Fintech, Regtech and the Role of Compliance in 2017

By Stacey English and Susannah Hammond

the answer company™
THOMSON REUTERS®

Table of contents

With thanks to Chloe Bloomfield and Helen Camfield

Executive summary

Thomson Reuters has undertaken its second global survey to assess the impact of developments in regtech and fintech on the role and remit of the compliance function in financial services firms. Compliance and risk practitioners from nearly 800 financial services firms across the world took part. As with other Thomson Reuters Regulatory Intelligence analyses, the findings have become a trusted source of insight for firms, regulators and their advisers worldwide. 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.

The focus on all things cyber, whether fintech, regtech or cyber resilience, has been gathering momentum. Discussions on the adoption and regulation of fintech and the impact of potential disruption to not only firms, but also potentially financial stability, have risen to the top of supervisory agendas. The Financial Stability Board (FSB), which operates under the aegis of the G20, is continuing to scan the horizon to identify, assess and address new and emerging risks to financial stability including fintech. The concern regarding the potential threat posed by fintech in no way undermines the potential myriad benefits.

The challenges for firms range from the need to have the appropriate skill sets at all levels of the business, to the capability to be able to evaluate possible regtech, fintech or insurtech solutions. All of which is set against a background of a near universal need to revamp legacy systems, while also implementing and embedding massive regulatory rulebook changes.

Key findings:

- There is a marked increase in the favorable opinion of fintech (including insurtech) innovation and digital disruption with 83 percent of respondents reporting a positive view (27 percent extremely positive). This is almost double the 2016 results where 42 percent reported a positive view (18 percent extremely positive).

- In parallel, there was a significant increase in the favorable opinion of regtech innovation and digital disruption with 75 percent of respondents reporting a positive view (26 percent extremely positive). In contrast, 40 percent reported a positive view in 2016 (15 percent extremely positive).

- The biggest financial technology challenge for firms in the coming year is seen as the need to upgrade legacy systems along with cyber resilience and technology risks. On the benefit side, the deployment of fintech is expected to lead to improvements in efficiency and productivity.

- In terms of risk and compliance involvement in assessing the implications of fintech innovation, there is substantially more engagement in 2017. Eighty one percent of respondents reported involvement, with 37 percent being fully engaged and consulted (63 percent in 2016 with 21 percent fully engaged and consulted.) The number of firms who felt that they did not need to be involved in assessing fintech dropped from 16 percent to just 2 percent.

- Skill sets continue to grow rapidly in risk and compliance functions to keep pace with developments in fintech, with 75 percent of respondents reporting a widening of skill sets and 28 percent investing in specialist skills. This is up from 56 percent in 2016, with 15 percent investing in specialist expertise. A regional outlier was Asia, where 84 percent of firms have invested in specialist skills to widen the skill set within their risk and compliance functions to accommodate developments in fintech and regtech innovation and digital disruption.

- Regtech solutions are increasingly impacting how firms manage compliance and have risen by almost a quarter to 76 percent in 2017 (52 percent in 2016). The number of respondents who reported having already implemented a regtech solution almost doubled in 2017 to 30 percent (17 percent in 2016). The majority of firms (69 percent, and 74 percent G-SIFIs) believe that the successful deployment of fintech/regtech should drive up efficiency and effectiveness, allowing more time to focus on value-added activities.

- The top three areas where compliance and regulatory risk management is most likely to be impacted by regtech at firms has shifted from 2016 to 2017. In 2017, the top three are: interpreting regulations and their impact (21 percent), implementation of regulatory change (16 percent) and capturing regulatory change (16 percent). In contrast, in 2016 the top three were: compliance monitoring (47 percent), regulatory reporting (40 percent) and capturing regulatory change (35 percent).

- The budget available for regtech continues to vary widely. Over a third (38 percent) of respondents expect their budget for regtech solutions to grow in the next twelve months (35 percent in 2016). At the other end of the spectrum, the number of firms that reported having no budget for regtech has dropped significantly to 9 percent in 2017 (24 percent in 2016).

The intelligence, technology and human expertise
you need to find trusted answers.

the answer company™
THOMSON REUTERS®

Introduction

Thomson Reuters Regulatory Intelligence undertook its initial review of fintech and regtech and the role of compliance as a result of the findings of the latest Cost of Compliance report[1] in 2016, which highlighted the increasing challenge raised by all aspects of technology. As reiterated in the findings from the Cost of Compliance report for 2017[2], the challenges from cyber resilience and technology risk remain a key concern for financial services firms.

Figure 1: The greatest compliance challenges the board expects to face in 2017 is/are

Thomson Reuters Regulatory Intelligence - Cost of Compliance 2017

Nearly 800 responses were received to the second survey to assess the impact of regtech and fintech and the associated role of the compliance function in financial services firms. Respondents came from the entire spectrum of financial services firms, large and small, together with all sectors and geographies. Globally systemically important financial institutions (G-SIFIs) were asked to identify themselves to enable comparison between themselves and other smaller firms. The survey closed in Q3 2017.

The types of technology considered in this report are fintech, regtech and insurtech. There are no universally accepted definitions, but, at its simplest, fintech is an IT-enabled solution for the financial services industry.

The FSB's working definition of fintech is "technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services." While the UK Financial Conduct Authority has defined fintech as "the intersection between finance and technology. It can refer to technical innovation applied in a traditional financial services context or to innovative financial services that disrupt the existing financial services market." It has further defined regtech as the "sub-set of fintech that focuses on technologies that may facilitate the delivery of regulatory requirements more efficiently and effectively than existing capabilities."

The International Association of Insurance Supervisors has added to the developing lexicon in a March 2017 report on fintech developments in the insurance industry. The IAIS introduced the term "insurtech" as a subset of fintech and defined it as "the variety of emerging technologies and innovative business models that have the potential to transform the insurance business."

The use of technology to enable the rapid and potentially disruptive development of new products and services has moved from a future concern to a current reality, with financial services firms across the spectrum now engaging with the potential opportunity to meet customers' needs (and indeed expectations) more efficiently and cheaply. Financial services firms and their compliance functions have always, not only embraced change, but also technological developments. The key difference with the current marketplace is the sheer pace and scale of that change.

1 https://risk.thomsonreuters.com/en/resources/special-report/cost-compliance-2016.html
2https://risk.thomsonreuters.com/en/resources/special-report/cost-compliance-2017.html

> "London ... has the most vibrant FinTech centre with revenues of £6.5 billion and employment of over 61,000, both of which are growing rapidly."
>
> Mark Carney, Governor of the Bank of England. Speech - "The high road to a responsible, open financial system" given at a Thomson Reuters Newsmaker (April 2017)

For compliance functions, the opportunities presented by regtech are myriad. The robust implementation of innovative technologies can help firms comply, and evidence compliance, with all relevant regulatory requirements. It is the potential for regtech to enhance the efficiency and effectiveness of compliance and risk management practices which is the focus for many regulators. For firms themselves, it may be a means of coping with change in the regulatory environment and driving down the costs involved in meeting the corresponding requirements. While fintech could result in new processes, new distribution channels, new products or new business organizations, it is regtech that should help firms comply with regulatory requirements and manage risk more effectively and efficiently.

Regulatory Developments and Activity

The fintech regulatory and policy developments around the world are seeking to achieve a balance between encouraging a potentially beneficial disruptive technology to flourish whilst at the same time protecting customers and financial stability. Individual jurisdictions are not only signing memoranda of understanding with each other, but also developing 'sandboxes' to encourage innovation. At the supranational level, consideration is being given to how best to coordinate the supervisory approach.

Figure 2: Implications of fintech developments for banks and bank supervisors

The Basel Committee on Banking Supervision (BCBS) published a consultative document on the implications of fintech for the financial sector in August 2017. Sound practices: Implications of fintech developments for banks and bank supervisors assesses how technology-driven innovation in financial services, or "fintech", may affect the banking industry and the activities of supervisors in the near to medium term.

Banking standards and supervisory expectations should be adaptive to new innovations, while maintaining appropriate prudential standards. Against this background, the Committee has identified 10 key observations and related recommendations on the following supervisory issues for consideration by banks and bank supervisors:

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

Source: Basel Committee for Banking Standards, Sound Practices: Implications of fintech developments for banks and bank supervisors (August 2017) https://www.bis.org/bcbs/publ/d415.pdf

> "One of the key characteristics of fintech is that it is borderless. While each financial market has many idiosyncratic factors, fintech can offer solutions that cut through different geographical and market boundaries."
>
> Norman Chan, Chief Executive, Hong Kong Monetary Authority. Speech – "Welcoming Remarks at HKMA Fintech Day" (October 2017)

Figure 3: Basel Committee of Banking Standards - Implications of fintech developments (August 2017)

	Innovation facilitators		
	Innovation hub A place to meet and exchange ideas	Accelerator "Boot-camp" for start-ups, culminating in a pitch presentation	Regulatory sandbox Testing in a controlled environment, with tailored policy options
Australia	ASIC	ASIC	ASIC
Belgium	NBB/FSMA		
ECB	SSM[31]		
Germany	BaFin		
Italy	BOI		
Hong Kong	HKMA		HKMA
Japan	BoJ/FSA		
Korea	FSC	FSC	
Luxembourg	CSSF		
Netherlands	DNB/AFM		DNB/AFM
Singapore	MAS	MAS	MAS
Switzerland	FINMA		FINMA
UK	BOE/FCA	BOE	FCA[32]

Source: BCBS-FSB Survey

Fintech Regulatory Engagement - Global Impact

At least 36 **Memorandums of Understanding** (MOUs) were signed between regulators in 2016 (10) and 2017 (26), forming frameworks and enabling access to information

Innovation hubs
Regulatory sandboxes

Source: Thomson Reuters Regulatory Intelligence – Fintech, Regtech and the Role of Compliance 2017

Between 2016 and 2017, half of regulatory sandboxes were launched by regulators in Asia. Of the 14 innovation hubs opened to date, more than half were in Europe.

"First, the risk that the cyber threat poses is so serious that we think it is critical that we have a group of people specifically focused on dealing with it. And, second, how we as a Division approach and deal with the enforcement interest in this space warrants a consistent, well-informed, and oftentimes, measured, approach; having a dedicated unit consider and address these issues will help us achieve this goal. ... we are also including within the responsibility of the (new) Cyber Unit our focus on the distributed ledger technology space, also known as blockchain technology. ...the emerging issues presented by blockchain technology warrant a consistent, thoughtful approach – and the best way to do that is to centralize the expertise and the focus in a single unit."

Stephanie Avakian, co-director, Division of Enforcement, U.S. Securities and Exchange Commission in a speech on The SEC Enforcement Division's Initiatives Regarding Retail Investor Protection and Cybersecurity (October 2017)

It is an increasingly rare regulator that has not published its policy and approach to fintech with both supranational bodies and domestic regulators assessing how best to encourage the innovation while preserving good customer outcomes and financial stability. One area that regulators have focused on in detail is the potential for distributed ledger technology (DLT) to transform the financial services industry.

The U.S. Financial Industry Regulatory Authority (FINRA) has defined DLT as involving "a distributed database maintained over a network of computers connected on a peer-to-peer basis, such that network participants can share and retain identical, cryptographically secured records in a decentralized manner." DLT (one potential of which is blockchain) has attracted significant interest and funding in the financial services industry in recent years. Several large financial institutions have established dedicated teams to explore the technology, and some market participants have formed consortia to create industry standards. Indeed, according to a 2016 report by the World Economic Forum, it is estimated that, over the past three years, more than U.S.$1.4 billion has been invested in DLT to explore and implement uses in the financial services industry.

The FSB has considered DLT as part of its work on fintech and reported that across a range of economic functions, financial institutions are investigating applications for DLT – for cross-border interbank payments, credit provision, capital raising and for digital clearing and settlement. The FSB concluded that the "potential gains for customers may be substantial."

"The fifth initiative is working with other regulators to understand developments, and help entrepreneurs in expanding their target markets into other jurisdictions. We signed MoUs with the Monetary Authority of Singapore in June, with the UK Financial Conduct Authority in March, and earlier this month with the Ontario Securities Commission, which not only provide for information sharing, but also for support for our home grown fintech start-ups in accessing markets in each other's jurisdictions.

We also recently concluded an agreement focused more on sharing information about developments with Kenya.

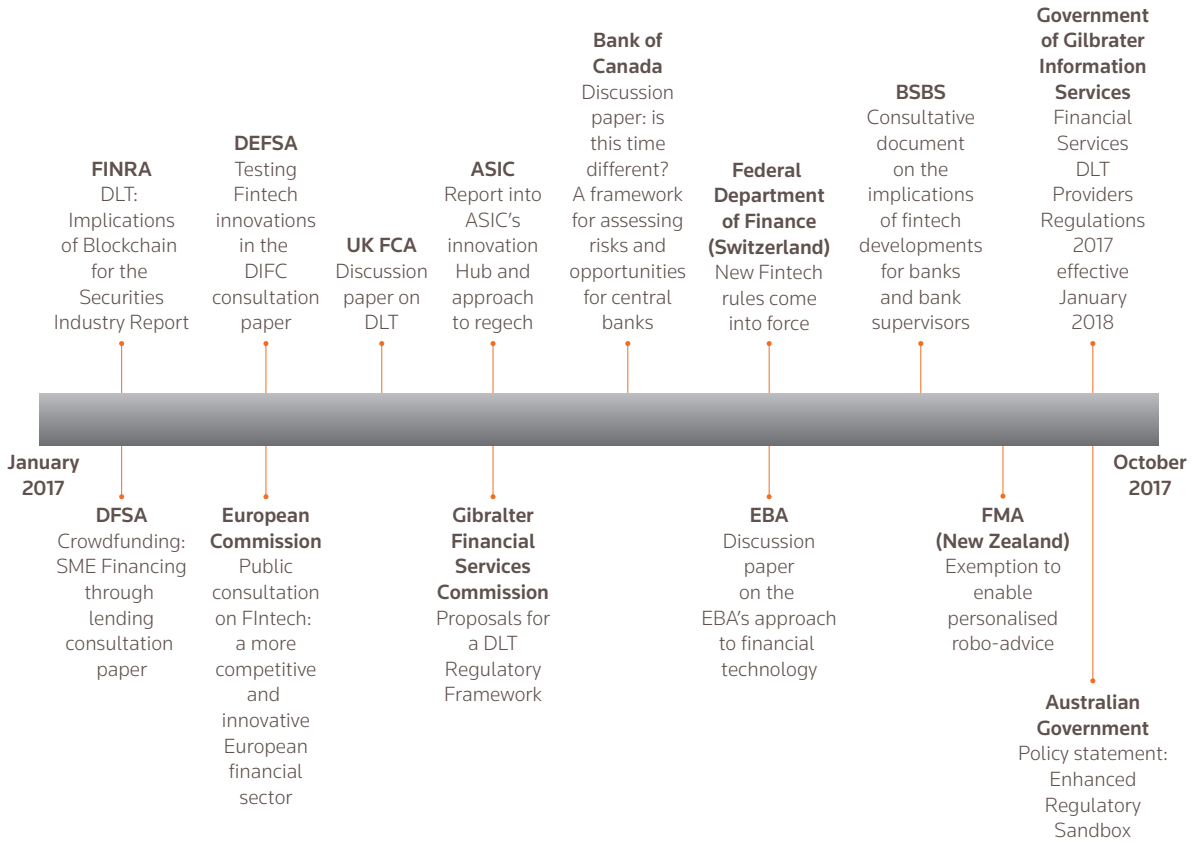
These formal arrangements build on regular and informal discussions we are having with counterpart authorities in Europe and the United States. As the fintech space knows no geographic boundaries, as initiatives in the region take off, we will need to expand these agreements to allow us to cooperate in the supervision of fintech entities."

Greg Medcraft, chairman, Australian Securities and Investments Commission, speech "Fintech: Opportunities, risks and challenges" to the Group of 100, National Executive Dinner (December 2016)

In the wake of the financial crisis, regulators increased the amount of dialogue across borders. The essentially borderless potential of technological solutions and, indeed, challenges, has driven a swathe of information sharing. Memoranda of understanding are now in place crisscrossing the globe as regulators share approaches, innovations and emerging good practice.

> "We also want supervision to keep up with the quick evolution of fintech. Just in the last two years, the number of crowd-funding platforms in the EU has increased by 115 percent. Europe has what it takes to develop a globally competitive fintech sector. But fintechs need coherent regulation to scale up and take full advantage of the single market. In our review, we give the ESAs a strong coordinating role for national fintech initiatives, such as innovation hubs and regulatory sandboxes."
>
> Valdis Dombrovskis, Vice-President at the European Commission. Keynote speech at the ESMA Conference (October 2017)

Figure 4 - Fintech and the regulators: Global Policy Developments in 2017



Source: Thomson Reuters Regulatory Intelligence – Fintech, Regtech and the Role of Compliance 2017

Figure 5 - Best Practices for Effective Development of Fintech

Asia Securities Industry & Financial Markets Association, June 2017

Based on Asia Securities Industry and Financial Markets Association Guidance - Best Practices for Effective Development of Fintech (June 2017)

THOMSON REUTERS REGULATORY INTELLIGENCE

NAVIGATE THE GLOBAL REGULATORY ENVIRONMENT WITH CONFIDENCE

Thomson Reuters Regulatory Intelligence delivers a focused view of the global regulatory environment, empowering compliance professionals to make well-informed decisions to manage regulatory risk using the most comprehensive and trusted intelligence available.

This solution cuts through the complexity and sheer volume of content within the regulatory environment by providing clarity on what is most important for your organization, in a cost-effective way.

- A full and up-to-date view of the regulatory environment, from the broadest global industry perspective down to the most granular detail.
- Coverage of over 750 regulatory bodies and more than 2,500 collections of regulatory and legislative materials from across the world – more than anyone else.
- Richest source of regulatory content: news, analysis, rulebooks, regulatory events and practical guidance.
- Actionable and practical information, from board level reporting to operational compliance management.

LEARN MORE AT RISK.THOMSONREUTERS.COM/REGULATORY-INTELLIGENCE

The intelligence, technology and human expertise you need to find trusted answers.

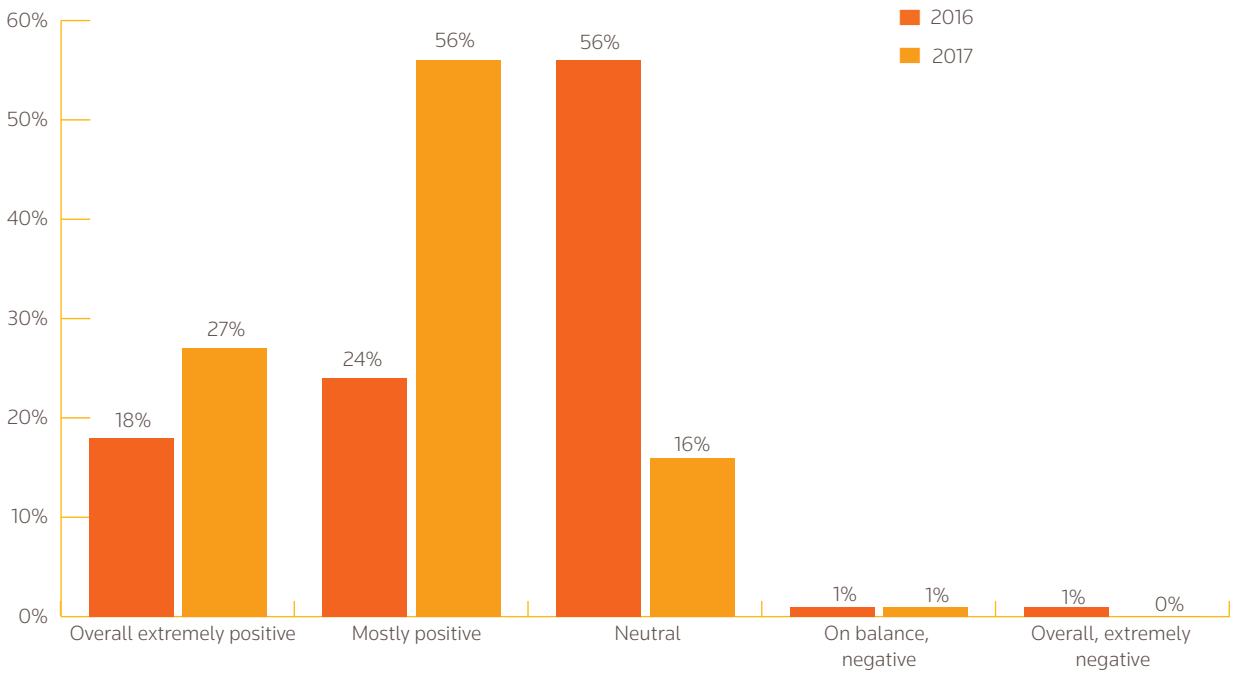
the answer company™
THOMSON REUTERS®

Industry Opinion

"...Fintech requires a more balanced attitude as between 'regulating the institution' and 'regulating the activity'; whereas the complex interplay between fintech and the current regulation can result in mismatches, with companies and service providers being regulated differently even if they perform substantially identical activities and with some activities not being well captured by the definition and/or scope of activities in the current regulation; whereas the current EU consumer and investor protection framework for financial services does not address all fintech innovations adequately."

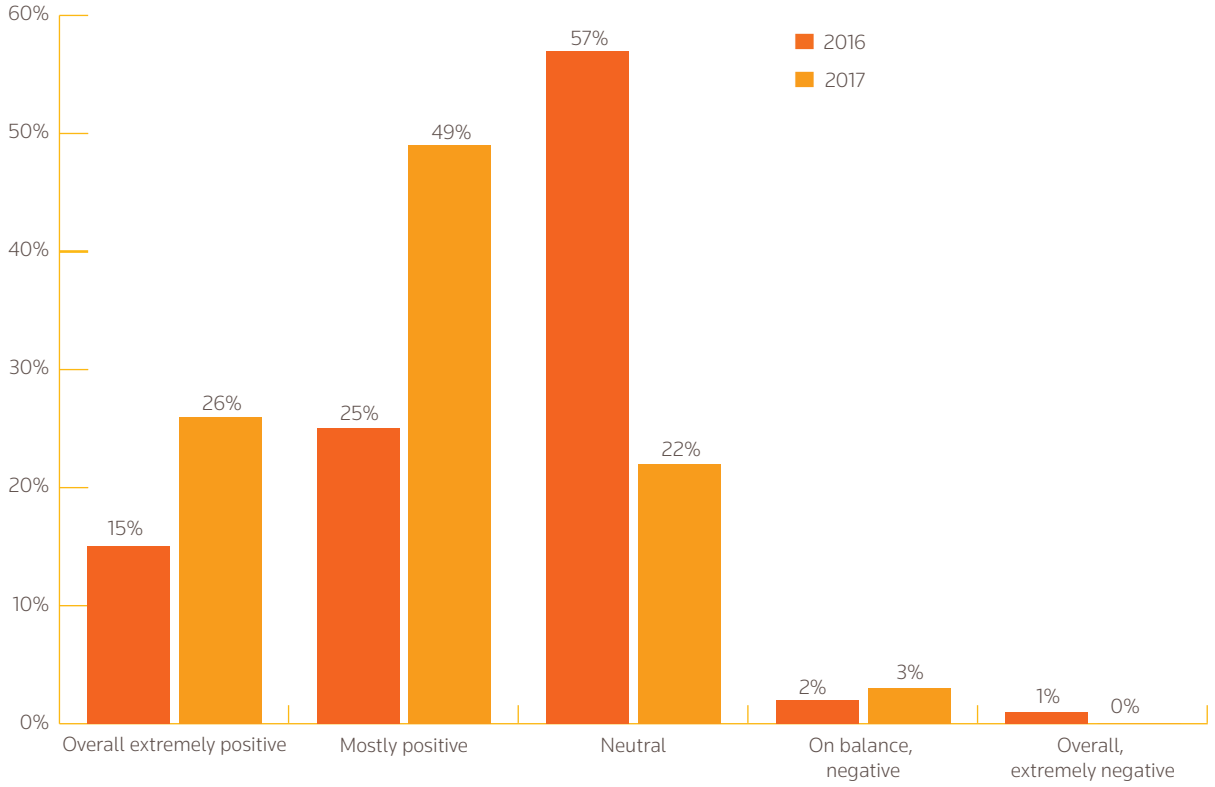
European Parliament resolution of 17 May 2017 on Fintech: the influence of technology on the future of the financial sector (2016/2243(INI)).

Figure 6 - What is your view of fintech (including insurtech) innovation and digital disruption?



Source: Thomson Reuters Regulatory Intelligence – Fintech, Regtech and the Role of Compliance 2017

Figure 7 - What is your view of regtech innovation and digital disruption?



Source: Thomson Reuters Regulatory Intelligence – Fintech, Regtech and the Role of Compliance 2017

Firms are warming up to the potential benefits of fintech and regtech. There has been a marked positive shift of respondents who view fintech and regtech innovation and digital disruption in a favorable light. In overall terms for 2017, 83 percent of respondents had a favorable opinion of fintech (including insurtech), innovation and digital disruption, with 27 percent reporting an extremely positive view. This is almost double the 2016 results, where 42 percent reported a positive view (18 percent extremely positive).

In parallel, there was a significant increase in the favorable opinion of regtech innovation and digital disruption, with 75 percent of respondents reporting a positive view (26 percent extremely positive). This was in distinct contrast to the 40 percent who reported a positive view in 2016 (15 percent extremely positive).

"To make things smoother—at least a bit—we need dialogue. Between experienced regulators and those regulators that are just beginning to tackle fintech. Between policymakers, investors, and financial services firms. And between countries.

Reaching across borders will be critical as the focus of regulation widens—from national entities to borderless activities, from your local bank branch to quantum-encrypted global transactions."

Christine Lagarde, IMF Managing Director. Speech – "Central Banking and Fintech – A Brave New World?" at the Bank of England Conference (September 2017)

Figure 8 - What are the greatest benefits you expect your company to see from financial technology in the next 12 months?

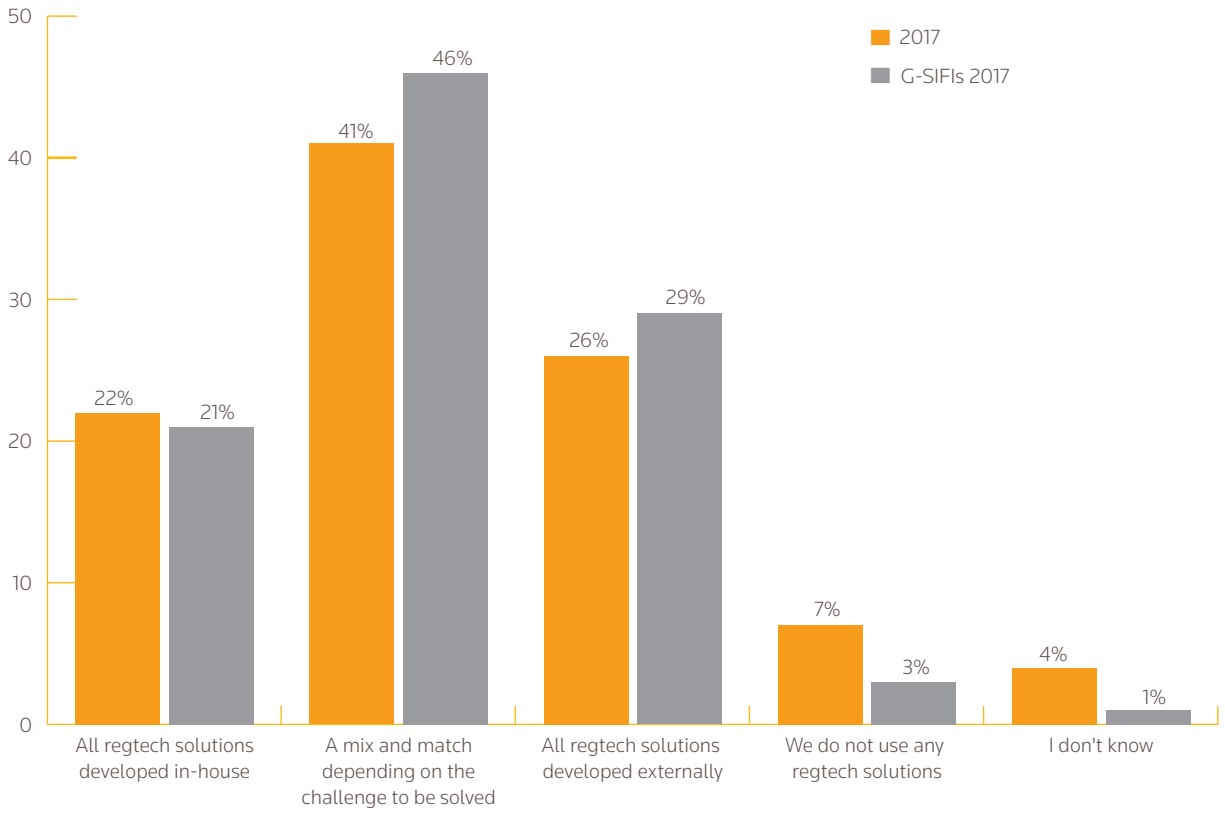
Source: Thomson Reuters Regulatory Intelligence – Fintech, Regtech and the Role of Compliance 2017

There were myriad expected potential benefits from fintech. Improved efficiency and productivity was seen as the largest potential benefit, with successful deployment of fintech and regtech enabling, among other things, more time to focus on value-added compliance activities. Other prominent potential benefits included greater commercial opportunities and advancing technology and better IT systems. Of particular interest to the compliance function is the capacity to implement and embed better compliance practices together with improved customer outcomes.

The expected benefits have contributed to the vast majority (93 percent) seeking to develop regtech solutions.

> "If an organization relies on third parties (such as outsourced or cloud based technology services) they remain accountable for the protection of any essential service. This means that there should be confidence that the security principles are met regardless of whether the organization or a third party delivers the service. For many organizations, it will make good sense to use third party technology services. Where these are used, it is important that contractual agreements provide provisions for the protection of things upon which the essential service depends."
>
> UK Department for Digital, Culture Media & Sport. Public Consultation – "Security of Network and Information Systems" (August 2017) the Bank of England Conference (September 2017)

Figure 9 - 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 2017

The question as to whether or not to develop regtech solutions in-house received a spectrum of responses with the majority of firms choosing a mix-and-match approach depending on the challenge to be solved. There is no one-size-fits-all. Regtech solutions developed in-house should have the benefit of being precisely tailored to the problem or issue to be solved, but external solutions may be able to leverage a different or wider skill set in the development of a potential industry standard solution.

As a regional outlier, the results in Asia are broadly similar, though with a greater emphasis on the development of regtech solutions in-house (28 percent in Asia as opposed to 22 percent in the wider population).

Wherever regtech is developed, it is incumbent on compliance and risk functions to be involved at all stages to ensure that any solution, either built in-house or purchased, is not only fit for purpose, but also remediates or improves the overall compliance position of the firm.

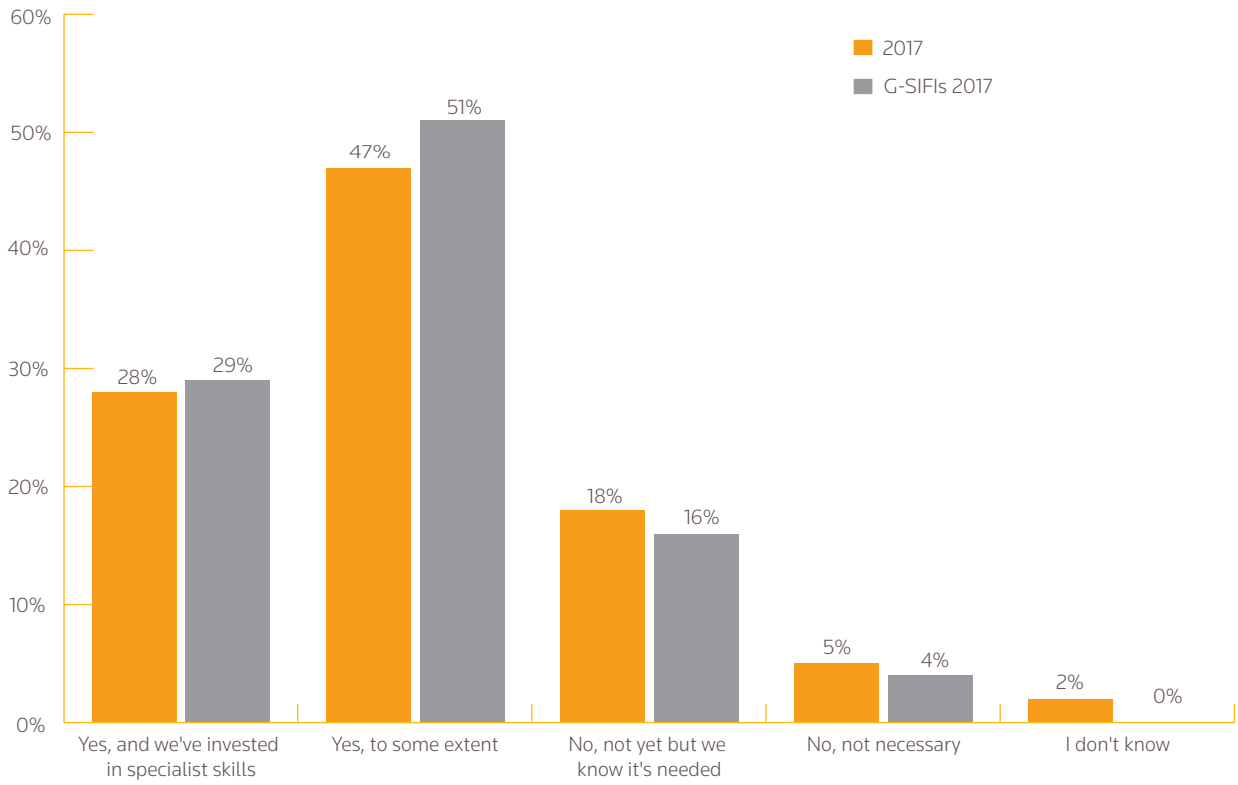
Budget and Skilled Resources

"Technology has significantly reshaped even our more traditional financial firms. One major financial firm reportedly has reduced its equity traders from 600 to just two. Now, one third of its overall employees—9,000 people—are computer engineers. Another major firm reported that it spent $9.5 billion on technology in 2016 alone. Many mainstream financial firms are now technology firms."

Kara M.Stein, Commissioner at the U.S. Securities and Exchange Commission. Speech – "A Joint Path Forward: Address at Eurofi" (September 2017)

Skill sets continue to grow rapidly in risk and compliance functions to keep pace with developments in fintech, with 75 percent of respondents reporting a widening of skill sets, with 28 percent investing in specialist skills. This is up from 56 percent in 2016, with 15 percent investing in specialist expertise. A regional outlier was Asia, where 84 percent of firms have invested in specialist skills to widen the skill set within their risk and compliance functions to accommodate developments in fintech and regtech innovation and digital disruption.

Figure 10 - 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 2017

There is widespread awareness of the need for training and skills in all aspects of fintech and regtech digital innovation and disruption. The point is illustrated by the results from a cybersecurity workshop reported on by the Financial Stability Board in October 2017, in which the private sector participants "noted the proliferation of cyber weapons and decreased costs for criminals to access attack tools. Against that background, they noted the comparative scarcity of cybersecurity trained professionals to help financial institutions respond. They cited the need to create capacity and develop a pipeline of talent. Participants also noted the need for better training of supervisory examination staff, while acknowledging that it is difficult for governments to compete with the private sector in attracting and retaining trained cybersecurity professionals. Private sector participants also emphasized the importance of training at all levels within firms. They noted that the majority of successful cyber attacks involve human error and stressed the importance of awareness training for all staff. They also discussed the importance of educating the board about cyber risks."

There is a growing demand for skills in specialist areas. As just one example, LinkedIn data requested by the Financial Times[3] showed there were more than 1,000 blockchain-related job adverts on the site in the week beginning May 29, 2017 - more than treble the level of a year ago. The same data also showed the number of blockchain ads is growing at more than 40 percent each quarter.

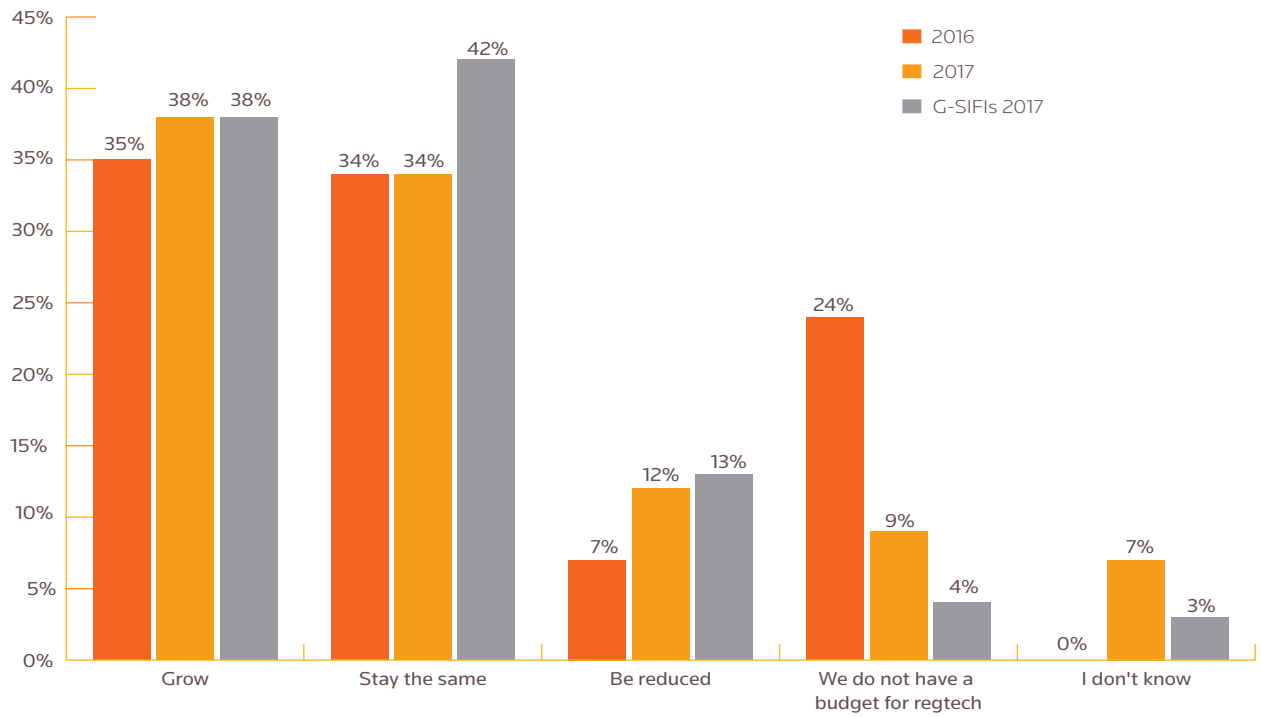
The need for specialist skills is not limited to firms. Regulators and policymakers alike are aware of the need to upskill. The BCBS August 2017 consultation on 'Sound practices: implications of fintech developments for banks and bank supervisors' made a specific recommendation such that:

Recommendation 7: Bank supervisors should assess their current staffing and training models to ensure that the knowledge, skills and tools of their staff remain relevant and effective in supervising new technologies and innovative business models. Supervisors should also consider whether additional specialised skills are needed to complement existing expertise.

Financial services firms of all shapes and sizes need to appreciate the critical importance of having access to the relevant skill sets, which may become a significant differentiating factor. To thrive in the new fintech age, firms (and regulators) would be well advised to undertake an IT skills audit that highlights and begins to remediate any gaps. Such an audit would also need to ensure the firm is prepared when regulators ask about skills at the board and other levels and about the potential (over) use of consultants. The audit should cover technological skills throughout the firm, not just in the IT department, to ensure all functions (risk, compliance and internal audit included) have the appropriate levels of IT expertise for their roles.

The investment in skills is just one of the uses for any budget allocated to fintech and regtech solutions.

Figure 11 - 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 2017

3 https://www.ft.com/content/e49e5310-4923-11e7-919a-1e14ce4af89b

The budget available for regtech continues to vary widely. Over a third (38 percent) of respondents expect their budget for regtech solutions to grow in the next twelve months (35 percent in 2016). At the other end of the spectrum, the number of firms that reported having no budget for regtech has dropped significantly to 9 percent in 2017 (24 percent in 2016). In the G-SIFI population, the majority of respondents stated that their budget would stay the same. Given G-SIFIs capacity to invest in compliance solutions, this may be due to the high initial investment that is being maintained.

From a regional perspective, those firms based in the U.S. and Canada were almost evenly divided on whether budgets for regtech solutions will grow (34 percent) or remain the same (39 percent) over the next 12 months. The same holds true for those firms based in rest of world, including Africa, Australasia, Middle East and Latin America.

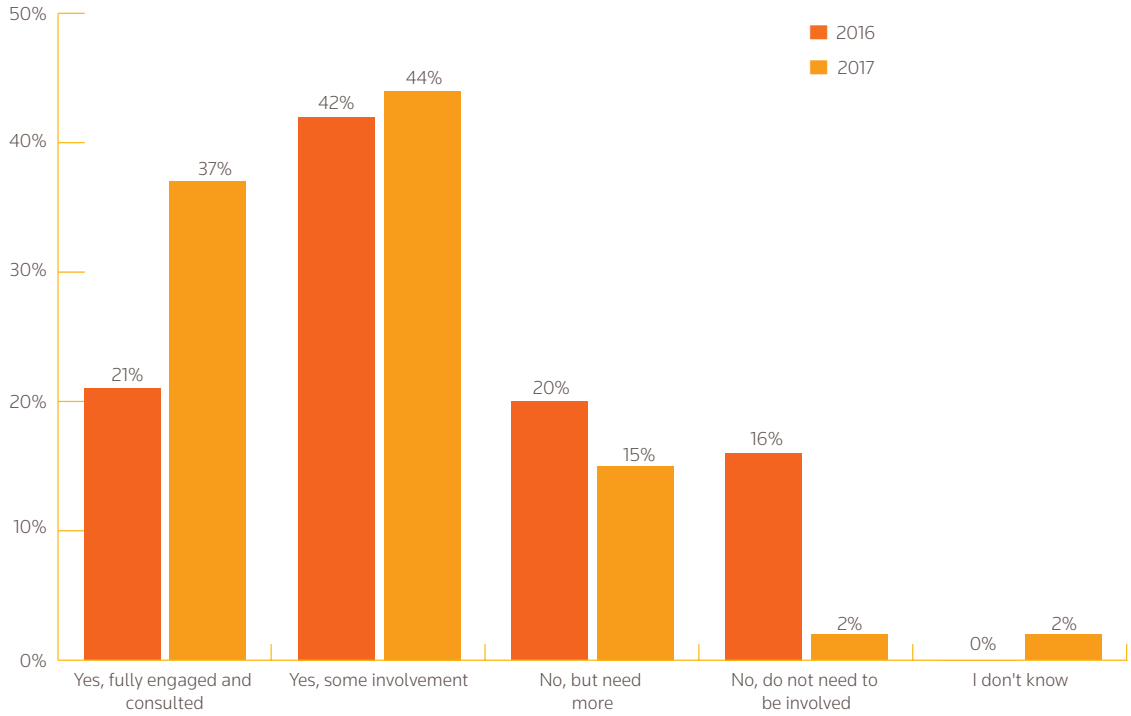
Board and Compliance Involvement

"Effective governance structures reinforce accountability by articulating clear responsibilities and lines of reporting and escalation. Effective governance also mediates competing objectives and fosters communication among operating units, information technology, risk, and control-related activities. Consistent with their missions and strategies, boards of directors (or similar oversight bodies for public entities or authorities) should establish the cyber risk tolerance for their entities and oversee the design, implementation, and effectiveness of related cybersecurity programs."

G7 Cyber Expert Group. Policy Paper – "G7 Fundamental Elements for Cyber Security." (October 2016)

In terms of risk and compliance involvement in assessing the implications of fintech innovation, there is substantially more engagement in 2017. Eighty one percent of respondents reported involvement, with 37 percent being fully engaged and consulted (63 percent in 2016, with 21 percent fully engaged and consulted.) The number of firms who felt that they did not need to be involved in assessing fintech dropped from 16 percent to 2 percent.

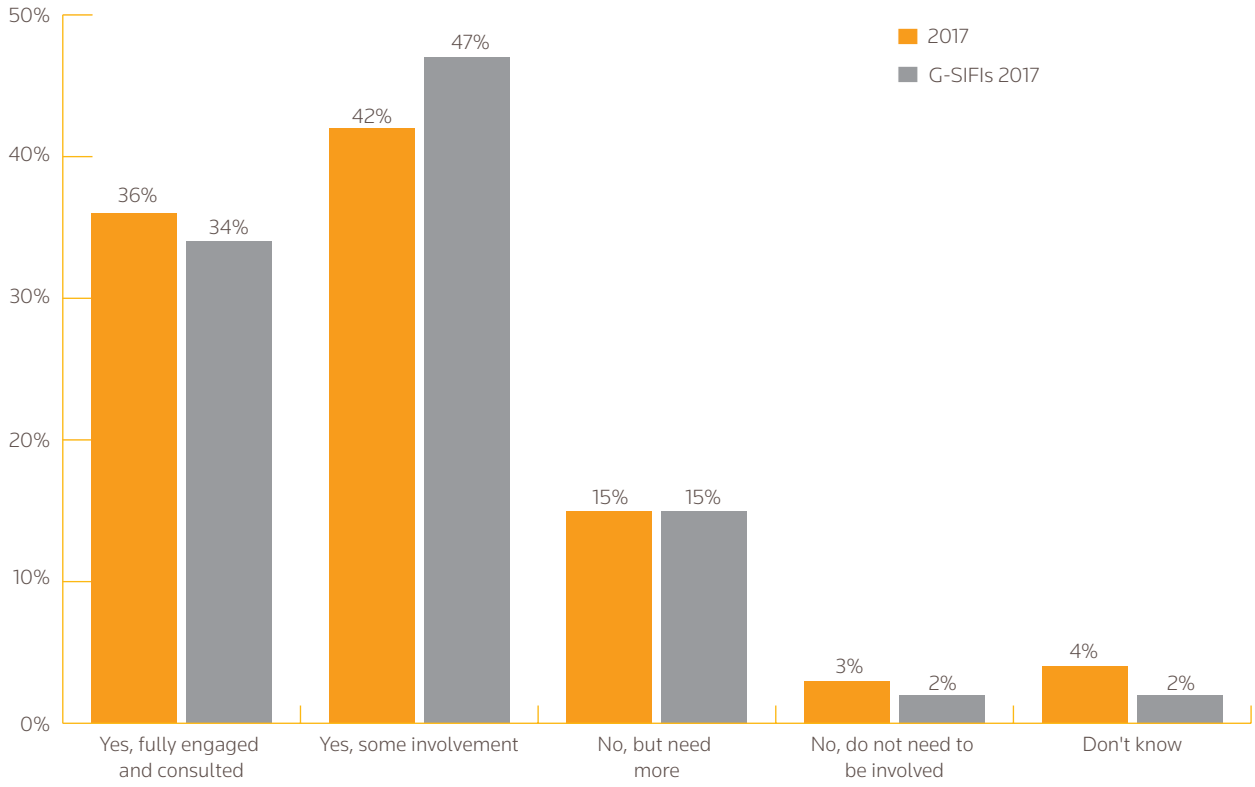
Figure 12 - Do the risk and compliance functions have enough involvement with your firm's approach to fintech, regtech and insurtech?



Source: Thomson Reuters Regulatory Intelligence – Fintech, Regtech and the Role of Compliance 2017

Perhaps the best demonstration of increasing risk and compliance function involvement in fintech, regtech and insurtech is the drop in those respondents that stated they did not need to be involved. This, combined with the increase in those reporting that the risk and compliance functions are fully engaged and consulted, paints a picture of far greater numbers of firms taking positive steps towards realizing the potential of fintech, regtech and insurtech.

Figure 13 - 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 2017

Over a third (36 percent, 34 percent for G-SIFIs) of respondents reported that their boards are fully engaged and consulted on its approach to fintech, regtech and insurtech. Regionally, boards in the U.S. and Canada were least involved in their firm's approach to fintech, regtech and insurtech (74 percent, split 36 percent fully engaged and consulted and 38 percent some involvement), compared to the UK and Europe (81 percent, split 34 percent fully engaged and 47 percent some involvement).

"Some boards are also recognizing the importance of carefully considered succession planning as part of their broader strategic planning. This ensures that boards don't just look to fill a vacancy as it arises but think about the skills and experience that will need to be replaced as each director's term is likely to end, as part of ongoing renewal planning. Most notably, recent appointments to some boards have added cyber and digital skills to the mix, to enhance board capability to provide appropriate review and challenge in this ever changing space."

Helen Rowell, deputy chairman of the Australian Prudential Regulatory Authority, speech entitled "Superannuation Governance in 2017: What does good look like?" delivered at the Australian Institute of Superannuation Trustees Governance Ideas Exchange in Melbourne (October 2017).

Boards may need to consider increasing their engagement in and commitment to technology. The January 2016 UK Treasury Committee response to major bank IT system failures remains relevant, despite the Rt Hon. Andrew Tyrie MP, then Chairman of the Treasury Committee, stating that: "The current situation cannot be allowed to continue. IT risks need to be accorded the same status as credit, financial and conduct risk. They are every bit as serious a threat to customers and overall financial stability. More and higher quality investment is probably required."

With that background, the Treasury Committee had made three, what it has called, 'suggestions', which will, in effect, steer the future UK regulatory and supervisory approach to IT in financial services. In outline, the three suggestions are:

- Banks need greater IT expertise at main board and subsidiary board level
- Much greater resources should be put towards modernizing, managing and securing banks' IT infrastructures
- Legal, regulatory, structural and cultural changes are needed to the way that banks manage their cyber security risks

The UK Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA) also outlined the six key themes arising from a review of critical infrastructure and technology resilience:

1. Board accountability for critical infrastructure – several firms were found to not have a designated individual to oversee IT risk at board level
2. IT expertise on the board – in some firms, there was limited IT subject matter expertise on the board
3. 3.Appreciation of conduct considerations within IT risk appetite statement needed to be improved
4. Maturity of three lines of defense model – IT risk management capabilities were found to be relatively immature across several firms. In particular, the FCA identified instances of inadequate delineation between the first and second line responsibilities, with substantial dependence on external consultancies to supplement second and third line capabilities. The FCA also observed that single points of failure and other risks inherent in IT architecture had been largely derived from external review, commissioned rather than through "business as usual" risk assessments
5. Breath of IT resilience scenarios required improvement
6. A potential over-reliance on third party assurance

"In many regulated institutions, there is no one clear owner for technologies in AML. In many cases, the responsibility is split between compliance, technology and operational areas, slowing down decision making on adoption of new potential solutions."

UK FCA Research Paper – "New Technologies and Anti-Money Laundering Compliance." (March 2017)

Impact on Compliance

"In the current context in which the drivers of innovation are facilitating rapid growth of the fintech industry, firms may develop without the necessary risk management expertise and under-estimate the level of risk they are taking on."

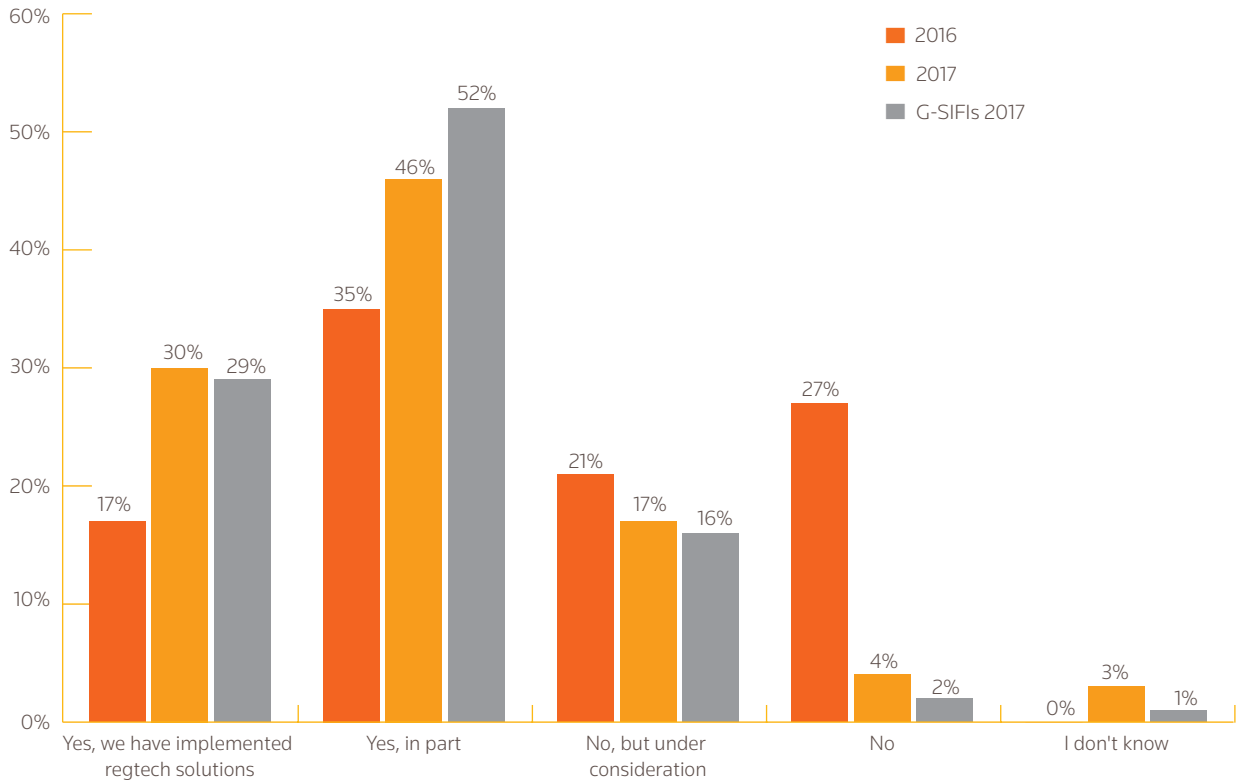
Financial Stability Board. Report - "Financial Stability Implications from Fintech: Supervisory and Regulatory Issues that Merit Authorities' Attention" (June 2017)

Figure 14 - Practical instances of the Basel Committee's Principles for Sound Management of Operational Risk (PSMOR) Applied to Fintech

PSMOR	Practical implementation for Fintech Development
Fundamental Principals of Operational Risk Management	
1 Ensuring a strong risk culture	Ensuring integrated risk culture shared throughout the supply chain
2 Risk management framework	Capturing fintech-driven new risks and risk profile changes
Governance	
3 Effectively implementing risk policies, processes and systems	Building up framework to capture and control fintech-driven new risks
4 Setting and reviewing risk appetite and risk tolerance	Setting appropriate risk appetite and tolerance with effective thresholds to trigger prompt remedial action
5 Implementing the policies, processes and systems to control risks	Ensuring prompt reporting, assessment and early risk mitigation for fintech-driven risks
Risk Management Environment	
6 Identifying/assessing risks in all processes and systems	Enhancing capacity to identify, assess and mitigate risks arising from extended processes and systems in fintech migrations
7 Assessing risks in the launch of every product, activity, process and system	Ensuring the timely and overarching identification, assessment of risks in the launch and delivery of fintech-driven processes and systems
8 Appropriate risk monitoring and proactive risk management	Updating the frequency of monitoring and reporting with appropriate escalation according to the size and nature of the risks
9 Strong risk control environment	Affording appropriate capacities and resources allocated to promptly and effectively control fintech-driven risks.
Business Resiliency and Continuity	
10 Business resiliency and continuity plans for severe business disruption	Incorporating business continuity and disaster recover plan with business disruption scenarios in fintech-driven processes and systems
Role of Disclosure	
11 Public disclosure of risk management	-

Based on Basel Committee for Banking Standards, sound Practices: Implications of fintech developments for banks and bank supervisors (August 2017) http://www.bis.org/bcbs/publ/d415.pdf

Figure 15 - Are regtech solutions impacting how you manage compliance?



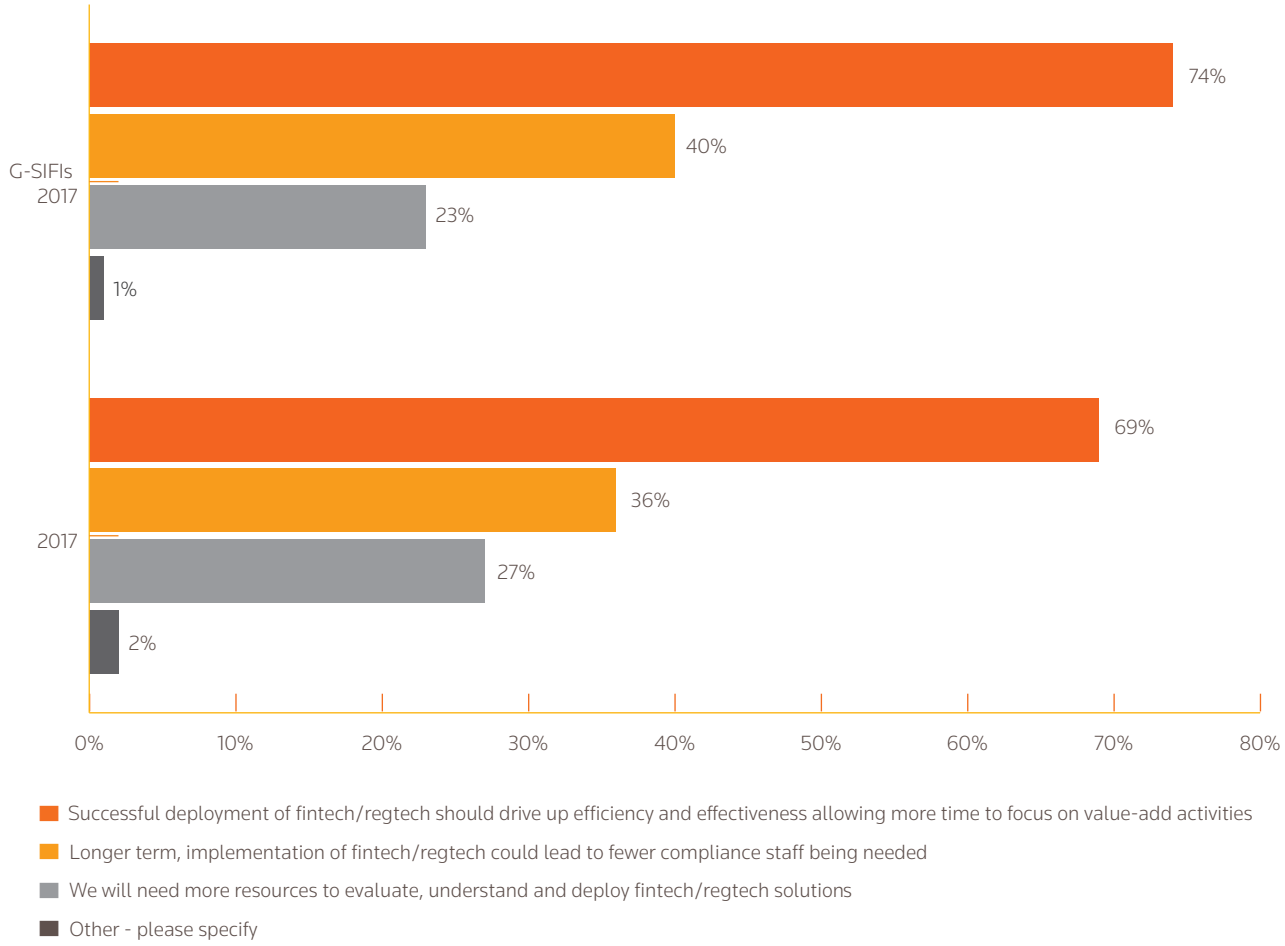
Source: Thomson Reuters Regulatory Intelligence – Fintech, Regtech and the Role of Compliance 2017

There has been a significant increase in the reported impact of regtech on the management of compliance. The number of firms that have implemented regtech solutions has almost doubled to 30 percent of respondents in 2017 (17 percent in 2016). Adding to the increased impact are both the substantial drop in those respondents reporting that regtech is not impacting how compliance is managed (27 percent in 2016 falling to 4 percent in 2017) and the 11 percent increase in number of firms who, in part, consider regtech solutions to be impacting how compliance is managed.

In a regional perspective, 84 percent of firms based in Asia consider, or in partly consider, regtech solutions to be having an impact on how they manage compliance.

> "We need to speed up our consideration of the fintech issues and think harder about what is the regulatory environment that is going to be appropriate. I think we have been complacent so far."
>
> **James Bullard, President of the Federal Reserve Bank of St. Louis. Interview with Reuters on interest rate and low inflation (October 2017)**

Figure 16 - What will be the impact of fintech/regtech on your compliance function?



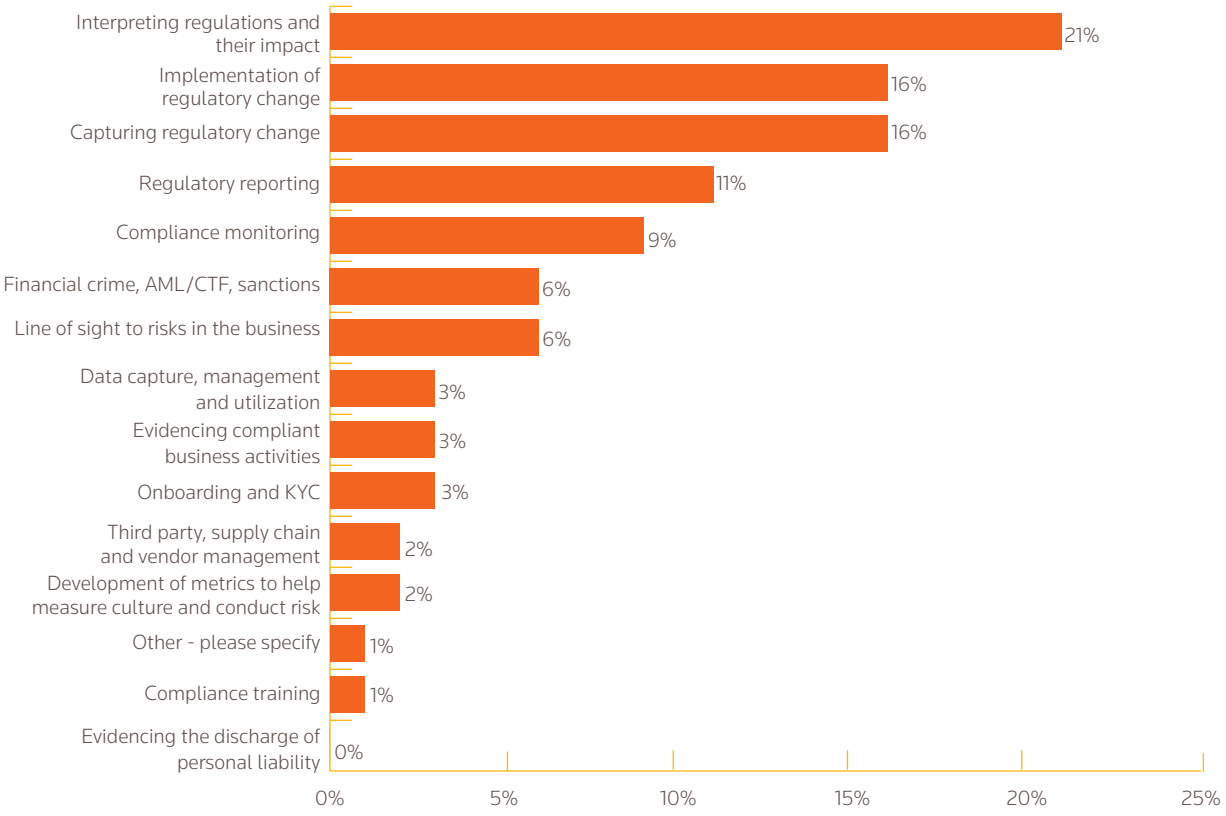
Source: Thomson Reuters Regulatory Intelligence – Fintech, Regtech and the Role of Compliance 2017

The biggest (69 percent, 74 percent for G-SIFIs) perceived impact of the successful deployment of fintech/regtech on the compliance function is seen to be the ability to drive up efficiency and effectiveness, thereby allowing more time to focus on value-added activities. One ramification of the move towards technology is the potential, longer-term need for fewer compliance staff. Whilst on the surface the need for fewer compliance staff could be seen as an adverse impact on the compliance function, the move to a smaller, more highly-skilled, greater value-added function should maintain, if not increase, salaries and the need for experienced compliance personnel.

Compliance is not alone. As just one example, according to an October 2017 article from the Financial Times, Nordea Bank will cut around 6,000 jobs, including at least 2,000 consultants, as part of a transformative move to maintain its competitiveness as part of a shift towards digital services such as the use of artificial intelligence to answer common customer queries.

Alongside the focus on skills and the need to invest in specialist skills is the quarter (27 percent) of firms that said they will need more resources to evaluate, understand and deploy fintech/regtech solutions.

Figure 17 - 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 2017

With three quarters of firms (76 percent) of firms reporting at least a partial implementation of regtech solutions, the top three areas where compliance and regulatory risk management is most likely to be impacted by regtech at firms going into 2018 are: interpreting regulations and their impact (21 percent); implementation of regulatory change (16 percent); and capturing regulatory change (16 percent).

This shows a distinct shift from the prior where the top three areas of compliance and regulatory risk management deemed likely to be impacted by the deployment of regtech were: compliance monitoring (47 percent); regulatory reporting (40 percent); and capturing regulatory change (35 percent). The year-on-year change may reflect the fast pace of change in the regtech marketplace, with both new solutions and firms' expectations continuing to evolve. The one consistent thread is that of capturing regulatory change.

Asia was again a regional outlier, with almost a quarter of firms (23 percent) saying that the implementation of regulatory change was most likely to be impacted by regtech. There were variations in top priorities, with capturing regulatory change seen as one of the more likely areas to impact firms in the U.S. and Canada (19 percent).

Compliance functions need to have the capacity and capability to evaluate regtech solutions. As part of the 2016 report, the approach and steps for compliance functions and their firms to consider were set out and bear repeating for use in the governance processes around regtech (and fintech or insurtech) solutions.

Lifecycle of a Regtech Solution

Figure 18 - Lifecycle of a Regtech Solution

Source: Thomson Reuters Regulatory Intelligence – Fintech, Regtech and the Role of Compliance 2017

- **Possible regtech solution** There are growing shopping lists of possible regtech solutions for firms to choose from. One way of prioritizing the range of solutions available may be to focus on the pinch points in existing compliance processes. This may include the need to speed up the full onboarding process for new clients, the ability to use "big data" for compliance monitoring, the need to detect possible insider dealing or abuse of trading limits, the ability to evidence all elements of a discretionary sale or even to collate, assess and evidence the skills sets on corporate governance committees and the board.
- **Research and capability** Once a possible regtech solution has been selected, due diligence will be needed to check the understanding of what it delivers, the assumptions in any data feeds, capture and processing, and its capacity to be integrated into the firm's existing systems (including the disaster recovery and business continuity plans). If the solution is to be provided by a third party (or even another group company), the due diligence protocols also need to include the usual steps for the assessment of a third-party outsourced provider. One practice step at this stage is to ensure all the research and due diligence is documented in detail, particularly with regard to the assumptions.
- **Assessment of value of solution** As with compliance there is no one-size-fits-all approach to assessing the value of a solution. Unlike the implementation of regulatory change, which is compulsory, the evaluation of one regtech solution over another (or to choose to do nothing) is at the discretion of the firm. One good practice step is to seek to include the widest possible range of criteria to maximize the accuracy of the value proposition and any possible trade-offs. The costs, in terms of both money and other resources, of implementation, embedding and testing, are obvious for inclusion, as are any maintenance or upgrade costs.

- Other elements to consider are: the value of any compliance time potentially freed up; the additional compliance testing which may be required to ensure the efficacy of the solution; the need for additional skills and/or training; the use of an already crowded IT change schedule for implementation; the impact of any additional information security or other cyber risks; the need to change existing reporting to accommodate new information flows; and the need to add another third-party outsourcer to the compliance monitoring program.

  As with the research stage, it is good practice to document the detail of the pros and cons considered as part of the assessment and the relative weighting given to each, and thereby support the final decision made. This is equally valuable if the decision is to do nothing and not invest in regtech, as the firm may well be asked the question by its regulators as to why regtech has not been employed.

- **Approval** Most firms have established approval processes involving sign-off by relevant stakeholders. Given the potentially hybrid nature of a regtech solution it may be that several different governance committees are involved in the sign-off and approval. Throughout the approval process, critical challenge needs to be in place to ensure all the potential additional risks are appropriately captured, measured and, where possible, offset. The approval process may well also impose success criteria and stipulate the period in which, say, the risk committee will require a full review of the operational success (or otherwise) of the solution.

- **Deployment** The implementation and embedding of any regtech solution is likely to be undertaken by the IT department within a firm, but it is critical the compliance function has sufficient skill to engage with and, if need be, oversee the process. Firms may wish to consider "parallel running" of existing protocols and any new regtech solutions until they are satisfied with the operational results of the regtech. This may be particularly useful if the regtech solution relies on outsourced processing of data. Detailed records should be kept of the exact technical nature of the implementation process employed to allow for trouble-shooting and any system or personnel changes.

- **Review and monitoring** As a matter of course, the efficacy of any regtech solution deployed must be tested in and of itself. Wherever possible, testing should obtain independent third-party confirmation that the solution, system or process is operating as expected. Any discrepancies should be followed up as a matter of urgency and assessed to see if they provide indicators to any process or control issues or with the underlying data flow assumptions made. With many IT implementations there is a process of "snagging" or "user acceptance testing" whereby a series of small tweaks are made until the solution is operating as expected.

- **Retirement, decommissioning** As part of the overall planning and management process, firms should consider how the solution would be decommissioned. Particular care needs to be taken with any elements of regtech which have been outsourced to ensure, if required, an orderly and auditable return of data.

Challenges for Firms

"Digitization offers no doubt considerable opportunities – but a host of opportunities for cyber-attacks as well. Cyber risk is the dark side of the same coin and adds a new nuance to risk management. What worries me is that IT security is frequently considered only from a cost angle."

Felix Hufeld, President of the Federal Financial Supervision Authority (BaFin). Speech - "What are the potential opportunities and risks of the digitization of finance for regulators?" at the G20 Conference on "Digitizing Finance, financial inclusion and financial literacy" (January 2017)

IT infrastructure

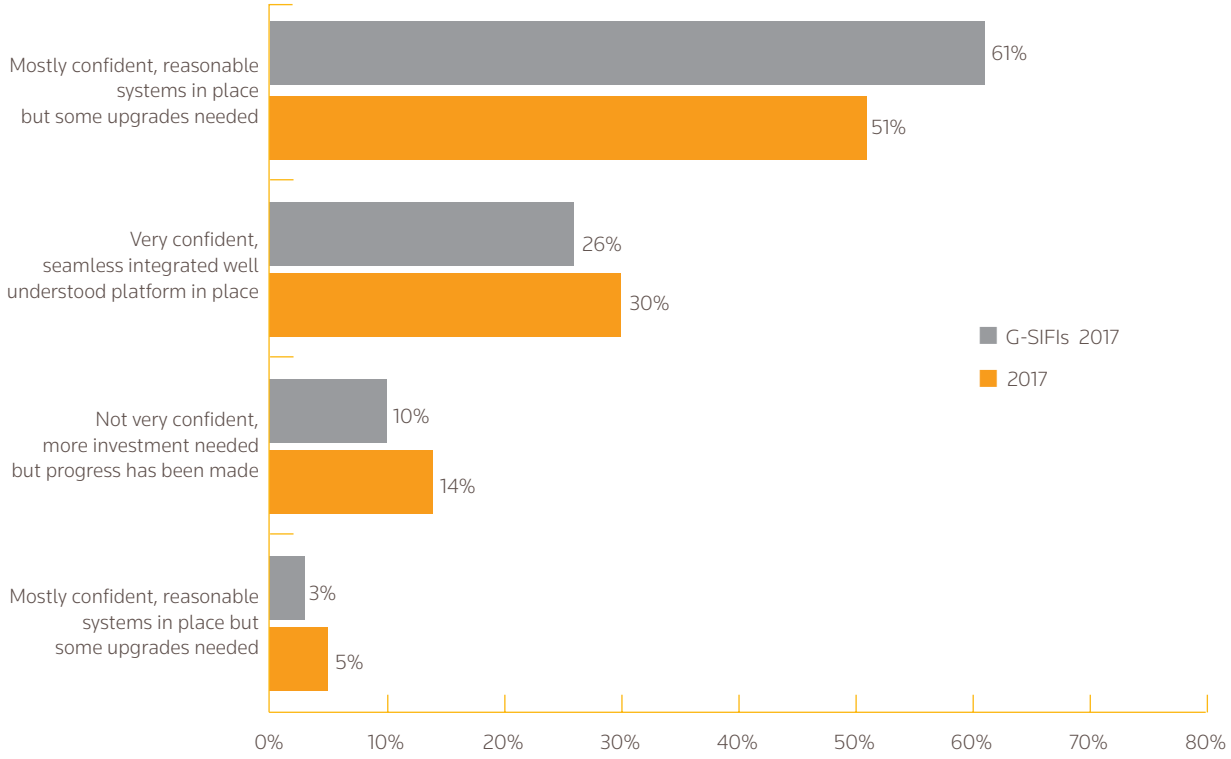
The biggest worry for firms with regard to technology is seen to be the need to upgrade legacy systems. All too many firms have a patchwork quilt of legacy systems with patches, fixes and work-arounds that often need substantial investment to upgrade. The upgrades required are made more challenging by the continuing huge amount of regulatory change absorbing much of the IT change capacity.

Figure 19 - What are the greatest financial technology challenges you expect your company to face in the next 12 months?

Source: Thomson Reuters Regulatory Intelligence – Fintech, Regtech and the Role of Compliance 2017

The balancing of commercial and compliance needs is perhaps at the heart of the issue. Without sufficient appropriate investment in technology and associated skills, firms will not have the infrastructure to enable them to thrive into the medium term, but the potential millstone of legacy systems needs to be tackled to ensure that the firm is able to reap the benefits of all aspects of technological innovation.

Figure 20 - How confident are you that your IT infrastructure is/will be able to support fintech, regtech and insurtech



Source: Thomson Reuters Regulatory Intelligence – Fintech, Regtech and the Role of Compliance 2017

It is a matter of potential concern that less than a third (30 percent in 2017, 26 percent for G-SIFIs) of respondents are very confident in their firms IT infrastructure ability to support fintech, regtech and insurtech. It goes without saying that a stable, seamless, integrated and well-understood platform is needed to ensure the successful and robust deployment of any fintech, regtech or insurtech solution.

Those fifth (19 percent) of respondents who reported being either not very confident or having no confidence at all in their IT infrastructures need to ensure that the issue is escalated, resourced and remediated as soon as is feasible. It is entirely possible that an IT infrastructure with such low confidence ratings will also be the root cause of other risk, compliance and business failings.

Cyber resilience

All things to do with technology risk and associated cyber resilience, whether risk, attack, crime or resilience are never far from the headlines, with companies of all shapes and sizes around the world vulnerable to attacks in the online world. In terms of cyber resilience, cyber risk, cyber crime as well as headline-grabbing cyber attacks, it is perhaps stating the obvious that good customer outcomes will be under threat in the event of a failure of cyber resilience.

The concerns are borne out by the statistics around cyber attacks which show the threat to be increasing, and increasing rapidly. In June 2017, the UK FCA updated its policy approach to cyber resilience and its expectations such that firms should be aware of the threat, able to defend themselves effectively and respond proportionately to cyber events. As part of that update, the FCA quoted a number of statistics to illustrate the increasing threat from cyber attacks, perhaps the most startling of which was the 1,700 percent[4] increase in cyber attacks reported to the regulator since 2014.

4 https://www.fca.org.uk/news/speeches/expect-unexpected-cyber-security-2017-beyond

"The first six months of 2017 have seen an inordinate number of cyber-attacks and they were not just the standard corporate breaches. Already there has been viral, state-sponsored ransomware, leaks of spy tools from US intelligence agencies, targeted denial-of-service attacks and full-on campaign hacking. Unfortunately, this is likely a prelude of more cyber-attacks to come.

Let me share with you some key statistics on cybersecurity:

- The global cost of cybercrime will reach U.S.$2 trillion by 2019, a threefold increase from the 2015 estimate of U.S.$500 billion.
- Last year, cybersecurity researchers estimate that criminals made over U.S.$1 billion through ransomware, with victims ranging from the chief executives of Fortune 500 companies to mom-and-pop businesses and private individuals.
- 1 in 131 emails contained malware in 2016, the highest rate in 5 years.
- 76% of organizations worldwide reported being victim of a phishing attack in 2016.
- Only 38 percent of global organizations claim they are prepared to handle a sophisticated cyberattack.
- Global spending to combat cybercrime will top U.S.$80 billion this year, with organizations increasingly focusing on detection and response."

Mohd Adhari Belal Din, assistant governor of the Central Bank of Malaysia (Bank Negara Malaysia). Remarks at the "Cybersecurity: Safeguarding the Future for Innovative Financial Inclusion" (August 2017)

What had previously often been seen as simply an IT issue has become a key issue for risk and compliance functions around the world, with the FCA stating its goal, in common with many other financial services regulators, to "help firms become more resilient to cyber attacks, while ensuring that consumers are protected and market integrity is upheld."

Figure 21 - Effective Cyber Security Practice

Manage the risk:
You need to know what information you hold and why you hold it. **Is it classifed? Do you review who has access to your most sensitive data? Do you understand your vulnerabilities?**

Encryption:
Protect your sensitive data. **Do you use encryption software to protect your critical information from unauthorised access?**

Disaster recovery:
Backup your critical systems and data, and test backup recovery processes regularly. **Do you know if you are able to restore services in the event of an attack?**

Network and computer security:
Keep systems, software and apps up-to-date and fully patched. **Do you make sure your computer network is confgured to prevent unauthorised access?**

User and device credentials:
Ensure your staff use strong passwords when logging on to hardware and software. Change the default Administrator credentials for all devices **Do you use two-factor authentication where the confidentiality of the data is most crucial?**

Awareness:
People are an integral part of the cyber security chain. **Do you educate your staff on cyber security risks?**

Accreditation:
Gaining a recognised accreditation, such as **Cyber Essentials**, could improve the security of your firm. **Do you align your firm to a recognised cyber scheme?**

Information sharing:
Sharing threat information with your peers, through networks such as the **Cyber Security Information Sharing Partnership (CiSP)**, is a vital tool in strengthening your cyber defences. **Are you a member of any informationsharing arrangements?**

Source: Based on UK Financial Conduct Authority. Infographic: Good Cyber Security – the foundations (June 2017)

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

The 2016 Verizon Data Breach Investigations Report provided an analysis of 2,260 data breaches and 64,199 security incidents from 61 countries. It found that ten vulnerabilities accounted for 85 percent of successful breaches. As part of the analysis, it was found that the vast majority of the vulnerabilities exploited in the attacks were not only well known, but had fixes available at the time of attack. Furthermore, some of the attacks used vulnerabilities for which a fix had been available for over a decade.

In October 2017, the Financial Stability Board reported on a workshop on cybersecurity between public and private sector participants from the financial services sector, noting that "effective cybersecurity requires a strategic, forward looking, fluid and proactive approach. They noted that it is not sufficient to simply look to past incidents and known risks, but that one must evaluate potential future threats. At the same time, participants stated that up to 90% of threats can be mitigated by basic cybersecurity hygiene."

If nothing else, firms need to consider what they would do if the worst happened and they became victims of a sophisticated cyber attack. Carefully thought-through and tested incident management and contingency plans need to be agreed, pre-emptively, at the highest levels of the firm. Such plans should include communication protocols (to media, regulators and customers as well as other stakeholders) and the authority levels needed to invoke disaster or recovery plans (such as, say, the switching of operating systems to a secure back-up location). An inherent part of testing whether planned security measures work is the follow-up investigation to assess any attack and the lessons to be learned.

Figure 22 - 10 Board Principles for Cyber Resilience

World Economic Forum, "Advancing Cyber Resilience: Principles and Tools for Boards". January 2017

Responsibility for cyber resilience
The board as a whole takes ultimate responsibility for oversight of cyber risk and resilience. The board may delegate primary oversight activity to an existing committee (e.g. risk committee) or new committee (e.g. cyber resilience committee).

Command of the subject
Board members receive cyber resilience orientation upon joining the board and are regularly updated on recent threats and trends – with advice and assistance from independent external experts being available as requested.

Accountable officer
The board ensures that one corporate officer is accountable for reporting on the organization's capability to manage cyber resilience and progress in implementing cyber resilience goals. The board ensures that this officer has regular board access, sufficient authority, command of the subject matter, experience and resources to fulfil these duties.

Integration of cyber resilience
The board ensures that management integrates cyber resilience and cyber risk assessment into overall business strategy and into enterprise wide risk management, as well as budgeting and resource allocation.

Risk appetite
The board annually defines and quantifies business risk tolerance relative to cyber resilience and ensures that this is consistent with corporate strategy and risk appetite.
The board is advised on both current and future risk exposure as well as regulatory requirements and industry/societal benchmarks for risk appetite.

Risk assessment and reporting
The board holds management accountable for reporting a quantified and understandable assessment of cyber risks, threats and events as a standing agenda item during board meetings.
It validates these assessments with its own strategic risk assessment using the Board Cyber Risk Framework.

Resilience plans
The board ensures that management supports the officer accountable for cyber resilience by the creation, implementation, testing and ongoing improvement of cyber resilience plans, which are appropriately harmonized across the business. It requires the officer in charge to monitor performance and to regularly report to the board.

Community
The board encourages management to collaborate with other stakeholders, as relevant and appropriate, in order to ensure systemic cyber resilience.

Review
The board ensures that a formal, independent cyber resilience review of the organization is carried out annually.

Effectiveness
The board periodically reviews its own performance in the implementation of these principles or seeks independent advice for continuous improvement.

Source: Based on World Economic Forum. Report: Advancing Cyber Resilience – Principles and Tools for Boards (January 2017)

Data Protection

Firms around the world are on notice that the regulatory focus on data protection is set to increase with the implementation of the General Data Protection Regulation (GDPR) in May 2018. The importance of data protection and information security was already increasing with concerns about cyber resilience and technology risk, with millions of individuals finding that their personal information had been stolen or otherwise compromised.

The GDPR introduces a raft of changes with a deliberately extra-territorial reach outside of the European Union as it covers all online dealings with EU citizens, no matter where in the world the business takes place. There are enhanced consent requirements, a right to be forgotten, increased portability rights and reporting requirements if a breach occurs. The increased obligations come with increased penalties of up to 20 million euros or 4 percent of global annual turnover for the worst offenses.

Figure 23 - Preparing for the General Data Protection Regulation (GDPR)

1. Awareness
You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2. Information you hold
You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3. Communicating privacy information
You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4. Individuals' rights
You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5. Subject access requests
You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6. Lawful basis for processing personal data
You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7. Consent
You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8. Children
You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9. Data breaches
You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10. Data Protection by Design and Data Protection Impact Assessments
You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation

11. Data Protection Officers
You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12. International
If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

Source: Information Commissioner's Office. Guidance: Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now (April 2017)

"Those organizations which thrive in the changing environment will be the ones that look at the handling of personal information with a mindset that appreciates what citizens and consumers want and expect. That means moving away from looking at data protection as a tick box compliance exercise, to making a commitment to manage data sensitively and ethically. When you commit, compliance will follow."

Elizabeth Denham, UK Information Commissioner. Speech - at the Institute of Directors Digital Summit (October 2017)

Closing thoughts

> "The rise of automation and journey towards AI raises the serious question about what might go wrong, and if it does, who will be accountable? We need to make sure we do not neglect this issue of accountability. Firms need to be held accountable in the same way they would for any breach."
>
> **Greg Medcraft, Chairman of the Australian Securities and Investments Commission (ASIC). Speech - "The importance of trust in a digital world" at the Stockbrokers and Financial Advisers Conference (May 2017)**

Technology permeates every aspect of financial services, bringing with it both challenges and opportunities. Fintech, regtech and insurtech are beginning to become common currency with regulators and firms alike, and the need for technological skills is ever more critical. Risk and compliance functions must understand how their roles are evolving and the ramifications of the shifting regulatory expectations which are seeking to encourage the next generation of technology and its uses. Firms need to appreciate that the investment in technological skills and solutions is set against a backdrop of both changing data protection requirements, increasing concern about cyber risk and, critically, with a growing specter of personal liability for senior managers. For many firms, cyber resilience and technology risk have already found a place on the board agenda.

There are extensive potential benefits from the successful deployment and use of technology with improved efficiency and productivity, together with greater commercial opportunities at the top of the pile. Other perceived benefits include advancing technology and better systems, better compliance practices and better customer interactions and outcomes. All of which could be a competitive advantage.

That competitive advantage comes at a cost and with a number of challenges. The greatest challenge is seen as the need to upgrade legacy systems, the challenge being all the greater for concerns about budgetary limitations and cost. In addition are the near universal challenges for financial services firms of cyber resilience and technology risk, the need to balance commercial and compliance needs, together with the continuing requirement to implement regulatory change.

Compliance functions have seen their roles and remits grow and change out of all recognition in the last decade. They have weathered the financial crisis, seen unprecedented volumes of regulatory change and now need to adapt to the wave of technological innovation sweeping financial services. The early signs of fragmentation highlighted in the 2016 report between the adopters and rejecters of fintech appear to have dissipated, with a shift towards more widespread budget availability and compliance engagement in 2017. There are no quick fixes, but compliance functions need to continue to work towards the goal of being able to reap the benefits of carefully selected, robustly deployed regtech solutions hosted on an upgraded, stable and seamless IT infrastructure.

About the authors

Stacey English is head of regulatory intelligence for Thomson Reuters with 20 years of regulatory compliance, risk and audit experience in financial services as a regulator and practitioner.

uk.linkedin.com/in/stenglish @regexperts @regulatorydata

https://blogs.thomsonreuters.com/financial-risk/authors/stacey-english/

Susannah Hammond is senior regulatory intelligence expert for Thomson Reuters with more than 25 years of wide-ranging compliance, regulatory and risk experience in international and UK financial services.

uk.linkedin.com/in/susannahhammond @SannaHamm

https://blogs.thomsonreuters.com/financial-risk/authors/susannah-hammond/

Visit risk.tr.com