KPMG

Regulation and supervision of fintech

Ever-expanding expectations

March 2019

kpmg.com

Contents

Executive summary

Fintech is already delivering significant benefits to consumers and investors; to financial services firms and financial market infrastructure; and to financial stability and financial inclusion. However, the increasing use of fintech solutions and emerging technologies also brings risks, to which regulators and supervisors are responding.

Consumers and investors are benefitting from both the emergence of new fintech solutions and the evolution of existing financial services providers. This has generated a wider range of financial products and services being delivered more efficiently and effectively, with competitive pressures on firms to adopt a more consumer-centric approach.

The regulatory and supervisory response to fintech has evolved through three stages. Initially, the response was to focus on the benefits of fintech and on supporting the growth and adoption of new fintech solutions. Regulatory intervention was limited to little more than fine-tuning to take account of the impact of fintech on the ways in which financial services were provided.

Fintech

"Technologically enabled financial innovation that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services."

Financial Stability Board

In the second stage, regulators and supervisors began to worry increasingly about the risks arising from fintech.

These risks can be characterised as risks to:

- Consumers and investors;
- Financial services firms; and
- Financial stability.

In the third stage, regulators and supervisors have been taking specific actions in response to these risks. This has included the development of international standards (these standards are shown in the timeline on pages 11-12), the implementation of increasingly detailed and prescriptive national rules and guidance, and shifts in supervisory priorities.

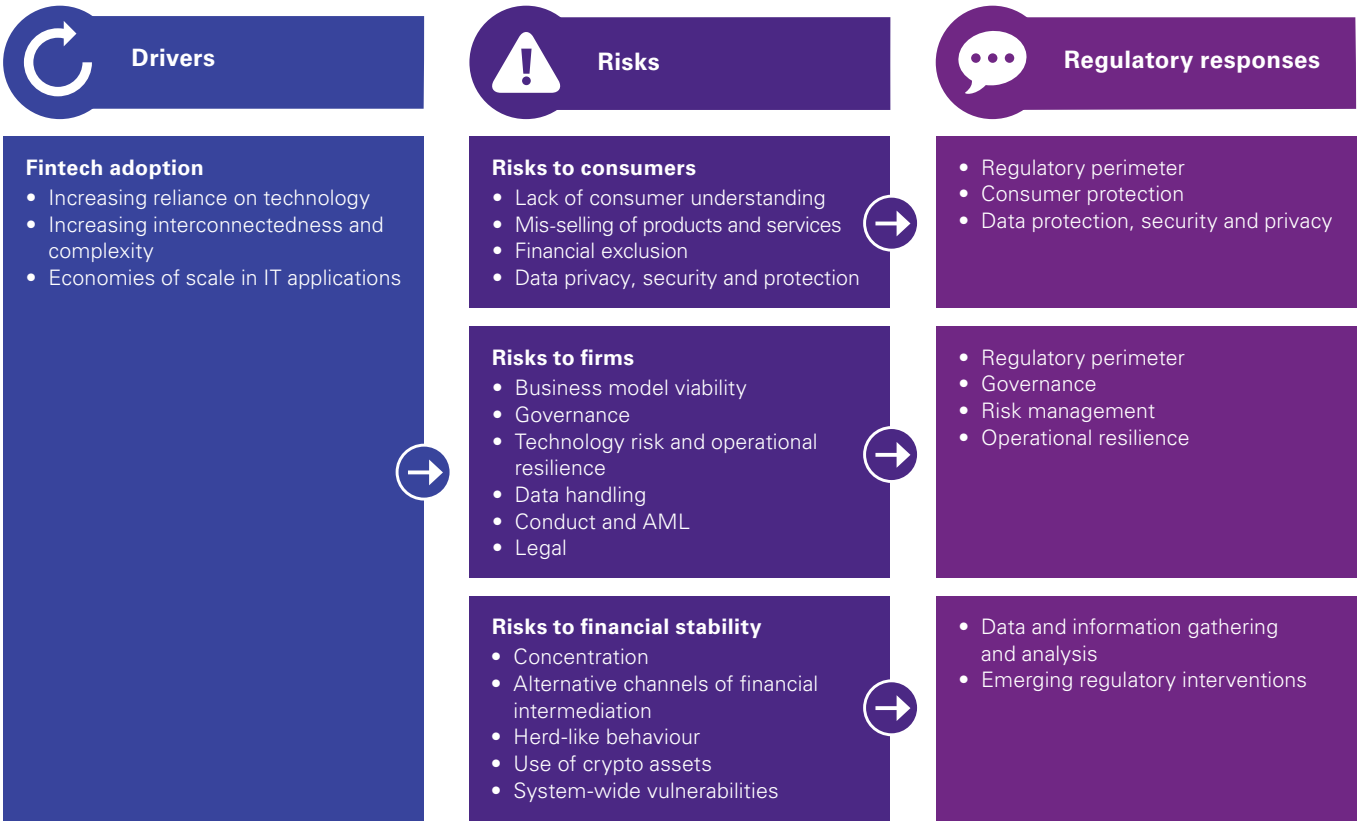
These initiatives cover a wide range of areas, including technology risk, cyber security and operational resilience more generally; data privacy; consumer protection; firms' governance and risk governance; and amendments to anti-money laundering requirements.

The emerging international standards have mostly taken the form of high-level principles, leaving national implementation (both regulation and supervision) to diverge considerably across jurisdictions and across different financial services sectors.

Financial services firms need to be able to demonstrate not only that they are in compliance with the growing array of fintech-related regulatory requirements but that they have considered and taken into account the various risks posed by fintech more generally.

Successful well-managed firms will adopt a proactive response to emerging risks and to evolving regulation and supervision, not a purely reactive response as and when regulatory and supervisory reactions are finalised.

Fintech regulation



Implications for firms

Firms entering the fintech space – established financial institutions, established non-financial corporates and start-ups – need to factor the ever-changing nature of regulation and supervision into their strategies, business planning, governance and risk management.

Overall approach

As with all business and operational developments, financial services firms need to consider the wide range of risks arising from the use of fintech and ensure that these risks are properly captured within a firm's risk governance structure and procedures.

Firms should also be aware of, and responsive to, the different ways in which regulation and supervision might affect their businesses, and to build this assessment into their strategic planning and risk mitigation activities.

This needs to be a proactive process, led by the firm itself, thinking in advance about how it can address and mitigate fintech-related risks, not a purely reactive response to regulatory and supervisory initiatives as and when they emerge.

Established financial institutions that adopt fintech may – at least initially – face different types of regulation and supervision to established fintech-enabled non-financial corporates and start-ups entering the financial services sector, but over time these differences are likely to diminish.

Redrawing the regulatory perimeter

Regulators are redrawing the regulatory perimeter to take account of new or changing products and services emerging as a result of fintech solutions and emerging technologies.

Governance

Ever-expanding regulations and supervisory expectations are being introduced to require the Boards and senior management of firms to understand, oversee and manage effectively the risks arising from the development and adoption of fintech solutions and emerging technologies.

Regulatory and supervisory pressures on firms' governance

- Board and senior management level awareness and understanding of fintech applications and fintech-related risks.
- Active board level engagement on issues such as cyber security, outsourcing, and operational resilience more generally.
- Clarity of senior management responsibilities and accountabilities for fintech applications.
- Board level consideration of the implications of fintech developments for the substance and viability of a firm's strategy and business model.

Risk governance framework

Regulators and supervisors are focusing on how fintech affects the core risk governance competencies of identifying, managing, measuring and controlling risks across the three lines of defence, and having the appropriate resources, skills and expertise to deliver this effectively.

Depending on the business activities and fintech applications adopted by a firm, this is likely to cover at least the development of new products and services, outsourcing, the use of artificial intelligence and the automation of both front and back office tasks, technology risk, cyber security, operational resilience, AML and conduct risk.

Data

While firms are expected to meet existing data protection requirements, they also need to take a proactive approach to the possibility that fintech developments may lead to a fundamental re-thinking of data privacy, security and protection by financial services regulators and by data protection authorities more generally.

Business model

Current and prospective regulation and supervision may have an impact on a firm's strategy and business model.

Some business opportunities may be constrained by regulators and supervisors intervening to prevent or limit what firms can do (for example, restrictions on sales of some products to more vulnerable and less sophisticated consumers and retail investors), while in other cases firms may need to adjust their product and service offerings in response to the costs of meeting regulatory requirements.

Different approaches across jurisdictions

Divergences across jurisdictions in the regulation and supervision of fintech activities are an important consideration for firms in deciding where to locate these activities. This could result in regulatory arbitrage where firms are attracted by lower regulatory requirements, but equally there have been examples of firms wanting to promote their fintech activities on the basis that they are regulated and supervised to high standards.

Regulatory and supervisory pressures on firms adopting fintech

Fintech risks

Regulators and supervisors have identified risks arising from three main fintech-related drivers, namely the increasing reliance of financial services firms on technology, the increasing interconnectedness within the financial sector, and the prospect of greater concentration and herd-like behaviour.

The list of fintech-related risks identified by regulators and supervisors has grown rapidly over the last few years. There are three main drivers of these risks.

Financial services firms are becoming increasingly reliant on technology and on the use of large data sets.

The use of technology is not new, but the pace of change has picked up markedly and expanded into areas that are new for many firms, including data collection and analytics, artificial intelligence, automation, robo-advice, cloud computing services, platforms, blockchain and crypto assets.

The financial sector is becoming increasingly interconnected and complex.

Examples of this include the outsourcing of many fintech-related functions and services, and the increasingly platform-based nature of many financial services.

Economies of scale tend to be strong in IT applications, leading to a natural tendency for a highly concentrated market with a small number of large providers.

Meanwhile, the use of the same or similar IT solutions by financial services firms may generate herd-like behaviour.

In response, regulators and supervisors have identified a wide range of risks – to consumers, to regulated firms themselves, and potentially to financial stability.

Risks to consumers

Although fintech should bring many benefits to consumers, there is also scope for consumers to be disadvantaged.

Lack of consumer understanding – consumers may not fully understand the nature and risks of the fintech-related products and services they are being offered.

Mis-selling of products and services – the adoption of new fintech solutions could inadvertently, or intentionally, provide new or different ways for manufacturers and distributors of financial products and services to mislead consumers, or to expose consumers to fraudulent activities. More complex value chains may also complicate the responsibilities and accountabilities for redress and remediation when misconduct occurs.

Financial exclusion – the increasing use of big data analytics offers scope for greater price and availability discrimination, while increasing digitalisation may exclude older and other vulnerable consumers.

Data privacy, security and protection – consumers are vulnerable to the loss of data, and may not understand the ways in which their data are being used.

Reduced competition – although the initial influx of new entrants has increased competition, and niche players are likely to continue to provide competition in some parts of the value chain, natural economies of scale in technology and data handling may eventually result in some markets being dominated by a small number of large firms.

Risks to firms

Although the precise nature of the risks depends on the types of fintech solutions and new technologies that firms are adopting, the identified risks to regulated firms fall into six broad categories.

Business model viability – fintech developments have increased the competitive pressures on many financial services firms. Some will struggle to survive.

Governance – the boards and senior management of firms may not have sufficient awareness and understanding of fintech and of fintech-related risks, and may therefore be unable to identify, measure, manage and control these risks effectively. Responsibilities and accountabilities for fintech and risk management may also not be sufficiently clear.

Technology risk and operational resilience – the increased reliance on technology, the increasing use of outsourcing to third party providers of technology and data, and other forms of increasing interconnectedness all serve to heighten risks around operational failures, control over third party providers and cyber security.

Financial institutions are becoming increasingly vulnerable to internal and external attacks, including cyber-attacks, and to operational failures that may arise from inadequate business continuity planning for IT systems and processes, or poor processes relating to IT change management – especially for firms with multiple and old legacy IT systems.

Fintech may prove to be yet another example of the familiar story of business developments running ahead of the ability of some firms to put in place the systems and controls necessary to manage and control the risks.

Data handling – as customer data become even more valuable this increases the potential for misuse and concerns about data privacy and protection. In addition, data limitations may make it difficult for firms to validate outcomes, not least where artificial intelligence is used to analyse data sets and to generate solutions.

Conduct and AML – fintech adoption and the resulting changes in how firms operate could result in firms struggling to meet conduct of business, market dealing and anti-money laundering requirements.

Legal – some fintech applications raise difficult legal questions, some of which remain to be fully resolved, not least where cross-border operations extend across different national legal and regulatory frameworks.

Risks to financial stability

Although mostly still at a stage where the risks to financial stability remain small, regulators are paying increasing attention to the potential risks to financial stability from a number of fintech-related developments. There is also the more general concern of whether there is sufficient information available to track accurately the magnitude and precise nature of some of these developments.

Concentration – successful fintech firms (and fintech adopters) and a small number of dominant third party suppliers may emerge as being of systemic importance.

Alternative channels of financial intermediation – non-bank providers of credit, payment systems and other financial activities may grow rapidly while not being regulated appropriately.

Herd-like behaviour – this may arise from the widespread use of similar machine learning and other strategies for lending or trading.

Use of crypto assets – although the use of crypto assets is relatively low, there are concerns that an increasing use of crypto assets could lead to financial instability as a result of price volatility and the potential impact of crypto assets on payment systems.

Vulnerabilities – from the increasing levels of operational risk and cyber risk in the financial system.

Regulation and supervision

Fintech is moving rapidly from 'under the regulatory radar' and is attracting growing regulatory responses and supervisory scrutiny. The list of regulatory and supervisory responses to fintech-related risks continues to lengthen. This will ratchet up over the coming years as the fintech sector and the adoption of fintech solutions continue to develop and grow, and as the associated risks evolve.

The regulatory response to fintech is moving on from high level principles – for example the ten "considerations" for banks and their supervisors set out in the Basel Committee's February 2018 sound practices paper on the implications of fintech developments – or a reliance on existing legislation and rules to a more detailed application of new rules and guidance to the specifics of fintech-related activities.

There may not yet be a one-for-one mapping of regulatory responses to each identified risk, but on past performance we can expect regulators to end up not far away from such an outcome.

Despite the growing number of sets of fintech-related international principles and standards, the implementation of these principles and standards remains very uneven and inconsistent at national level, while some countries have introduced very detailed regulations in some specific areas.

Our earlier paper *Regulation 2030: what lies ahead?* raised the question of whether the regulatory response to fintech might provide an opportunity to redraw the boundaries about where consumer/investor responsibility begins and ends, or similarly to use fintech as a way of improving risk warnings and then leaving the choices and consequences to consumers/investors. All the evidence to date points in the opposite direction, so firms can expect ever more detailed regulation of their fintech-related activities, especially (but by no means only) where they touch on retail consumers and investors.

Regulation

The regulatory response to fintech takes many forms.

Regulatory perimeter – some fintech developments, such as the use of crypto currencies, the outsourcing of cloud computing, and the move of some non-financial services firms into the provision of specific products and services such as lending to SMEs and retail payments systems, raise questions about where the regulatory perimeter should be drawn. The regulatory net is widening, and some firms that are currently outside the perimeter may find themselves subject to regulation in the future.

As the regulatory net widens, the intensity of regulation may also increase. For example, the regulatory requirements on loan-based and investment-based crowdfunding have tended to expand from their initial emphasis on clear communications and risk warnings to funders. These requirements have shifted to a focus on service providers holding capital-type resources to protect funders in some circumstances, and putting in place adequate procedures for credit risk assessment, governance, systems and controls, and complaints handling. This is also reflected in guidance on fintech credit licence applications, with a focus on governance, internal controls, operations, capital and liquidity.

Retail conduct – regulators are turning to familiar approaches to consumer protection in the fintech age, using a mixture of (a) transparency and disclosure to raise consumer awareness of the nature and risks of products and services, (b) prohibiting or limiting the sale of some products and services to retail customers, and (c) re-writing detailed conduct of business requirements to adapt them to fintech developments.

Data and artificial intelligence – existing data protection legislation, such as the EU General Data Protection Regulation (GDPR), already covers some of the data protection issues arising from fintech.

But fintech developments are continually highlighting new areas in which additional or refined regulation may be required, for example in the use of artificial intelligence and distributed ledger technology, and in the general trend towards the gathering of an ever-broader range of financial and non-financial data from, and sharing across, a wider set of parties. A more intense debate can be expected about whether there are appropriate frameworks in place for the gathering, storing, sharing and use of data, both domestically and cross-border.

Governance of regulated firms – regulators are increasingly setting rules or guidelines that focus on ensuring that boards and senior management have sufficient awareness and understanding of the fintech applications being used by the firm, in order to manage the risks effectively. Some regulators are also requiring firms to identify clear individual senior manager responsibilities and accountabilities for managing fintech-related risks.

Within this approach, some regulators are also focusing on board and senior management responsibilities in specific areas of risk such as algorithmic trading, cyber security, outsourcing to third party service providers, and operational resilience more generally.

Risk management – although mostly covered by existing regulatory requirements on risk management, some fintech developments have generated regulatory responses calling for regulated firms to address specific fintech-related emerging risks within their risk management framework. This has included the money laundering and market abuse risks in the use of crypto assets; the risks arising from the use of distributed ledger technology in payment, clearing and settlement systems, and more generally in the storing and validation of transactions data; the application of outsourcing principles to specific fintech applications such as cloud computing and artificial intelligence; the testing and use of artificial intelligence, machine learning and 'big data' across a range of applications; and data privacy, security and protection.

Cyber security – regulators are generally focusing on the national implementation of international standards in the key areas of governance, workforce skills and capabilities, identification (risk analysis and assessment), protection and detection (access management, information security, security controls, expertise and training, monitoring and testing, and information sharing), and incident response (crisis management, recovery and learning lessons).

Open banking – regulation has in part constituted a market in open banking by establishing the basis on which data can be shared between different parties, usually through an application programming interface (API).

Accounting and regulatory treatments – fintech can generate new types of exposure, such as to crypto assets, requiring the clarification or revision of the accounting and regulatory (risk weight) treatments.

Financial stability – the first steps by regulators here are likely to continue to focus on data and information gathering and analysis, but in due course some regulatory interventions may emerge in response to fintech-related risks to financial stability.

Endorsing industry and other codes and principles – regulators and supervisors may rely in part on codes and principles developed by the industry or by other agencies.

For example, the EU Commission has established a High-Level Expert Group on Artificial Intelligence, tasked with making recommendations on policy development and on ethical, legal and societal issues related to artificial intelligence. The Group proposed a draft set of artificial intelligence ethics guidelines in December 2018.

Similarly, in the UK the government has established a Centre for Data Ethics and Innovation. Although not itself a regulator, the role of the Centre will be to analyse and anticipate gaps in governance and regulation that could impede the ethical and innovative deployment of data and artificial intelligence (AI); agree and articulate best practice, codes of conduct and standards that can guide ethical and innovative uses of data and AI; and advise government on the specific policy or regulatory actions required to address or prevent barriers to innovative and ethical uses of data and AI.

Main regulatory responses to emerging technologies and fintech solutions

	Changing the regulatory perimeter	Disclosures to consumers	Limits on retail investor access	Governance of firms	Firms' risk management	Operational resilience of firms	Data protection	AML	Concentration and competition
Crypto assets	✓	✓	✓					✓	
Distributed ledger technology					✓	✓	✓		✓
Cloud computing					✓	✓	✓		✓
Crowdfunding	✓	✓	✓	✓	✓				
Payment systems	✓	✓		✓	✓	✓	✓		✓
Artificial intelligence, machine learning and use of big data		✓		✓	✓		✓		✓

✓ : Denotes the main types of regulation that are being introduced in response to each type of fintech development.

Supervision

Supervisors are increasingly reflecting fintech-related issues in their supervisory priorities. This is seen most generally in areas such as cyber security, outsourcing, operational resilience and AML.

To a large extent the focus here is on the 'basics' of how regulated firms identify, monitor and manage the risks to them arising from fintech. Supervisors are reviewing and evaluating how firms address these risks through their strategic and business planning, new product approval and outsourcing procedures, and risk management practices more generally; and how firms monitor and review the impact of fintech on their compliance with applicable regulatory requirements, including those related to consumer protection and data protection.

More specifically, supervisors are focusing (to varying degrees across countries) on:

Business models and viability – whether a firm has a well-considered strategy and business model that takes account of fintech developments and provides a solid basis for the continuing viability and sustainability of the firm.

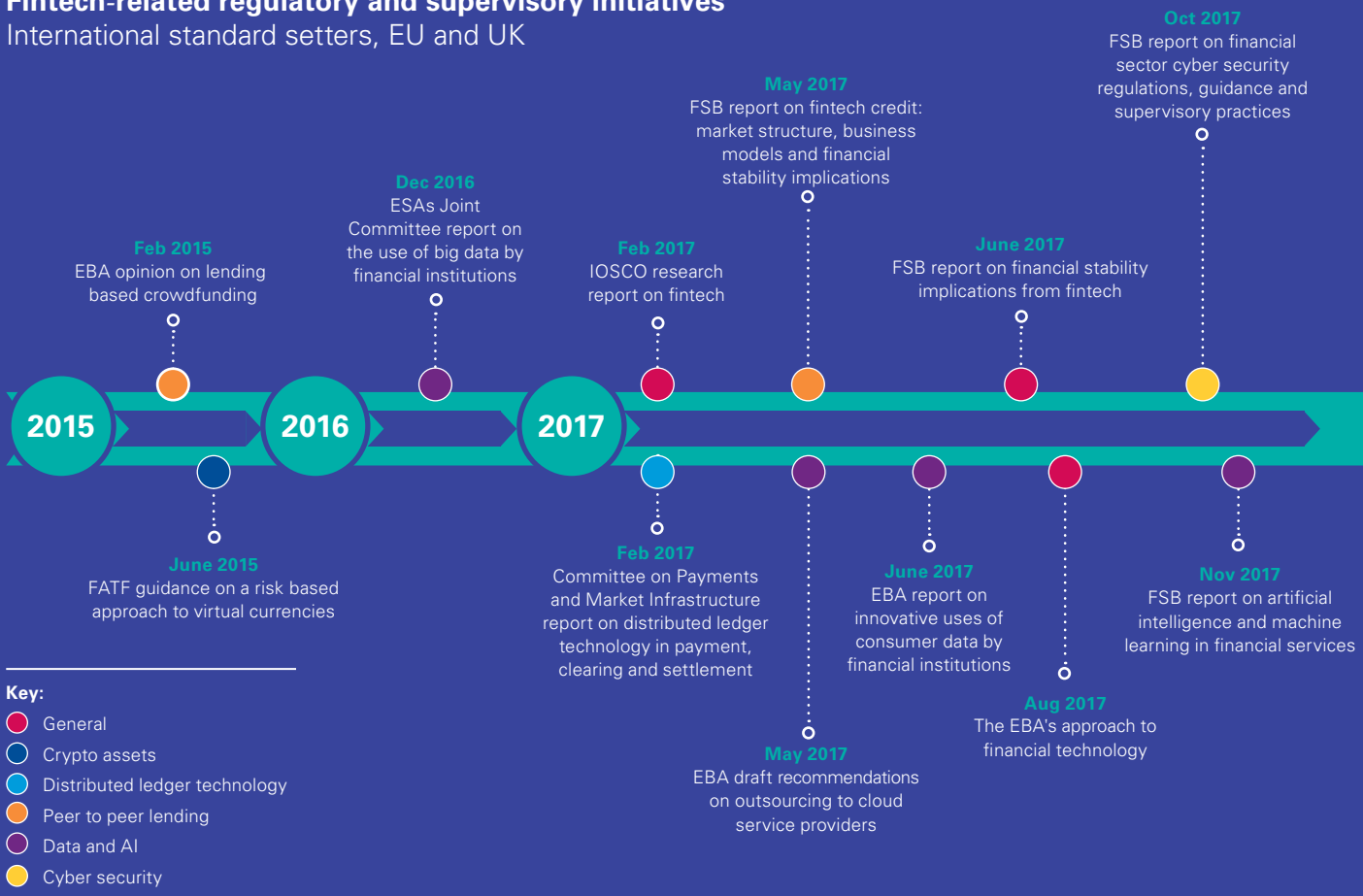
Governance – how well boards and senior management understand fintech and its related risks, and how well a firm has identified, assessed and addressed these risks.

Risk management function – whether firms have reshaped their internal organisation in response to fintech developments, with adequate resources and clear reporting lines across all three lines of defence; and whether firms (and indeed their supervisors) have the technical capabilities required to manage technological innovation, including hiring for appropriate skill sets such as data scientists, mathematicians and statisticians.

Conduct – in addition to complying with specific detailed regulatory requirements, whether firms are taking a more wide-ranging view of how fintech may be changing the risks facing consumers and how these risks might be addressed.

Fintech-related regulatory and supervisory initiatives

International standard setters, EU and UK



Outsourcing – whether firms are exercising appropriate oversight over third party providers, including the firm's access and audit rights, and the implications of outsourcing for business continuity, recovery and resolution planning.

Cyber security – whether firms can demonstrate that they have in place effective governance, risk identification, security controls (over access management, incident management, network security and end-user computing), detection and prevention, testing, incident response and information sharing.

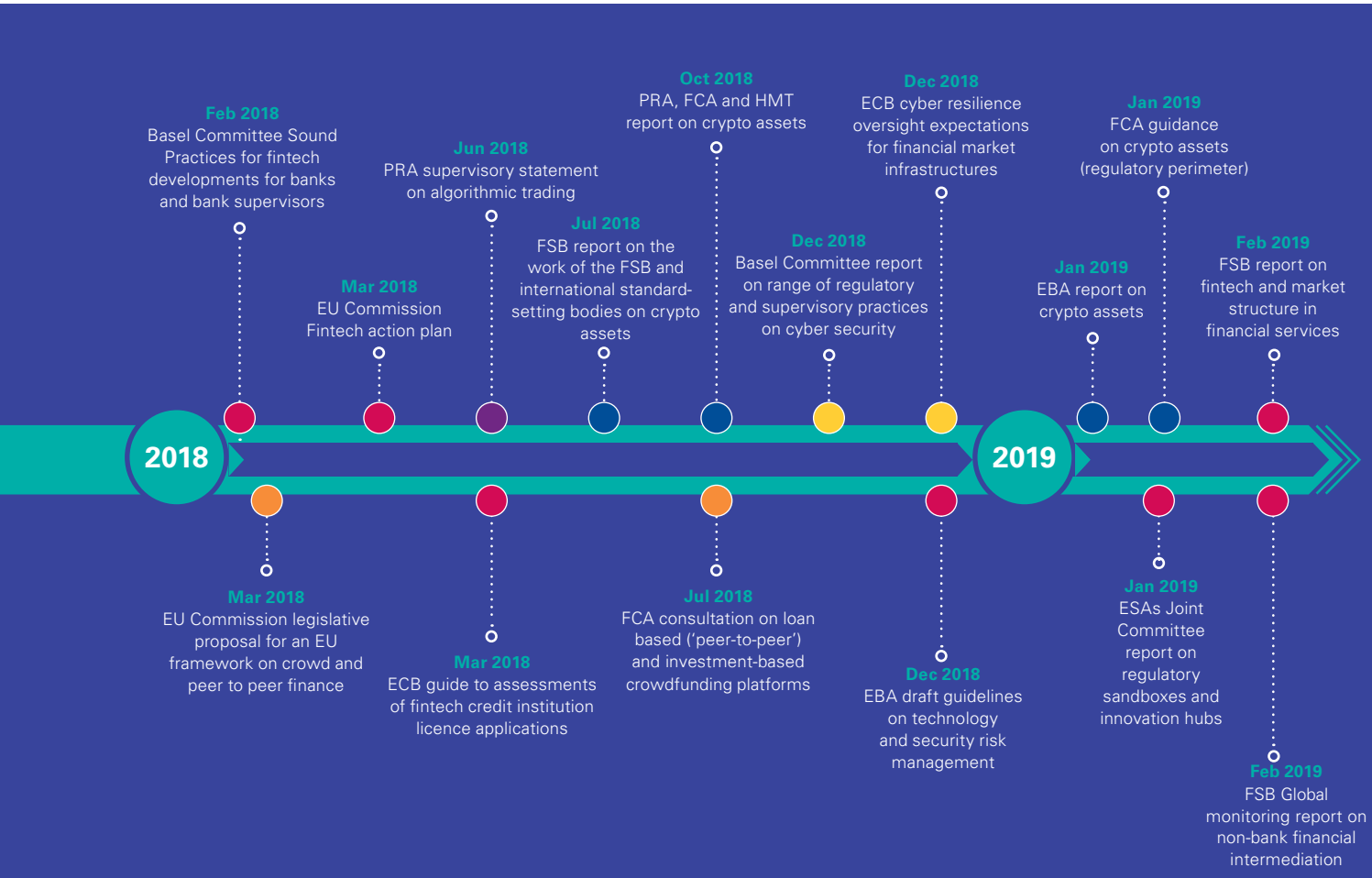
In addition, major firms may be expected to advance from meeting core requirements towards implementing more advanced tools (such as technology and risk management tools) to manage cyber risks more proactively, and to drive innovation in people, processes, technology and information sharing to enhance cyber resilience.

Artificial intelligence and machine learning – how well firms control and mitigate the risks arising as they make increased use of AI and machine learning, not least in terms of governance, understanding, and relationships with third party providers.

Firms active in this area are being asked to demonstrate that they understand and can manage effectively the risks that greater use of AI and machine learning might pose.

Sandboxes – using sandboxes and innovation hubs to test fintech applications and to identify and address risks in a constrained environment.

"Suptech" – the use of fintech by supervisors to improve the regulatory reporting process and the supervisory analysis of data and other information (for example to detect outlier firms, money laundering, fraud and suspicious trading patterns).



How KPMG can help

KPMG member firms have established teams of specialists able to help financial institutions to identify opportunities and benefits from fintech, and to support them in addressing a wide range of fintech-related risks.

KPMG member firms work with both incumbent financial institutions adopting fintech solutions and a wide range of fintech businesses, from early stage start-ups to established fintech providers. Our fintech network spans financial services including digital banking, payments, lending, insurance and wealth management.

KPMG professionals can support financial institutions through:

Helping financial institutions to realise the potential of fintech

Helping financial institutions to grow their business, explore new innovative solutions, meet evolving customer demands, and enable them to remain relevant and competitive in the evolving landscape.

Combining domain expertise

Bringing together KPMG expertise in audit, tax, corporate finance, legal services, cyber security and regulation with fintech expertise to deliver global solutions that are not only on the cutting edge of technology, but also sustainably aligned to the overall processes and frameworks of the client.

Identifying and addressing fintech-related risks
Gap analysis and remediation.

Providing an enterprise-wide Operational Resilience framework

Offering a framework that incorporates fintech and fintech-related risks into designing and building operational resilience, starting with strategy and governance and extending through all aspects of execution.

Offering a technology and innovation matchmaking platform

KPMG Matchi connects financial institutions and other corporations with a global community of leading-edge technology providers. This can help resolve issues or support new opportunities by using a more targeted sourcing approach across our fintech database, reducing significantly the time it takes clients to target, select, test and implement the optimal fintech solutions.

Applying an end-to-end framework and tools for artificial intelligence solutions

Ensuring that AI solutions have integrity, are explainable, are free from prejudice, and are agile and robust in order to be used effectively and trusted when making decisions; and to support financial institutions in the development and deployment of AI and the use of risk, compliance and audit functions in managing relevant risks.

Developing scalable regtech solutions

Harnessing emerging technologies for accelerated, robust, and less costly risk management, compliance and regulatory reporting processes, based on an understanding of how financial institutions can use regtech as a digital transformation enabler, helping them improve customer service, develop new offerings and achieve greater competitive differentiation.

Providing fintech insights to financial services clients

KPMG member firms are at the forefront of current and future developments in technological and commercial innovation across banking, insurance, capital markets and other financial services; and in providing insights and thought leadership on the development of fintech regulation and supervisory approaches. KPMG fintech publications include an annual Fintech 100 report listing the top 50 established and top 50 emerging fintech businesses globally, and Pulse of Fintech, a six-monthly review of investment in the fintech sector.

Connecting financial services and fintech clients

KPMG arranges fintech showcases, networking events and start-up pitching events which bring together fintech businesses, financial institutions and investors.

Contacts

Ian Pollari
Global Co-Leader of Fintech
KPMG International
T: +61 2 93358408
E: ipollari@kpmg.com.au

Anton Ruddenklau
Global Co-Leader of Fintech
KPMG International
T: +44 20 76942224
E: anton.ruddenklau@kpmg.co.uk

James Lewis
Head of EMA FS Risk & Regulatory Insight Centre
KPMG International
T: +44 20 73114028
E: james.lewis@kpmg.co.uk

Clive Briault
Senior Advisor, EMA FS Risk & Regulatory Insight Centre
KPMG International
T: +44 77 95351927
E: clive.briault@kpmg.co.uk

Chris Steele
Director, Banking Risk and Regulation
KPMG in the UK
T: +44 77 99886782
E: chris.steele@kpmg.co.uk

David Milligan
CEO, Matchi
KPMG in South Africa
T: +27 60 9977174
E: david.milligan@matchi.biz

Rachel Bentley
Fintech Senior Manager
KPMG in the UK
T: +44 78 25114912
E: rachel.bentley@kpmg.co.uk

Pierre Guerineau
Manager
KPMG ECB Office
T: +49 69 95871224
E: pguerineau1@kpmg.com

kpmg.com

CREATE. | CRT109370A | March 2019