FINTECH, REGTECH AND THE ROLE OF COMPLIANCE IN 2020

THOMSON REUTERS®

Contents

Executive summary 3

Introduction 5

Budget and skilled resources 7

Increasing role of technology and the role of personal liability 11

Board and compliance involvement 16

Impact on compliance 18

Industry opinion 22

Challenges for firms 26

Cyber risk 29

Closing thoughts 32

Executive summary

The ebb and flow of attitudes on the adoption and use of technology has evolving ramifications for financial services firms and their compliance functions, according to the findings of the Thomson Reuters Regulatory Intelligence's fourth annual survey on fintech, regtech and the role of compliance. This year's survey results represent the views and experiences of almost 400 compliance and risk practitioners worldwide. During the lifetime of the report it has had nearly 2,000 responses and been downloaded nearly 10,000 times by firms, risk and compliance practitioners, regulators, consultancies, law firms and global systemically-important financial institutions (G-SIFIs).

The report also highlights the shifting role of the regulator and concerns about best or better practice approaches to tackle the rise of cyber risk.

The findings have become a trusted source of insight for firms, regulators and their advisers alike. They are intended to help regulated firms with planning, resourcing and direction, and to allow them to benchmark whether their resources, skills, strategy and expectations are in line with those of the wider industry. As with previous reports, regional and G-SIFI results are split out where they highlight any particular trend.

One challenge for firms is the need to acquire the skill sets which are essential if they are to reap the expected benefits of technological solutions. Equally, regulators and policymakers need to have the appropriate up-to-date skillsets to enable consistent oversight of the use of technology in financial services. Firms themselves, and G-SIFIs in particular, have made substantial investments in skills and the upgrading of legacy systems.

Key findings

- The involvement of risk and compliance functions in their firm's approach to fintech, regtech and insurtech continues to evolve. Some 65% of firms reported their risk and compliance function was either fully engaged and consulted or had some involvement (59% in prior year). In the G-SIFI population 69% reported at least some involvement with those reporting their compliance function as being fully engaged and consulted almost doubling from 13% in 2018, to 25% in 2019. There is an even more positive picture presented on increasing board involvement in the firm's approach to fintech, regtech and insurtech. A total of 62% of firms reported their board being fully engaged and consulted or having some involvement, up from 54% in the prior year. For G-SIFIs 85% reported their board being fully engaged and consulted or having some involvement, up from 56% in the prior year. In particular, 37% of G-SIFIs reported their board was fully engaged with and consulted on the firm's approach to fintech, regtech and insurtech, up from 13% in the prior year.
- Opinion on technological innovation and digital disruption has fluctuated in the past couple of years. Overall, the level of positivity about fintech innovation and digital disruption has increased, after a slight dip in 2018. In 2019, 83% of firms have a positive view of fintech innovation (23% extremely positive, 60% mostly positive), compared with 74% in 2018 and 83% in 2017. In the G-SIFI population the positivity rises to 92%. There are regional variations, with the UK and Europe reporting a 97% positive view at one end going down to a 75% positive view in the United States.
- There has been a similar ebb and flow of opinion about regtech innovation and digital disruption although at lower levels. A total of 77% reported either an extremely or mostly positive view, up from 71% in the prior year. For G-SIFIs 81% had a positive view, up from 76% in the prior year.
- G-SIFIs have reported a significant investment in specialist skills for both risk and compliance functions and at board level. Some 21% of G-SIFIs reported they had invested in and/or appointed people with specialist skills to the board to accommodate developments in fintech, insurtech and regtech, up from 2% in the prior year. This means in turn 79% of G-SIFIs have not completed their work in this area, which is potentially disturbing. Similarly, 25% of G-SIFIs have invested in specialist skills for the risk and compliance functions, up from 9% in the prior year. In the wider population 10% reported investing in specialist skills at board level and 16% reported investing in specialist skills for the risk and compliance function. A quarter (26%) reported they have yet to invest in specialist skills for the risk and compliance function, but they know it is needed (32% for board-level specialist skills). Again, these figures suggest 75% of G-SIFIs have not fully upgraded their risk and compliance functions, rising to 84% in the wider population.
- The greatest financial technology challenge firms expect to face in the next 12 months have changed in nature since the previous survey, with the top three challenges cited as keeping up with technological advancements; budgetary limitations, lack of investment and cost; and data security. In prior years, the biggest challenges related to the need to upgrade legacy systems and processes as well as budgetary limitations, the adequacy and availability of skilled resources together with the need for cyber resilience. In terms of the greatest benefits expected to be seen from financial technology in the next 12 months the top three are a strengthening of operational efficiency, improved services for customers and greater business opportunities.

- G-SIFIs are leading the way on the implementation of regtech solutions. Some 14% of G-SIFIs have implemented a regtech solution, up from 9% in the prior year with 75% (52% in the prior year) reporting they have either fully or partially implemented a regtech solution to help manage compliance. In the wider population, 17% reported implementing a regtech solution, up from 8% in the prior year. The 2018 numbers overall showed a profound dip from 2017 when 29% of G-SIFIs and 30% of firms reported implementing a regtech solution, perhaps highlighting that early adoption of regtech solutions was less than smooth.
- Where firms have not yet deployed fintech or regtech solutions various reasons were cited as to what was holding them back. Significantly, one third of firms cited lack of investment; a similar number of firms pointed to a lack of in-house skills and information security/data protection concerns. Some 14% of firms and 12% of G-SIFIs reported they had taken a deliberate strategic decision not to deploy fintech or regtech solutions yet.
- There continues to be substantial variation in the overall budget available for regtech solutions. A total of 38% of firms (31% in prior year) reported that the expected budget would grow in the coming year, however, 31% said they lack a budget for regtech (25% in the prior year). For G-SIFIs 48% expected the budget to grow (36% in prior year), with 12% reporting no budget for regtech solutions (6% in the prior year).

We hope the findings are useful in developing and benchmarking your firm's practices.

Susannah and Ashley

Introduction

> Technological innovation has the power to create new services for consumers but also to reshape financial market structures. [...] The whole value chain is being impacted by fintechs as well as by bigtechs, which are introducing almost every day new ways to pay, to provide credit, to get insurance and, of course, to invest within capital markets. By doing so, they are also modifying the financial ecosystem that we supervise and may contribute to an increase or a shift of risks in the financial system."
>
> **Denis Beau**, first deputy governor of the Bank of France, November 2019

Respondents to the fourth fintech, regtech and the role of compliance survey once again came from the spectrum of financial services firms across all geographies, from G-SIFIs to technology start-ups. G-SIFIs were asked to identify themselves to enable comparison between themselves and other, smaller, firms.

The report provides unparalleled insight into how financial services firms' risk and compliance functions are responding to the digital and technological transformation. Individual fintech, regtech, insurtech and suptech solutions are omitted but rather the main points for firms and their boards and risk and compliance functions to take into account when considering the use of technology-enabled solutions.

Where the appropriate permission was received, quotes (some anonymized) from both respondents and practitioners have been included to highlightspecific issues.

The results of this year's survey show a growing maturity in approach from financial services firms. Some firms are developing technology solutions in their in-house labs, others are buying up fintech and/or regtech start-ups but, despite investment in IT infrastructure and specialist skills, there remains a fair degree of caution about the widespread adoption of technology.

Technology and its associated potential risks have become important topics for regulators, who are considering everything from regtech sandboxes to cyber risk and the financial stability implications of "bigtech" entering the financial services marketplace. Regulators are encouraging the use of technology and see the potential benefits for customers, but they remain concerned about the possible risks and challenges, particularly where they could compromise the required "good customer outcomes". This holds true in the day-to-day use of IT as well as for the adoption of new forms of technology. Firms have suffered headline-making IT incidents and outages leaving customers often unable to access their accounts or at risk of loss when their data has been corrupted or stolen.

Fintech regulatory and policy developments are seeking to balance the possible benefits against the need to protect customers and ensure financial stability. Equally, firms are on notice that while innovation is a good thing it must not be at the expense of the customer.

How can regulators, government or supra-national bodies help more with the development of fintech/regtech?

Source: Thomson Reuters Regulatory Intelligence - Fintech, Regtech and the Role of Compliance 2020, by Susannah Hammond and Ashley Kovas

The top three areas where regulators, government or supra-national bodies (such as the Financial Stability Board) can help more with the development of fintech and regtech were cited as being: clear messaging on regulatory expectations, engaging with the industry and more support for innovation in terms of incentives and encouragement.

A critical element of the clear messaging on regulatory expectations is the need for cross-border consistency of approach. Numerous memoranda of understanding have been signed between regulators, and bodies such as the Global Financial Innovation Network (GFIN) have been created to facilitate the engagement between firms and regulators and create a framework for cooperation between regulators themselves.

The challenges faced by regulators and firms alike are made all the more profound by a dearth of specialist technical skills, particularly those needed to combat cyber-attacks and build cyber resilience. The depth of the issue was shown in an International Monetary Fund survey of 40 developing jurisdictions which revealed that 92.5% face skills shortages in cyber-security regulation and supervision. "Anecdotal evidence points to a similar situation in advanced economies," the IMF said.

> As the pace of technological change increases it requires regulators to adapt to a new landscape and devise new ways of working together. There are still many areas to look at and in many ways our work is just beginning. We expect future challenges to include understanding and working with data privacy and data-sharing requirements across many jurisdictions and regulators."
>
> **Global Financial Innovation Network (GFIN)**, GFIN – One Year On, June 2019

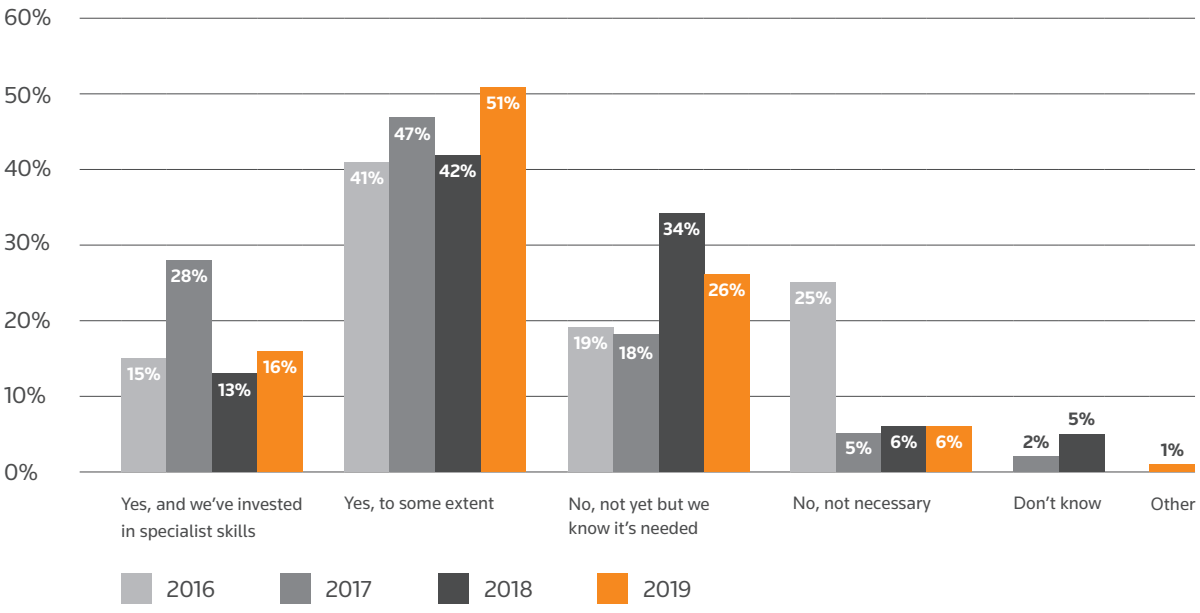
Budget and skilled resources

> ...This lack of readily-available solutions throws up a further challenge — we need to develop the solutions ourselves, in-house. This means we need access to people who can actually build these new tools and make sense of the vast amounts of data that we ingest, people who have certain skills that haven't necessarily been sought by regulators in the past. We can identify the skills we may need, but behaviours and attitudes are equally important."
>
> **Nick Cook**, director of innovation at the UK Financial Conduct Authority, June 2019

Firms need to invest and reinvest in the specialist skills needed to rise to the challenge of developments in fintech, insurtech and regtech innovation and digital disruption. For the risk and compliance function 67% of firms have widened the skill set with 16% choosing to invest in specialist skills. There was some regional variation with 71% of firms in the United States and Canada and 70% of firms in Australasia reporting a widening of skill sets, compared with 59% of firms in the Middle East and 61% of firms in the UK and Europe.

A quarter of firms (26%) reported they had yet to widen the required skill set but knew it was needed. Time is running out for firms if they fail to invest in appropriate skills for their risk and compliance function. Firms will be unable t o get the best out of possible solutions or to avoid the worst of the risks if they lack appropriately skilled resources, preferably in-house.

Have you had to widen the skill set within your risk and compliance functions to accommodate developments in fintech, insurtech and regtech innovation and digital disruption?

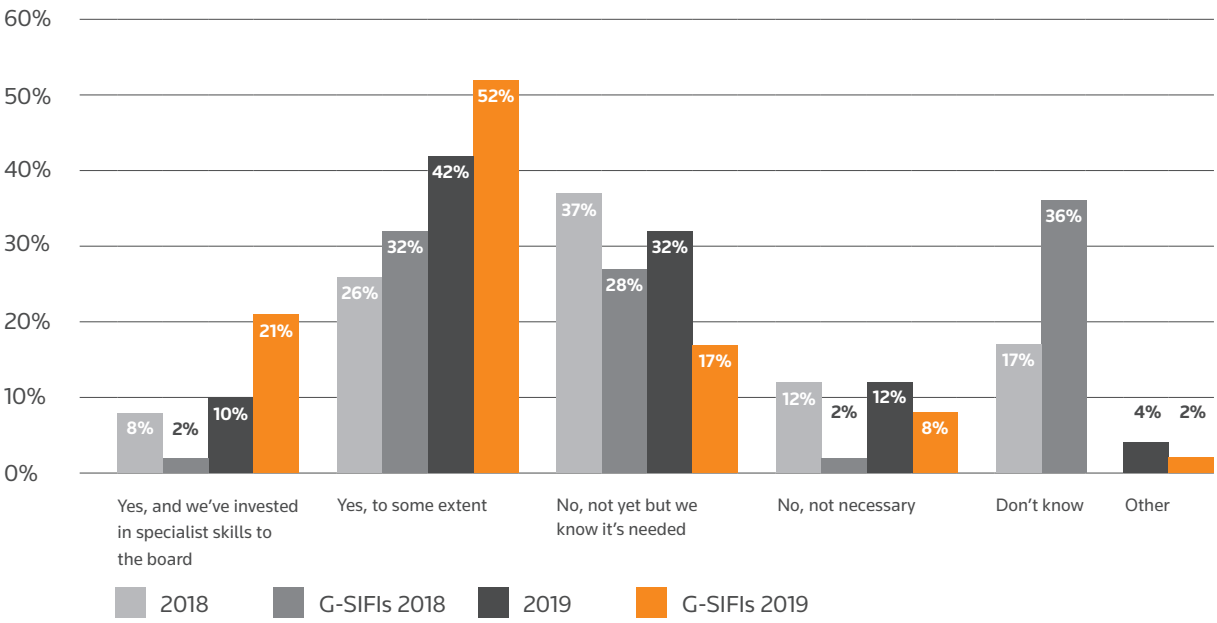


Source: Thomson Reuters Regulatory Intelligence - Fintech, Regtech and the Role of Compliance 2020, by Susannah Hammond and Ashley Kovas

The percentage of G-SIFIs who have specifically invested in and or appointed people with specialist skills at board level has grown significantly from 2% in 2018 to 21% in 2019. At the same time, the number of G-SIFIs which have, to some extent, widened the skill set at board level has also increased (32% in 2018 to 52% in 2019). This is in contrast to the wide population of firms where a third (32%) know that investment in specialist skills is needed but this has not yet happened. The adoption of technology should be considered a firm-wide issue and must not be left to the IT function.

Firms should consider upskilling the board (and other areas of the firm) to be a priority to help to ensure well-informed decisions are made and technology risks are managed. In a world where accountability regimes are proliferating, senior individuals must have the requisite skills to discharge their responsibilities.

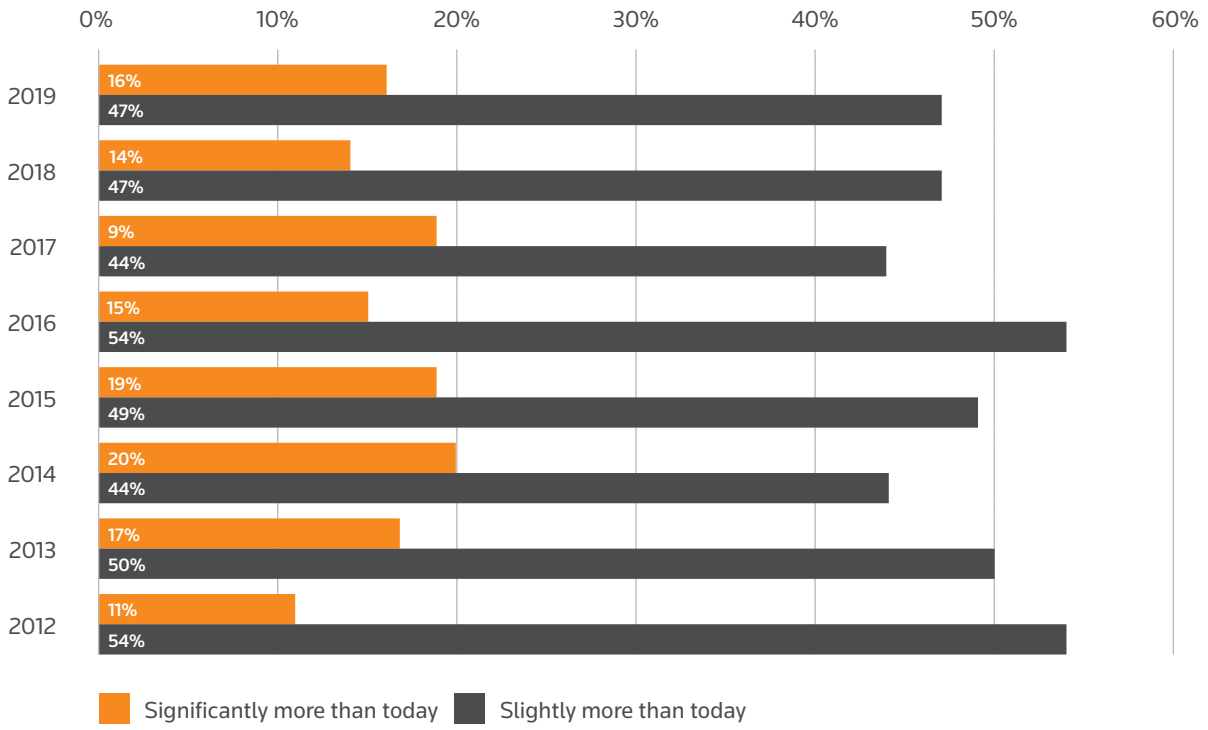
Have you had to widen the skill set at the board level to accommodate developments in fintech, insurtech and regtech innovation and digital disruption?



Source: Thomson Reuters Regulatory Intelligence - Fintech, Regtech and the Role of Compliance 2020, by Susannah Hammond and Ashley Kovas

From a regional perspective, more than half (54%) of firms in the UK and Europe have widened the skill set at board level (10% invested in or appointed specialist skills, 44% widened the skill set to some extent) which may, at least in part, be due to the roll-out of the UK Senior Managers and Certification Regime. Asia is close behind with 53% (10% invested in or appointed specialist skills, 43% widened skill set to some extent) with North America at 43% (11% invested in or appointed specialist skills, 32% widened skill set to some extent).

Over the next 12 months, I expect the total compliance team budget to be...

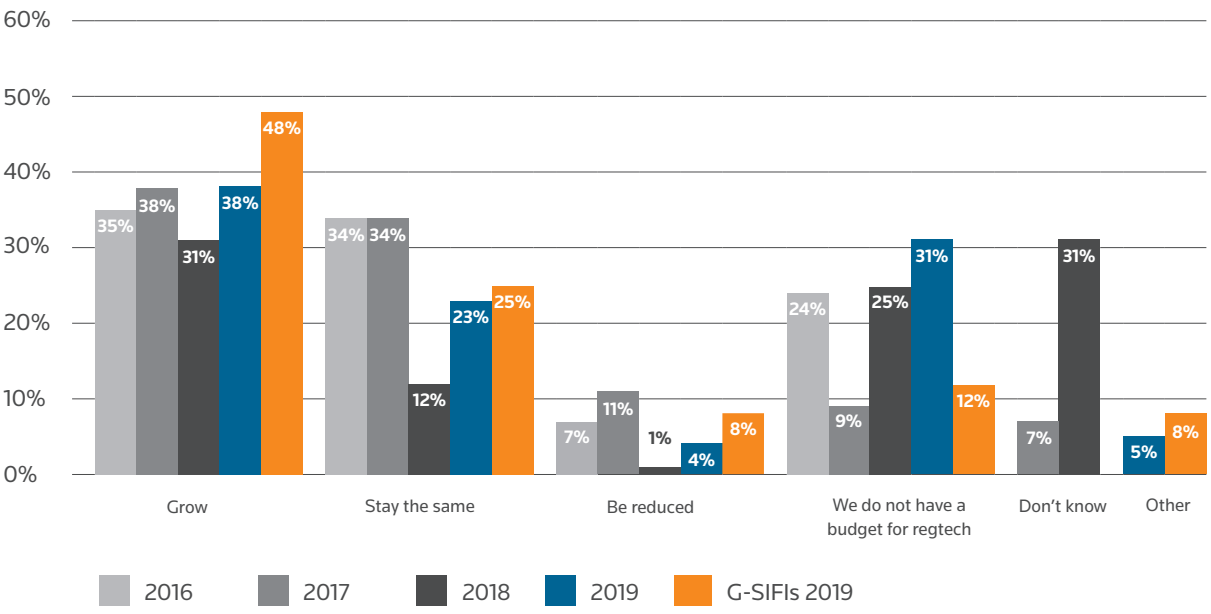


Source: Thomson Reuters Regulatory Intelligence - Cost of Compliance 2019: 10 years of regulatory change, by Stacey English and Susannah Hammond

Thomson Reuters Regulatory Intelligence's 10th annual report on the cost of compliance[1] showed that firms expected budgets to continue to grow with those expecting a significant increase rising from 9% in 2017 to 16% in 2019. It may be that the expected increase in compliance budget is seen to cover the need for regtech solutions as 31% of firms reported they lacked a budget for regtech.

> ...When we look at successful examples of technology adoption, it's not just about state-of-the-art technology. It's about how you manage the change – especially changes to mindsets. It takes time and effort to convince people that a new technology is worth the cost, the effort or the potential risk."
>
> **Eddie Yue**, Chief Executive of the Hong Kong Monetary Authority, November 2019

Your firm's budget for regtech solutions over the next 12 months will:



Source: Thomson Reuters Regulatory Intelligence - Fintech, Regtech and the Role of Compliance 2020, by Susannah Hammond and Ashley Kovas

[1] Thomson Reuters Regulatory Intelligence Cost of Compliance 2019
http://financial-risk-solutions.thomsonreuters.info/cost-of-compliance-2019

More than a third of firms (38%) expect their firm's budget for regtech will grow in the coming year with a further quarter (23%) expecting their budget will remain the same. The budget expectations are higher for G-SIFIs with almost half (48%) expecting their regtech budget to grow and a further quarter (25%) expecting their budget to remain the same. G-SIFIs are investing the most to be able to reap the potential benefits of technology and also have the most to gain, given the likely size and complexity of their risk and compliance responsibilities.

> Regulatory and supervisory technologies are developing in response to various demand and supply drivers. On the demand side, regulatory pressure and budget limitations are pushing the market toward an increased use of automated software to replace human decision-making activities. This trend is reinforced by supply drivers such as increasing computing capacity and improved data architecture. Market participants are increasingly using new automated tools in areas such as fraud detection, regulatory reporting and risk management, while potential applications of new tools for regulators include greater surveillance capacity and improved data collection and management. With these new tools come challenges and risks, notably operational risk. However, with appropriate implementation and safeguards, regtech and suptech may help improve a financial institution's ability to meet regulatory demands in a cost-efficient manner and help regulators to analyse increasingly large and complex datasets."
>
> **European Securities and Markets Authority report on trends, risks and vulnerabilities No 1,** February 2019

Increasing role of technology and the role of personal liability

> Holding individuals and firms to account when IT failures happen is essential, not only to prevent individuals making the same mistakes again, but also to focus the attention of senior management on the risk of incidents and incident management. The regulators must use the enforcement tools at their disposal to hold individuals and firms to account for their role in IT failures and poor operational resilience. The regulatory mechanisms to ensure accountability for failures must have teeth, and equally as importantly, be seen to have teeth."
>
> **UK Treasury Select Committee report: IT Failures in the Financial Services Sector**, October 2019

The fundamental difficulty for regulated firms' IT systems is that failures in those systems will be, with some inevitability, systemic in nature, at least for the firm. A small error in the system may have a disproportionately large effect, particularly if the firm's own assurance processes fail to uncover the error for an unreasonable length of time.

In November 2019, the UK Prudential Regulation Authority (PRA) fined several Citigroup companies a total of £43.9 million for breach of the regulatory reporting requirements. Citigroup had failed on many occasions to submit accurate information in its returns. Its reporting system was inadequate, the regulator's investigation found.

The firm failed to apply appropriate human resource to the problem, particularly after it was uncovered. In such cases, the issue is the firm's relationship with the regulator rather than with customers, markets or competition. Systemic problems in any of these constituencies are likely to yield an enhanced risk of regulatory action.

It is easy to see how an area such as regulatory reporting could fail to come top of a firm's resourcing priorities; for the firm this is a routine back-office matter of little, if any, importance to the "bottom line". The regulator, however, needs accurate information to perform its function in safeguarding the financial system. A failure to provide information of acceptable quality will inevitably lead to sanction, particularly where the firm is substantial in size.

Some might suggest this case is not relevant to IT systems as such because for Citigroup this was a largely manual system, albeit supported by technology. It was therefore subject to human error. All systems are subject to human error, to varying degrees. Even the most sophisticated fintech or regtech solution will fall apart at its weakest link and that will always be the result of human interaction, perhaps in initial coding or in erroneous input.

In October 2019, the UK Treasury Select Committee published a report entitled "IT Failures in the Financial Services Sector" which noted the greater prevalence of IT incidents in financial firms. Not all such incidents have any effect on customers or markets and those that do attract significant media coverage. Firms clearly do not plan their errors, so have no control over the size of detriment an error may cause. Any system incident must therefore be treated as a serious concern because it will be taken as an indicator of the firm's approach to IT generally.

The select committee lamented the absence to date of enforcement against individuals, particularly senior managers, for IT failings. It asked regulators to consider whether changes to "requirements or standards" are needed to hold individuals accountable. If incidents continue to occur, without individual sanction, then the committee and parliament "will have to consider whether the powers it has given to the regulators are fit-for-purpose". This is highly likely to happen in the future.

When asked which part of compliance and regulatory risk management is most likely to be affected by regtech, 14% of firms selected evidencing the discharge of personal liability. This is a significant increase compared with previous years, where personal liability was given less priority than other areas such as onboarding and KYC, financial crime and compliance monitoring. Regionally, Australasia led the way with 22% of firms selecting evidencing the discharge of personal liability most likely to be affected by regtech.

This use of technology is conceptually wider than managing individuals' responsibility for technology. It amounts to the use of technology to support the apportionment of personal responsibility. It will make the actions of individuals transparent. For example, a digital signature by an individual will confirm that person has completed certain acts. A confirmation could amount to an attestation to support a senior manager in meeting their own required standards.

The majority of firms said the applicability of the relevant regulatory regimes in their jurisdiction was clear enough to make decisions about creating regtech and fintech solutions. Some firms, however, see ambiguity in regulatory interpretation and approach, data protection and privacy, cloud systems, know your customer (KYC), customer due diligence (CDD), anti-money laundering (AML), and cryptocurrencies.

> Regulation is not seen as a barrier but some firms stress the need for additional guidance on how to interpret current regulation. Firms do not think regulation is a barrier to [machine learning] deployment. The biggest reported constraints are internal to firms, such as legacy IT systems and data limitations. However, firms stressed that additional guidance around how to interpret current regulation could serve as an enabler for [machine learning] deployment."
>
> **Bank of England**, Machine Learning in UK Financial Services, October 2019

As part of the survey respondents were asked, "Is the applicability of the relevant regulatory regime in your jurisdiction clear enough for firms to make decisions about creating and consuming regtech and fintech solutions?" Here is a selection of their responses:

...I think the picture is quite clear, but some boards of directors of some companies are afraid to venture into some areas of technology and therefore they turn to reject the idea...

...Regulation is changing, and it creates a gap between when the models are developed and when they can be implemented...

...The regime is very clear, it's more about finding the right regtech solutions that are fit-for-purpose today and in the future given the size and scope of obligations and new obligations coming through...

...It's more for the regulatory regime to catch up with regtech and fintech solutions, as some of the solutions we are trying to implement fall within the "grey areas"...

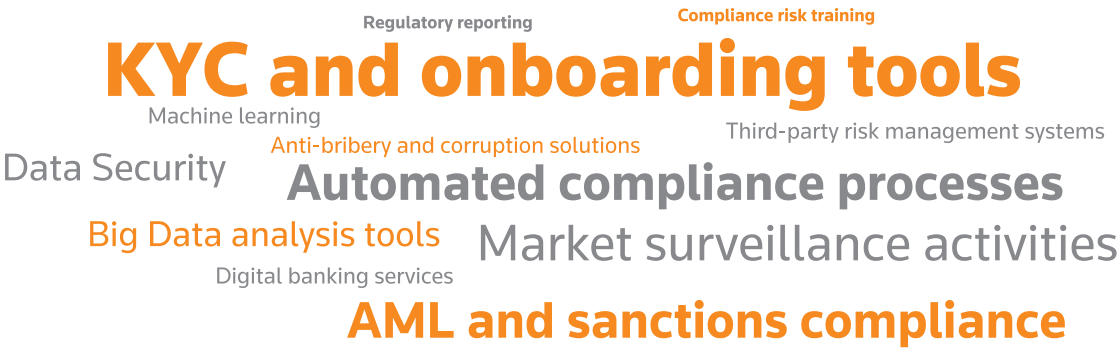
...Regulators struggling to keep up with fintech as financial services regulations was mainly written before the fintech began. Use of Big Data requires changes in laws on fairness of use, privacy, protection and enforcement. Cyber security, cloud services, data residency and privacy overlay AML/KYC obligations. In short, many daunting and intersecting areas of compliance...

...Yes, the regulations are clear enough. Ambiguity exists in the interpretation and execution of the regulation based on legal or business interpretation of specific components of a regulation...

...Regulatory clarity is required particularly for small medium-sized business operations...

...Regulatory interpretation is subjective and needs more interaction and clarification from regulators....

What solution have you introduced/are in the process of introducing and to meet what compliance need?



Source: Thomson Reuters Regulatory Intelligence - Fintech, Regtech and the Role of Compliance 2020, by Susannah Hammond and Ashley Kovas

The top three solutions being used by firms were to meet the following compliance needs:

1. KYC and onboarding tools

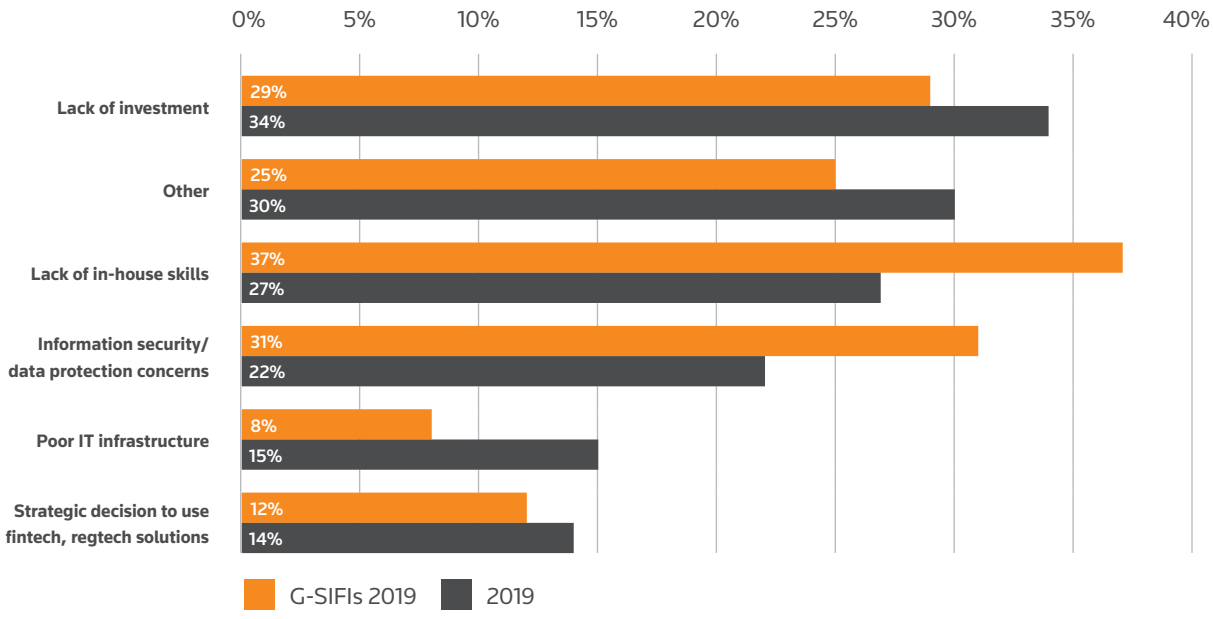
2. AML and sanctions compliance

3. Market surveillance activities (e.g. trade and transaction monitoring)

This year, the survey was extended to ask firms what is holding them back from deploying fintech or regtech solutions. More than a third (34%) of firms said lack of investment, closely followed by lack of in-house skills (27%) and concerns around information security and data protection (22%). For G-SIFIs, 37% said lack of in-house skills was the foremost reason holding them back from deploying fintech or regtech solutions.

Other areas identified as holding firms back from deploying fintech or regtech solutions include alignment to business strategy, lack of executive buy-in from the board, and cost. Those firms where deployment is in progress are investigating solutions as they develop in the industry.

If your firm has not yet deployed fintech or regtech solutions, what is holding you back?



Source: Thomson Reuters Regulatory Intelligence - Fintech, Regtech and the Role of Compliance 2020, by Susannah Hammond and Ashley Kovas

Some 14% of firms and 12% of G-SIFIs have made a deliberate strategic decision not to deploy fintech or regtech solutions. It is likely such a decision will need to be kept under review. To the extent that fintech/regtech fulfils its promise of greater efficiency, firms which fail to embrace it will be at a competitive disadvantage. Caution is a viable approach as the market's hidden hand determines which technology solutions will survive and fail.

Other reasons specified for not yet deploying fintech or regtech solutions...

Lack of skilled resources

Evolving regulatory developments

Deployment in progress

Budgetary limitations and cost

Other technological priorities

Too early to tell

Lack of executive buy-in

Alignment with business strategy

Source: Thomson Reuters Regulatory Intelligence - Fintech, Regtech and the Role of Compliance 2020, by Susannah Hammond and Ashley Kovas

"Given the rapid pace of innovation and the markets supporting it, taking a principles-based approach to regulating digital assets and other fintech products would permit a period of development and observation. After we fully understand the outcomes and potential risks of digital assets, it may be appropriate to adopt more tailored and targeted rules, or a more balanced combination of principles and rules. What we don't want to do is take a heavy hand and snuff out innovation altogether."

Dr Heath P Tarbert, chairman and chief executive of the U.S. Commodity Futures Trading Commission, November 2019

Board and compliance involvement

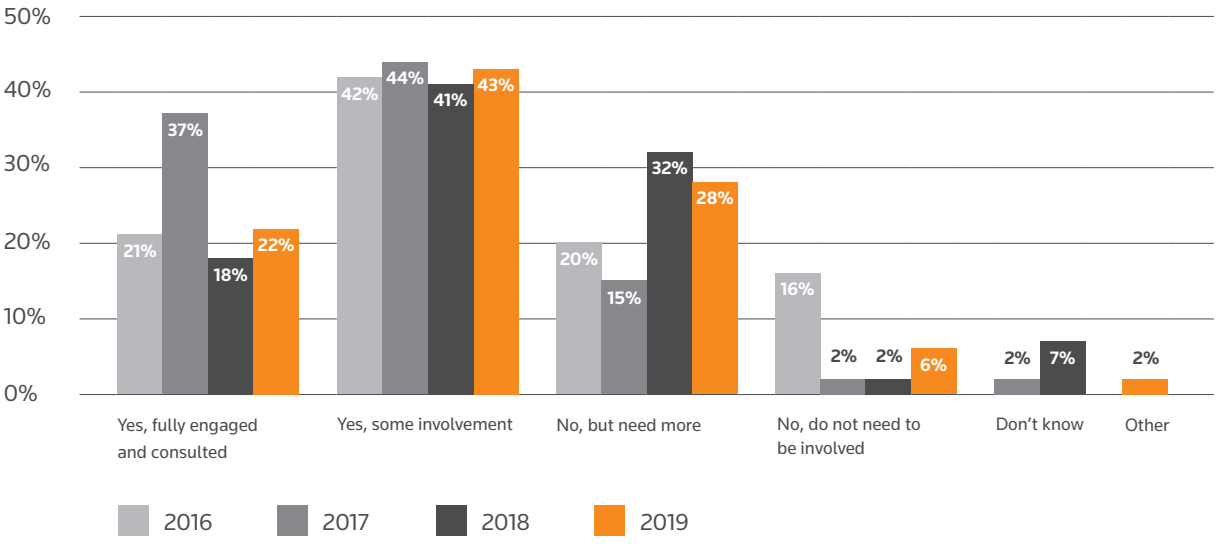
> ...even today, insurers are able to carry out procedures such as risk assessments and claims processing without involving a single human being. However, the management board must not just shift responsibility to machines and algorithms as they can with certain work processes. The ultimate responsibility has to remain with the management board – with people. For this reason, we will not accept models that are presented to us as a black box."
>
> **Felix Hufeld,** president of BaFin, June 2019

As aforementioned, the systemic implications for firms of their use of fintech and regtech mean it is important to consider their use at the strategic level of the firm. "Alignment with business strategy" was one of the most frequent responses given by firms for their delay in implementing technological solutions. This is comforting in showing those firms understand the need to engage with strategy.

It is to be hoped, though, this systemic awareness applies to all fintech or regtech solutions, including those in the back office. They may appear administrative and unrelated to the development of the business. The damage that may flow from a systemic problem even in the back office, however, suggests they may equally have strategic consequences.

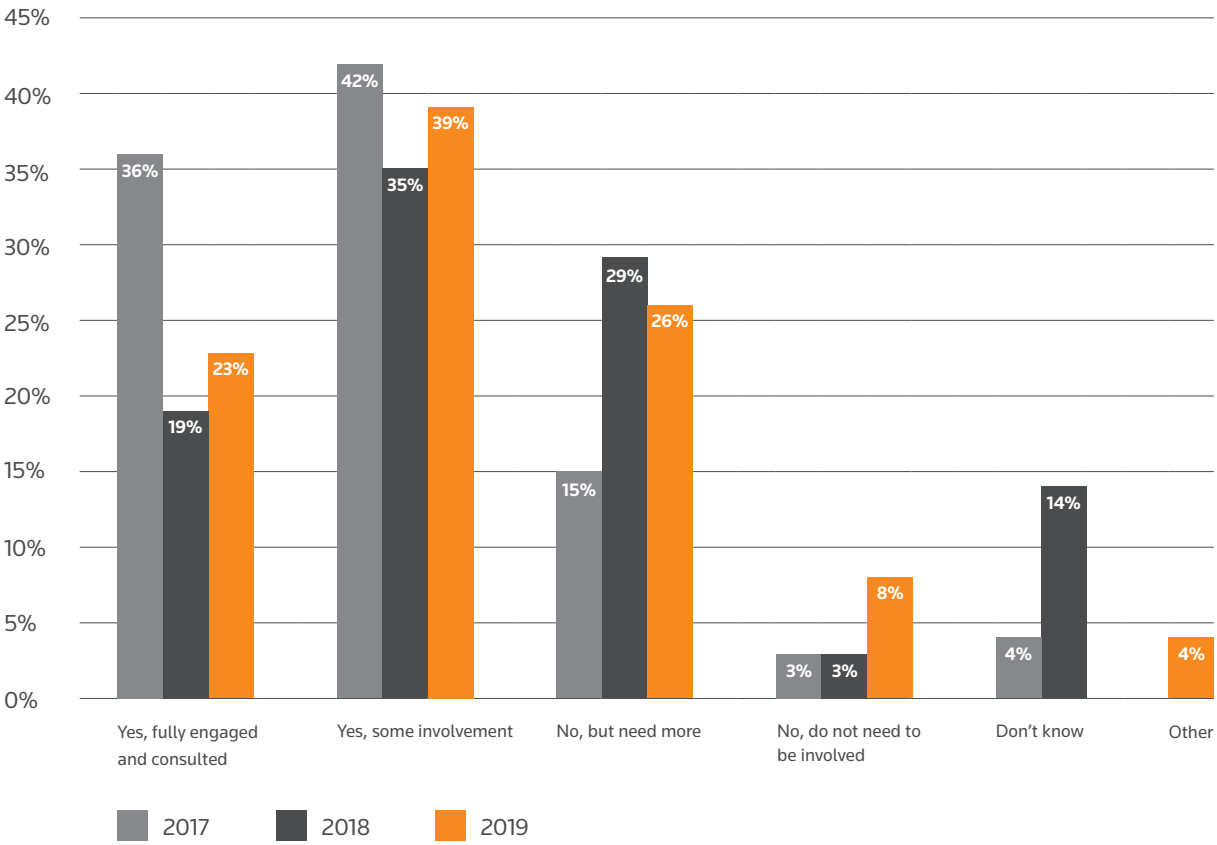
The majority of firms reported their control functions have some involvement in the firm's approach to technology; a significant number believe more involvement is required. Full engagement was at 34% in Africa, compared with 28% in the United States and Canada, 27% in the Middle East and 21% in the UK and Europe. Full engagement in Asia was 17%.

Do the risk and compliance functions have enough involvement with your firm's approach to fintech, regtech and insurtech?



Source: Thomson Reuters Regulatory Intelligence - Fintech, Regtech and the Role of Compliance 2020, by Susannah Hammond and Ashley Kovas

Does your board have enough involvement in your firm's approach to fintech, regtech and insurtech?



Source: Thomson Reuters Regulatory Intelligence - Fintech, Regtech and the Role of Compliance 2020, by Susannah Hammond and Ashley Kovas

Firms also reported their boards have some involvement, but 26% consider more involvement is needed. This figure is consistent worldwide, with between one quarter and one third of firms saying greater involvement is needed.

Regionally, the UK and Europe leads the way with 30% of boards considered fully engaged with fintech and regtech. In the United States and Canada 15% are fully engaged, with 21% in Asia and 26% in the rest of the world.

Impact on compliance

“

ASIC can see a future where artificial intelligence including machine learning, text analytics, voice analytics and other technologies are a seamless component of financial services firms’ business models. A future where firms can record, store and analyse all communications with consumers using these tools. This would provide firms with near to real-time insights, as well as after-the-fact insights on quality and compliance. We believe this can in turn aid strategic business insight analysis and training and development and improve risk and compliance outcomes at scale — with greater efficiency and at a reduced cost.”

James Shipton, chair of the Australian Securities and Investments Commission, September 2019

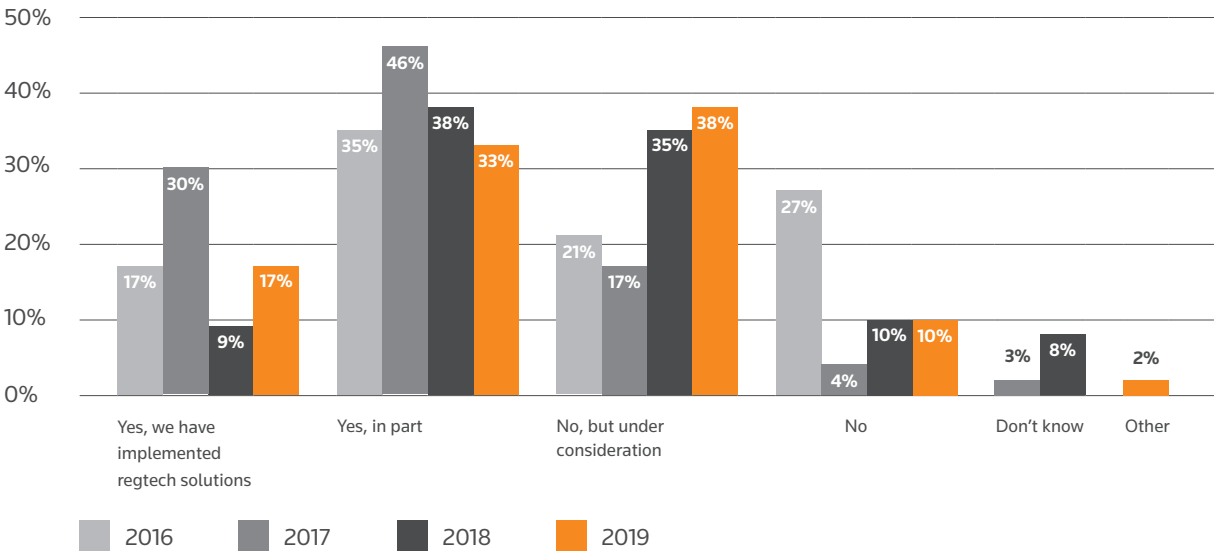
Compliance’s involvement with its firm’s development of regtech solutions will likely involve a number of viewpoints. First, there is a need to ensure the new system is properly coded at the outset. This is made difficult due to the risk of human misunderstanding between the firm and supplier, and also the possibility of error in delivering the agreed system.

Secondly, there will be a need to ensure the system is used as originally intended, bearing in mind it may not be fit for additional purposes that later arise. The changing use of a system requires control.

Third, there is a need to review the integrity of the system on a continuing basis. This should be more than establishing tolerances and looking for exceptional variances. A fundamental error in the system may not exhibit any suspicious variances; all of the output could be tainted by the same error.

Compliance is likely to be the driving force for the firm’s regtech solutions since they will be perceived as of use primarily to compliance itself. It is important for firms not to regard regtech as the junior party to fintech. Although the latter may be seen as more commercially relevant, the consequences of getting regtech wrong will be equally systemic.

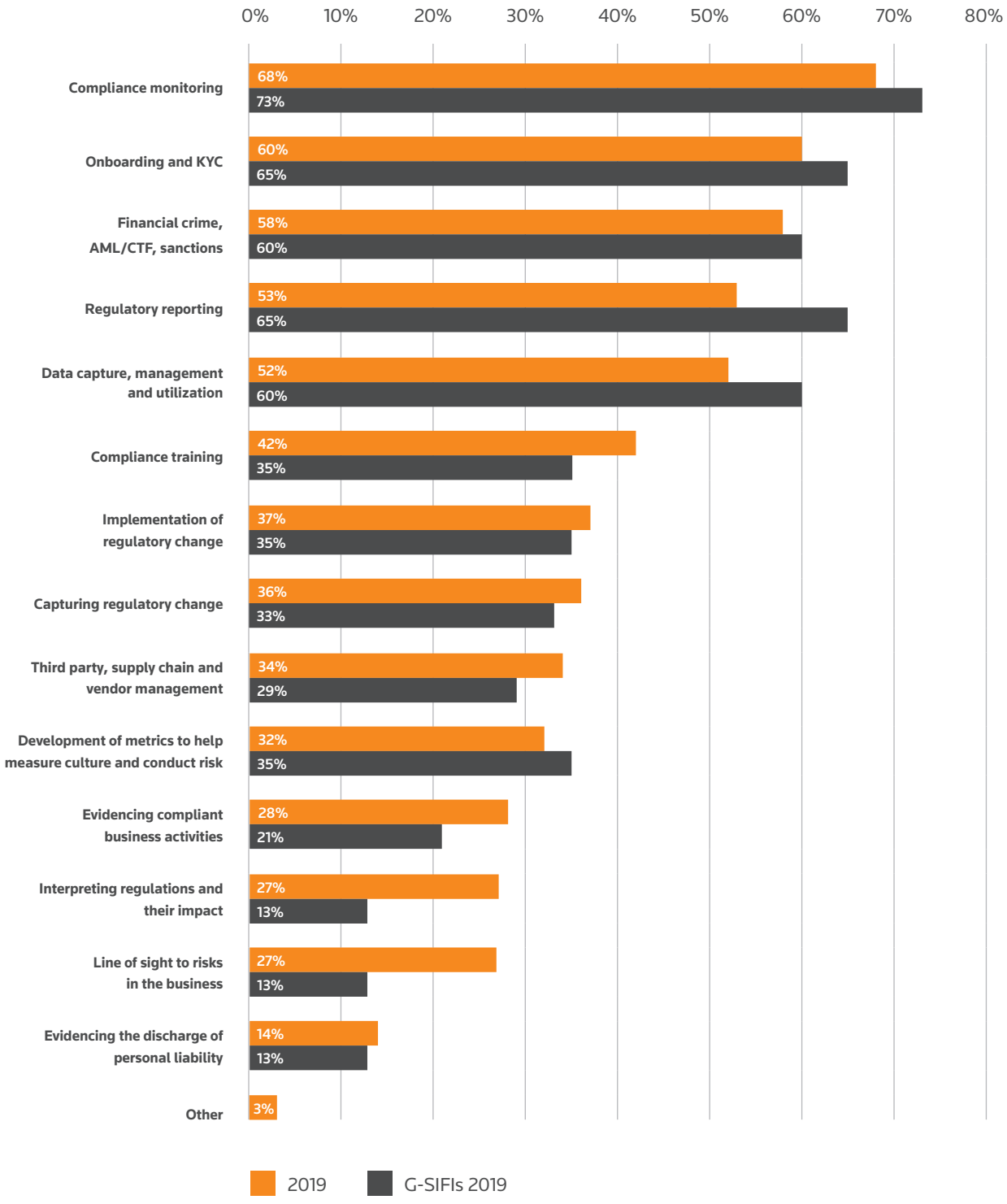
Are regtech solutions impacting how you manage compliance?



Source: Thomson Reuters Regulatory Intelligence - Fintech, Regtech and the Role of Compliance 2020, by Susannah Hammond and Ashley Kovas

A total of 38% of firms have regtech under consideration with 33% saying it is already having an impact on the management of compliance; 17% of firms have already implemented regtech solutions. In Asia, 13% have implemented such solutions, while in Australasia 15% have done so. This increases for the UK and Europe (21%) and the United States and Canada (20%).

Which part of compliance and regulatory risk management is most likely to be impacted by regtech at your firm?



Source: Thomson Reuters Regulatory Intelligence - Fintech, Regtech and the Role of Compliance 2020, by Susannah Hammond and Ashley Kovas

The top three areas within compliance and regulatory risk management most likely to be affected by regtech have remained consistent since 2018. This year, the top three areas were identified as:

1. Compliance monitoring (68%)

2. Onboarding and KYC (60%)

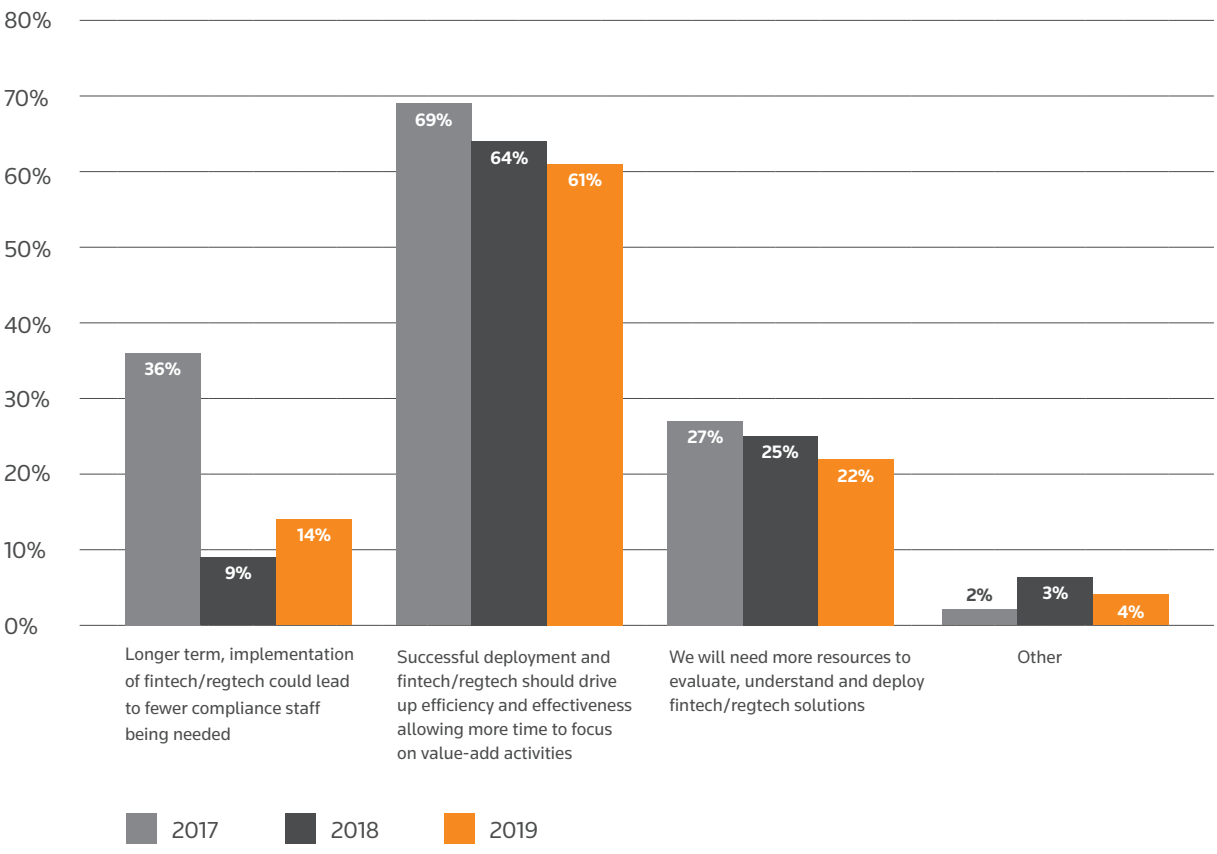
3. Financial crime, AML/CTF, sanctions (58%)

It is perhaps unsurprising the first use of regtech is related to process automation in monitoring, onboarding, KYC and financial crime. This will free up compliance resource for tasks requiring judgement. Admittedly, some firms may have prioritized these process areas to reduce human resource in compliance. Firms nevertheless need to maintain the necessary skills to monitor the new regtech system itself. The employment of fintech is similar to an outsourcing arrangement. Regulators expect firms to maintain sufficient expertise to be able to second-guess outsource providers, and the same applies here. This resource can be maintained within the firm or bought in as and when needed.

The greatest financial technology challenges you expect your firm to face in the next 12 months are...

...In my opinion, the financial technology challenges that my organization will face in the next 12 months are not so much about legacy systems, but rather more on people factors. Essentially, it all starts with the people within the organization who are not susceptible to organizational change and innovation.

What will be the impact of fintech/regtech on your compliance function?



Source: Thomson Reuters Regulatory Intelligence - Fintech, Regtech and the Role of Compliance 2020, by Susannah Hammond and Ashley Kovas

Firms clearly see the efficiency and resourcing implications arising from use of fintech/regtech. It is, however, instructive that only 22% of firms believe more resources are needed to evaluate, understand and deploy fintech/regtech solutions. It is to be hoped this reflects an existing technological literacy in the firms, rather than a misunderstanding of the importance of those tasks. As noted elsewhere, failure to get fintech right first time may have costly consequences for the firm. Even if great effort is expended to get it right first time, there remains a need to ensure continuing adequacy and usage of the technology. Constant review is a necessity.

> Technology enables more transactions, among many more people, sometimes more anonymously. We have seen the emergence of new unregulated spaces like virtual assets. FATF recognises the significant benefits that financial innovation such as blockchain may deliver to the financial system and the broader economy - they have the potential to make certain financial services cheaper and faster, and to make them more accessible to people. However, virtual assets pose serious money-laundering and terrorist-financing risks that criminals and terrorists can exploit - and that they are already exploiting. We have seen cases of money laundering and terrorist financing using virtual assets, as well as attempts to use virtual assets to evade UN sanctions."
>
> **Xiangmin Liu,** president of the Financial Action Task Force, September 2019

In December 2019, the Bank of England, PRA and FCA published co-ordinated consultation papers on new requirements to strengthen operational resilience in the UK financial services sector. The proposals make clear regulators' expectations that firms and financial market infrastructures are expected to take ownership of their operational resilience and that they will need to prioritise plans and investment choices based on their impacts on the public interest. If disruption occurs firms are expected to communicate clearly, for example providing customers with advice about alternative means of accessing the service. Under the proposals, firms and FMIs will be expected to:

- identify their important business services that, if disrupted, could cause harm to consumers or market integrity, threaten the viability of firms or cause instability in the financial system
- set impact tolerances for each important business service, which would quantify the maximum level of disruption they would tolerate
- identify and document the people, processes, technology, facilities and information that support their important business services
- take actions to be able to remain within their impact tolerances through a range of severe but plausible disruption scenarios.

> Operational resilience is not about protecting the reputation of your firms or the reputation of the industry as a whole. It is about preventing operational incidents from impacting consumers, financial markets and UK financial system."
>
> **Megan Butler**, executive director of supervision at the UK Financial Conduct Authority, December 2019

Industry Opinion

Technology-enabled solutions have driven a wave of start-ups pushing the bounds of innovation and using the new capabilities offered by concepts such as artificial intelligence and machine learning. Financial services firms themselves are also developing solutions in-house often in ring-fenced 'labs' where innovations are tested before beginning to be deployed.

In this section a range of views from the industry have been collated to illustrate the multi-faceted approaches taken and varying attitude towards new forms of technology.

The greatest financial technology challenges you expect your firm to face in the next 12 months are...

...Acute shortage of FinTech talent, more regulations, increased collaboration between traditional financial services and fintechs and more cyber-security/data breaches and enforcements...

"As regulation and data outpace compliance, regtech brings welcome structure and precision for focusing and prioritising critical resources. Regtech finds the 'needle in the haystack', providing insight how it got there so compliance can prevent it getting lost again."

Stacey English, chief digital officer, Corlytics

"I worked for 10 years as a compliance officer, and although management would pay for sufficient technology to monitor money laundering and other types of financial crime risk, it was not as useful as it could have been, partly because we were understaffed. Also, we needed more training on how to use the technology better, particularly how to get the most from the tools and link them to those used by other departments."

Former AML compliance officer for a large, global bank, NY office

"Technological advances have great promise for improving the effectiveness and efficiency of compliance functions at global financial institutions. Transactions can be reviewed and filtered by use of artificial intelligence and other technology methods that can assist in the fight against financial crimes, ensuring compliance with the Bank Secrecy Act, anti-money laundering laws, and OFAC sanctions requirements. Financial institutions should consider these advancements, paying particular attention to the reliability of the technologies and methods used, as with any vendor management program."

Maria Vullo, former superintendent of the New York Department of Financial Services and now CEO of Vullo Advisory Services, PLLC

In this section a range of views from the industry have been collated to illustrate the multi-faceted approaches taken and varying attitude towards new forms of technology.

"Regtech is, like any tool, a great support mechanism for the compliance function. But like any tool, it is only as good as the system into which you input it. A system will not by itself solve issues, but it will do a couple of things: it will add welcome automation and objectivity to a process. Computational analysis helps us understand our own data and processes better and allows us to look critically at any process. It is not, however, a means to let the machine take over a function completely. Controls keep all systems in check by providing oversight, and model governance was meant to create the balance in the operational systems by providing quantifiable evidence that a system is working effectively. Also, the staff that are in charge of managing such systems must be equipped for success with adequate training, controls and permissions to manage the systems. Without the oversight and controls, there is not much to stop exploitation, abuse or even cyber influence. Making the program work with the systems is the key to success in balancing technology and operations."

Debra Geister, CEO at Section 2 Financial Intelligence, Minnesota, United States

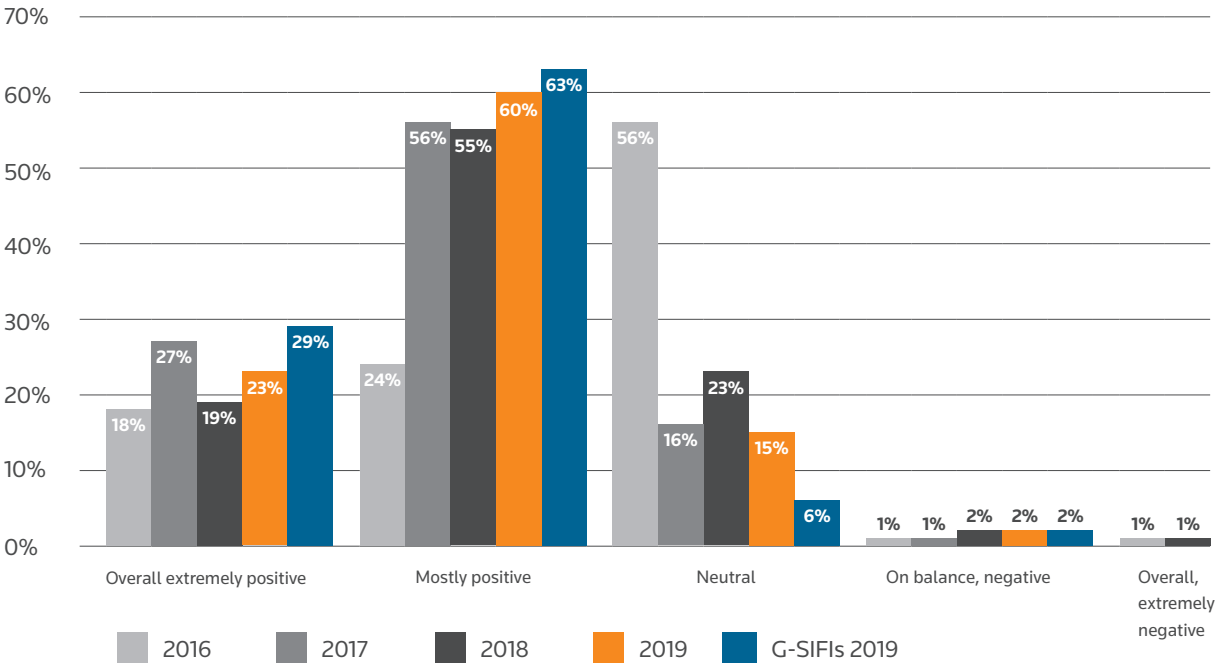
"As outsourced compliance principals, we use our clients' technology. We always try to conform to the culture and systems that our clients use. For smaller firms in particular, I don't think adequate and affordable technologies exist to monitor risk. Although I believe that our clients do a good job monitoring their risk, the majority of it is incredibly time-consuming for their internal staff and for us as outsourced regulatory compliance principals. I find that the technology either isn't cost-effective for the smaller firms, or in many cases does not meet the demands of the client in a holistic way."

Deirdre Patten, compliance principal and founder, Patten Training & Review, Texas, United States

"We use regtech for front-end KYC and customer due diligence screening, mainly. We should be using it for cybersecurity purposes more, but there is still a "it might not happen to us" mentality here. Regtech has made compliance work easier and more effective, but it can be easy to depend too much on it – I think we're not being skeptical enough, sometimes. And it's used best when people know their roles well – who oversees the technology, who tests it, who updates it."

Senior BSA/AML compliance officer at a large, global bank (NY office)

What is your view of fintech (including insurtech) innovation and digital disruption?

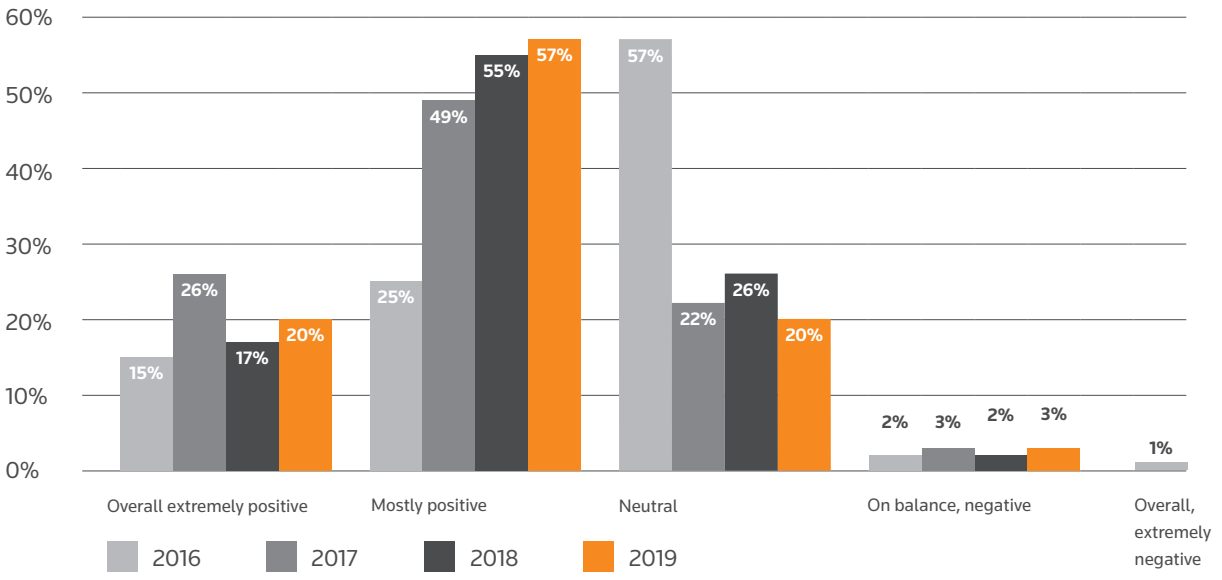


Source: Thomson Reuters Regulatory Intelligence - Fintech, Regtech and the Role of Compliance 2020, by Susannah Hammond and Ashley Kovas

The last three years show a relatively steady view on fintech (including insurtech) innovation and digital disruption with 83% expressing either a mostly or extremely positive view. What is clear is that the neutrality of view on fintech from 2016 is no longer the case, with 56% of respondents reporting a neutral view of fintech in 2016 compared with 15% in 2019.

As with the view on fintech, there has been a relatively steady and overall positive view of regtech innovation and digital disruption. A total of 77% (20% extremely positive, 57% mostly positive) expressed a positive view of regtech and, again, the neutrality reported in 2016 (57%) has reduced by almost two thirds to 20% in 2019.

What is your view of regtech Innovation and digital disruption?



Source: Thomson Reuters Regulatory Intelligence - Fintech, Regtech and the Role of Compliance 2020, by Susannah Hammond and Ashley Kovas

A view from Thomson Reuters Ventures

The regtech industry is maturing and as a result Thomson Reuters Labs is seeing a shift in how regulators, corporations and the start-ups and vendors that serve them are using technology. The goal of regulation has always been to shift human behavior positively. Traditionally this is done by monitoring behavior and retroactively punishing non-compliance, but increased cost pressure and the rapid advancement of technology is helping to prevent things like fraud and money laundering by creating infrastructure that is resilient enough to detect and prevent negative behavior, be it malicious or unintended.

The technologies at play in the regtech industry are transformational, but it is the growing prevalence and intersection of these technologies that are creating new opportunities. By highlighting select examples, we hope to illustrate this ongoing shift from reactive to proactive compliance.

- Identity verification and customer onboarding remains one of the least customer-friendly and most expensive compliance activities that banks, and other professional advisors need to perform. It is still mostly performed in person and require customers and agents to meet in person to authenticate documents and verify a person's identity. The biometrics on modern smartphones however are now capable of running facial recognition models as well as AI that can be trained to verify government documents, all of this is enabled by cloud platforms that aggregate data and makes it available in real time anywhere in the world. Thanks to the intersection of these technologies, identity verification is becoming faster, more effective, less expensive, and improving the overall customer experience.
- Adverse media screening has become essential as an early indicator of involvement with money laundering, drug trafficking, financial fraud, organized crime, terrorism and more, but using human initiated search to monitor the entirety of the media landscape is prohibitively expensive and is therefore traditionally reserved for only the highest risk customers. Automated processes are changing this paradigm. The use of social channels, data mining, sentiment analysis, and the use of techniques like adversarial neural networks to detect deep fakes, all has the potential to lower the cost of comprehensive adverse media screening and improve outcomes.
- Self-sovereign identity, while still several years away from mass adoption, has the power to upend the current model where states and private corporations own and administer an individual's identity. The combination of mobile biometrics and distributed ledger technology will allow individual to control their personal data and share it selectively and for a limited amount of time. These future systems will have a higher degree of trust by design and as such has the potential to further reduce the friction inherent in ID verification and authentication.
- AI driven risk assessment and customer due diligence is becoming more prevalent. The barriers to entry for AI are being lowered continuously as technologies are being developed that will make it easier to adopt and manage AI applications. Technologies like transfer learning, which uses pre-trained models, reduces the reliance on technical expertise, while approaches like top-down artificial intelligence can beat data-hungry approaches by modelling what a human expert would do in the face of high uncertainty and little data. Hardware requirements are also being lowered by software that is capable of running AI models on traditional CPUs instead of specialized GPUs. As the technology matures, we are seeing a democratization of AI and a much broader application in regulatory use-cases.
- Regulators are embracing technology too. Supervisory technology (suptech) is growing as a category as government agencies embrace the use of innovative technology to support their supervisory functions. By digitizing reporting and regulatory processes, regulators can more efficiently and proactively monitor risk and compliance at financial institutions. This creates opportunity for regtech start-ups as well as corporations to more closely align their activities with regulators, further reducing the compliance burden.

The rapid advance of these technologies and industry's increased appetite for "technology first" solutions means the next large regulatory challenge may not be met with a knee-jerk increase in staffing. In fact, we are already seeing this shift; hundreds of new companies have been formed to respond to the GDPR regulation coming out of the EU, all of which promise increased compliance and lowered cost through the application of technology. We expect that any substantially impactful new regulation will see a similar, technology-driven, response from the regtech industry. We also expect to see an acceleration in the use of technologies that not only lowers the cost of compliance through automation, but also moves organizations away from reactive remediation towards proactive prevention.

Thomson Reuters Ventures is a corporate venture capital fund focused on driving innovation in law, tax, compliance, government, and media. It provides the necessary capital and support to help grow start-ups operating at the intersection of commerce and regulation.

QUINTEN FOURIE – director, emerging technology investments

NICK JAREMA – VP strategy, operations & investments

Innovation in financial services has the capacity to bring many benefits for consumers, the economy and society in general. It is essential to the effective functioning of a competitive economy. However, here is where a challenge lies for financial regulators. Innovation is good, but not all innovations are good, and not all good innovations are done well."

Ed Sibley, deputy governor at the Central Bank of Ireland, November 2019

Challenges for firms

> ...the increasing growth of big tech could have a more profound impact on the industrial organisation of financial services. The financial hierarchy could be reversed, with banks relegated from being in the centre of the financial system to a subordinated player to payment services provided by big tech companies."

Pablo Hernández de Cos, chairman of the Basel Committee on Banking Supervision and governor of the Bank of Spain, November 2019

Technological challenges for firms come in all shapes and sizes. There is the potential, marketplace changing, challenge posed by the rise of bigtech. There is also the evolving approach of regulators and the need to invest in specialist skill sets. Lastly, there is the emerging need to keep up with technological advances themselves.

The challenges for firms have moved on. In the first three years of the report the biggest financial technology challenge facing firms was that of the need to upgrade legacy systems and processes. This year the top three challenges are expected to be the need to keep up with technology advancements; perceived budgetary limitations, lack of investment and cost, and then data security.

Basel Committee on Banking Supervision: 10 key implications and considerations on emerging supervisory issues arising from financial technologies and innovation

(1)	The overarching need to ensure safety and soundness and high compliance standards without inhibiting beneficial innovation in the banking sector.	**(6)**	International cooperation between bank supervisors.
(2)	The key risks for banks related to fintech developments, including strategic/profitability risks and operational, cyber and compliance risks.	**(7)**	The need to adapt the supervisory skill set.
(3)	The implications for banks of the use of innovative enabling technologies.	**(8)**	Potential opportunities for supervisors to use innovative technologies ("suptech").
(4)	The implications for banks of the growing use of third parties, via outsourcing and/or partnerships.	**(9)**	The relevance of existing regulatory frameworks for new innovative business models.
(5)	Cross-sectoral cooperation between bank supervisors and other relevant authorities.	**(10)**	Key features of regulatory initiatives set up to facilitate fintech innovation.

Source: Pablo Hernández de Cos, chairman of the Basel Committee on Banking Supervision and governor of the Bank of Spain, November 2019.

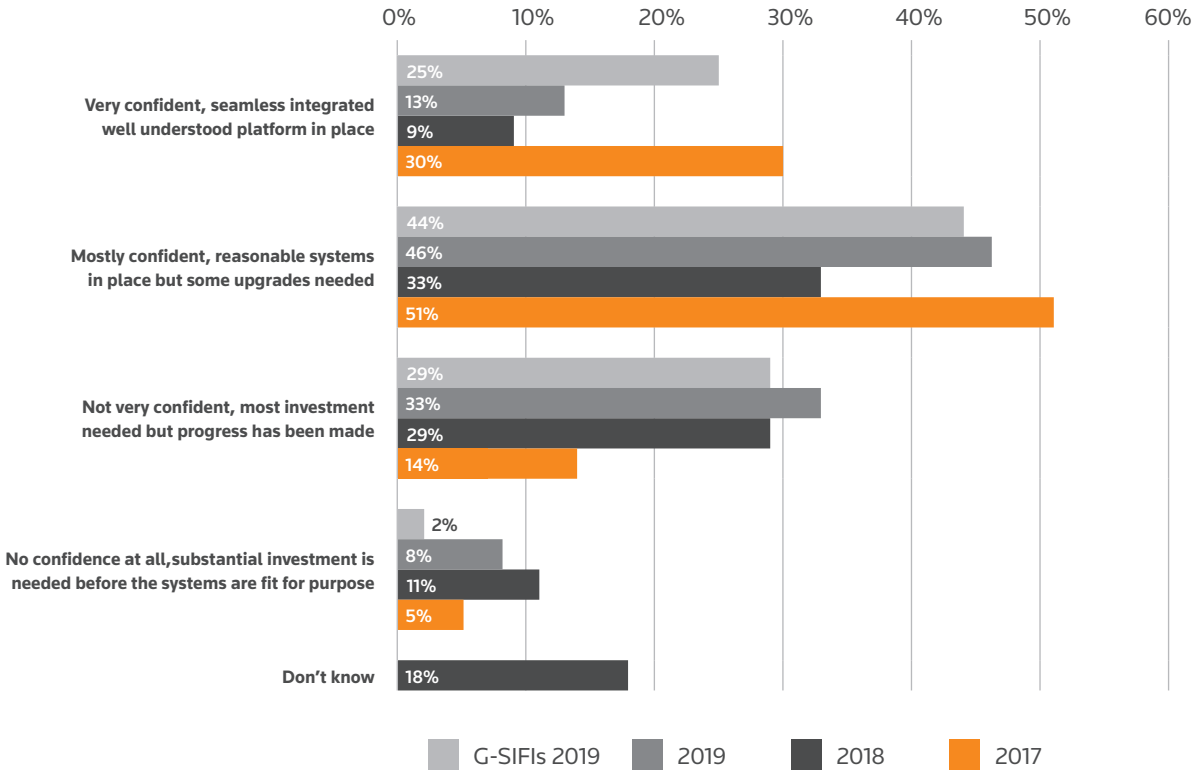
The greatest financial technology challenges you expect your firm to face in the next 12 months are...

Source: Thomson Reuters Regulatory Intelligence - Fintech, Regtech and the Role of Compliance 2020, by Susannah Hammond and Ashley Kovas

The need to upgrade legacy systems and processes has not gone away even if it is now seen to be less of a challenge. More than half of firms (59%) reported they were either very or mostly confident that their IT infrastructure was or would be able to support fintech, regtech and insurtech solutions, up from 42% in the prior year. A third (33%) reported they were far from confident and that more investment was needed, though progress has been made.

Firms choose to face the challenges of financial technology to reap the expected benefits which have themselves moved on. In the prior year, the greatest benefits expected to be seen from financial technology were greater efficiency and accuracy, improvements in compliance monitoring and reporting and better product delivery and customer experience. This year the top three benefits are seen as being strengthened operational efficiency, improved services for customers and greater businesses opportunities.

How confident are you that your IT infrastructure is/will be able to support fintech, regtech and insurtech solution?

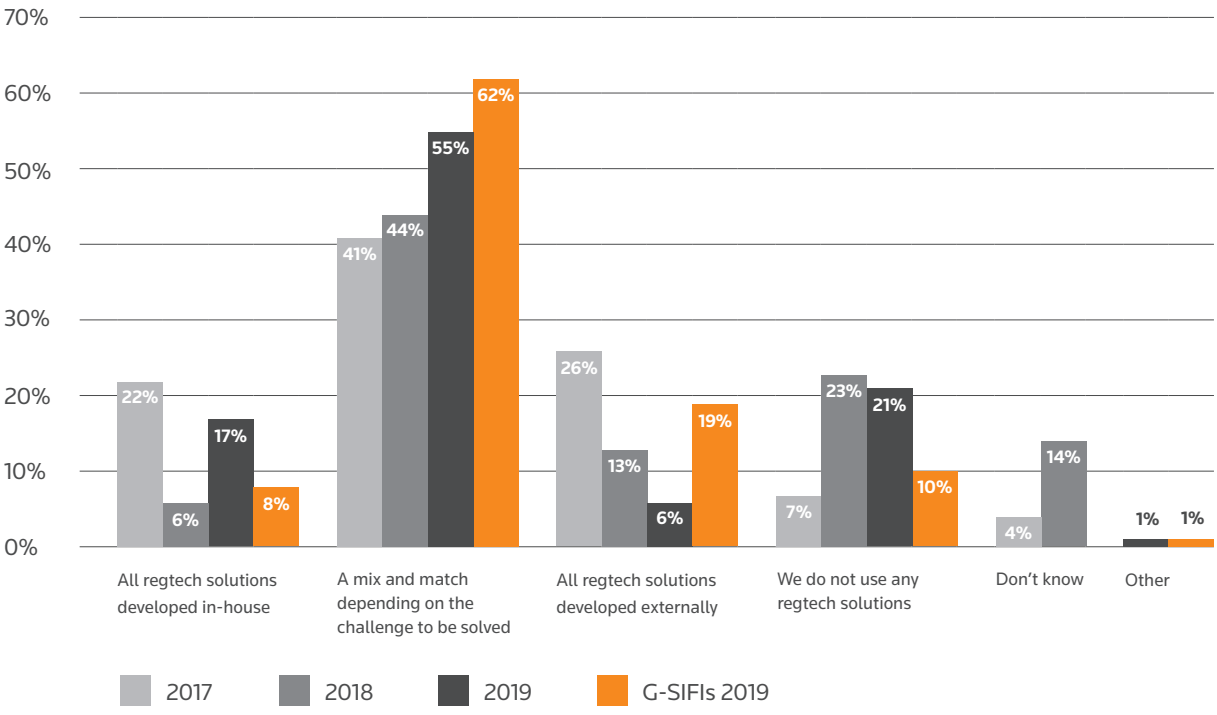


Source: Thomson Reuters Regulatory Intelligence - Fintech, Regtech and the Role of Compliance 2020, by Susannah Hammond and Ashley Kovas

The greatest benefits you expect your firm to see from financial technology in the next 12 months are...

Source: Thomson Reuters Regulatory Intelligence - Fintech, Regtech and the Role of Compliance 2020, by Susannah Hammond and Ashley Kovas

Are you developing regtech solutions in-house or are you looking at external solutions?



Source: Thomson Reuters Regulatory Intelligence - Fintech, Regtech and the Role of Compliance 2020, by Susannah Hammond and Ashley Kovas

Cyber risk

As cyber attacks do not know borders, information sharing and reporting are essential elements to combat threats. Although there are different views on the format and platforms that should be used to share threat intelligence. Cooperation among authorities and supervised firms should be strengthened to enhance cyber resilience for the interconnected global financial system."

Cyberscecurity Risk Supervision, Monetary and Capital Markets Department, International Monetary Fund, September 2019

Cyber risk and the need to be cyber-resilient is a major challenge for financial services firms which are targets for hackers. They must be prepared and be able to respond to any kind of cyber incident. Good customer outcomes will be under threat if cyber resilience fails. One of the most prevalent forms of cyber attack is ransomware.

There are different types of ransomware, all of which will seek to prevent a firm or an individual from using their IT systems and will ask for something (usually payment of a ransom) to be done before access will be restored. Even then, there is no guarantee that paying the fine or acceding to the ransomware attacker's demands will restore full access to all IT systems, data or files.

Many firms have found that critical files often containing client data have been encrypted as part of an attack and large amounts of money are demanded for restoration. Encryption is in this instance used as a weapon and it can be practically impossible to reverse-engineer the encryption or "crack" the files without the original encryption key – which cyber attackers deliberately withhold.

What was previously viewed often as an IT problem has become a significant issue for risk and compliance functions. The regulatory stance is typified by the UK Financial Conduct Authority (FCA) which has said its goal is to "help firms become more resilient to cyber attacks, while ensuring that consumers are protected and market integrity is upheld". Regulators do not expect firms to be impervious but do expect cyber risk management to become a core competency.

Good and better practice on defending against ransomware attacks

Risk and compliance officers do not need to become technological experts overnight but must ensure cyber risks are effectively managed and reported on within their firm's corporate governance framework. For some compliance officers, cyber risk may be well outside their comfort zone but there is evidence that simple steps implemented rigorously can go a long way towards protecting a firm and its customers.

Any basic cyber-security hygiene aimed at protecting businesses from ransomware attacks should make full use of the wide range of resources available on cyber resilience, IT security and protecting against malware attacks. The UK National Cyber Security Centre has produced some practical guidance on how organizations can protect themselves in cyberspace, which it updates regularly. Indeed, the NCSC's 10 steps to cyber security have now been adopted by most of the FTSE350.

NATIONAL CYBER SECURITY CENTRE: 10 STEPS TO CYBER SECURITY

1	**Set up your risk management regime**	Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a risk management regime across your organisation, supported by the board and senior managers.
2	**Network security**	Protect your networks from attack. Defend the network perimeter, filter out unauthorized access and malicious content. Monitor and test security controls.
3	**User education and awareness**	Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.
4	**Malware prevention**	Produce relevant policies and establish anti-malware defences across your organization.
5	**Removable media controls**	Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.
6	**Secure configuration**	Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.
7	**Managing user privileges**	Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.
8	**Incident management**	Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.
9	**Monitoring**	Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.
10	**Home and mobile networking**	Develop a mobile networking policy and train staff to adhere to it. Apply the secure baseline and build to all types of device. Protect data both in transit and at rest.

Source: 10 Steps to Cyber Security Infographic, National Cyber Security Centre, November 2018.

Good advice on the general prevention of a ransomware attack is to seek to ensure company-confidential, sensitive client or other important files are securely and regularly backed up in a remote, un-connected back-up or storage facility. As with other aspects of compliance, the basics done consistently well will go a long way toward providing firms and their clients with a reasonable level of cyber resilience. A firm that has been a victim of a ransomware attack should use all possible means to regain access to IT systems and client files as swiftly and cleanly as possible. This may mean paying any ransom demanded as a matter of urgency. The follow-up action is then to learn all possible lessons to prevent a recurrence of the attack.

Some specific good and better practice recommendations on preventing ransomware attacks include:

- Checking the firm has basic protection against malware and it is up to date – malware being an umbrella term to cover any code or content that could have a malicious, undesirable impact on systems.
- Ensuring all devices have the latest security "patches".
- Removing all unnecessary user accounts (such as guest and administrator accounts) and restricting user privileges to only what is required.
- Removing or disabling any unnecessary software to reduce the number of potential routes of entry available to ransomware attackers.
- Segmenting the network so that if an attack does take place the damage suffered is limited
- Ensuring the firm has an offline and offsite back-up of all critical systems (with the aim of protecting any back-up from also being encrypted as part of an attack)
- Training staff to recognize a ransomware attack if it does manage to get past any anti-malware protection in place.

Some specific good and better practice recommendations for preparing to recover from a ransomware attack include:

- Ensuring the firm has an effective back-up policy and process in place and that it has been regularly tested as working. An essential element of any effectiveness testing is to consider how the firm can seek to ensure that any back-up will not also be maliciously encrypted in the event of a successful ransomware attack.
- Including cyber-attack scenarios in all business and disaster recovery plans and, again, testing regularly to ensure they work as planned.
- Once any ransomware has been removed, ensure a full security scan and penetration test of all systems and network is carried out. If attackers were able to get ransomware onto the firm's systems, they may have gained other access that has not yet been detected.

Cyber security has become a significant regulatory risk and firms must ensure they manage and, whenever feasible, mitigate cyber risks, including ransomware. The compliance function must ensure that cyber risks are expressly included in the range of risks considered, and that the board is prepared to discuss the actions taken to ensure that all reasonable steps have been taken to embed cyber resilience throughout the firm.

Closing thoughts

> The pace of change, together with the borderless nature of technology, requires an appropriate level of caution to be taken, through financial services firms taking risk-based approaches to strategic and business initiatives. Financial services firms need to make informed choices about where and how they are going to adapt and make sure that the associated risks are understood, considered, and measured as they make changes to their processes and business models."

Ed Sibley, deputy governor at the Central Bank of Ireland, November 2019

The financial services industry has much to gain from the effective implementation of fintech, regtech and insurtech but practical reality is there are numerous challenges to overcome before the potential benefits can be realised. Investment continues to be needed in skill sets, systems upgrades and cyber resilience before firms can deliver technological innovation without endangering good customer outcomes. An added complication is the business need to innovate while looking over one shoulder at the threat posed by bigtech.

There are also concerns for solution providers. The last year has seen many technology start-ups going bust and far fewer new start-ups getting off the ground – an apparent parallel, at least on the surface, to the bubble that was around dotcom. Solutions need to be practical, providers need to be careful not to over promise and under deliver and above all developments should be aimed at genuine problems and not be solutions looking for a problem.

There are nevertheless potentially substantive benefits to be gained from implementing fintech, regtech and insurtech solutions. For risk and compliance functions much of the benefit may come from the ability to automate rote processes with increasing accuracy and speed. Indeed, when 900 respondents to the 10th annual cost of compliance survey report were asked to look into their crystal balls and predict the biggest change for compliance in the next 10 years, the largest response was automation.

What is the biggest change you predict for compliance in the next 10 years?

Source: Thomson Reuters Regulatory Intelligence – Cost of Compliance 2019: 10 years of regulatory change, by Stacey English and Susannah Hammond.

Technology and its failure or misuse is increasingly being linked to the personal liability and accountability of senior managers. Chief executives, board members and other senior individuals will be held accountable for failures in technology and should therefore ensure their skill set is up-to-date. Regulators and politicians alike have shown themselves to be increasingly intolerant of senior managers who fail to take the expected reasonable steps with regards to any lack of resilience in their firm's technology.

This year's findings suggest firms may find it beneficial to consider:

- Is fintech (and regtech) properly considered as part of the firm's strategy? It is important for regtech especially not to be forgotten about in strategic terms: a systemic failure arising from a regtech solution has great capacity to cause problems for the firm – the UK FCA's actions on regulatory reporting, among other things, are an indicator of this.
- Not all firms seem to have fully tackled the governance challenge fintech implies: greater specialist skills may be needed at board level and in risk and compliance functions.
- Lack of in-house skills was given as a main reason for failing to develop fintech or regtech solutions. It is heartening that firms understand the need for those skills. As fintech/regtech becomes mainstream, however, firms may be pressed into developing such solutions. Is there a plan in place to plug the skills gap?
- Only 22% of firms reported that they need more resources to evaluate, understand and deploy fintech/regtech solutions. This suggests 88% of firms are unduly relaxed about the resources needed in the second line of defence to ensure fintech/regtech solutions are properly monitored. This may be a correct conclusion, but seems potentially bullish.

About the authors

SUSANNAH HAMMOND

Susannah Hammond is senior regulatory intelligence expert for Thomson Reuters with more than 30 years of wide-ranging compliance, regulatory and risk experience in international and UK financial services.

uk.linkedin.com/in/susannahhammond

@SannaHamm

ASHLEY KOVAS

Ashley Kovas is senior regulatory intelligence expert for Thomson Reuters with more than 30 years' experience in financial services regulation.

uk.linkedin.com/in/ashleykovas

@AshleyKovas

Visit **https://legal.thomsonreuters.com/en/products/regulatory-intelligence**

Our intelligence working for you

About Thomson Reuters Regulatory Intelligence

Thomson Reuters Regulatory Intelligence is a market leading solution that empowers you to make well-informed decisions to confidently manage regulatory risk, while providing the tools to make proactive decisions and action change within your organization. It has been developed with a full understanding of your compliance needs – locally and globally, today and in the future.

Learn more: **legal.tr.com/regulatory-intelligence**

THOMSON REUTERS®