Fintech, Regtech and the Role of Compliance in 2022:

Challenges arising from technological opportunities

By Susannah Hammond and Mike Cowan

THOMSON REUTERS®

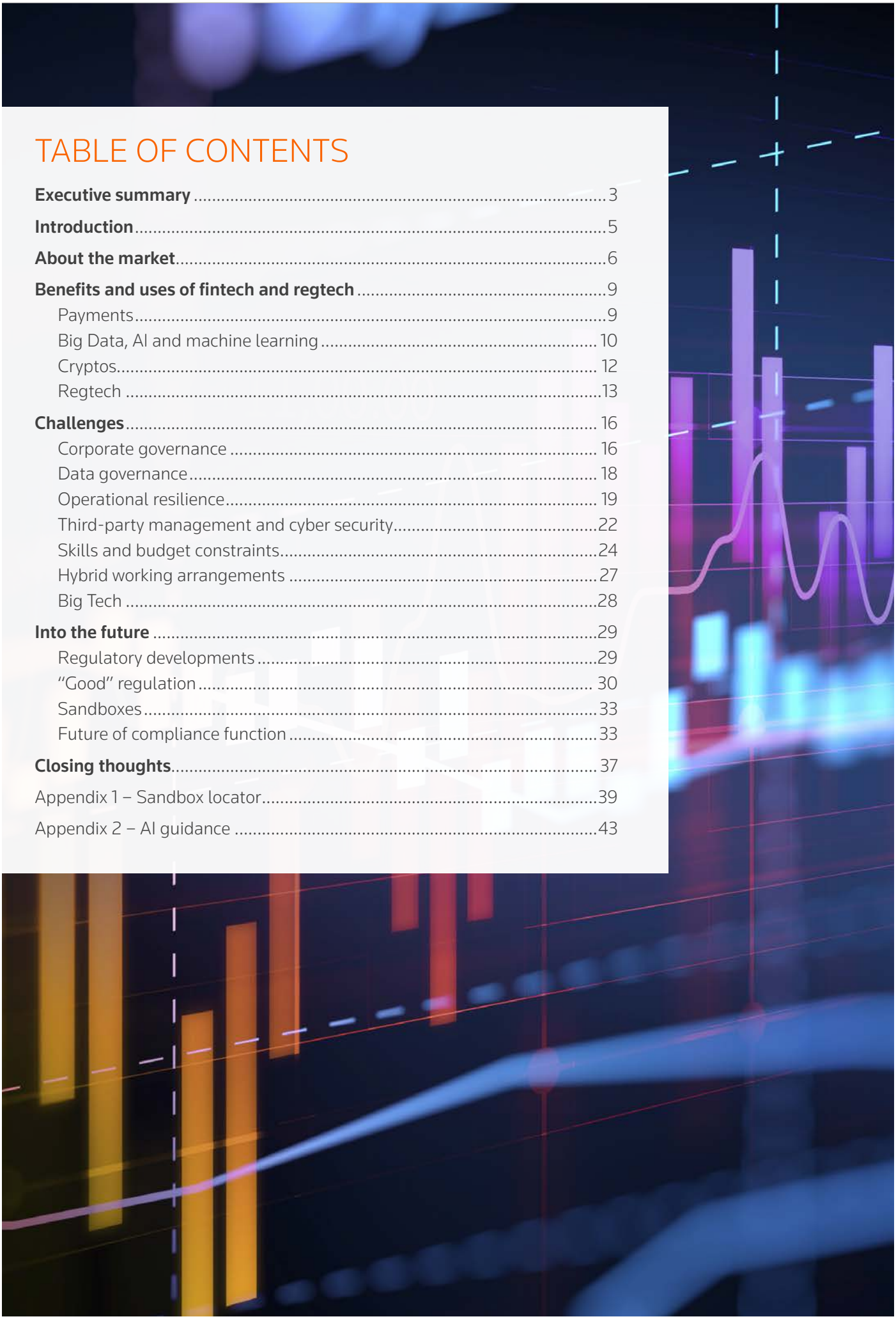


TABLE OF CONTENTS

Executive summary 3

Introduction 5

About the market 6

Benefits and uses of fintech and regtech 9

- Payments 9
- Big Data, AI and machine learning 10
- Cryptos 12
- Regtech 13

Challenges 16

- Corporate governance 16
- Data governance 18
- Operational resilience 19
- Third-party management and cyber security 22
- Skills and budget constraints 24
- Hybrid working arrangements 27
- Big Tech 28

Into the future 29

- Regulatory developments 29
- "Good" regulation 30
- Sandboxes 33
- Future of compliance function 33

Closing thoughts 37

Appendix 1 – Sandbox locator 39

Appendix 2 – AI guidance 43

EXECUTIVE SUMMARY

Digital transformation has been a fundamental enabler for financial services firms. It is hard to underestimate the opportunities firms can derive from the implementation of technological solutions but maximising their potential can present challenges. Regulatory Intelligence's (RI) sixth annual survey and report on fintech, regtech and the role of compliance explores these challenges, particularly in the context of corporate governance and risk management.

The most significant challenges highlighted by respondents to this year's survey concerned data, operational resilience, the management of third parties and skill sets.

- **Data** — Data is the strategic asset of the digital age, and firms need to embed data governance frameworks as a core competency within their corporate governance arrangements.
- **Operational resilience** — Digital solutions, which at times operate critical business functions, must be resilient to any disruption. Equally, risk and compliance applications must be able to accommodate any shift to alternative working patterns.
- **Third parties** — Third parties are crucial to the development of many fintech applications. Outsourcing or third-party arrangements need to be part of firms' risk management infrastructure.
- **Skill sets** — Firms need to invest in more specialist technological skills, although determining what those skills should be is a challenge in its own right.

Growth of the marketplace

Overall, respondents were enthusiastic about the use of applications. This year's survey painted a picture of a well-populated marketplace and some compelling business cases for fintech use in many sectors.

This year's survey identified the top three uses for fintech as payments, information/data security and customer relationship management, and for Global Systemically Important Financial Institutions (G-SIFIs) as payments, product development and, equal third, information/data security and recordkeeping.

Regtech is a subset of fintech, and this year the survey questions were flexed to separate out some of the answers between regtech and wider fintech applications. Respondents reported that regtech solutions were having a growing impact on the management of compliance.

At a firm level, regtech applications were mainly being used for compliance monitoring and anti-money laundering (AML)/sanctions checking. At a compliance function level, applications were being used for compliance monitoring, regulatory reporting, financial crime (including AML/counter-terrorism financing (CTF) and sanctions), as well as onboarding and know-your-customer (KYC).

The impact of regulatory change also featured strongly, with around a third of firms reporting that regtech will affect the implementation of regulatory change, the way it is captured and the way regulations and their impact are interpreted.

Regulatory environment

Many jurisdictions have already introduced detailed regulations — notably for payment systems — with which firms must comply, whether they use fintech solutions or not. A dedicated regulatory framework for fintech applications is evolving but is disparate and varies from jurisdiction to jurisdiction.

This year's survey asked respondents about what they saw as the main elements of an effective regulatory approach for both fintech and regtech. The hallmark of "good" regulation was seen to be regular interaction between regulator and industry. Many issued a plea for greater international coherence in terms of the regulatory approach to both regtech and fintech.

Data governance and cyber resilience were considered to be the main areas where additional regulation and guidance was needed. This was mirrored by respondents' feedback concerning the greatest financial technology challenges they expect their firms to face in the next 12 months, which were data governance, availability of skills, cyber resilience and regulatory approach.

Looking forward

The establishment of a well-resourced compliance function that can successfully navigate the use of digital solutions will be one of the best investments a firm can make. The governance of vast quantities of data, alongside regulatory change, increasing cyber risk and threats from Big Tech, is certain to drive more widespread use of technological solutions in the coming years.

INTRODUCTION

> *"Digitalization is not confined to the banking industry, of course. But it has already left a strong imprint on banks, and all signs point to even more sweeping changes ahead."*
>
> **Andrea Enria, chair of the Supervisory Board of the European Central Bank, September 2021**

The fintech, regtech and the role of compliance survey has, in its lifetime, attracted more than 2,500 respondents. Almost 450 respondents from all sectors of financial services — from G-SIFIs to technology start-ups — took part in this sixth survey. As G-SIFIs are often seen as a leading indicator of future behaviour, they were asked to identify themselves, to enable comparison with other, smaller, firms. As with previous reports, regional and G-SIFI results are split out where they highlight a particular trend.

The survey results are intended to help financial services firms with planning, resourcing and direction, allowing them to benchmark whether their approach, skills, strategy and expectations are in line with those of the wider industry.

The latest survey looks at how fintech is being used in 2021/2 and provides a snapshot of the marketplace. This year, new questions have been included to explore how firms and their compliance functions use technology, and how they would like to be able to use it. New questions assess the relationship between firms and regulators when it comes to technology, and what "good" is beginning to look like for the regulation of fintech and regtech.

The report assesses the extent to which firms are turning the technological challenges they face into opportunities, embracing the new ways of working and navigating the evolving regulatory approach. The report homes in on areas that directly affect the compliance function.

Where permission was received, quotes (some anonymized) from respondents have been included where they highlight specific issues.

ABOUT THE MARKET

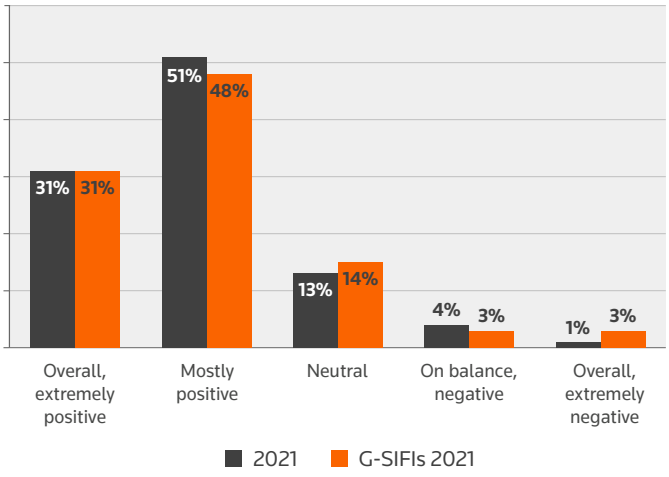
In 2018, it was estimated that the international fintech market was worth circa $130 billion, and was predicted to grow significantly in the following four years. The pandemic certainly affected this growth, but the fintech sector coped better than many industries. Investment in fintech applications topped $40 billion in 2020 (an increase on 2019).

In September 2021 the Bank for International Settlements (BIS) issued a paper entitled, "Funding for Fintechs: Patterns and Drivers". "Fintechs have raised over $1 trillion in equity in more than 35,000 deals globally since 2010," the BIS said. Bringing the figures up to date, the BIS pointed out that "by 2020, the capital raised by fintechs reached 5% of the value of global equity deals, up from less than 1% in 2010".

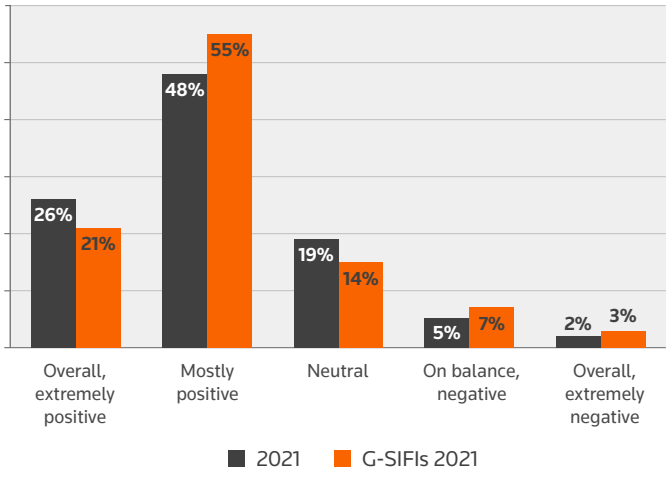
The BIS report commented on the diversification among fintechs, noting that "equity funding for fintechs is higher in countries with more innovation capacity and better regulatory quality". The United States, the European Union (EU), the UK and China remain the main locations where fintech is flourishing, it said.

FIGURE 1:

Fintech: What is your view of innovation and digital disruption?



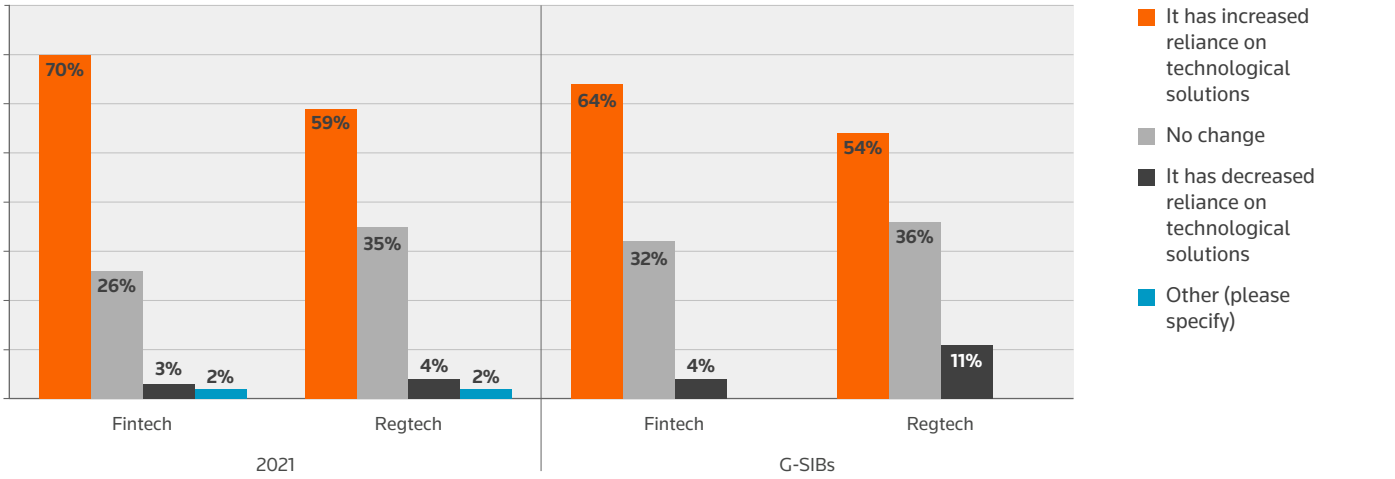
Regtech: What is your view of innovation and digital disruption?



Source: Thomson Reuters 2021

As in previous years, respondents were "mostly positive" about the fintech market, and about regtech in particular. The majority acknowledged that more widespread use of fintech applications was necessary in future. Some 70% said the pandemic had influenced their use of fintech applications, and 64% said the same with regards to regtech applications.

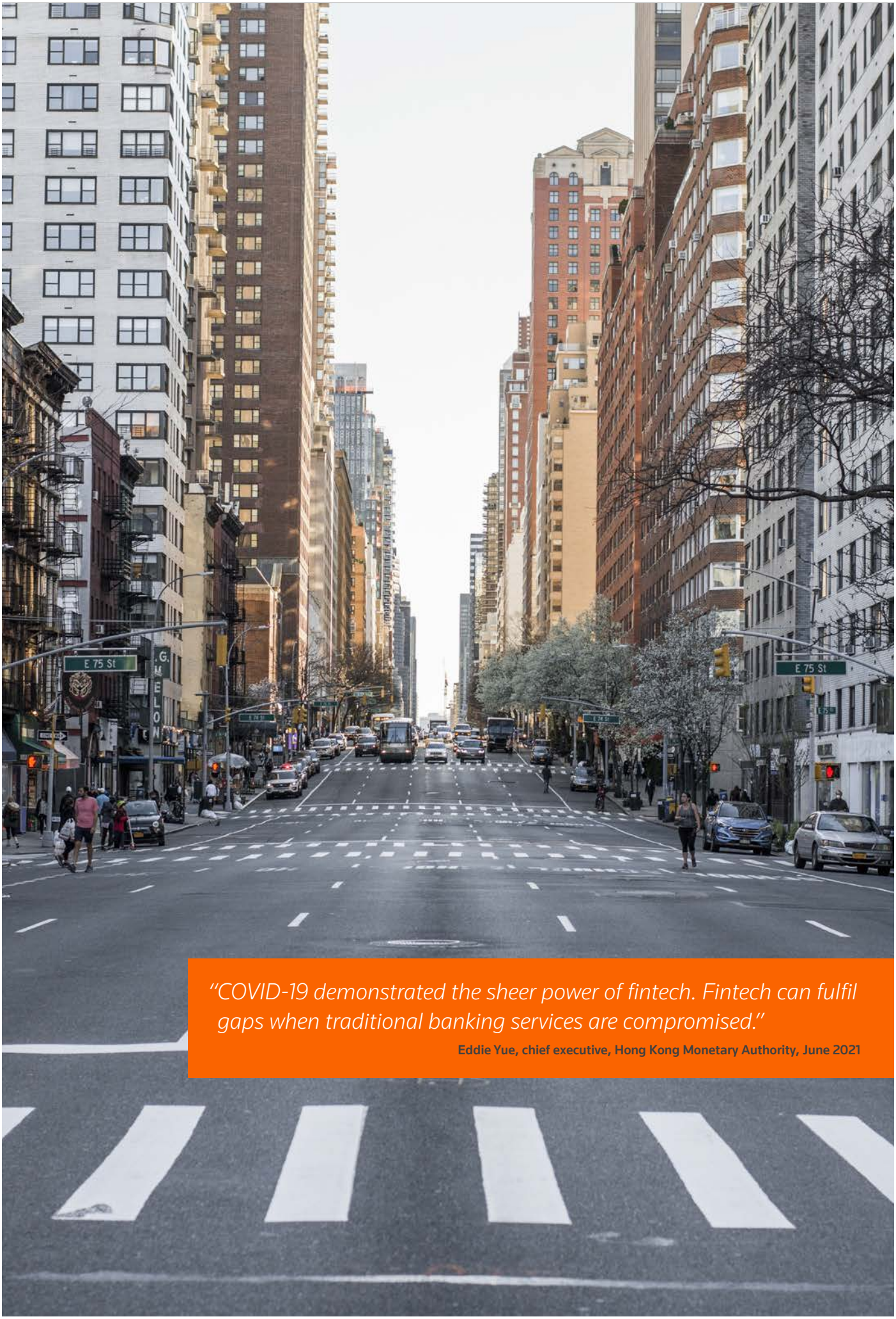
FIGURE 2:
How has the pandemic impacted your firm's use of technological solutions?



Source: Thomson Reuters 2021

Many firms said the pandemic had increased their reliance on technological solutions, although around a third reported no change. Given the disruption caused, these results suggest a heightened state of preparedness such that some firms already had sufficient levels of technological sophistication.

For many firms, the use of technology to support compliant activities remains work-in-progress. Firms are using fintech and regtech solutions to undertake, and evidence, rote compliance activities, freeing up time which compliance officers can devote to more value-add activities such as assessing the impact of regulatory change. Compliance officer time is also being devoted to the consideration of the various forms of technology, a process which often highlights the need for investment in specialist, preferably in-house, skill sets.



"COVID-19 demonstrated the sheer power of fintech. Fintech can fulfil gaps when traditional banking services are compromised."

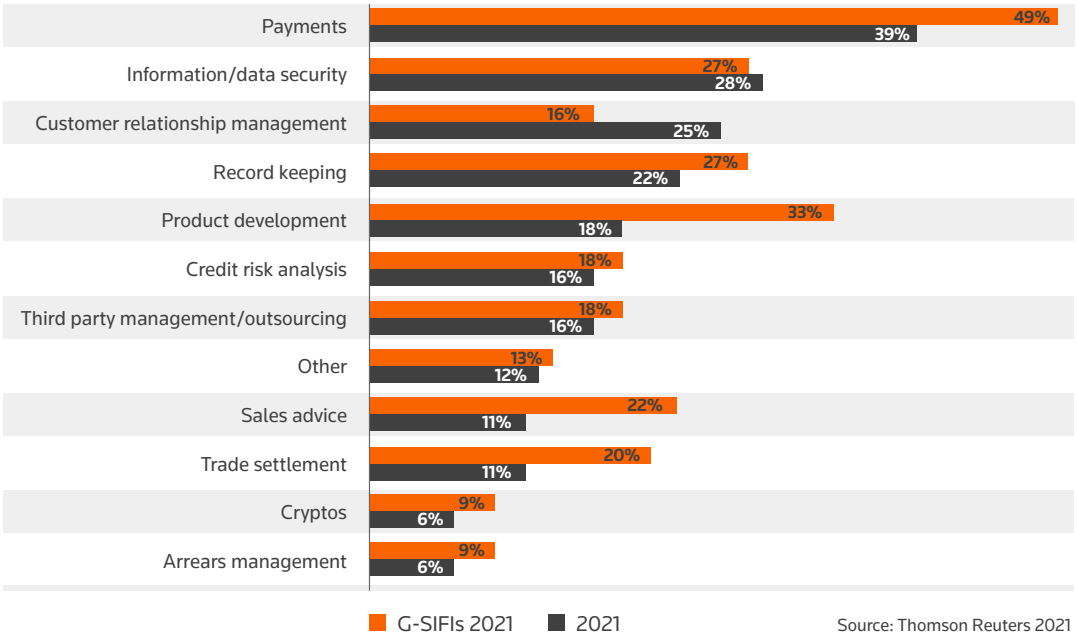
Eddie Yue, chief executive, Hong Kong Monetary Authority, June 2021

BENEFITS AND USES OF FINTECH AND REGTECH

Fintech solutions have been applied to several operational applications which have the customer at the centre of their use. Just under half (49%) of G-SIFIs and 39% of all firms listed payments as the main purpose for using fintech. This was closely followed by information and data security for all firms (28%) and product development for G-SIFIs (33%).

More than half of respondents based in the Middle East (57%) and Africa (53%) were using fintech for payments, compared with 18% in Continental Europe and 14% in Australasia.

FIGURE 3:
What are you using fintech for?



Source: Thomson Reuters 2021

Payments

Whether motivated by the pandemic or by advances in technology, the use of automated payment system applications has increased, providing customers with more convenient ways of payment while reducing the cost of transaction handling for firms. The significant increase in the number of payment service operators has, however, been accompanied by a parallel increase in fraud, and has given rise to data security, operational resilience and third-party management concerns — topics that are covered in the next section.

Payment services can have both regulated and non-regulated elements, and compliance officers need to be able to distinguish between the two and apply risk assessments as appropriate.

The operation of payment systems is governed by a plethora of rules and guidance across different jurisdictions. For example, in 2021 the UK laid the draft Payment and Electronic Money Institution Insolvency Regulations 2021 before parliament and the European Commission consulted on an EU-wide instant payments scheme.

The International Monetary Fund (IMF) and the BIS have also issued guidance on how applications should operate, to try to establish best practice.

In May 2020, the IMF's paper, "Fintech and Payments Regulation: Analytical Framework", introduced a four-step process for regulating payment services:

1. **Identifying payment activities** — activities are organised into six groups: (i) account issuance; (ii) electronic money issuance; (iii) domestic funds transfer; (iv) cross-border funds transfer; (v) merchant acquisition; and (vi) digital payment tokens.
2. **Licensing entities and designating systems** — the provision of payment solutions (including through fintech applications) is mainly regulated through individual jurisdictional licensing arrangements. In the UK, payment service providers need to be authorized by the national regulators. In the United States, both national and state regulators have a responsibility for licensing and regulating money transmission providers.
3. **Analyzing and managing risks** —risks can fall under five categories: funds protection, financial integrity, cyber/data security, access to payment systems and interoperability.
4. **Promoting legal certainty** — there must be a sound legal framework for payment systems.

"Financial authorities now face the task of deciding whether the risk profile of different payment services is appropriately reflected in their regulatory frameworks," the BIS said in a July 2021 paper on regulating digital payment services and e-money.

> *"With their technical expertise and financial muscle, BigTech companies can potentially be catalysts for sweeping changes in the financial sector. They are able to bundle a range of services, while making use of the information customers have left behind to target their services more directly to each one."*
>
> **Ida Wolden Bache, deputy governor of Norges Bank (Central Bank of Norway), May 2021**

Big Data, AI and machine learning

There is a distinction between Big Data and Big Tech. The two overlap, but Big Data and its use in association with AI and machine learning can be beneficial for firms. The threat posed by Big Tech, i.e., the activities of the large IT players in the financial services sector, is a risk that financial services firms need to consider. This section considers Big Data and AI. The challenges posed by Big Tech are included in the next section.

The German regulator, BaFin, has introduced principles for the use of algorithms. These include:

- Clear management responsibility
- Appropriate risk and outsourcing management
- Preventing bias and ruling out types of differentiation that are prohibited by law
- Data strategy and data governance
- Compliance with data protection requirements
- Ensuring accurate and reproducible results
- Documentation to ensure clarity for both internal and external parties
- Appropriate validation processes
- Using relevant data for calibration and validation purposes

Artificial intelligence is another area where fintech applications are seen to add value to stakeholders. The European Commission, for example, has announced significant investment in AI applications, although the EU has also recognized that this investment needs to be accompanied by a strong regulatory framework.

Compliance officers should take note of the components of the proposed regulatory structure. They include not only existing legislation such as the General Data Protection Regulation (GDPR) but also "the use of high-quality datasets, the establishment of appropriate documentation to enhance traceability, the sharing of adequate information with the user, the design and implementation of appropriate human oversight measures, and the achievement of the highest standards in terms of robustness, safety, cyber security and accuracy"[1].

Appendix 2 of this report provides a practical introduction to AI and machine learning.

> *"AI spending is forecast to double by 2024, growing from $50.1 billion in 2020 to over $110 billion in 2024. The forecasted compound annual growth rate (CAGR) for this period is approximately 20%. Furthermore, worldwide revenues for the AI market, including software, hardware and services, are forecast to grow to $327.5 billion in 2021 and reach $554.3 billion by 2024 with a five-year CAGR of 17.5%."*
>
> **"*Realize the Full Potential of Artificial Intelligence*", a report commissioned by the Committee of Sponsoring Organizations of the Treadway Commission, September 2021**

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021DC0205

Cryptos

As of the third quarter of 2021, cryptos were estimated to be an asset class worth $2.1 trillion. Cryptos could, if they fulfil their potential, drive considerable positive change in the financial services sector by making payments and transfers more efficient.

> *"While I'm technology-neutral, I am anything but public-policy neutral. As new technologies come along, we need to be sure we're achieving our core public policy goals. Further, for those who want to encourage innovations in crypto, I'd like to note that financial innovations throughout history don't thrive long outside of public policy frameworks. In finance, that's about protecting investors and consumers, guarding against illicit activity, and ensuring financial stability."*
>
> **Gary Gensler, chair, U.S. Securities and Exchange Commission, September 2021**

The speed and reach of transactions, however, together with the potential for anonymous activity and for transactions without financial intermediaries, also make crypto-assets vulnerable to misuse, and raise the risk of money laundering.

Policymakers, regulators and firms must all play their part in ensuring that cryptos are as "safe" as possible, not only in terms of investment risk but also with regards to regulatory certainty and cyber resilience.

Supranational policymakers must continue to work toward consistent definitions of what falls within the regulatory perimeter. Under current regulatory regimes, cryptos may be treated as a currency, an investment or a security, or they may not be covered at all. Cryptos, and bitcoin in particular, may have gone mainstream, but there is a need for clarity in terms of how they are supervised.

A good first step would be alignment on definitions. Even if jurisdictions decide to ban some or all cryptos (particularly for retail customers), it would be on the basis that international financial services had a common understanding of what was legal, and where.

> *"... there is no such thing as cryptocurrencies, they are all crypto-assets"*
>
> **Christine Lagarde, president of the European Central Bank, at a Reuters Newsmaker with Christine Lagarde, April 2021**

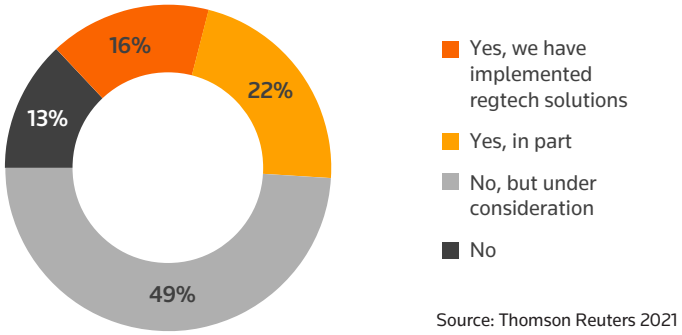
Several countries — notably Singapore, Bermuda, the EU and the UK — are at the forefront of crypto-asset adoption and are establishing themselves as crypto-friendly. Parts of Africa and India, meanwhile, have taken steps to restrict or prohibit citizens from owning or using cryptos.

Harmonization or coordination of rules will be essential, but may not happen for some years. In the interim, the regulatory landscape for digital assets will evolve, probably not as rapidly as some desire and likely at a much slower pace than the technology itself.

Regtech

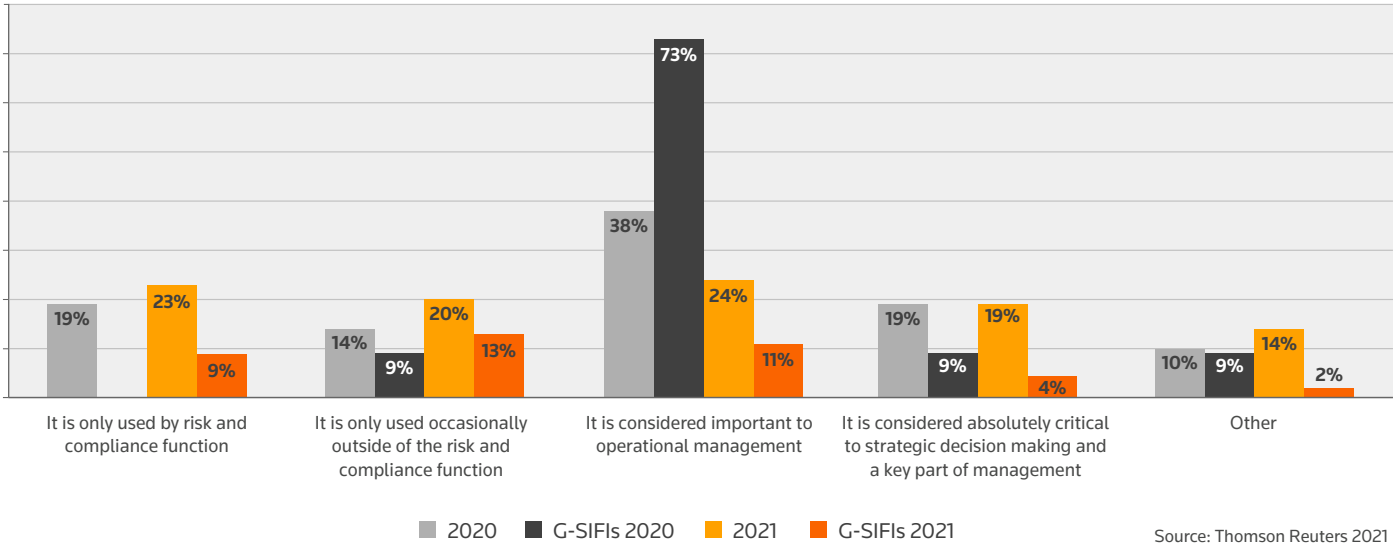
Respondents reported that regtech solutions were increasingly having an impact on the management of compliance. Almost half (49%) are now considering regtech solutions to manage compliance, up from 34% in the previous year. This is the highest since the question was first included in the 2016 survey, when 21% of respondents had regtech solutions under consideration.

FIGURE 4:
Are regtech solutions impacting how you manage compliance?



Source: Thomson Reuters 2021

FIGURE 5:
How is the output from regtech used within your firm?

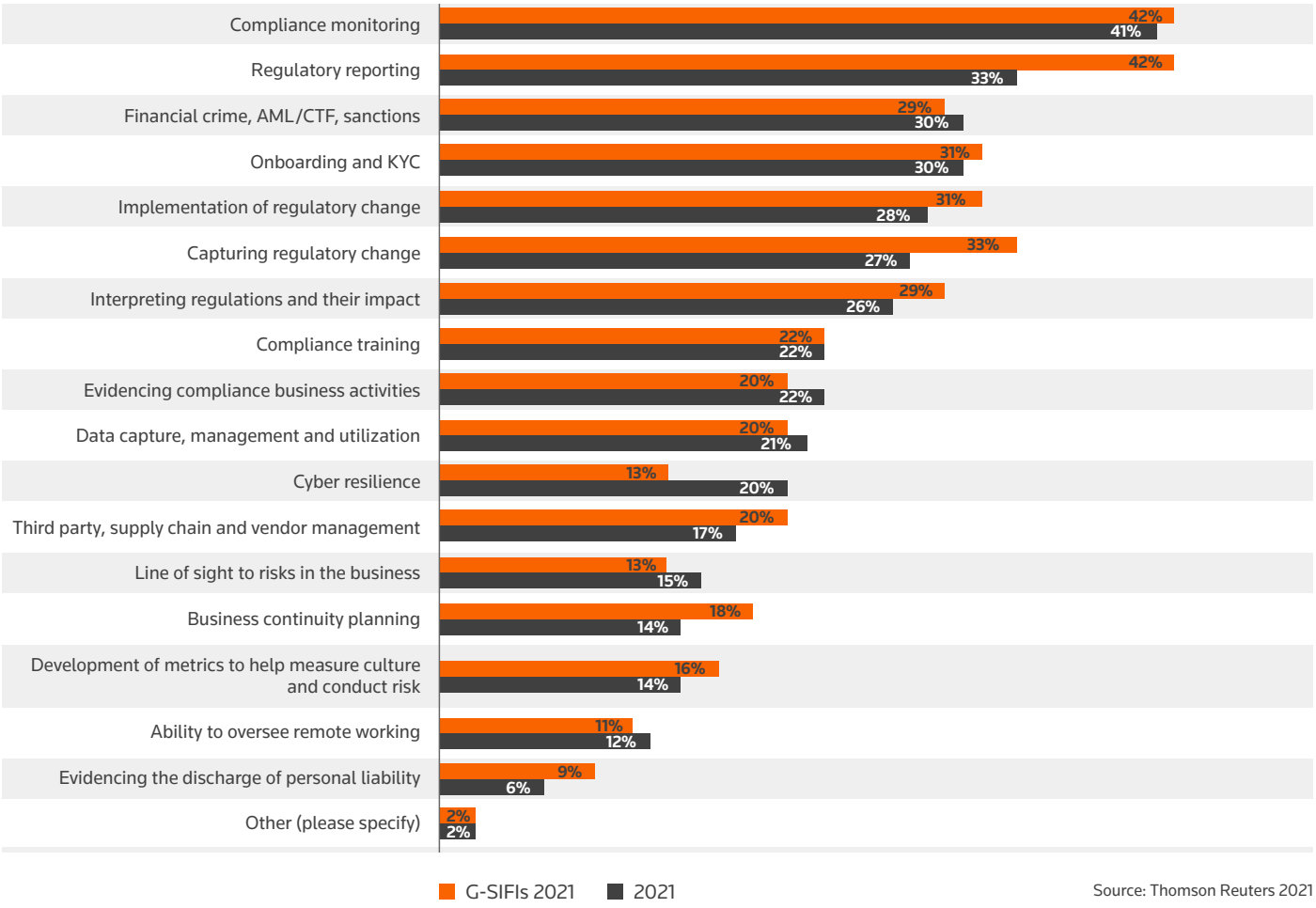


Source: Thomson Reuters 2021

The ways firms use the outputs from regtech solutions has varied over time, and while more firms are considering the adoption of regtech solutions, the output from those solutions already in use has yet to become a trusted source of management information. It may be that the solutions need to be further embedded and tested, or that at least some of the solutions deployed have failed to live up to their potential.

Respondents nevertheless reported that regtech solutions were likely to be used in a wide range of compliance procedures within their firms. At the top was compliance monitoring and regulatory reporting, followed by financial crime and onboarding, as well as elements of regulatory change management.

FIGURE 6:
Which part of compliance and regulatory risk management is most likely to be impacted by regtech at your firm?



Source: Thomson Reuters 2021

These results are reflected in responses about the solutions being introduced, to meet the compliance needs of automated governance, risk and compliance (GRC) solutions: financial crime, AML/CTF and sanctions compliance and the capturing and implementation of regulatory change (regulatory change management).

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

"... GRC technology to monitor compliance and manage frameworks, registers, and monitor risks."

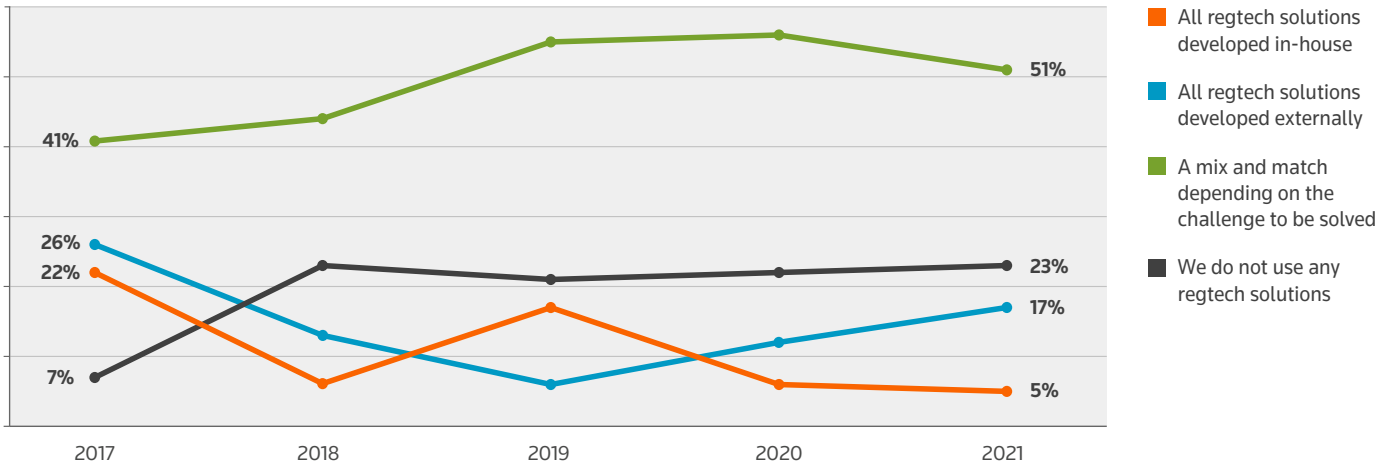
Head of risk and compliance, Australia

FIGURE 7:
What solution have you introduced/are in the process of introducing and to meet what compliance need?

Source: Thomson Reuters 2021

Most firms are developing regtech solutions through a mixture of external and in-house initiatives, 41% in 2017, moving up to 51% this year. The percentage of firms developing all regtech solutions in-house has fallen to 5%, perhaps once again highlighting the dearth of in-house specialist technology skills.

FIGURE 8:
Are you developing regtech solutions in-house or are you looking at external solutions?



Source: Thomson Reuters 2021

A total of 23% of respondents reported not using any regtech solutions. There could be several local reasons for this, including size of firm, availability of budget and compatibility of legacy IT systems. As the digital transformation of financial services continues apace, however, those who opt not to adopt technological solutions may well find themselves at a strategic and economic disadvantage.

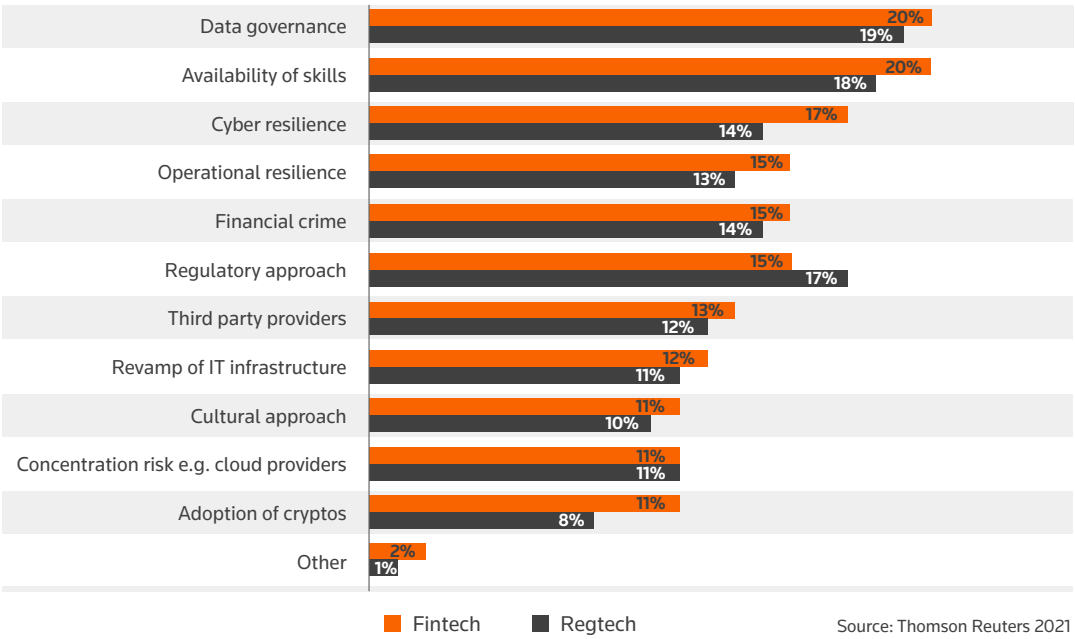
CHALLENGES

> *".. the market learned to adapt, fast. At the Bank our main base for operations has been 'home' ever since. As we plan for the future, we do want staff to come back to the office and interact in person. But there is no vision to return to the world of January 2020."*
>
> **Rohan Churm, head of the Foreign Exchange Division at the Bank of England, July 2021**

Data governance (20% fintech, 19% regtech) and availability of skills (20% fintech, 18% regtech) were listed as the top challenges firms expect to face in the next 12 months with regards to fintech and regtech. For G-SIFIs, availability of skills ranked slightly higher for fintech (22%). Cyber resilience came in third, with 17% for fintech and 14% for regtech, although adoption of cryptos came in third for G-SIFIs (20%).

Data governance was listed as one of the greatest fintech challenges among firms in Asia (31%), compared with just 5% for firms in the Middle East.

FIGURE 9:
The greatest financial technology challenges you expect your firm to face in the next 12 months are...



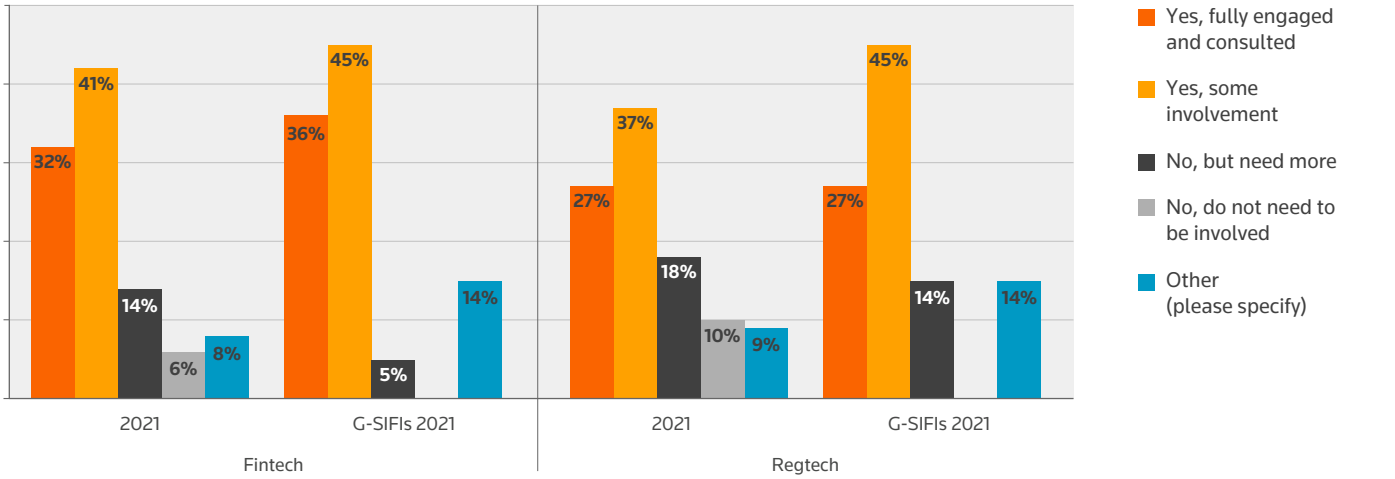
Source: Thomson Reuters 2021

Corporate governance

Last year's report highlighted the need for strong corporate governance within firms, and this year's report continues that theme. Respondents identified the need for both boards and risk and compliance functions to be involved with fintech and regtech initiatives.

Almost three-quarters (73%) of boards were involved with their firm's approach to fintech (81% G-SIFIs), while 64% were involved with regtech (72% G-SIFIs). Almost a third (32%) were fully engaged and consulted at board level on matters related to fintech, compared with 27% for regtech.

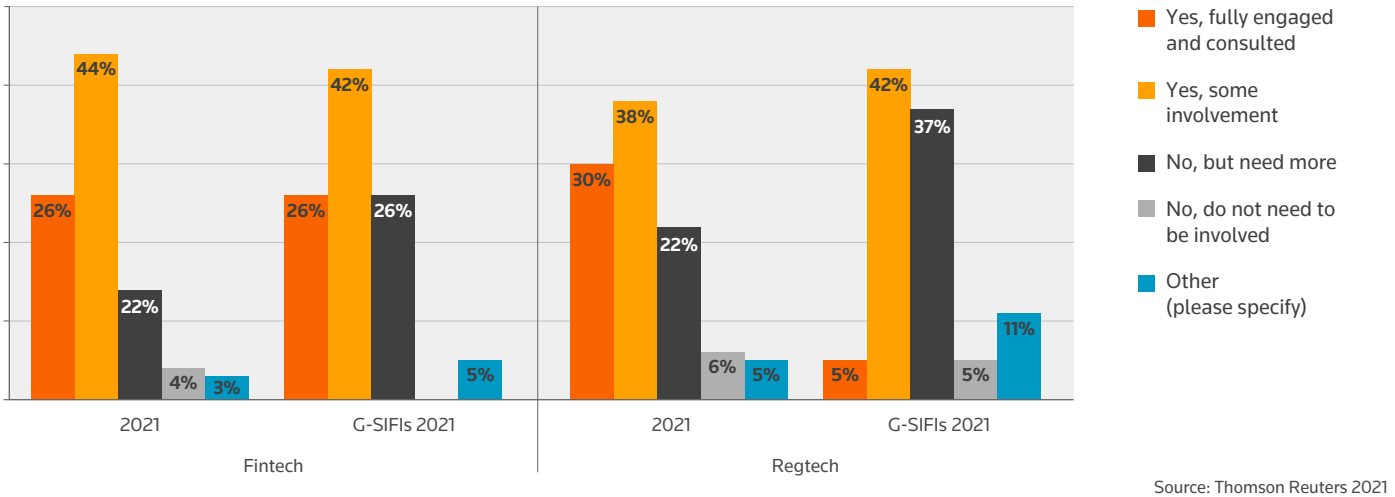
FIGURE 10:
Does your board have enough involvement in your firm's approach to fintech, regtech?



Source: Thomson Reuters 2021

For the risk and compliance functions, 70% were involved in their firm's approach to fintech, with 26% fully engaged and consulted. While 68% were involved in their firm's approach to regtech, 30% were fully engaged and consulted.

FIGURE 11:
Do the risk and compliance functions have enough involvement with your firm's approach to fintech and regtech?

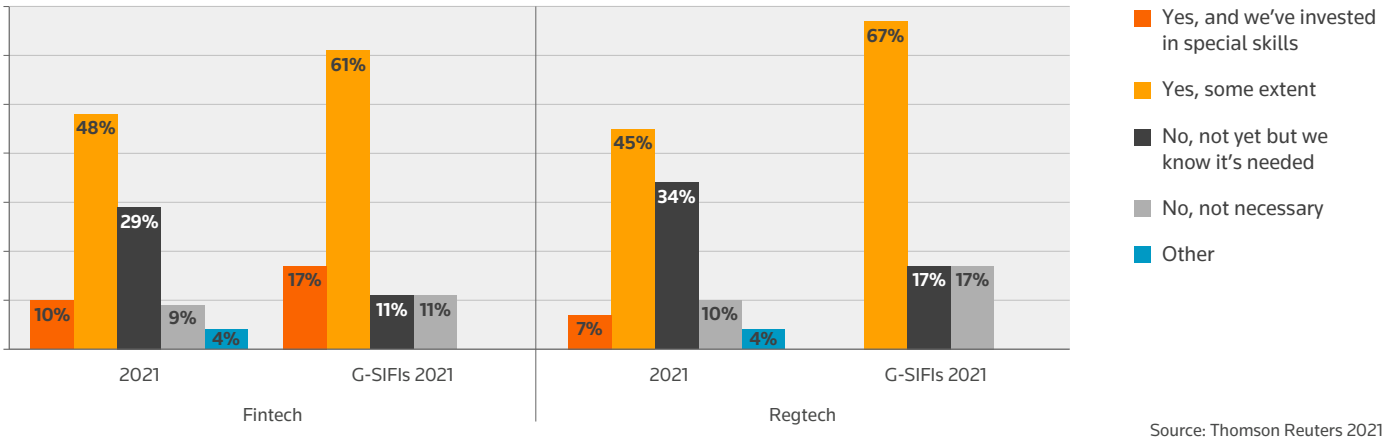


Source: Thomson Reuters 2021

Investment in specialist skills remains difficult for many firms. The survey separated out responses for fintech and regtech innovation and digital disruption. Just 10% of firms had widened the skill set of their risk and compliance function to accommodate developments in fintech innovation and digital disruption, and only 7% had done so for regtech innovation. Despite this year's split, previous years have shown similar trends, with just 15% investing in specialist skills in 2020 and 16% in 2019. G-SIFIs were slightly ahead, but there is still much room for improvement.

Firms in the Middle East are far ahead of peers, with 43% widening skill sets within the risk and compliance functions and investing in specialist skills.

FIGURE 12:
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 2021

Data governance

What is the one thing you would like technological innovation to be able to deliver for your firm in the next 12 months?

"Better insight into what data we have and where it is retained."

Senior director, United States

Risk and compliance and the proper functioning of activities such as trading and reporting and risk management depend on the security, accuracy, timeliness and integrity of data.

Data risk can take many forms, and depends on the specifics of an organization, the way it manages technology and its framework for governing data. Firms and their compliance officers may wish to consider the following sources of risk when deciding their approach to data governance:

- **Business continuity and operational risk** — dependence on critical data sources can lead to significant loss of capability should those sources be interrupted or corrupted.
- **Security and confidentiality risk** — ineffective controls for the protection of data can result in inadvertent disclosure or unauthorized access to data, either internally or externally.
- **Commercial trading risk** — both humans and machines rely on accurate data to achieve optimal outcomes in trading, investing and risk management.
- **Aggregate exposure risk** — occurs when data pertaining to risk positions in different parts of a firm, or running through different systems, cannot be aggregated into a consistent, centralized picture of risk exposure in a timely way. This could give rise to significant and unanticipated firm-wide exposures.
- **Regulatory enforcement risk** — regulators are taking punitive action against firms which consistently fail to meet their reporting obligations in an accurate and timely manner. Firms that are unable to map their data accurately to the requirements of multiple different reporting obligations risk financial, reputational and regulatory consequences. Regulators can take enforcement action for a range of other data-related failures that lead to operational instability, lack of transparency and conduct issues.
- **Ownership and rights risk** — ambiguity and misunderstanding of commercial rights regarding data is an increasing risk.
- **Security and conduct risk** — this results from inadequate controls over permissions for access and manipulation of data which may lead to opportunities for misconduct.

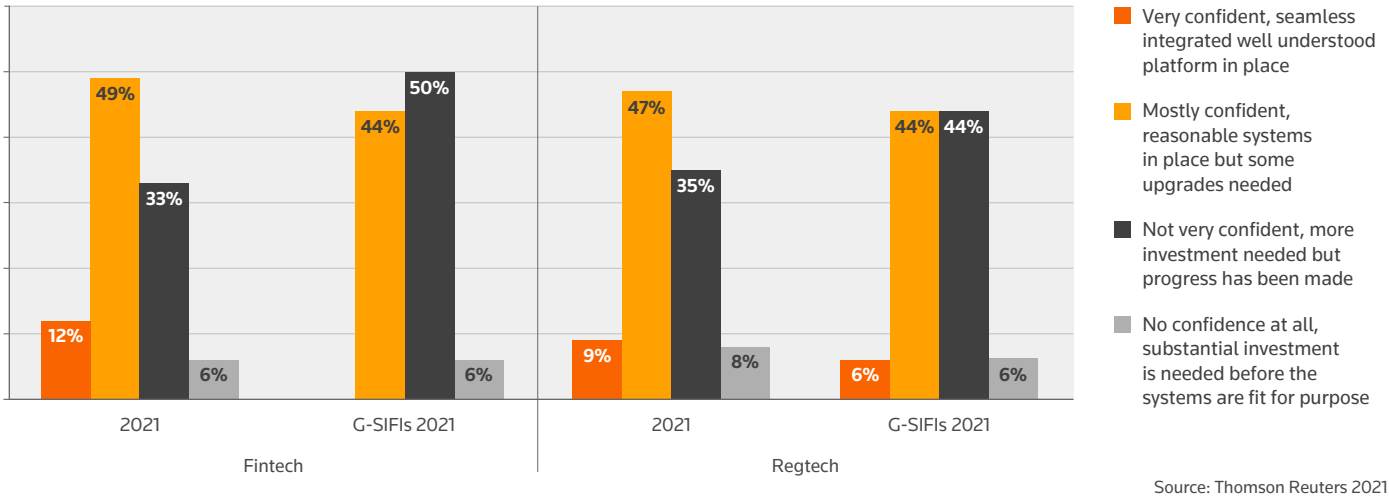
"Data: At OSFI, we benefit from a strong, principles-based approach to supervision and regulation, which provides us with the good relationships that enable innovative analysis and data requests. But, our legacy data environment doesn't adequately fuel our analytical curiosity — in other words, we over-rely on ad-hoc data requests because our legacy data environment does not fully meet our needs. We will invest to change that outcome and that should be welcome news to FRFIs who have been so helpful to us with our ad-hoc data asks."

Peter Routledge, superintendent, Canadian Office of the Superintendent of Financial Institutions, September 2021

Operational resilience

The ability of existing firms' IT infrastructure to support future fintech and regtech solutions has been a concern for some time, and this year's results were no exception. Almost half of firms said reasonable systems were in place, although upgrades were needed for fintech (49%) and regtech (47%) solutions.

FIGURE 13:
How confident are you that your IT infrastructure is/will be able to support fintech, regtech and insurtech solutions?



Source: Thomson Reuters 2021

For a variety of reasons, operational resilience cannot be a one-off exercise, but needs to evolve continually:

- **External threats** — Pandemic-style events could happen again. Political, economic, social and environmental factors can all lead to significant business interruption. The world is now more alert to the threats posed by such systemic events, but there will be an expectation in future that firms "do better next time". The lessons learned from the past 18 months must be turned into preparations for the next disruptive event.
- **Need to adapt business models** — As shareholders, investors and customers place increasing pressure on firms, the need to adapt business models becomes even more urgent.

- **More widespread use of technology** — whether this is as a direct result of the pandemic or not, more and more firms are turning to technology to undertake their operations.
- **Third-party management and outsourcing** — See section below.
- **Regulatory scrutiny** — Regulators are developing their supervisory approaches to include further scrutiny of firms' operational resilience plans.

Regulators have long been concerned about operational resilience. Recent initiatives include:

- **Financial Stability Board** — For some years the Financial Stability Board (FSB) has made it a priority to look at financial resilience in high-risk parts of the financial services sector. This year it included cyber and operational resilience in its work programme and has issued[2] its effective practices for cyber incident response and recovery.
- **Basel Committee** — The Basel Committee has issued its principles[3] for operational resilience. These focus on seven areas: governance; operational risk management; business continuity planning and testing; mapping interconnections and interdependencies; third-party dependency management; incident management; and ICT.
- **EU** — The EU published a draft regulation[4] on digital operational resilience for the financial sector that would introduce a harmonized framework on digital operational resilience in Europe.
- **UK** — The Prudential Regulation Authority (PRA)/Financial Conduct Authority (FCA) and the Bank of England have recently issued their policy papers[5] on operational resilience. The PRA paper focuses on governance, the difference between operational risk and operational resilience, and looks at business continuity and outsourcing.
- **United States** — The Federal Reserve, the Office of the Comptroller of the Currency (OCC) and the Federal Deposit Insurance Corporation have issued an interagency paper[6], "Sound Practices to Strengthen Operational Resilience". These practices cover areas such as governance, operational risk management, business continuity management (BCM), third-party risk management, scenario analysis and surveillance, and reporting operational resilience.
- **Australia** — The Australian Prudential Regulation Authority (APRA)[7] has updated its guidance for prudential standards, BCM, outsourcing and risk management, and the Australian Securities and Investments Commission (ASIC)[8] has issued guidance on the operational resilience of market intermediaries.
- **Hong Kong** — The Hong Kong Monetary Authority (HKMA) has issued principles[9] for operational resilience.
- **Singapore** — The Monetary Authority of Singapore (MAS) has produced guidance on operational resilience.

[2] https://www.fsb.org/2020/10/effective-practices-for-cyber-incident-response-and-recovery-final-report/

[3] https://www.bis.org/bcbs/publ/d509.htm

[4] https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

[5] https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/operational-resilience-sop

[6] https://www.federalreserve.gov/supervisionreg/srletters/SR2024.htm

[7] https://www.apra.gov.au/covid-19-a-real-world-test-of-operational-resilience

[8] https://asic.gov.au/regulatory-resources/markets/market-supervision/operational-resilience-of-market-intermediaries-during-the-covid-19-pandemic/

[9] https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210421e1.pdf

- **Ireland** — The Central Bank of Ireland has issued a consultation paper[10] setting out proposed cross-industry guidance on operational resilience. The core principles of any operational resilience framework, the central bank said, are board and senior management ownership of the operational resilience framework; the identification of critical or important business services and of all activities, people, processes, technology and third parties involved in the delivery of these services; the setting of impact tolerances for each of these identified services; the testing of firms' ability to stay within those impact tolerances during a severe but plausible operational disruption scenario; and the continuous review of how firms responded and adapted to disruptive or potentially disruptive events so that lessons learned can be incorporated into operational improvements to continually enhance their operational resilience.

There are some common themes running through these various pieces of policy and guidance:

- **Definition of operational resilience** — There appears to be consensus that operational resilience entails the following main steps: identify, prepare, respond and adapt, recover and learn. A version of this definition is used in all jurisdictions as the basis upon which to develop approaches to operational resilience.
- **Governance** —Most regulators mention the need for sound governance, and this means that operational resilience should be led by the board and treated as a main strand of corporate governance, embedded into the fabric of a firm. In the UK, boards are specifically required to approve the important business services identified for their firm and the impact tolerances that have been set for each of these. In addition, firms should establish accountability and responsibility for the management of operational resilience, including implementation of the policy.
- **Identification of important business services** — Firms must identify their important business services. Business services deliver a specific outcome or service to an identifiable user external to the firm and should be distinguished from business lines, which are a collection of services and activities.
- **Impact tolerances** — A new theme emerging from the UK PRA is the need for firms to set an impact tolerance for each of their important business services. An impact tolerance is the maximum tolerable level of disruption to an important business service, as measured by a length of time, in addition to any other relevant metrics. Firms should set their impact tolerances at the point at which any further disruption to the important business service would pose a risk to the firm's safety and soundness.
- **Mapping** — Firms need to identify and document the necessary people, processes, technology, facilities and information required to deliver each of their important business services. Many regulators mention inter-dependencies and the need to be aware of risks within a range of internal and external relationships. These should also be mapped and assessed, to establish whether they are critical to operational resilience.
- **Scenario testing** — Firms should regularly test their ability to remain within impact tolerances in severe but plausible disruption scenarios. Impact tolerances assume a disruption has occurred, and so testing the ability to remain within impact tolerances should not focus on preventing incidents from occurring.

[10] https://www.centralbank.ie/docs/default-source/publications/consultation-papers/cp140/cp140---cross-industry-guidance-on-operational-resilience.pdf?sfvrsn=5

Third-party management and cyber security

Regulators now place more emphasis on the way firms assess their third-party relationships. As the use of cloud storage facilities and reliance on fintech firms has become more widespread, regulators have been keen to underline the risks and strengthen control requirements.

One upshot of the pandemic was that some firms sought to shorten supply chains and to bring activities back in-house, to enable line of sight and continuity of management. Other firms reviewed their outsourcing arrangements and revised the associated governance.

The management of outsourcing arrangements is a mirror image of how those operations would be managed had they been undertaken in-house. Compliance officers need to review in-house corporate governance arrangements to assess whether they cover the oversight of outsourced arrangements, for example:

- **Governance arrangements** — Outsourced and third-party arrangements need to be managed within a clear corporate governance structure. Risks need to be managed within a firm-wide risk management framework. Terms of reference for risk committees and operational risk committees (or equivalents) need to include the responsibility for outsourced arrangements. Ownership needs to be apportioned to facilitate greater line of sight by boards into outsourced arrangements.
- **Assessment of third parties** — Due diligence needs to be carried out continuously on all third parties. Specifically, firms need to review new and potential outsourcers to establish which would be considered "material" and therefore subject to heightened regulatory scrutiny.
- **Operational resilience** — An outsourced agreement needs to be treated as if it were an internal operational area for business continuity processes. Appropriate due diligence, monitoring, reporting and exit strategies need to be in place to ensure the smooth continuity of operations should something go wrong.
- **Data** — Data management arrangements for security, access, archiving, classification, destruction, etc., need to be put in place to ensure that third parties only get access to the data they are authorized to use, and that firms can retrieve data should they need to: at exit of the contract, for example.

Cyber security

The adoption, at speed, of new, hybrid ways of working was not without its challenges. Existing and new risks were either heightened or emerged — a combination of those seeking to take advantage of the crisis and the consequences of new and different ways of deploying the technology itself.

The Financial Action Task Force (FATF) issued several updates about the impact of the pandemic on financial crime. "Criminals have used the sharp increase in online activity to develop targeted malware campaigns, ransomware or phishing attacks with fake links to government stimulus packages, infection rate maps and websites selling personal protection supplies. The pandemic also resulted in an increase in human trafficking and exploitation of workers. Most disturbing of all, with children unable to attend school and spending more time online, members reported a rise in online child exploitation," FATF said in January 2021.

FATF has also championed the use of digital solutions "including fintech, regtech and suptech to the fullest extent possible".

"The increasing use of digital services and the widespread reliance on technology, together with the growing use and interconnectedness of third-party products and services, are increasing financial market infrastructures' vulnerability to cyber attacks. Financial experts single out cyber attacks as the number one risk for the global financial system."

Fabio Panetta, member of the executive board of the ECB, September 2021

In September 2021, the OCC issued a "cease-and-desist" order on MUFG Union Bank[11] for non-compliance with the required standards on information security. The bank was found to have "engaged in unsafe or unsound practices regarding technology and operational risk management". The order sets out baseline compliance expectations for cyber security and is a useful codification for all firms in assessing the adequacy of their approach to cyber resilience. There are a series of recommended steps which can be used as the basis for a gap analysis:

- The formation of a specific compliance committee to oversee compliance with cyber-security requirements.
- The creation of an action plan to work toward full (and evidenced) compliance with the requirements. The board is responsible for the oversight of any action plan, which should contain detail on success criteria and timescales. In addition, the board should receive formal updates on quarterly basis.
- The development of a plan to improve board and senior manager oversight of technology and operational risk, which must include consideration of how issue remediation affects risk.
- The enhancement of the technology and risk assessment process, with the aim of the firm being then able to use its technology and risk assessments to report to the board on technology risk.
- As an extension of the improvement in technology and risk assessment, similar enhancements are also needed to make the risk governance framework fit-for-purpose.
- The development of a written information security program to bring policies, procedures, processes and internal controls into line with compliance requirements and then to be maintained to reflect evolving operating practices. The processes should specifically include an approach to ensure good data management and reporting.
- The board has responsibility for governance and oversight and should:
  - "authorize, direct and adopt corrective actions" to achieve the required compliance;
  - ensure the firm "has sufficient processes, management, personnel, control systems and corporate and risk governance" to meet its continuing compliance obligations;
  - ensure that senior managers and other personnel "have sufficient training and authority to execute their duties and responsibilities";
  - hold senior managers and other personnel "accountable for executing their duties and responsibilities";
  - require "appropriate, adequate and timely reporting" to the board by senior managers of corrective actions; and
  - address any non-compliance with corrective actions in a timely and appropriate manner.

[11] https://www.occ.gov/static/enforcement-actions/ea2021-037.pdf

> *"The risks from cyber threats and incidents to the global banking system have been increasing over the past years. Covid-19 has further heightened these risks. In light of the evolving nature and scope of cyber risk, banks must continue to improve their resilience to cyber security threats and incidents."*
>
> **Pablo Hernández de Cos, chair of the Basel Committee on Banking Supervision and governor of the Bank of Spain, September 2021**

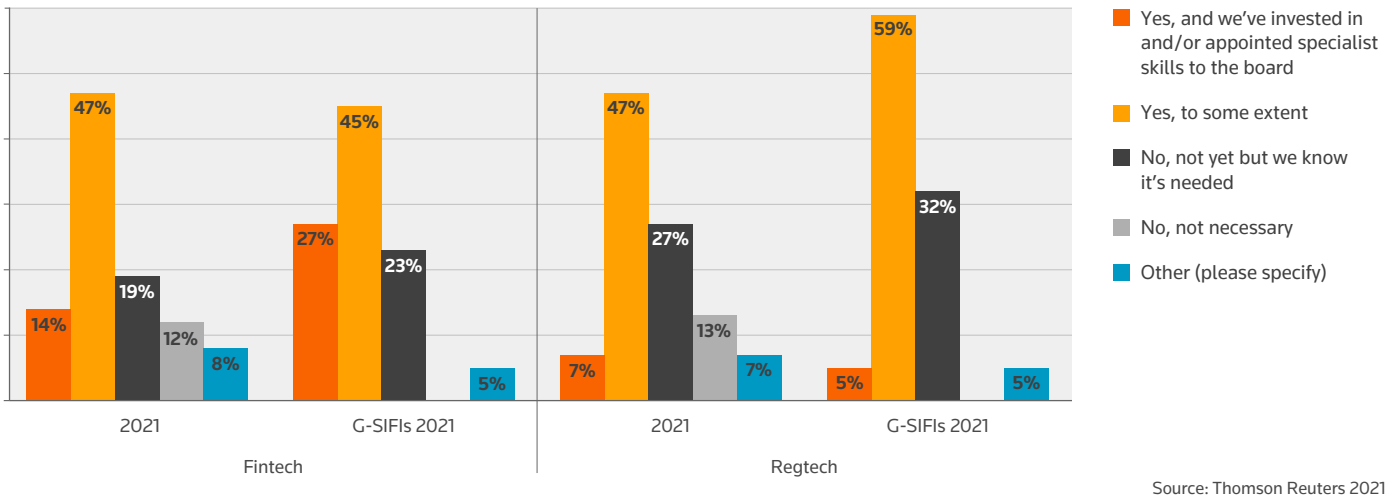
Skills and budget constraints

In previous years, the report has highlighted the need for firms to have skill sets that enable them to understand and manage fintech applications. In this year's survey, 61% of boards have had to widen the firm's skill set to accommodate developments in innovation and digital disruption regarding fintech (72% G-SIFIs), compared with 54% regarding regtech (64% G-SIFIs).

> *"Many have found the journey difficult. The use of technology, specifically new technology, often requires shedding old habits, updating cultural norms, upskilling employees and adjusting ways of thinking. Connecting the dots between digital initiatives, strategy and business enablement is challenge, and is not one that all institutions – or regulators – have made seamlessly."*
>
> **Dubai Financial Services Authority Annual Report 2020, May 2021**

From a regional perspective, 30% of firms in the Middle East had invested in or appointed specialist skills to the board concerning fintech, although only 10% had done so with regards to regtech. Only 3% of firms based in the United States and Canada had invested in or appointed specialist skills for fintech, and none had done so with regards to regtech.

FIGURE 14:
Have you had to widen the skill set at board level to accommodate developments in innovation and digital disruption?

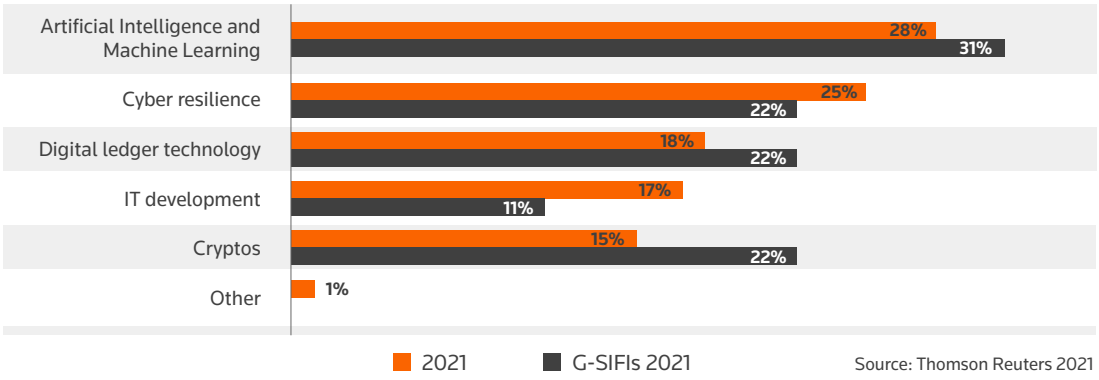


Source: Thomson Reuters 2021

Firms are continuing to invest in specialist skill sets, with a heavier focus on getting fintech (as opposed to regtech) specific skills at board level. There remains a dearth of specialist technological skills, something which is made more difficult by the requirement for firms to have a more diverse workforce. For many firms, it remains the right decision to invest in in-house skill sets, particularly at the most senior levels.

> *"...a lack of awareness of regtech. This is especially the case at board and senior management level, where leaders are often not fully on board with regtech adoption because they do not fully understand its potential benefits."*
>
> **Arthur Yuen, deputy chief executive, Hong Kong Monetary Authority, November 2020**

FIGURE 15:
What skills do you see risk and compliance needing in the future?

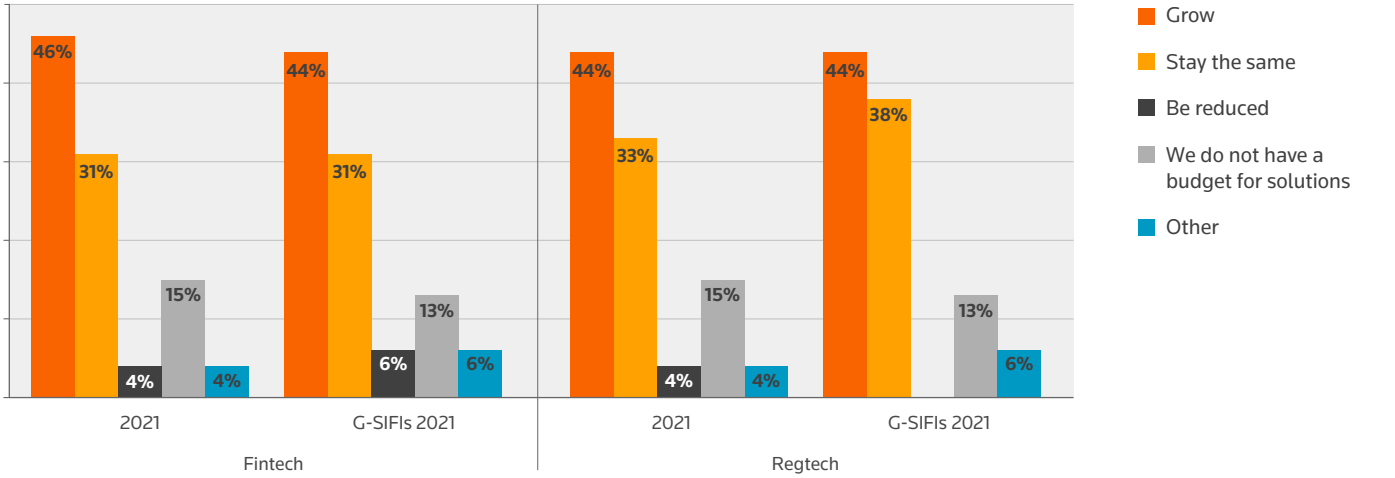


Source: Thomson Reuters 2021

Artificial intelligence and machine learning ranked the most important skills needed by risk and compliance in the future; regionally, this was the case for more than a third of firms in Asia (35%), the Middle East (33%) and Canada (33%).

A large proportion of the budget allocated to digital solutions is likely to be allocated to "buying" the skills needed for both the board and the risk and compliance function. Overall, budgets for fintech and regtech solutions are expected to grow in the next 12 months, although just under a third of respondents expected budgets to remain the same for fintech (31%) and regtech (33%) solutions. Regionally, 56% of firms in Continental Europe and 50% of firms in the United States expected budgets to increase in the next 12 months for fintech solutions. But, 22% of firms in Continental Europe expected budgets for both fintech and regtech solutions to reduce, however.

FIGURE 16:
Your firm's budget for fintech/regtech solutions over the next 12 months will:



Source: Thomson Reuters 2021

Between 13% and 15% of respondents said they lacked a budget for fintech or regtech solutions. It may be that budget for such areas is not separated out from the wider IT or business development budgets, but if it is a matter of resource constraint, those firms will need to think about their priorities.

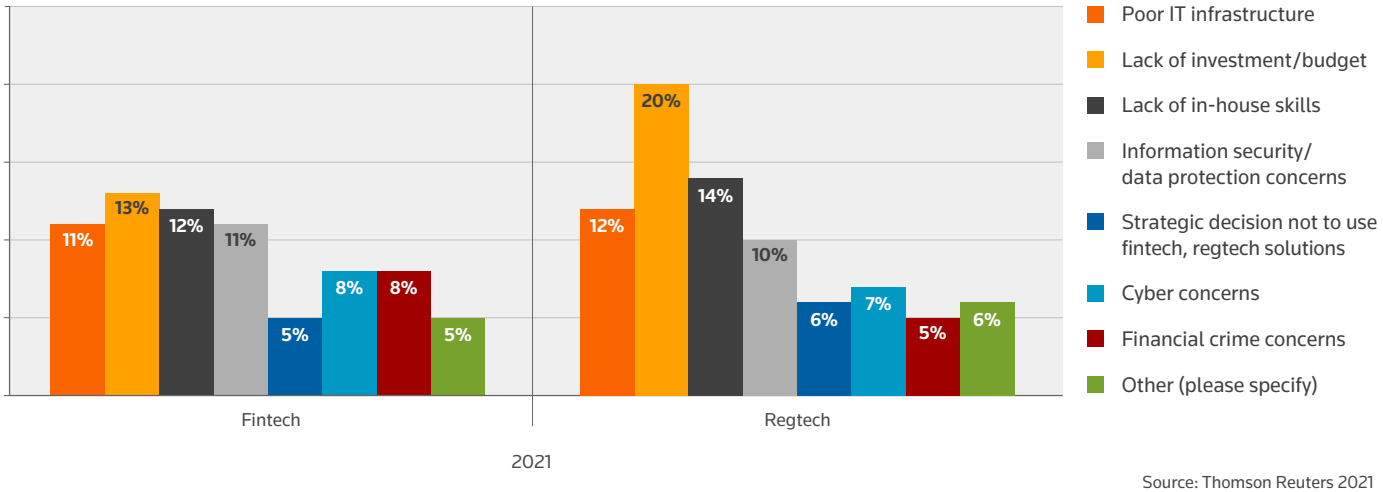
At some firms there appears to be a persistent lack of investment in technological solutions. This manifests itself in various ways for example, through continuing failure to address poor IT infrastructure or through holding back investment in the kinds of in-house skills and budget required to deploy fintech or regtech solutions.

A small minority of respondents said their firms had taken the strategic decision not to use fintech and regtech solutions.

There is likely to come a tipping point at which firms decide they can no longer afford not to invest in technology.

> *"...now is the right time for the banking industry to double down on fintech development. It is time to work together as a whole to embrace the number untapped possibilities that fintech can bring. Fintech has the potential to become a major economic growth engine in the post-pandemic era; and it would be in the banking industry's best interests to be a part of this progression."*
>
> **Eddie Yue, chief executive, Hong Kong Monetary Authority, June 2021**

FIGURE 17:
If your firm has not yet deployed fintech or regtech solutions, what is holding you back?



Source: Thomson Reuters 2021

Hybrid working arrangements

Hybrid or at least flexible working arrangements are here stay. In October 2021, the UK FCA codified its previous expectations regarding, among other things, the need for firms to prove that there is satisfactory planning on a range of governance, culture, technological and control risks, such that:

- That there is a plan in place, which has been reviewed before making any temporary arrangements permanent and which is reviewed periodically to identify new risks
- There is appropriate governance and oversight by senior managers under the senior managers regime, and by committees such as the board, and by non-executive directors where applicable, and that this governance is capable of being maintained.
- A firm can cascade policies and procedures to reduce any potential for financial crime arising from its working arrangements.
- An appropriate culture can be put in place and maintained in a remote working environment.
- Control functions such as risk, compliance and internal audit can carry out their functions unaffected, such as when listening to client calls or reviewing files.
- The nature, scale and complexity of its activities, or legislation, does not require the presence of an office location.
- It has the systems and controls, including the necessary IT functionality, to support the above factors being in place, and these systems are sufficiently strong.
- It has considered any data, cyber and security risks, particularly as staff may transport confidential material and laptops more frequently in a hybrid arrangement.
- It has appropriate recordkeeping procedures in place.
- It can meet and continue to meet any specific regulatory requirements, such as call recordings, order and trade surveillance, and consumers being able to access services.
- The firm has considered the effect on staff, including wellbeing, training and diversity and inclusion matters.
- Where any staff will be working from abroad, the firm has considered the operational and legal risks.

"The above is an indicative and non-exhaustive list. It's important any form of remote or hybrid working adopted should not risk or compromise the firm's ability to follow all rules, regulatory standards and obligations, or lead to a failure to meet them," the FCA said.

Big Tech

There is a general acknowledgment from regulators and central banks of the growing risk posed by Big Tech firms' ability to enter financial services and scale up quickly.

The BIS has recently outlined the policy challenges which the rapid growth of Big Tech firms poses to regulators and central banks:

- the mitigation of financial risks;
- the oversight of operational resilience and consumer protection means the authorities will need a more in-depth understanding of, and will need to undertake more systemic monitoring of, Big Tech business models;
- the potential for excessive concentration of market power;
- data governance concerns;
- some central banks' oversight does include the competitive functioning and efficiency of the payment system, but their mandates do not normally encompass the broad range of competition and data privacy issues that arise in relation to the activities of Big Techs in financial services.

> *"In addition to traditional policy concerns such as financial risks, consumer protection and operational resilience, the entry of Big Techs into financial services gives rise to new challenges surrounding the concentration of market power and data governance."*
>
> **Bank for International Settlements (BIS) Bulletin No.45 – Regulating Big Techs in Finance, August 2021**

In September 2021, the Financial Stability Institute (part of the BIS) published a report[12], "Big Tech Regulation: What is Going On?", which considered the regulatory initiatives that have emerged in China, the EU and the United States. Each of these jurisdictions has focused on different policy areas, but the greatest number of initiatives have been conducted in the area of competition. The initiatives generally seek to achieve a balance between addressing the different risks posed by Big Techs and preserving the benefits they bring in terms of market efficiency and financial inclusion.

The BIS report offers a typology of regulatory actions and focuses on five policy domains: competition, conduct of business, operational resilience, financial stability and, critically, data. "Given the large potential for Big Techs to abuse their technological and data superiority to quickly dominate different market segments and adopt anticompetitive practices, preserving market contestability has become a top priority for authorities in China, the EU and the U.S.," the report said.

Specifically, the use of consumer data is core to Big Techs' business models, which rely on a large number of users interacting in a digital ecosystem. This activity produces data that is then used as an input to offer products and services that generate further user activity and, in turn, more data (the data-network-activities, or DNA loop). The ability to gain insights from users' data provides Big Techs with a significant competitive advantage.

It is that competitive advantage that politicians and regulators are seeking to corral.

"All in all, recent initiatives in China, the EU and the United States represent important steps in combating relevant risks posed by Big Techs," the FSI report said.

It remains likely that regulators will need to introduce further specific controls for Big Techs if, as expected, their presence in the financial system continues to grow, either directly or through their engagement with financial institutions. It is also likely that, to address the risks that Big Techs generate through their unique (DNA loop) business models, any new policy actions will largely follow an entity-based approach and require close cooperation between competition, data and financial authorities.

[12] https://www.bis.org/fsi/publ/insights36.pdf

INTO THE FUTURE

> *"By now, it is clear that early investment in digital transformation has helped the financial sector to adapt and stay resilient in spite of the enormous disruption brought about by the COVID-19."*
>
> **Josephine Teo, minister for manpower and second minister for home affairs, Singapore (January 2021)**

Last year's report highlighted the need for firms to establish strong corporate governance in terms of their fintech developments, and the main report was followed by an additional report on the governance lifecycle for fintech/regtech[13].

Strong corporate governance remains integral to the effective implementation of fintech, but regulators are beginning to apply requirements to fintech applications, and firms need to be up-to-speed and compliant with any regulations introduced.

Regulatory developments

The speed with which the fintech sector has grown has prompted governments and regulators to introduce regulations which allow the marketplace to grow in a controlled way, and which help counter the potential threat Big Tech poses to traditional financial services.

> *"And if things develop as some might believe, tomorrow's financial system will not be made up of banks, central banks and national currencies but of electronic signals that transfer cryptocurrencies from one digital wallet to another."*
>
> **Ida Wolden Bache, deputy governor of Norges Bank (Central Bank of Norway), May 2021**

These regulations address both generic fintech strategy and also the individual areas in which fintechs are developing.

From a generic standpoint, the most notable policy document to appear in 2021 was perhaps the UK government's release of the Khalifa review[14]. This review was asked to identify priority areas to support the fintech sector. Its conclusions provide a structure for the future development of fintech.

Khalifa suggested a five-point plan which made wide-ranging recommendations in terms of policy and regulation, skills, investment, international considerations and national connectivity.

The following recommendations will be of particular interest to compliance officers:

- **Deliver a digital finance package that creates a new regulatory framework for emerging technology:** The UK must prioritize new areas for growth and cross-industry challenges such as financial inclusion, and adopt specific policy initiatives that will help create an enhanced environment for fintech, such as digital ID and data standards.

[13] https://legal.thomsonreuters.com/en/insights/reports/regtech-the-governance-lifecycle
[14] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971371/KalifaFintechReview_ExecSumm.pdf

- **Implement a "Scalebox" that supports firms focusing on scaling innovative technology:** This would include enhancing the Regulatory Sandbox, making permanent the digital sandbox pilot, introducing measures to support partnering between incumbents and fintech and regtech firms, and providing additional support for regulated firms in the growth phase.
- **Establish a Digital Economy Taskforce (DET):** Multiple departments and regulators have important fintech competencies and functions. The DET would be responsible for collating this into a policy roadmap for tech and digital, and in particular the digital finance package. It would provide a "single customer view" of the government's regulatory strategy on tech and a single touchpoint for the private sector to engage.
- **Ensure fintech forms an integral part of trade policy:** The UK must build upon early successes and continuing industry engagement, and further develop its trade policy in relation to fintech, to ensure a coherent and consistent approach, as well as to secure commitments in its future trade agreements that would benefit fintech.

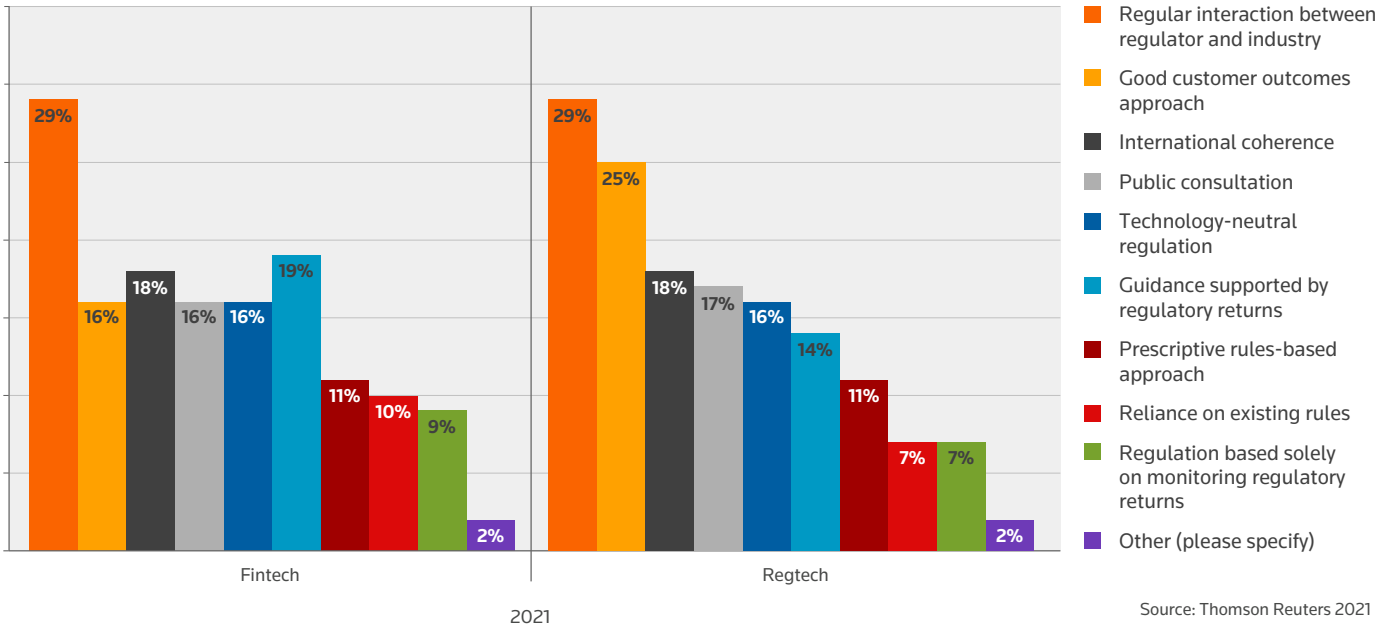
"Good" regulation

> *"We need all market participants to think critically about the risks they face, including those I highlighted today, like complex synthetic and structured products, climate change, and cybersecurity threats. Issuers should disclose certain risks so that investors can make informed decisions. Market participants should think about their counterparties and markets, and make sure due diligence includes an understanding of how counterparties are prepared against risks and how they may fare in times of market upheaval.""*
>
> **Commissioner Caroline A. Crenshaw, U.S. Securities and Exchange Commission, September 2021**

For the first time, respondents were asked for their views on the hallmarks of "good" regulation split between fintech and regtech applications. The top three hallmarks of good regulation for regtech were listed as regular interaction between regulator and industry (29%), guidance supported by regulatory returns (19%) and international coherence (18%).

The top three hallmarks of good regulation for fintech were listed as regulator interaction between regulator and industry (29%), good customer outcomes approach (25%) and international coherence (18%).

FIGURE 18:
What do you consider to be the hallmarks of good regulation with regards to fintech/regtech?



Source: Thomson Reuters 2021

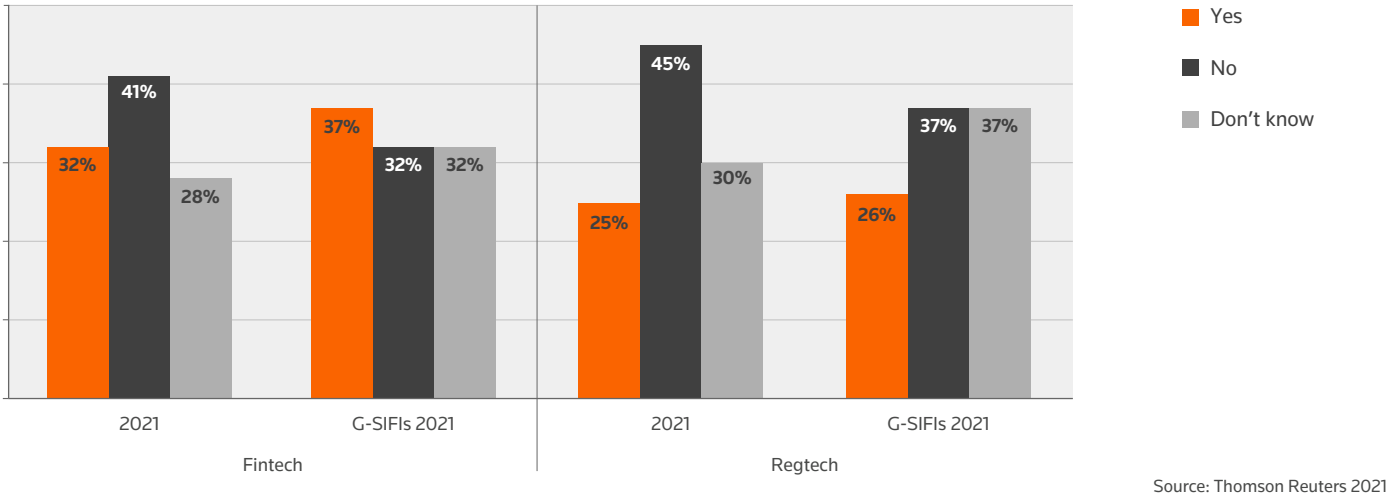
"Sometimes we'll work in collaboration with private sector, and sometimes our role will be to act more as a 'critical friend'. And sometimes, as with [Real-Time Gross Settlements], that will mean timely upgrades to critical technology, while at other times it can mean working right at the cutting edge, as with out work on central bank digital currencies and artificial intelligence (AI)."

Dave Ramsden, deputy governor, Markets and Banking at the Bank of England, April 2021

The largest financial institutions are communicating most with regulators about their approach to fintech (37%) and regtech (26%). There is an apparent disconnect between firms considering that regular interaction with regulators is a hallmark of "good" regulation and the practical reality of how many firms have discussed their approach to fintech and regtech with their regulators.

Regionally, 67% of firms in the Middle East reported regulators had spoken to them about their approach to fintech (44% for regtech), compared with 42% of firms in the United Kingdom (33% for regtech) and 42% of firms in Africa (31% regtech). Regulators in both the Middle East and the UK are taking an active role in supporting innovation in financial services, through regulatory sandboxes, new policies and adapting existing frameworks. In particular, the Dubai Financial Services Authority (DFSA) is a founding member of the Global Financial Innovation Network.

FIGURE 19:
Has your regulator spoken to you about your approach to fintech/regtech?

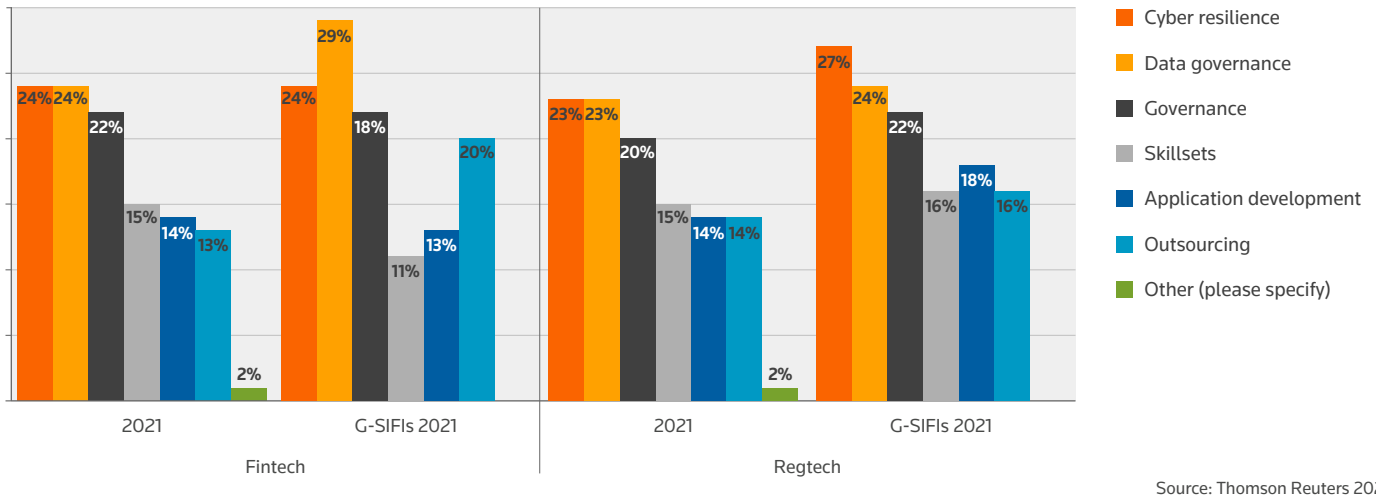


Source: Thomson Reuters 2021

The areas in which additional regulation and guidance are seen to be needed give a clear indication of future areas of concern for firms and their compliance officers. Data governance (24% fintech, 23% regtech) and cyber resilience (24% fintech, 23% regtech) were listed as the top areas where firms would appreciate additional regulation or guidance regarding fintech and regtech. Regionally, almost a third (32%) of firms in Australasia said additional regulation or guidance was needed on data governance regarding fintech.

> *"It is true that in our study, regtech firms ranked regulators as the fifth highest barrier to regtech adoption. But interestingly, banks thought the opposite. They actually ranked regulators as the third lowest barrier."*
>
> **Arthur Yuen, deputy chief executive, Hong Kong Monetary Authority, November 2020**

FIGURE 20:
In what areas is additional regulation/guidance needed?



Source: Thomson Reuters 2021

Sandboxes

One way in which regulators and the industry are collaborating is through the use of "sandboxes" for the joint development of future fintech applications. The phrase "sandboxes" conjures up images of children's play areas and buckets and spades, and in some ways that is an accurate analogy of what is happening in the fintech market.

A sandbox is an environment where vendors can freely test future products by creating the characteristics of live business scenarios, demonstrating responses from the product and also any dependencies included in the sandbox. This allows financial services firms, regulators and fintech providers to see the near-accurate customer outcomes of operational systems in confined, controlled environments.

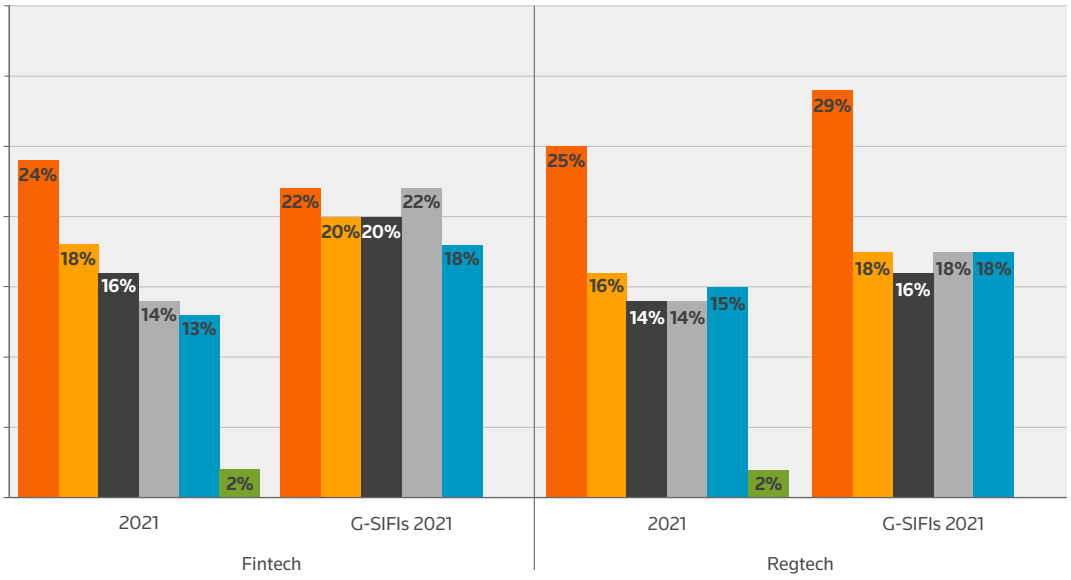
Appendix 1 sets out a list of major sandboxes and their criteria.

Future of the compliance function

The risk and compliance view of the impact of fintech and regtech was positive, but mixed. Around a quarter of respondents felt that the successful deployment of fintech/regtech should drive up the effectiveness of the compliance function, allowing more time to focus on value-add activities. There was also the sense that compliance functions will need "more" to gain the most benefit from technological solutions. Specifically, more skilled resources to evaluate, understand and deploy fintech/regtech solutions and the ability to devote more skilled resources to develop/maximize the strategic potential of technological solutions.

Technologically-enabled shifts in working arrangements have given compliance officers the flexibility to work remotely, but in the longer term, implementation of fintech/regtech could lead to fewer compliance staff being needed. It is the rote compliance tasks which are most likely to be automated, leaving more skilled, qualitative tasks to be undertaken by compliance personnel.

FIGURE 21:
What will be the impact of fintech/regtech on your compliance function?



Source: Thomson Reuters 2021

FIGURE 22:
The greatest benefits/values you expect your firm to see from financial technology in the next 12 months are:

Source: Thomson Reuters 2021

The top five were:

1. Improved efficiency
2. Optimized reporting and data analytics
3. Improved customer experience
4. Automation
5. Reduction of costs

Respondents had a substantial wishlist as to what they would like regtech solutions to be able to do for them.

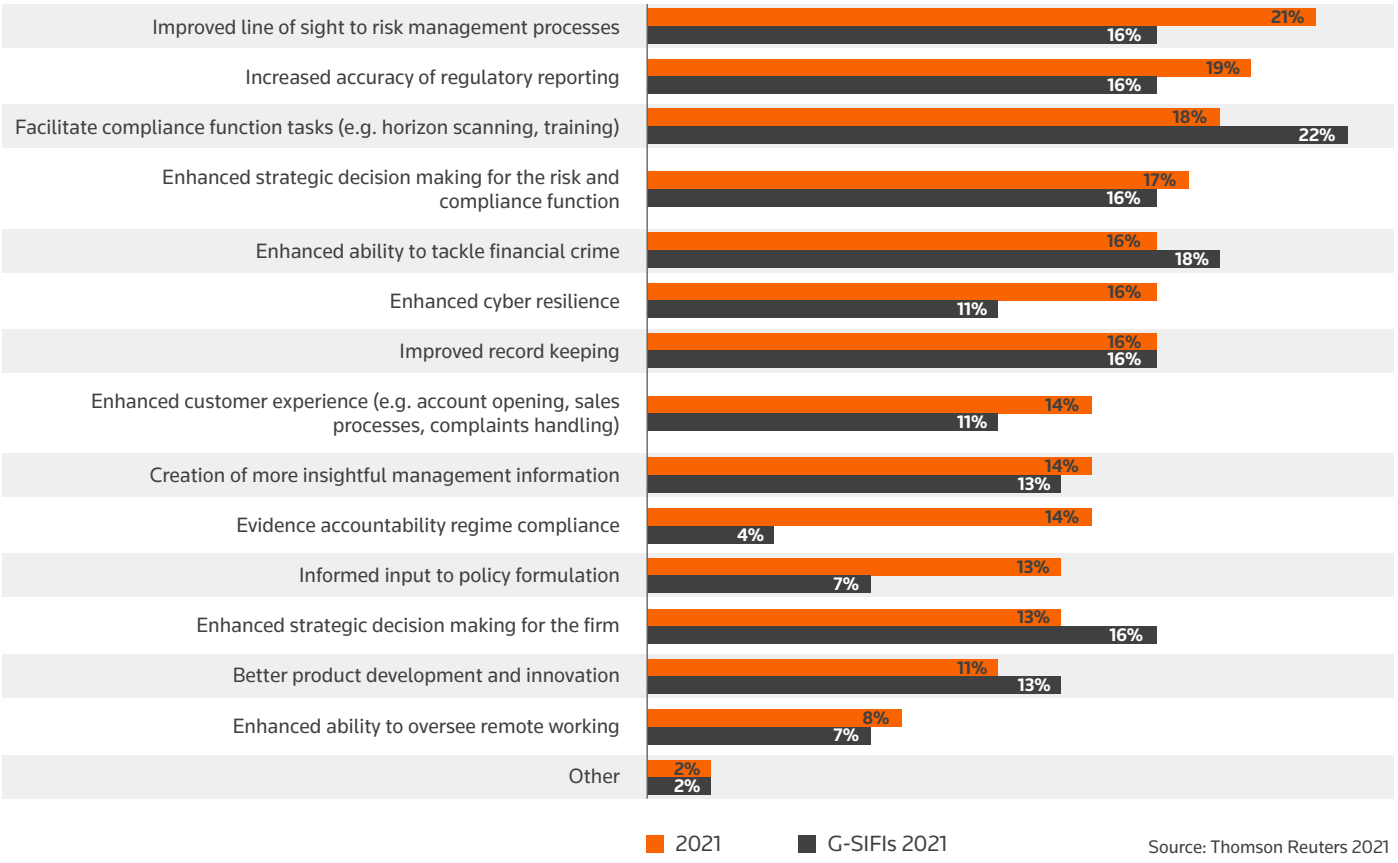
At the top was improved line of sight to risk management processes (21%) and increased accuracy of regulatory reporting (19%). The previous year, the top requirement was for enhanced strategic decision making for the risk and compliance function (52% in 2020), followed by improved accuracy of regulatory reporting (47% in 2020). G-SIFIs had somewhat different priorities, with the facilitation of compliance function tasks such as horizon scanning and training (22%) listed as the top requirement.

WHAT IS THE ONE THING YOU WOULD LIKE TECHNOLOGICAL INNOVATION TO BE ABLE TO DELIVER FOR YOUR FIRM IN THE NEXT 12 MONTHS?

"... I am very keen to see technological offers in combination with international legal knowledge allowing companies to manage their compliance (regulatory, contractual) in a more accessible, easy and fluent manner, with easy access to information and updates. Especially mid-sized firms suffer under the weight of compliance obligations and need more ways to integrate compliance controls easily into their business culture."

Anonymous, Continental Europe

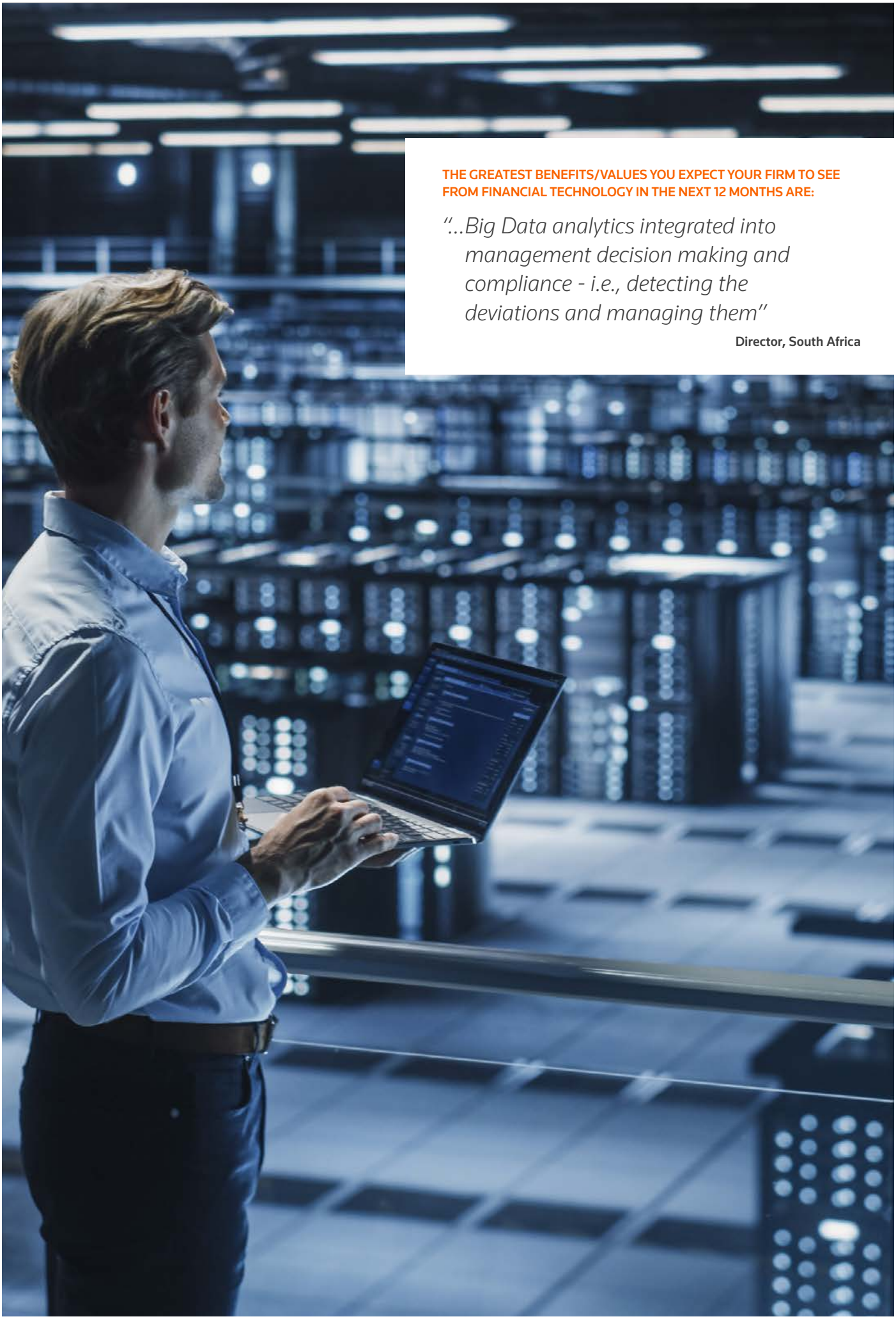
FIGURE 23:
What would you like regtech to be able to do for your firm?



Source: Thomson Reuters 2021

"...we believe that regtech solutions offer clear benefits to banks, customers, and regulators alike. For Banks, they can leverage on regtech solutions to enhance risk management quality and reduce costs. For example, in the area of financial crime and transaction monitoring, some banks still have teams dedicated to the manual remediation of false positives. But others have already used regtech solutions to put automation in place. In doing so, not only have their alert outputs become more accurate, the process also freed up precious resources to focus on higher value tasks, including in particular their interactions with customers."

Arthur Yuen, deputy chief executive, Hong Kong Monetary Authority, November 2020



THE GREATEST BENEFITS/VALUES YOU EXPECT YOUR FIRM TO SEE FROM FINANCIAL TECHNOLOGY IN THE NEXT 12 MONTHS ARE:

"...Big Data analytics integrated into management decision making and compliance - i.e., detecting the deviations and managing them"

Director, South Africa

CLOSING THOUGHTS

A thread which runs throughout the report is that of data, and the need for a stronger focus on all elements of data governance. The size of the issue is not to be downplayed. It is estimated that every person online produced 1.7 MB of data every second in 2020, amounting to 1.145 billion gigabytes of data a day. The world produced twice as much data in 2021 as in 2019, and this is predicted to increase exponentially in the next five to 10 years.

FIGURE 24:
What is the one thing you would like technological innovation to be able to deliver for your firm in the next 12 months?

Source: Thomson Reuters 2021

The point on data is borne out by the responses to the question about the one thing firms would like technological innovation to deliver in the next 12 months, the top five being:

1. Data aggregation and governance.
2. Process automation and efficiency.
3. Enhanced customer experience.
4. Cost savings.
5. Automated monitoring of regulatory change.

"It has been said that in the digital economy, data is the new oil. Many technology companies follow a business model in which they use their customers' data to refine and expand the range of products and services they offer [...] This, in turn, pulls more and more business onto their platform, which generates more data, and so on. If that business model were used as a foundation for the dominant method of payment in the economy, the issuer would gain control over an enormous range of data — bringing with it overwhelming market power. In effect, a technology company could become the gatekeeper of the entire economy, with concerning implications for privacy, competition and inclusion."

Timothy Lane, deputy governor, Bank of Canada, February 2021

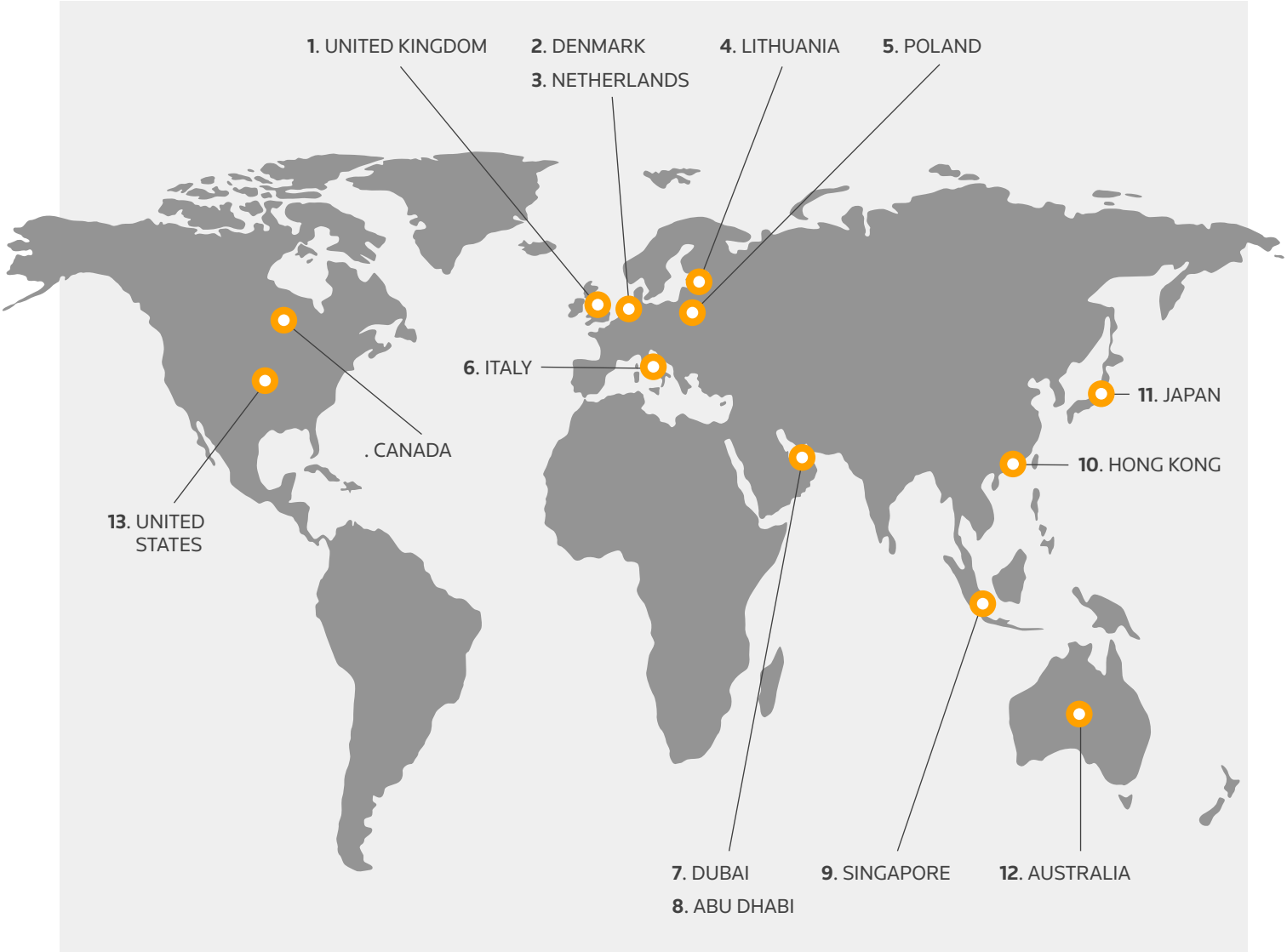
Firms need to embrace the fact that data is a vital strategic asset, and from there build a business-wide approach to data aggregation, management, storage, security, retrieval and destruction; in other words, build a business-specific approach to data governance. The successful governance of data will have multiple benefits including greater line of sight to risks being run in a hybrid working environment and enhanced recordkeeping.

To deliver on data governance, firms will need to invest wisely in both skills and infrastructure. Firms need to re-assess their priorities in a (post-) pandemic world.

APPENDIX 1 – SANDBOX LOCATOR

In August 2021, the European Securities and Markets Authority (ESMA) published a joint report on fintech regulatory sandboxes and innovation hubs. "Innovation facilitators can help competent authorities to keep pace with developments by gaining near –'real time' insights into emerging technology (such as distributed ledger technology, big data analytics, artificial intelligence and machine learning) and their application in the financial sector," it said.

The map below sets out the sandboxes initiated or supported by regulators and government bodies in the financial services industry.



EUROPE

1. *United Kingdom*

May 2016 – Regulatory Sandbox (Financial Conduct Authority)

In September 2021, the FCA began accepting applications for its Second Digital Sandbox with The City of London Corporation, to support the testing and development of new products and services in the area of ESG data and disclosure.

2. *Denmark*

October 2017 – Regulatory Sandbox (Finanstilsynet – the Danish Financial Supervisory Authority)

The Danish Financial Supervisory Authority established its sandbox initiative, the FT Lab, which aims to provide a basis for testing innovative financial products and services; promote the development of beneficial financial products and services for consumers; enable the Danish FSA to better understand fintech; and support the use of new technology in the financial sector.

3. *Netherlands*

January 2017 – Regulatory Sandbox

In a joint initiative with De Nederlandsche Bank and the Autoriteit Financiële Markten, a regulatory sandbox was formed to support the financial services industry with innovative products and services.

4. *Lithuania*

September 2018 – Regulatory Sandbox (Lietuvos Bankas)

The Bank of Lithuania officially launched its regulatory sandbox in September 2018, forming part of the Bank's strategic directions for 2017-2020. The regulatory sandbox is open to both existing authorized financial institutions and new market entrants.

5. *Poland*

October 2018 – Regulatory Sandbox (Komisja Nadzoru Finansowego)

The Polish Financial Supervision Authority (UKNF) developed its regulatory sandbox following an application by the UKNF and Ministry of Finance to the European Commission during the third round of the Structural Reform Support Programme 2017-2020 (SRP Regulation).

6. *Italy*

July 2021 – The Fintech Committee and Regulatory Sandbox

The Ministry of Economy and Finance issued the ministerial decree no. 100/2021 on April 30, 2021, forming a Fintech Committee and Regulatory Sandbox for the financial services industry. The sandbox will allow fintech operators to test innovative solutions, benefiting from a simplified transitional regime in constant dialogue with the supervisory authorities: the Bank of Italy, Consob and IVASS. The application window for the first cohort of the sandbox will be open from November 15, 2021 to January 15, 2022.

UAE

Innovation is a key pillar of the UAE's economic growth and recently ranked first regionally in the 2020 Global Innovation Index

7. *Dubai*

May 2017 – Innovation Testing Licence Programme (Dubai Financial Services Authority)

Dubai's version of a regulatory sandbox is the DFSA Innovation Testing Licence (ITL) Programme — a licensed sandbox designed to enable ITL holders to test new and innovative financial products, services, and business models.

8. *Abu Dhabi*

September 2018 – Fintech digital sandbox (Abu Dhabi Global Market)

The ADGM launched its digital sandbox to accelerate financial services innovation and financial inclusion in the UAE, allowing financial institutions and fintechs to experiment and test products and solutions in a digital platform environment supported by regulatory standards.

ASIA

9. *Singapore*

June 2016 – Regulatory Sandbox (Monetary Authority of Singapore (MAS))

August 2019 – MAS launches "Sandbox Express" to provide firms with a faster option to test innovative financial products and services in the market.

10. *Hong Kong*

September 2016 – Fintech Supervisory Sandbox (FSS) (Hong Kong Monetary Authority)

September 2021 – Fintech Supervisory Sandbox 2.0 (HKMA)

The HKMA uses the experience obtained from the FSS to launch Fintech Supervisory Sandbox 2.0, which has new features, including a Fintech Supervisory Chatroom to provide feedback to banks and tech firms at an early stage of their fintech projects; tech firms can access the Sandbox by seeking feedback from the HKMA through the Chatroom without going through a bank; and the sandboxes of the HKMA, the Securities and Futures Commission (SFC) and the Insurance Authority (IA) are linked up so that there is a single point of entry, if needed, for pilot trials of cross-sector fintech products. The FSS 2.0 is also open to regtech projects or ideas raised by banks or tech firms.

11. *Japan*

June 2018 – Regulatory Sandbox as part of Future Investment Strategy (government of Japan)

The government of Japan introduced its regulatory Sandbox framework in June 2018, in accordance with the Act of Special Measures for Productivity Improvement. It has been included in the Act on Strengthening Industrial Competitiveness since July 2021. Companies, including those overseas, can apply to conduct demonstrations under the new framework and test innovative technologies such as AI or blockchain for future business.

AUSTRALASIA

12. *Australia*

September 2020 – Enhanced Regulatory Sandbox (Australian Securities and Investments Commission)

ASIC's Enhanced Regulatory Sandbox (ERS) supersedes the previous regulatory sandbox (launched in 2016) and allows for testing of a broader range of financial services and credit activities for a longer duration of up to 24 months.

NORTH AMERICA

13. *United States*

October 2018 – Strategic Hub for Innovation and Financial Technology (FinHub) (U.S. Securities and Exchange Commission)

The SEC launched its Strategic Hub for Innovation and Financial Technology (FinHub) in October 2018 and acts as a resource for public engagement on fintech-related issues and initiatives at the SEC.

14. *Canada*

February 2017 - Regulatory Sandbox (Canadian Securities Administrators)

The Canadian Securities Administrators regulatory sandbox allows firms, including fintech firms, to register or obtain exemption from securities law requirements that may create a barrier to business models.

October 2016 – Ontario Securities Commission Launchpad

The OSC's launchpad was designed to support innovative businesses, assisting, and testing innovative business models in capital formation, transaction and service efficiency and fairness.

APPENDIX 2 – AI GUIDANCE

AI and machine learning: A practical introduction

An understanding of AI-associated algorithms and how they are built is imperative if firms are to properly identify and manage AI-related risk. In practice, AI is developed by humans through the use of software programming (code). Just as there is a need for governance and controls in financial reporting or software development due to the human element, organizations need governance and controls for AI as well. Boards and executives will, however, be unable to help monitor controls effectively without a basic understanding of what AI does and how it is built.

What algorithms do

There are three common classes of machine learning algorithms: non-deep-learning, deep-learning, and reinforcement learning. The goal of these AI models is to create a classification, a prediction, or the generation of novel data.

- **Non-deep-learning** classifies, finds patterns and predicts outcomes. Common models include regressions, clustering, decision trees and support vector machines. They can help with many useful and common problems such as demand forecasting, cross-selling propensity and risk classification.
- **Deep-learning algorithms** have been a game changer. These methods of classifying and predicting have driven the AI revolution of the last decade. Imaging, natural language processing, and anomaly detection have achieved state-of-the-art results using deep neural networks. The conversational bots that are helping people navigate customer service on a website comes from this AI technology. A simple automation can be applied more widely, such as voice-to-text on a cell phone, or it can be used to recognize and translate handwriting, utilizing the data to aid in the effort.
- **Reinforcement learning models** examine an environment and develop the ability to make a sequence of decisions that aims to find the best positive path forward. Such models can learn to win chess and Go tournaments against human grandmasters. Practical applications include route optimization, factory optimization and cyber vulnerability testing.

How algorithms are built

Every algorithm should link to the business strategy. Algorithms are designed by humans to contribute to informed decision-making that creates the intended business value. There are six steps to building a machine learning model:

1. **Problem definition** — Considering a business problem and how machine learning could solve it.
2. **Data profiling** — Identifying the data sources needed to solve the problem and what additional data is needed. An emerging trend within AI is the development of new sensors and data collection for the sole purpose of improving AI performance. Organizations need to ensure that data is fair and balanced across ethical and performance dimensions.
3. **Data preparation** — Determining what is needed to transform, normalize, and cleanse the data, and creating a testing and validation approach.
4. **Algorithm evaluation** — Leveraging leading practices to select the algorithms required to solve the problem. Often, data science teams will develop multiple algorithms in parallel to determine the best performing model. It's important to establish the correct performance evaluation criteria.
5. **Model development** — Training, testing and validating all identified algorithms with the data and implementing approaches such as regularization.
6. **Model deployment, monitoring, and maintenance** — Incorporating machine learning operations and monitoring structures along with processes to address model drift. Model performance can degrade if the activities in the environment change over time (for example, models that predict electricity consumption need to be updated over time as solar panels gain traction with consumers).

Source: Research report on realizing the full potential of AI commissioned by the Committee of Sponsoring Organizations of the Treadway Commission, September 2021

THOMSON REUTERS®

Thomson Reuters is a leading provider of business information services. Our products include highly specialized information-enabled software and tools for legal, tax, accounting and compliance professionals combined with the world's most global news service – Reuters.

For more information on Thomson Reuters, visit **tr.com** and for the latest world news, **reuters.com**.

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.thomsonreuters.com/en/products/regulatory-intelligence**

About the authors

Susannah Hammond

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. She is co-author of "Conduct and Accountability in Financial Services: A Practical Guide" published by Bloomsbury Professional.

Mike Cowan

Mike Cowan is a senior regulatory intelligence expert for Thomson Reuters with more than 25 years' experience of compliance, regulatory, risk and internal audit in UK financial services both as a regulator and a practitioner.

THOMSON REUTERS®