Accelerating digital finance

The new reality publication series

March 2021

kpmg.com/regulatorychallenges

New publication series

The EMA FS Regulatory Insight Centre is pleased to publish the sixth paper in its thought leadership series ***Financial Services: regulating the new reality.***

As the focus of government and businesses have moved from initial response to the COVID-19 pandemic, through resilience concerns, to recovery and the new reality, financial services regulators are moving out of a phase of adjustment and support, and are looking to the new reality.

This paper looks at how the financial services industry – both existing firms and new market entrants – are being called upon to deliver digital finance, to embrace its benefits and to manage the risks arising from new technologies, digitalisation and data handling. Over the coming months, look out for further articles and papers in which we will continue to build on the themes identified in the first overview paper.

Financial services: regulating the new reality

Remote governance and controls

Delivering sustainable finance

Ensuring stable capital markets

Financial resilience in banking: a balancing act

Look out for further articles and papers in this thought leadership series that will consider other "new reality" issues.

Contents

Introduction

The pandemic has been a technological catalyst. It has caused change on a greater scale and at a faster pace than any firm's planned IT strategy or any regulatory initiative. Initial lockdown measures to manage the pandemic caused years of change to take place in months, as firms moved to, and continue to operate, large-scale remote working. Some firms were better placed to handle this rapid increase in use of technology and digitalisation of services and delivery, others less so. Disruption by new technologies became more palatable during the pandemic, resulting in faster adoption and progress, but introducing risks that will outlast the pandemic and its after-effects.

The pandemic also saw greater cooperation between industry and regulators to help consumers. And it has provided added impetus to governments' and regulators' plans to encourage moves towards digital finance, including digital currencies, and to adjust laws and regulations to reflect these new forms of finance and the widening use of technology. This paper touches on a number of key themes in the growing stream of outputs from policymakers and regulators.

Developments in digital finance could transform how consumers and businesses make payments and raise finance and could assist economic recovery. Regulators recognise the benefits of new technologies and the digital society but are concerned about new and heightened risks. They are seeking to encourage market entry by new types of firms and technological tools – **BigTech** and **FinTech** – but are conscious of the need to redefine the regulatory perimeter and to avoid an unlevel regulatory playing field. They are concerned about the size and scale of infrastructure providers and the potential implications for competition and resilience.

Traditional financial services firms are making increased use of **technology,** via third-party suppliers, joint ventures or in-house development. The use of distributed ledger technology (DLT) is taking off, as are artificial intelligence (AI) and machine learning (ML), with a new generation of advanced analytics and AI – "AAAI" – tools being developed. New technologies are evolving fast and the "internet of things" – including mobiles and watches – is enabling greater access. The next wave of innovation promises not only to make things even faster, smaller and better but also to add the sense of a "human" touch to digital functionality, to meet customers' psychological need to feel they are interacting with people and not cold machines.

80% of CEOs say the pandemic has accelerated digital transformation

77% say they will continue to build on digital collaboration and communication tools

Source: KPMG's CEO 2020 Outlook

The trend in **digitalisation** – doing more things in a digital way rather than on paper or face-to-face – has accelerated rapidly. Use of cashless payments has increased, new forms of cashless payments, digital currencies and crypto-assets are emerging, and there has been an increase in online investment tools. Communications are becoming more immediate. Online descriptions of services and products can be dynamic and customised, and therefore more engaging and educative.

Increased digitalisation and new technologies can result in **better experiences and outcomes for consumers,** but the regulators wish to mitigate risks such as aggressive selling practices and the biased (intentionally or otherwise) presentation of product information that could prevent consumers making informed decisions. More generally, existing conduct rules need to be re-thought to recognise the fundamental shifts in the construction of financial services and products, and how they are delivered and communicated. There are specific concerns about vulnerable and financially excluded customers, who may fall even further behind in an increasingly digital world, and that digitally excluded consumers should not become cash excluded. Firms need to consider whether changes to business practices are to the benefit of all customers (or, at least, not to their detriment), in addition to benefits to the firm itself. Firms need to balance their own commercial interests with those of their end customers.

> "Covid is not a traditional *cyclical* shock whose effects will eventually wash-out. It is instead a *structural* shock with lasting implications for the behaviour of individuals and the business models of companies."
>
> **Andrew Haldane**,
> Executive Director, Bank of England,
> November 2020

The fundamental building blocks underpinning all technologies and digitalisation are **infrastructure** and **data.** Firms need to ensure the integrity of exponentially expanding databases and that they have the expertise to store and analyse them, whether in-house or via outsourcing to third parties. They need both to protect customers' and market confidential data and to share them in order to deliver services more efficiently and across borders. They need to use data ethically and to have robust governance and controls in place regarding their use of data.

The regulatory focus on the **technological resilience** of firms continues. Outsourcing to third parties, cybersecurity and managing of IT risks are common themes in recent papers. These topics are not new, but there has been an increase in cyber security incidents during the pandemic and regulators are concerned about heightened (and new) risks in an increasingly digital world. Look out for our next new reality paper for a discussion on the broader topic of operational resilience.

Good governance is needed across the piece. Effective controls are essential around internal processes, the storage and use of data, communications with customers and counterparties, and contractual arrangements with third parties. The positions of Chief Technology Officer and Chief Data or Information Officer, in addition to Chief Operating Officers, are becoming mainstream. And the use of **RegTech** applications has increased.

The regulators themselves are trying to keep abreast of change, in the way they monitor wholesale and retail market activity, and how they use data submissions from firms and technological applications to perform their supervisory and enforcement activities. Use of **SupTech** applications by regulators is on the rise.

Key messages for CEOs

- New technologies bring new and emerging risks. Firms need to think innovatively about how to identify, measure and manage these risks, including the use of new techniques and tools.
- New business models – including joint ventures with technology companies and platforms – make the ecosystem and customer interactions more complex in managing conduct and financial crime risks.
- The ever-increasing dependence on good data heightens risks around quality, privacy, security, retention, ethics and sovereignty.
- Given the changing nature of products and services, of how they are delivered, and of communications with customers and counterparties, regulators are underlining the need for firms to consider the end-customer, throughout the business and at all stages of a product lifecycle.
- Firms need to review their overall risk management framework, across the lines of defence, and to attract staff with new skill sets, in a highly competitive market.
- Technology can help firms to improve their governance, systems and controls, to run their businesses more efficiently, and in their communications with regulators.
- Technology can help to support and evidence a culture of focusing on good experiences and outcomes for the end-customer, including robust product governance.

01. Encouraging and regulating innovation

Regulators are seeking to encourage innovation in financial services. They are establishing mechanisms to help new types of firm to enter the market and regulated firms to innovate their products and services. At the same time, they are concerned about the potential dominance of BigTech firms and how best to regulate in an increasingly digital environment. The perimeter of what is and is not regulated activity is being challenged. There are tensions between entity-level regulation and supervision versus borderless technology.

In July 2020, the Bank of International Settlements (BIS) issued a paper summarising the policies put in place around the world in response to the pandemic, to encourage the use of digital finance. Measures ranged from designing cash-in/cash-out networks as essential services, reducing or waiving fees, and relaxing know-your-customer (KYC) procedures to facilitate remote onboarding and use of digital channels. As countries began to emerge from the first lockdown phase, new policy measures included direct public support for FinTech providers and users, and the provision of sandboxes.

The BIS aims to foster international collaboration among central banks on innovative financial technology, in part to help authorities tackle cross-border issues. Its Innovation Hub's 2021/22 work programme has six thematic priorities: SupTech and RegTech, next-generation financial market infrastructures, central bank digital currencies, open finance, cyber security and green finance. It has launched an Innovation Network of experts from member central banks, who will work on the six priorities. Projects will be spread across existing hub centres and new locations coming online in 2021.

Regulatory sandboxes now exist in several countries around the globe. Their focus varies, but commonly they provide a regulatory framework that allows FinTech start-ups and other innovators (including regulated firms) to conduct live experiments on new products in a controlled environment with real clients, under supervision. These sandboxes also tend to offer pro-active regulatory support where a firm's innovative solution (generating good customer outcomes) is hampered by an existing regulatory requirement or the requirements are unclear. A new generation of digital sandboxes is emerging, such as the one opened by the UK FCA in October 2020, which will focus on new digital products and solutions that detect and prevent fraud and scams, support the financial resilience of vulnerable customers and improve access to finance for small and medium-sized enterprises (SMEs). As with the first generation of regulatory sandboxes, the digital sandbox is open to both regulated and unregulated firms, including technology businesses that are seeking to serve regulated firms.

A focus on BigTech and FinTech

The Financial Stability Board's (FSB's) October 2020 report considered the financial stability implications from the provision of financial services by BigTech firms in emerging market and developing economies (EMDEs). It found that the expansion of BigTech firms has generally been more rapid and broad-based in EMDEs than in advanced economies. Lower levels of financial inclusion in EMDEs create demand for BigTech firms' services, particularly among low-income and rural populations that are under-served by traditional financial institutions. Increasing availability of mobile phones and internet access help to service that demand and create new data sources.

BigTech firms have enabled financial services that can be cheaper, more convenient and tailored to users' needs, offering opportunities to improve consumer welfare and support financial stability. However, the expansion of BigTech activity also gives rise to risks and vulnerabilities, where customers have lower financial literacy and when firms make greater use of personal data, including those acquired from their non-financial business. BigTech firms can be subject to heightened operational risks, and competition from BigTech firms may reduce the profitability and resilience of incumbent financial institutions and lead to greater risk-taking. Strong regulation (founded on the principle of "same risk, same regulation"), supervision and other policy measures can play a key role in supporting innovation in financial services and mitigating risks, the FSB says.

A second BIS paper, in August 2020, explored how FinTech financing is regulated, highlighting that the proliferation of new technology-enabled business models has raised questions about the regulatory perimeter. Authorities are assessing whether their existing regulatory framework needs to be adjusted. Their decisions are likely to depend on:

— Potential risks to consumers and investors, financial stability and market integrity

— Assessment of how these new activities might benefit society in terms of strengthening financial development, inclusion and efficiency

— How risks are dealt with under the existing framework and whether opportunities for regulatory arbitrage have emerged

The BIS noted that the overall challenge for authorities is to maximise the benefits of FinTech innovations, while mitigating potential risks for the financial system.

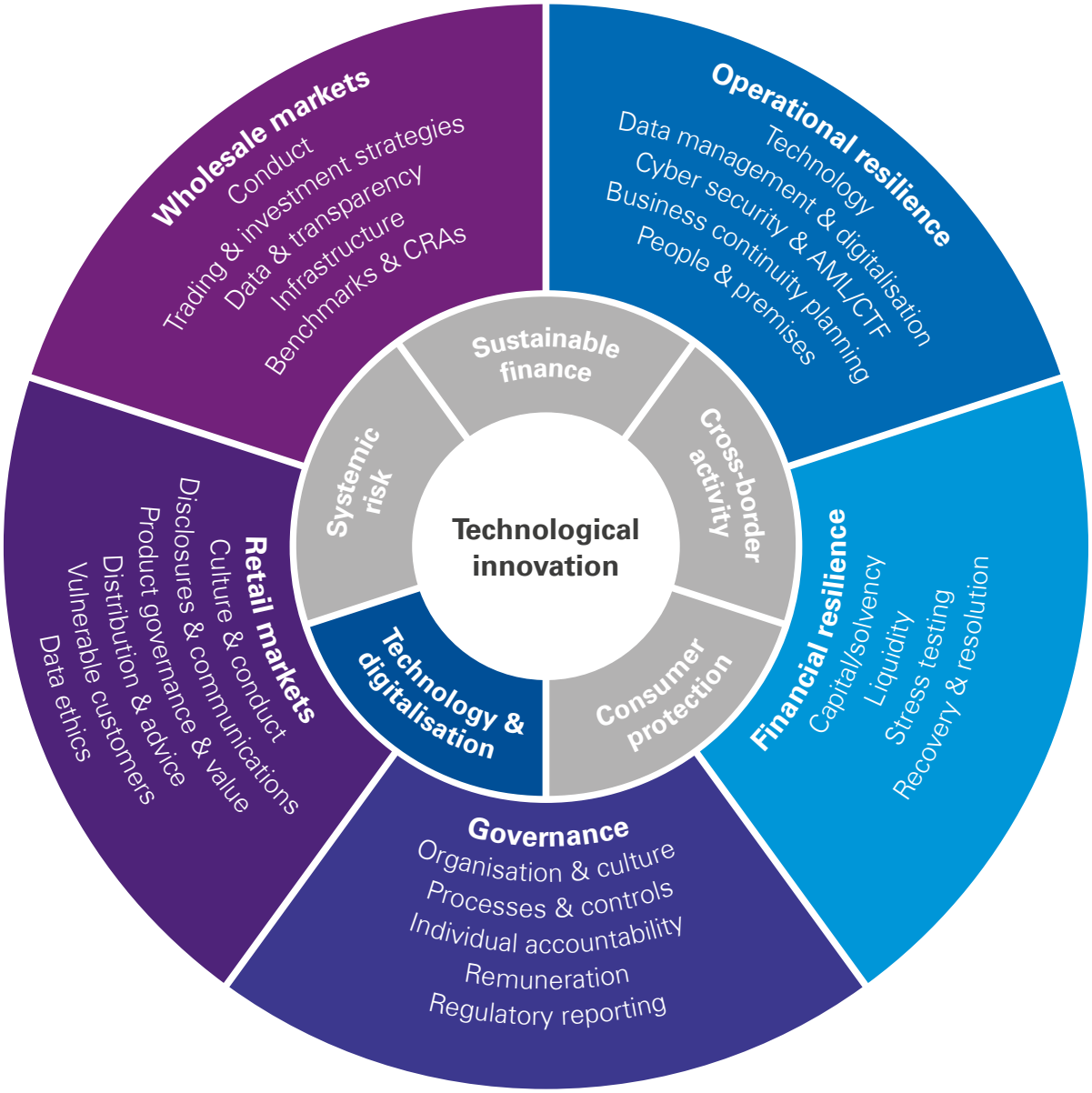
A third BIS paper in February 2021 describes the debate about how regulation should evolve to encourage fair competition between traditional banks and new FinTech and BigTech players. Some advocate moving from an entity-based to an activity-based regulatory approach under the "same activity, same regulation" principle. However, the paper suggests there is limited scope for further harmonising the requirements for different players in specific market segments without jeopardising higher-priority policy goals, and there is a strong case for relying more on entity-based rules. The BIS says the regulatory framework should incorporate entity-based requirements for BigTechs in areas such as competition and operational resilience, to address the risks stemming from the different activities they perform. This would help regulation to achieve its primary objectives and serve to mitigate competitive distortions.

"... the proliferation of new technology-enabled business models has raised questions about the regulatory perimeter."

The European Commission' Digital Markets Act proposes rules to prevent digital companies from taking over financial firms by leveraging consumer data or freezing out traditional banks and payment providers. The measures are designed to prevent unfair conditions that "gatekeepers" sometimes impose. Gatekeeper companies are defined by reference to annual revenue, average market value and number of users or EU businesses serviced.

Unfair practices would include hoarding client data and using that information to gain an advantage over competitors or restricting people from using alternative services, the Commission says (see also Chapter 4 on data protection issues). The rules would stop BigTech firms from issuing loans tailored to people based on their data, unless the same information is made available to all financial companies. At the other end of the size spectrum, start-up FinTech firms can encounter barriers to exploring the full potential of the market, such as different licencing procedures. This leads to fragmentation of their activities on a country-by-country basis, making it harder for them to grow and scale up across borders.

Technology & digitalisation: a regulatory priority



Five key drivers are influencing priorities in regulatory agendas.

Consumer protection and financial stability are the bulwarks of much financial services regulation, but the impacts of the pandemic and lock-down measures have brought additional topics to the fore. Volatility in capital markets has led to a renewed focus on systemic risk in relation to computer-led trading strategies and certain types of funds. Also, the pandemic has accelerated trends in the use of technology and digitalisation and demands for sustainable finance, and there are new challenges to doing business across borders. These three trends are now equally prominent drivers of regulatory priorities.

A study by the European Parliament's Committee on Economic and Monetary Affairs highlights several lessons for the regulation and supervision of FinTech companies from the Wirecard case. It notes the complexity of FinTech companies, their technologies and the broad span of their operations, both in terms of bundled services and geographical scope. It says this raises concerns for both customer protection and financial stability. The European Commission has asked the European Supervisory Authorities for advice on the regulation and supervision of FinTech activity; specifically, how to address "same activity, same risk, same rules" issues, more fragmented value chains, the scope of the supervisory perimeters, the prudential risks related to non-bank lending and the protection of clients' funds.

Encouraging and regulating DLT

There is currently limited use of this potentially transformational technology in market infrastructure. Existing financial services regulations were not designed with DLT and crypto-assets in mind and sometimes cause regulatory obstacles. DLT can allow for near real-time settlement, thereby reducing counterparty risk during the settlement process. It could mitigate some cyber risks that centralised market infrastructures raise, such as the single point of failure. It could decrease costs by freeing up capital through reduced need for collateral posting, and automated processes could simplify back-office processes.

The European Commission has proposed a regulatory pilot that will provide a safe environment (a sandbox approach) and evidence for a possible permanent EU regulatory regime. The pilot will not be open to unauthorised firms, so may limit access by smaller innovative fintech firms. The regulation limits the size of the issuance or trading of transferable securities on DLT market infrastructure and excludes sovereign bonds. Trading on DLT infrastructures will be subject to the Market Abuse Regulation. ESMA will be mandated to review MiFID II data reporting and pre- and post-trade transparency rules and to propose amendments for financial instruments issued via DLT.

The DLT Regulation will create the concepts of DLT multilateral trading facilities (MTFs) and DLT securities settlement systems. Existing authorised MTFs or securities settlement systems operated by an authorised central securities depository will be allowed to be authorised as a DLT equivalent and apply for temporary exemptions to existing regulation that curtails the use of DLT. For example, existing regulation envisages trading and settlement functions performed by different infrastructures. If granted the necessary exemptions under the pilot, a DLT MTF could perform functions usually performed by CSDs, such as settlements and safekeeping.

Insurance: doing business differently

In June 2020, EIOPA[1] sought to understand better the insurance value chain, new business models arising from technology and the associated risks, in order to help EIOPA more effectively support regulators as the sector evolves. The paper primarily focused on developments in relation to platforms and ecosystems. EIOPA defined a platform as a technical framework for multiple firms to interact with each other, and an ecosystem as an interconnected set of services allowing firms to address a broad variety of client needs in one integrated experience.

EIOPA noted that increasing complexity in how insurance is being manufactured and distributed, with new kinds of distributors and products emerging, can challenge existing supervisory and regulatory practices. Increased use of outsourcing is expected to transform the way products and services are provided, with benefits for consumers – products that are better targeted, better quality and better value for money. However, it creates new conduct and prudential risks, amplifies or relocates existing risks (operational, IT, security, governance and consumer protection), and can lead to legal and compliance issues.

EIOPA highlighted possible areas for further work:

- More specific analysis of possible regulatory responses to third parties in the value chain
- A follow-up study focusing on the impact of platforms and ecosystems
- Adapting disclosures and advice requirements to the digital world
- Analysis of broader measures that might underpin sound digital markets in insurance and insurance-related data

1 European Insurance and Occupational Pensions Authority

02. Digital payments, currencies and assets

There is a wave of innovation around crypto-assets and technology-based offerings, with corresponding regulatory interest, and central banks are developing digital currencies. There is particular regulatory focus on how to improve payments systems.

Improving payment systems

In October 2020, the FSB set out its high-level road map for developing cross-border payment systems and processes that are faster, more inclusive, less expensive and more transparent, by:

— Committing to a joint public and private sector vision

— Co-ordinating on regulatory, supervisory and oversight frameworks

— Improving existing payment infrastructures and arrangements to support cross-border payments

— Increasing data quality and straight-through processing by enhancing data and market practices

— Exploring the potential role of new payment infrastructures and arrangements

The volume of cashless payments has increased, but cash currently remains the predominant method of retail payments in the EU and the EU payments market is still fragmented. The Commission's vision is:

— A broad and diverse range of high-quality payment solutions, supported by a competitive and innovative payments market, and based on safe, efficient and accessible infrastructures

— Competitive home-grown and pan–European payment solutions, supporting Europe's economic and financial sovereignty

— The EU makes a significant contribution to improving cross-border payments with non-EU jurisdictions, thereby supporting the international role of the euro and the EU's "open strategic autonomy"

Its strategy is based on four interlinked pillars: increasingly digital and instant payment solutions with pan-European reach; innovative and competitive retail payments markets; efficient and interoperable retail payment systems and other support infrastructures: and efficient international payments. For more detail, see here.

Technology companies offering payment services in the eurozone face European Central Bank (ECB) oversight to deliver the principle that the same activities should be subject to the same rules, whether performed by regulated financial firms or Fintech firms. The regulatory perimeter could be adjusted to ensure consistent regulation.

Creating digital currencies

A BIS report of October 2020 sets out foundation principles and core features for central bank digital currencies (CBDCs) – digital payment instruments, denominated in the national unit of account, that are direct liabilities of the central bank. The BIS principles emphasise that:

— A central bank should not compromise monetary or financial stability by issuing a CBDC

— A CBDC would need to co-exist with and complement existing forms of money

— A CBDC should promote innovation and efficiency

Arguments for and against issuing a CBDC and the design choices are driven by domestic circumstances and there will be no one-size-fits-all CBDC, but domestic CBDCs would still have international implications. Co-operation and coordination are therefore essential.

BIS carried out experiments with the Swiss central bank and stock exchange, focusing on how banks and other financial firms can, technically and legally, deal with a wholesale CBDC within the industry's plumbing — as distinct from a retail CBDC that the public would use. The experiments showed that companies could transfer CBDC-backed tokens without any legal issues and make records through DLT. Also, DLT could plug into existing payment system architecture and settle tokens.

> "Crypto-assets have been a focus of regulators around the globe for some time, with regulatory initiatives focusing on the assets themselves, the trading of them or both."

As part of the EU's retail payments strategy, the ECB and European Commission are developing the concept of a digital euro. The Commission notes that a digital euro could support the digitalisation of the EU's economy and its strategic autonomy. Correspondent banking services have been curtailed in recent years, raising questions of how to move money safely across borders. However, a digital euro could pose a threat to EU banks if introduced without the right design features and safeguards. Consumers could switch to holding digital euros rather than cash deposits, which can incur fees and offer little return at current rates. Losing deposits would cost banks a vital source of funding and could lead to increased lending rates.

Regulating crypto-assets

Crypto-assets have been a focus of regulators around the globe for some time, with regulatory initiatives focusing on the assets themselves, the trading of them or both. That trend has increased. However, BIS's November 2020 working paper warns that policymakers must avoid driving stablecoin technology into the ground. "It is essential for authorities [to] have the tools, skills and technology to identify the evolution or creation of stablecoins, in particular global stablecoins, and to build appropriate regulatory and supervisory frameworks," the report said.

The European Commission has issued a draft regulation of markets in crypto-assets (MiCA). The aim is to clarify the application of existing EU rules to crypto-assets and introduce a new, harmonised legal framework for crypto-assets covered by existing rules. It defines three different types of crypto-assets:

— crypto-assets, which are digital representations of value or rights that may be transferred and stored electronically, using DLT or similar technology

— asset-referenced tokens, which purport to maintain a stable value by reference to fiat currencies or commodities and can be used as a means of payment (i.e. stablecoins)

— e-money tokens, which can also be used as a means of payment, but their value is established by reference to only one fiat currency

MiCA will impose different levels of authorisation on the issuers of the different types of assets. There will be rules on capital requirements, conflicts of interest, governance, custody of reserve assets, complaints handling etc. Some requirements will be more stringent for significant asset-referenced tokens and e-money tokens. Crypto-assets falling under MiCA will be subject to bespoke measures to prevent market abuse.

MiCA will grant to national regulators the power to authorise and supervise crypto-asset service providers, with ESMA establishing a register of such firms. The MiFID II definition of financial instrument will be amended to clarify, beyond legal doubt, that such instruments can be issued via DLT. DLT market infrastructures will temporarily be exempted from certain MiFID II provisions to enable them to develop solutions for the trading and settlement of crypto-assets that would qualify as financial instruments. The Commission is also considering updating the prudential rules for crypto-assets held by financial firms and will explore how to leverage DLT to improve capital-raising operations of SMEs.

In the US, the Office of the Comptroller of the Currency (OCC), regulator of US federal banks announced in September 2020 that financial institutions can begin offering cryptocurrency services for customers, in a move described as "a major development" by experts.

03. Digitalisation of customer communications

Firms have embraced and deployed technological solutions to meet the needs of customers, while lockdown measures are in place. Call centres and self-service portals have increased. However, implementation at speed has potentially given rise to conduct risk issues and lack of co-ordination, which may have resulted in dis-jointed customer journeys and/or poor outcomes.

Digital communications with customers about products and services have increased and seem set to be a permanent feature. This calls into question whether disclosure requirements that presume static, paper-based documents should be amended to allow dynamic online disclosures, which can more easily provide bespoke information and promote customer understanding and engagement. More generally, are conduct rules that largely presume face-to-face contact, fit-for-purpose in the digital age?

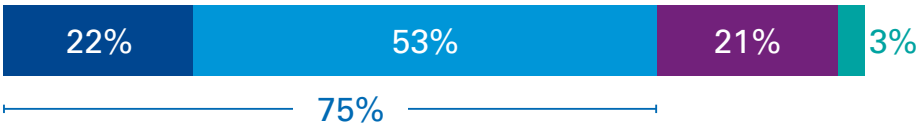
Regulators were already focused on the increase in platforms and portals that provide guidance or advice on investments – **robo-advice.** Given the sharp uptake by consumers of online services in general during the pandemic, this focus has increased.

A report from the European consumer advocacy group, Better Finance found the robo-advice market has not taken off as expected despite benefits like low fees, easy access and limited conflicts of interest. However, the results of its "mystery shopping" will give regulators further food for thought. Better Finance found "extreme divergences" in investment recommendations, with the same investor profile getting results that ranged from 9 to 95 percent exposures to equities. It also found poor transparency on past performance and investment risks, limited disclosures on conflicts of interest and no questioning of customers' sustainability preferences.

Digital identity

The pandemic has accelerated trends in the digitalisation of client onboarding. Given social distancing measures, firms increasingly turned to digital KYC checks to facilitate more remote customer onboarding approaches. The use of different forms of digital identity is spreading and the interest of policymakers in this topic is increasing.

Accelerated progress on digital customer experience



Progress has sharply accelerated, putting us years in advance of where we expected to be
Progress has accelerated by a matter of months
Progress is the same as before the pandemic
Progress has lapsed

Source: KPMG 2020 CEO Outlook COVID-19 Special Edition

Widespread use of digital identity could improve access to financial services and therefore aid financial inclusion, but it could also disenfranchise the digitally incapable and increase risk for other types of vulnerable customers. Regulators are attuned to both its benefits and risks.

Digital identity facilitates mass data infrastructures, leverages scale and reduces operating costs. It is not perfect – verification issues can persist – but it can be underpinned by a robust KYC methodology. Use of digital identity has similar issues to traditional methods – identification, authentication and consent – but the issues manifest themselves in different ways. Access to quality and quantity of data is necessary for building robust authentication.

Cross-border issues are significant and require global co-operation. A digital ID can include data about payments and transactions made by that person, but this raises additional data privacy concerns. It can help firms to identify and tackle financial crime but, if an ID is stolen, it could increase the opportunity for criminal activity.

Despite these challenges and risks, the appeal of digital identity is that it provides a more consistent and robust approach, departing from subjective processes. A robust digital ID could also enable SMEs to enlarge their markets – potential funders could use it to reduce the work required at the identification phase of onboarding. However, a digital ID requires co-operation between regulators and industry to maximise the benefits and mitigate the risks.

Some countries are already acting. Singapore has developed national digital identity infrastructure based on a trusted ID system that extracts data from a golden data source and provides a straightforward onboarding process, supporting people through their life cycle. India has brought 1.5 billion people onto a public data infrastructure and Estonia has introduced a DLT-based public digital identity system, alongside extensive online provision of state services.

Culture is a key variable in rolling out digital identity programmes. **Acceptance of the need to embrace digital identity requires customer trust in the form of the ID, an understanding of how it will (and will not) be used, trust in the data attached to the ID and trust in the entity handling the data.**

Customer 2030

- AI will power mass personalisation and micro-consumption
- Customers will reject generic products for services that achieve their goals
- Good service will mean frictionless transactions; safe, fast and automated
- Democratised finance will reach previously marginalised groups such as vulnerable individuals and SMEs denied credit
- Consumers will understand the value of their data and demand a return

04. Managing and using data

Available data and new types of data sources are increasing at considerable pace. Policymakers regard data as an essential resource for economic growth, competitiveness, innovation, job creation and societal progress, and data-driven applications as benefitting citizens and businesses in many ways.

Regulated firms face challenges in the collation, storing, analysis and transfer of data, especially customer data, including reliance on third parties. The transfer of customer data between firms and across borders is being encouraged via "open finance" initiatives is subject to data protection laws. And the ethical use of data is being defined by regulators.

The ECB's latest review of IT risks in banks defines **IT data integrity risk** as the risk that data stored and processed by IT systems are incomplete, inaccurate or inconsistent across different systems. This applies equally to customer, market and firms' own data. Data quality management refers to defining roles and responsibilities for managing the integrity of the data in IT systems (e.g. data architects, officers, custodians and owners/stewards), to provide guidance on which data are critical from a data integrity perspective. The ECB says that data quality management should be subject to specific IT controls in the different phases of the IT data life cycle, in order to resolve identified IT data integrity issues and properly manage direct-to-customer (B2C) online services.

Efficient and reliable mechanisms for ensuring **data quality** are fundamental. Data are distributed across an organisation and may be organised to a limited extent. "Data lakes" can be costly to establish and many financial services groups continue to operate disparate data systems. There can be challenges in analysing data using different taxonomies and domain sets, and many firms still rely on manual checks.

Firms need to put in place a governance framework for **alternative data sources,** to assess the completeness of the data, validity of the data and the quality of resulting analyses. New technologies can be leveraged to collect and submit large amounts of both structured and unstructured

data. Unstructured data (e.g. from social media) can contain useful insights into client behaviour and developments within a firm or sector, which structured data (such as market prices and ratings) may not reveal. However, unstructured data is often collected in a format that makes it difficult to process, which in turn makes it challenging to analyse efficiently.

The growth in available data, of all types, requires expanded **storage infrastructure** and more efficient search and indexing protocols. One solution to address the rising cost of data storage is to make more use of cloud technology, but this has both advantages and challenges. Cloud service providers can offer geographically dispersed infrastructure and heavy investment in security, providing firms increased resilience and allowing them to scale more quickly and operate more flexibly. However, firms can encounter operational, governance and oversight issues (particularly in a cross-border context), provider concentration risk and increased cyber vulnerability, as noted in Chapter 5.

To share or not to share

While governments, regulators and industry grapple with the legal issues around the transfer of customer data between entities and across borders, the financial sector is being encouraged to embrace "Open Finance". Open Finance is the term used to describe data-sharing principles to enable third-party providers to access customers' data across a broader range of financial sectors and products, including savings and investments. The UK FCA consulted in December 2019 on extending open bank data-sharing principles to other sectors. For more detail read KPMG's "Engaging with Open finance"

The latest consultation from EIOPA seeks views on whether and how far insurance value chains should be opened up by the sharing of insurance-related and specific policyholder data amongst insurance and non-insurance firms. The paper considers an open insurance definition and use cases, the risks and benefits of open insurance, regulatory barriers and possible areas to consider for a sound open insurance framework.

The exchange of both personal and non-personal data through (open) application programming interfaces can facilitate industry-wide innovation and increase the agility of businesses in responding to changes in customer needs and expectations. However, it could also give rise to new or amplified risks such as data security, cyber risks, interoperability challenges, and liability, ethical and broader consumer protection issues. Increased data sharing, especially if combined with AI or ML tools, could also increase financial exclusion.

EIOPA – like other regulatory bodies – is trying to find a balance between regulatory objectives related to data protection and competition, while supporting innovation, efficiency, consumer protection and financial stability.

> "Efficient and reliable mechanisms for ensuring data quality are fundamental."

The ethical use of data

In its June 2020 consultation, IOSCO refers to the definition of ethics as "a set of moral principles or rules of conduct that provide guidance for our behaviour when it affects others" and has suggested that fundamental ethical principles include honesty, fairness, diligence, care and respect for others. Ethical conduct follows those principles and balances self-interest with both the direct and indirect consequences of that behaviour for other people.

IOSCO went on to observe that, in the context of AI and ML, ethical concerns may arise where the data the models use are biased because data cleaning, data transformation and anonymisation of data were not adequately considered. The models may then behave in a biased way (for example, exhibit social biases) and potentially recommend undesirable outcomes.

There are questions about how these types of ethical considerations can continue to be met by firms and their employees as algorithmic models play an increasingly important role in the functioning of markets.

IOSCO's Fintech Network identified robo-advice as one type of AI/ML application with significant potential ethical implications. While most robo-advisors use simple rule-based algorithms, some are moving towards the use of predictive ML algorithms. IOSCO says that firms should be careful when using large pools of alternative, non-traditional datasets, such as satellite data or twitter feeds, to ensure that the developed models do not discriminate against a certain segment of the population and that the AI/ML-driven decisions are fair and unbiased.

The Network identified five primary themes that could underpin the ethical use of AI and ML techniques:

- **Beneficence – "do good":** ensuring the model is being used and/or acting in good faith, in the best interest of investors and with market integrity
- **Non-malfeasance – "do no harm":** having the ability to understand and interpret AI/ML based decisions to identify where misconduct may be taking place
- **Human autonomy,** including auditability: ensuring humans have power over what the model can and cannot decide
- **Justice:** accountability and transparency: ensuring there is accountability at senior level for the actions of the model and that accountability comes with appropriate understanding of the models, to be able to demonstrate justice, internally and with clients
- **"Explain-ability":** ensuring the outcomes arising out of the models can be explained

Firms can mitigate unintended ethical risks and challenges caused by the use of such tools, by focusing on their risk management over the electronic-to-electronic data cycle and their culture, accountability, expertise and operational resilience.

05. A focus on resilience

Regulators are concerned about firms' resilience to heightened technological risks, with outsourcing to third parties, cybersecurity and management of IT risks being common themes.

Outsourcing

The FSB is consulting on issues and challenges relating to outsourcing and third-party relationships, including over-reliance on a small group of technology providers. The FSB says that firms should ensure their contractual agreements with third parties grant to them, and to supervisory and resolution authorities, appropriate rights to access, audit and obtain information from these third parties.

These rights can be challenging for firms to negotiate and exercise, particularly in a multi-jurisdictional context. As part of its FinTech Action Plan, the European Commission intends to prescribe standard contractual clauses for such outsourcing agreements. Meanwhile, ESMA has issued new guidelines on outsourcing to cloud service providers and cloud aggregators (where the outsourcing is intermediated by another third party). Firms should review their existing outsourcing arrangements against the new guidelines by end-2022.

The guidelines are in line with existing EBA and EIOPA guidance but go further in several areas and may make outsourcing to cloud service providers more onerous. **Firms must put in place a specific strategy for any cloud outsourcing services, including appropriate governance arrangements and more stringent cyber security measures.** Before contracting with a provider, firms should carry out analysis and due diligence, include specific terms around auditing and subcontracting, and agree an exit strategy. Firms or groups also subject to EBA and EIOPA guidance might have preferred an aligned approach, and the guidelines around governance, oversight and documentation may be challenging for smaller IT departments. The need to complete a very specific cloud strategy may be outside the capability of some firms, which will need to seek external guidance.

Cyber security

The FSB's final report on effective practices for Cyber Incident Response and Recovery sets out a toolkit of 49 practices across seven components: governance, planning and preparation, analysis, mitigation, restoration and recovery, co-ordination and communication, and improvement.

The European Commission's new cybersecurity strategy includes overhauling existing rules for critical sectors. The 2016 Networks and Information Security (NIS) Directive will be extended to cover additional sectors and place stricter requirements on "essential entities", including financial services and cloud and data service providers. A Critical Entities Resilience Directive will impose rules to protect physical assets, networks and grids from being tampered with, and give greater powers to cybersecurity authorities to issue warnings, impose fines, force a temporary halt to services and suspend licences.

Firms will need to pay closer attention to the cybersecurity of their software and hardware suppliers: supply chain security. The Commission is undertaking a risk assessment of supply chains for critical and strategic industries, which could lead to future rules on software companies.

IT risk

The ECB sends an annual IT Risk questionnaire to all significant institutions it supervises in order to collect standardised information regarding the assessment of IT risks, structured around the EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP). The latest review found that:

- Year-on-year, banks' self-assessments have become more prudent but are still optimistic regarding IT governance
- A significant number of banks rely on end-of-life systems for critical processes
- Several banks are exposed to high concentration risk, with over half concentrating 50% of their total IT outsourcing contract value with a single external provider
- The large majority of critical findings, not addressed for more than one year, related to IT security risk, which continues to be a significant challenge

The main shift was reported in areas with high supervisory attention, namely data quality management and IT risk management, but control scores were noted to be the weakest. The ECB expects IT and cyber risk to be part of banks' general risk governance and management framework, with broad awareness of these risks across the entire organisation.

Digital operational resilience

The European Commission has coined the term "digital operational resilience". This builds on existing regulatory expectations around operational resilience, but focuses on the ability of firms to build, assure and review their operational integrity from a technological perspective. A new regulation – DORA – will establish comprehensive rules for all regulated firms. See here for more detail and look out for our forthcoming new reality paper on the broader subject of operational resilience.

06. Governance of, and by, technology

Regulators are emphasising that increased use of technology requires firms to revisit their governance arrangements and controls to ensure they have the right level of expertise and understanding at senior management levels in order to govern well and to identify emerging and heightened risks. AI and ML are attracting particular regulatory attention in this regard.

Equally, technology can help firms to govern their businesses, manage risks and improve customer outcomes. In particular, regulated firms are using technological applications – RegTech – to ensure they have a full understanding of the rules to which they are subject and to check or validate their compliance with those requirements.

The points raised in Chapter 4 about data governance apply to the governance of digitalisation and use of technology across the piece. Technological applications can challenge traditional governance arrangements and controls and increase the divide between the tech savvy and technophobes. The positions of Chief Technology Officer and Chief Data or Information Officer, in addition to Chief Operating Officer, are being created, in part to help bridge this divide at senior management level. Extensive remote working is challenging traditional governance structures and controls (see our new reality paper, "Remote governance and controls").

AI and ML governance and controls

IOSCO consulted until late October 2020 on appropriate regulatory frameworks in the supervision of market intermediaries and asset managers that utilise AI and ML. It proposed six measures that reflect expected standards of conduct and are equally applicable to any technology:

1. **Governance and responsibilities:** designated senior management responsible for the oversight of the development, testing, deployment, monitoring and controls of AI and ML.
2. **Development, testing and ongoing monitoring of techniques:** adequate testing and monitoring of algorithms, to validate the results of an AI and ML technique on a continuous basis.

3. **Knowledge and skills:** staff with adequate skills, expertise and experience to develop, test, deploy, monitor and oversee the controls over the AI and ML that the firm utilises. Compliance and risk management functions should be able to understand and challenge the algorithms that are produced and conduct due diligence on any third-party provider, including on their level of knowledge, expertise and experience.
4. **Operational resilience:** firms to understand their reliance upon and manage their relationship with third-party providers, including monitoring their performance and conducting oversight.
5. **Transparency and disclosure:** disclosure of the use of AI and ML by firms.
6. **Systems and controls:** firms should have appropriate controls in place to ensure that the data on which the performance of the AI and ML systems depend are of sufficient quality to prevent biases and are sufficiently broad for a well-founded application of AI and ML.

Although the final guidance will not be binding, IOSCO has encouraged regulators to consider these proposals (as well as the proportionality of any response) in the context of their legal and regulatory frameworks.

Some national regulators were already active in this space. Back in 2019, for example, the Dutch National Bank said financial firms using AI should pay attention to the soundness, accountability, fairness, ethics, skills and transparency ("SAFEST") aspects of applications they develop. The Dutch regulators set out principles regarding the design of digital advice to customers to make informed decisions and on consumer protection in the online market, focusing on the use of behavioural manipulation and the prevention of unethical practices.

The Bank of England and FCA are exploring uses, impacts and challenges of AI in financial services and how regulation could be used most effectively through their Artificial Intelligence Public Private Forum (AIPPF). The AIPPF includes financial firms, academics and technology firms and seeks to leverage learnings from other industries.

> "Technological applications can challenge traditional governance arrangements and controls and increase the divide between the tech savvy and technophobes."

Meanwhile, in relation to internal risk frameworks and modelling, firms are grappling with understanding how data bias can affect their AI/ML models and how best to eliminate it.

Use of RegTech grows

The pandemic forced regulators rapidly to adjust or ease certain requirements, or introduce new ones, such as bans on short selling. RegTech applications helped firms to spot and adapt to these changes. RegTech also enabled firms to automate and amend processes to improve their effectiveness in a remote working environment. As noted in Chapter 3, given social distancing measures, firms increasingly turned to digital KYC checks and other methods to facilitate more remote customer onboarding approaches. The FSB's October 2020 report on the use of RegTech and SupTech found that over half of RegTech uses are in the areas of fraud detection, anti-money laundering (AML) and countering terrorist financing (CTF), and KYC.

RegTech can reduce costs, increase consistency, expand coverage, improve the effectiveness of compliance and reduce key person risk. Its use can improve compliance and customer outcomes, enhance risk management capabilities, and generate new insights into the business for improved decision-making, the FSB said. However, the report also noted that authorities are vigilant to possible risks that could arise from the use of RegTech, with resourcing risk, cyber risk, reputational risk and data quality issues at the top of their list of concerns. The role of data standards and the importance of effective governance frameworks were also emphasised by the FSB.

In Europe, EBA conducted a RegTech survey until September 2020, inviting all relevant stakeholders, including financial institutions and ICT third party providers, to share their views and experience on the use of RegTech solutions. The aim of the survey was to understand better the ongoing activity in this area, raise awareness on RegTech within the regulatory and supervisory community, and inform any relevant future policy discussion specifically in the areas of AML/CFT (ongoing monitoring of the business relationship and/or transaction monitoring). creditworthiness assessment, compliance with security requirements and standards (information security, cybersecurity, payment services) and supervisory reporting.

EBA also sought views on ways to facilitate the adoption and scaling up of RegTech solutions across the EU while acknowledging and looking to address the underlying risks. The survey focused on:

- Mapping and understanding existing RegTech solutions
- Identifying the main barriers and risks related to the use of RegTech solutions
- Identifying potential ways to support the uptake of RegTech across the EU

Pandemic impacts RegTech firms

Despite the increased opportunities for Regtech to show its potential, the pandemic could also negatively impact the business models of RegTech firms. Funding, recruitment, cash flow and projects are being affected by the economic downturn, and the decline in venture funding is impacting future investment rounds. A high proportion of start-ups and scale-up RegTech firms may be at risk of failure as they embark on raising funds or have taken on cost burdens associated with growth. Such firms may also face a temporary fall in client demand as financial services firms prioritise other more business-critical projects or their own financial resilience.

07. Regulators embrace technology

Regulators are trying to keep abreast of change in the way they perform their supervisory and enforcement activities, including taking advantage of technology to improve the efficiency of their own processes, revamping their websites and adopting new data collection methods. They are increasing using technology – "SupTech" – to interrogate the reports and submissions they receive from firms and to monitor market activity. The pandemic provided a test case for how SupTech can be used, allowing regulators to respond with greater speed and agility.

Lockdown measures caused many regulators to move to electronic-only communications with regulated firms, using online meeting applications, not requiring hard copies of application forms or submissions, and accepting e-signatories. Indications are that this will remain a feature going forward, even when restrictions are fully lifted. Regulators are keen, though, to reinstate visits to regulated firms' premises to interrogate what is happening in practice, rather than relying solely on firm's submissions or telephone/online calls.

The FSB's October 2020 report on the use of RegTech and SupTech found that the substantial increase in availability and granularity of data and new technology have increased the opportunities provided by SupTech applications. The FSB noted that the use of SupTech can improve oversight, surveillance and analytical capabilities, and generate real-time indicators of risk to support forward-looking, judgement-based, supervision and policymaking. However, the report also noted that authorities are vigilant to possible risks that could arise from the use of SupTech, including the risk of over-reliance on methods built on historic data, which could lead to incorrect inferences about future trends.

Most respondents to the FSB's survey already had in place a SupTech, innovation or data strategy. ESMA's Strategic Orientation for 2020-22 includes significant expansion of its digital communications by creating a more responsive, informative and user-friendly website. This includes enhancing its IT systems and data analysis capacity to create a data hub for EU securities markets. It will help ESMA to gather market intelligence, develop retail risk metrics and identify potential causes of investor harm.

An example of national regulators adopting new strategies is the Spanish regulator's (CNMV's[2]) Plan de Actividades 2020, which sets out four priorities – digital transformation, sustainability, remote working by regulatory staff and boosting competitiveness of the Spanish market by speeding up its own administrative processes.

The importance of data and analytics

Switzerland and Austria have each adopted a data standard, while other regulators are inclined to leave it to industry, including the UK PRA and FCA. However, they set out ambitious data strategies in January 2020. They want to be smarter in the way they use data and advanced analytics, to transform the way they regulate and to reduce the burdens on firms. They are seeking to automate responses and be more proactive, and to ensure the solutions they are developing are flexible and future proof.

> "... smarter in the way they use data and advanced analytics."

Flexible sourcing of data, including use of media coverage, complaints data, firms' operational data and external industry data bases, will enable the UK regulators to move away from sole reliance on firms' regulatory returns. Success criteria will be improved data quality, simpler submission process for firms, reduced reporting burden on firms, and improved data combining and analytics. The regulators continue to be open to new ideas and innovation and are keen to collaborate and not do everything themselves.

The future of onsite inspections

In our paper, "Remote governance and controls", we noted the challenges for firms of large-scale and prolonged remote working. We also considered the implications for regulators, including the need for a fundamental re-assessment of the data they need and for what purpose. And for both supervisory and enforcement activities, there is now a significant question to answer: **how to inspect and enforce in a largely remote working world? Is an increased reliance on data and desk-based analyses sufficient?**

2 Comisión Nacional del Mercado de Valores

Contact us

Francisco Uria Fernandez
EMA Head of FS and Banking & Capital Markets
T: +34 9145 13067
E: furia@KPMG.es

Karim Haji
UK Head of Financial Services
T: +44 20 7311 1718
E: karim.haji@kpmg.co.uk

James Lewis
Co-Head of EMA FS Regulatory Insight Centre
T: +44 20 7311 4028
E: james.lewis@kpmg.co.uk

Kate Dawson
EMA FS Regulatory Insight Centre
T: +44 20 7311 8596
E: kate.dawson@kpmg.co.uk

Julie Patterson
EMA FS Regulatory Insight Centre
T: +44 20 7311 2201
E: julie.patterson@kpmg.co.uk

Fabiano Gobbo
Global Leader, Financial Risk Management
T: +39 0267 6431
E: fgobbo@kpmg.it

Dr Kay Swinburne
Chair of EMA FS Regulatory Insight Centre
T: +44 207 311 2588
E: kay.swinburne@kpmg.co.uk

Michelle Adcock
EMA FS Regulatory Insight Centre
T: +44 20 3306 4621
E: michelle.adcock@kpmg.co.uk

Philip Deeks
EMA FS Regulatory Insight Centre
T: +44 20 7694 8545
E: philip.deeks@kpmg.co.uk

kpmg.com/regulatorychallenges

CREATE | CRT134110A | March 2021