

2023

State of Compliance Benchmark Report

Benchmark your compliance strategy against industry trends

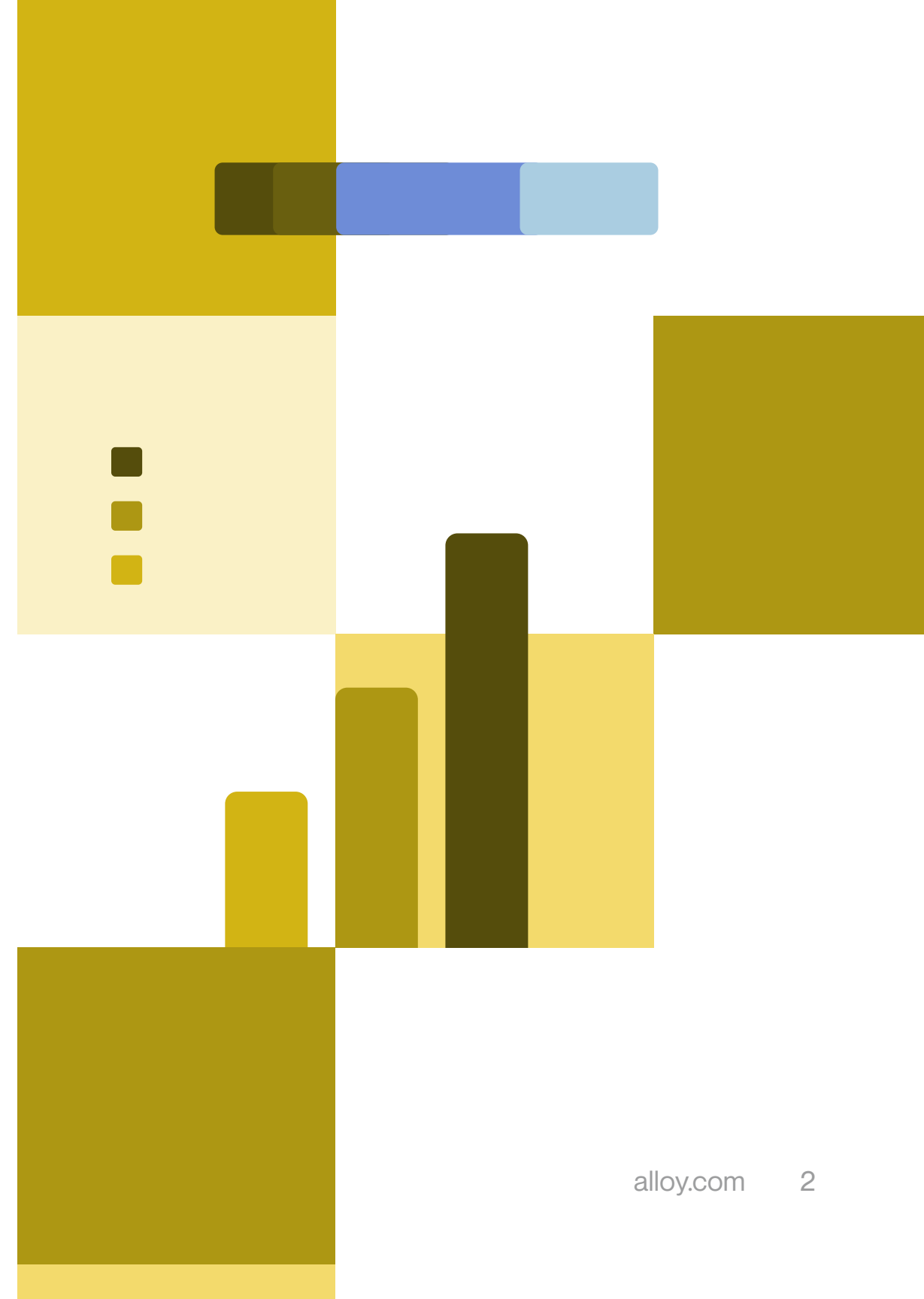


Introduction

The United States regulatory compliance landscape emerged when the first US operating bank was established in 1791 and has continued to evolve ever since. One of the most notable changes happened nearly two centuries later when the Bank Secrecy Act (BSA) was signed into law in 1970, requiring banks to report cash transactions over \$10,000.

In 2001, The Patriot Act was passed in response to the 9/11 terrorist attacks. The Patriot Act required banks to establish more robust anti-money laundering (AML) programs and perform customer due diligence, including Know Your Customer (KYC) and Know Your Business (KYB) checks, to prevent financial crimes such as terrorist financing, human trafficking, and money laundering.

In 2021, the Establishing New Authorities for Businesses Laundering and Enabling Risks to Security (ENABLERS) Act was introduced to close more gaps in the BSA by extending AML requirements to professional service providers involved in financial transactions — most notably third-party payment service providers and including some fintechs.



While not all fintechs are directly regulated (yet), many fintechs have partnerships with chartered banks that are regulated. Sponsor banks often include in their contracts that their fintech partners must adhere to their same compliance obligations. Contracts also typically state that fintechs are financially responsible for any fines the sponsor banks face due to non-compliance by their fintech partners. Over the past year, these bank/fintech partnerships have seen a lot of increased scrutiny from regulators, and that is not expected to slow down any time soon.

The stakes for compliance are high. Regulators can hand out hefty fines, shut down products, shutter companies, and even issue prison sentences. The increasingly complex global regulatory environment has added to the resource-intensive and legally onerous burden of compliance for financial services companies. Simply put, the set-it-and-forget approach to managing compliance no longer works. Instead, companies need to integrate compliance throughout the entire customer lifecycle.

Alloy surveyed more than 200 professionals working in compliance-related roles at fintechs, ranging from startups to some of the largest fintechs. We asked them about their compliance strategies and the effects of regulatory compliance on their organizations.

Table of contents

04	About the survey
08	Key findings
12	Compliance deep dive
26	SAR filings
29	Risk tolerance
32	Conclusion

About the survey

About the survey

Methodology

Alloy surveyed over 200 fintech professionals to understand industry perceptions of compliance, risk, and fraud within fintech.

Respondent Requirements

- Must be ages 18-65
- Must live in the U.S.
- Must work in Financial Technology or fintech industries
- Must have decision making knowledge when it comes to compliance decisions within their organization
- Must be at least a manager in Financial Technology/fintech

The survey was conducted by [Qualtrics](#), a leading survey platform that powers +1B surveys every year.



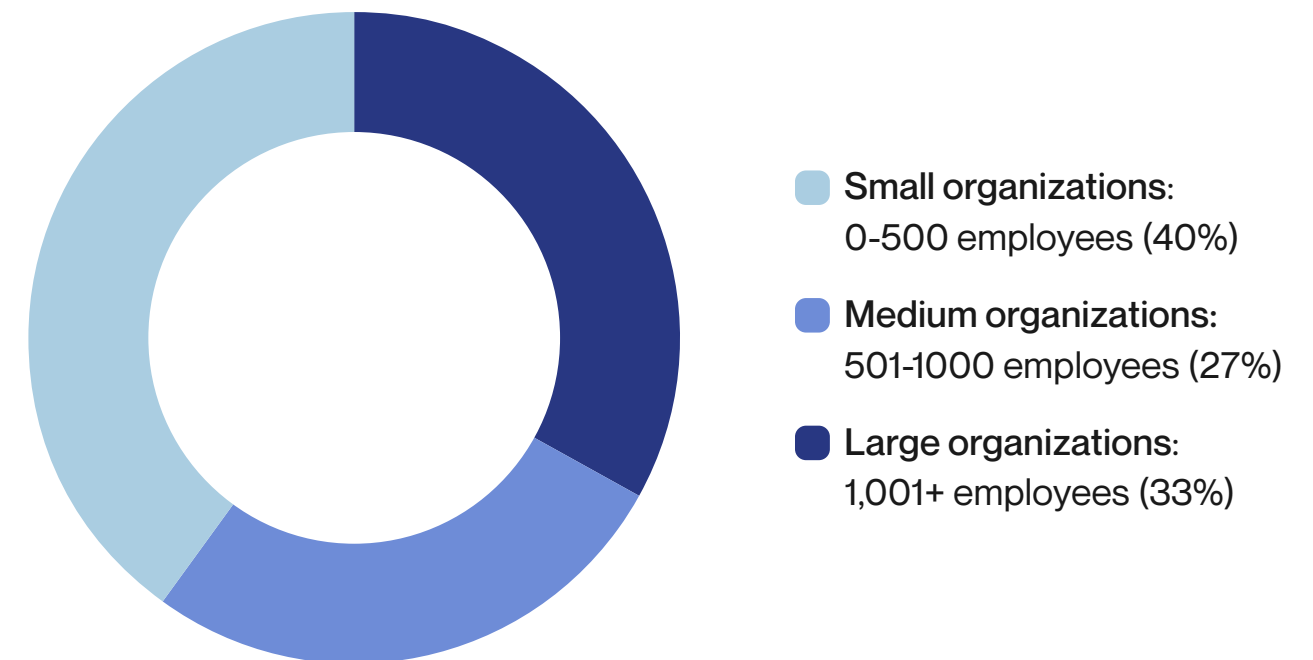
Dates fielded 6/6/23-6/12/23



Sample size 202N Total

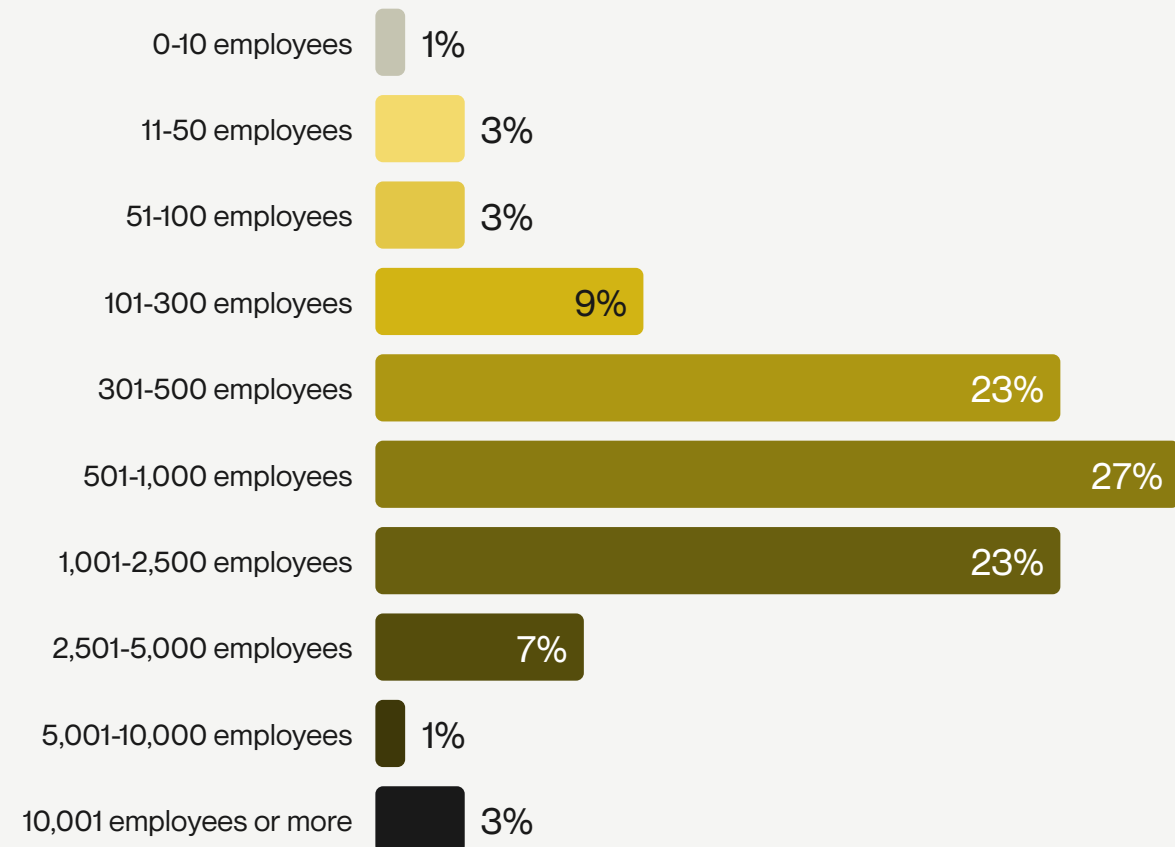
Demographic segments

All respondents self-identified as working in fintech. This means that some respondents may work at organizations that are directly regulated or are part of responsible bank/fintech partnerships, while other respondents may not be directly regulated.



Demographics | Total

Employees



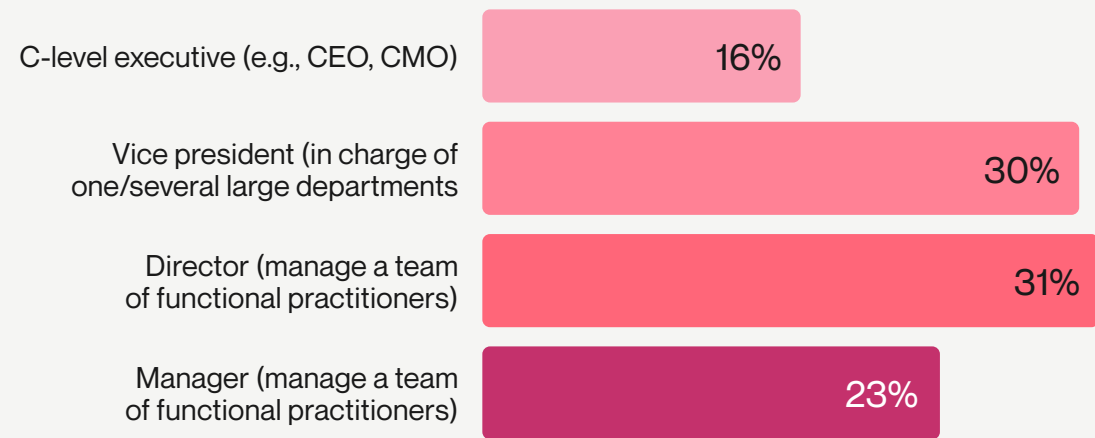
Knowledge and involvement in organization decision making

	Key Decision Maker	Decision Influencer	Significant knowledge but no decision making involvement	Some knowledge	No knowledge or involvement	Don't know/ doesn't apply
Fraud	60%	22%	7%	6%	3%	2%
Compliance	65%	28%	4%	3%	0%	0%
Risk technology	63%	20%	10%	6%	1%	0%

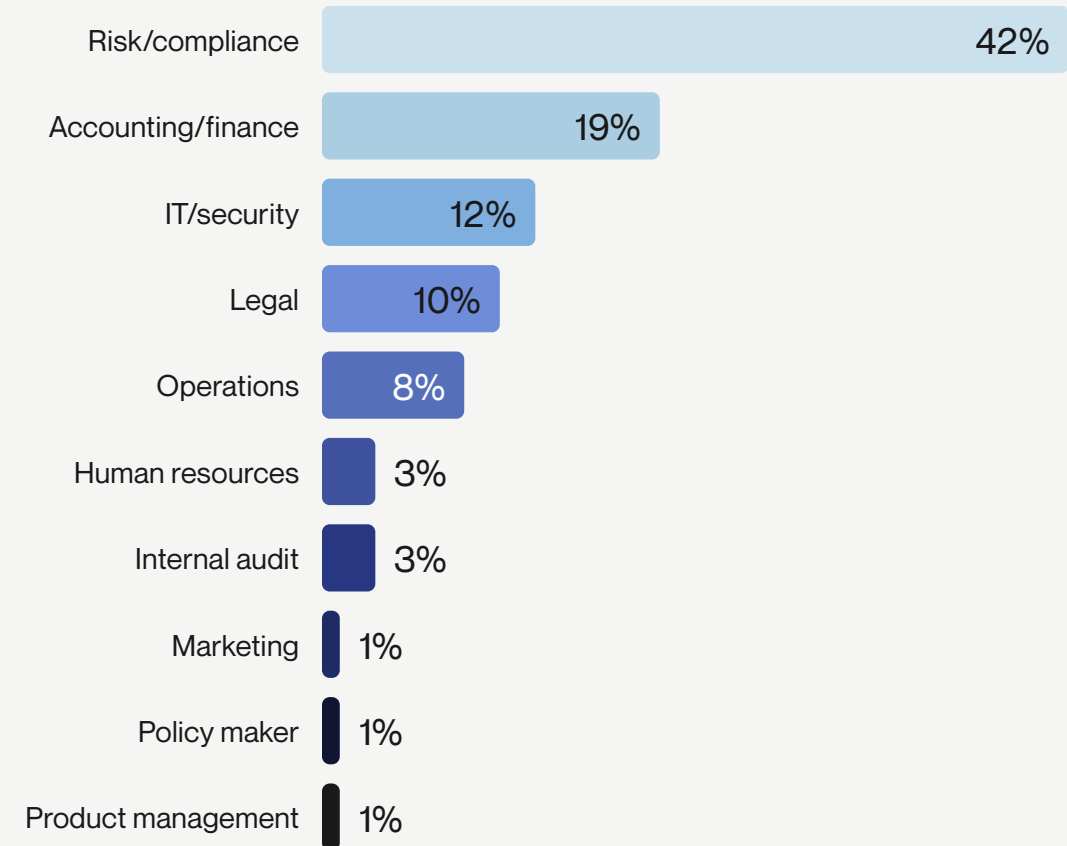
Demographics | Total

Job position

Respondents had to be at least a manager to qualify

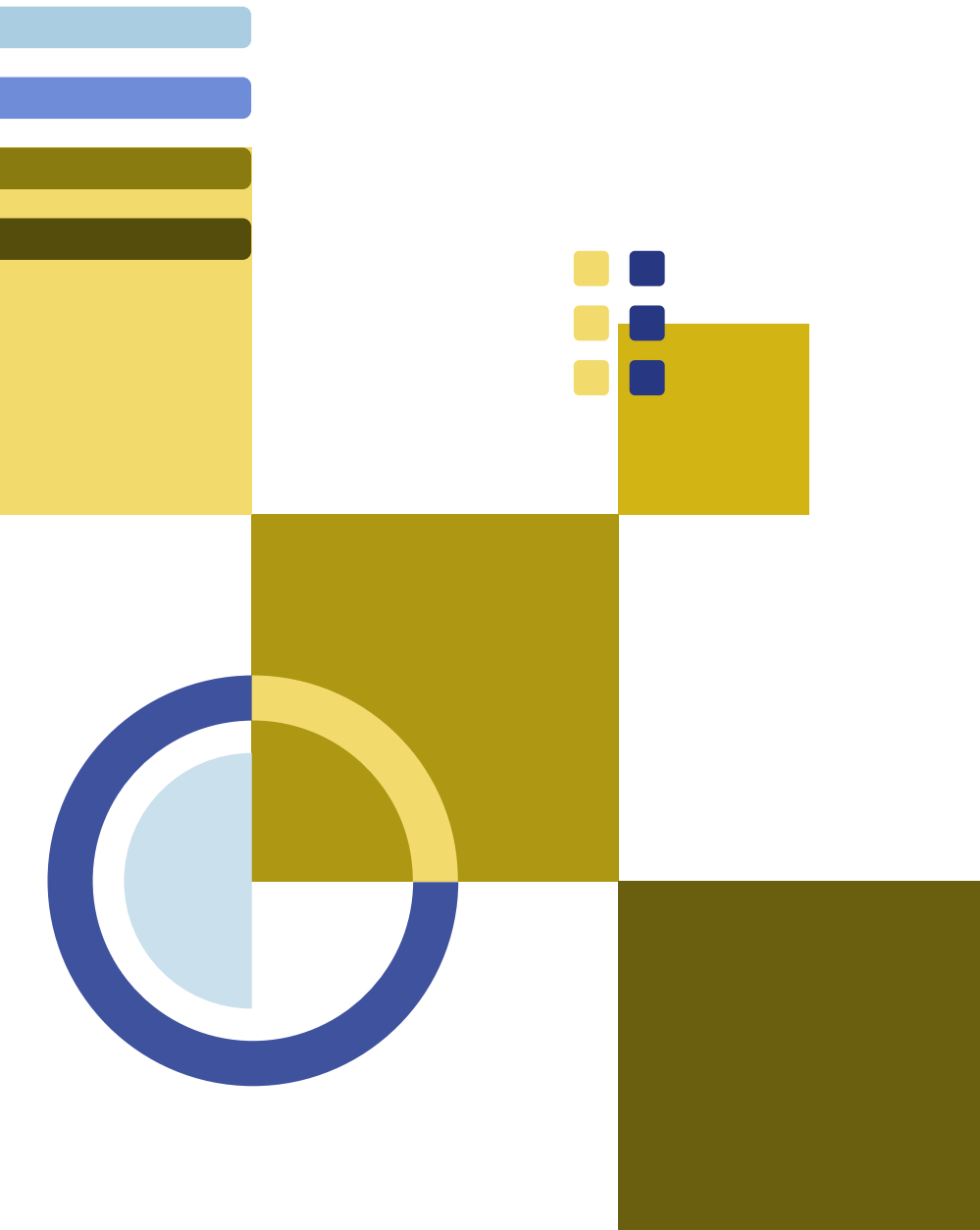


Current department



Key findings

Quick stats



● **93% of respondents** said it was somewhat or very challenging to meet compliance requirements

● **55% noted that lack of automation** is one of their biggest barriers to meeting BSA compliance requirements

● **84% of respondents** are using or exploring AI/ML to help them meet compliance requirements

● **86% of respondents** said their organization paid more than \$50,000 in compliance fines in the last year

Compliance



Challenges exist and companies are doing what they can to address them.

Organizations are allocating many resources to compliance-related activities, yet struggle to meet compliance requirements. Compliance teams have no shortage of support, dedicating several team members to compliance departments, utilizing third-party platforms for compliance management, and allocating enough funds on compliance-related activities. Most respondents are also currently using AI/ML or are open to using it for compliance.



Still, there is opportunity for continued improvement, especially when it comes to automation (writing/filing SARs etc.)

Despite compliance efforts, 93% of respondents find it at least somewhat challenging to meet compliance requirements within their organizations. One key barrier identified for meeting compliance requirements is a lack of automation. Dedicated compliance teams are spending much of their time writing and filing suspicious activity reports (SARs), suspicious transaction reports (STRs), and currency transaction reports (CTRs) which could be taking away time from more impactful compliance-related activities.



Fines have less of an impact on compliance decisions, but fuel concerns and could indirectly impact customer confidence.

Customer confidence has the greatest impact on compliance decisions. Fines have lower impact in general, but are considered a leading concern for compliance in the coming year. The ability to meet compliance requirements is less of a concern while the financial cost of compliance and financial loss from fraud will have an impact.

Other findings



SAR process varies by organization size.

Organizations have anywhere from 1-49 employees dedicated to filing SARs, while typically filing 0-10,000 per year. On average, it takes one to two weeks to create and file them. Money laundering and tax evasion are the leading indicators for suspicious activity.



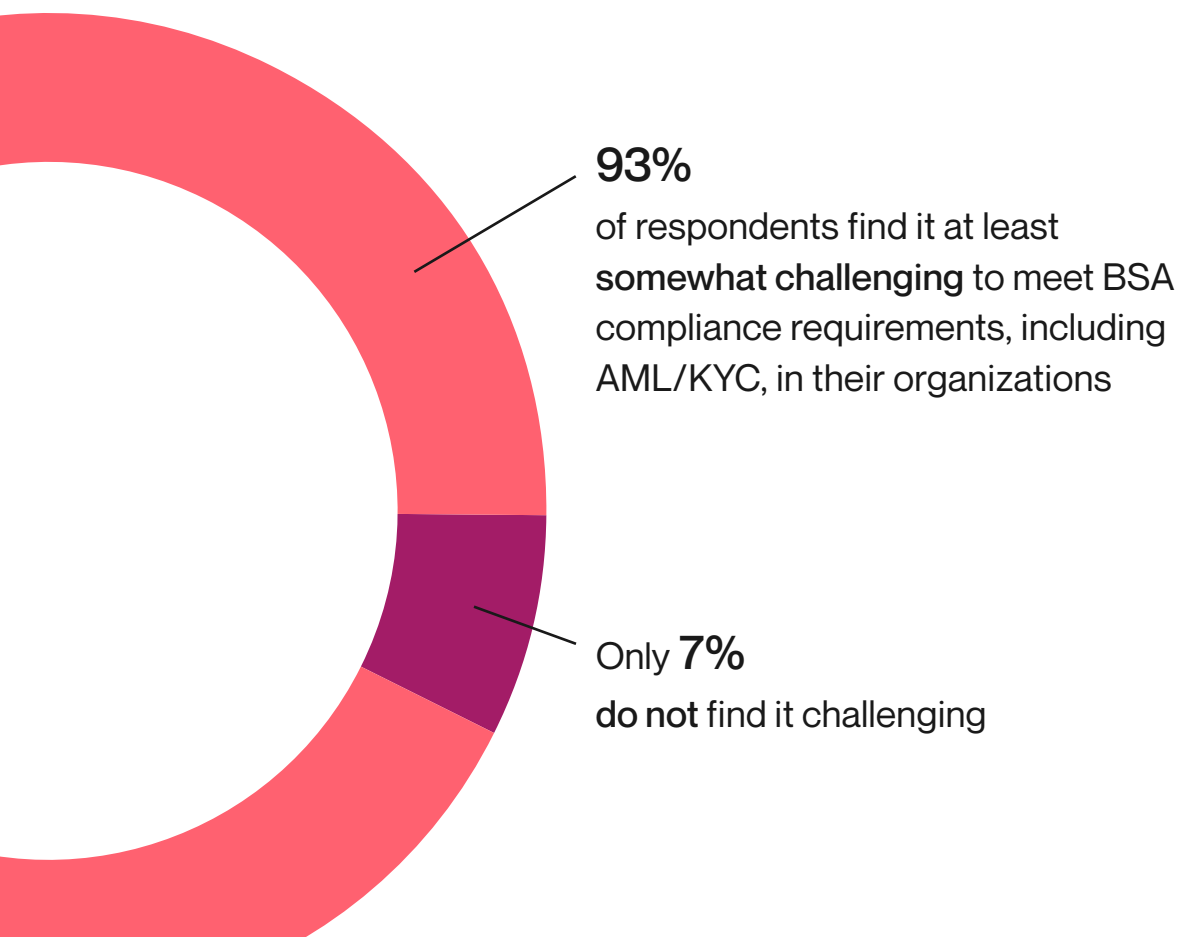
Risk tolerance is on the rise.

Risk tolerance has increased for 86% of respondents over the past year. Respondents said that changes in the regulatory environment as the top factor when determining their risk thresholds.

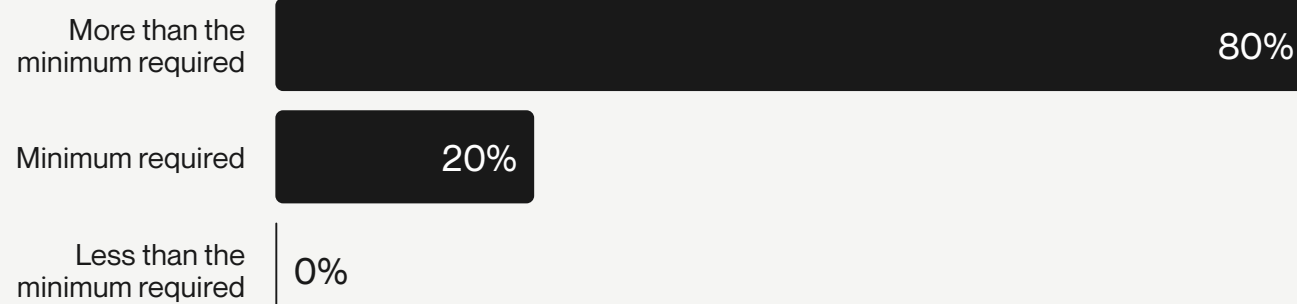
Compliance deep dive

Most fintechs go beyond minimum compliance requirements

Bank secrecy act (BSA) compliance requirements, including anti-money laundering (AML) and know your customer (KYC), are no walk in the park for organizations. Despite challenges, most organizations strive to do more than the minimum requirements.



Level of compliance requirements organizations are achieving



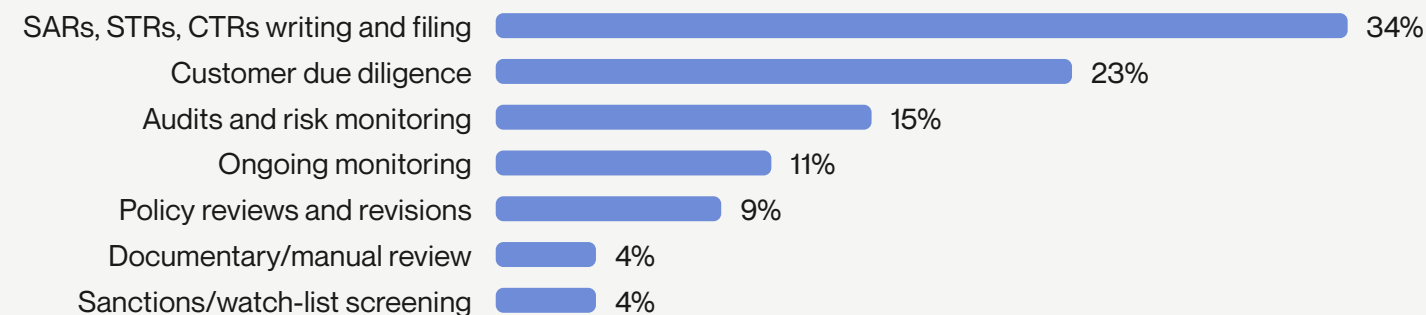
 Alloy insight

Organizations that go above and beyond the minimum required to achieve compliance are future-proofed against changes in the regulatory environment and taking a stronger stance against the rising threat that fraud poses on fintechs.

Fintechs are investing heavily in compliance teams

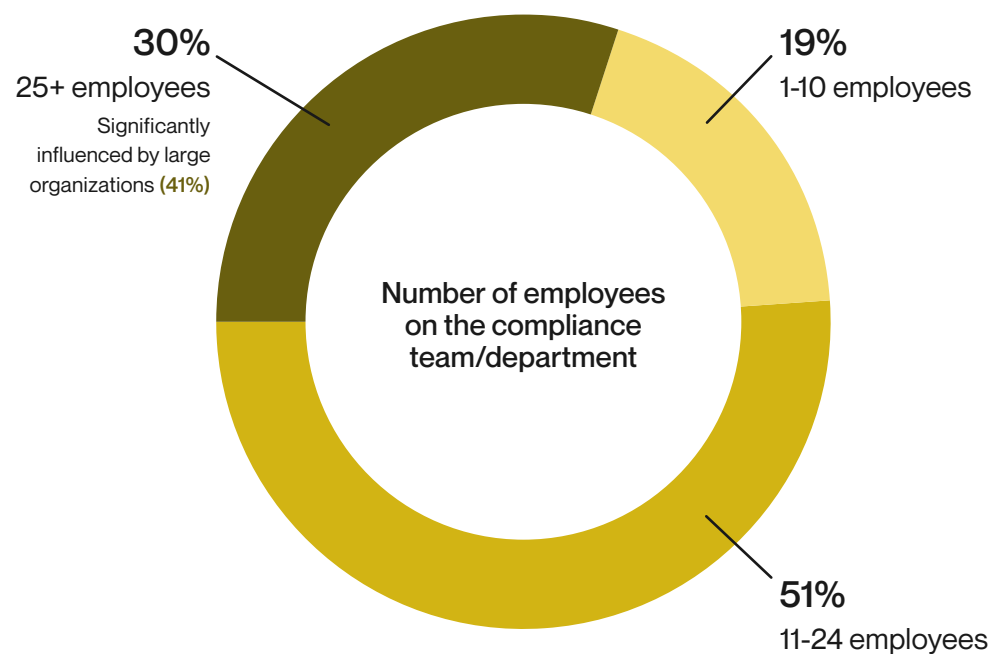
Compliance teams are typically comprised of 11+ employees, and they spend most of their time writing and filing suspicious activity reports (SARs), suspicious transaction reports (STRs), and currency transaction reports (CTRs).

What aspect of compliance management requires the most time?

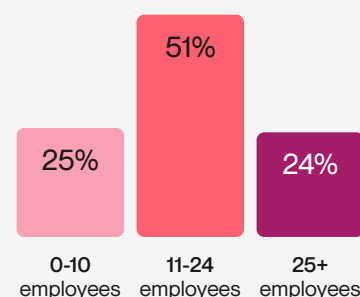


BENCHMARK

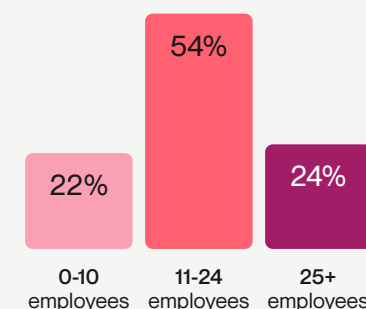
Small and medium organizations typically have 11-24 employees on their compliance teams. Unsurprisingly, large organizations compliance teams skew slightly bigger.



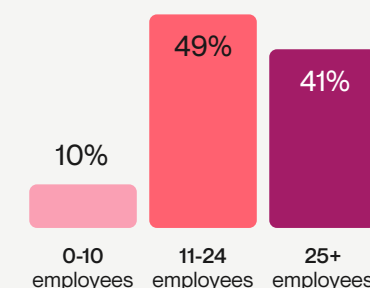
Small organizations 0-500 employees



Medium organizations 501-1,000 employees



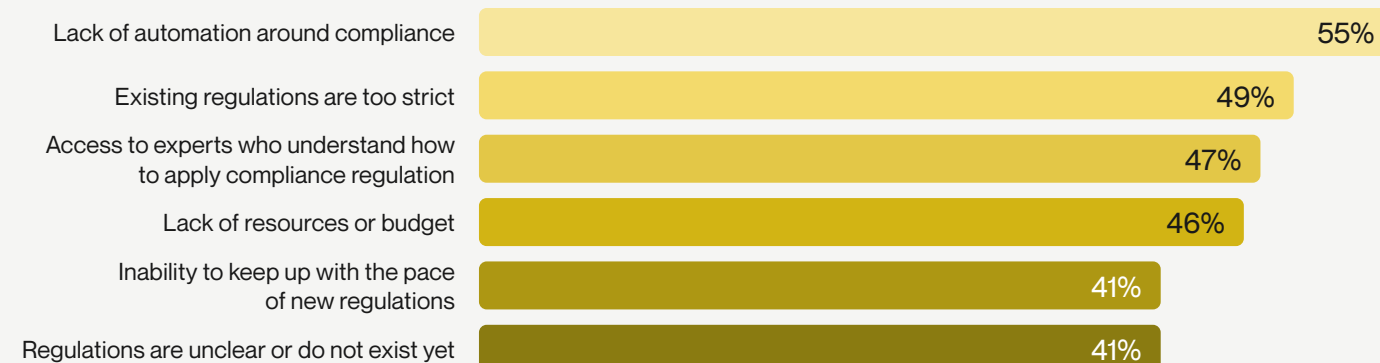
Large organizations 1,001+ employees



Lack of automation is the leading barrier for meeting BSA requirements

In general, lack of automation is perceived as the biggest barrier to meeting BSA requirements, including AML and KYC. Organizations spend the most time filing and writing SARs, STRs, and CTRs (pg. 10-11), which could represent opportunity for further automation.

Leading barriers to meeting compliance requirements



BENCHMARK


Barriers to compliance differ slightly by organization size

Existing regulations is the leading barrier for small organizations. Meanwhile, lack of automation is the top barrier for medium-sized organizations, and unclear or yet to exist regulations is the leader for large organizations.



Lack of automation is the leading barrier for meeting BSA requirements for all job titles, *except Vice Presidents*

Consistent with the total respondent pool, lack of automation around compliance is the leading barrier to meeting BSA compliance requirements. VP's identify unclear or nonexistent regulations as their leading barrier.

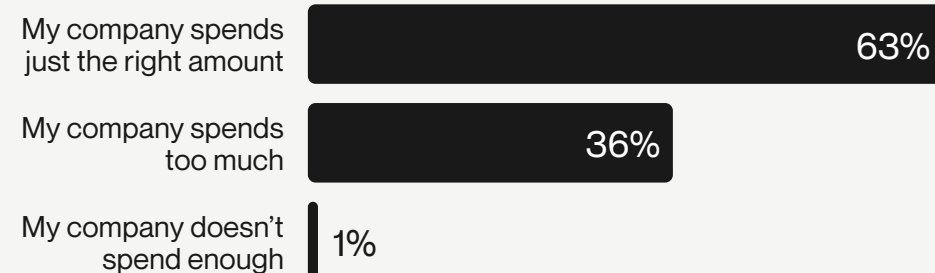
 Text color indicates leading barrier for that group

	C-Level Executive n=32	Vice President n=60	Director n=63	Manager n=47
Lack of automation around compliance	63%	42%	67%	53%
Existing regulations are too strict	63%	40%	49%	49%
Access to experts who understand how to apply compliance regulation	50%	45%	48%	45%
Lack of resources or budget	56%	30%	60%	28%
Regulations are unclear or do not exist yet	41%	50%	33%	40%

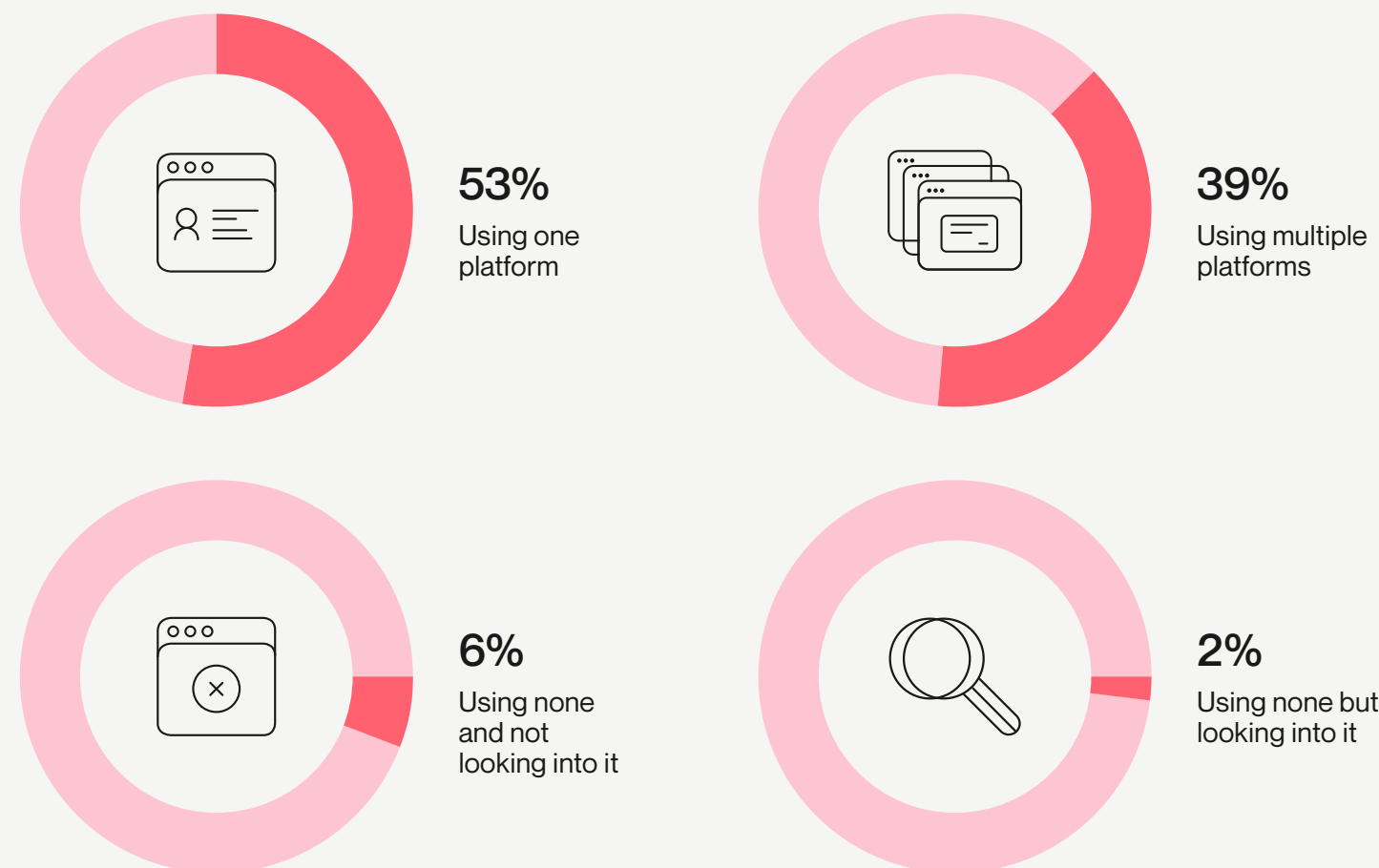
Companies believe their investments in compliance are worthwhile and most use at least one third-party platform

Two-thirds of respondents believe their organization is spending enough on compliance-related activities, while roughly one-third believe they are spending too much. 93% of respondents indicate their organization is using at least one third-party platform.

Feelings towards organization compliance-related activities budget



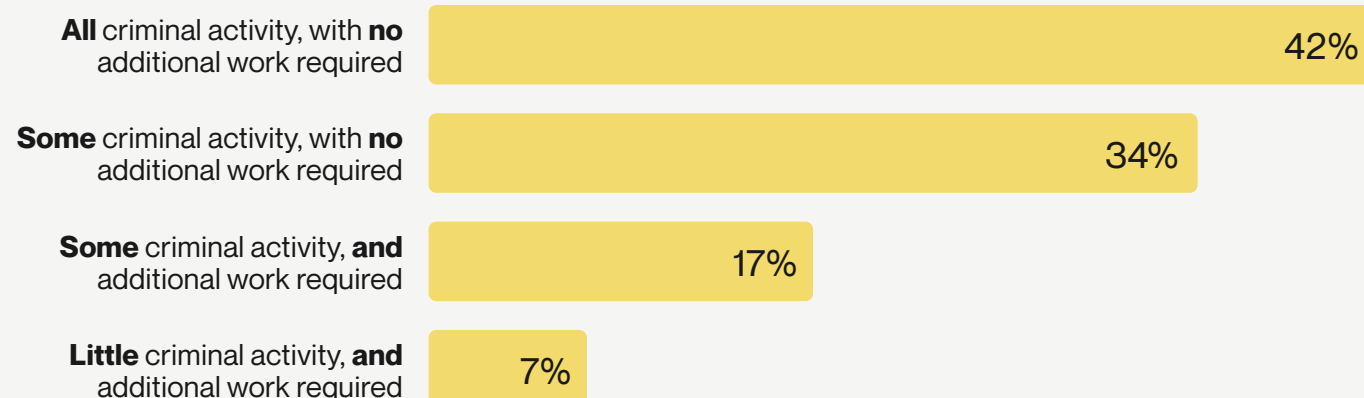
Third-party platform usage for compliance management



Regulations serve as a starting point for preventing criminal activity, but additional work may still be required

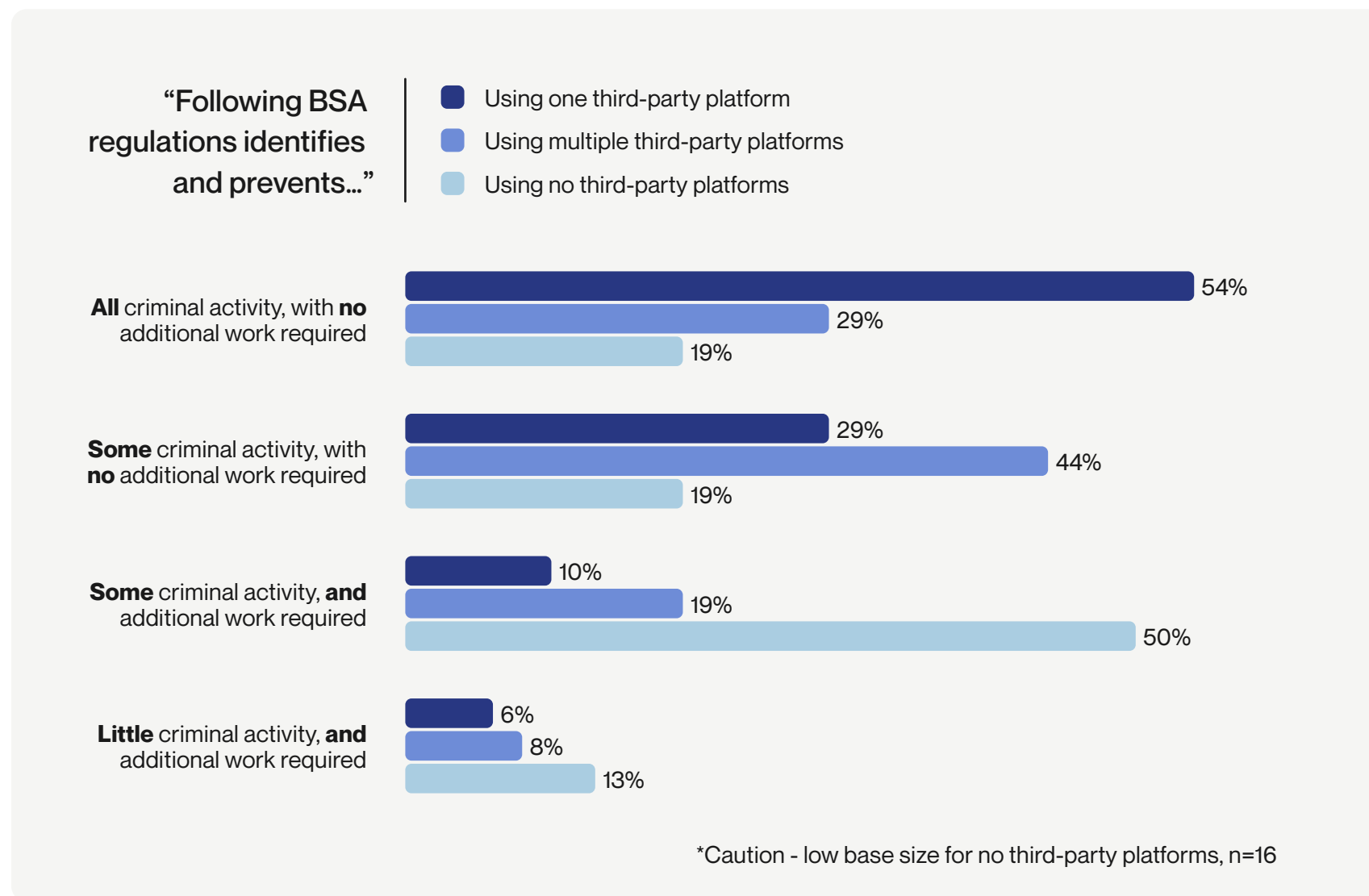
Approximately 76% of respondents believe that following BSA regulations helps identify and prevent at least some criminal activity with no additional work required.

“When new applicants are onboarded, following BSA/AML/KYC regulations identifies and prevents...”



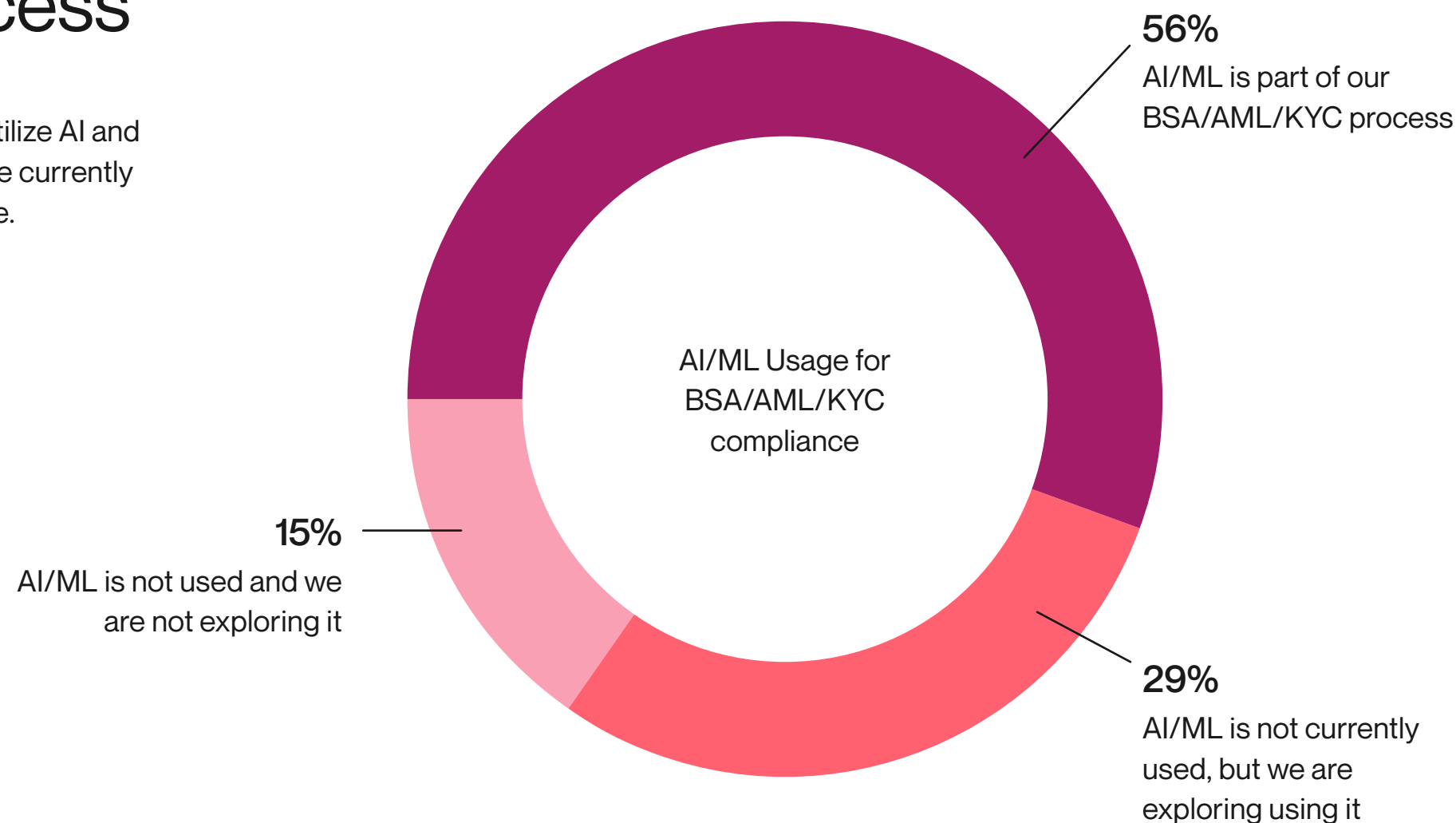
Third-party platforms help organizations identify and prevent more criminal activity

Organizations that use one third-party platform for compliance activities are more likely to indicate they are able to identify and prevent all criminal activity by following BSA regulations than organizations who are using multiple or no third-party platforms.



Most fintechs are incorporating AI/ML into their compliance process

85% of respondents are currently utilizing or plan to utilize AI and machine learning in their compliance process. 56% are currently using it, while 29% are gearing up to use it in the future.

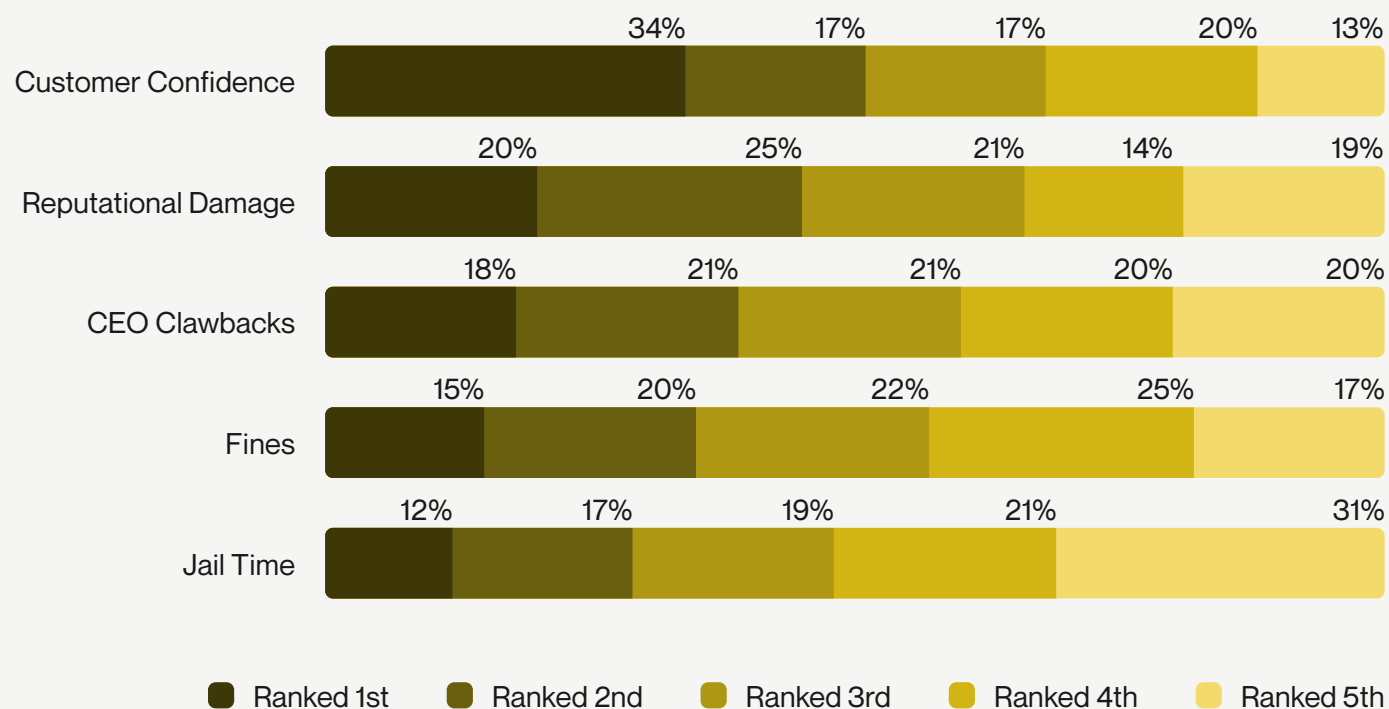


Customer confidence has the greatest impact on BSA compliance decisions

Customer confidence was ranked 1st by 34% of respondents, while reputational damage was ranked 2nd by 25%. Though fines have less of a direct impact on compliance decisions, they could negatively impact customer confidence and organizational reputation.

Greatest impact on compliance decisions

Ranked from 1st to 5th

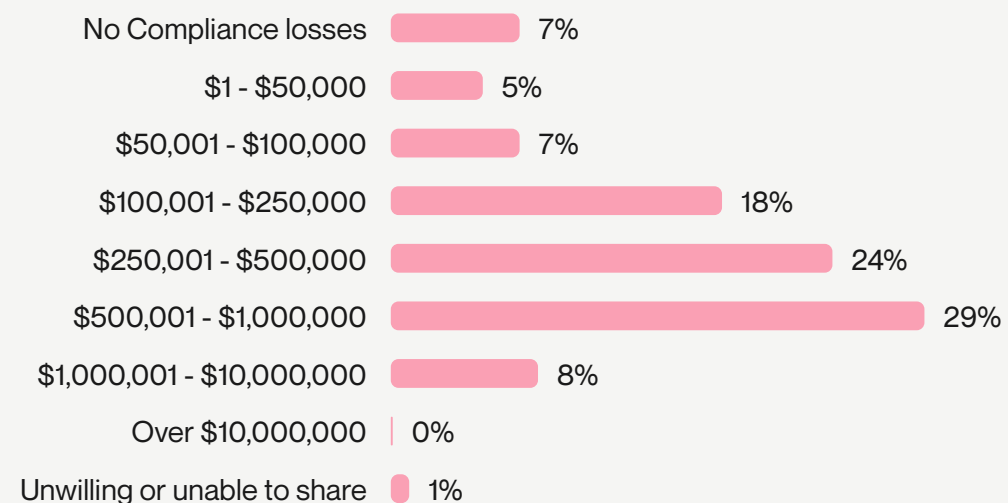


Most organizations experience some degree of fines/penalties

Over 60% of respondents reportedly paid at least \$250,000 in compliance fines over the past 12 months.

Money lost due to compliance fines/penalties

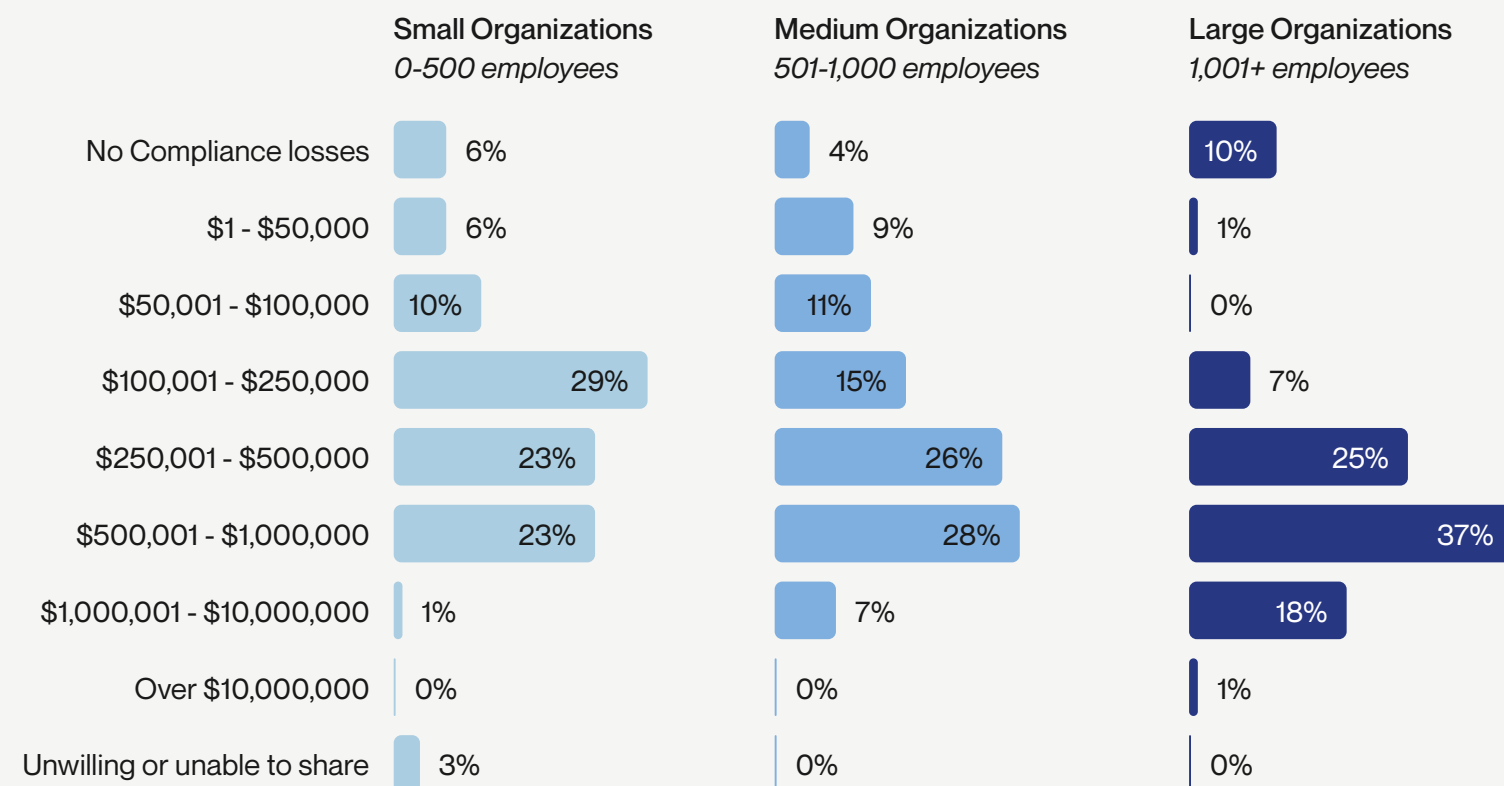
Past 12 months



BENCHMARK by company size

Unsurprisingly, large organizations experience higher losses due to compliance

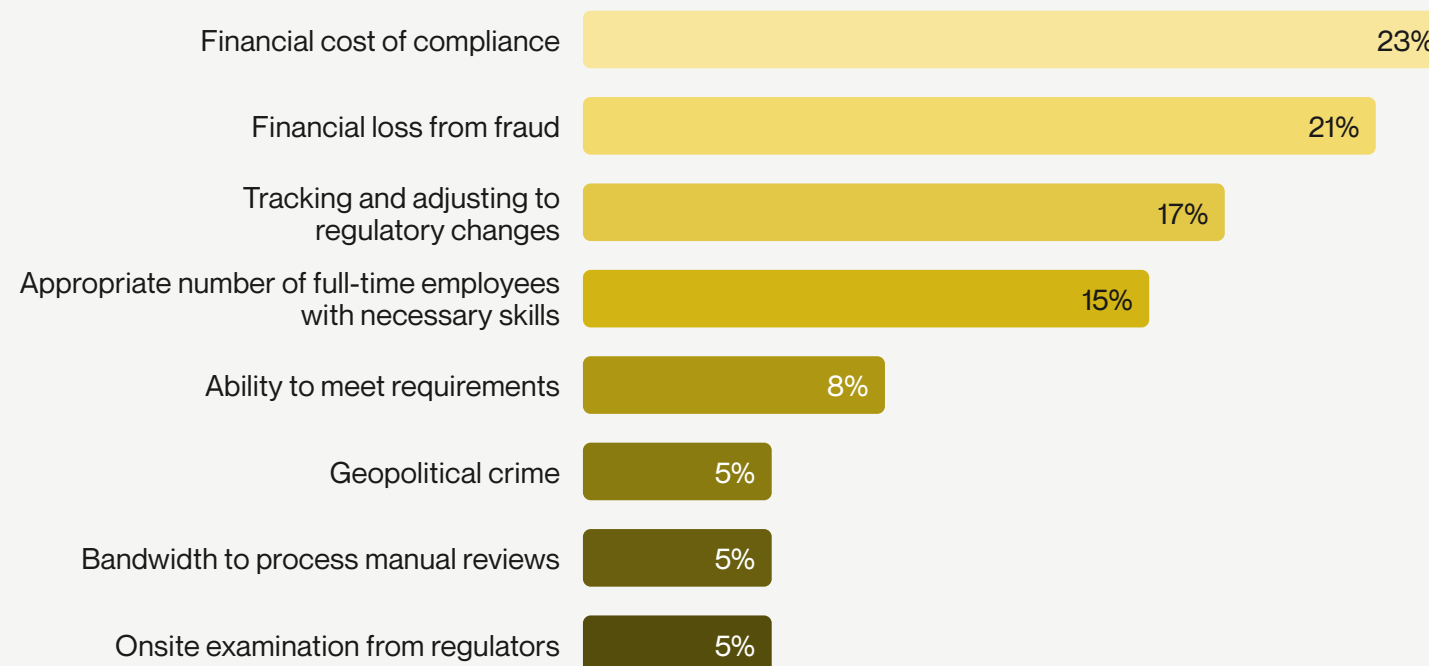
Money lost due to compliance fines/penalties Past 12 months



Organizations are concerned about the financial implications of compliance in the coming year

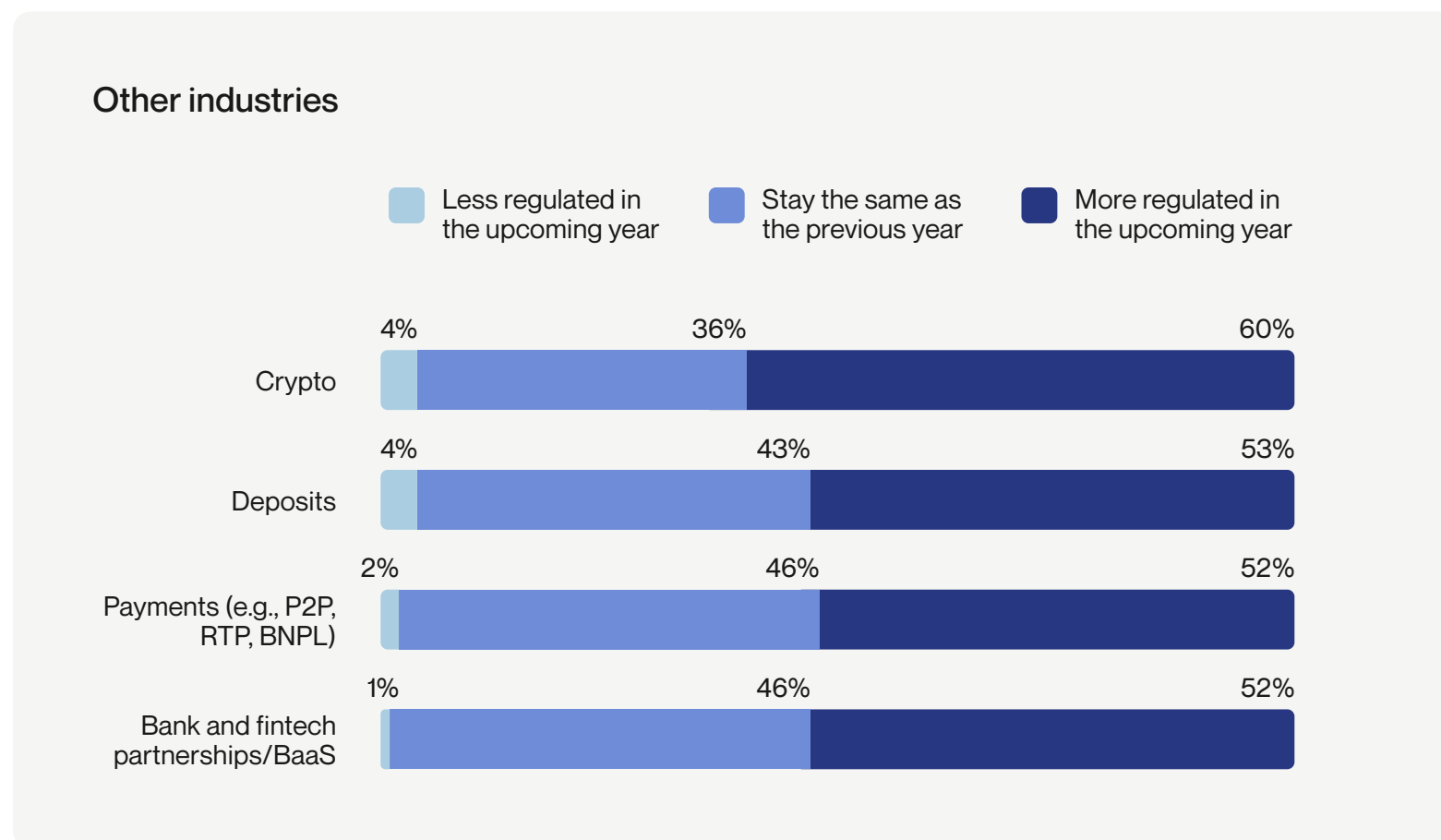
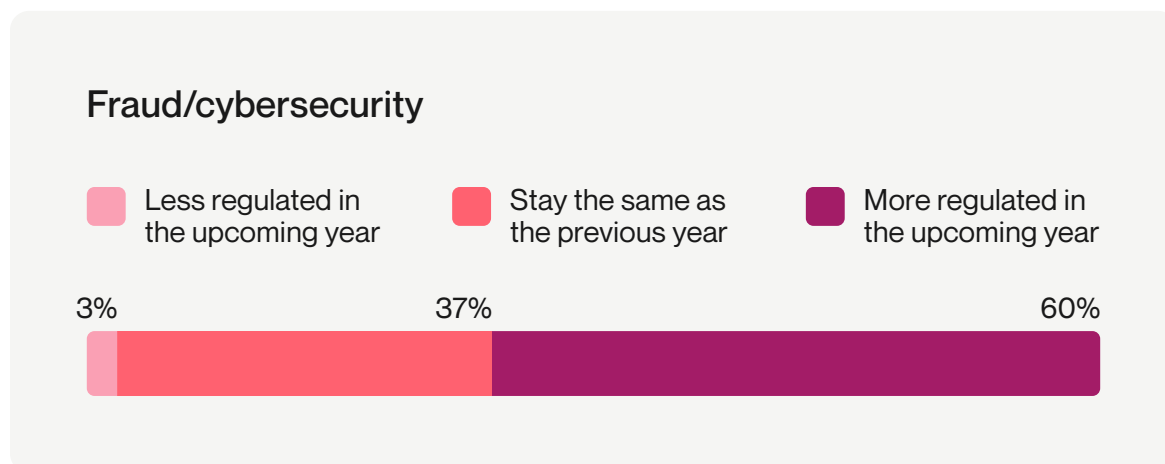
Overall, respondents are most concerned about financial burdens (e.g., compliance costs, loss from fraud) that could impact their BSA compliance in the next 12 months. Only 8% said they were concerned about meeting compliance requirements, despite 93% indicating that staying compliant is at least somewhat challenging (see pg.9). This could mean that organizations are confident in their ability to overcome compliance challenges.

Leading compliance concerns for the coming year



Fraud and cybersecurity are expected to be more regulated in the upcoming year

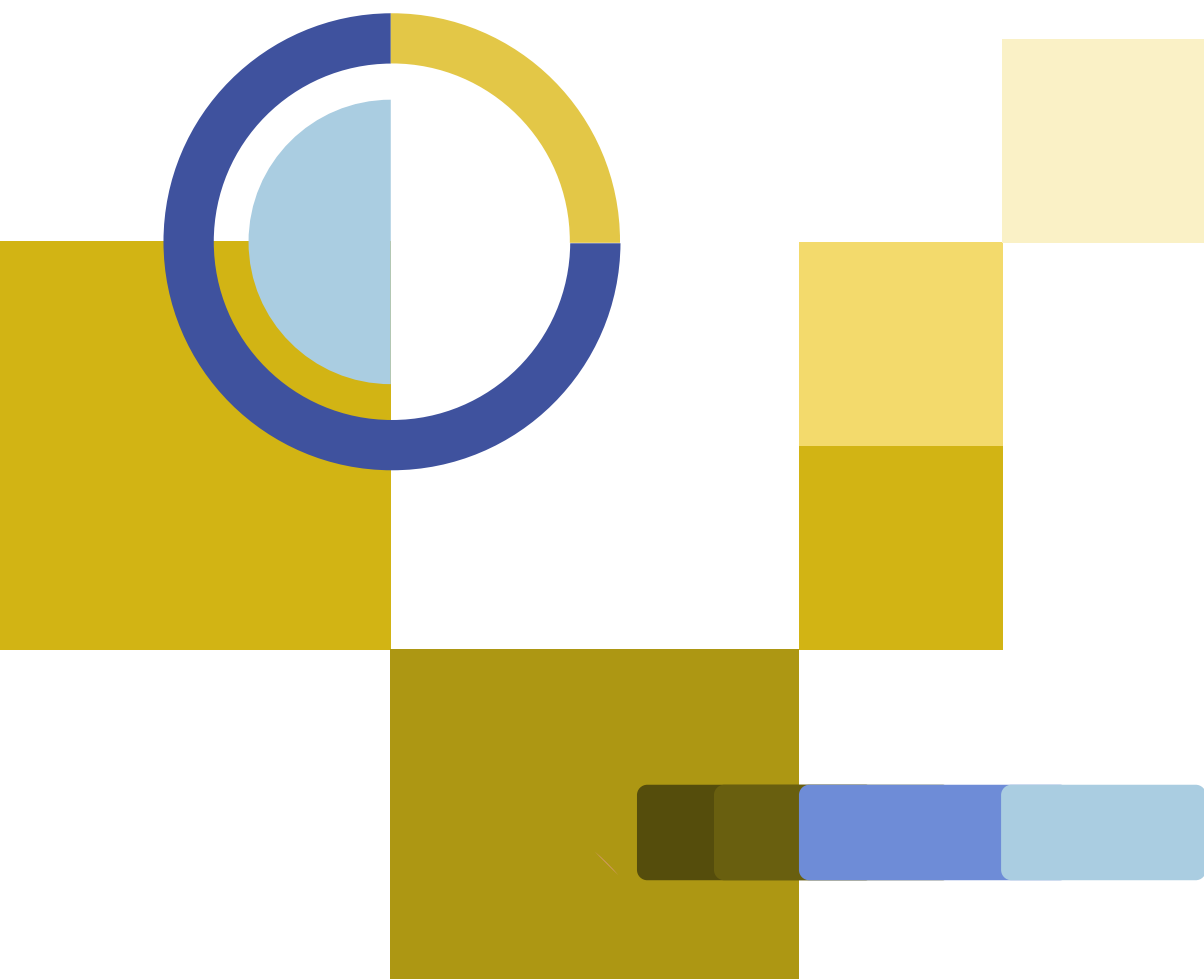
Most (60%) respondents expect to see greater regulation of crypto and fraud/cybersecurity in the next twelve months. Generally, respondents are split in their predictions on other areas (e.g., deposits, payments, bank/fintech partnerships)—around half of respondents predict enhanced regulations, while roughly the same amount believes it will stay the same as in the previous year.



Where will compliance go next?

Predictions from Gizelle Barany,
General Counsel at Alloy:

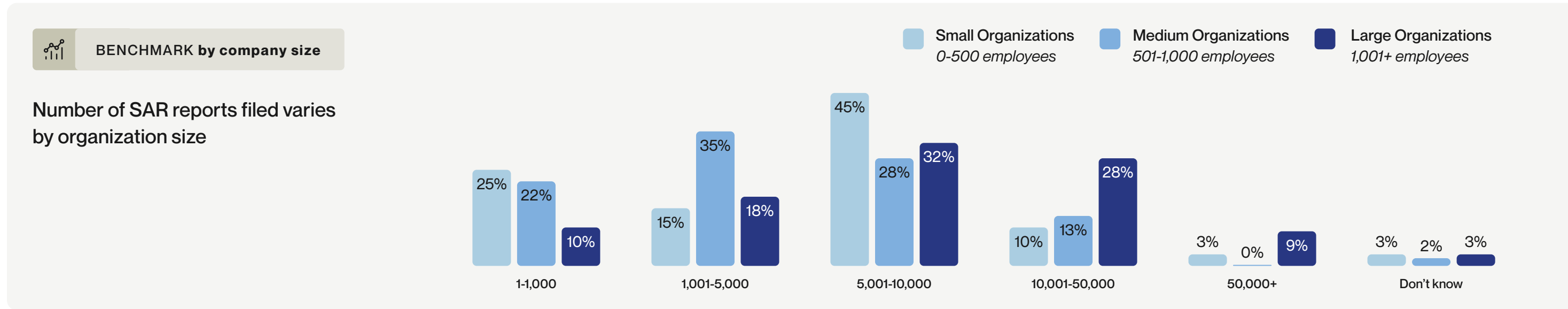
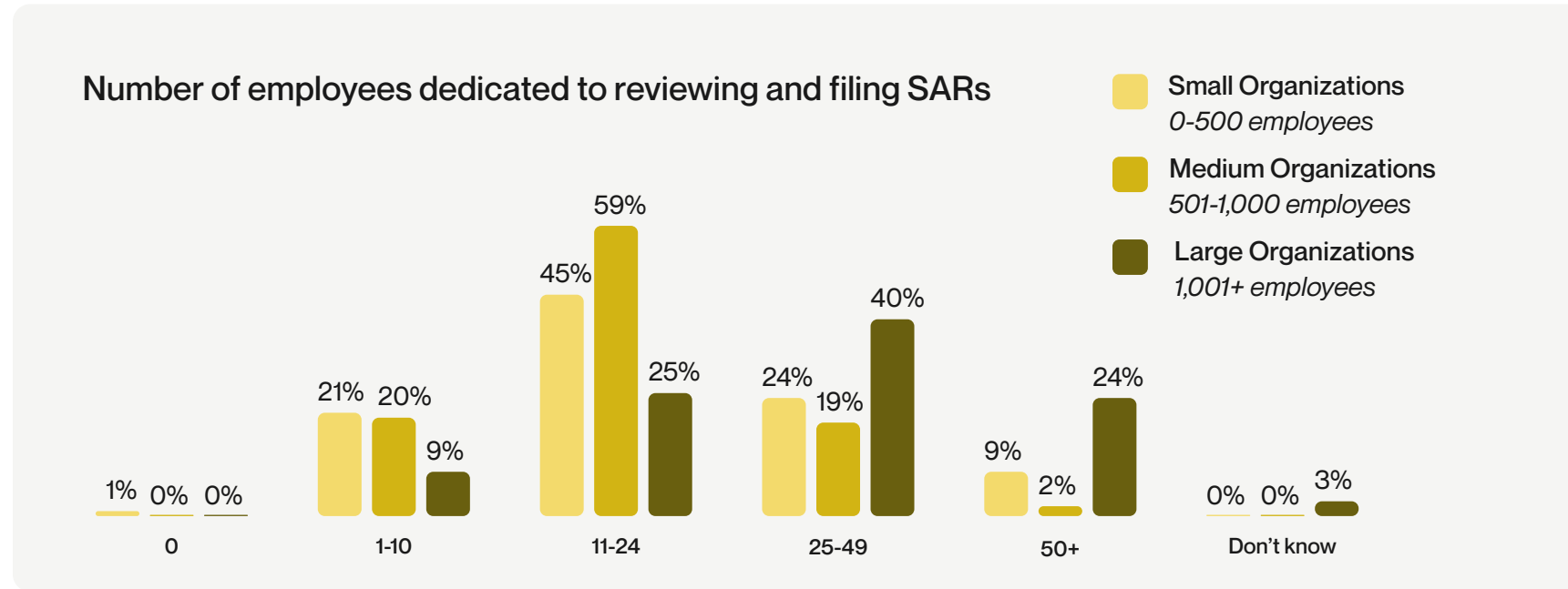
The next 12 months will likely bring regulation of the use of AI/ML in financial services with a strong focus on protecting consumers from resulting disparate impacts. We will also continue to see heightened focus on banks' regulatory requirements to have appropriate oversight and control over the third parties that enable them to bring their products and services to a broader client base. For these reasons, it is wise for fintechs to invest in compliance as compliance is foundational to their offerings.



SAR filings

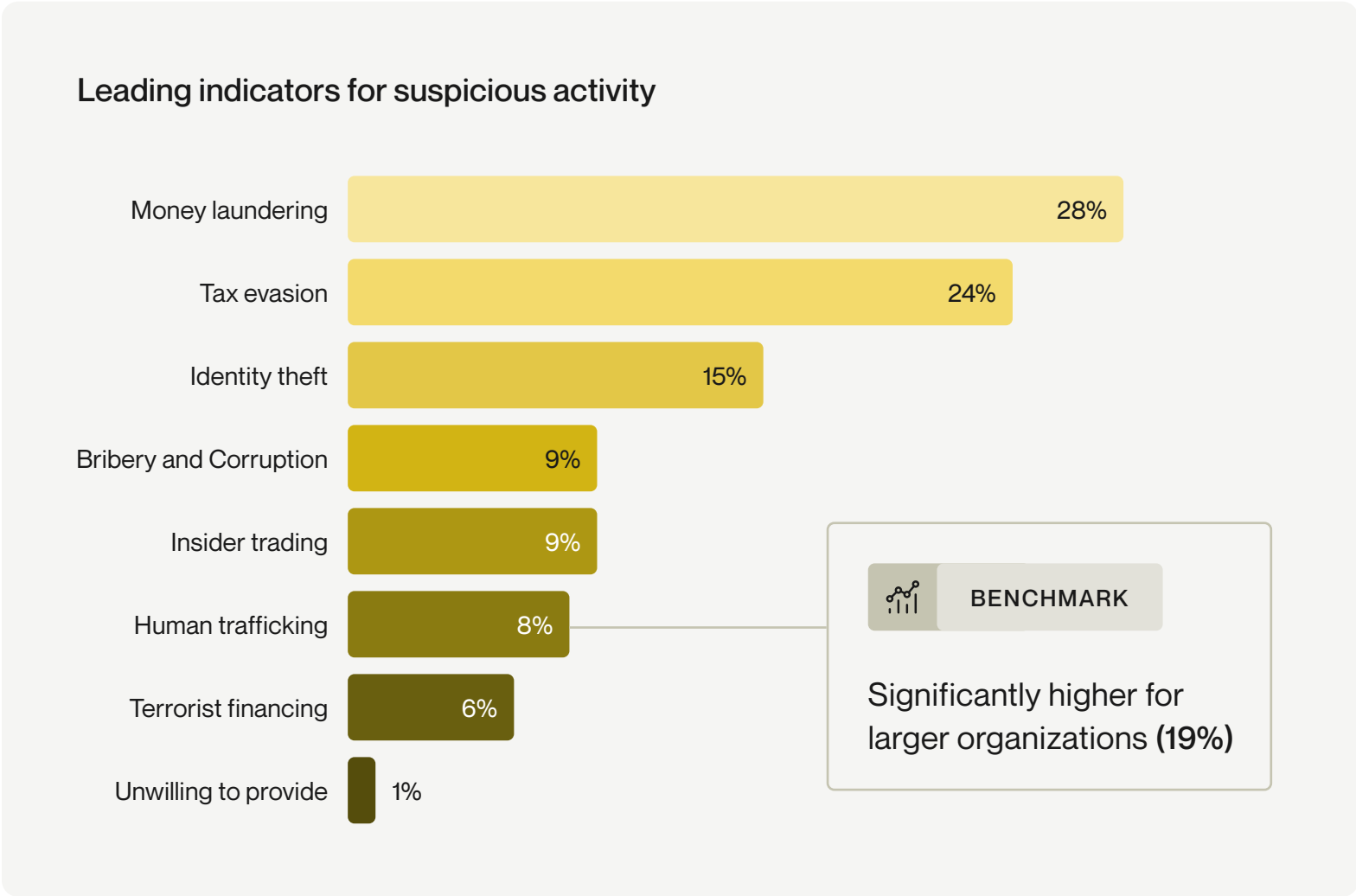
SAR filing processes depend on the size of the organization

Small and medium-sized organizations file up to 10,000 SARs per year and have 1-24 employees dedicated to reviewing/filing. Large organizations file up to 50,000 SARs per year and have 25+ employees dedicated to reviewing/filing. No matter the organization size, it typically takes 1-2 weeks to review and create each individual SAR.



The leading indicators for suspicious activity are typically financially driven

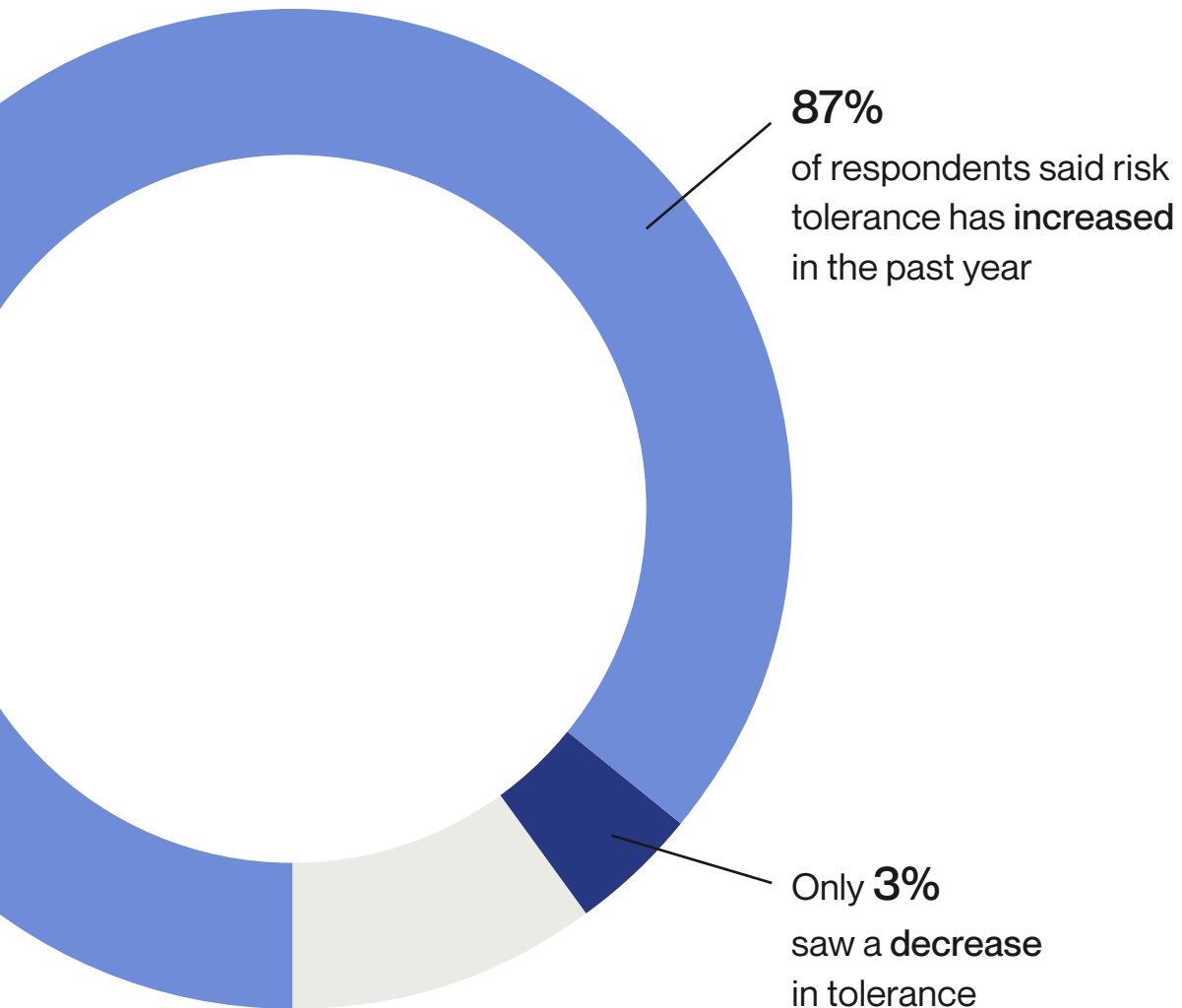
Money laundering and tax evasion are the leading types of suspicious activities for organizations. Larger organizations experience higher levels of human trafficking compared to smaller companies.



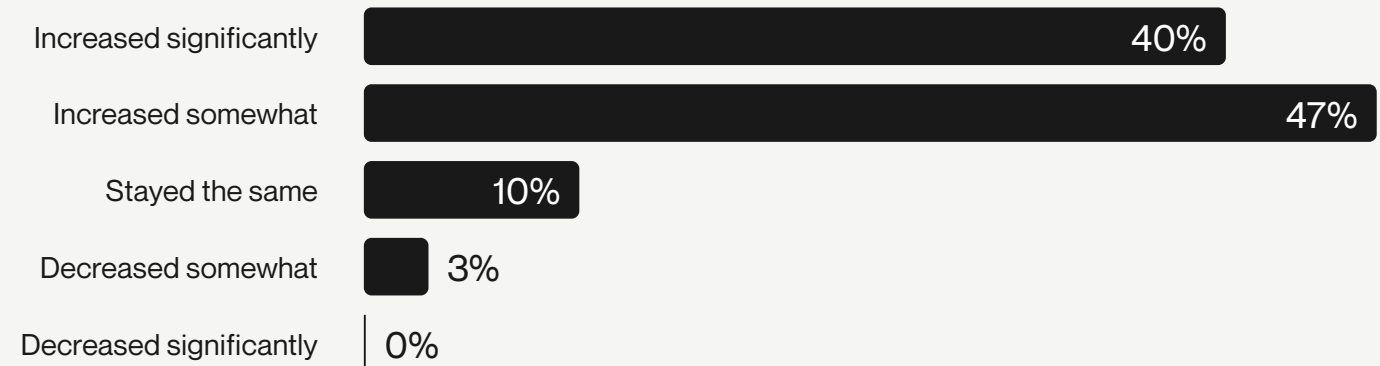
Risk tolerance

Risk tolerance is on the rise

Risk tolerance has increased for 86% of respondents organizations over the past year.



Risk tolerance change over the past year



Alloy insight

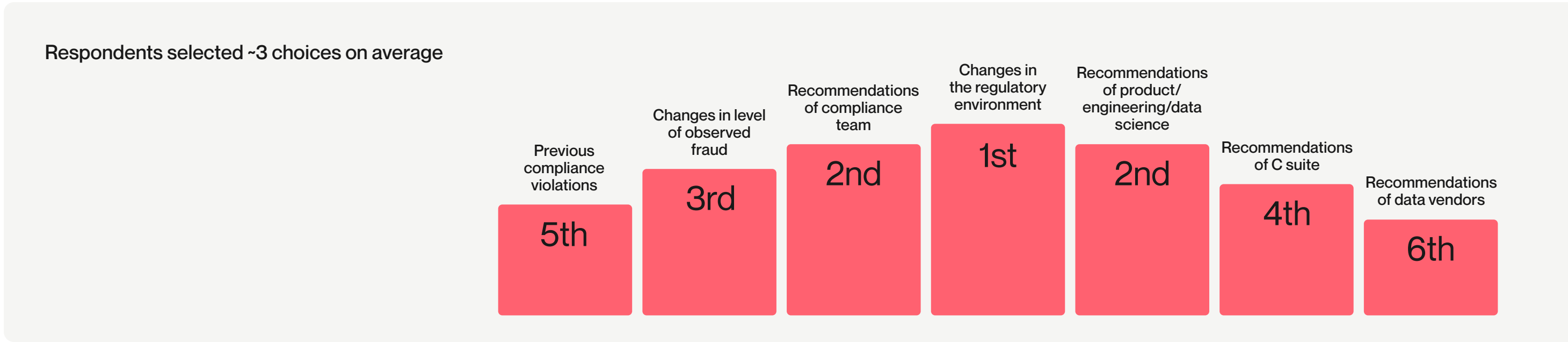
This stat may seem surprising, given the significant amount of fines that respondents reported, additional costs of regulatory non-compliance (reputational damage, legal fees, etc), and the overall industry-wide rise in fraud. However, despite the challenging fraud and compliance landscapes, fintechs are still facing enormous pressure to reduce customer friction and grow fast. At the same time, the recent economic downturn has made it even more difficult for fintechs to continue on in the state of hyper-growth they saw at the beginning of the pandemic. These pressures could be leading to an increased risk tolerance as they try to find ways to grow their customer base.

Organizations consider many factors when determining risk thresholds

Respondents cited changes in the regulatory environment, recommendations of their compliance team, and recommendations of their product, engineering, and data science teams as the top factors they consider when determining risk threshold rules.

 Alloy insight

Many factors go into determining a fintech’s risk tolerance, including fraud risk, growth goals, and compliance scrutiny. At the same time, different decision-makers in the organization will provide different recommendations. To maintain a robust compliance program, compliance professionals must align on a risk threshold that makes the most sense across the entire organization.



Conclusion

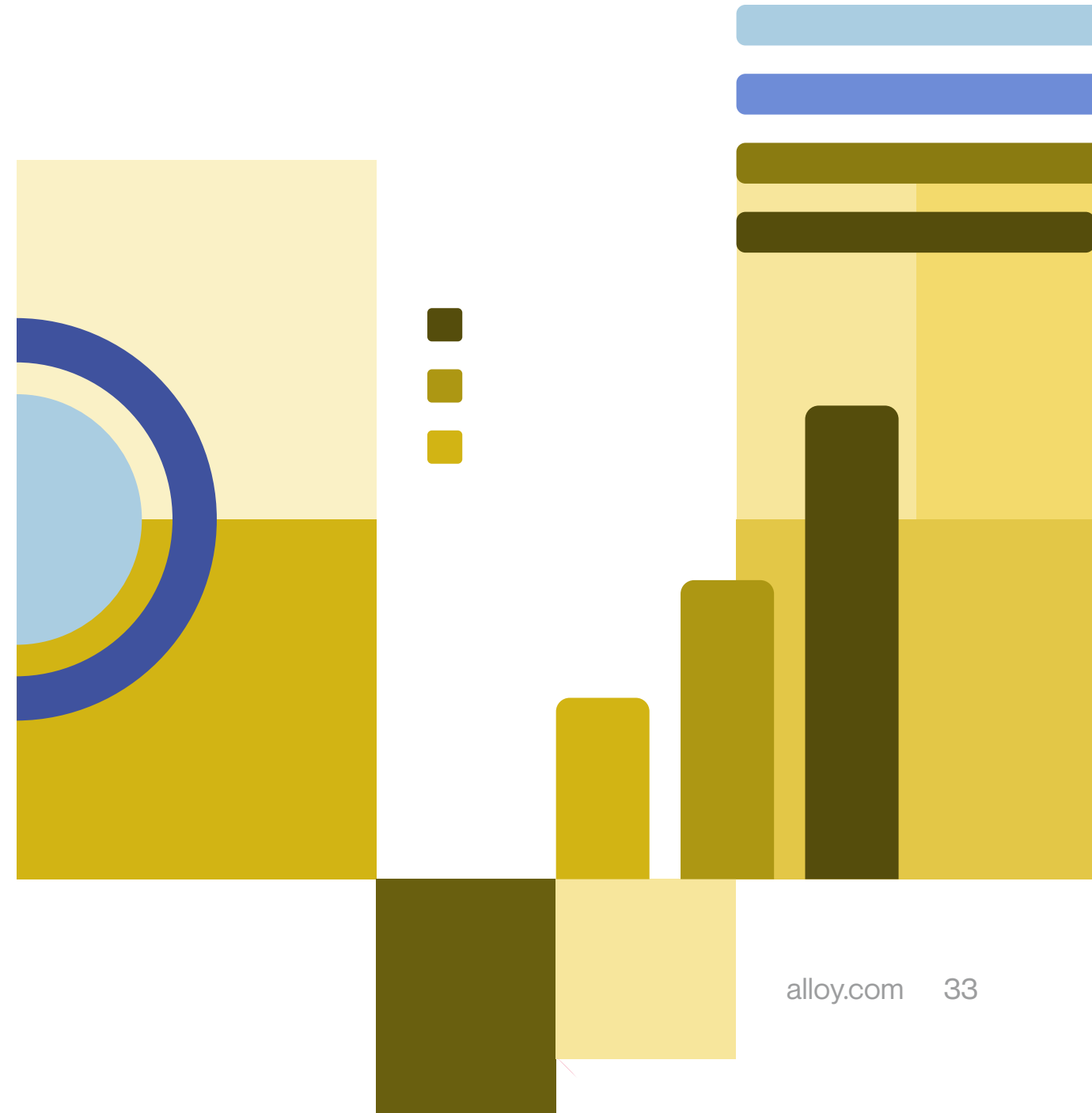
Conclusion

In the digital finance era, banks and fintechs have the potential to serve nearly everybody, but the burden of compliance often holds them back. Building and executing robust compliance programs can be confusing, time-consuming, and expensive.

Compliance regulations have been in place for years, but even companies that are well-resourced still struggle with them. At the end of the day, the goal of these regulations is to stop financial crime. However, fraudsters and bad actors are moving way faster than regulators can keep up with. As new types of risks emerge and regulations eventually follow, it becomes even more challenging to stay compliant and prevent financial crime while keeping costs down.

Many organizations are seeing success when they turn to third-party platforms to help them identify and prevent financial crime. Still, fraud and compliance can't be managed in silos; compliance, fraud, product, and leadership teams need to work together to build robust compliance programs.

Organizations that focus on understanding their customers' identities across the customer lifecycle will be most equipped to stay compliant while minimizing access to bad actors.



About Alloy

Alloy solves the identity risk problem for companies that offer financial products. Today, nearly 500 banks and fintechs turn to Alloy's end-to-end identity risk management platform to take control of fraud, credit, and compliance risks, and grow with confidence. Founded in 2015, Alloy is powering the delivery of great financial products to more customers around the world. Learn more at alloy.com.