2023 Compliance Trends Report

The Rise of Continuous Compliance

DRATA

drata.com

Executive Summary

Welcome to the 2023 Compliance Trends Report, a research-based white paper that offers insights from growing companies.

This year, Drata surveyed 300 established and enterprise organizations to measure the pulse of the state of risk and compliance to identify trends, perceptions, and organizational impact. Through this research we identified three significant trends associated with compliance maturity, how much time companies are spending on related projects, and why they now feel it drives business forward.

Among the research takeaways, we identified a notable shift in perception around the value and outcomes compliance offers—moving away from a burden and towards a business accelerator.

In doing so, there was a clear divide between these two polarized perceptions, all of which were centered around the maturity level of an organization's compliance program. More specifically, **organizations who have adopted or achieved some level of continuous compliance identify compliance as a business accelerator,** whereas point-in-time or manual compliance is seen as a blocker or red tape. From these insights and others, the theme for this report emerged, *The Rise of Continuous Compliance*.

Throughout this paper, we will offer insights, analysis, and supporting information to further support this shift, and trends we can expect to see across the next five years.

Key Data Points

The following takeaways identify the most impactful trends discussed throughout this report:

100%

100% of organizations see **value in adopting continuous compliance.**

9 in 10

Over **9 in 10 companies plan to achieve continuous compliance** in the next five years.

87%

87% of organizations indicated negative outcomes as a result of low compliance maturity.

3 in 4

3 in 4 companies who have achieved some level of continuous compliance **feel their program is a business driver.**

76%

76% of companies who **follow a point-in-time compliance approach** feel the related effort is a burden.

4,300

IT and security professionals spend an average of **4,300 hours annually achieving or maintaining compliance.**

Contents: Inside the Report

Introduction

There's a mind shift on the horizon, and the way organizations implement risk and compliance programs will significantly change for the better. In the past, compliance has been perceived as a necessity, a box to check, and in some cases a burden. The cost of manual compliance and the time it takes away from other key priorities cause some leaders to treat compliance as a necessary evil. However, in the past few years, compliance has seen great strides that enable scalability, a reduction in manual effort, and better alignment with cybersecurity concepts.

This shift is directed by the maturing of compliance approaches. Companies are moving away from reactive and manual approaches, into a proactive compliance posture driven by automation. Security-first organizations now treat compliance as jumping-off points that lead to better security and risk reduction practices, align it with Zero Trust concepts, and considerably enable organizational transparency.

In turn, compliance has become a business accelerator, where those who have adopted it see greater organizational trust, shorter sales cycles, gains in competitive differentiations, and greater visibility beyond a point-in-time snapshot of their compliance posture.

This shift is due to the rise and adoption of continuous compliance, which will see a majority of companies pursuing it across the next five years.

> Continuous compliance is the technological concept that iterates beyond the constraints of point-in-time compliance. The concept enables organizations to use automation for greater visibility into the state of their risk and compliance controls.

A Brief History of Risk and Compliance

In 1992, now more than two decades in the past, SAS 70 was released and laid the groundwork for risk and compliance frameworks such as SSAE 16 (which birthed SOC 1, SOC 2, and SOC 3) in 2010, and separately, the International Organization for Standardization's (ISO) initial release of ISO 27001 in 2005. Amidst the evolution in frameworks that move beyond data centers and into the cloud, HIPAA was released in 1996 to protect private health information, and in 2018, the EU released GDPR to protect the data of its citizens.

During this time, compliance was frequently treated as a baseline or a checkbox that organizations must align with to prevent fines and reduce the possibility of breaches or other security incidents. Arguably, this is because the systems in place are considered arduous, burdensome, and require a steep learning curve to those who haven't started their compliance journey elsewhere. This is particularly detrimental to startups and small businesses who are already resource-constrained, but have a vision of their own to follow.

As a result, it's no surprise that companies of all sizes have historically seen compliance as a burdensome requirement, because that is exactly what it was. Compliance is driven by regulation with both tangible consequences for failure to comply, and just as many intangible reputational impacts to the business. Therefore, reactive or manual compliance is seen as a system that forces organizations to pull the e-brake and shift their energy and resources while the deliverable still only yields a snapshot in time.

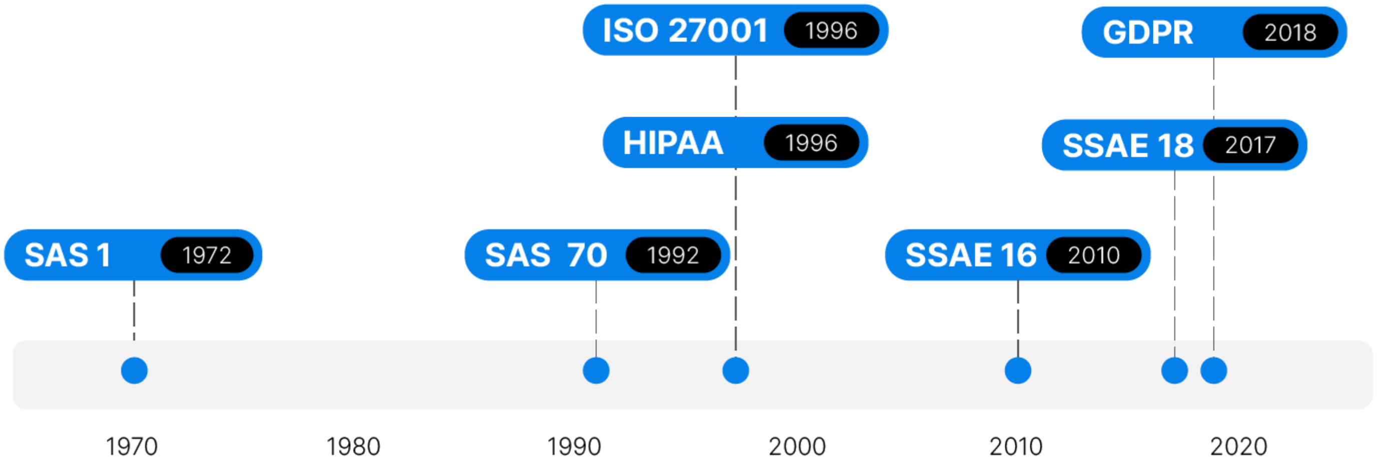
For some organizations, compliance can be misconstrued as a form of cybersecurity, because on the box, that is what it spells out—a system that requires processes and controls to ensure information is secure. Point-in-time compliance offers the foundation for cybersecurity, but is missing the critical element that allows it to truly bridge the gap; the difference being between reactive, active, and proactive states of compliance maturity.

The Rise of Continuous Compliance

As technology and user habits shift towards a world that needs Zero Trust concepts, organizations require constant verification and vigilance to achieve active and proactive states of compliance. To accomplish this, organizations are shifting to continuous compliance which intertwines people, processes, and technology resulting in full visibility of the status of risk and compliance controls.

More specifically, continuous compliance bridges the gap between scheduled third-party validation (attestations and audits) and uses automation to limit ambiguity or internal human bias/errors to prove evidence of compliance in real time. In turn, organizations gain cybersecurity capabilities that are otherwise unavailable to point-in-time or manual compliance processes. Continuous compliance is rapidly evolving, and within the next five years, it will further blur the line between compliance concepts and cybersecurity.

Throughout this paper we will support the conclusions above with the evidence of a research study supported by 300 risk and compliance professionals working in fast growing organizations across the United States.



Methodology

The findings are driven by an online survey of 300 U.S.-based growing and enterprise organizations. These organizations have between 300 and 1000 employees, and their revenue ranges from $1 million to $15 billion, with a majority averaging in the middle. Respondents represent a range of GRC-related and IT security titles.

Companies are represented across fintech, healthtech, SaaS, and other technology industries. In terms of compliance and what they maintain, surveyed companies align with ISO 27001, SOC 2, GDPR, CCPA, HIPAA, PCI-DSS, and others.

Shifting From Point-in-Time to Continuous Compliance

How Often Companies Review Compliance Controls

Compliance is as much a trust-building exercise as it is the foundation towards building mature security and risk management programs. One of the leading indicators that an organization is building a mature compliance program is that they're able to provide evidence beyond the requirements of individual frameworks.

More specifically, compliance has historically been treated as a checkbox that indicates a company has met the bare minimum requirements to protect customer/user data. However, mature organizations are taking advantage of continuous compliance (automation) to gain daily or real-time visibility into the status of their frameworks.

Take for example, AICPA's SOC 2 Type 2 audit report that assesses the controls of a service organization, typically for security purposes, and offers a snapshot in time typically ranging anywhere from three to 12 months. Within this audit window, organizations provide necessary evidence to a third-party accredited auditor during an attestation to demonstrate a company has the required controls in place to protect sensitive information.

Today, there are a multitude of approaches for a company to achieve and maintain compliance. A good analogy of the current state of compliance-related technology is that of how people manage their personal taxes each year.

For example, annual taxes can be manually completed using IRS provided forms necessary accounting steps, which can be a cumbersome process and is anxiety-inducing to anyone who has ever tried it. Others may choose a tool that walks you step by step through the process, asking you all the right questions to reduce risk (a tax audit or incorrectly reporting your income and deductions), and even integrate into your bank accounts and other financial platforms. And finally, for more complex scenarios like small business owners, multiple property owners, or other less common scenarios, it may not be worth the hassle of managing it yourself and you go to a CPA who provides hands-on guidance the entire way.

Like each of these approaches to annual taxes, the same can be applied to continuous compliance (automation) when compared to point-in-time or manual approaches. More specifically, we can map conducting your taxes manually to how an organization would manually collect related compliance and risk evidence, which is often managed through dozens of spreadsheets. A manual approach requires a high level of expertise around governance and related processes and organization with associated materials—and if there are any errors, you won’t know until after the fact.

Like tax accounting software that walks you step-by-step through the process, conducting compliance programs and related processes with a legacy GRC provides a similar outcome. These project management tools replace some spreadsheets with a platform, but the output and visibility can leave organizations at risk. While they reduce the level of governance expertise needed, you may become aware of any errors once it’s too late.

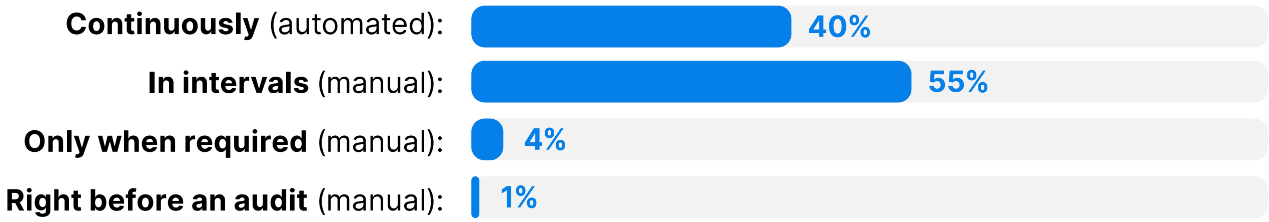
Lastly, there are tax accounting solutions that are highly configurable, integrate with existing financial institutions and platforms, and do all of the heavy lifting for you. This is most similar to compliance automation platforms that deliver continuous compliance. Unlike the former examples, these solutions enable real-time visibility into controls, evidence, and related tests—removing blindspots and encouraging a proactive state of compliance maturity.

> The resulting adoption of an automated solution enables organizations to move to a mature compliance status that enables proactive efforts. These proactive efforts build confidence and in turn, increase trust internally and externally.

This begs the question, is there value in checking the status of your various frameworks and controls on a daily basis?

Before we answer that, let's break down what compliance concept and level of maturity the surveyed organizations have achieved to date. When asked how often teams review the status of compliance controls, respondents said:

Frequency of Compliance Control Reviews



In this situation, continuous is defined as achieving up to real-time or daily verification of the status of controls or is on a pathway towards it.

The other three responses align with point-in-time compliance and lack the necessary automation for continuous verification. Intervals can be as little as once a month or once a quarter, and typically are based on the policies an organization sets or the requirements associated with the framework. The other two are self-explanatory, and indicate they follow a manual or reactive compliance approach.

> Today, **40% of respondents** have achieved some level of continuous compliance. However, **91% of respondents** indicated they are confident they will achieve continuous compliance in the next five years. Clearly, the direction the industry is heading is towards continuous compliance as the standard by which they are measured.

This is a clear indicator that nearly **3 in 4 organizations** feel there is value in continuous compliance and verifying the status of controls daily.

Reactive Compliance

According to the study, **87% of organizations** with a reactive compliance maturity faced negative consequences as a result. Manual compliance programs force teams into a reactive position that can create greater risk and put them in a more vulnerable state.

Simply being aware of a situation is half the battle, and without the capability of regular automated tests and evidence collection, there are known blindspots that prevent a team from adequately communicating the status of their controls and most likely security posture.

Although there is a clear indicator that the majority of respondents find value in continuous compliance, the consequences of those who do not currently have it indicate a range of concerning outcomes stretching from a slow down in business, security breaches, fines, and more.

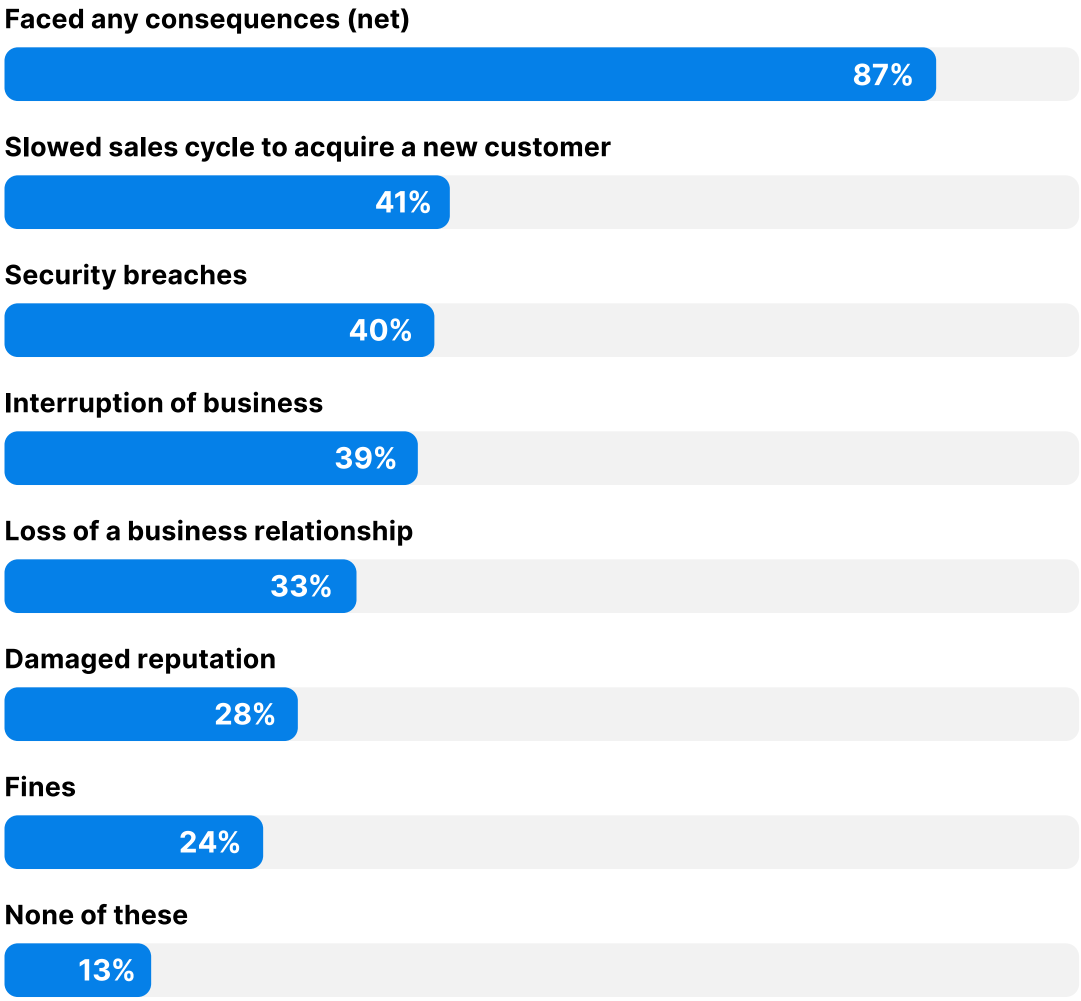
> According to the study, the great decelerator to businesses without continuous compliance is the direct impact to their bottom line. Of the respondents, **41%** indicated the most common impact is a slowdown on the sales cycle.

This can be in part due to a lack of necessary evidence beyond the snapshot manual compliance offers and needing bridge documentation or a lack of accessibility to policies—both of which impact a potential customer's ability to trust an organization's infrastructure.

Beyond business accelerators, the most concerning consequence suggests that 40% of respondents faced a security breach that may have been minimized blind spots created from manual compliance efforts.

Based on these findings, it's not surprising to see that related outcomes such as interruption to the business (39%), loss of business relationships (33%), damaged reputation (28%), and fines (24%) trailed not far beyond. However, of respondents, only 13% indicated that there have been no reported consequences for a lack of continuous compliance.

Consequences of Point-in-Time Compliance

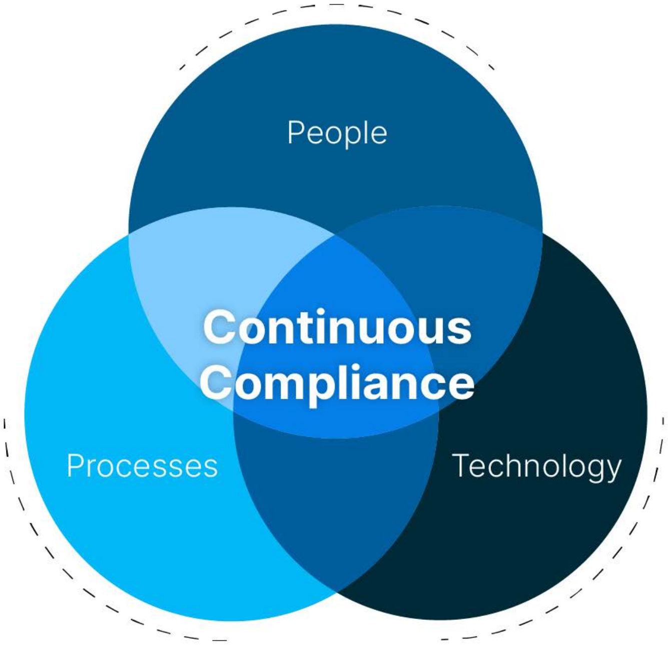


Achieving Continuous Compliance

> According to the survey, **100%** of respondents who have yet to achieve continuous compliance feel there is value in elevating their compliance maturity with automation.

The journey towards continuous compliance reduces many of the risks previously identified by teams with point-in-time compliance, and in fact, indicate signs of business acceleration.

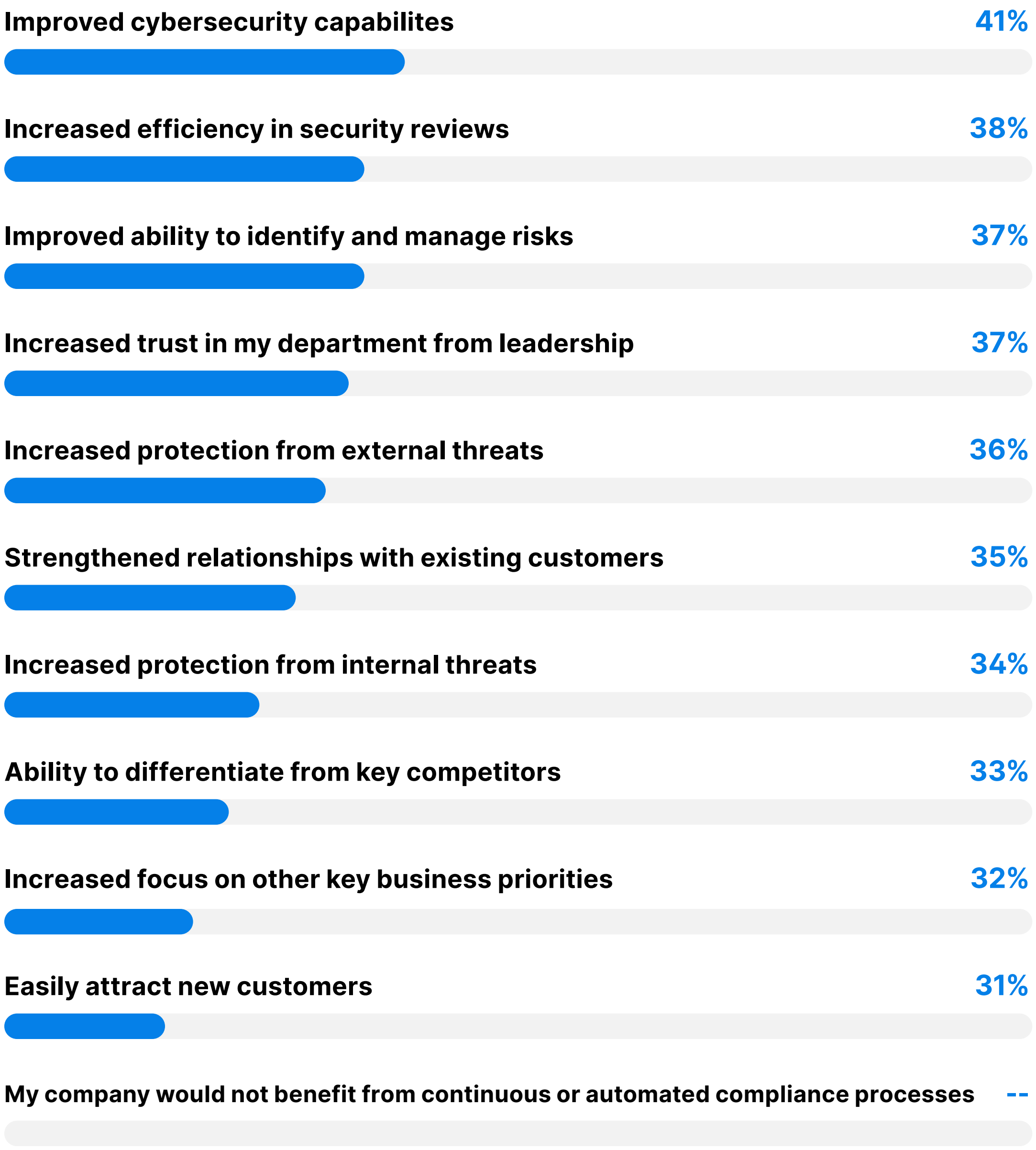
Processes and resources alone can't sufficiently fulfill the requirements necessary to achieve continuous compliance. In order to scale compliance capabilities, technology plays a critical role, and in particular automation. In fact, continuous compliance is achieved at the intersection of people, processes, and technology—a common theme among many robust cybersecurity concepts.



This elevated state of compliance maturity does require all three elements. It would be inefficient to build a program that required dozens, if not hundreds, of governance personnel to manually check the daily status of systems, reach out to multiple stakeholders for daily updates on personnel, and pull engineers away from work to manually review the status of something like an encrypted AWS bucket.

Beyond saving time and resources, survey respondents indicate that achieving continuous compliance will not only improve their security posture—while noting that point-in-time compliance practices are not cybersecurity in and of itself—but also build trust. In a world of Zero Trust, it's challenging to start with a baseline of zero and climb the mountain required to close deals and establish relationships, but respondents feel continuous compliance opens those doors.

Perceived Benefits of Continuous Compliance



Proactive Continuous Compliance Builds Trust and Accelerates Business

Among organizations who have already achieved some level of continuous compliance there are clear indicators that the concept enables them to move to a proactive maturity level and bridge the gap into cybersecurity. Among this group, 33% indicated they have already fully achieved a proactive state of compliance, whereas most others are seeing iterative benefits as they further mature processes.

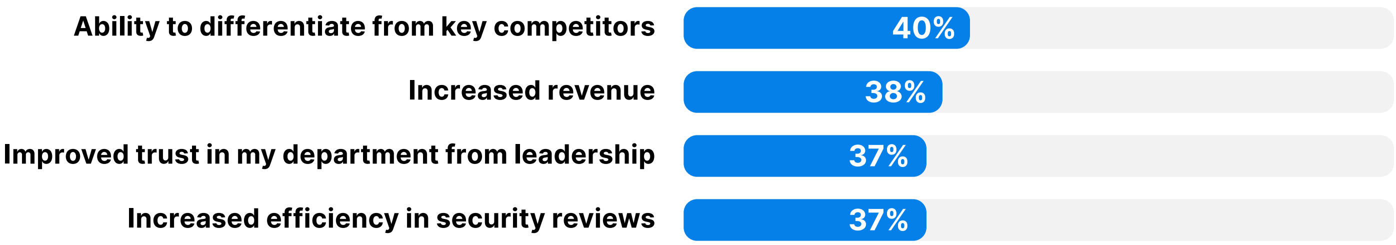
As stated in previous sections, point-in-time compliance lacks the necessary scalability or ability to incorporate the concept of trust through transparency due to it only offering a snapshot in time.

> According to surveyed organizations, the number one outcome of continuous compliance is their ability to build and establish trust.

More specifically, **67% of organizations** feel the concept enables them to more easily attract new customers. This data point aligns with the notion that many companies are still implementing the approach, and we expect to see across the board increases to nearly 100% across the next five years.

Similarly, constant verification of controls builds internal trust through increased visibility and even accelerates the business through revenue and market presence. Additionally, 33% of organizations were not only able to save time on getting and maintaining compliance, but are also able to shift more energy to accelerating the business.

Benefits of Continous Compliance, Some Level of Continous Compliance

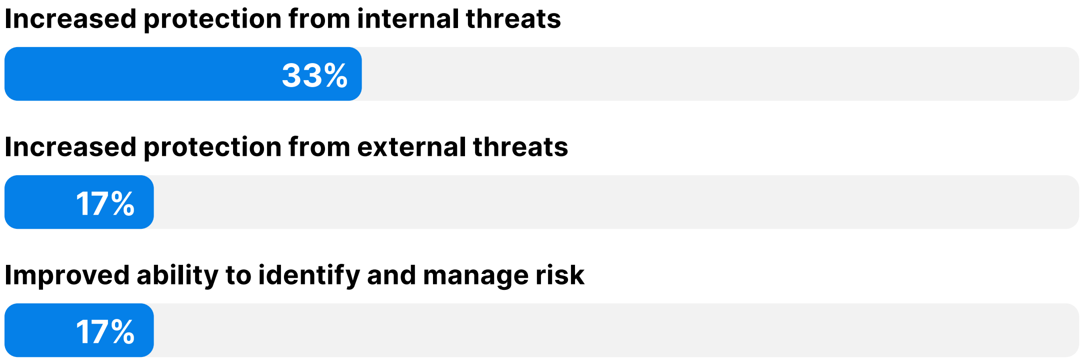


Continuous Compliance is the Foundation of Cybersecurity

Historically, compliance has always been a strong foundation for cybersecurity programs. Achieving a proactive or active state of compliance goes beyond that foundation and fully connects it as a bridge offering visibility into an organization's security posture. Automation reduces blindspots through constant verification—which is the key to building trust—but more importantly, the time to respond to risk vulnerabilities and breaches in policy.

Though today, continuous compliance is by no means a replacement for cybersecurity strategies, programs, or technology. Related technology enhances continuous compliance and creates a pathway towards a culture of security for newer organizations.

Benefits of Continuous Compliance, Achieved Continuous Compliance



Although there are many use cases for why continuous compliance is necessary in order to maintain a mature security posture, one of the most common concerns is the scalability of the organization and managing personnel.

Drivers Towards Compliance Maturity

As laid out in previous sections, the benefits of achieving a continuous or a proactive state of compliance enable organizations to build trust, accelerate the business, and even extend into cybersecurity capabilities. However, depending on the current compliance maturity level of an organization, there are hurdles that impact their ability to adopt the concept.

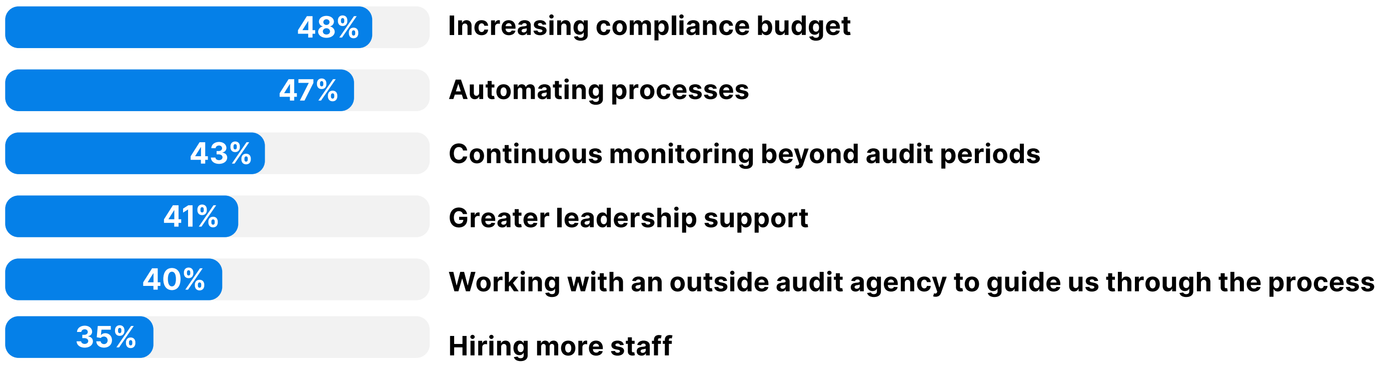
> Today, **60% of surveyed** organizations have yet to achieve some stage of continuous compliance; however, **91%** have a degree of confidence that they will reach continuous compliance in the next five years.

Filtering down further, **71% are completely or very confident**, and an additional **26% are somewhat or a little confident** they will reach continuous compliance in the next five years.

While this certainly offers a promising outlook and dedication towards trust building motions, there are trends that paint a clear picture among those who are less confident about their blockers.

Organizations who are less certain about their ability to achieve continuous compliance face challenges ranging from budget constraints, to priority of resources, and even internal buy-in. Among organizations surveyed, 65% of efforts to adopt continuous compliance are always or often deprioritized, and another 35% feel it is sometimes deprioritized due to other business goals or initiatives.

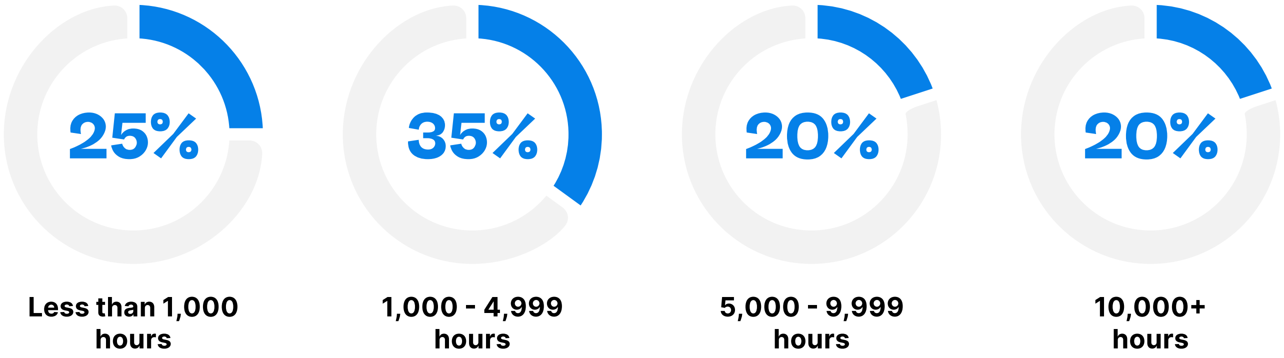
Compliance Maturity Gaps



As expected, when comparing organizations who have achieved some level of continuous compliance to those following a point-in-time approach, there are similar levels of concern around staffing. Staff shortages are a common point of contention for organizations of all sizes, but more specifically in association to engineering and cybersecurity skill sets.

In regards to staff requirements to maintain compliance, the primary factors are associated with frameworks/regulations they support, organizational size, and value of the program. However, there is one intriguing point of data that further illustrates an organization's compliance maturity level: overall related resources.

Hours Spent on Compliance per Year



Even though staffing and resources are a common issue, the above table indicates that related effort is not slowing down. This is a clear indicator that teams are being asked to do more with few resources and staff, and this is particularly true for those following a point-in-time approach.

However, among companies who have achieved some level of continuous compliance, there are several common threads:

67%

67% have **larger teams** (50% for point in time)

4,636

For large teams, 4,636 is the average annual hours spent on compliance (4,197 for point in time)

4,496

For smaller teams, 4,496 is the average annual hours spent on compliance (4,278 for point in time)

Tying the thread together, organizations who have achieved some level of continuous compliance are better equipped to demonstrate the value of their program, and in turn, dedicate more resources towards compliance and supporting additional frameworks. The side effect is that less unaffiliated staff are pulled into the process, or their roles are greatly minimized and puts less burden on other organizational priorities.

Tying the thread together, organizations who have achieved some level of continuous compliance are better equipped to demonstrate the value of their program, and in turn, dedicate more resources towards compliance and supporting additional frameworks. The side effect is that less unaffiliated staff are pulled into the process, or their roles are greatly minimized and puts less burden on other organizational priorities.

Confidence in Compliance on The Rise

Regardless of an organization's current state of compliance maturity, the good news is that the majority are generally confident in their program.

In the past year, 71% of organizations rated their compliance capabilities as excellent or very good, and only 29% as good or fair (0% self-rated as poor). When comparing an organization to that of their peers of a similar size and in the same industry, the results were slightly more favorable with 75% rated as excellent or very good, and 25% as good or fair.

However, breaking these numbers down further indicates that there is an incremental 10% improvement to compliance maturity between those who have achieved some level of continuous compliance and those who have yet to do so. More specifically, 77% of those who have achieved continuous compliance indicate an excellent or very good rating, whereas 67% of those following point-in-time compliance rated their program as excellent or very good. We expect greater levels of confidence in these programs across the next five years as more organizations get closer to their ideal compliance maturity level.

Budget and Resources Offer Greatest Impact to Risk Management

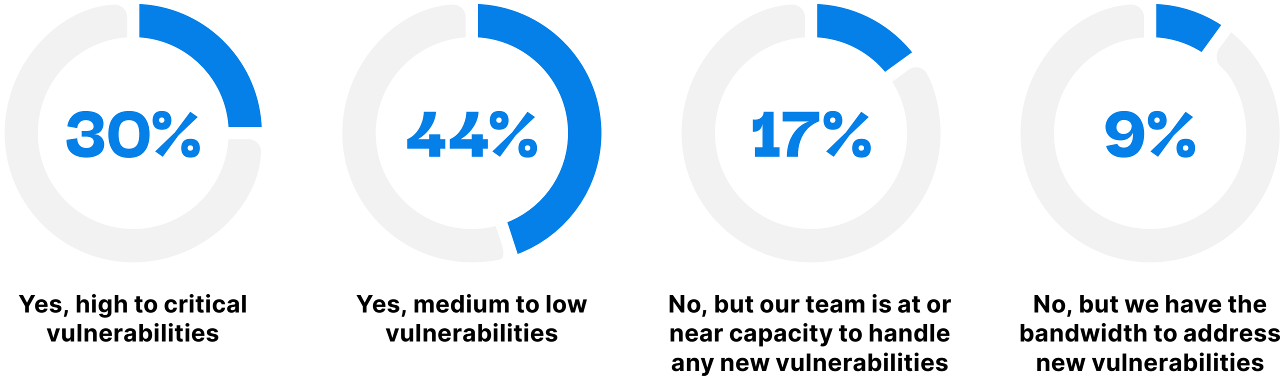
An organization's ability to assess, manage, and respond to risks are all key trust metrics wrapped in the umbrella of continuity. However, organizations state that budget and resources often play the largest role in related capabilities. In the context of compliance, risk not only encompasses cyber threats, but any organizational risk that impacts continuity.

Contributing metrics can be represented by service availability, mean time to resolution (MTTR) in the event of an outage, and how quickly an organization identifies incidents. Further, factors that most commonly trigger an outage or trust-breaking event are typically identified during risk assessments and continuous monitoring. But for less mature organizations with manual systems, these can become blindspots and negatively impact continuity metrics.

Two of the most impactful blockers that prevent an organization from enhancing their risk and compliance capabilities come down to budget (40% for point-in-time compliance, 30% for continuous) and resources.

> More specifically, **74% of organizations** feel they are not able to adequately address vulnerabilities due to budget and resources and only **9%** feel they have the necessary team.

Vulnerability Impact Due to Bandwidth and Resource Constraints



Even beyond these results, constraints to compliance and cybersecurity budgets are the norm; however, the above chart indicates clear consequences of inadequate resources that show in the form of drastic impacts to a key trust metric: business continuity.

Continuous Compliance Accelerates Businesses

Compliance should be a business accelerator; however, it is often seen as a burden or forced exercise. With this in mind, we sought out to find the why behind this sentiment, and any relevant trends or shifts in the market.

The foundational elements of risk and compliance established more than 20 years ago indicate, though typically required through regulation, that at its core was to always be a trust-building exercise. That exercise can offer third-party validation, a system that encourages organizations to be transparent with how they secure information, and the tools needed to build relationships.

The fact is that a majority of organizations agree with both statements. Of surveyed organizations, **74% feel that compliance is a burden** with **51% of them completely or strongly agreeing**, but there is only one leading reason behind this.

We analyzed multiple factors that could further narrow down the answer for why there is such a negative or burdensome perception of compliance. We can now confidently exclude risk monitoring and detection capabilities, confidence in user/employee adherence to security policies, and organization shifts in priorities as factors.

Our findings indicate that sentiment associated with compliance is directly connected to the current state of compliance maturity an organization has achieved.

> Our findings indicate that sentiment associated with compliance is directly connected to the current state of compliance maturity an organization has achieved.

Of organizations surveyed, **75%** who have achieved continuous compliance feel their program is a business accelerator, establishes trust, and bridges the gap into cybersecurity capabilities. Conversely, **76%** those who follow a point-in-time or manual compliance approach feel the related effort is burdensome or time consuming.

While continuous compliance is a newer concept, the technology that enables it is quickly advancing. Based on findings in this report, it's clear that relevant solutions should align compliance as business differentiator to increase revenue, build internal and external trust, and act as a strong foundation for cybersecurity.

To learn more about continuous compliance and how to move to a proactive state of compliance maturity, connect with our team.

Appendix A

Terms, Definitions, and Abbreviations

The following are common terms, definitions, or abbreviations used throughout this report.

Continuous Compliance (Proactive) is the technological concept that moves beyond point-in-time compliance that allows organizations to use automation for full visibility into the state of their risk and compliance controls. This concept merges people, processes, and technology to fulfill Zero Trust concepts of constant verification, and enables organizations to build trust through transparency.

Controls are policies, processes, and systems as they relate to various frameworks. Controls are also measures that an organization puts in place to meet regulations, industry standards, and laws as they relate to compliance. Related measures can range from physical, technical, or administrative; however, in regards to security compliance, some examples are access controls, data encryption, training programs, risk assessments, and related policies or procedures.

SOC 2 is a type of audit report that assesses the controls of a service organization related to security, availability, processing integrity, confidentiality, and privacy of the system. It is designed to give assurance to customers that the service organization has controls in place to protect their data and ensure the service is delivered effectively. The report is based on the AICPA's (American Institute of Certified Public Accountants) Trust Services Principles and Criteria. The report is intended to help organizations demonstrate to their customers and regulators that they have robust controls in place to protect sensitive information.

Point-in-Time Compliance (Reactive) is the legacy or manual compliance processes an organization follows to ensure it meets regulatory and privacy requirements. Though it may be assisted with technology, this process only yields deliverables that are locked into a specific window of time, and does not gain the benefits of automated tests or evidence collection, which in turn results in immature compliance practices and a reactive state.

Trust Through Transparency is a proactive organizational concept that aligns with companies who feel transparency is a critical element in building trust. Through technology and continuous compliance, organizations are able to share with customers, partners, and others in their ecosystem constant visibility into their security posture and controls. When applied with technology and automation, this removes ambiguity and human errors that are otherwise associated with point-in-time compliance or manual internal audits.