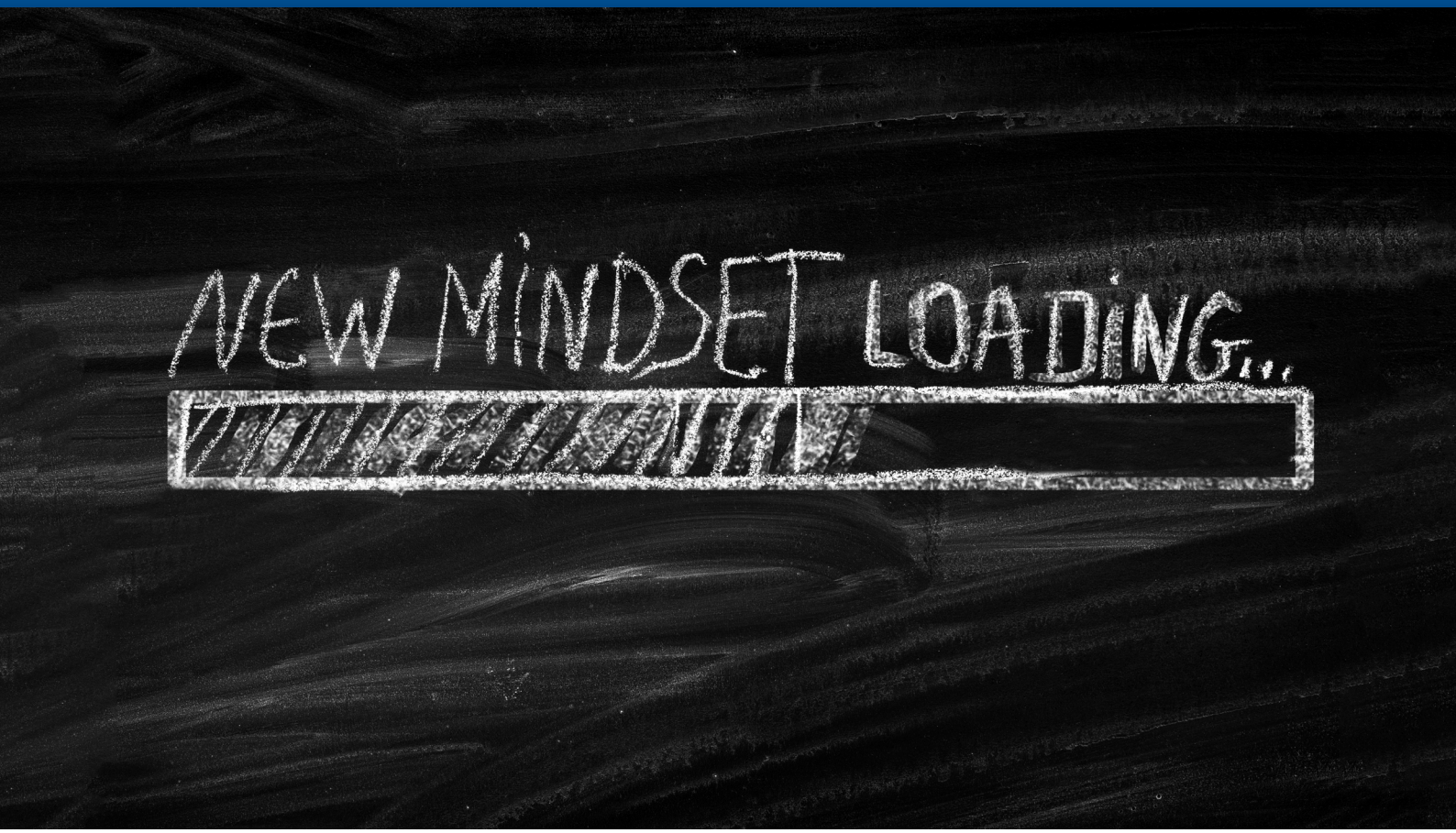


AN OPERATIONAL SHIFT IN MINDSET

Regulators are calling on firms to be able to protect and sustain their core business functions not just when it's business as usual but also in times of stress or disruption. But who does this concern, what does it entail and how are affected participants expected to respond? Below we capture some of the latest regulatory guidance to emerge on what will no doubt require a change in thinking about operational resilience.

On 5 December 2019, the Bank of England (BoE), the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) ("UK regulators") published joint Consultation Papers on operational resilience:

1. BoE and FCA joint foreword: Building Operational Resilience: Impact Tolerances for Important Business Services (accessible here).
2. CP19/32 FCA: Building Operational Resilience: Impact Tolerances for Important Business Services and Feedback to DP18/04 (accessible here).
3. CP29/19 PRA: Operational Resilience: Impact Tolerances for Important Business Services (accessible here).
4. The PRA also published CP30/19: Outsourcing and Third Party Risk Management, which firms are encouraged to read alongside CP29/19 (accessible here).
5. The new proposals further develop the earlier 2018 joint Discussion Papers (accessible here).

The latest proposals set out requirements and expectations for firms and financial market infrastructures (FMIs) to identify their important business services by considering how disruption to the business services they provide can have impacts beyond their own commercial interests:

- Firms must set a tolerance for disruption for each important business service, ensure they can continue to deliver their important business services and be able to remain within their impact tolerances during severe but plausible scenarios.
- Proposals also include requirements to map and test important business services to identify vulnerabilities in firms' operational resilience and drive change where needed.

UK regulators want to bring about a change in how the financial services industry thinks about operational resilience – a shift in mindset – informed by public interest. It's not just external threats, such as cyber-attacks, that firms need to be vigilant against: they need to be resilient against a far wider range of potential operational issues.

UK regulators are looking for outcomes focused on the continuity of supply of the financial products and services that people, businesses and the wider economy rely on most. Even in the event of severe operational disruptions.

But what is operational resilience?

Describing operational resilience as "the ability of firms and FMIs and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions", UK regulators will be asking chairs and CEOs what strategic decisions and investment choices they're making to build operational resilience into their business models and to maintain the supply of important business services in the event of a major incident or (what they call) "a severe, but plausible, scenario."

Who are the proposals directed at?

PRA-designated investment firms

Enhanced scope SM&CR firms

Solvency II firms

Other firms include: banks, building societies, recognised investment exchanges, and entities authorised or registered under the Payment Services Regulations 2017 and Electronic Regulations 2011.

What should firms do?

Identify their important business services and map successful delivery back to the key underlying resources.

Test their ability to withstand a severe event with reference to an impact tolerance.

Use the test results to identify resilience gaps and make investment choices that increase their ability to provide these important business services even when severe disruptive events happen.

Mapping

UK regulators are concerned that complex interdependencies could increase the likelihood of a major disruptive event spreading quickly. In terms of the types of solution that they expect to see, this includes more joined-up engagement with important suppliers to dependent authorised firms and a proper understanding of such suppliers' resilience arrangements.

Impact tolerances

These are considered to be the maximum tolerable level of disruption to an important business service, including the maximum tolerable duration of a disruption. UK regulators expect to know that a firm has planned for the worst but are able to continue to deliver important business services when the worst does happen. In simple terms, they want customers to be protected by the actions firms take now.

Testing

Testing a firm's ability to remain within its impact tolerance during a severe event is likely to reveal gaps and weak points in the resources that support the firm's ability to deliver important business services.

The joint consultation papers go further than the 2018 discussion paper by explaining that where gaps are identified, firms are expected to take actions to ensure they remain within their impact tolerances.

Risk appetites for a firm shouldn't be set solely in line with strategic objectives, as this can work against achieving the continuity of supply of an important business service.

Important business service

A business service is provided by a firm or FMI to an external end-user or participant. This business service becomes an "important business service" when a disruption to its provision could cause intolerable harm to consumers or market participants; to the soundness, stability or resilience of the UK financial system; or to the orderly operation of the financial markets. It could threaten policyholder protection, safety and soundness, or financial stability.

UK regulators aren't prescriptive in this regard, but they've provided guidance on how to go about identifying an important business service.

Culture change

While UK regulators believe that rules can give clarity about their expectations, operational resilience is also about cultural change. Where possible, the proposals sit alongside established operational risk-management practices.

The resilience outcome is what's most important to UK regulators, not simply a firm's ability to demonstrate compliance. Every senior manager will need to know what they're responsible and accountable for, which includes the requirement for firms to establish clear lines of responsibility for the management of operational resilience.

What happens next?

Both the FCA and the PRA consultation papers are open until 3 April 2020.

In the meantime, UK regulators will continue to engage with the financial services industry and the wider public on their proposals.

Subject to feedback received, the PRA will work to develop its new operational resilience rules (as set out in its Operational Resilience Parts) for publication in H2 2020. The proposed implementation date for the proposals is H2 2021.

The FCA expect to publish its finalised rules in the second half of 2020.

As mentioned at the beginning of this briefing, the PRA also published a consultation paper (CP30/19) on proposals for modernising the regulatory framework on outsourcing and third-party risk management. These proposals look to pursue the following:

Objectives

- Facilitate greater resilience and adoption of the cloud and other new technologies, as set out in the BoE response to Future of Finance Report.
- Take into account EIOPA's draft Guidelines on Outsourcing to Cloud Service Providers and EBA's Guidelines on ICT and Security Risk Management.
- Complement the policy proposals on operational resilience in PRA CP29/19.
- Implement the European Banking Authority's (EBA's) Guidelines on Outsourcing Arrangements.

Next steps

Responses are requested by 3 April 2020. The PRA proposes to publish its final policy on the proposals in CP30/19 in H2 2020, with implementation of most of the proposals shortly after.

Treasury Committee IT failures findings report

On 28 October 2019, the House of Commons Treasury Committee also published its Report into IT Failures in the Financial Services Sector (accessible here), following an inquiry that began back in November 2018.

The inquiry was launched in response to a number of high-profile IT failures at banks and other financial institutions that reportedly affected large numbers of customers. The Treasury Committee examined the causes and consequences of IT failures in the financial services sector and what was being done by industry and the FCA, the PRA and the BoE to promote operational resilience in light of the rise of digital banking services.

Current levels of financial services IT failures are unacceptable and failures of third parties can't be used as excuses when IT incidents occur, but upgrading legacy IT systems will help reduce risks.

Who is the report aimed at?

The report sets out a number of recommendations for regulators, the UK government and firms. It'll also be of interest to any individuals who fall under the Senior Managers and Certification Regime (SM&CR), fintechs and outsourced technology providers operating in the financial services sector (including providers of cloud services).

The report finds:

- The current level of financial services IT failures is unacceptable.
- Regulators must act to improve operational resilience of the financial services sector.
- Levies in the financial sector should increase so regulators can hire experienced staff.
- Regulators must use enforcement powers so failures don't go unpunished.
- There should be increased individual accountability for FMIs under the SM&CR.
- Upgrading legacy IT systems will help reduce risks.
- There is a need to address poor IT change management and recognise the importance of testing.
- Failures of third parties cannot be used as an excuse when IT incidents occur.
- Regulators should amend rules/guidance if regulated firms aren't managing service providers to standard.
- There is a strong case for concentrated cloud services sector to be regulated.
- Firms must resolve customer complaints and award compensation quickly.
- New technology and innovation can facilitate operational resilience but also pose risks.
- Fintechs with access to data but only regulated in the open banking regime pose risks.

Next steps

Though a large number of the Treasury Committee's recommendations are addressed to regulators rather than to firms, the report also provides firms with a good indication of the likely direction that regulatory and supervisory focus will take.

Regulators are expected to respond to the report and to publish consultation documents on operational resilience in the UK's financial sector that are now expected to be published after the recent general election.

In the interim, firms should ensure that they're taking steps now to address, as relevant, the key conclusions and recommendations of the report.

FSB: geographically dispersed infrastructures in the clouds

On 9 December 2019, the Financial Stability Board (FSB) published a report looking at the adoption of cloud computing and data services across a range of functions in financial services. The report, Third-Party Dependencies in Cloud Services: Considerations on Financial Stability Implications (accessible here), looks at the inherent risks when geographically dispersed infrastructures are created. This could cause issues for operational governance and oversight considerations, particularly in a cross-border context and when linked to the concentration of those providers. This may result in restricting the ability of financial institutions and authorities to assess whether a service is being delivered in line with legal and regulatory obligations.

Next steps

The report concludes that there do not appear to be immediate financial stability risks stemming from the use of cloud services, but authorities may engage in further discussion to assess:

- The adequacy of regulatory standards and supervisory practices for outsourcing arrangements.
- The current standardisation efforts to ensure interoperability and data portability in cloud environments.
- The ability to cooperate and coordinate, and possibly share, information among regulators when considering cloud services used by financial institutions.

Operational resilience and the board

Following a recent roundtable discussion we held with firms on the topic of operational resilience and a deeper dive into cyber resilience, it was clear that boards need to engage more than ever with this evolving risk. Key highlights concerning operational and cyber resilience for boards and seniors managers are:

- Operational risk: It's a board responsibility requiring the same attention as other board responsibilities.
- Cyber resilience isn't a separate topic: it's a core responsibility.
- "What is the operational or cyber risk?" should be built in to every board decision.
- Responsibility for operational risk can't be delegated: the board is responsible for third-party failures.
- The risks of failure aren't limited to the firm but will affect the firm's clients.
- Seniors don't need to understand the technology but the risks to the firm and its clients.

Questions firms will need to answer

The FCA will be asking Chairs and CEOs what strategic decisions and investment choices they are making to build operational resilience and to maintain the supply of important business services in the event of a major incident and will look at the following:

- First, firms should identify their important business services and map successful delivery back to the key underlying resources;
- Second, they should test their ability to withstand a severe event with reference to an impact tolerance; and
- Third, they should use the test results to identify resilience gaps – and make investment choices that increase their ability to provide these important business services – even when severe disruptive events happen.

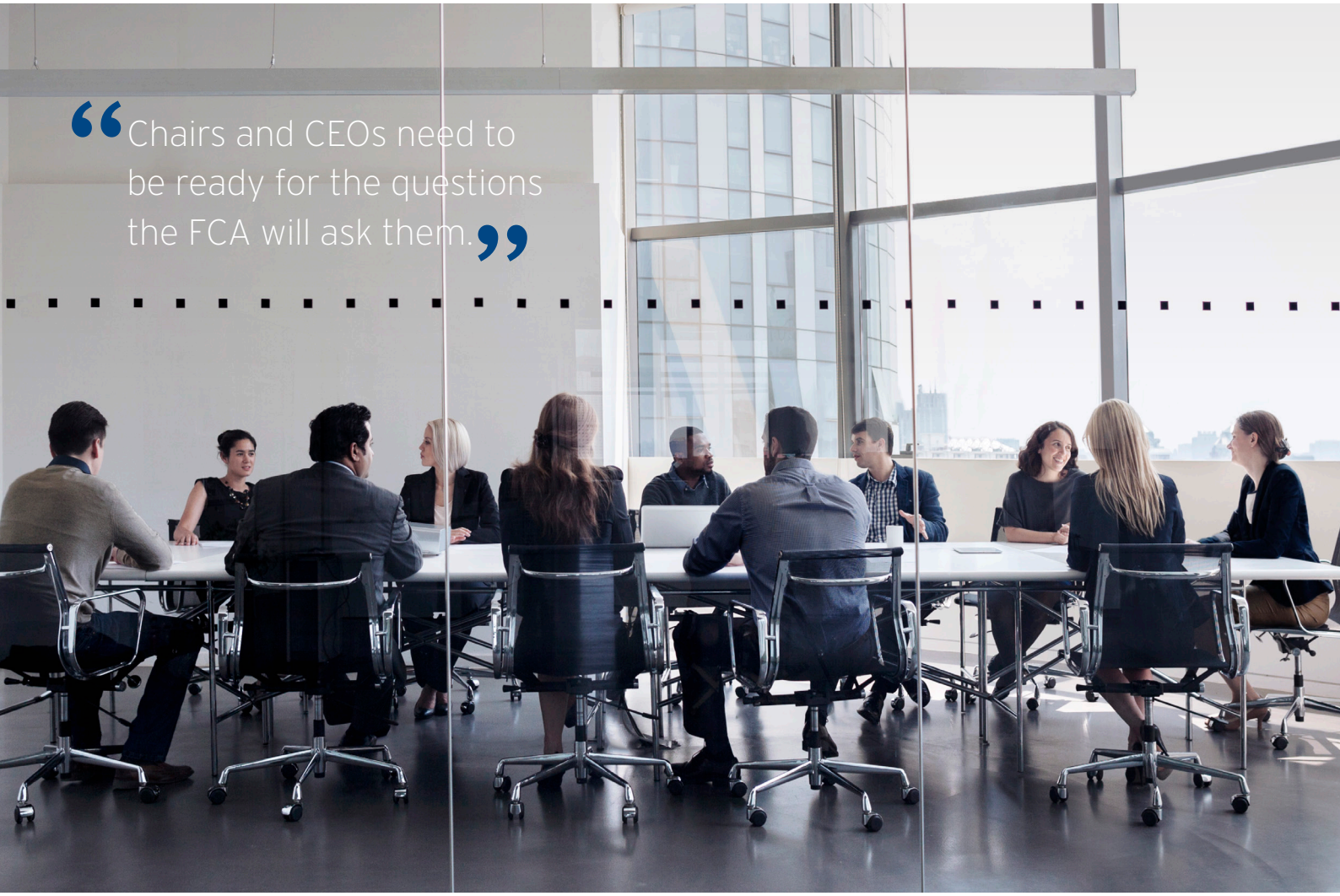
If risk appetite is only set in line with corporate strategic objectives, which are inevitably anchored to profitability and cost reduction, this can work against achieving the continuity of supply of an important business service.

Planning to deliver

In summary, the FCA want firms to build operational resilience because they believe it is in the public interest to do so.

- Operational risk is, as the name suggests, a risk.
- Operational resilience on the other hand is an outcome. It is a step change, where the FCA expect firms to be forward looking and making decisions today that help prevent harm tomorrow.
- Impact tolerance requires firms to think about services from the perspective of their consumers, as well as the wider UK financial system and financial markets.
- Remediation requires firms to not only test their ability to withstand a severe event with reference to an impact tolerance, but to use those results to identify resilience gaps.

Look out for our more detailed article on operational resilience in the next edition of Global News & Views coming in 2020.



Please contact for further details:

David Morrison
Global Head of Trustee and Fiduciary Services
david.m.morrison@citi.com
+44 (0) 20 7500 8021

Amanda Hale
Head of Regulatory Services
amanda.jayne.hale@citi.com
+44 (0)20 7508 0178

Ann-Marie Roddie
Head of Product Development Fiduciary Services
annmarie.roddie@citi.com
+44 (1534) 60-8201

Caroline Chan
APAC Head of Fiduciary Business
caroline.mary.chan@citi.com
+852 5181 2602

Shane Baily
EMEA Head of Trustee and Fiduciary Services
UK, Ireland and Luxembourg
shane.baily@citi.com
+353 (1) 622 6297

Jan-Olov Nord
EMEA Head of Fiduciary Services
Netherlands and Sweden
janolov.nord@citi.com
+31 20 651 4313

www.citibank.com/mss

GRA31112 01/20