1 October 2020

A response to the PRA Consultation Paper (CP29/19) Operational Resilience: Impact tolerances for important business services and the FCA Consultation Paper (CP19/32): Building operational resilience: impact tolerances for important business services and feedback to DP18/04

About us

UK Finance represents nearly 300 of the leading firms providing finance, banking, markets and payments related services in or from the UK. UK Finance was created by combining most of the activities of the Asset Based Finance Association, the British Bankers' Association, the Council of Mortgage Lenders, Financial Fraud Action UK, Payments UK and the UK Cards Association. Our members are large and small, national and regional, domestic and international, corporate and mutual, retail and wholesale, physical and virtual, banks and non-banks. Our members' customers are individuals, corporates, charities, clubs, associations and government bodies, served domestically and cross-border. These customers access a wide range of financial and advisory products and services, essential to their day-to-day activities. The interests of our members' customers are at the heart of our work.

Overview

UK Finance is pleased to respond to the co-ordinated consultations from the FCA and PRA (together, "**the authorities**") on strengthening the operational resilience of the UK's financial sector.[1] UK Finance members recognise the importance of operational, alongside financial, resilience in the face of rapid technological changes and challenges as well as the increased inter-connectivity of the financial market, the growing number of participants, increased use of outsourced service providers and the evolving threat landscape. We agree with the elements of the definition adopted for operational resilience as "*the ability of firms and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions*". In particular, the inclusion of the learning element within the definition reflects the reality that, in today's inter-dependent and inter-connected ecosystem, building a resilient financial sector relies on promoting a culture of collaboration and trust between not just financial sector participants, but also industry and its regulators.

Our members welcome Bank of England proposals for improving the operational resilience of Financial Market Infrastructures (FMIs) in order to protect the wider financial sector and UK economy from the impact of operational disruptions. We note the importance of improving the operational resilience of FMIs given the risk from a failure of a market infrastructure is multiple times the risk of failure of any one bank.

Overarching Principles

Our members would like to emphasise the particular importance of four overarching principles that we encourage the authorities to consider and apply across the constituent elements of operational resilience, namely: collaboration; proportionality; international alignment; and ongoing guidance.

Collaboration: Collaboration will be key to the success and effectiveness of policies on operational resilience. While operational incidents are primarily events to avoid, mitigation and recovery from them are also points of learning. As an industry, we are keen to collaborate with the regulators in a pragmatic

[1] https://www.fca.org.uk/publication/consultation/cp19-32.pdf and https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/cp2919.pdf

way that reflects the diverse nature, and size, of our membership. We continue to reiterate the notion that 'one size' does not fit all.

Proportionality: Proportionality must be a key pillar of the authorities' proposals given the disparate business models, risk profiles, size and, in many cases, global nature of our members. We would especially note that considerations relevant for a retail bank may not apply to a wholesale bank. We support the authorities' intention not to create an unnecessarily prescriptive mapping process and see this as a good example of a proportionate approach.

International alignment: Of key importance is the need to ensure greater alignment of UK policy with rules, principles and guidance issued by global regulators and standard setters. In many instances, we anticipate the UK will be more advanced in both its thinking and progress on operational resilience. We therefore strongly encourage greater cross-border collaboration between international regulators. This will assist the significant number of global firms we represent, and enable them to plan appropriately the parts of their business which have extra-territorial impacts.

Where the UK rules diverge from international standards, international firms headquartered outside the UK and UK firms with significant operations outside the UK could face different or even conflicting requirements from other regulators. Given that firms rely on numerous end-to-end processes and shared services across jurisdictions, any divergence between the UK rulebook and global standards would challenge their global support models and increase inefficiencies and complexities in meeting the policy objective of operational resilience.

This is demonstrated for example by the draft Principles for Operational Resilience, on which the Basel Committee on Banking Supervision (BCBS) is consulting until 6 November 2020. Our members note that the BCBS principles draw on,[2] but diverge from, the UK authorities' proposals in that they have as their focus 'critical operations' rather than important business services.

The authorities should continue to work closely with other international regulators to encourage a common approach to operational resilience to reduce the risk of conflicting requirements. Many services received by UK regulated legal entities are provided by out-of-country subsidiaries and vendors who additionally provide the same services to other group entities. A common regulatory approach, including consistency with vocabulary and definitions, would avoid potentially conflicting requirements on service providers such as the requirement solely by UK regulators to set impact tolerances for each important business service.

In addition to alignment of the UK rules with international policy and alignment between the PRA and FCA, we consider that close coupling will be needed between the approaches adopted by the PRA's and FCA's policy and supervisory teams. For example, if the policy team promotes an outcomes-based approach, interpreting the currently proposed implementation timeframe as more of a checkpoint where they expect firms to have made progress, but not necessarily have completed implementation, then supervisory teams must also take this approach into account and be flexible on delivery timescales to firms.

Ongoing guidance: Operational resilience implementation in the industry requires a commitment from the authorities to ongoing guidance. This principle is important in relation to lessons learned and scenario testing and is also equally applicable to the establishment of Important Business Services and Impact Tolerances. For example, given the importance of the learning component of operational resilience enhancement, we believe an early thematic review of firms' designed approaches to lessons learned

---

[2] https://www.bis.org/bcbs/publ/d509.pdf, at para 11: "The principles for operational resilience set forth in this consultative document are largely derived and adapted from existing guidance that has already been issued by the Committee or national supervisors over a number of years". Footnote 9 reads: "See eg *Bank of England and Financial Conduct Authority, "Building the UK financial sector's operational resilience" (December 2019)*; The European Commission, *Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure (December 2019)*; the Monetary Authority of Singapore, *Ensuring Safe Management and Operational Resilience of the Financial Sector (April 2020)*, and the International Organization of Securities Commissions (IOSCO), *Principles on Outsourcing (May 2020)*."

following a scenario exercise, perhaps with guidance on identified good practice, would provide members with a useful steer. We also welcome the support from the authorities (via CMORG) to the ongoing work of the ORCG to allow industry players to work together to develop a library of scenarios (e.g. pandemic, terrorism, severe weather event, etc.) going forward to increase synergy and reduce overlapping efforts.

COVID-19

The COVID-19 pandemic has been an atypical disruption of significant size, scale and duration, however the disruption has had a limited impact due in particular to the increased digitisation of services and the fact this was a known and high probability risk already foreseen by the industry. Furthermore, the pandemic is a market wide event that occurred over a period that afforded firms sufficient time to pivot to alternative infrastructure. UK Finance members therefore view the COVID-19 pandemic as an example (albeit exceptional) of a business continuity event that should be contrasted with the type of shock event the authorities' operational resilience proposals are designed to address, namely events that occur without lead time and cause immediate disruption.

Given the above our response does not focus specifically on COVID-19 experiences other than to reflect our concerns about its bearing on the setting of implementation timescales for the operational resilience requirements. The pandemic has, however revealed the interconnectedness of markets, firms, utilities, local and national governments. This highlights that coordination among multiple stakeholders (for example the CMBCG in the case of COVID-19), as well as convening power by the official sector, is critical to supporting operational resilience of the sector. The pandemic has also highlighted the need for development of global standards and/or a global framework, so that industry has a common framework to point to rather than separate jurisdictional frameworks.

Structure of our response

We are largely supportive of the outcomes-focused approach that the authorities are taking. We believe that identifying important business services, setting impact tolerances for these services, and then scenario testing to test ability to deliver within impact tolerances in severe but plausible scenarios is an appropriate approach to improving operational resilience. Indeed, many UK Finance members already have started to adopt a similar approach at the core of their operational risk management and resilience frameworks. Some firms have already started to identify their important business services, map their resources and set impact tolerances, while others are still at the start of this journey.

However, there are elements within the policy proposals which, in our view, require further consideration before those policy proposals are finalised. Additionally, there are elements which our members do not currently support.

We have presented our responses thematically in the sections below, taking both of the authorities' consultations together. Whilst it is a closely related subject, we will be submitting a separate response to the proposals on outsourcing and third party risk management, which form part of the FCA's consultation[3] and which are contained in a separate consultation paper from the PRA.[4]

In addition to the issues explored in the sections below, our members wish to raise the following general questions relating to the scope of the proposals:

- We assume that the scope of Operational Resilience applies to the HoldCo, not just the ringfenced bank (RFB). However, there are some entities within HoldCo that fall outside of UK regulation. We would welcome further guidance on the legal entities that are in scope of these requirements.

[3] See Chapter 8, FCA CP19/29, https://www.fca.org.uk/publication/consultation/cp19-32.pdf

[4] https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/cp3019.pdf

- Ringfencing: What is the relationship between the Ringfenced Bank and the non-Ringfenced Bank with regard to operational resilience? Are there any situations where ringfencing rules would 'trump' operational resilience?

- Recovery & Resolution Planning (RRP): Our members note that the BCBS consultation envisages an explicit link between operational resilience and RRP. The finalised UK regulatory policy requirements on operational resilience should clarify how these align to the policy requirements within the PRA supervisory statement SS9/16 'Ensuring operational continuity in resolution'. The final policy should provide some flexibility in the development of operational resilience frameworks to account for those cases where linkage to RRP may not be appropriate.

1. Important business services

Elements we support

We agree that firms need to identify important business services and welcome the authorities' further refinement of the definition since their original joint Discussion Paper in 2018.[5] We agree that it would not be beneficial to firms for the authorities to effectively pigeonhole activities by imposing a prescriptive taxonomy of important business services. Firms must make individual judgements.

However, it must be noted that not all important services have such a "point of contact". Examples include settlement, treasury services, financial reporting, other critical support functions, or indirect services such as through open banking application programming interfaces (APIs). Whilst firms will have discretion whether or not to categorise those non-customer-facing services as important business services, the finalised proposals need to be clear about expectations regarding these areas. In particular, the finalised policy should clarify whether they should be independently subjected to the requirements of the proposed rules, or whether they should only fall in so far as important business services are dependent on them.

Elements requiring further consideration

UK Finance members have concerns about the authorities' expectations of the level of granularity they should apply when identifying their important business services. Whilst we note that both consultation papers set out high level factors firms may use to identify important business services,[6] they contain inconsistencies in how they present granularity. The examples provided by the authorities are valid, however most examples in the consultation papers are focused on retail banking. Whilst the consumer harm connection is clear for retail services, it is less so for wholesale banks. Therefore it would be valuable to understand the authorities' view on wholesale services such as derivatives or custody, and in particular how we should approach what is considered acceptable / unacceptable harm to the ultimate consumer. UK Finance recommends that there be further consultation and discussion between the authorities, firms and industry bodies ahead of policy publication to establish clarity on just how specific firms ought to be when identifying their important business services.

Our interpretation of the discussion paper and consultation papers was that the focus for firms should be on existing customers, and therefore services that support prospective business have been largely considered out of scope, save for certain limited markets or in cases where there is limited scope for substitution. We would welcome additional clarity on this aspect particularly given the PRA's focus on the prudential aspects and potential implications (systemically or in relation to a firm's viability) that a

[5] https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf?la=en&hash=4238F3B14D839EBE6BEFBD6B5E5634FB95197D8A

[6] See for example FCA CP19/32 at 4.20.

disruption to these services supporting prospective business may have on a firm. The PRA paper[7] implies that there should be alignment to Recovery and Resolution Planning (RRP) through considering the impact of failure of a service and its potential to inhibit the functioning of the wider economy including at a point of resolvability by the BoE of a firm. At the highest level, this suggests important business services should map to Critical Functions to provide end-to-end resilience of a service. If this is the policy intention the industry would welcome collaboration with, and input from, the authorities on how the operational resilience CPs will be linked to PRA supervisory statement SS9/16 'Ensuring operational continuity in resolution', including any proposed future changes to SS9/16. Members consider that the best way to achieve clarity on this point is to include references to SS9/16 and to use common terminology. It is noted that the operational resilience CPs refer to 'important business services' whereas SS9/16 refers to 'critical services'.

However, we consider that RRP and Operational Resilience should also be clearly differentiated in some areas. For example, firms should be allowed to align multiple Critical Functions to one Important Business Service (and vice versa) where they deem the approach as sensible and supportive of the desired business outcome.

Elements we do not support

The finalised policy should clarify the definition of an 'external end user'. Our members do not consider that the authorities themselves should be included in the definition. The finalised policy should clarify that mandatory regulatory reporting is not a business service (and consequently not an important business service), and is therefore a separate obligation outside the scope of the requirements relating to operational resilience.

2. Impact tolerance

Elements we support

Industry supports the introduction of impact tolerances, informed by robust, relevant and meaningful metrics that a firm decides to adopt for each important business service. However, please refer to our comments in the 'Overview' section above, where we emphasise the need for international alignment, particularly as there is no equivalent of the concept of impact tolerance in other proposals outside of the UK.

Elements requiring further consideration

The definitions of impact tolerances are different and require harmonisation and further clarification. The authorities should work closely together in considering how the following issues can be improved, whilst taking into account industry collaboration and proportionality.

When defining impact tolerance as a maximum level of disruption, the difference in terminology used by the FCA and PRA is confusing and the authorities should explore how their definitions can be harmonised.

When considering the relationship between the FCA's concept of "intolerable" customer harm and impact tolerances, it is important to note that duration alone is not the most effective way of setting impact tolerances and we would urge the regulator to introduce more guidance on how best to define (and therefore manage) customer harm. It is also important to note that many disruptive scenarios will impact multiple services simultaneously and that the aggregated impacts across those multiple services would potentially cause harm after a much shorter duration than if a single service was impacted. Transaction

[7] See PRA CP29/19 at 2.5(a), which requires that, when assessing the risk a business service poses to financial stability, firms should assess the potential to inhibit the functioning of the wider economy, in particular the economic functions listed in SS19/13 'Recovery planning'.

volume and/or transaction value could be important determinants in assessing harm and impacts, but firms may also need to consider business services and activity which do not directly produce customer transaction impacts.

Whilst we acknowledge that "intolerable" harm will vary according to customer type, the industry requires further consultation with the authorities to gain further clarity as to where in those customers' contact with the firm the impact tolerance should be placed, in particular the extent to which the authorities expect firms to segment their customer base and identify different impact tolerances for different client sub-groups.[8] For example, would a firm be expected to respond more quickly for a smaller, but more vulnerable, customer sub-group? Whilst members do not object to this in principle, it raises questions as to whether it would be more appropriate for firms to develop communications solutions targeted at certain customer sub-groups rather than to invest substantial amounts on infrastructure overhaul, across all of their client groups,. This may also have the unintended consequence of firms electing not to service those vulnerable client categories if it is a prohibitively high risk and costly to do so, bearing in mind that customer vulnerability is often transient.

Wholesale firms would also benefit from further clarity on what is considered ‘intolerable harm’ to their clients. It would be useful for our members to understand whether the authorities intend to provide industry-wide guidance to firms on where the authorities believe impact tolerances should be set. Alternatively do the authorities intend to encourage collaboration from firms and market participants on these areas. We note this necessary level of cross-level co-ordination would also be likely to stress the proposed implementation time frames.

We consider that the industry is aligned that impact tolerance serves primarily as a forward-looking planning tool. As a result our members request clarification on how the supervisors will use impact tolerances. Will the principle of proportionality be applied (assuming reasonable justification is provided) or do supervisors intend to use impact tolerance statements as a benchmarking tool, with the implication of quasi-mandated tolerances? Equally, our members have a concern that the proposed PRA Rule 2.5 may be interpreted as a compliance standard post-event which is not supported by the narrative in the draft supervisory statement (Paras 3.4, 3.15, 6.8).

Connected with each of the above comments, we refer to our overarching comments on international alignment in the 'Overview' section. We are concerned that allowing the architecture of the UK supervisory authorities to be reflected in the design of impact tolerances may result in a solution which becomes unique to the UK and therefore inconsistently applied across financial services. This will have impact for financial institutions with a global presence, but also for tooling, documentation and training provided by external organisations who may find it too complex to deal with UK specific regulations. This may also introduce fragmentation between jurisdictions, which, given the interconnected nature of many critical business services, would significantly impair the goal of raising the wider industry’s operational resilience.

Elements we do not support

We consider that the proposal that dual-regulated firms be subject to multiple impact tolerances to meet the different statutory objectives of the PRA and FCA may add unnecessary complexity and cost and involve a significant time to monitor / test multiple impact tolerances to ensure important business services remain within those set tolerances. For example, the PRA is proposing that group important business services are identified with impact tolerances being set from them. It is not clear how this proposal would work in practice alongside or with the important business services and their impact tolerances. With the FCA also requiring the identification of important business services with impact tolerances, those firms that are of systemic importance to the UK economy will potentially need to identify three ‘sets’ of important business services and impact tolerances.

---

[8] This clarification is particularly necessary given that the FCA's current definition of impact tolerance refers to "intolerable harm to any one or more of the firm's clients".

In addition, due to the complexities of comparing multiple business lines, for dual-regulated firms the assessment of resilience will necessitate the development of some quantitative metrics or standards. Determining the appropriate measure and any methodologies relating to them may become a logistical challenge unless sufficient time is provided to allow for the appropriate design. We suggest regulators engage particularly with the larger and more complex organisations to initiate a discussion on this matter. Given this will be an iterative process, we also encourage that due consideration be given to the implementation timeline in this regard.

There is insufficient information within the consultations to clarify how firms could meet these requirements and balance the concerns of both the FCA and PRA during a stress event.

3. Mapping

Elements we support

We support the requirement to undertake resource mapping and acknowledge that it is key to highlighting areas of operational resilience vulnerability. However our members have identified that process and resource mapping is likely to be one of the most resource intensive elements even where it is possible to leverage from existing work, and there are number of areas for further consideration.

Elements requiring further consideration

i. Practical considerations

Ultimately, technology solutions will need to be developed to address the difficulty in keeping maps of such complicated systems up-to-date in an economically efficient way. Integrating existing data stores into a unified end to end view across a business service presents challenges. Indeed, our members note that some elements of mapping highlighted in the authorities' consultations are not practical to map at this stage, for example, data/information and 4th parties.

Given that the map for any firm or entity will take iterations and time to build, supervisors should be ready to acknowledge that an incomplete, but best efforts, picture that enables effective prioritisation and timely action is preferable to pursuing a complete picture at all costs due to the threat of regulatory sanction.

Our members note that mapping must be made available to supervisors on request and would welcome further clarity on what must be supplied.

ii. Level of granularity

We would like to seek clarity over both the granularity of mapping required and whether all parts of an important service need to be mapped. Our members agree with the draft BCBS principle that the approach and level of granularity of mapping should be sufficient for banks to identify vulnerabilities and to support testing of their ability to stay within the bank’s risk tolerance for disruption considering the bank’s risk appetite, risk capacity and risk.

iii. Intra-group services

Where service is provided by another Group entity outside the UK perimeter, is there an expectation to map these to the same granularity as units within the UK perimeter?

We could expect the level of mapping required to be to whatever level is necessary to manage the dependency, or from another perspective to be consistent with treating these entities on an arms-length basis.

iv Third party services

We would seek additional clarity and guidance from the authorities on how far we need to go in mapping the outsourcing chain to confirm the outsourced service is 'operationally resilient'. Clarity is required on the practicalities of mapping in a third-party firm given that some of the data (for example resourcing) may be sensitive information, a challenge which could be amplified by any cross-jurisdictional regulatory inconsistency. While we would intend to make every effort to understand the resources supporting services provided by 3rd parties, we would be grateful of regulatory recognition that this may not always be possible and the level of detail will be higher level than for internally managed services. Practices will need to develop, such that sufficient and appropriate information flows from outsource providers, to allow mapping to take place to appropriate levels.

Additionally, where a third party outsources part of their service delivery to a 4th or even 5th party, do our members need to map and validate resilience directly with these 4th and 5th parties or is it sufficient to ensure the 3rd party is doing this? Our members note that existing EBA guidelines already require firms to determine whether the part of the function to be sub-outsourced is critical or important and, if so, record it in the outsourcing register. This requirement arguably already introduces mapping of these sub-outsourcing arrangements and the UK Authorities should not look to duplicate requirements in this respect.

It is difficult for firms individually to assess systemic concentration risk. We would expect the authorities to take the lead on the identification and sharing of outsourced / third party supplier concentration risks help address this challenge. Our members note the PRA's intention to consider the development of an online portal to receive submissions from firms' outsourcing registers (section 1.22 of CP30/19) and consider that this is an initiative that should be taken forward to support the identification of supply chain concentration risk within the industry.

Further consideration should be given as to how the authorities can, and should, take action to remediate vulnerabilities occurring in third parties that operate outside the regulatory perimeter.

v. Proportionality

With regard to proportionality, the industry needs to have a tiered approach that supports the mapping of processes at the appropriate level of detail to meet the resilience needs and align with existing approaches. In addition, adapting to the contemplated models is likely to require significant effort to develop and maintain, and will require mapping of end-to-end processes, applications and people, including updating policies and management information tools.

A proportionate approach must also take into account the practical challenges some UK Finance members face in obtaining meaningful and sufficiently detailed information from unregulated third parties to inform the mapping process. We would also note that service providers vary in nature and activity (FMIs, cloud service providers, etc.), and therefore also in the potential systemic risks they pose in case of a disruption, We would urge the UK authorities to consider these issues when evaluating proportionality. This is a key area where the authorities need to engage with firms and industry bodies ahead of policy publication.

4. Scenario testing

Elements we support

We agree that firms should be testing a number of scenarios against the assumption of failure ensuring that response and recovery actions work in all severe but plausible scenarios. Scenario testing should include communication planning and execution.

Elements requiring further consideration

As outlined below, UK Finance members have concerns relating to the policy design for scenario testing, the role of the authorities will play in information sharing, and the parameters for scenario testing.

Firstly, while we support prudent scenario testing, the policy design needs to be proportionate. Firms will face challenges in their capacity to test against multiple scenarios for multiple important business services, and then to capture the necessary changes within business lines. Our current understanding is that all impact tolerances will need to be tested for each important business service on an annual basis. This raises a number of specific questions, on which industry collaboration with the authorities will be necessary, including:

- Do all important business services need to be reviewed annually? Could all important business services be covered over, for example, a 24-month rolling programme?
- Do all impact tolerances need to be reviewed annually (which as a minimum would be a multiplier of x2) or could a mix of FCA and PRA tolerances across each be sufficient?
- Do all resource types (IT, third-party, people, data, property, etc.) need to be reviewed annually for each important – as each resource derives different scenarios?
- Would scenarios need to cover of each resource-type by important business service and by impact tolerance? If so, for some UK Finance members this could multiply into 300+ scenarios annually, which could require a prohibitive level of resources to be devoted to the exercise.

We would additionally seek clarity on when the testing should be paper-based vs simulation vs live systems. Given, as noted above, that the resources required to execute each type of testing can be significant, a value judgement will be required to determine which is best, while also ensuring a "do no harm" approach to testing.

Secondly, our members envisage that industry collaboration and information sharing is likely to increase and mature. Firms suffering disruption will build "muscle memory" over time, and, conversely, firms with good levels of robustness will experience fewer incidents and therefore take benefit from the scenarios and learnings from other firms. However there is also the risk that competition pressure may lead to a restriction in information sharing. Therefore, as outlined in the 'Overview' section we consider that the authorities have a responsibility to commit to providing ongoing guidance to all firms to assist with the learning element within the definition of operational resilience. The authorities should adopt a proactive approach towards sharing details of operational incidents and/or near misses.

Thirdly, our members would request clarification of the authorities' expectations around the parameters of scenario testing. Members would like to raise the following points:

- A distinction needs to be drawn between existing cyber exercises and operational resilience testing. While we understand the theoretical distinction, the resource demand internally will have significant overlap and with the number of tests related to cyber resilience growing, it is essential that authorities coordinate between the two regimes. For example, the recently published EBA Guidelines on ICT and Security Risk Management[9] require firms to consider ICT and security risk management to be part of their operational resilience. The Guidelines include a section (section 3.7) on business continuity management, of which Guideline 82 states: '*A financial institution should consider a range of different scenarios in its business continuity plan, including extreme but plausible ones to which it might be exposed, including a cyber-attack scenario, and it should assess the potential impact that such scenarios might have. Based on these scenarios, a financial institution should describe how the continuity of ICT systems and services, as well as the financial institution's information security, are ensured*'.

[9] https://eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf

- With regard to para 6.5, of the PRA's proposed supervisory statement, we support the degree of discretion given in terms of format but in terms of frequency there is a risk of underestimating the time and expertise that will be required to design, agree and then execute meaningful scenario exercises for each important business service on an annual basis. For example, is detailed analysis (e.g. through simulation) of one scenario for each important business service every year adequate? Or does a more high-level examination of 3-5 different scenarios for each important business service over the course of the year provide a more rounded level of assurance. In either case, this step can only really start once the identification of the important business service, impact tolerance and mapping steps have been completed.

Finally, scenario testing is another area that would be affected by a lack of international alignment and we would refer to our comments in the 'Overview' section.

5. Governance, communications and self-assessment

i. Governance

We believe the authorities should engage with industry to collate views on how to operationalise senior management responsibility. For example, assigning responsibility at business service level does not align with the usual governance structure of most organisations, and the industry would appreciate practical guidance on how to navigate ownership. In particular, we think supervisors should emphasise the need for collective responsibility in implementation/ execution across the SMF community or equivalent as vital for success. In line with the Senior Managers & Certification Regime (SM&CR) responsibilities managing internal operations or technology, the CP identifies the SMF 24 (COO) executive as the most appropriate responsible executive for implementation. While SMF 24 may be best placed to oversee implementation, we view that ownership can sit with another functions (for example, a business SMF as accountable overall).

We would welcome further guidance on whether other SMFs (notably SMFs 2, 4, 6 & 7) should have statements of responsibility around Operational Resilience, and what they should be so that not diluted or misunderstood. The relevant SMFs will need to be responsible, but not limited to:

- Business continuity;
- Cyber-security;
- Information technology;
- Internal operations;
- Operational continuity;
- Outsourcing procurement and vendor management;
- Management of services shared with other group members.

Both regulators have stated the importance of board responsibility in ensuring a successful resilience strategy is executed across the firm. The FCA CP notes that boards should be sufficiently engaged in setting effective standards for operational resilience, and in doing so should allocate themselves sufficient time to establish the business and risk strategies. The FCA CP also highlights that board members and senior management should possess sufficient knowledge, experience and skills necessary for the discharge of responsibilities. While we accept the fact that the board has a very important role to play, our members have concerns regarding a wider trend toward assigning ever greater responsibility upon the board for specific risk areas (e.g. cyber-security).

We support the proposals from the authorities that impact tolerances for important business services (and the operational resilience framework as a whole) should be signed-off at board-level, to ensure there is

appropriate senior level support, ownership and oversight. However, our members wish to emphasise the importance of recognising that the board's main function is to challenge the bank's strategy, including in relation to operational resilience issues. Many of the responsibilities will be managed effectively at executive management levels, with board oversight. While boards need to have the resources to hand to allow them to provide that effective challenge, we consider it is important to avoid suggestions that boards should set strategy rather than challenge strategy set by the business.

ii. Communications

The FCA CP emphasises the need for fast and effective internal and external communication strategies to be put in place, and that, from an internal standpoint, planning should address how to contact key individuals, operational staff suppliers and regulators. UK Finance members agree with the communication proposals. We would, however, seek clarification from the authorities about the role they will play in coordinating communications relating to cross-firm / systemic disruptions.

iii. Self-assessment

Our members note that the policy proposals require firms to prepare a self-assessment document with the initial self-assessment due on the first anniversary of finalised policy (likely Q1 2022) being published and then annually.[10] We would appreciate practical guidance from the regulators on the essential components of a self-assessment (governance, risk remediation, etc.).

Clarification would also be helpful on whether the authorities intend to provide any guidance on the format for the self-assessment and guidance on the qualitative and quantitative data that will be required to evidence testing outcomes. Whilst we would be opposed to regulatory prescription, we consider that some level of standardisation would enable the PRA and FCA to effectively perform comparisons between the self-assessments received from firms and bring a level of consistency of content. Further, UK Finance members would welcome the opportunity for further discussion with the authorities to gain clarification around timelines. We welcome the publication of the updated Regulatory Initiatives Grid, which outlines that final policy is expected in Q1 2021 and will be followed by "at least a 12-month implementation period". The consultation papers refer to 'periodic' self-assessment. Further clarity is needed on the dates for the submission of the first self-assessment, the frequency of ongoing submissions to the authorities and what constitutes a noteworthy change outside of an annual assessment cycle.

Whilst the consultation papers make reference to a three-year period to operate within impact tolerances, most material activity would need to be completed by the end of 2021 to inform a self-assessment and allow time for remediation of vulnerabilities by early 2024. Members are also concerned that the consultation papers set out express timescales in starker language than some of the authorities' verbal language in various forums as to the position to be reached by the end of 2021/early 2022. Speeches given by the authorities suggest that the proposed timelines are flexible as long as they see firms make significant progress. The finalised proposals should make clear the expectations on firms.

6. Implementation time-frame

UK Finance members consider that the proposed maximum timeframe of three years for firms to comply with the published policies will prove challenging for many firms, particularly those that are considered systemically important to the UK economy. The likely biggest challenge will be remaining within impact tolerances, especially for business services with significant external dependencies. This timescale is aggressive and may drive unintended consequences, for example by increasing concentration risk if some participants are forced to leave the market. Implementation under aggressive timeframes will mean

[10] FCP CP 19/32 at 7.17; PRA CP 29/19 at 4.29

key resource supporting BAU activities around resilience will be ‘stretched’, which could result in further unintended consequences. This has been compounded by the resource challenges presented by the COVID-19 pandemic. Additionally, until assessment cycles are matured and embedded, it is not possible to establish what level of remediation will be necessary and could result in significant, multi-year investments.

Due to the rushed implementation and remediation timeline, and especially given that the implementation timeline and regulatory expectations from other jurisdictions are not yet clear at this stage, it is possible that firms will approach operational resilience as an expensive tickbox compliance exercise. In our view this would not be an optimal outcome, as the industry stands ready to harness the benefits of the policies and improve operational resilience especially given that current events caused by COVID-19 are testing response capabilities.

We suggest that a more practicable approach would be a "phased approach" setting the requirements in the form of a road map with appropriate checkpoints that individual firms can meet in agreement with their firm's Supervisors based on what needs to be implemented and is feasible based on scale and complexity. We note that a phased approach has been proposed for implementation of the PRA's proposals on outsourcing.

Such a phased approach will allow us to learn from past experiences in a meaningful way. We would highlight again the importance of collaboration between industry players and the authorities. This will be key in the implementation and subsequent remediation processes, as we work together to ensure the new concepts introduced by the UK (and soon international) authorities are fit-for-purpose and genuinely strengthen operational resilience in the financial system.

We would welcome further discussion with the authorities on how a phased approach could be adopted. One possible approach would be for the authorities to review and agree designs at staged gateways for key components of the operational resilience framework, including:

- development of business service catalogues and identification of important business services;
- mapping of resources for important business services;
- definition of impact tolerance methodology and setting of impact tolerances for each important business service;
- scenario testing approach and scope and;
- definition and completion of the self-assessment document.

These gateways could operate as standard "deadlines" across the industry, or be firm-specific.

With regard to remediation timeframes, the section in the FCA’s consultation on ‘Transitional Arrangements’ needs clarification. As drafted, it implies that vulnerabilities identified in Cycle #2 also need to be remediated by early 2024 (i.e. 2 years).

Given the comments noted above, it would be useful for the authorities to state in their policies that, whilst a three year implementation timeframe is desired, they will work closely with their regulated firms to agree a timeline separately that is appropriate to the firm with an expectation that the timeline will need to be supported by a road map or project plan that is agreed with/or by) the relevant regulator.

7. Cost Benefit Analysis

We agree there are clear benefits to achieving operational resilience, but the industry estimates of the cost implications far exceed those presented in the CBA. Further regard must be given to proportionality, and there are a number of dependencies that will affect cost.

Conclusion

While we support the outcomes-based approach, we consider that the authorities' aim of strengthening the sector's operational resilience should follow the overarching principles of proportionality, international alignment, collaboration, and ongoing guidance. There are several aspects of the proposals that UK Finance members do not currently support. In particular, we consider that dual-regulated firms being subject to multiple impact tolerances to meet the different statutory objectives of the PRA and FCA will add unnecessary complexity and cost. We ask also that the finalised policy clarify that mandatory regulatory reporting is not a business service, and consequently cannot be an important business service.

There are several areas that would benefit from further consideration and potentially discussion between our members and the authorities ahead of final policy publication. These relate to the required level of granularity for both business service identification and mapping, the level of interlinkage between operational resilience and recovery and resolution, and the design and parameters for scenario testing. Finally, we have made suggestions for phased implementation and have requested clarification in relation to the dates for first and ongoing submissions of self-assessments to the authorities.

We hope you find UK Finance's response helpful and we would be happy to discuss any of the points raised in further detail.

Responsible Executives

Andrew Rogan
Director, Operational Resilience
andrew.rogan@ukfinance.org.uk
020 3934 0263

Daisy Johnson
Analyst, Operational Resilience
daisy.johnson@ukfinance.org.uk