINE

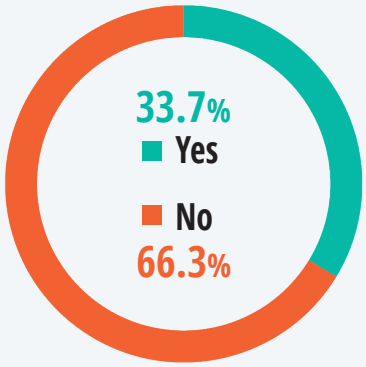
All manufacturers surveyed (100%) agree that cost is important, but software and IT services organizations (85.2%) and retail and consumer goods organizations (87.5%) are more heavily focused on integrations.

Despite the tremendous amount of thought that goes into the cost of doing business, two-thirds (66.3%) of all CISOs surveyed said that their organization does not measure the operational cost of managing compliance. Larger organizations (71.7% with 10,000+ employees and 74.5% with $1B+ in revenue) were most likely to say they do not measure this expense.

Of the organizations that do measure the operational cost of managing compliance, more than three quarters (75.4%) track all costs while 14.5% track compliance expenses and 10.1% track IT costs.

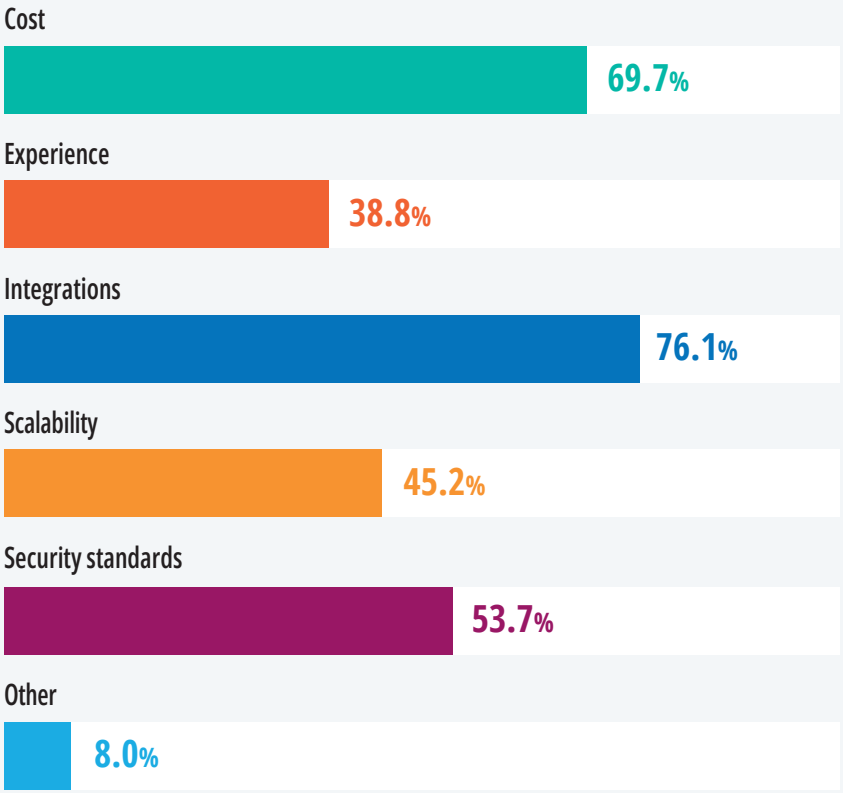
Many CISOs have also discovered that when using technology to enhance their compliance program, cost savings are not usually among the benefits. In fact, just 16.3% said they are compared to 33.2% of organizations that were able to supercharge their staff and 35.8% that used technology to minimize risk. Small- to medium-size businesses were more likely to say they experienced a cost benefit, with 22.4% of businesses with 201-1,000 employees and 21.9% with $101M-$500M in revenue stating that technology made a positive impact in this regard.

Do you measure the operational cost of managing compliane?



FINANCE SERVICE COMPANIES ARE MOST CONCERNED ABOUT REGULATORY REQUIREMENTS (62.5%), BUT MORE THAN HALF (56.2%) ALSO THINK ABOUT COST.

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



CONCLUSION

GRC INNOVATIONS MAY BE MISSED AS BUSINESSES PLAY IT SAFE AND ARE UNABLE TO DETERMINE HOW MUCH THEY SHOULD SPEND ON COMPLIANCE

The CISO Society 2025 State of Continuous Controls Monitoring Report reveals CISOs' views on GRC and applicable tools, how they're addressing their challenges, and the capital they're spending to achieve and maintain compliance. Nearly all CISOs (94.2%) are confident that continuous controls monitoring will improve compliance and security within their organization.

More than half (57.9%) use GRC tools to collect and maintain compliance evidence, but of those who don't, 46.2% blame it on their insufficient budget. Manufacturers, healthcare, education, and software and IT services organizations are particularly limited in this regard.

Budgetary challenges may explain why 71.8% of organizations emphasize cost when making important decisions. Just over 31% of CISOs said that budget and costs are behind their company's resistance to change. More than half (55.8%) consider security and compliance to be a cost center versus a business enabler. And yet 66.3% said their organization does not measure the operational cost of managing compliance. Without that information, they may not have clear insights into how much they actually spend and may be unable to determine how much they should spend.

With cost always top of mind, half of the CISOs admitted that their annual compliance budget has surpassed $200,000. However, most (82.1%) are not yet using GenAI tools or functions within their compliance program. Almost one-third (33.2%) have instead chosen to incorporate automation without GenAI tools, and nearly four-fifths (79.8%) are confident automation will reduce the burden of manual processing. More than one in ten (13%) are taking advantage of Compliance as Code (OSCAL or OCSF) but all respondents noted that there are barriers to adoption, including the belief that manual processes are easier. Forty-one percent attributed their lack of use to the fact that "no one" is using it. An equal number of respondents said that the technology is still hard to understand. This suggests that organizations need to better understand the benefits Compliance as Code provides, how it differs from existing solutions, and why they should give the technology a second look.

In order for tech providers to break through, there needs to be wider adoption in the industry. CISOs must also be more open to the idea that current processes don't need to break before change is embraced and that their compliance programs need more innovation than is currently used. While not all technologies prove to be a silver bullet, history has shown that nimble organizations – particularly those that are on the forefront of innovation – are far more successful than those that play it safe. ■

The CISO Society

RegScale