



# Emerging risks and evolving responses

**Exploring the challenges  
facing banking – and how  
the industry can respond**

December 2018

---

[kpmg.com/uk/banking](https://kpmg.com/uk/banking)

# Contents



**Executive  
summary**

4

**1 Emerging risks**

6

**1.1** Technology

8

**1.2** Societal

12

**1.3** Financial stability

14

**2 Evolving responses**

16

**2.1** Developing agility

18

**2.2** Evolving regulation  
and compliance

24

**2.3** Building resilience

28

**Conclusion:  
financial services  
fit for the future**

30

# Executive summary

## What risks do banks face now and tomorrow – and how can the industry respond?

There was once a time when these questions might have felt easier to answer. Today, fast-changing technological, social and market developments make the landscape harder to read. In this report, we attempt to bring some clarity to the picture, looking at emerging risks in depth and exploring some of the ways in which market participants and supervisors are responding.

Technology heads the list of transformative forces in financial services. The shift from monolithic players toward ecosystems and the platform economy is creating a marketplace that is more interconnected and interdependent. While this opens up opportunities for incumbents, new market entrants and customers alike, it also poses important questions about accountability and regulation – especially as customer data becomes simultaneously more available and more valuable. Fast-evolving cybercrime also puts the market on its mettle.

Alongside technology, social factors add challenges. Financial firms are expected to be more agile, transparent and trustworthy – yet automation, while reducing costs, may rob them of vital knowledge and compel them to take direct responsibility for job losses. Fintech and big data could also distance firms from their customers at precisely the time they need to be closer to them.

And although risk ratios have improved post-crisis, there are question marks over whether risk has just transferred back to the market and whether the trend towards passive investments will impact volatility. There are many potential stress events on the horizon – and concerns over whether platform economies in finance could lead to greater concentration of risk.

Despite this complex, dynamic risk environment, there are signals that both market participants and regulators are evolving responses to confront and adapt to it. We are seeing banks build more agile, customer-focused operations that are overcoming the challenges of legacy technology with new software architectures. There is a recognition that digital, data-driven propositions need to be at the heart of financial firms' offers. There are likely to be moves towards partnerships as banks lose their advantage in distribution, and a focus on agility in production. By bringing together risk and finance in an integrated function, banks could access more actionable insights that improve agility further.

Regulation is moving beyond its initial supportive response to fintech and actively looking to address the areas that fintech impacts: from platform economy risks to consumer protection, cross-border issues and acknowledgement that the 'regulatory perimeter' is a dynamic concept that must be frequently reassessed. Supervisory Technology (SupTech) has the potential to make supervision more effective, and technology – together with renewed processes – has the potential to improve regulation around algorithmic trading.

Finally, in recognition of the fact that things can go wrong no matter how many responses are in place, regulators and firms alike are looking to improve resilience so both firms and markets can bounce back more effectively from shocks.

“

*Despite this complex, dynamic risk environment, there are signals that both market participants and regulators are evolving responses to confront and adapt to it.*

# Emerging risks

## Introduction

**Three key areas of risk confront financial firms and regulators today:**



**Technology**



**Societal**

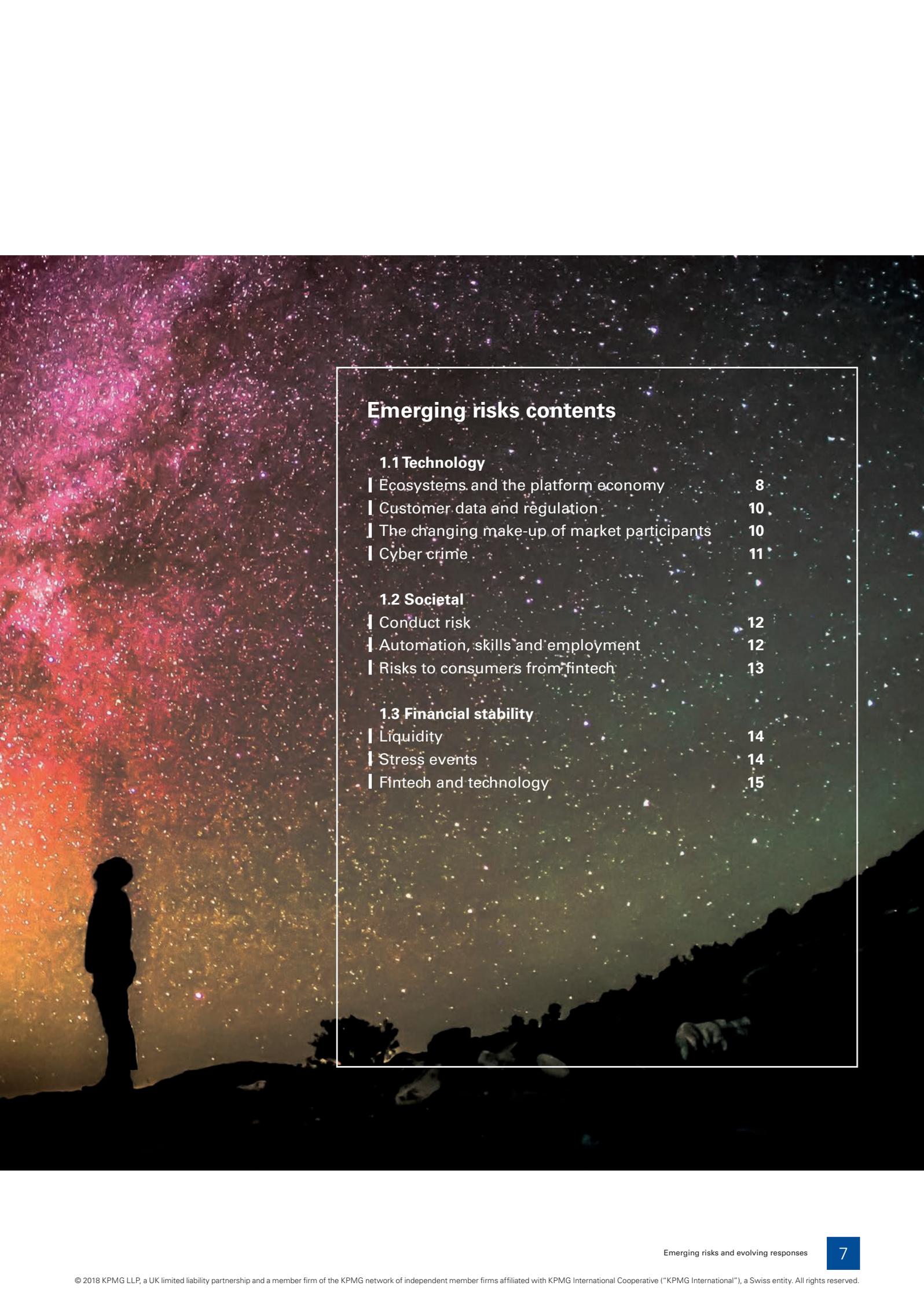


**Financial  
stability**

Increasingly dependent on technology, markets are evolving into complex ecosystems that can become opaque – at precisely the time that customers are demanding more transparency.

Automation may have unintended consequences, placing social obligations on financial firms.

And markets may present challenges around liquidity and a spectrum of stress events.



## Emerging risks contents

### 1.1 Technology

Ecosystems and the platform economy	8
Customer data and regulation	10
The changing make-up of market participants	10
Cyber crime	11

### 1.2 Societal

Conduct risk	12
Automation, skills and employment	12
Risks to consumers from fintech	13

### 1.3 Financial stability

Liquidity	14
Stress events	14
Fintech and technology	15

# Emerging risks

## 1.1 Technology

### Ecosystems and the platform economy

There's no question that in recent years, financial markets have become more reliant on technology. They are more interconnected, and more interdependent. Banks now depend on a complex ecosystem of infrastructure – from cloud services, exchanges and platforms to valuation and data providers, and retail payment systems. All of this is now critical infrastructure but much of it is outside the banks' own control and beyond the regulator's scrutiny. As it is more integrated, this ecosystem creates more 'weak spots' for cyberattacks.

In its July 2018 discussion paper *Building the UK financial sector's operational resilience*<sup>1</sup>, the Bank of England and PRA identified five technology-related challenges created by today's context of technological complexity and hostile cyber environment:

**Technical innovations** that change the nature of payment systems and markets: fintech, artificial intelligence, distributed ledger technology and crypto assets.

**Changing behaviours**, in which consumers of financial services respond to innovation and interact with financial services differently, demanding instant and mobile access, and faster transactions.

**Keeping pace:** the need to plug skills gaps and manage obsolescence in the face of rapid technical change (see page 12).

**Challenging environment:** an increase in the frequency and sophistication of cyber threats and financial crime (see page 11) and cost pressures in response to competition from disruptive market entrants.

**System complexity**, in particular the proliferation of third parties, the potential for concentration risk and cross-border dependencies.

<sup>1</sup> <https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper>



Risk management needs to account for this and accept that as technological third parties becomes more interdependent, failure is inevitable.

It is for this reason that the PRA and FCA are consulting widely on the subject of operational resilience. This starts from the point that failure is inevitable and that what matters is how financial institutions prepare and react. In spring 2018, during the difficulties caused by its system upgrade, TSB became a target for cybercriminals, with a spike in phishing attacks targeting the bank's customers<sup>2</sup>. This illustrates the need for a resilience approach that not only prepares for the consequences of system failure itself, but also takes into account the potential knock-on effects that such an outage can cause.

So risk management and operations functions at banks have to assess and mitigate their own risk in the context of a financial system that is more intrinsically linked than ever. Most importantly, banks' own operational resilience depends on their ability to assess the resilience of the many third-party service providers on which they depend.

On page 16 we look in more depth at the steps banks can take to build resilience in this context.

### **Transparency: should markets or regulators drive it?**

This complex ecosystem lacks transparency and its interconnectedness could lead to consequences we don't yet understand. How do we get more transparency and assurance? Should this come from regulation? It may not be necessary for much of it – exchanges, for example, are already tightly regulated but it may be inevitable for some. The markets are already demanding greater transparency, and we are seeing more assurance proactively provided to the market. In other cases, regulation is starting to draw in new businesses, for example in the benchmarks space, where benchmark administrators, contributors and users are impacted by the regulatory requirements. It may make sense to see regulation as a spectrum – from tight, formal regulation at one end to management by market forces at the other, depending on how critical the technology or data is. Transparency is key.

### **Platform ecosystems are complex. Where do responsibilities lie?**

Interconnectedness is speeding up as financial services become platform-based and open banking creates new possibilities. This trend is positive for customers, who get more choice and better services but it creates new risks: a more complex supply chain, with more potential points of failure; and a lack of clarity about where responsibility lies. If you choose a product from an open banking provider and they direct your money to a specific bank, where does the conduct risk sit? It's similar to the question alluded to at the start, around who is responsible for fake news on social media platforms.

<sup>2</sup> <https://www.computerweekly.com/news/252442316/Huge-rise-in-TSB-themed-mobile-phishing-attacks-amid-IT-meltdown>

# Emerging risks

## Customer data and regulation

### **An increasingly valuable resource**

Customer data is an important area of emerging risk, growing both in value and the potential for misuse. Data breaches have taken centre stage in recent months, with Facebook and British Airways among the highest-profile and highest-impact attacks. Tesco Bank was also fined in 2016 for its data breach<sup>3</sup>, in which fraudsters stole £2.26m from customers. It's reported that the £16.4m fine could have been significantly higher had the EU General Data Protection Regulation (GDPR) been in force at the time<sup>4</sup>.

Today, customer data is a more valuable currency for both its owners and its custodians. For the customers of financial services, it can be the basis for more relevant and tailored products, and better service. It now has much broader market value in financial services, where beyond banks, it can be sold by new account information service providers to third parties and used to make decisions about where to place people's money or how to improve their spending.

### **More constraints needed?**

While GDPR has tightened privacy and raised the bar around the response to data breaches, there's a question of whether financial firms should be subject to further constraints that reflect the special status of customer financial data. After all, in financial services, much customer data is highly sensitive and there is a high risk to both firms and customers if it is used fraudulently. It can also be used to offer services that may not meet customer needs or offer good value for money.

## The changing make-up of market participants

### **Strategic alliances need agile regulation**

Looking further out, now that the days of banks growing through major acquisitions are mostly behind us, firms are instead using formal strategic alliances based around their individual USPs (for example balance sheet, technology or user experience). This means regulators – and regulation – will need to be more agile, because they will have to regulate through a customer journey rather than focusing on single entities.

### **New entrants have different risk appetites**

There also seems a certain inevitability about the further expansion of GAFA (Google, Apple, Facebook, Amazon) into financial services, and these firms have different risk appetites compared with traditional players.

Experience in other sectors suggests that scale economies on technology platforms often lead to dominant providers, as with GAFA, which raises the question of whether regulation should push back against this trend on the grounds of competition and market stability, or accept it and focus on the regulatory response.

<sup>3</sup> <https://www.bbc.co.uk/news/business-45704273>

<sup>4</sup> <https://www.computing.co.uk/ctg/news/2476645/tesco-would-face-fines-of-up-to-gbp19bn-under-gdpr-for-tesco-bank-breach>



## Cyber crime

### Fast-evolving threat

Unlike traditional patterns of fraud, which the financial industry knows how to combat, cyber crime is less well understood and evolves rapidly. The industry's continuing digitisation opens up new avenues for cyber criminals to attack and manipulate our financial systems to their benefit.

While cyber crime is now an everyday challenge for the financial industry, care is needed in avoiding complacency as criminal groups become increasingly aware of opportunities to manipulate our interconnected and interdependent financial systems and market infrastructure.

Cyber crime has become commoditised, industrialised and transnational underpinned by a vibrant black market in crime as a service. This \$600 billion a year industry shows unique agility and innovation, placing demands on banks and other financial institutions to detect and investigate cyber crime quickly as the opportunities for rapid cash out grow. This requires an integrated approach to spotting unusual and anomalous activity across all channels, which brings together the best of fraud control and cyber intelligence.

New partnerships are required between banks, law enforcement, government and technology firms to detect patterns of cyber crime; and most importantly to disrupt the infrastructure used by those criminals groups, whether it is a fake website collecting credentials or the latest attack on a network of compromised computers. Artificial intelligence will find its place in automating detect and response of cyber crime, but will also be applied by criminals to good effect to improve their targeting and social engineering of bank customers.

State backed attacks on our financial infrastructure are becoming increasingly likely, as nations invest in offensive cyber capabilities. These 'black swan' low-probability/high impact events have the potential to create a systemic risk to our increasingly interconnected financial systems and play a key part in driving regulatory concerns over operational resilience.

“

*Artificial intelligence will find its place in automating the detection and response of cyber crime, but will also be applied by criminals to good effect to improve their targeting and social engineering of bank customers.*

# Emerging risks

## 1.2 Societal

### Conduct risk

#### Increased transparency

The conduct and culture of banks, as with all institutions, is more transparent than ever before. Different groups of stakeholders increasingly demand it too. There are now five generations in the workplace, all with different expectations and value sets but all supportive of more transparency and calling out misconduct. In the UK, the Senior Managers and Certification Regime (SMCR) is designed such that firm's leaders and senior management have clear accountability for fostering the right behaviours amongst staff. The link between remuneration and these behaviours is now a clear focus for regulators. SMCR has been mirrored around the world in places like Hong Kong, the US and Australia.

#### Faster response needed

This transparency trend creates risk because firms may not be agile enough to respond when examples of bad practice – or misreported bad practice – snowball rapidly, as we saw in 2018 with TSB and Oxfam. Customers also expect higher levels of speed and security today. Although Environmental, Social and Governance Reporting is broader and more rigorous than corporate social responsibility, executives have difficulties seeing the problems it would solve, so it doesn't always get the focus it deserves.

### Automation, skills and employment

#### Keeping the insights that are lost to automation

Another important social trend is automation, which has already transformed banking. Its potential to take over traditional risk analysis roles – or at least functionalise them – poses important questions. When machines are doing all the calculations, what new skills are needed? For example, how do banks find people with the right breadth of experience to be able to identify faults – in technical analysis or see the bigger picture?

A useful comparison is satellite navigation, to which we outsource our own ability to navigate and locate ourselves. With satnav, we know where we are – but have no idea how we got there. So as automation gathers momentum, one of the challenges for banks is how to develop people's skills so that they still understand the journey as well as the destination. One response for risk functions is a 'mobility agenda' – to ensure risk professionals have a variety of roles and different contract modes so they have the mindset to see the bigger picture and identify the root causes of issues.



## Risks to consumers from fintech

### Will banks be obliged to reskill the unemployed?

Nothing damages trust like major job losses. So who will be responsible for retraining those made redundant by automation? When high-earning teams on front office trading desks are automated out of existence, there is limited societal impact from those redundancies. However, the coming wave of automation could lead to large-scale back office job losses, which will have a much bigger social impact. Banks may have to re-skill and prepare their employees for future jobs outside of the firm – or risk a public backlash. That's an unexpected consequence: technology driving a need for banks to invest in their contribution to society. It may therefore be helpful for firms to consider the types of automation they are deploying.

### Replacement vs. augmentation

The deployment of technology to automate existing processes can have a wide-ranging effect on the human workforce. In some cases, it is a direct replacement of labour that brings immediate societal impacts – think of the effect that the car had on livery stables, or that ATMs had on bank tellers. 'Augmenting' technologies, on the other hand, can create new and more productive types of work, for example the online research portals that freed up scientific researchers to focus on higher-value work. Looking at automation through this lens can help banks find the best strategic approach.

### Less transparency and fairness?

With fintech, financial institutions are becoming more customer-centric and providing better and more personalised products and services. However, there is a risk that the profit motive and an unchanged culture may lead some to use fintech to sell products and services that do not meet customer needs or represent poor value for money.

Similarly, while digitisation and artificial intelligence (AI) can streamline customer service, they can also distance financial institutions from their customers in a way that potentially impacts conduct requirements. And just as AI has the potential to 'de-skill' financial firms, it could also make it harder for customers to understand how a credit or insurance decision was reached.

Digitalisation may also impact financial inclusion, disadvantaging some groups – for example older consumers or those with limited access to digital channels – while advantaging others.

### The downsides of better data

Big data creates scope for unfair treatment and conflicts of interest between firms and their customers. Insurance, for example, has traditionally worked on the basis of pooling risks. But with vastly more data at their disposal, insurers can create bespoke risk profiles and pricing that may make some risks uninsurable or prohibitively expensive.

Data privacy and data protection issues may arise from the growing volumes of customer data, access to and storage of this data, and the flows of data (often across national borders) between financial institutions and third-party service providers. Consumers are likely to become increasingly aware of the value of their data, and of the ways in which it is being used, leading to denial of access issues and possibly data manipulation by consumers.



# Emerging risks

## 1.3 Financial stability



### Liquidity

Banks' traditional risk ratios may have improved post-crisis. But has the risk just transferred back to the market? There's a question of whether there is enough liquidity to keep operating as normal during a stress event. Increased capital requirements mean that banks now have less capacity to stabilise markets, which leads to more volatility. A recent study showed that post-crisis market prices are twice as sensitive to asset sales as before the crisis, due to the reduced shock-absorbing capacity of market makers.

#### Passive danger?

This impact of the liquidity question is likely to be accelerated and amplified by electronic markets and the vast amounts of assets that are now in passive investment strategies, which are estimated to account for one-third of AUM in the US, or \$8 trillion. Passive investment strategies can provide customers with efficient access to diversified investments with reduced management fees. However, critics have called funds placed in passive investment strategies as 'dumb money' because it is invested without due consideration of a company's management team, governance or innovation. Current growth trends suggest that passive funds will own the entire issuance of all listed stocks by 2030. This is clearly unrealistic and a reversal in the trend is inevitable.

### Stress events

#### Multiple triggers

Stress events are an ever-present financial risk and today there are a great many potential triggers for them. It's unclear, for example, how the unwinding of Quantitative Easing and the de-globalisation trend will play out. Simmering political tensions are becoming fully fledged trade and information wars. And there's the question of regulatory divergence. Post-crisis, the G20 sought common standards – now they are moving apart, for example with the redlining of Dodd Frank in the US. Markets, and capital, will behave differently.

A no-deal Brexit could also trigger a stress event – and other scenarios could impact banks' client bases. Would a hard Brexit freeze up working capital for SME customers? How will it affect the wider economy and who's best-placed to assess overall impacts – banks or regulators?



“

*The opacity of AI and machine learning of interconnectedness among financial markets and institutions.*

## Fintech and technology

### A spectrum of risks

As we have discussed in section 1.1, fintech and technology pose a spectrum of risks to financial firms as a counterweight to the many benefits they offer. The same is true on the larger, systemic scale. Scale economies akin to those enjoyed by GAFAs could lead to greater concentration, even to the point of single dominant operators. The opacity of AI and machine learning models creates inherent risk, as does the increasing of interconnectedness among financial markets and institutions.

Systemically important firms and infrastructure could fail if the fintech or new third-party dependencies upon which they rely fails. And large funding flows on fintech lending platforms could grow in volatility thanks to lower lending standards, untested risk assessment processes and the anticipated pro-cyclicality of fintech-based lending.

# Evolving responses

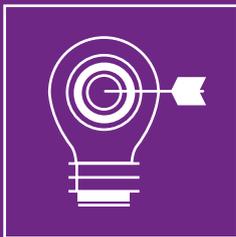
## Introduction

**Banks and regulators alike are evolving their approaches to deal with the emerging risk landscape.**

Among financial firms, agility is the aspiration: to be able to respond and move fast, overcoming the hindrance of legacy cultures and technologies and finding new ways to gain insight and advantage.

Regulators, for their part, are alert to the need not only to adapt their activities but also to redraw the regulatory perimeter itself.

And everyone is thinking more actively about the concept of resilience, recognising that today's levels of risk and complexity mean that at some point, failure is inevitable.



**Agility**



**Regulation  
& compliance**



**Resilience**

## Evolving responses contents

### 2.1 Developing agility

- | Five steps to a more nimble operation 18
- | Building an agile operating model 20
- | Integrating risk and finance to improve transparency and efficiency 22

### 2.2 Evolving regulation and compliance

- | Alternative approaches to regulation that reflect emerging risks 24
- | The use of SupTech 25
- | The regulation of algorithmic trading 27

### 2.3 Building resilience

- | Developing the ability to bounce back from shocks 28

# Evolving responses

## 2.1 Developing agility

### Five steps to a more nimble operation

Speed, not size, will increasingly drive bank profits. Yet incumbents aren't known for agility. After decades of regulation-driven change, banks are tired of it,

preferring stability to restructuring. The typical tension between business-as-usual and change can also hamper innovation.

#### But some practical short-term steps can build the foundation for a more flexible long-term business model

Customers connect with banks that communicate clear brand values and turn away from companies they perceive as inauthentic. To understand how products and services are meeting customer needs, leading banks combine ad-hoc surveys with data from digital channels. They also embrace design thinking, applying product design rigour to the new discipline of 'customer journey architecture' and can also use customer observation (via ethnographic research) to understand user intent. This helps replace the long-established 'product push' approach with customer-centric processes.

#### 1 Change the culture

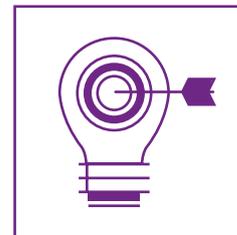
At a recent banking webinar, two-thirds of attendees noted that 'Culture is one of the biggest blockers to driving agility.' Agile cultures need to embed collaboration, self-reinvention and fail-fast, and incentivise staff on customer value and continuous improvement. Collaborating with customers as products are developed also helps to remove constraints. Structurally, an evolution from command-and-control hierarchies toward flatter structures and multidisciplinary teams creates an organisation better suited to innovation and dynamism. Some banks are already using 'tribes,' 'chapters' and 'squads' to deliver new services. These structures can spur creativity and engagement, and attract talent that might otherwise choose GAF A or fintech startups.

#### 2 Focus on the customer

#### 3 Put technology first

From cloud and platform technology to APIs, new architectures are being deployed that allow new digital front ends to change at speed while legacy systems operate behind a protective layer of input and output interfaces.

Meanwhile, microservice software architecture enables major applications to be developed in small, discrete modules that can be built, reviewed and tested independently. This dramatically increases speed and agility and reduces risk compared with the old 'rip and replace' approach. Cloud adoption in particular has enabled leading banks to add agility where it once wasn't possible, with the potential to significantly improve and simplify back-end operations in banks. Regulators are becoming concerned about what happens if access is withdrawn at the discretion of the cloud provider, or data is lost if a provider collapses. But providers have responded quickly, offering 'containers,' or immutable storage that enable banks to store and retain data in an inerasable and non-rewritable format, so it is portable from one provider to another.



Innovation is the new standard, and the pace of change is no longer dictated solely by the banking peer group. Banks can learn from tech companies and industries that have successfully transformed, including automotive, hospitality and music. Outside of financial services, CIOs are investing massively in data-led technologies as they recognise that data underpins digital value. It is estimated that spending on modern data technologies will outstrip legacy technology spending within two years.

#### 4 Bank on data and change

#### 5 Achieve agility through acquisition



In section 1.1 we noted that banks' old model of growth through acquisition was being replaced by a move to strategic alliances. However, many banks are using acquisition for developing technology capabilities, for example RBS buying FreeAgent to add accounting software to its SME offering. Elsewhere, banks are making minority and venture investments to build capability, such as BBVA's stake in a number of digital banks, and investments by Santander InnoVentures. Leading banks are also unbundling their business models from vertically integrated structures, disintermediating between distribution, production and servicing, as in the Dutch mortgage market.

# Evolving responses

More importantly, 80% of incremental revenues will be driven by these new data-driven digital propositions by 2022<sup>5</sup>. Data and digital will become increasingly material to business model change, and data will become the principal driver of success. By changing the perception that CDOs (Chief Data Officers) are gatekeepers rather than salespersons of data, banks can empower them to monetise the data they have.

Banks should also look to reorganise distribution around segments and markets, with digital and data as a primary focus. This would replace the traditional product, channel or organisational matrix. Perhaps most importantly, banks should remember that innovation is not magic, but rather a core strategy to the future of the business that should be run as a portfolio on three levels:

**Incremental:** Classic process improvement.

**Transformational:** Targeting new revenue pools, while remaining tethered to the existing business P&L to avoid being an 'island of innovation.'

**Disruptive:** Testing new business models with iterative fail-fast methods.

Lastly, banks should be open to partnerships, alliances and affinities to spread the workload of future transformation and bring in diverse thinking and wider skillsets. Banks should be clear on their core competencies and where partnering can add competitive advantage.

## Building an agile operating model

### Specialise to optimise

It may seem obvious that banks need to focus on the markets, client segments and product categories where they have genuine pricing power and points of differentiation. But these fundamentals were often overlooked in the benign pre-crisis market conditions that incentivised firms to chase scale while any associated inefficiencies were masked. It is these inefficiencies that are now resurfacing amid today's tougher regulatory requirements and a more challenging interest rate environment.

Many successful banking strategies now involve a renewed focus on 'the core.' Naturally, this means different things to different institutions. For some it means a core client segment, for others a core product set or capability, others still a core geography. It's a trend gaining traction in Europe, with many creating non-core divisions. Even the largest global players are shifting focus and investment spend to markets where they have scale in their chosen products and customer segments.

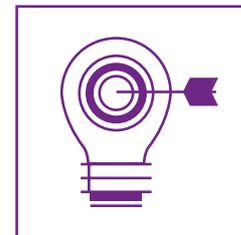
Becoming more focused is a logical response to the environment that banks now find themselves in, but it does raise its own set of problems. In particular, it makes banks more vulnerable to changes in their own market segment.

### Embedding flexibility

As the pace of change increases – whether due to innovation, regulation or competition – a bank's vulnerability increases. In the absence of a crystal ball, the only way that banks can manage this risk is by embedding flexibility into their operating models so they can adjust rapidly to the way they serve their chosen market.

In exploring how banks can make their operating models more agile, it is necessary to disaggregate banking into its two core components, 'production' and 'distribution,' since each brings different opportunities and challenges.

<sup>5</sup> Source: Bloomberg Article *The Five Key Areas to Drive Agility in Banking*



## Disruption to distribution

Distribution was once an area where size was an unequivocal advantage; a large physical footprint and broad customer reach have previously acted as barriers to entry. However, this model is being challenged by technology and by initiatives such as Open Banking and PSD2, which require sharing of data across banks, challenge the incumbents.

These changes enable new entrants to own the layer between the bank and its customers, giving them the ability to provide better service at a lower cost.

Banks could choose to retreat from distribution entirely or compete by upscaling their own technology options to meet changing customer demand. However, with fintech and GAFAs alike showing interest in banking services, partnership may offer a more agile route, with distribution co-sourced or outsourced. This could provide a cost-effective and scalable distribution model allowing banks to focus on production, which is more highly regulated and therefore less susceptible to threats from new entrants.

## Driving performance from production

Performance in production is driven by three inputs: innovation, price and flexibility.

Banks have traditionally been better at the first of these. But as product cycles are shortening, quickly eroding leaders' advantages, the ability to deploy and redeploy balance sheet resources to the next-best option is critical.

Banks need an operating model that supports efficiency in pricing, and flexibility of resource utilisation. This means moving away from a distribution-led operating model, where business lines follow customer groups and balance sheet management is an afterthought. Such a model too often leads to short-term profits that turn into long-term drags on profitability, which can tie up capital years after origination and erode long-term returns.

More savvy management of balance sheet resources and capacity is one answer. This can be done by rebalancing the power between demand (the business lines) and supply (treasury and legal entity management). Too often, business lines make demands on financial resources to drive promised growth but are not adequately held accountable if the demand does not materialise, resulting in surplus supply. This inevitably results in feast and famine. Certain business lines have surplus capital while others are starved of the resources for growth, as scarce balance sheet resources are locked up in the wrong areas.

With multi-disciplinary balance sheet management functions, as described in the KPMG paper *Balance sheet options: the returns dilemma*<sup>6</sup> firms can reduce balance sheet inefficiency and put more tension in the supply/demand process. This allows a more dynamic allocation of resources in the short-to-medium term whilst ensuring a longer-term perspective on balance sheet management beyond the first year of the financial plan.

This is not to suggest a complete reversal of the current state of affairs to a balance sheet first, business unit second approach, merely a much greater balance between supply and demand of resources. Otherwise there will be neither the ability nor the political will to reallocate and rebalance between products and business lines. Unlike in distribution, where one path to agility is decentralisation, agility in production must be achieved through increased centralisation.

<sup>6</sup> [https://assets.kpmg.com/content/dam/kpmg/uk/pdf/2017/07/balance\\_sheet\\_optimisation.pdf](https://assets.kpmg.com/content/dam/kpmg/uk/pdf/2017/07/balance_sheet_optimisation.pdf)

# Evolving responses

## Integrating risk and finance to improve transparency and efficiency

Leading banks have been talking about integrating risk and finance operations with the aim of securing a single, consistent and multidimensional view of their businesses for more than a decade. But with a few exceptions, relatively little progress has been made. One key reason is that data management has been seen as an operational process rather than an asset.

### Exploiting the value of data

Finance has traditionally enjoyed unique access to enterprise-wide data but has used it solely for financial reporting, concentrating mainly on the P&L. Meanwhile, risk has concentrated on assessing risk to the balance sheet, an area of focus for regulators as well shareholders. However, it should be a given that management decisions are taken on the basis of maximising returns on equity exploiting all the data at an organisation's disposal. Equally, banks should be able to switch seamlessly from a business unit view to a legal entity view, given that the underlying data is the same. For a bank, the finance and risk functions are the natural venue for this work, given underlying governance, control and data transformation skillsets.

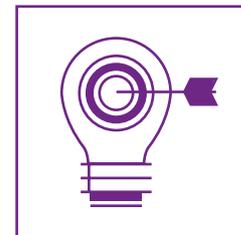
There are four reasons why the integration of risk and finance helps agility:

**1** It can deliver a much more consistent and standardised view of the risk-adjusted returns that banks are achieving throughout their business.

**2** Data transformation provides crucial insight into customer behaviours, enabling the development of better products and services.

**3** These gains allow for a more efficient allocation of capital.

**4** Integrated ways of working and a common infrastructure improve control and reduce duplications and inefficiency.



“

*The aim should be to create a shared service that is capable of providing data quality and management services as well as integrated reporting and advanced analytics to every other part of the enterprise: treasury, compliance and middle and front office functions.*

### **Envisioning a new model for integrated risk and finance**

Building a new, integrated risk and finance function is a significant exercise. The aim should be to create a shared service that is capable of providing data quality and management services as well as integrated reporting and advanced analytics to every other part of the enterprise: treasury, compliance and middle and front office functions. The newly integrated function would be the bank's data management centre of excellence, with a single underlying infrastructure.

It will need relocated personnel along with new staff in areas such as data science and advanced analytics, and should be presented as a positive career option in order to attract the right talent. The initiative would be proof that data really is seen as a value-creating asset within the bank. Smaller, separate risk and finance functions would remain in place, able to create their own added value from the improved insights that the new function creates.

For the organisation as a whole, this will be a profound transformation. The opportunity is to create an enterprise-wide asset that delivers greater actionable insight than existing functions could hope to create individually. Its activities will go to the core of the bank's operations and strategy, including its management of capital – far beyond what could comfortably be procured from third-party providers or advisers.

# Evolving responses

## 2.2 Evolving regulation and compliance

### Alternative approaches to regulation that reflect emerging risks

#### Regulatory responses to fintech and other risks

The initial regulatory response to fintech developments was supportive: it emphasised encouraging innovation, using regulatory sandboxes, accelerators and innovation hubs and taking a technology-neutral approach. However, we are now clearly entering a much trickier phase for regulators, who have to identify, assess and respond to the risks as well as the benefits posed by fintech developments to regulated firms, financial stability, and consumers.

It is likely that existing regulation and supervision will be adapted in several areas impacted by fintech:

**Outsourcing** – managing ‘platform economy’ risks from cloud and data service providers

**Cross-border legal issues** posed by new innovations

**Assessing the ‘regulatory perimeter’** – and updating it regularly

**Seeking common standards** where national regulators are diverging

“

*Regulation is also likely to spread to firms that are currently outside the regulatory perimeter, for example if they are important as providers of third-party services to regulated firms or of potential systemic importance.*



There will be growing regulatory and supervisory focus on financial institutions' governance and risk management frameworks to ensure that risks arising from fintech developments are properly identified, understood, managed and monitored.

We will also see new regulations in areas such as consumer protection, cybersecurity (contingency planning, information sharing, monitoring, and incorporating cybersecurity in the early design of IT systems), data privacy, governance and disclosure frameworks for big data analytics, and the authorisation and regulation of new fintech firms.

Regulation is also likely to spread to firms that are currently outside the regulatory perimeter, for example if they are important as providers of third-party services to regulated firms or of potential systemic importance.

The initial 'let innovation thrive' approach is therefore likely to be overwhelmed by concerns about the various risks arising from fintech and by concerns about level playing fields and minimising regulatory arbitrage.

This raises the spectre of more intensive regulation of fintech than might have been expected. And there is a risk that this may impact the pace of innovation, the ability of fintech to drive competition and the availability for consumers of new products and services.

## The use of SupTech

Just as technology presents opportunities for financial institutions, supervisors and regulators can also use it to make their own processes more efficient. It has the potential to make supervision more timely, proactive, predictive and automated.

Developments are anticipated across several areas in the coming decade:

**A more real-time approach** to analysing data to support risk assessments, review exercises and transaction monitoring

**Direct access to data** from a firm's own systems rather than relying on out-of-date, pre-formatted reporting

**Use of artificial intelligence** to analyse 'big data' across regulatory reports and a wide range of data sources, for example to detect breaches, market manipulation and to develop predictive systems

**More preventative ex ante supervisory actions** – using predictive capabilities to take earlier actions as soon as solvency, liquidity, conduct or other issues are anticipated

**The exchange of real-time information** across supervisory colleges.

Despite the benefits of these approaches, there remains the possibility that the pace of change may be held back, as supervisors consider factors such as the balance of human judgement vs. automation, the governance and control of SupTech, their own IT capabilities, and restrictions on the cross-border information sharing.

# Evolving responses

“““

*Firms now need to test and control for operational resilience, market disruption, market abuse, anti-competitive behaviours, compliance with venue rules and consistent good client outcomes. Traditional software testing techniques struggle to cope with this.*



## The regulation of algorithmic trading

Because algorithmic trading removes the human factor from a dealing desk's inherent risk profile, it should provide opportunities to better define and control for good outcomes. However, the complexity of algorithmic trading environments means things can go wrong in many other ways.

Defining and controlling the point of failure is neither clear nor easy and the stakes are high for senior managers in this recently regulated area. Regulators expect a clear line of personal accountability for executives in charge of algo trading activities – and for firms to evidence understanding and documentation of their algorithms.

Firms now need to test and control for operational resilience, market disruption, market abuse, anti-competitive behaviours, compliance with venue rules and consistent good client outcomes. Traditional software testing techniques struggle to cope with this. In the complex algorithmic trading environment, with multiple potential points of failure and a high degree of interconnectivity and interdependence, there are three ways in which firms can improve governance and controls:

**1 Reduce inherent risk exposure by designing system architecture that prevents some risks from crystallising**, for example by allowing information flows within the algorithmic trading stack to be separated, and independently provisioned and controlled. Systems architecture should support the effective implementation of a 'need-to-know' principle, for example by creating containers for different types of algorithms, with independently controlled interfaces and execution environments.

**2 Consider a more integrated approach to running controls around pre-trade, real-time monitoring, best execution, capacity testing and market abuse.** At large banks, these processes are typically run by different teams using different systems and data. In an algorithmic trading environment, issues with any of these processes often compromise outcomes and compliance: for example, systems running slowly due to capacity issues may impact best execution as well as contributing to market disruption. Firms will get a better grip on risks and identify issues faster when they integrate monitoring across these disciplines.

**3 Consider emerging risks in algorithmic trading** – for example the pursuit of ever-increasing speed and low latencies or developments around privacy and data mining.

# Evolving responses

## 2.3 Building resilience

### Developing the ability to bounce back from shocks

The FCA's definition of operational resilience is: "the ability of firms, financial market infrastructures (FMIs) and the sector as a whole to prevent, respond to, recover and learn from operational disruptions". For a firm, operational resilience needs to encompass a range of areas: cyber risk, technology, people, facilities, and third parties and outsourced providers.

The topics covered in the first part of this paper illustrate why resilience has become such an urgent concept today. Technology is evolving at great speed, creating vulnerability as new technologies have to work with legacy systems. Supply chains have become more complex, with more interdependence and data exposure. Customers want 24/7, always-on service and expect their data to be kept secure. Threats are evolving, particularly in the cybercrime space, and incidents gain rapid exposure via social media. Finally, efficiency and cost-cutting are high on the agenda in competitive and disrupted markets. In this context, resilience is essential.

How can they go about creating an organisation that's operationally resilient? Several themes have emerged from the FCA's recent consultation<sup>7</sup> that act, in effect, as a roadmap for operational resilience.

Please see themes shown opposite.

Does this roadmap survive contact with reality? Only partially. Recent KPMG roundtable events with financial institutions suggest there are many challenges: it's widely accepted that operational resilience is 'still developing'. Firms are concerned that the required impact tolerances and measures are not clear, and they struggle with conflicting internal demands. The toughest challenges are with the FCA's top priorities: mapping processes from end to end, and achieving board-down ownership and accountability. In response to the Discussion Paper, embedding a 'business services' view is the highest priority for the majority of firms.

The roundtables also confirmed that firms had some distance to go to measure up to the Regulator's other resilience themes. Testing is mostly limited to specific, known scenarios and does not stress all facets of resilience; and recovery planning does not address all of the interactions and interdependencies across the firm. As for accountability, most firms think COOs are responsible for driving the resilience agenda. Achieving consistent approaches across third parties remains a challenge, and communication strategies need to be more effective.

“

*As for accountability, most firms think COOs are responsible for driving the resilience agenda. Achieving consistent approaches across third parties remains a challenge, and communication strategies need to be more effective.*

<sup>7</sup> <https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper>



## Themes that have emerged from the FCA's recent consultation

### 1 **Board-down**

The Regulator recommends that the resilience agenda should be driven by the Board and senior management, linked to the Senior Managers Regime and with clear ownership and accountabilities.

1

2

### 2 **End-to-end**

Firms are often siloed and have processes that span external suppliers. They need to 'walk the journey', mapping services from end to end, to establish an effective view of resilience.

3

### 3 **Measured**

To measure resilience, we need to know what it consists of. Often, measurement is focused on information technology. Yet IT is a lag indicator: it typically fails because something else has failed, for example when a new online product collapses under the weight of poorly-forecast demand. So the focus should be on finding forward-looking measures of resilience, and then measuring and reporting them against set tolerance limits.

4

### 4 **Resilience culture**

How do you think about resilience in everything you do? Resilience should be used as a key criterion across management decisions and business activities, and be core to a firm's culture.

5

### 5 **Recovery-centric**

This means working on the assumption that at some point, you're going to fail. The Regulator wants to see this mindset embedded in financial organisations, with an appropriate balance of prevention vs. recovery and the use of playbooks that are aligned with end-to-end services.

6

### 6 **Testing**

Business functions need to be fully engaged in resilience testing, which should include multiple points of failure across third parties and end-to-end services.

7

### 7 **Communication**

Strategies here should emphasise accountability, speed and customer/stakeholder segmentation – and should include social media monitoring and response.

# Conclusion

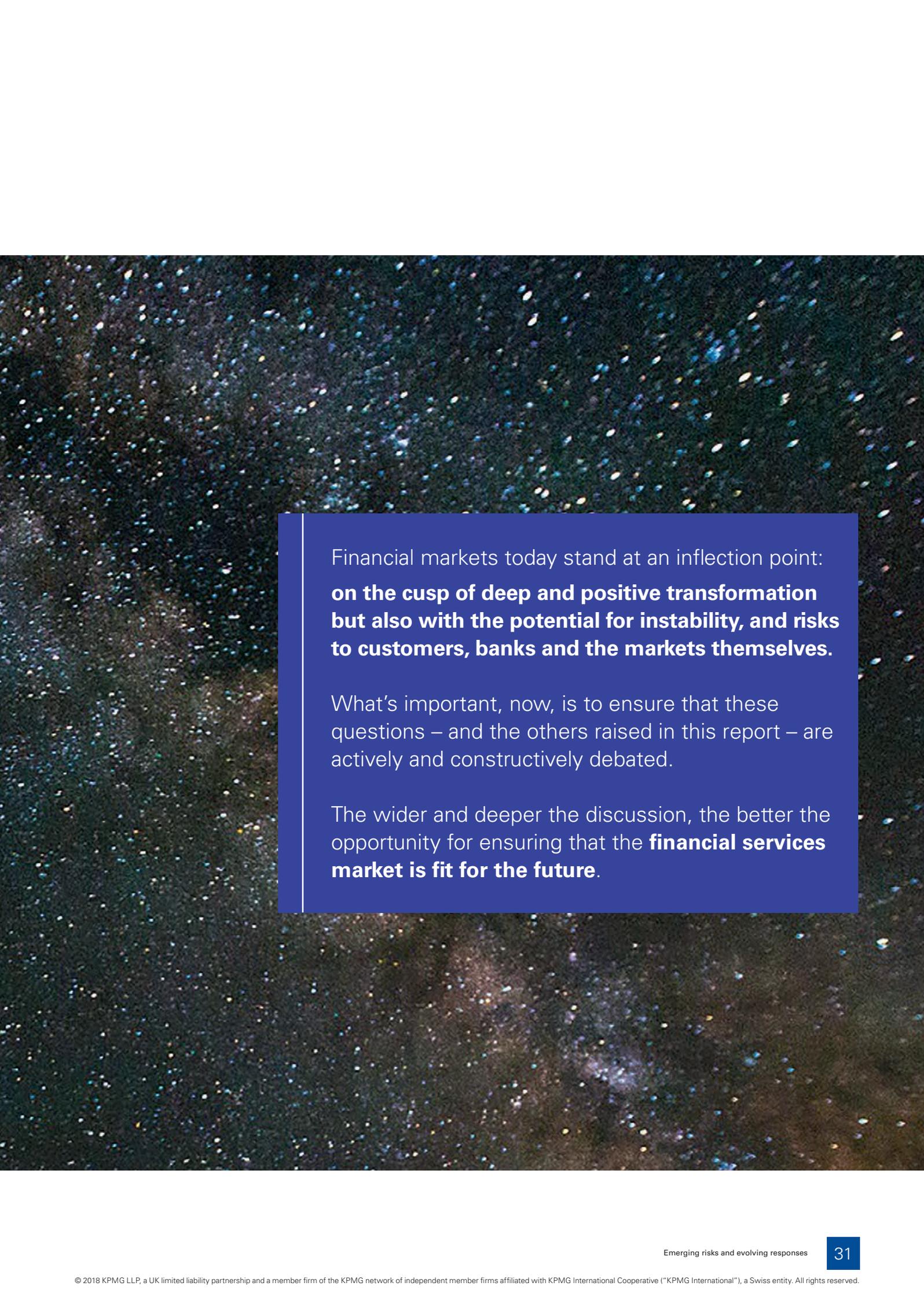
## Financial Services fit for the future?

**Looking at the scale and depth of emerging risks that the market faces, it's valid to question whether the responses that this report has also discussed will be enough.**

Can banks become agile fast enough?

Can a supervisory balance be struck that continues to stimulate innovation while at the same time protecting customers and markets?

Will technology platforms create as many problems as they solve?



Financial markets today stand at an inflection point:  
**on the cusp of deep and positive transformation but also with the potential for instability, and risks to customers, banks and the markets themselves.**

What's important, now, is to ensure that these questions – and the others raised in this report – are actively and constructively debated.

The wider and deeper the discussion, the better the opportunity for ensuring that the **financial services market is fit for the future.**

# Contact us



**Karim Haji**  
Partner, Head of Banking

+44 (0)7795 666 763  
karim.haji@kpmg.co.uk



**Peter Rothwell**  
Partner, Banking Risk

+44 (0)7826 531 190  
peter.rothwell@KPMG.co.uk



**David Ferbrache**  
Chief Technology Officer, Cyber Security

+44 (0)7780 225 463  
david.ferbrache@kpmg.co.uk



**Chris Steele**  
Director, Banking Regulation

+44 (0)7799 886 782  
chris.steele@kpmg.co.uk



**Julian Morgan**  
Partner, Banking Risk

+44 (0)7768 031 840  
julian.morgan@kpmg.co.uk



**Joe Cassidy**  
Partner, Financial Services

+44 (0)7780 956 784  
joe.cassidy@kpmg.co.uk



**Roger Acton**  
Senior Manager, Banking

+44 (0)7708 794 549  
roger.acton@kpmg.co.uk

[kpmg.com/uk/banking](https://kpmg.com/uk/banking)



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2018 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

**CREATE.** | CRT106306 | December 2018