REGULATORY COMPLIANCE

REGULATORY COMPLIANCE

Distributed in
THE TIMES

Published in association with
International Compliance Association
The Association of Governance Risk & Compliance
RegTech Insight From A-TEAM GROUP

Contributors

Ben Edwards
A freelance journalist specialising in finance, business, law and technology, with more than a decade of editorial writing experience.

Jack Apollo George
A writer and semiotician interested in the ethics and aesthetics of technology, sustainability and cultural change, with articles published in the *New Statesman* and *The Day*.

Sally Percy
A business journalist specialising in leadership and management, and editor of *Edge*, the official journal of the Institute of Leadership & Management.

Ouida Taaffe
Editor of *Financial World*, the magazine of the London Institute of Banking & Finance. She has also previously covered the telecoms market.

Raconteur

Campaign manager
Jean-Philippe Le Coq

Reports editor
Ian Deering

Deputy reports editor
James Sutton

Editor
Sarah Vizard

Chief sub-editor
Neil Cole

Sub-editor
Christina Ryder

Commercial content editors
Laura Bithell
Joy Persaud

Associate commercial editor
Phoebe Borwell

Head of production
Justyna O'Connell

Production executive
Sabrina Severino

Design
Kellie Jerrard
Harry Lewis-Irlam
Colm McDermott

Illustration
Sara Gelfgren
Celina Lucey
Samuele Motta

Design director
Tim Whitlock

@raconteur · raconteur-media · @raconteur.stories

raconteur.net /regulatory-compliance-2023

DATA PRIVACY

Is it time for GDPR 2.0?

Five years on from the arrival of GDPR, the UK is weighing up post-Brexit divergence as a chance to refresh the data protection rules. What might that mean for compliance?

Jack Apollo George

The information superhighway slows for no one. Data and capital have crossed borders with greater ease than people for decades. But try to move the personal data of Europeans outside the EU and you'll be in serious trouble.

As the gold standard for data privacy, the General Data Protection Regulation (GDPR) undoubtedly has teeth. For instance, in May, Meta's EU base in Ireland was fined €1.2bn by the European Data Protection Board (EDPB) for breaching the flagship data protection law. Andrea Jelinek, the chair of the EDPB, alleged that Meta had engaged in "systematic, repetitive and continuous" transfers of personal user data from the EU to the US. To date, it's the biggest fine levied under GDPR.

The UK adopted GDPR in 2018. In the five years since then, British businesses have become fully aligned with those on the Continent regarding data regulation. You'll have noticed the pop-ups asking you to accept cookies or to opt in to a company's data privacy policy when you visit their website. That's GDPR in action: nominally putting your data in your hands, and giving you the choice to share it online if you so please.

That said, the mechanism is clunky. Plenty of sites don't have a 'no' button immediately available, which makes it easier to click 'yes' without fully being aware of the consequences. And the demands on the compliance side are far from negligible, especially when dealing with large amounts of personally identifiable data.

Various other issues have also arisen, with complaints ranging from the fact that GDPR takes a 'one-size-fits-all' approach – its provisions not being tailored to different sizes of business, sectors or data use cases – to broader concerns that it overburdens those businesses designated as data controllers.

In the past few years, then, there have been murmurs of the UK taking advantage of Brexit to create its own, distinct data protection regulation. The goal: to cut red tape and empower British businesses via a new and improved policy. The fear: deviating from a global gold standard, diluting personal protections and hurting consumer confidence.

Proposals for a new, UK-wide data protection bill are working their way through parliament. The secretary of state for science, technology and innovation, Michelle Donelan, introduced the Data Protection and Digital Information Bill in March. The announcement promised a "common-sense-led" law that would reduce the "costs and burdens" to British businesses.

According to a government spokesperson, modernisation is the prime focus of this bill. "Our new Data Protection Bill seizes a post-Brexit opportunity to bring our data rules into the current decade, delivering £4.7bn for the UK as a result," they say. "The new regime will reduce burdens on businesses, boost the economy and unlock innovation across the UK, all while building on our already high standards for the protection of personal data."

One of the key challenges in refreshing GDPR, however, will be achieving so-called EU data adequacy, which allows EU data to flow freely to a third-party country. This would ensure there are no trade fallouts with European partners, which could otherwise prove incredibly costly to British businesses. As evidenced by high-profile GDPR-related fines, the US does not have EU data adequacy.

But legal analysis of the government's new bill has found several areas of potential divergence from GDPR, including the possibility of commercial enterprises being exempted from some data protection requirements if the data is being used for purposes that could "reasonably be described as scientific". That would indicate an attempt, albeit a risky one, to empower businesses and researchers by avoiding one-size-fits-all red tape.

But on the other side of the Channel, some are asking if GDPR needs to get stricter, not more flexible.

"Europe should double down on its flagship data protection law," comments Townsend Feehan, CEO of IAB Europe, an association representing digital advertisers and marketers across the continent. "GDPR empowers people in a way no other privacy law does. However, five years on, we are at risk of having choices taken out of people's hands and placed into powerful aggregators such as web browsers and operating system manufacturers."

Even among businesses required to comply with GDPR, there seems little appetite for any loosening of the rules or lifting of the compliance burden. That's because giving consumers control, via pop-ups and clear privacy policies, can be a positive thing, and because complying with GDPR has improved businesses' data practices generally.

Alex Laurie is senior vice-president of global sales engineering at identity verification software provider ForgeRock. He acknowledges that while the implementation of GDPR hasn't always been straightforward, "what it has unequivocally achieved is a new level of trust among consumers".

"What we'd expect to see next," he comments, "is even more control being given back to consumers, who should get to decide which information is shared with what providers, instead of mass-sharing all of their personal data."

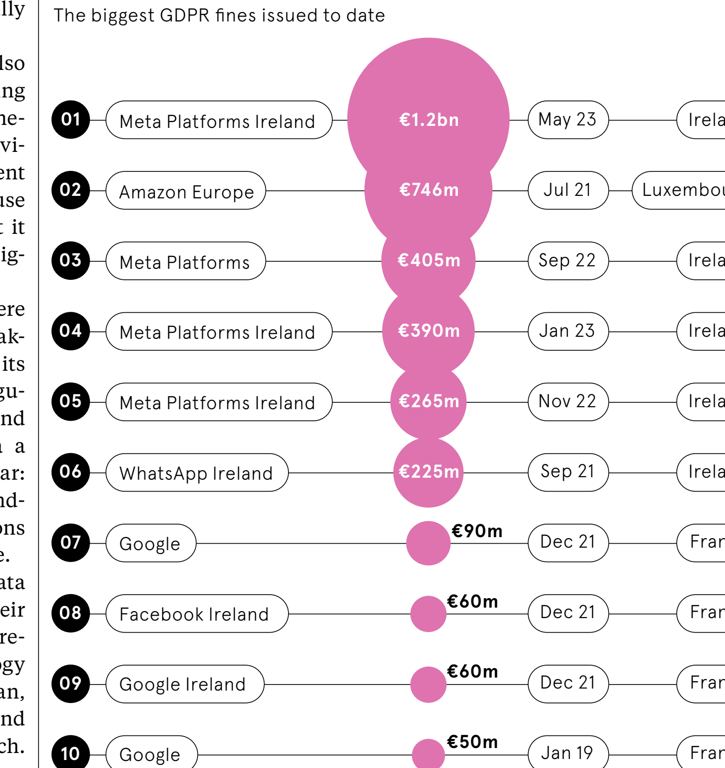
Scott McKinnon, field CISO for EMEA at US cloud company VMware, suggests that the focus for future regulation should be on encouraging a more holistic "privacy by design" approach. This means "not only evaluating a company's adherence to the law, but also its effectiveness in safeguarding individuals' privacy".

"By adopting this approach," he explains, "businesses will be incentivised to prioritise privacy protection, rather than solely focusing on meeting regulatory requirements."

Whether the UK government's new bill achieves the right balance of enshrining personal data protections while also alleviating burdens for businesses remains to be seen. Either way, after five years of GDPR, the UK is undoubtedly moving into a new era of data protection.

THE US TECH GIANTS ALREADY HAVE A GDPR COMPLIANCE PROBLEM

The biggest GDPR fines issued to date



CMS, 2023

SUSTAINABILITY

The power of green purse strings

Armed with some significant incentives, trade finance providers are well-positioned to help businesses achieve good ESG standards in their supply chains. But can they really police this model themselves, without the guiding hand of a regulator?

Ouida Taaffe


Daniel Balakov via iStock

Blissful ignorance is no longer an option. From January 2026, large corporates with operations in Europe will need to have full oversight of the environmental, social and governance (ESG) standards in their supply chains, under the terms of the EU's Corporate Sustainability Reporting Directive (CSRD). And from January 2027, the rules tighten up even further, to include smaller firms.

Given that large companies often have tens of thousands of suppliers around the world – and many tiers of suppliers – that won't be easy. But help may be at hand.

Big corporates use trade banks to provide supply chain finance (SCF). That's to say, they ask their bank to extend credit to a supplier on better terms than the small firm could command on its own. It's a form of receivables finance, and can be used to encourage certain behaviours.

Walmart, for example, works with HSBC to source cheaper finance for suppliers that have better sustainability ratings as part of its global Sustainable Supply Chain Finance programme. The smaller firms benefit from pricing that is linked to Walmart's credit rating.

The idea now is that SCF could be used as a carrot to encourage better flows of data around ESG compliance and higher ESG standards.

This already seems to be a growing trend. "The number of conversations we are having with clients on embedding sustainability into their supply chains has increased significantly over the last 12 months," says Vasilka Shishkova, solutions structuring director for global trade and receivables finance at HSBC. She explains that the demand is largely down to the new disclosure and reporting requirements.

The CSRD does not mandate any specific penalties for non-compliance, but the expectation is that no one will want to be the skunk at the ESG picnic. That would mean higher costs of finance and reputational problems.

The current guidelines may also be just the start. Research by HSBC and the Boston Consulting Group in 2021 showed that global supply chains account for up to 80% of the world's total carbon emissions. Unless supply chains adapt to become greener, more socially responsible and reflective of good governance practices, the planet has a serious problem.

So, could a combination of reporting guidelines like the CSRD and incentivised 'self-regulation' via SCF be the solution? Or does there always need to be a regulator making companies toe the line?

It's a question made all the more important by a rising awareness of the various issues in global supply chains, from hidden child labour to the destruction of rainforests and toxic oil spills. But as Angela Francis, director of policy solutions at WWF-UK, explains, supply chains can undoubtedly be a force for good. "Trade is an enormous driver of innovation," she says. "We have got to use it to drive net zero."

Some corporates are already rejigging their supply chains to do just that. "The rules of engagement are changing," says Shishkova. "Previously the goal was producing the best quality at the lowest price. Now, increasingly, conversations are about transitioning manufacturing processes to embed ESG." That can even sometimes lead to dropping suppliers which can't meet ESG standards or reporting requirements, she adds.

Of course, that kind of decision won't always be an easy call. "One problem is that smaller companies – both buyers and sellers – don't necessarily have the required data, especially when you get down to the deep tiers," observes Rebecca Harding, an international trade consultant who created the world's first automated sustainability scoring system for trade finance.

Still, based on the sums involved alone, the idea of using SCF to drive good ESG standards does look convincing. According to HSBC's research, up to half of the $100tn (£79tn) investment needed to achieve net zero by 2050 has to be directed towards SMEs. SCF could be a useful conduit for that.

Then there's the global reach that trade finance offers. Shishkova argues that SCF could ultimately achieve a far greater impact than legislation or other conventional forms of ESG regulation, on the grounds that supply chains connect millions of companies worldwide.

But hitting the mark remains a work in progress. "Most banks would say that if you can get targeted money to businesses in supply chains, that can help both the supply chain and the bank to be more sustainable," says Harding. "The problem is that it's hard to know what, say, 'green' really means."

There are other practical issues too, Harding adds. "Supply chain finance tends to move quite quickly – within 30 days. Getting the right data, at the right time, can be both expensive and unwieldy."

A further challenge – for SCF providers and regulators alike – is that dealing with ESG is a moving target. What needs to be done will change as the climate transition proceeds and the planet warms. What's more, many problems, such as the loss of biodiversity, are so-called 'externalities' that are not yet priced into business models.

"Regulators want to know about the ESG-related risk exposures of banks because regulators are tasked with overseeing financial stability. But this looks backward and not forward to the ESG transition that needs to take place," says Harding. That could, she says, lead to more 'green-hushing', where firms focus on toeing the current regulatory line and keep quiet about what's needed for the future.

Harding suggests that SCF providers and their clients should approach regulators to discuss what rules, standards and data would help the banks to effectively incentivise more sustainable supply chains. "So, for example, the regulations could be changed to allow different capital ratios [at banks] for more sustainable assets," she suggests.

After all, the banks are just part of a much bigger – and highly politicised – space, Harding explains. "Trade is being weaponised and the sustainability agenda is being weaponised. The banks are the foot soldiers in this space and they are being told to go over the top. They're damned if they do and damned if they don't."

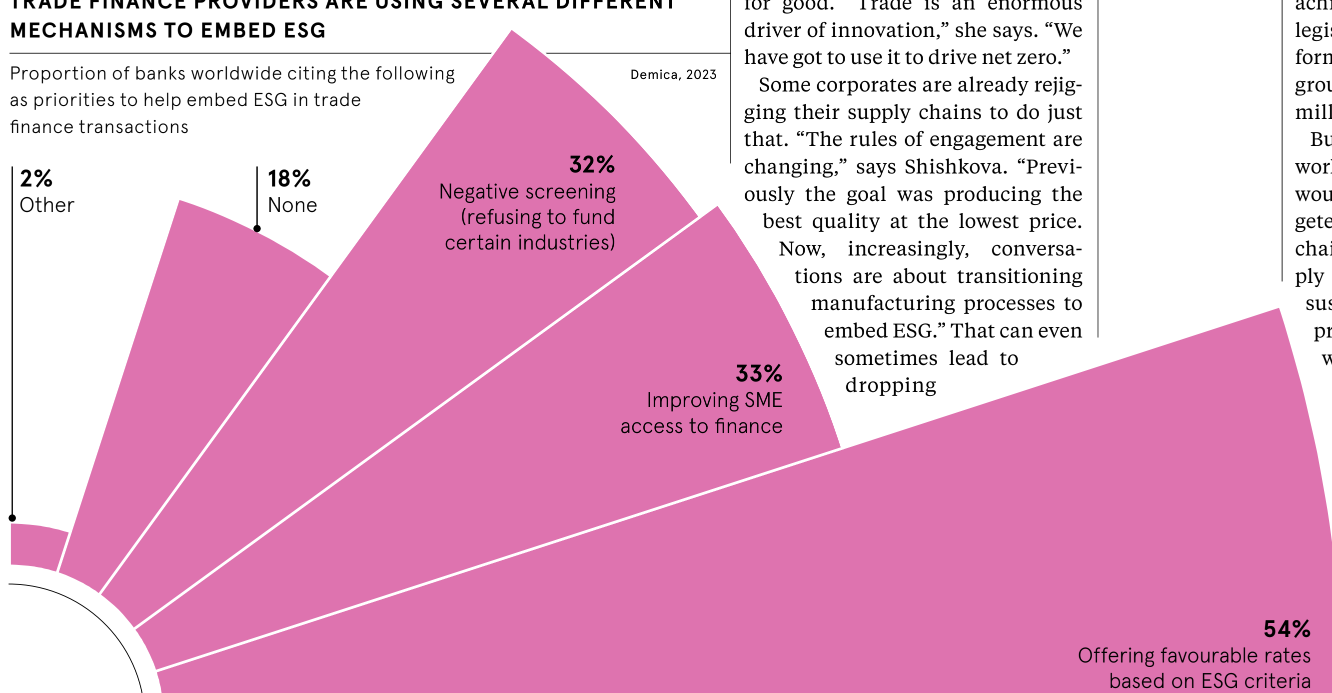
Fundamentally, in Harding's view, the need for good ESG standards in supply chains means that banks are being asked to shift from a value-based model to one that prioritises values. But a banking and funding model not built on market prices is a radical departure.

"A new values-based economic system requires a public discussion," Harding says. "For example, should the rich north try to impose its values on the global south?" That's hardly, of course, the sort of question a bank can be expected to answer alone.

TRADE FINANCE PROVIDERS ARE USING SEVERAL DIFFERENT MECHANISMS TO EMBED ESG

Proportion of banks worldwide citing the following as priorities to help embed ESG in trade finance transactions

Demica, 2023



INSIGHT

'Compliance is assuming an ever more strategic role'

The rise of ESG is a chance for compliance teams to step up and help companies do the right business in the right way, says the International Compliance Association's **Pekka Dare**

In today's dynamic business environment, the remit of compliance practitioners is constantly evolving. Current priorities include ESG and supply chain risk; rapid technological change; financial crime and other threats to consumer protection from the cost-of-living crisis; the growing scope and complexity of sanctions regimes; and more besides.

And in the face of such change, compliance is assuming an ever more strategic role, helping organisations navigate this landscape, and ultimately enabling good business.

The rise of ESG is a prime example of this. Compliance practitioners can make an essential contribution towards meeting ESG obligations, by helping organisations identify their ESG risk appetite and exposure, and by influencing ESG strategy. This includes understanding emerging global ESG standards, reporting frameworks and regulations, and then designing and implementing policies, procedures and controls to adhere to them.

Climate risk and reporting is one area receiving considerable attention. For instance, in the UK, regulators' expectations are ramping up, with the Prudential Regulation Authority (PRA) requiring business leaders to articulate how climate considerations are integrated into their organisations' strategies, governance structures and risk management processes. Meanwhile, the Financial Conduct Authority (FCA) has urged firms to develop clear net-zero transition plans, despite final rules still being in development.

To date, the limited availability and poor quality of data has hindered climate risk assessments, reporting and planning. While many organisations have some grasp of their scope one and scope two emissions (those directly or indirectly associated with day-to-day operations), measuring scope three emissions (those embedded in the value chain) is proving more challenging, particularly for businesses with complex global footprints.

With that in mind, the PRA expects firms to have a "counterparty engagement strategy". This should help them understand how their counterparties plan to manage climate risk exposures, and will then inform their decisions on which customers to accept and which sectors to operate in.

As well as requiring improved transparency around ESG in businesses' supply chains, regulators are also paying closer attention to the products and services that firms offer. Terms such as "green" or "sustainable" have historically been poorly defined. Now though, as a consensus emerges around appropriate metrics for assessing the environmental and social impact of products and services, organisations increasingly run the risk of greenwashing. Compliance teams will play a major role in ensuring that businesses walk the walk here.

Finally, organisations must also embed ESG objectives within their broader values, goals and culture to avoid the shortcomings of a tick-box approach. For compliance, similar work took place following the 2008 financial crisis, as regulatory attention shifted from monitoring firms' adherence to rules and principles towards scrutinising organisational purpose and outcomes. This required firms to initiate sweeping programmes of cultural change.

So, while ESG may seem like new territory for compliance, it is really a natural extension of the strategic direction the role has taken over the past decade, as the overlaps between ESG and broader financial conduct and financial crime compliance make plain. Indeed, NGOs such as Transparency International increasingly highlight the interactions between bribery and corruption, poor governance, and negative environmental and social impacts.

The emergence of ESG, then, is simply a new frontier in compliance's ongoing mission: to help the right business be conducted in the right way.


Pekka Dare
President,
International Compliance Association

Commercial feature

Four defining trends for the future of regulation

Increasing complexity and higher volumes of data have entered the regulation conversation, compelling financial institutions to shift their compliance strategies

The pace and complexity of regulation that's built up since the global financial crisis has made it harder than ever for financial firms to manage compliance - from trade reporting mismatches to sprawling and increasingly outdated systems, financial institutions are assessing if there may be a better way to handle regulatory change.

Paul Rennison, director of product management at deltaconX, walks through some of the key regulatory and compliance developments that the C-suite will need to be prepared for in the coming months.

01 Data standardisation goes global

The wave of financial regulation that came out in the wake of the global financial crisis, such as the Dodd-Frank Act in the US and the European Market Infrastructure Regulation (EMIR) in the EU, has created a mountain of reporting requirements that are expensive to comply with, says Rennison. One of the shortcomings with those rules is a lack of standardisation; trades could be reported by both counterparties in slightly different ways, resulting in significant amounts of reporting data that doesn't match up, he explains.

As regulators seek to refresh those rules, the International Organization of Securities Commissions (IOSCO) and the Committee on Payments and Market Infrastructure (CPMI) are working together to create a common lexicon for trade reporting to establish greater data harmonisation across jurisdictions. This can improve accuracy but also reduce the expense of having to retain and manage complex data sets that vary depending on where the trade took place. "Standardising this makes it easier for an apple to equal an apple wherever you trade that apple," says Rennison.

> Standardising this makes it easier for an apple to equal an apple wherever you trade that apple

02 'The growth of grey IT'

Organisations have fewer resources at their disposal after many people left the industry during the pandemic, while the pace of regulatory change remains relentless, says Rennison. "It's never a single project within a firm; it's a programme of work," he says. "It's like painting the Forth Bridge - you get to the end and look back, and you have to go and start again."

This ongoing monitoring and managing of rule changes is expensive. Systems that were robust when post-financial-crisis regulations were first implemented are growing outdated. "It is hard to get continuing reinvestment; you get stuff bolted on to keep it going, so you get the growth of grey IT which becomes even more expensive to maintain as it starts to die," says Rennison. Organisations need to start reassessing their approach to technology and how to manage compliance where change is constant, and costs continue to surge.

03 Outsourcing strategies for uncertain times

The cost of managing in-house compliance systems is prompting many organisations to consider outsourcing strategies, especially where the benefits of the cloud can be realised. In the past, data was retained in-house because it was deemed to be commercially sensitive information and too high risk to go beyond the organisation's firewall, says Rennison. Over the past 10 years, that view has shifted as organisations recognise the potential savings - particularly as datasets get bigger and more costly to manage in-house, he says.

By moving to the cloud, systems can be lighter, more agile and more elastic, making it easier to scale in tandem with the growth in data volumes. "If I can get someone else to operate the services for me, then I can take that finite, scarce internal resource and reallocate it somewhere else," Rennison says. "You're taking away a lot of the water-carrying functions - the repeat operation processes - so your compliance team can do higher-value work with the data collected."

04 Driving proactive compliance with AI

Regulators are already adopting AI to support their analysis of reporting data, helping them look for patterns or behavioural changes at both a market level and also at an individual entity level, says Rennison.

The end goal for using AI in this way is the hope that it can help regulators spot incidents like the collapse of Lehman Brothers or Silicon Valley Bank before they happen. "That can enable regulators to start providing warnings rather than just being reactive," he says. AI is also giving regulators more confidence to analyse larger data sets, with financial institutions expected to supply even more detailed reporting information to support that deeper analysis. AI will also help compliance teams better analyse trading data to bolster efficiency and develop a complete understanding of their risk exposures.

For more information, visit deltaconx/report2023

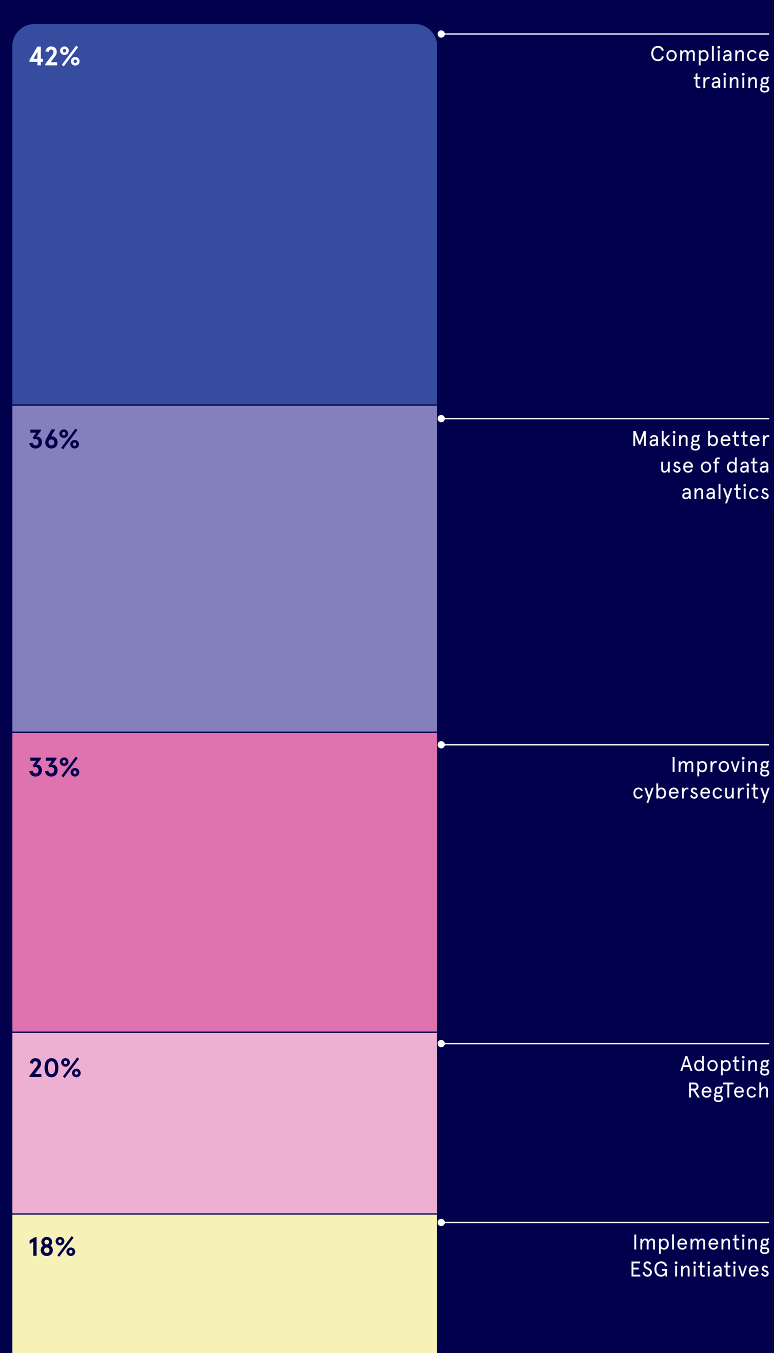
deltaconX
unifying regulatory compliance

THE STATE OF KYC IN 2023

Know Your Customer processes have been a mainstay of the compliance function for 20 years or more, serving as the first line of defence in safeguarding businesses from money-laundering and the various other financial, security and reputational threats out there. But with greater geopolitical uncertainty, a rising tide of cyber threats and tighter budgets all complicating the picture, where do KYC teams stand?

STAYING UP TO DATE DOMINATES, PUSHING ESG DOWN THE AGENDA

Percentage of compliance professionals prioritising the following in 2023, worldwide and cross-industry



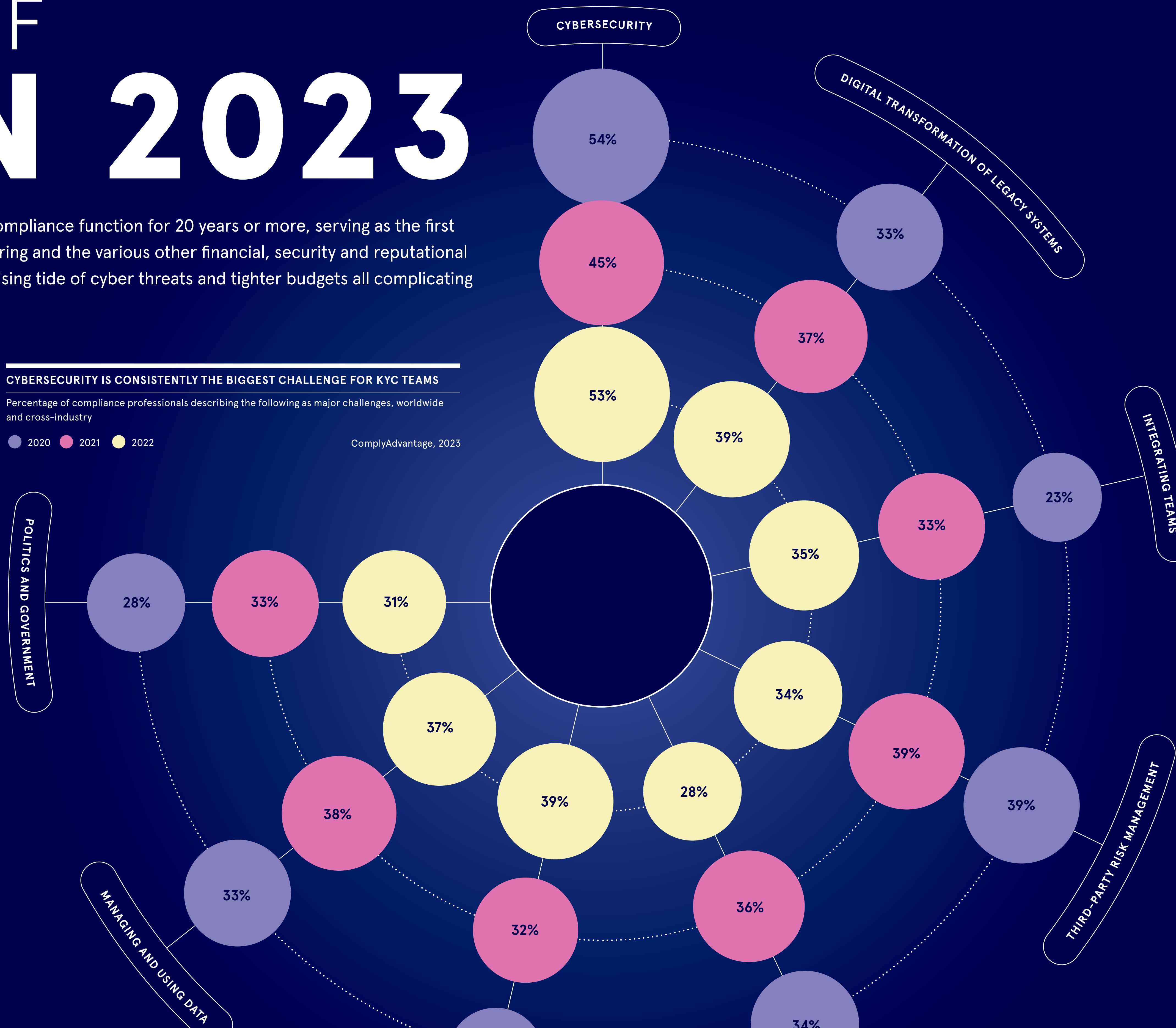
NorthRow, 2023

CYBERSECURITY IS CONSISTENTLY THE BIGGEST CHALLENGE FOR KYC TEAMS

Percentage of compliance professionals describing the following as major challenges, worldwide and cross-industry

2020 2021 2022

ComplyAdvantage, 2023



45%

of compliance teams would like to automate data and document collection for KYC

Fenergo, 2022

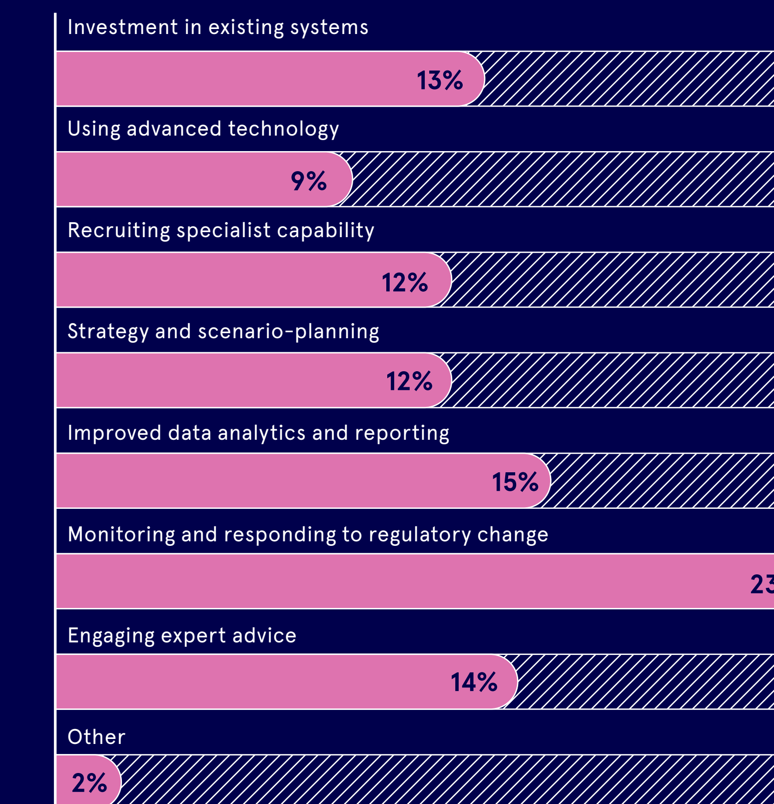
1%

of firms still do all their KYC checks manually

Fenergo, 2022

FEWER THAN ONE IN TEN COMPLIANCE TEAMS EXPECTS TO ROLL OUT NEW TECH

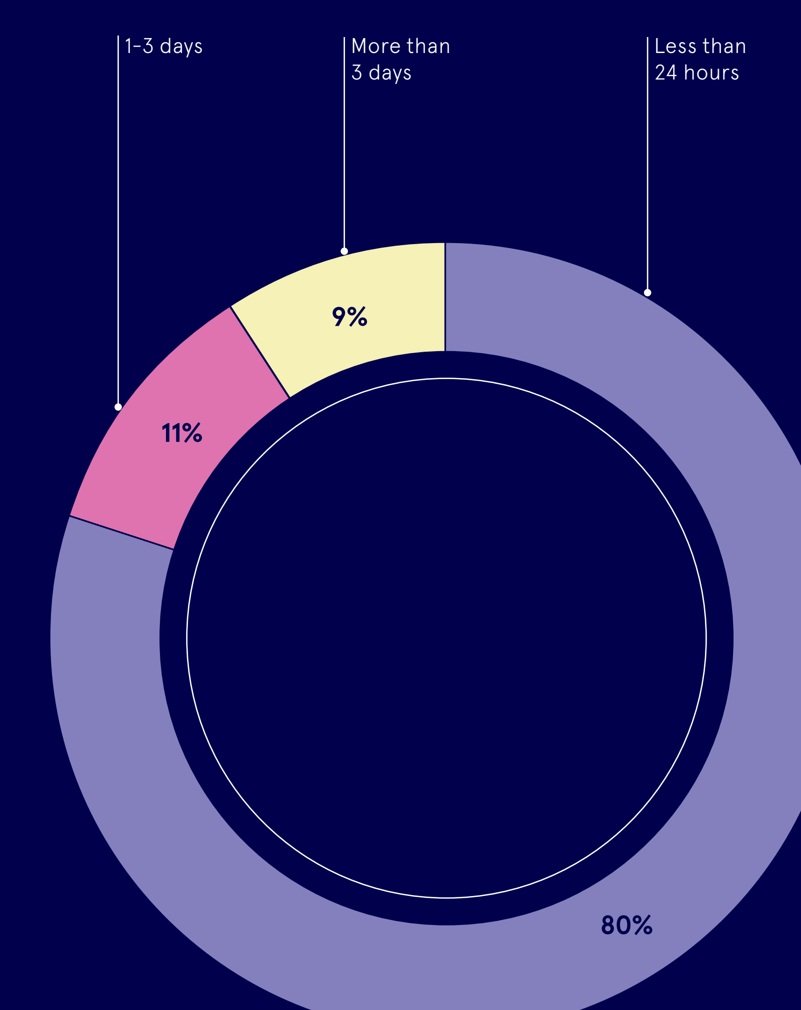
Share of compliance professionals worldwide expecting to implement the following solutions in the near term



Deloitte, 2022

A FIFTH OF ALL KYC CHECKS TAKE MORE THAN 24 HOURS

Average time to complete a KYC check, worldwide and cross-industry



NorthRow, 2023

OPERATIONS

The art of doing more with less

Regulations are changing at record pace and budgets are tighter than ever. To cope, compliance teams will need a new mindset, new skills and new technology

Sally Percy

Keeping up with today's rapidly changing regulatory landscape is a task of some magnitude. Nobody wants to drop the ball, and that puts the onus firmly on compliance teams to ensure their companies don't fall foul of punishing fines or suffer significant reputational damage.

It's a task made more complex by the sheer breadth of activity in the regulatory space. For instance, the recent proliferation of data privacy laws globally has created large volumes of work for compliance teams. At the same time, they have had to navigate a tighter sanctions regime due to the Ukraine war, while also responding to the rise of sustainability-related regulations. This is in addition to monitoring a stream of other regulations specific to the countries where they operate, as well as to their individual industries and sectors.

But while the remit of compliance teams continues to expand, their budgets and resources are not keeping pace. A recent survey by Thomson Reuters Regulatory Intelligence of more than 350 compliance leaders in financial services identified their greatest challenges in 2023 as being the volume and the implementation of regulatory change, followed by the pressure to balance budgets and resources, and retaining skilled personnel.

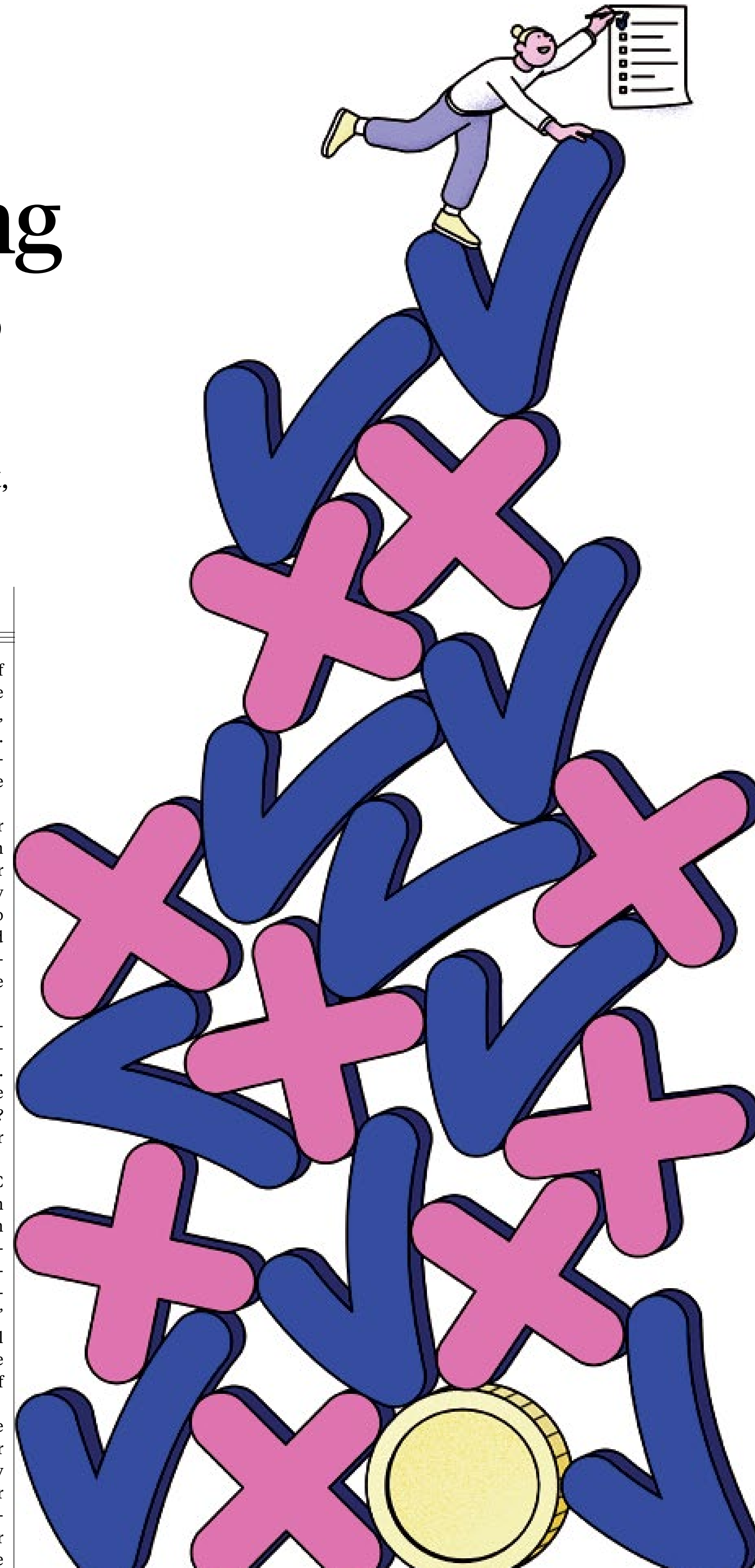
Nearly three-quarters (73%) of respondents to the survey expected an increase in regulatory activity over the next year. Yet 62% of respondents expected the size of their compliance team to stay the same over the coming 12 months, and 5% believed it would reduce. What's more, nearly half (45%) expected their budget to remain the same as today or to shrink.

"The constraints are tight for every company," acknowledges Tom Cowles, chief compliance officer for US-based cloud storage company Box. "In today's economy, we have to optimise our business spend and manage higher interest rates and labour costs. Fundamentally, we have to do more with less."

What this requires in practice, according to Cowles, is ruthless prioritisation of what seems important. "We ask, where can we make the most impact from our investments? For us, it's spending time on our riskiest areas."

Kate Armitage, EMEA and APAC compliance director at OneStream Software, agrees that prioritisation is fundamental to the effective functioning of a robust compliance function. "There's always a lofty ambition to do everything straight away," she says. "But we don't want to boil the ocean. So, we plan, we delegate and we use our team to the best of their abilities."

Armitage stresses that compliance functions must be "ever prepared for change". Her team does this by watching webinars, signing up for data feeds and reports, and attending events. "You learn to keep your eyes and ears to the ground and be aware of what's going on," she says.



If they are to operate effectively with lean resources, it is critical that compliance functions are staffed by the right people, who have the right skills and the right mindsets.

"Compliance is often viewed as a cost centre, the voice of 'no', and the stopper to everything the business wants to do," says Hilary Wandall, chief ethics and compliance officer at business data provider Dun & Bradstreet. "But if it is perceived that way, people will try to avoid it as much as possible and it won't be able to attract talented professionals who like to drive change."

She argues that the compliance function must support the business to grow sustainably. "I talk about compliance as a function that builds trust, if it's done well," she says.

The Thomson Reuters research highlights that communication, critical thinking and internal influence are among the most important skills required by today's compliance professionals, alongside attention to detail, integrity and subject-matter expertise.

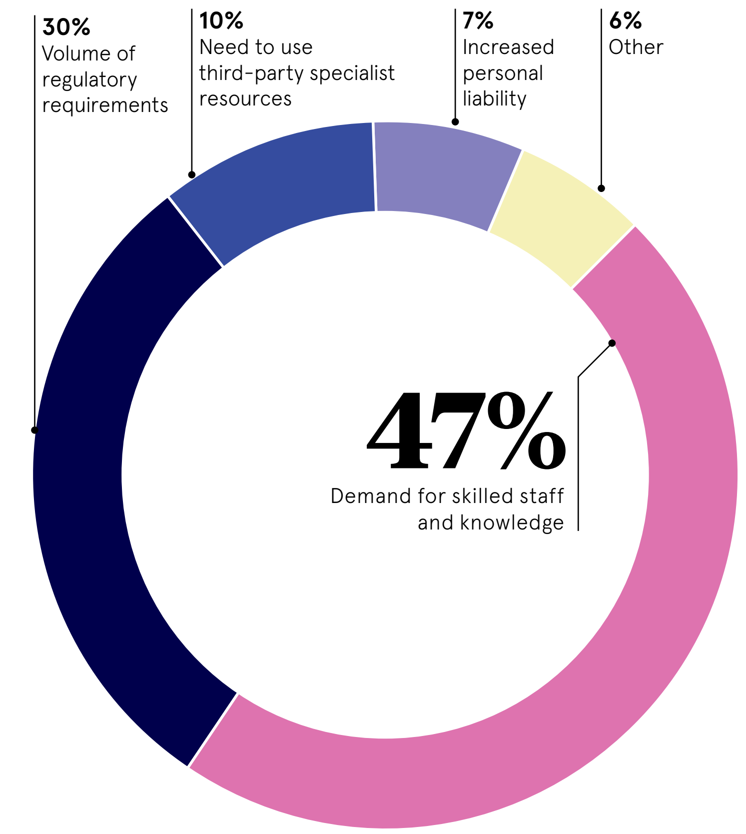
Linda Gibson is head of regulatory change for EMEA at BNY Mellon Pershing, which provides clearing, custody, settlement and dealing services to wealth management clients and institutional broker dealers. She advises compliance functions to attract staff with a commercial focus, who can see the bigger picture. Compliance professionals must embrace the "thoughtful" approach needed to implement 'principles-based' regulations such as the Financial Conduct Authority's consumer duty, she observes.

Compliance teams are overcoming their budgetary and skills constraints by collaborating more effectively with their colleagues in risk and governance. If, for instance, a compliance monitoring team plans to test an area of the business, they could inform their colleagues in risk and governance with a view to sharing the scope.

> For low-risk use cases, where the consequence of failure is low, can we use AI to do 100% of that work? Probably

FOR COMPLIANCE TEAMS, COST PRESSURES ARE MOUNTING ON MULTIPLE FRONTS

Reasons why compliance professionals in global financial services expect the cost of senior compliance staff to increase



Thomson Reuters Regulatory Intelligence, 2022

"Instead of three teams looking at the same area within a year, there would be a coordinated effort," explains Gibson. "That makes for better efficiency for the risk functions and for the affected area of the business, which is not potentially interrupted three times."

Of course, the goalposts for compliance frequently move. This year has brought an explosion of interest in generative AI technologies, combined with growing concerns that these technologies represent an existential threat to society. With policymakers now taking a keen interest in AI, companies should expect to have to comply with some significant AI regulation in future. This will inevitably affect the skills that their compliance teams will need.

"Compliance experts need to know exactly how regulation will affect all areas of the business," says Wandall. "So, compliance professionals will need to understand AI, generative AI and how prompt engineering works, and what the risks are if it all goes wrong."

To boost their efficiency, then, compliance professionals will also need to make better and wiser use of AI, the cloud and other technologies in their own work. This includes automating processes – as far as they can. According to research by IT consultancy Accenture, 93% of compliance professionals believe that new technologies will make compliance easier by automating human tasks, removing human errors and improving the effectiveness and efficiency of the process.

Cowles reveals that Box is looking at how it can use its own AI tool to summarise the system and organisation control reports of its third-party vendors. Nevertheless, he's conscious that there's a "spectrum of risk" associated with AI, which is why the business is still trying to establish the extent to which it's appropriate to use the technology.

"For our highest-risk use cases, we can use AI to do the work a lot quicker," he says, "but we do still need to double-check. But for low-risk use cases, where the consequence of failure is low, can we use AI to do 100% of that work? Probably. But we're still trying to find the line in the sand."

What, then, does the compliance team of the future look like?

In terms of size, it's unlikely to be much larger than it is today given the expectation that it will exploit new technological tools. The cost constraints on companies mean that it is unlikely to benefit from a much bigger budget, either – at least in the short term.

Nevertheless, it will demand even deeper levels of subject-matter expertise, which will suit ambitious compliance professionals who are looking to upskill and enhance their standing internally.

"The expertise of the individuals in the compliance department will need to be better," comments Martin Hartley, group chief commercial officer at consultancy Emagine. "Because they will be the ones who are focused on the strategy and the decision-making. The personal touch will still be there, but the legwork can be done by machine learning and AI."

Gibson thinks that compliance functions will continue to be lean, but will be more integrated with the business. "It's good news for people who are looking to join the compliance industry," he says, "because ultimately they will have an even more varied and satisfying job."

Commercial feature

Entity portfolio management made simple

Mercator's knowledge and focus on entity portfolio management services, in tandem with its technology solution, helps global companies navigate an increasingly complex regulatory environment

The last few years have not been easy for business leaders. The industries they work in have been significantly impacted by a myriad of risks and threats. As the consequences of the pandemic and Brexit continue to unravel, global businesses have been further buffeted by a war on Europe's borders. This perfect storm of challenges has created a global cost of living crunch, an energy security crisis and supply chain shortages. In an era of uncertainty, where nothing is what it was, large-scale regulatory changes are emerging across the entire financial services sector.

In this challenging environment, how do general counsels, company secretaries and c-suite managers – who are responsible for managing hundreds, if not more, companies across dozens of countries – ensure healthy governance, transparency and accountability across their global portfolio of entities? How do they avoid fines and prevent reputational risk by filing correctly while meeting deadlines?

It's a conundrum that the Citco group of companies (Citco), experts in independent fund administration for the alternative investment industry, wrestled with for some time before coming up with a solution. Led by Kariem Abdellatif and building on the specialised servicing platform that it developed in the late 2000s, in 2021, Citco created Mercator by Citco, a centralised platform that provides clients with efficient, effective, and consistent Entity Portfolio Management services (EPM).

"What separates Mercator from other platforms," says Abdellatif, "is our people. Spanning 180 different jurisdictions, Mercator pools its specialist team's vast accumulated knowledge of complex regulatory frameworks in each territory into a knowledge bank. This pool of knowledge, delivered through our proprietary technology platform, Entica, provides our clients with unrivalled and unparalleled visibility 24/7, 365 days a year."

Whenever an individual corporate maintenance-related regulation changes, Mercator registers and vets it. Subsequently, clients receive a notification via the Entica platform, which Abdellatif explains "is a custom-designed single pane of glass that gives clients total control over their global entity workflows."

Entica, says Abdellatif, "instantly notifies the company secretaries and general counsels whose businesses are likely to be directly affected by the regulatory change, providing full transparency on fundamental regulatory adjustments to the right people in the right place at the right time... In this sense, Entica is very much a vector for knowledge delivery."

> The data-centric platform enables businesses to gain a fully accurate and truly-objective picture of the landscape

Beyond enhanced visibility and predictability, the system also delivers cost-efficiency benefits. Says Abdellatif: "Due to significant variations between clients, it is very difficult to provide one single figure for cost savings. However, we have seen instances where clients achieved between 30 to 35% in savings by using Mercator's offering. That said, the vast majority are primarily interested in the robustness of the framework, avoiding fines and mitigating risk, which of course, are also costs."

In terms of efficiency, anecdotally at least, "Entica is also adding great value", says Abdellatif. "As part of a continuous improvement drive, we are constantly talking to our clients. Many organisations tell us that Entica is so deeply woven within the fabric of their businesses that it has become the metaphorical 'water cooler' where company secretaries, accounting departments, tax divisions, and auditors gather and start to communicate."

The data-centric platform generates unique perspectives, which enables businesses "to gain a fully accurate and truly-objective picture of the landscape".

Abdellatif, who has accrued over three decades of experience in the international corporate servicing sector, explains: "We aggregate a lot of data on our system, which means it can be interrogated to discern different practices. Counter-intuitively, our 2023 UK EPM special report revealed that despite the cost-of-living crisis, high inflation and interest rates, the UK is actually 36% cheaper and 40% faster than the combined average of 180 jurisdictions worldwide for incorporating and managing multinational legal entities. This really highlights the power of data to bring to the fore patterns and trends that we wouldn't have been previously able to identify."

With more and more companies turning to EPM specialists, he hopes that EPM will be recognised as a discipline in its own right. As for Mercator, Abdellatif says that "it's looking with considerable interest to the potential of artificial intelligence".

"In the future, AI may well prove to be a powerful tool that will augment the stellar insights that our staff, our most precious resource, provide to our clients," he concludes.

That is no doubt a sentiment that Gerardus Mercator, the pioneering Flemish cartographer after which the business is named, would have shared.

Find out more about Mercator's services and technology at mercator.net

MERCATOR® By CITCO

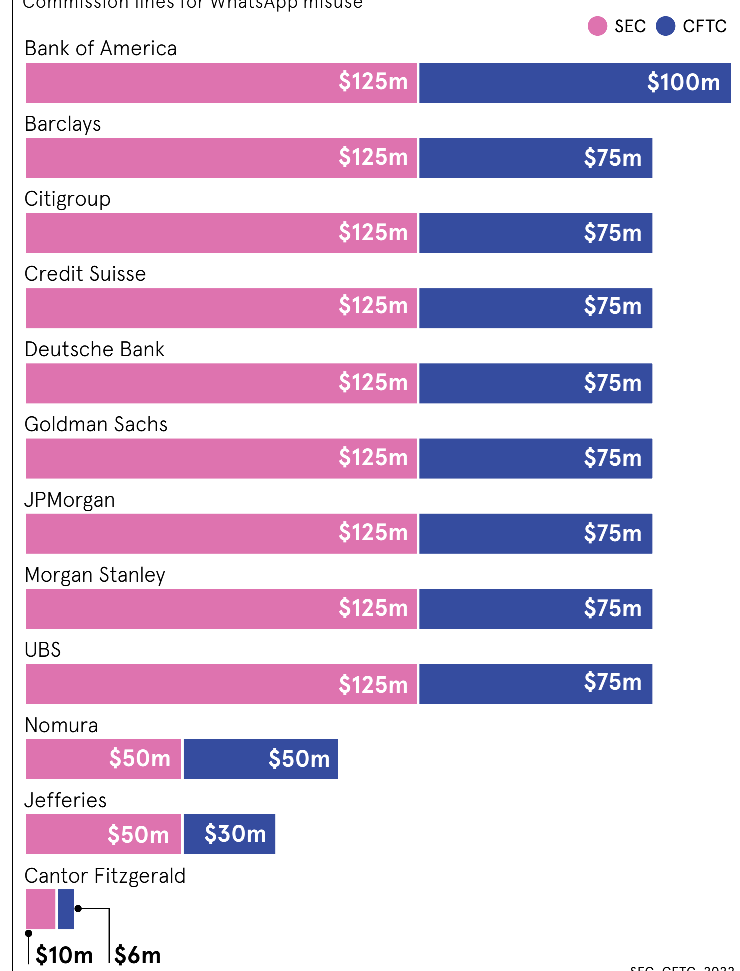
COMMUNICATIONS

Nixed messages

FreshSplash via iStock

SOME BIG-NAME US BANKS HAVE BEEN HIT WITH SOME BIG FINES

Securities and Exchange Commission and Commodity Futures Trading Commission fines for WhatsApp misuse



SEC, CFTC, 2022

Messaging apps like WhatsApp can create major headaches for businesses if employees are mixing personal and professional communications with clients, raising data protection issues and the threat of regulatory fines

Ben Edwards

WhatsApp may be a convenient way for businesses to keep in touch with clients, but it has proven costly for some of the world's biggest financial institutions. Around a dozen banking giants, including JPMorgan and Goldman Sachs, were hit with fines totalling more than $2bn (£1.6bn) last year for failing to monitor messages sent via unauthorised apps such as WhatsApp.

The episode underscored the risks that businesses face from the explosion in new digital communication channels and the challenges of keeping tabs on what employees are sharing on them.

While the use of unauthorised communications long pre-dated Covid, the pandemic accelerated it as the lines between home and work blurred – something that has persisted as hybrid working policies have become more established.

"The office is a controlled environment, where compliance has oversight," says Damon Batten, a partner at regulatory consultancy Bovill. "But when you're at home, it's easy to just pick up and use your personal device and of course in that environment there isn't any oversight."

That means work and personal communications are also blending. "When you have a relationship with a client, they may also be a friend, or at least a contact in your network. So your communications with them may veer between the professional and the personal, especially if they are taking place on these messaging apps," explains Batten.

Given the more challenging competitive landscape and the pressure on firms to maintain margins, there is also often a willingness to communicate with clients however the client wants, even if that means using unauthorised channels, comments Alex Viall, chief strategy officer at Global Relay.

> If you say that WhatsApp is banned, regulators will apply extra scrutiny because they know it's probably still going on

"People often think that to satisfy the customer – and keep their business – they need to respond on-demand via whatever channel the customer wants to use," says Viall. "Given the proliferation of new channels, this is a complex problem."

While the banking fines were handed out for failing to keep proper records, rather than for any market abuse, there is an elevated risk that if employees communicate with clients via an informal channel they may let slip information that they shouldn't, says Batten. Organisations and individuals may also risk reputational damage if communications sent on such channels are later subject to legal disclosures.

"People need to understand that whatever they send digitally could come back to bite them," says Viall. "So they need to take care that if it appears in a court of law in five years' time, they would be happy to hear a prosecutor read it out."

In addition, organisations need to think about issues of data governance that could arise if employees use unauthorised apps for business communications. "Using an authorised application for work communications allows the business some level of control, such as applying retention periods so that the information isn't held for too long," explains Gayle McFarlane, a partner at Eversheds Sutherland.

This is especially relevant since the introduction of the EU's General Data Protection Regulation and the increase in data subject requests, whereby businesses have a legal obligation to disclose the information they hold on an individual. If employees use unauthorised apps to communicate it can complicate the retrieval of relevant data.

In some cases, employees might be reluctant to disclose messages they shared on social apps because the content could be professionally embarrassing. But if they are tempted to press the delete button, it would have serious consequences. "If they do that, they run the risk of committing a criminal offence under the Data Protection Act, which relates to destroying personal data after a request has been made for its disclosure," says McFarlane.

But it isn't just financial services firms that need to be concerned about employees using unauthorised communications channels.

"Data protection principles and information security principles apply to any business, in any industry," explains Frank Schemmel, senior director of privacy and compliance at DataGuard. "The risk is that if you mix private and business data, you can then have uncontrolled storage and publication of confidential information. In that scenario, the misuse of popular messaging services for business communication affects any company."

That's a mantra which also applies to internal messages, not just communications with customers. If employees are chatting with each other on social messaging apps and it occasionally involves business-related matters, those messages would then fall under regulatory scope for data protection rules.

"The decision for companies to take is whether they need an institutional record for ephemeral water cooler-type conversations," says McFarlane. "Sometimes you will because you're carrying out regulated business. But at other times there may well be a greater risk in capturing chit-chat than there is in not capturing it."

That means unregulated organisations need to think carefully about their communication policies. For instance, what channels do they want to allow, how long do they want to retain data so they don't keep transient conversations that don't have business relevance but could be misconstrued if caught up in a disclosure process.

Some regulated businesses, such as banks, have simply responded by prohibiting these messaging apps. A study by Global Relay this year found that 59% of compliance teams have banned WhatsApp and other similar applications because of the recent banking fines. Despite that, only 2.6% of respondents said they were confident that banning such apps is an effective solution.

"It's a knee-jerk reaction in response to the regulatory enforcement," says Viall. "If you send the message to everyone that WhatsApp is banned, that is a first step. But you put yourself at considerable risk if that is your only approach. Regulators won't accept that and will apply extra scrutiny because they know it's probably still going on."

Outright bans may also put firms at a competitive disadvantage if their peers have adopted technology to allow employees to use WhatsApp in a compliant way, by filtering out personal messages and keeping a record of the business communications.

"It's important to find a solution to this," says Viall. "This isn't a trend. It's become a part of life."

Commercial feature

How a risk-based approach could cut your compliance costs

Combining a risk-based approach with the benefits of automation could help compliance teams handle the arrival of new rules more effectively

A deluge of new regulations is increasing pressure on global compliance teams. From the European Union's General Data Protection Regulation (GDPR) and Digital Operational Resilience Act (DORA) to the UK's Telecommunications Security Act (TSA), keeping up with the volume and pace of regulatory change has never been tougher. In 2022, there were more than 61,000 regulatory alerts issued globally – equivalent to 234 regulatory updates every day, according to Thomson Reuters.

And the risks of non-compliance are growing. For the most serious GDPR infractions, for example, fines can be as steep as €20m or 4% of annual revenue, whichever is higher. This intensifying regulatory backdrop, coupled with the threat of severe financial penalties, is making it more important than ever for companies to improve the way they manage compliance.

"There's a lot of overlap between these different regulations, but quite often they will go to different parts of the organisation," says Simon Marvell, co-founder and director of Acuity Risk Management. "So they tend to be looked at independently, and that takes an awful lot of effort with an awful lot of duplication."

Many organisations take what Marvell calls a bottom-up view of compliance, where managers or audit teams run down a checklist of controls and requirements and tick yes or no as to whether the control is in place.

"If it's not in place, then they will usually ask: 'What's the potential consequence? How likely is it to happen?' And then they give it a red, amber or green flag based on how concerned they are about it from a risk point of view," says Marvell. "That means every requirement and every regulation is treated in the same way as you go down the checklist, which is pretty inefficient and costly. That approach doesn't work very well because the auditor or person asking those questions often isn't someone who understands risk or can understand what the wider implications of the control failing would be."

61,000
regulatory alerts were issued globally in 2022

That's equivalent to
234
regulatory updates every day

The most serious GDPR infractions can result in fines of up to
€20m

Thomson Reuters, 2023

A more efficient and effective way is to take a top-down, risk-based approach that starts by looking at the objectives that organisations are seeking to achieve, Marvell says. Take an organisation's supply chain, for example. Some new regulations, such as TSA and DORA, expect companies to manage risk across their supply chains. To manage that third-party risk, companies often take a bottom-up approach and send out questionnaires to their suppliers asking them about the policies and controls they have in place.

"Again, it's a checkbox exercise and people can be a little liberal with the truth, so it's a time-consuming process that doesn't really tell us anything about risk at all," says Marvell.

A risk-based approach instead looks at what the material risks are to the business within their supply chain. For instance, if a business objective is to grow market share, that could be threatened if, say, a product design supplier suffered a data breach and the company's intellectual property (IP) was stolen, says Marvell.

"That's the starting point – what is really important to the business, and then narrowing down and focusing on the areas where there could be a material impact. So, if the concern is about IP theft, then that's the risk you need to protect against," he says.

This risk-based approach also helps companies to prioritise when attempting to deal with multiple regulations at the same time, making it easier to develop risk mitigation strategies, says Kerry Chambers, CEO at Acuity Risk Management.

This is where technology and automation can help, by enabling organisations to manage overlapping compliance requirements via a framework which maps the policies and controls that organisations already have in place against the relevant regulations. Done well, that could significantly reduce duplicated effort.

Technology can also allow compliance teams to quantify the potential financial cost of certain risks instead of categorising threats with a vague 'low', 'medium' or 'high' impact assessment.

> Where organisations have complex regulatory compliance requirements… using technology can streamline and automate the risk management process

"When you look at risks such as loss of IP, for example, there are severe financial implications to that," says Marvell. "By using technology to assess that risk and understand the potential financial loss profile, you can then have a discussion with senior leadership about what level of financial risk is tolerable to the organisation. And if you can understand the levels of financial risk, that can help you to make ROI-type (return on investment) decisions about what you're prepared to spend to mitigate those risks."

Given the pace of regulatory change, automation in particular can make it easier for organisations to ensure their compliance efforts are up to date, while also maintaining a catalogue of evolving risks and mitigations. That can drastically reduce manual effort, making compliance teams more efficient.

"Where organisations have complex regulatory compliance requirements – particularly global organisations that have cross-border compliance concerns – using technology can streamline and automate the risk management process," says Chambers. "It also allows organisations to look at risk in real time across their entire business, enabling them to make much more informed business decisions."

Technology can also help when it comes to capturing and storing evidence for auditors and regulators to demonstrate compliance. That's particularly important if there is an adverse event, such as customer data being stolen by hackers. Effective evidence storage can make the difference between a big fine or a lighter sanction.

"Regulators recognise that you can't avoid risk altogether, so you may still have a data breach," says Marvell. "But if you've got evidence that shows you've been diligent and considered this risk and implemented certain processes and controls to manage it, there's a very realistic prospect that there will be no fine or a much smaller fine than otherwise would have been the case."

Companies that are not investing in technology to help them manage regulatory change will ultimately continue to struggle under the weight and pace of new compliance requirements, elevating the risk of non-compliance.

"If you're not using technology, then as an organisation you will have limited efficiency. That will make your decision-making processes slower, and there's increased risk of human error. That will hinder you when it comes to making good decisions for the organisation," says Chambers.

Find out more at https://bit.ly/acuity-stream

ACUITY RISK MANAGEMENT