



# By the Numbers:

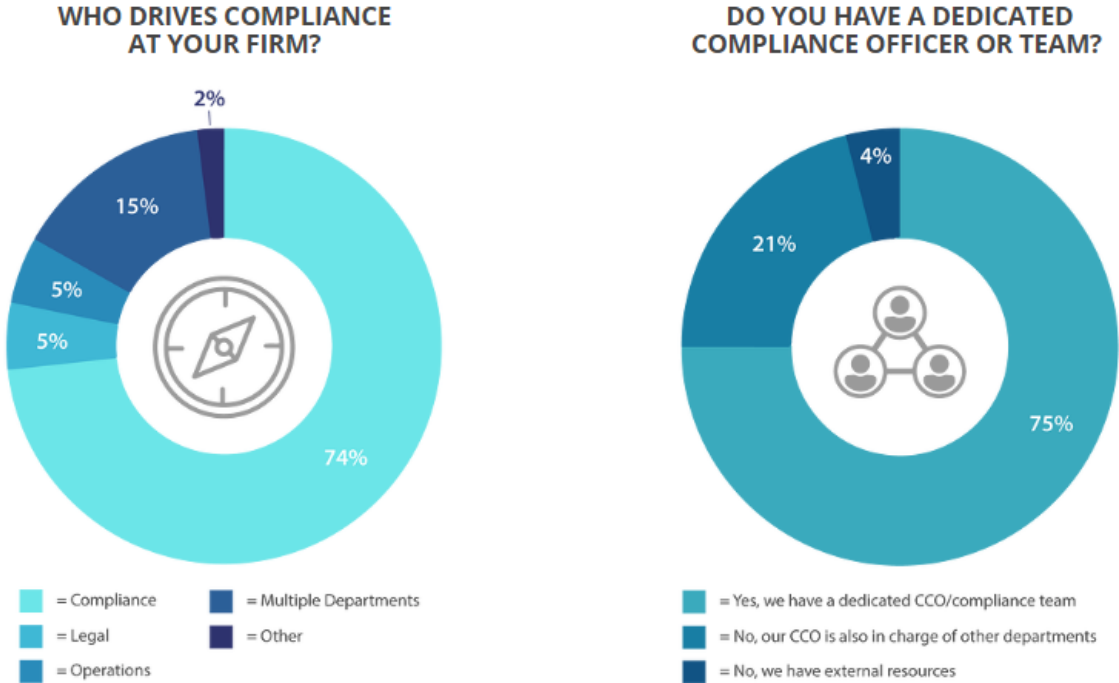
## A Compliance and Regulatory Technology Analysis for the Financial Services Industry

The *By the Numbers* analysis illustrates a comprehensive array of regulatory histories and compliance operations trends and statistics through clear charts.

To say the regulatory compliance landscape is evolving would be a significant understatement. In fact, given the consistent rate of evolution within the space, it would be more accurate to say that the only constant is change. Simply “keeping up” is no longer enough. For a compliance professional to successfully mitigate the risk points of their financial firm, they must stay ahead of trends, looking towards the future to proactively arm their firm with the appropriate compliance protocols and procedures.

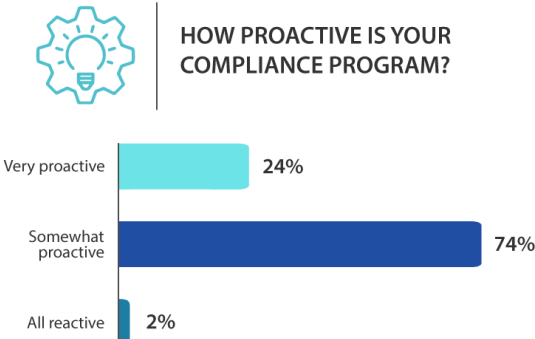
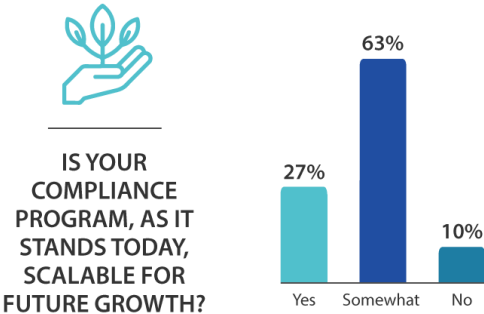
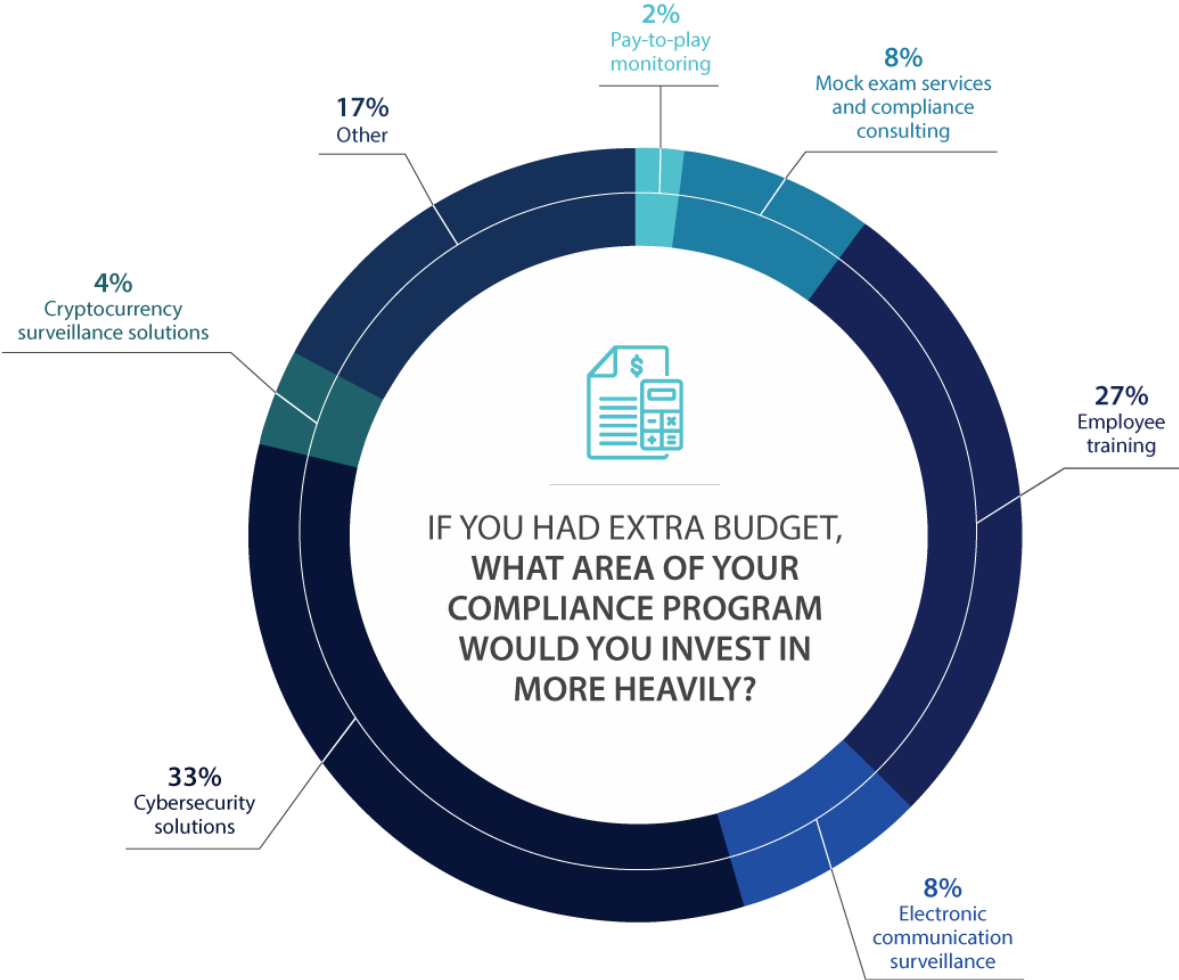
Given the fluctuation in both risk and requirements for compliance teams, analysis of both trends and trajectory has become an essential component in determining the inherent risk and subsequent requirements of your firm’s compliance program. In this proprietary research, we sought to get a look under the hood, examining how firms are functioning, what risks are taking priority and where investments are being made. In doing so, we have provided readers with insight into not only the actions of their peers, but the trajectory of the industry as a whole.

RIA in a Box and ComplySci, in conjunction with the ComplySci portfolio of firms, consistently work to empower compliance professionals with the technology, education and consulting resources necessary to meet the demands of an evolving landscape. This guide will serve to provide insight into how firms, like yours, are addressing those challenges and meeting the requirements of compliance head on.



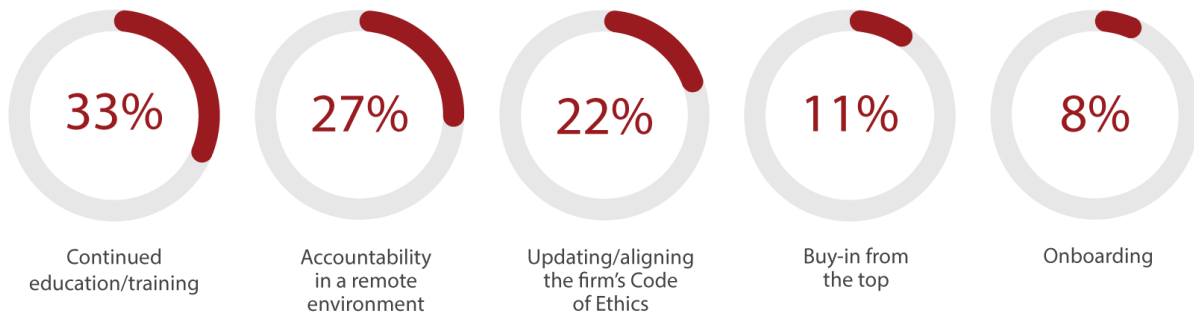
# 1. An overview of firms today

As a compliance professional serving an investment adviser, broker-dealer or other type of financial firm, you've likely faced new challenges and risk areas this past year. Identifying areas of risk and core challenges can help you to address how to evolve your compliance program to meet compliance requirements in the most efficient and effective manner.





## BIGGEST COMPLIANCE CHALLENGES FOR RIA FIRMS



RIAs, and compliance professionals in general, are currently trying to gauge their internal comfortability with cybersecurity by assessing the level of cybersecurity knowledge throughout the firm. The assessment of your staff's cybersecurity awareness is a critical first step to help determine what protocols and procedures your firm must implement. All firms should consider implementing different levels of cybersecurity training based on roles within the firm.

As consultants to RIA firms, we strongly recommend our clients consider risk management strategies like implementing cybersecurity insurance to protect their firm. "In today's world, it's not a question of if you're going to get hacked, it's a matter of when," said Director of Compliance Dorothy Podzemny.

While cybersecurity insurance is not required, it is an extra layer of support. As of late, there is much more interest in cybersecurity insurance from our client base, which is likely due to the increased quantity and sophistication of cyber attacks.

We recommend firms continuously conduct engaging cybersecurity training. It is a best practice to use platforms to test employee's cybersecurity knowledge and readiness to determine the effectiveness of your current training, and assess then if more training is required.

### The top three regulatory concerns related to cybersecurity and compliance:

- 1. Safeguarding clients:** Your firm should be safeguarded enough to make it troublesome for a hacker to breach your clients' information.
- 2. Training:** Make sure your employees are up to date on the latest cybersecurity training. Whether outsourced or internal, you need to hit all points in your cybersecurity manual and address any cyber trends.
- 3. Safeguarding your own data and equipment:** Use MFA, VPN's, encryption, complex passcodes or push notifications to enter your platforms. Proper safeguards for internal controls within your firm are essential to mitigating cyber risk.

## 2. Addressing SEC and FINRA rules and regulations

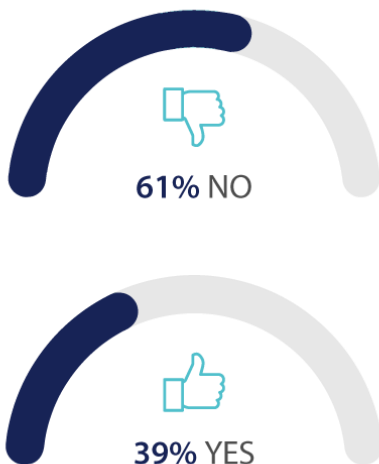
The past year has seen an onslaught of new rules and regulations from the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA), much of which highlights the direction of the financial industry as a whole. With a clear trend towards digital currencies and investments, the SEC has laser-focused its Examination Division on cyber and crypto-related risks.

As firms seek to advance their offerings and broaden the services they provide to clients, they will need to contend with the new risks that come along with it. Looking at the regulations and risk alerts will provide guidance around how firms should begin to think about the future of their compliance programs...and what they can do to proactively protect themselves and their clients from such risk.

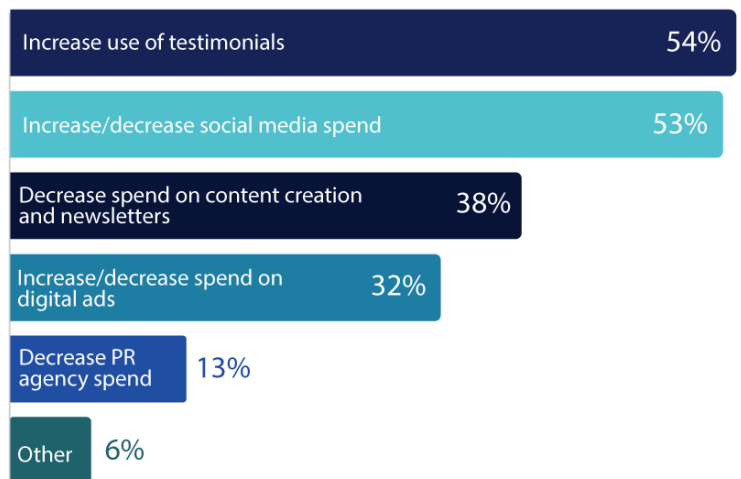
Another important tip is to enact a [“No Blame”](#) policy. Employees should feel free to report when they or someone else may have inadvertently done something to put the firm at risk. There should be no repercussions. You will want to know immediately when an employee has opened a suspicious attachment or downloaded something off the internet which may contain a virus. The faster they inform you, the faster you can address the issue.



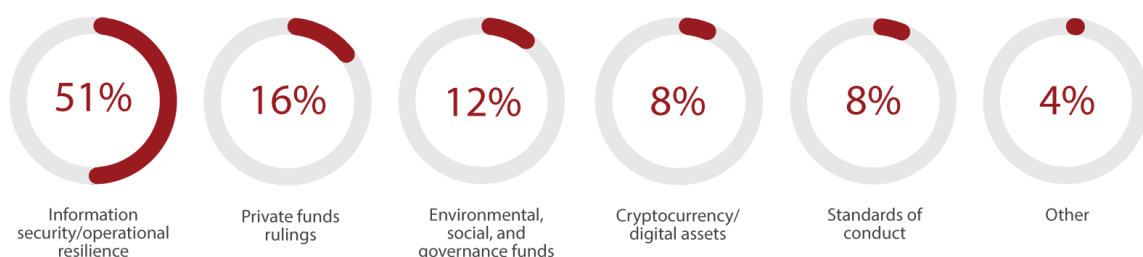
IF YOU ARE SEC REGISTERED, DO YOU PLAN TO TAKE ADVANTAGE OF THE SEC NEW ADVERTISING MARKETING RULE IN 2022?



IF YOU ARE PLANNING TO TAKE ADVANTAGE OF THE SEC NEW ADVERTISING RULE, HOW DO YOU ANTICIPATE YOUR STRATEGY WILL CHANGE?\*

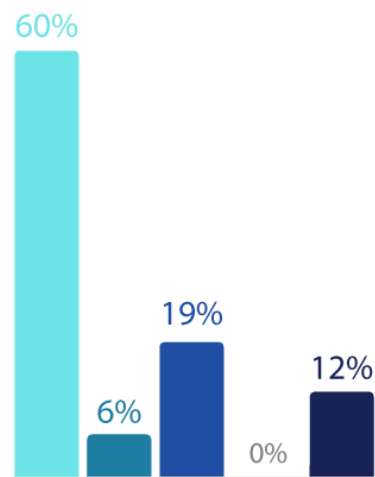


WHICH OF THE SEC PRIORITIES IS THE MOST CONCERNING FOR YOUR COMPLIANCE PROGRAM?

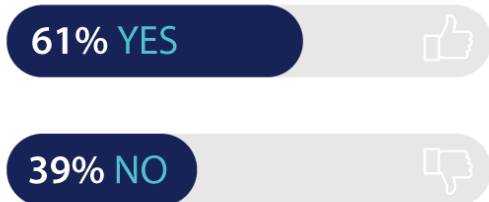


WHICH OF THE SEC'S RECENTLY PROPOSED RULES/AMENDMENTS DO YOU THINK WILL IMPACT YOUR FIRM THE MOST IN TERMS OF COMPLIANCE DUTIES?

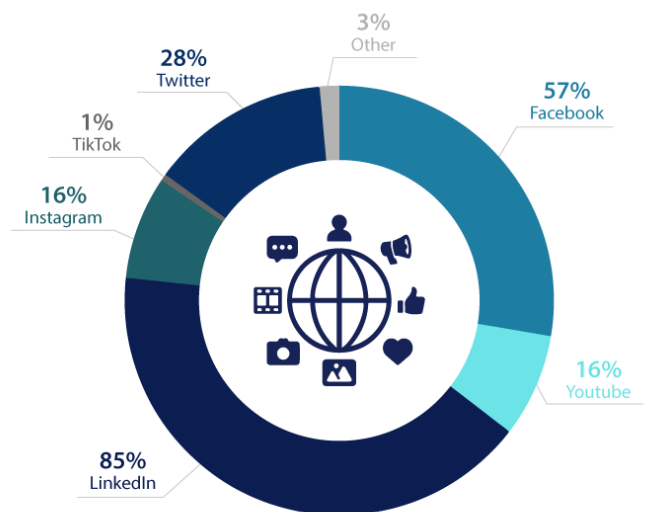
- --- Cybersecurity risk management
- --- Climate-related disclosures
- --- Private fund investor protection
- --- Registration and regulation of security-based swap execution facilities
- --- Other



DO YOU BELIEVE YOUR EXISTING MNPI POLICIES/PROCEDURES WILL BE ADEQUATE SHOULD THE SEC'S NOVEL APPROACH BECOME AN ENFORCEABLE RULING?



WHAT SOCIAL MEDIA PLATFORMS DOES YOUR FIRM UTILIZE REGULARLY FOR BUSINESS PURPOSES?\*



Ask a compliance consultant:

**1. We saw quite a substantial number of proposed rules and risk alerts thus far in 2022, do you expect the trend to remain and how can firms best navigate this growing complexity?**

First and foremost, it's important to really drive home the fact that proposed rules are not finalized rules. The notion of a proposed rule is one of the initial steps in the implementation process for a new rule. For instance, we witnessed the proposed amendments to modernize the Advertising and Cash Solicitation Rules close to three years ago. Although the new rule, which is referred to as the "Marketing Rule," was approved on Dec. 22, 2020, the compliance date isn't until Nov. 4, 2022. All of which is to say, the timeline for the implementation of a proposed rule is generally incredibly lengthy.

However, that doesn't mean you shouldn't be paying attention to these proposed rulings. The trend is not slowing, and as long as the financial world continues to develop new strategies for investing, there are going to be changes to existing rules and regulations.

Luckily, the regulators provide clues or golden nuggets of wisdom for firms in the way of risk alerts. These alerts act as guidance for the vulnerabilities, which regulators are actively seeing impact the industry. Firms should treat them as a roadmap for how to manage their own compliance program more effectively. Additionally, it is extremely critical for firms to pay attention to both FINRA and the SEC's priority letters as they offer insight into what they may be highlighting in the next six to 12 months.

## **2. Which of the SEC/FINRA proposed rules and/or amendments caused the most challenge for your clients? Do any of the rules or amendments have a substantially higher threshold for risk? Can you speak to that?**

There are a few different proposed and adopted rules that have come up in conversation recently, including the cybersecurity proposal, private equity proposal and the adopted DOL PTE 2020-02.

Where I typically see the most confusion or potential for risk is in regard to how a firm should implement these rulings. Although the regulators provide guidance, each firm must make its own decision on how to implement these rulings based on their firm's activities. For many firms, it is necessary to seek outside counsel to ensure the policies and procedures match the fundamentals of the newly adopted rule.

## **3. And for the marketing rule, what is the # 1 thing advisors are coming to you for help with? What's their biggest concern about the new rule?**

Like the other rules I spoke about, the Marketing rule presents challenges for many firms, specifically in implementation. While it's being called the New Marketing Rule, it is actually an amalgamation of two existing rules: the old advertising rule and the old solicitor rule. Because the new rule combines different aspects of previous rulings, firms have discovered that some previously unauthorized actions are now permissible and vice versa.

Firms are coming to consultants to better understand the regulation itself and how it impacts their organization. A major factor the industry struggles with is in regard to their policies, determining if there is true need to add language to your policy based on whether or not you are taking part in that specific activity. This can be exceptionally impactful because once you have made a statement of that kind within your policy, you need the checks and balances to confirm follow through, which ultimately adds an extra layer of responsibility.

When it comes to regulators, simply having a process isn't enough, you need proof that you are putting your words into actions.



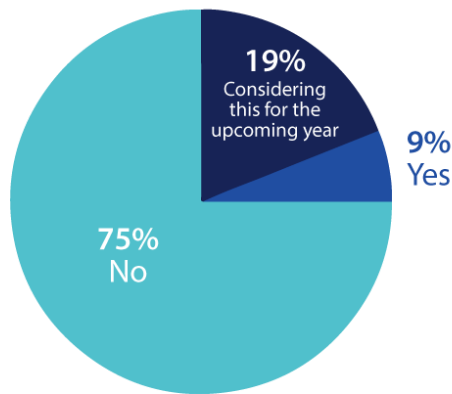
### 3. The evolution of the compliance landscape

The rules and regulations put out by the overarching regulatory bodies aren't the only variable impacting the evolution of the compliance landscape. In fact, compliance itself is shifting as the financial industry works towards a more digital-centric future. Threats around cybersecurity and cryptocurrency, which even five years ago were barely a blip on the radar, now constitute a significant percentage of the risk faced by advisory firms.

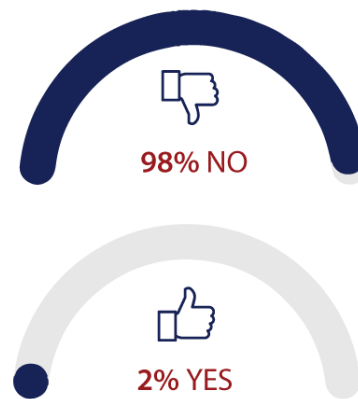
An analysis of the industry points to these areas being more trend than fad, with a significant and long-lasting shift taking place for both consumers and firms alike. Evolving with these trends is essential to a firm's long-term success, however, understanding how these trends will impact the compliance of your firm, and the risk you and your clients face, is crucial to avoiding unnecessary consequences.



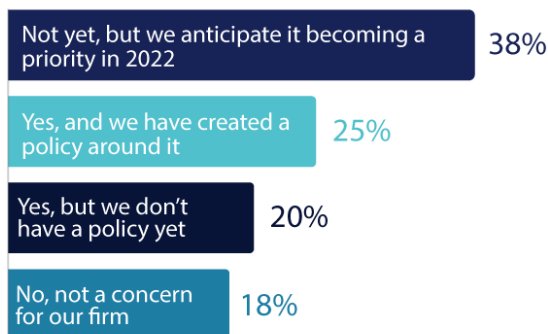
DOES YOUR FIRM ADVISE CLIENTS ON DIGITAL ASSETS SUCH AS CRYPTOCURRENCIES?



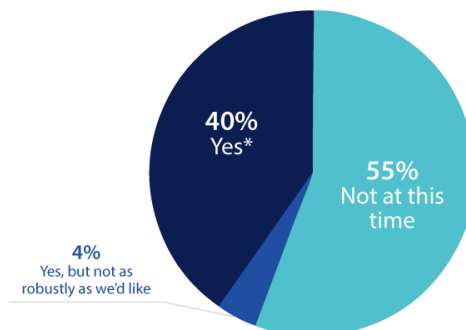
HAVE YOU EXPERIENCED A CYBER ATTACK WITHIN THE LAST YEAR?



IS MONITORING CRYPTOCURRENCY A COMPLIANCE PRIORITY?



DOES YOUR FIRM REQUIRE PRECLEARANCE FOR DIGITAL ASSET TRADING SUCH AS CRYPTOCURRENCY?



\*On par with employee trading requirements for other securities.



All financial firms must have a cybersecurity plan in place tailored to how their business model is set up. There is no one cybersecurity plan that capable of addressing all financial firms' unique business models.

Consider whether your firm operates with manual processes using physical files vs. digital processes like cloud storage. Your cybersecurity plan needs to be custom fit to those unique circumstances. Review the National Institute of Standards and Technology at the U.S. Department of Commerce (NIST) framework to decide what your cybersecurity policies and procedures could currently be lacking.

### **Ask a compliance consultant:**

#### **1. For any RIAs that are not advising clients on digital assets, why? What are their concerns?**

In my experience, many RIAs are not advising clients on digital assets due to the regulatory uncertainty.

Advisers are focused on their client's long-term investing goals. It's impossible to determine how digital assets will factor into long term goals and so they are unwilling to bear the risk. RIAs may not want to risk advising on these assets in the absence of a sound policy on the dos and don'ts from regulators.

#### **2. Can you discuss the regulatory considerations for advising on digital asset investments?**

Consider the nature of it, is it suitable and appropriate for your client? How can you prove it is appropriate for your clients' goals? Advisers need to prove they are acting in their clients' best interests.

If a firm chooses to advise on digital asset investments, they need to do so in a smart, responsible manner way. Not everyone is educated on digital assets. It is trendy, so there are a lot of clients who show interest in investing their money, however, it can lead to a certain degree of recklessness from an investor perspective.

The SEC has not determined out how they will regulate crypto because of the variation in classification for digital currencies. This has left firms in an environment in which they are trying to navigate around potential triggers and pain points without a clear roadmap for what those triggers actually are.

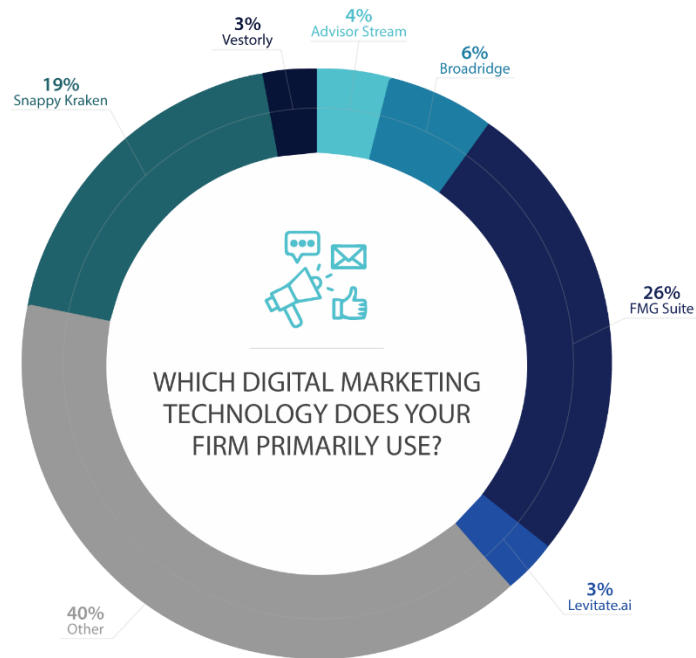
#### **3. How about for regulatory considerations for monitoring employee's digital asset trades?**

A firm should only monitor employees if they are also advising on the same digital assets or cryptocurrencies. Consider conflicts of interest and incorporate a strategic education plan to help train employees around best practices in regards to investing clients' money in cryptocurrency.

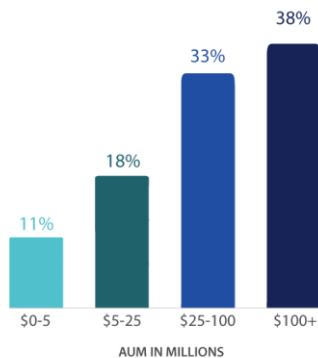
## 4. The increasing role of software and technology for financial firms

Within the last decade, technology and software adoption within the financial industry has skyrocketed, with firms integrating new platforms to serve a variety of needs including marketing, CRM, financial planning and reporting systems. While many of these platforms or technology offerings serve a specific need within the firm, in order to ensure data siloes don't create even more work for your employees, it is essential that these solutions "speak" with one another, sharing data and insight from one platform to another.

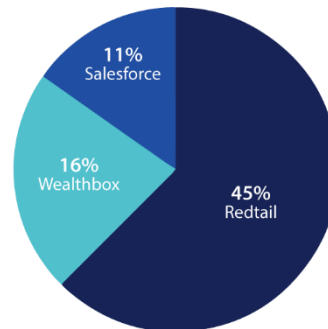
Technology holds the power to alleviate manual work and increase effectiveness throughout your firm, by taking advantage of best-in-breed technologies you leverage a powerful resource for your firm. And by integrating these technologies in a manner that allows data to flow from platform to platform (where appropriate) you reduce the risk of critical data points falling through the cracks.



CRM ADOPTION RATE BY AUM

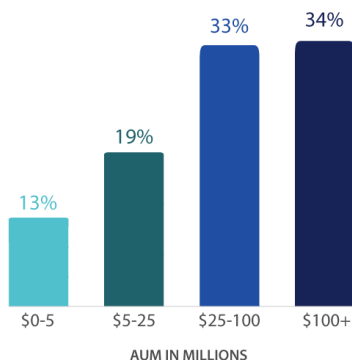


TOP THREE CRM SYSTEMS

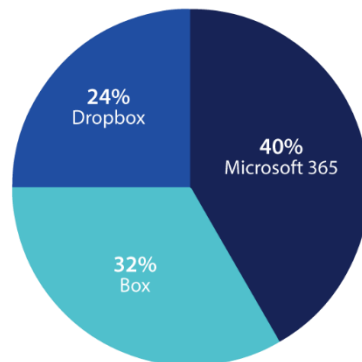




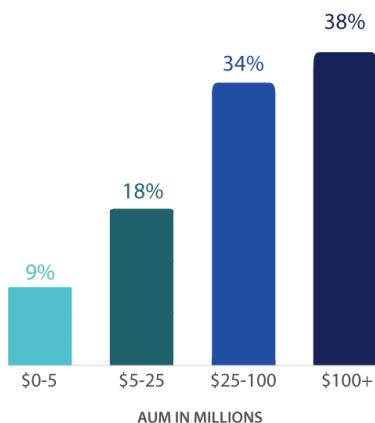
DOCUMENT STORAGE ADOPTION RATE BY AUM



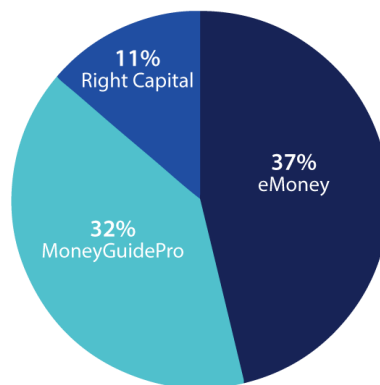
TOP THREE DOCUMENT STORAGE SOLUTIONS



FIRMS OFFERING FINANCIAL PLANNING SERVICES BY AUM



TOP THREE FINANCIAL PLANNING SOFTWARE PROVIDERS



### Ask a compliance consultant:

#### 1. What are some of the most common questions you hear from RIAs regarding the Marketing Rule?

Most of our questions come from state registered RIAs, for whom the SEC marketing rule is not applicable. It's important to navigate the differences between the two types of firms (state registered and SEC registered) to determine the relevant regulations.

As for SEC registered clients, they often ask about how to treat solicitors, now referred to as "promoters". Additionally, we often discuss the necessary reports required for advertising. I always like to note, for performance reporting, one-on-one performance reports are acceptable. Meaning if it's not viewed by more than one person, you don't have to provide an additional disclosure of your performance in the past five years.

## **2. Can you discuss the different considerations firms should keep in mind when deploying new strategies?**

Advisers like to set their firms apart from competitors, and rightly so, but you can get in trouble with that, so I always advise to eliminate the fluff and stay away from subjective content. Stick to fact-based statements. A couple of key pieces of advice:

- Do not incorporate another firm's fees to prove your prices are lower. A regulator would likely have you remove that because you are intentionally cherry-picking other firms to make yours look attractive.
- Watch the way that you market yourself and the firm. People get terms mixed up. For instance, reps of the firm refer to themselves as investment advisers when it is actually the firm that is the investment adviser.
- Disclosures are key. They prevent misconceptions and misunderstandings of materials. And as a best practice, it's fine to list awards, but if they're paid for, it strips your credibility.

## **3. What policies do you recommend firms put in place related to remote work?**

Make sure your firm monitors and archives emails. If an adviser makes a remote workplace their permanent work location, they must disclose that they work from that address. Supervisors must be able to monitor individuals' client-related activity regardless of where they work.

## **4. How should they be testing these policies?**

Ensure you have the capability to monitor emails and business activities. You can do an on-site audit of the remote environment, but no matter how you go about it, all activities, including electronic activities, should be captured. I typically recommend VPN access or virtual desktops for these instances.

## **Any other comments?**

Typically, a client's biggest concern is being audited. Stay on top of your compliance tasks. Use a compliance calendar to ensure you never miss a date. The calendar is key.

## **5. Investing in compliance technology**

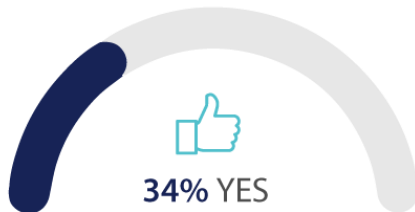
The pace of evolution within the compliance industry has created a maelstrom of competing priorities for compliance professionals, not the least of which being the management of enormous quantities of data flowing into their organization. As firms strive to address the new risks and regulations being brought by regulators, they are faced with a decision: continue with manual processes, checking and rechecking potential risk points, or invest in a comprehensive regulatory compliance technology designed for accuracy and dependability.

Determining the right compliance technology partner for your firm is an exercise in self-reflection and awareness, demarcating your firm's unique needs and must-haves and how they align with a provider's capabilities.

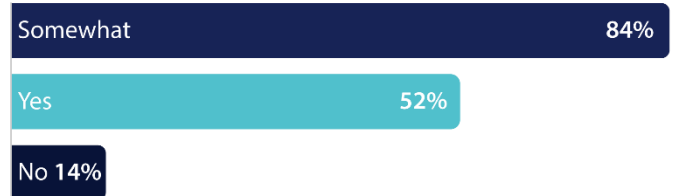
When finalized, the decision to invest in a compliance technology partner can yield numerous benefits including a more cohesive culture of compliance, precise compliance workflows that cross every T and dot every I and the ability to meet heightened compliance goals.

**security training may be the first critical step in any firm's cybersecurity plan, the next key focus should be on thoroughly [securing the firm's network and devices](#).**

ARE YOU CONSIDERING A NEW COMPLIANCE TECHNOLOGY SOLUTION?



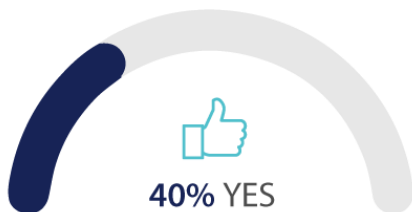
ARE REGULATORY CHANGES CAUSING YOUR COMPLIANCE TEAM TO MORE SERIOUSLY CONSIDER AUTOMATION?




WHICH CHARACTERISTIC DO YOU CONSIDER THE MOST ESSENTIAL IN A COMPLIANCE TECHNOLOGY PARTNER?



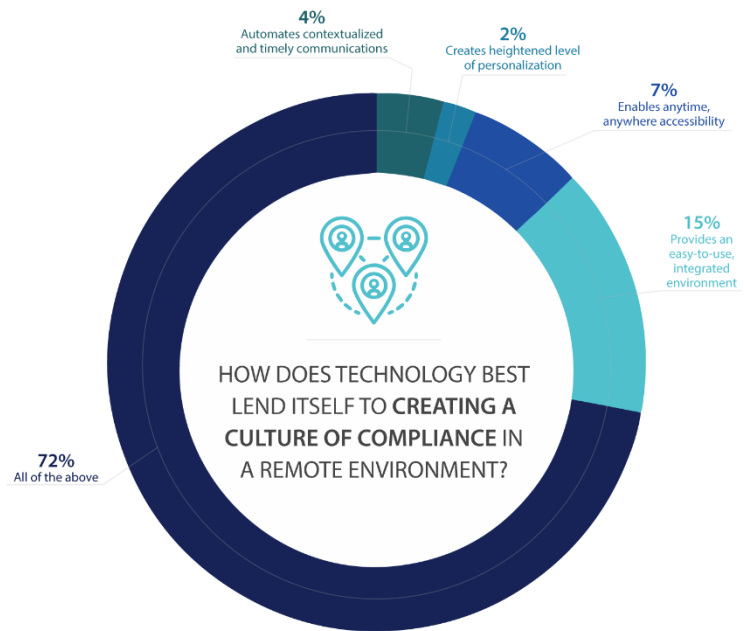
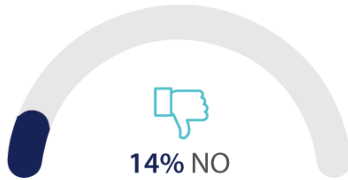
HAS YOUR FIRM INTEGRATED A COMPLIANCE TECHNOLOGY TO ASSIST WITH ANNUAL REVIEW PROCESSES?



 DO YOU FEEL YOUR EXISTING TECH STACK SUFFICIENTLY ADDRESSES THE SEC'S HEIGHTENED REGULATIONS AND PRIORITIES?



DO YOU FEEL YOUR TECHNOLOGY INTEGRATION HAS MADE DEVELOPING A CULTURE OF COMPLIANCE EASIER?



### Ask a compliance consultant:

#### 1. When it comes to your clients who have invested in technology, what has been the catalyst for that move? What are some of the core challenges they are solving for?

The major catalyst for investing in technology is the time savings. However, for every firm there is a cost/reward analysis:

- For smaller firms, the benefit is often found in what the technology takes away. If you are the CEO and CCO, you likely have an overflow of responsibilities and if technology can help ease some of that burden without putting too much strain on budgets, then the investment is likely worth it.
- For larger firms, the benefit of technology is in the streamlining of processes. With hundreds of employees to monitor, manual processes simply aren't feasible.

Ultimately, no matter the size of your firm, the integration of your tech stack is crucial. If your compliance technology doesn't speak with to other technologies the firm uses, you end up right where you started, manually processing data to keep your firm afloat.

#### 2. When you advise clients on whether or not they should begin to work with a technology provider, what are some common pieces of advice you offer? Any advice for those firms going through the migration process currently?

Technology is there to facilitate your compliance supervision, saving time and effort. However, a new technology doesn't have to mean a complete transformation of your compliance processes. When implementing a new compliance technology, make sure your procedures line up with what the technology does, meeting all of your requirements to ensure there is no buyer's remorse down the line.

Additionally, make sure your firm doesn't neglect the fact that responsibilities of supervision are still in place even while migrating to your new technology. Installing a new software or system doesn't mean putting your compliance program on pause.

### 3. We often say technology is just one piece of the puzzle, can you speak a little about the pillars of compliance (tech, people, education) and why each pillar plays such a critical role?

Sometimes, firms will buy a new technology and think they've solved all their problems, and to some extent that's true. However, having the tool and utilizing it are two different things. Not only do you need buy-in from your leadership and your employees, but you have to create an environment where your entire team understands how to use the technology, when they should use it and the benefit of having this kind of solution in place. After all, it's difficult to have an operational compliance monitoring program if your team isn't giving you the information you need to effectively surveil risks.

I am a believer in the power that comes from combining technology and knowledge. I often find that outside consultants are able to find the gaps that still need to be addressed even after a technology has been implemented. Taking that time to integrate people, education and technology is especially important in developing a risk assessment for your firm, actively identifying those activities which could derail your firm.

At the end of the day, it really is a marriage. Without compliance technology systems, you could be spending too much time manually assessing risk. Without outside expertise, you're only experiencing and pulling from your personal knowledge base, which could be limited in scope. You really need both.

## 6. Political contribution compliance during an election year

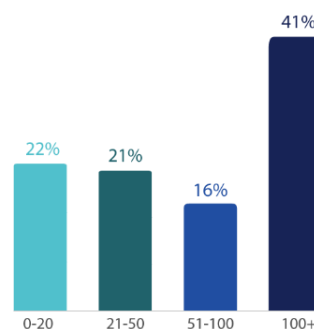
Political activism has resulted in a spike in pay-to-play compliance risk for those financial firms reliant on government contracted work. While many might be inclined to give this area of risk more credence during an election year, a political contribution compliance breach can have a detrimental impact even during typically off years. Gauging your level of risk in this area is just the first step to complying with federal, state and local regulations. Incorporating an active employee education program will help to alleviate some of this risk, clearly defining what regulations are applicable to your firm and your covered associates and how they should go about preclearing any and all contributions.



WHERE DOES POLITICAL CONTRIBUTION MONITORING RANK IN YOUR LIST OF COMPLIANCE PRIORITIES?



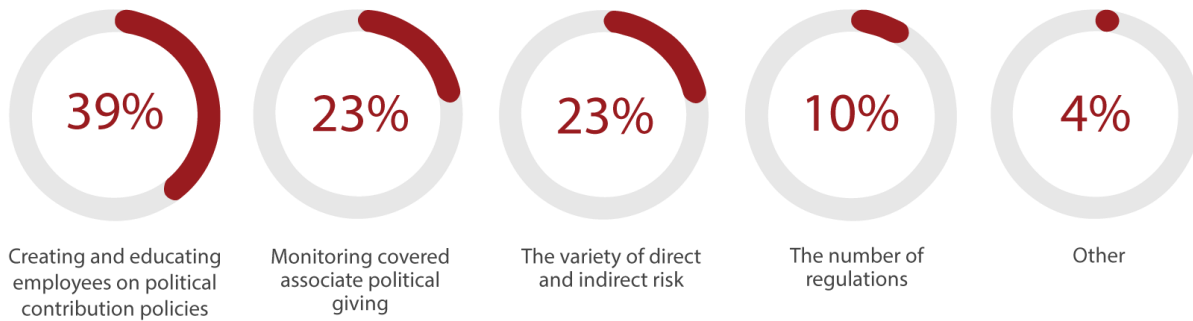
HOW MANY COVERED ASSOCIATES DO YOU CURRENTLY MONITOR?







## TOP CHALLENGES IN POLITICAL CONTRIBUTION COMPLIANCE



## Conclusion

Taking a snapshot of an industry is just that, a snapshot of a moment in time. However, it can often yield incredible insight into the trends and trajectory of an industry, offering insight into future challenges, endeavors and behaviors. In analyzing both firm and more specifically compliance programs over the first half of 2022, it's clear that rapid evolution is necessary. With new risks impacting compliance priorities and new regulations directing compliance requirements, professionals are being tasked with the near impossible: meeting every challenge flawlessly, ensuring no detail is missed and compliance is maintained.

In taking on this challenge, many compliance professionals have leaned into the technological advancements designed to help streamline the historically manual processes. And as a result of bringing on comprehensive compliance software and platforms, your peers are better able to meet these challenges and maintain an effective program, which protects their firm and its clients.

Understanding the challenges your peers face and how they go about meeting them can often be one of the best tools in proactively furthering your compliance program, ensuring that should you ever meet that same risk, you're prepared.

The expert insights shared throughout this page are brought to you by RIA in a Box Director of Compliance Dorothy Podzemny, RIA in a Box Director of Compliance Jametriss Roulhac, and NRS Senior Director, Consulting Services Ismael Manzanares. The proprietary data is comprised of survey results from the ComplySci portfolio of firms: [RIA in a Box](#), [ComplySci](#), [illumis](#), and [NRS](#).

Data from RIA in a Box is gathered annually from more than 2,000 RIA firms around the United States. ComplySci data was sourced from live webinars, with participants including investment advisers, hedge fund managers, broker-dealers and more.