DRATA

↗ EXECUTIVE SUMMARY

Compliance Trends Report

The Rise of Continuous Compliance

EXECUTIVE SUMMARY

Welcome to the Executive Summary of our 2023 Compliance Trends Report. This document is a condensed version of our research-based whitepaper that measures the state of risk and compliance to identify trends, perceptions, and organizational impact. For the full version, please **download it here.**

By surveying 300 established and enterprise organizations, we identified trends associated with compliance maturity, how much time companies are spending on related projects, and the shift in perception of compliance—moving away from a burden and towards a business accelerator.

From these insights and others, the theme for this report emerged, **The Rise of Continuous Compliance.**

What is Continuous Compliance?

As technology and user habits shift toward a world that needs Zero Trust concepts, organizations require constant verification and vigilance to achieve active and proactive states of compliance. This is Continuous Compliance. More specifically, this concept bridges the gap between 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.

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

100%

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

4,300

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

9 in 10

over 9 in 10 companies **plan to achieve continuous compliance** in the next 5 years

3 in 4

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

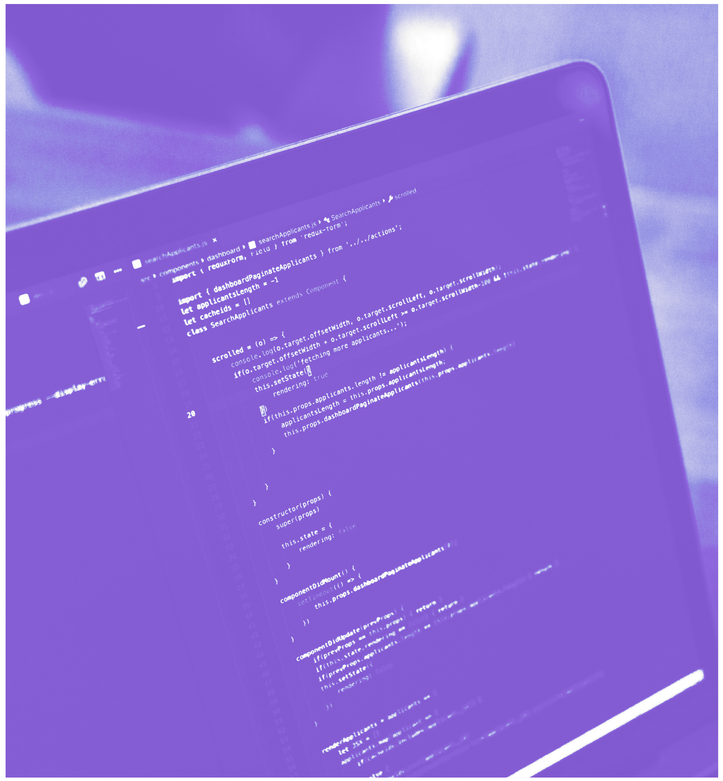
76%

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

87%

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

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.

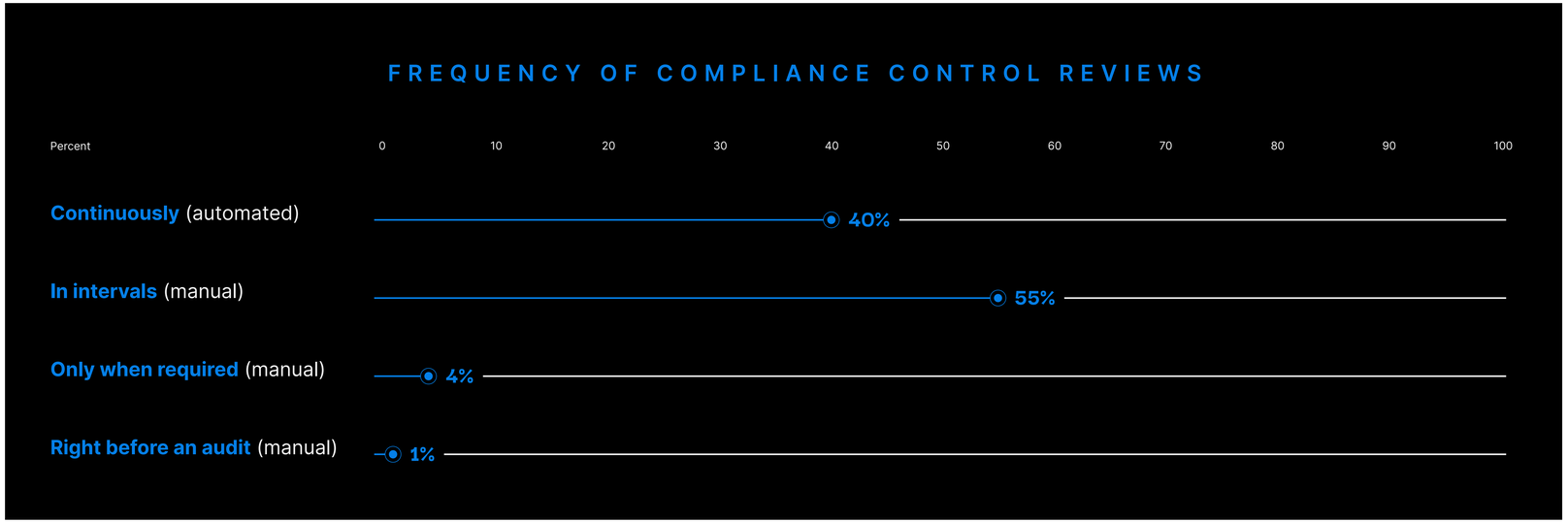
More specifically, compliance has historically been treated as a checkbox that indicates a company has met the bare minimum requirements to protect customer/user data. However, mature organizations are taking advantage of continuous compliance (automation) to gain daily or real-time visibility into the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

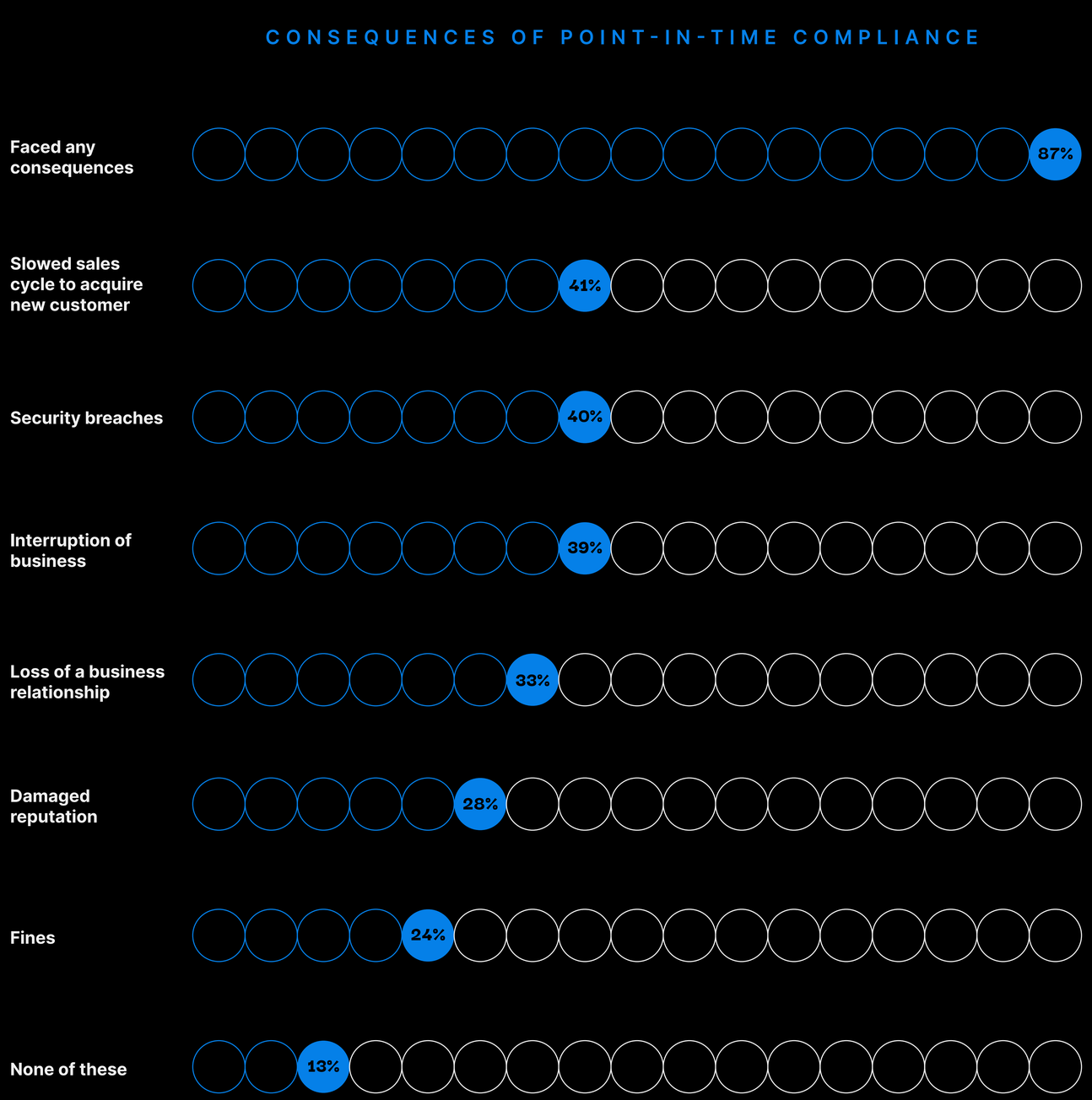
This begs the question, is there value real-time visibility into compliance? Before we answer that, let's see if our surveyed organizations currently run an automated or manual compliance process.

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

Today, **40% of respondents** have achieved some level of continuous compliance. However, 91% of respondents indicated they are confident that 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.**

In the following sections we'll cover the problems associated with reactive, point-in-time compliance and the benefits of continuous compliance.





Reactive Compliance Holds You Back

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 teams from adequately communicating the status of their controls and most likely security posture.

Proactive Continuous Compliance 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.

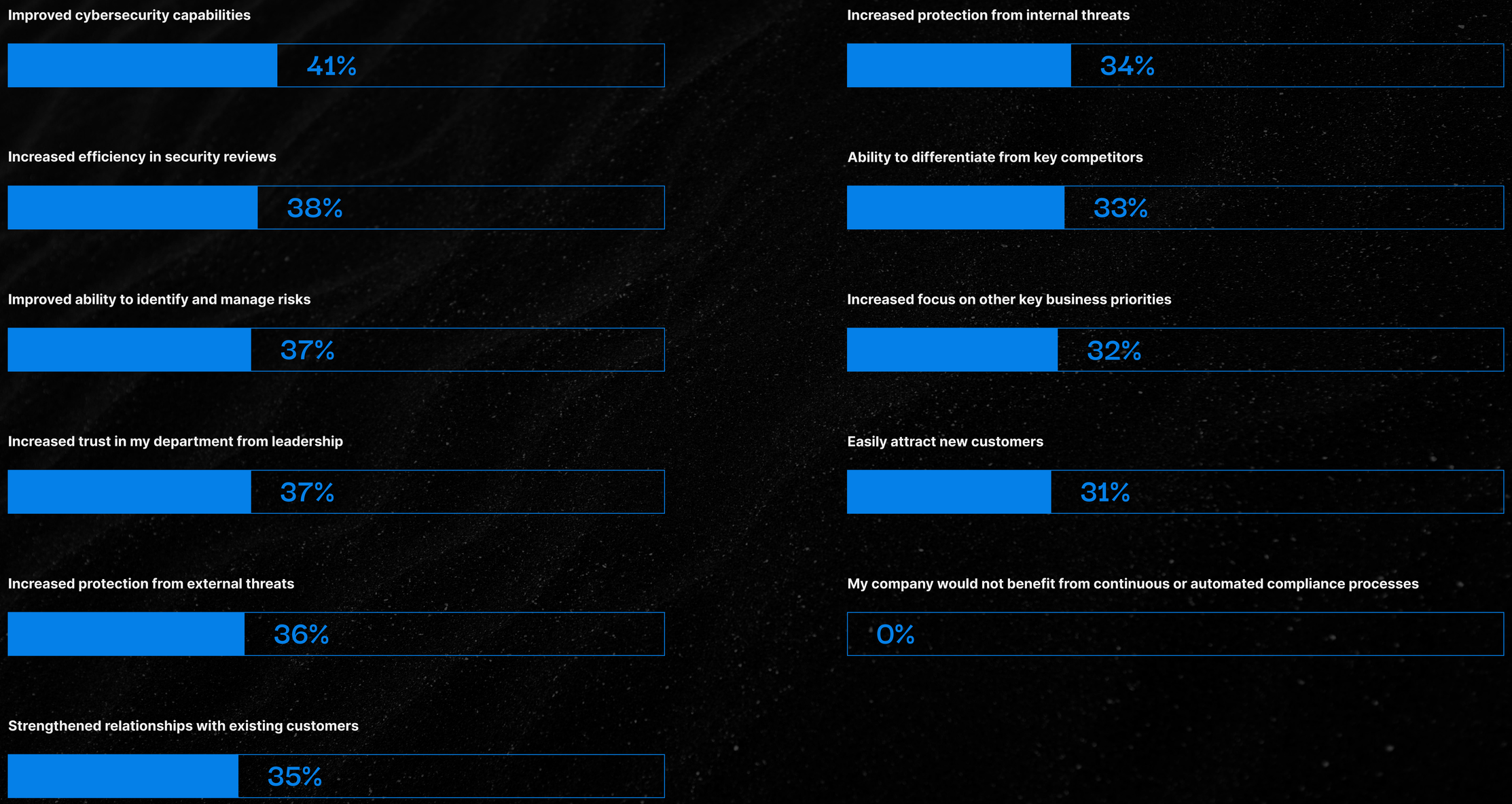
More specifically, **67% of organizations** feel the concept enables them to more easily attract new customers.

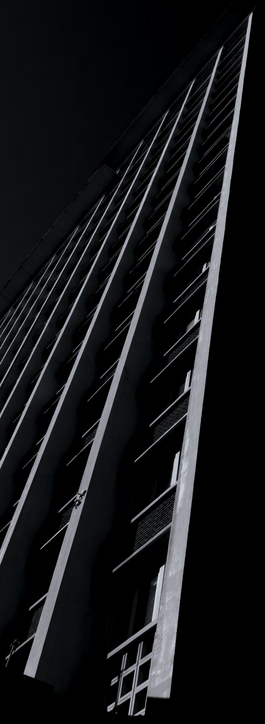
This data point aligns with the notion that many companies are still implementing the approach, and we expect to see across the board increases to nearly 100% across the next five years.

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.

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

FREQUENCY OF COMPLIANCE CONTROL REVIEWS



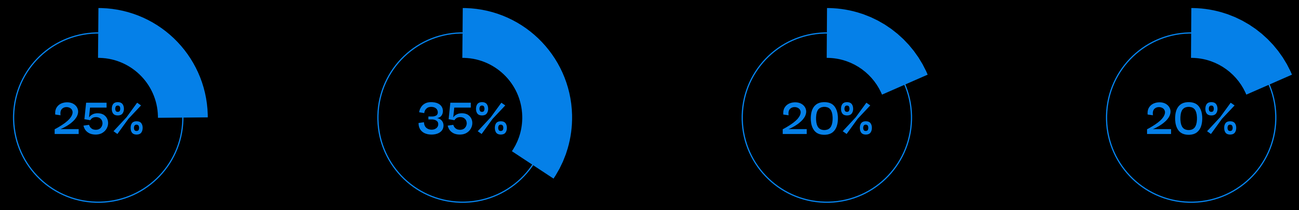


Drivers Toward Compliance Maturity

COMPLIANCE MATURITY GAPS

Increasing compliance budget	48%	Greater leadership support	41%
Automating processes	47%	Working with an outside audit agency to guide us through the process	40%
Continuous monitoring beyond audit periods	43%	Hiring more staff	35%

HOURS SPENT ON COMPLIANCE PER YEAR



Less than 1,000 hours	1,000 - 4,999 hours	5,000 - 9,999 hours	10,000+ hours

We've seen the benefits of continuous compliance. So what's preventing adoption?

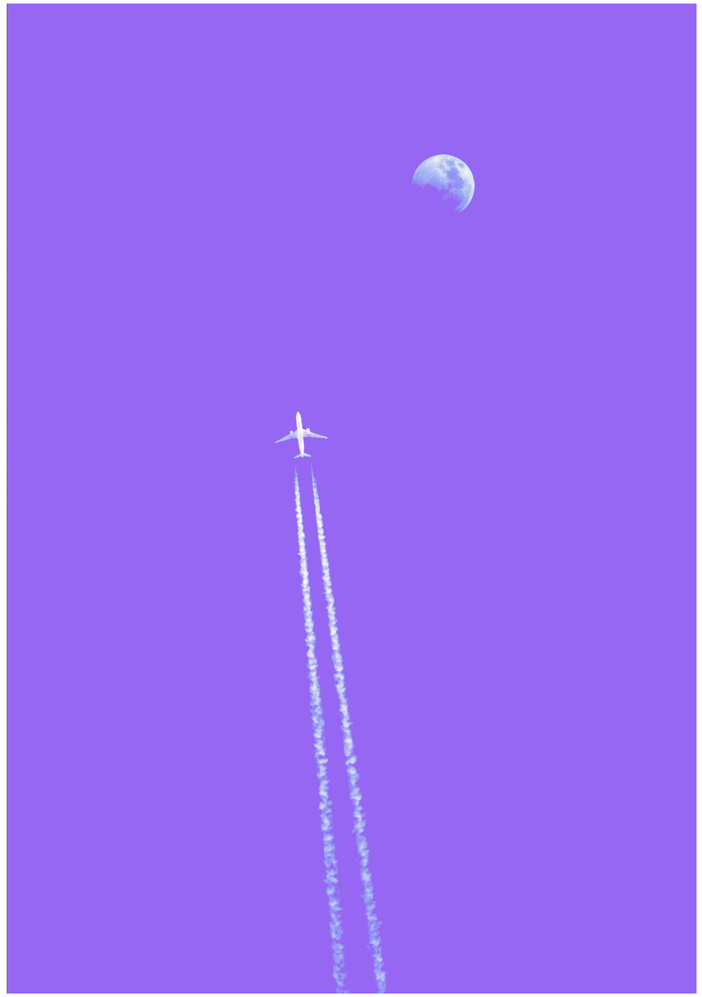
Organizations who are less certain about their ability to achieve continuous compliance face challenges ranging from budget constraints, to priority of resources, and even internal buy-in. Among organizations surveyed, **65% of efforts to adopt continuous compliance are always or often deprioritized,** and another 35% feel it is sometimes deprioritized due to other business goals or initiatives. In regards to staff requirements to maintain compliance, the primary factors are associated with the type and number of frameworks/regulations they support, organizational size, and value of the program.

Even though staffing and resources are a common issue, the above table indicates that related effort is not slowing down.

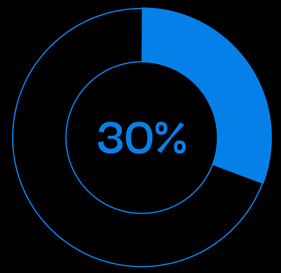
This is a clear indicator that teams are being asked to do more with few resources and staff, and this is particularly true for those following a point-in-time approach.

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.

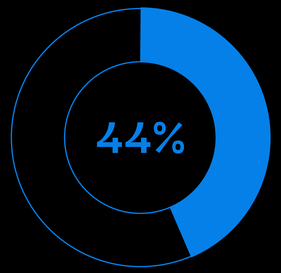
Confidence in Compliance is on The Rise



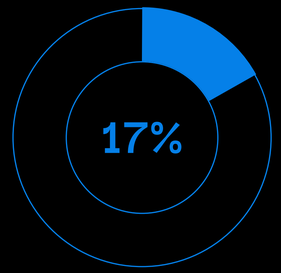
VULNERABILITY IMPACT DUE TO BANDWIDTH AND RESOURCE CONSTRAINTS



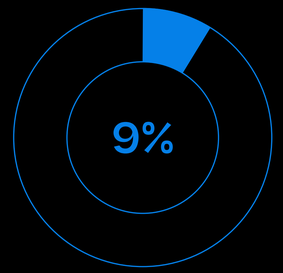
Yes, high to critical vulnerabilities



Yes, medium to low vulnerabilities



No, but our team is at or near capacity to handle any new vulnerabilities



No, but we have the bandwidth to address new vulnerabilities

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.

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, 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.

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.

Rethink and Reframe Compliance

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.

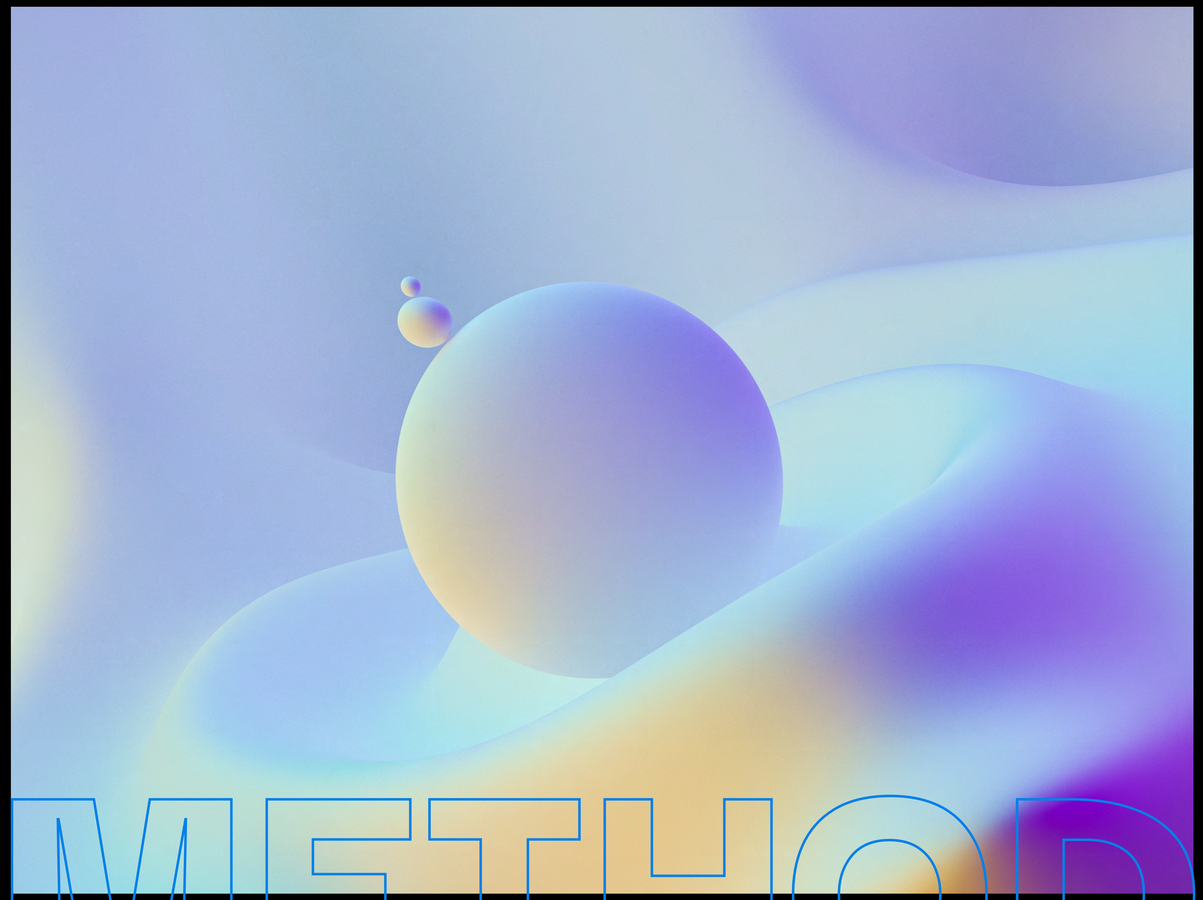
The fact is that a majority of organizations agree with both statements. Of surveyed organizations, **74% feel that compliance is a burden** with 51% of them completely or strongly agreeing, but there is only one leading reason behind this.

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.

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 a business differentiator to increase revenue, build internal and external trust, and act as a strong foundation for cybersecurity.



METHODOLOGY

DRATA

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.

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