NorthRow

State of compliance trends report 2023

TRENDS, CHALLENGES AND PRIORITIES

A report by NorthRow to help compliance professionals prioritise their strategies and accelerate growth safely.

Onboard. Monitor. Remediate

In 2023, as compliance professionals navigate the ever-changing regulatory landscape, the need for a function that leads the charge in ensuring continued compliance while supporting growth, improving the customer experience, and continuing the ongoing fight against financial crime is increasingly critical.

2022 threw global events, new regulations and record-breaking fines into the compliance melting pot. And yet, the war against bad actors, money launderers and criminals continues to wage. As fraudsters evolve and continue to develop their shady strategies, so too must our compliance teams.

Now, more than ever, compliance forms a critical part of an organisation's growth and strategy. Non-compliance opens the floodgates for financial, security and reputational damage, while allowing criminals to flood the financial system with dirty money.

One-third of the world's economies are predicted to slip into recession in 2023 (IMF, 2023) and compliance budgets are expected to shrink as a result. New initiatives may be shelved, increases in team headcount may be paused, and expenditure reduced. Meanwhile, the high regulatory expectations for every organisation's AML compliance programme remain unchanged.

To remain compliant with anti-money laundering expectations in 2023, organisations will likely have to do more with less, figure out when and where to use technology to streamline processes and deliver operational efficiencies at every turn.

We've collected data from interviews with almost 50 compliance professionals across more than a dozen industries to find out:

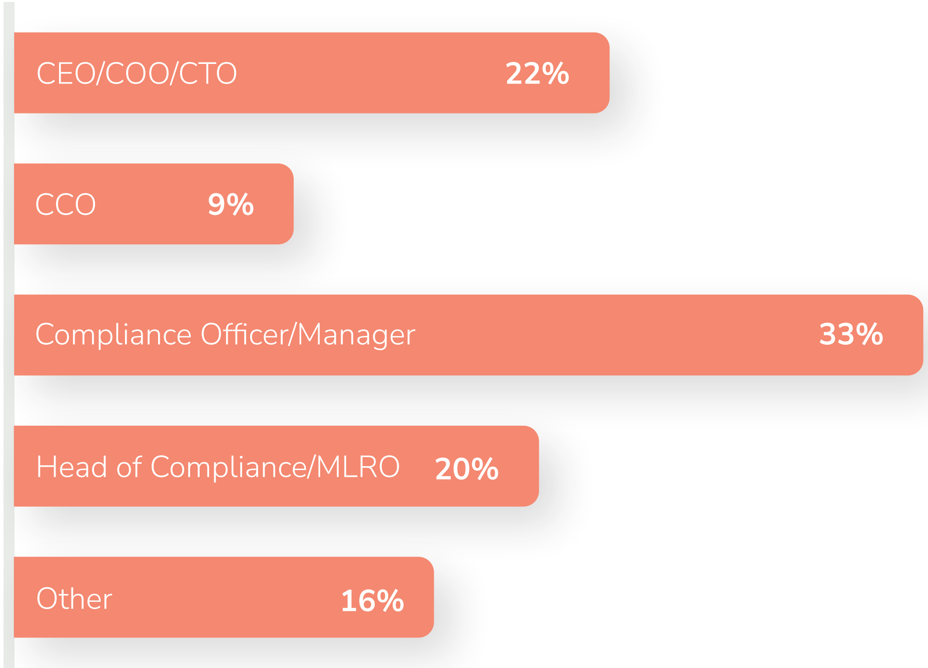
- Trends set to transform compliance
- Potential obstacles and challenges
- Where your peers spend their time
- A new era of digital compliance
- The perception of the department
- The future of compliance

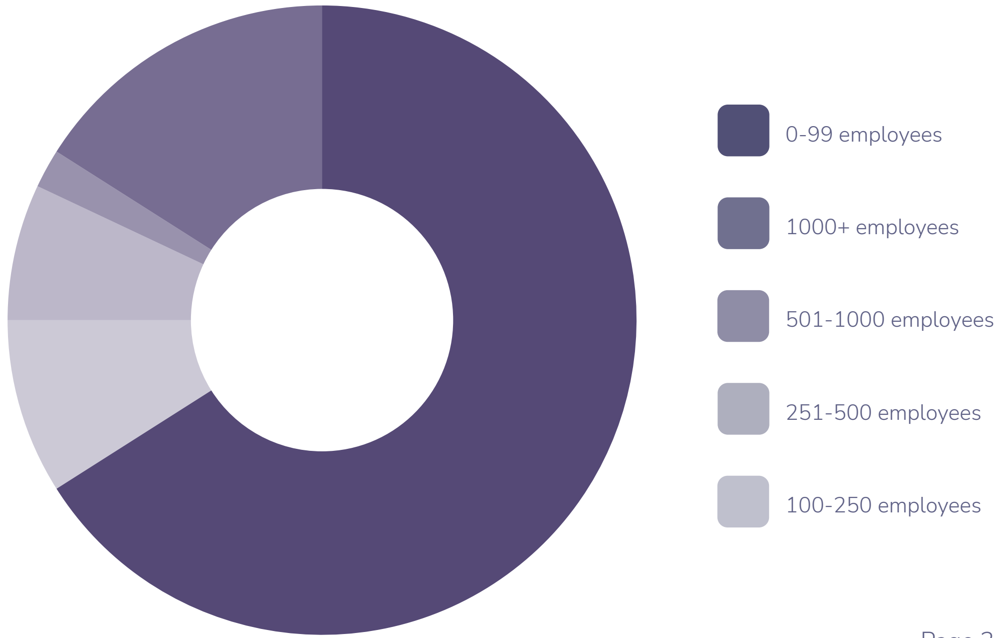
The first in a series of annual studies from NorthRow surveys senior leaders, heads of department, compliance and risk professionals on common themes from across the profession and asks them to share their top priorities and challenges.

This report is designed to offer compliance teams a better understanding of emerging trends and insight into what their peers are focusing on in 2023.

SURVEY DEMOGRAPHICS

Who did we interview?





KEY TRENDS IN COMPLIANCE

Emerging trends and priorities in compliance

In 2022, compliance teams faced persistent change and disruption, from economic uncertainty and the lasting effects of the pandemic to ongoing instability and strained relations between NATO and Russia.

With 2023 expected to bring heightened economic, regulatory and social uncertainty, compliance leaders must rethink how they provide critical services and strategic guidance.

In surveying a cross-section of the compliance landscape, we uncovered precisely where leaders plan to focus their efforts for success in 2023.

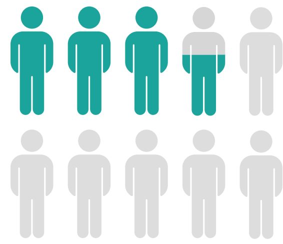
Unsurprisingly, given the inevitable change that continually affects the profession, **compliance training is the top priority for 42% of respondents.** Remaining current on skills, knowledge and training is a defining part of success in compliance.

Additionally, training is an excellent way to future-proof the department. Especially, in such a changeable environment, ensuring as little a knowledge gap as possible among compliance team members is key in supporting both current and planned business activities.

Making use of data and analytics, coupled with comprehensive reporting is another key priority for compliance teams looking ahead to 2023, being cited by 36% of respondents.

36%

cite data analytics and reporting as a key priority for 2023.



Data and analysis is crucial in moving from knowing your customers to truly understanding them. Armed with as much insight as possible, compliance teams are able to generate valuable business and management reports, uncover which cases are utilising the most resources and gain a deep understanding of KYC and KYB success rates.

What's more, data and analytics are not only reducing operational workloads in case management, but they can also be used in the prevention of financial crime. Compliance teams that are making use of advanced analytics can improve the KYC process, refine sanctions screening, and monitor ongoing client activity, helping to identify risks proactively.

A third of respondents also cite cybersecurity as one of their top priorities for the coming year. Regulated businesses are required to gather sensitive customer information as part of the KYC and KYB process, including identity verification documents, source of wealth and funds, adverse media reports, sanction list screening and PEP checks.

Ensuring that the internal systems and processes involved in the acquisition of this data is secure and free from prying eyes is critical. Any sort of vulnerability can lead to data breaches that can paralyse entire businesses through fines, legal proceedings and reputational damage.

Not only is cyber and information security a key part of data collection in terms of AML and KYC processes, but ensuring robust business-wide cybersecurity protocols can help to prevent data breaches, social engineering attempts, malware and viruses from devastating cyberattacks. Seasoned cybercriminals will attempt to access sensitive data for crimes such as

> In a data-driven financial environment, cybercrime has emerged as a major concern for regulators and institutions, with criminals manipulating computer systems and online financial services to commit money laundering, fraud and other crimes.
>
> **The European Institute of Management and Finance**

identity theft and fraud, but may also seek to perpetrate other forms of financial crime including theft and scams in order to steal money from your business, your customers or both.

A company's strategy must include anti-fraud, anti-money laundering, and cyber security initiatives as top priorities, with adequate budgets for employee training, tools, and constant monitoring for any vulnerabilities.

Conversely, **ESG initiatives and introducing RegTech were bottom of the priority list for compliance leaders, being cited by just 18% and 20% of respondents respectively.** Given the amount of focus placed on ESG initiatives and the value of introducing technology into compliance in recent months, one would hope that the lower rankings of these two business-critical factors on priority are simply down to the fact that these initiatives are in-hand and being effectively managed as part of wider compliance efforts and strategies.

Look for 2023 to see a broader welcoming of FinTech and RegTech strategies, including aggressively using AI to more quickly review domestic and international instant payment mechanisms. Regulators and investigators will also give more attention to the volatile and currently imploding crypto sector.

Association of Certified Financial Crime Specialists

FACING THE CHALLENGE

Potential obstacles and challenges in 2023

The challenges facing compliance professionals and those in the businesses of financial crime prevention evolve on a near-daily basis. Whether it's new regulations to contend with, mastering new technologies, attracting talent or staying on top of the latest trends in financial crime and money laundering techniques; compliance professionals must be nimble enough to think on their feet and pivot at a moment's notice.

While one of the biggest lures for those entering the field of compliance is the ever-changing nature of the sector and the notion that 'no two days are the same', there is mounting pressure on professionals to pay attention to, and revise, compliance processes as these changes come about. Failing to do so could result in non-compliance and hefty fines from the regulators.

Reflecting our findings into the priorities facing compliance professionals, **keeping abreast of regulatory and political change tops the list of challenges** that leaders are bracing for in 2023.

Cited by nearly half of our respondents (42%), the task of managing regulatory requirements evolves as the nature of technology, money and society evolves.

Regulation is often issued in response to societal changes (such as the surge in interest in cryptocurrencies and NFTs, or the recent Russian invasion of Ukraine) or to keep up with changes in technology (challenger banks and Buy Now Pay Later solutions for example).

The challenge of staying on top of regulatory change is only magnified in cases where firms operate globally. Complying with cross-border and multi-jurisdictional AML rules can be a difficult task for compliance teams. There may be different AML regulations in place in different jurisdictions for regulated institutions, making compliance at all levels a demanding task.

Reflecting this, **the challenge of sufficient data coverage and accuracy for AML compliance poses a further challenge for one-third (33%) of our respondents.**

Accurate data is the cornerstone of a robust KYC/B process. Whether gathering information on private individuals and corporate structures, or screening for sanctions and other adverse data, compliance teams need to be able to review potential matches, explore additional information and exclude false positives quickly as part of the onboarding process.

Manual KYB checks alone can involve compliance teams searching company records for days on end, thumbing through case files, chasing down documents from Ultimate Beneficial Owner (UBOs) registers, and verifying endless pages of company accounts and financial statements. This, which can ultimately stretch an already lean department's resources, can also have a detrimental effect on time-to-revenue and cash flow.

42%

Regulatory and political change

33%

Data coverage and accuracy

31%

Resource capacity and capability

31%

Ongoing monitoring

A DAY IN THE LIFE

Where your peers are spending their time

The role of a compliance officer is extremely diverse. Amongst other day-to-day duties, responsibilities include staying on top of legislation changes and reporting requirements, understanding complex company structures, and improving the customer experience.

A single day can consist of providing financial and AML regulatory advice to colleagues, onboarding a new client, screening existing ones, assessing regulatory risks, reviewing client cases, reading press articles, organising training sessions on AML regulations for customer-facing staff, meeting with regulators for audits, and so on. Every day brings a new challenge, which they must always be prepared to meet.

And so, with such critical responsibility, our research uncovered some astonishing insights into the true cost of ensuring AML compliance.

According to our respondents, the **most common checks being undertaken are KYC onboarding checks, being cited by a third.**

KYC checks, ascertaining proof a person is who they claim to be, usually involves basic ID checks, credit checks, and routine PEPs and sanctions screening.

For **one in five of our respondents, these checks are taking more than 24 hours to complete.** And, for 9%, these checks take more than 3 business days.

Of course, not every KYC check is straightforward and further investigation may be required where PEPs, sanctions or other high-risk indicators are flagged, thus delaying the process somewhat. But, in today's 'always on' environment, customers expect to be onboarded swiftly. 3-5 business days is simply not good enough.

Proving who we are online is seemingly still cumbersome for some institutions, rife with inefficiencies and often across varying channels to prove who we are - in some cases, taking customers offline to prove their identities in person or by posting sensitive identity documents.

With abandonment rates in financial services rocketing, cumbersome application processes where too much personal information is requested and, where there is not an end-to-end digital process in place, customers are being required to visit branches (where firms still have physical locations!) or offices in person with physical documents in hand. Consumers want on-demand, digital-only onboarding.

What's more, this surge in abandonment is costing serious cash. In research by P.A.ID Strategies, it's estimated that £5bn is lost each year to abandonment during the onboarding process in the financial services sector alone.

From our research, these processes are continuing to take too long for an increasingly digital-savvy consumer base who expect to access products and services as quickly as they can log in to their social media accounts.

20%

of KYC checks take more than 24 hours

KYB checks are taking a similar, disproportionate amount of time to complete. **One in five also cite that KYB checks are taking more than 24 hours to complete,** with 8% sharing that this takes more than 3 business days.

Granted, KYB checks are, by nature, more thorough than a typical KYC check. Access to richer data is needed to investigate UBOs, PSCs, financial reports, adverse media, and, where required, ID&V checks for business directors and key stakeholders.

A KYB check on one business can incorporate dozens of individual checks of both the entity itself and its associated stakeholders.

Reassuringly, the **average onboarding success rate across all respondents is a healthy 80%.** But, this is coming at a cost.

When asked to estimate the approximate **percentage of business revenue being spent on compliance costs, the average figure shared by our respondents was an eye-watering 25%.**

What's more, **18% estimated that more than 50% of revenue was being spent on compliance costs.** At a time when budgets are being cut throughout the economy, and a recession looming, can firms really afford to be spending such significant amounts on compliance?

Without doubt, dramatically slashing compliance budgets is a false economy. Any perceived cost savings can be easily wiped out by a hefty fine from the regulators, and any damage associated with non-compliance to a company's reputation can be difficult to recover from.

A recent report from Thomson Reuters shared an anecdote from a respondent discussing the challenge of budget vs. compliance: "the biggest challenge I expect to face is rolling out a champagne and caviar compliance programme on a bread and water budget."

There has to be a more cost-effective option that balances compliance with customer experience.

Most common types of data required to achieve compliance

Personal identification data	77%
Information on PEPs and sanctions	53%
Basic company information	51%
Adverse media	27%
PSCs and UBOs	22%
Credit reference agency data	16%
Information on CCJs	11%

Most commonly used data sources

Companies House	33%
UBO/PSC registries	31%
Dow Jones	29%
International registries	29%
LexisNexis	24%
Electoral Roll information	16%
Experian	13%

Others included Bureau van Dijk (4%), Dun and Bradstreet (4%), Accuris (7%), Equifax (9%), and Creditsafe (4%).

THE FUTURE OF COMPLIANCE

A new era of digital AML compliance

Today's leaders are already aware of the powerful capabilities of digitisation across departments, from marketing and finance to operations and IT. Time-saving, cost-saving, driving efficiencies, happier staff...the benefits of introducing technology are endless.

And yet, according to our research, compliance teams seem slow to adopt this area of digital transformation. Technology which is designed to make their working lives easier, and provide a better customer experience across the board.

Just 38% are currently using RegTech (regulatory technology), software created to ease the management of client onboarding, regulatory monitoring, reporting, and compliance. Worryingly, **40% use basic office productivity tools such as word processors or spreadsheets** to manage their compliance processes.

Regulated institutions of all sizes are becoming more digital in their daily operations, and improving customer experience and boosting efficiency remain high on leaders' agendas. The logical next step for regulated institutions is to further leverage digitisation for compliance. Through the use of RegTech, compliance teams can deliver process efficiencies, costs, and a more confident and connected compliance strategy.

> The evolution of FinTech necessitates a parallel development of RegTech. Regulatory overlaps and contradictions are not uncommon, and financial institutions have, unsurprisingly, looked to RegTech to optimise their compliance management.
>
> **CFA Institute**

Of those that do use RegTech, respondents report a number of key benefits. From having a central location to manage compliance and controls, to the effective management of compliance cases, facilitating informed decision-making, and the ease of understanding and visualising trends in compliance performance.

Those that don't, cite **budget as the main prohibitive reason for not investing in RegTech (66%)**. And yet, when you consider our earlier insight into the proportion of revenue being spent on compliance costs, surely this begs the question: can compliance costs be better allocated?

Insufficient resources and a lack of time are seen as further blockers to considering RegTech, being cited by 16% and 11% respectively.

Naturally, there will always be cases that require further due diligence before you safely commit to onboarding them, continue an ongoing relationship, or not. It is these cases which often result in a higher proportion of manual activity and intervention required. And yet, when 100% of compliance is being managed manually or via spreadsheets, these single, complex cases can consume a significant portion of compliance teams' time.

This is often where the vast amount of compliance costs stem from and where time is being spent. It is estimated that a staggering 90% of compliance costs sit within just 10% of cases!

Using RegTech allows for the automation of comprehensive KYB and KYC checking processes, including identity, document and liveness verification tools, and compliance teams can streamline their onboarding processes with client verification in real-time.

With tech doing most of the heavy lifting, talented compliance professionals can focus on the cases where they can most add value, leaning on their expertise to ensure compliance.

WHY COMPLIANCE IS ESSENTIAL

The perception of compliance as a valued strategic partner

In many organisations, compliance is perceived as a 'necessary evil' that firms must undertake to avoid undue involvement with regulators and enforcement bodies.

There is usually a distinct separation between the compliance function and the rest of the organisation, which can lead to a lack of communication and synergy between the two. It is important for compliance teams to have a degree of autonomy, but it is equally as important that the function is fully integrated into all aspects of the organisation's day-to-day operations.

Compliance teams are coming under increasing pressure to speed customer cases up and arrive at an onboarding decision, especially in sectors where a commission payment is involved (such as in the property sector) for closed deals.

In cases where businesses are overly risk-averse or, if there is a backlog of cases awaiting compliance checks, customer-facing teams may take to seeking out ways to 'smuggle' unverified clients through loopholes in compliance processes.

It is imperative that everyone within a firm that is involved in onboarding and managing customers, sees compliance as a critical activity and abides by defined processes.

Overall, **the perception of compliance among respondents is high, with 73% stating it had a positive or very positive perception within their businesses.** However, this does mean that more than one in five feel that it is being perceived less favourably.

Here are just some of the reasons why respondents felt the department wasn't valued in their business...

"Compliance is like paying taxes; it is a necessity, without any feelings or sentiments attached to it."

"Few really know what compliance and ethics is!"

"Because of the reaction to all things compliant...'We HAVE to do this'."

LOOKING AHEAD

The future of the compliance profession

As we look to 2023 and beyond, we asked our respondents what the future of compliance might look like in their business in the next 12 months.

Their responses varied hugely: some are bracing for an onslaught of regulation, others are looking to automate processes and become more data-driven, developing a firm position as a trusted advisor to the C-suite, and more focus on expanding their influence within their respective businesses.

Equally, some shared concerns around the tightening of regulation, more complications within the profession and the difficulties for smaller firms to comply with requirements.

Here are just some of the predictions from our respondents as to what the future of compliance will look like in their business, and the profession as a whole in 2023 and beyond:

"The compliance function is likely to **expand within the company.** With the industry as a whole, I think there will be **more requirements around sanctions and PEPs.**"

"Automation needs to be implemented and resources used to **target areas of opportunity for growth and development of the business.**"

"It will all be **100% automated.** While we are fully automated now, it still takes a lot of employee oversight."

"More data driven, less manual verification - **instantaneous verifications**."

"We will be looking to **automate our onboarding and KYC checks** as much as possible and get defined processes in place."

NorthRow provides software which empowers compliance officers to make faster decisions and onboard customers in seconds, not days whilst complying with ever-changing legislation, so that they can contribute to their business' growth, safely.

Registered Office Address:
85 Great Portland Street, First Floor
London
W1W 7LT

Email: info@northrow.com
Phone: +44 (0) 1235 375000

northrow.com

NorthRow