A response to the Joint Discussion Paper: Building the UK financial sector's operational resilience

5 October 2018

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 joint PRA, Bank of England, and FCA (the regulators) Discussion Paper (the DP) on *Building the UK financial sector's operational resilience*[1], and recognise the importance of operational, alongside financial, resilience in the face of rapid technological change, continuing cyber-attacks, greater use of outsourcing, and unplanned system outages. We are generally supportive of the approach that the regulators are taking and have responded on a thematic basis, rather than to the individual questions, to address the main overarching aspects we have drawn from the DP.

We agree with the intent behind the concept of prioritised 'business services' as a way of aligning an integrated approach to operational resilience across a firm, against the materiality of the services to sector, consumer and firm.

Inevitability of operational failure is a helpful concept as it reinforces proactive and pragmatic preparations and dispels the often-held myth that a firm's control environment negates the possibility of disruption.

There should not be a one-size-fits-all approach given the disparate business models, size and, in many cases, global nature of our members. 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.

For boards the principle of and approach to 'impact tolerance' contemplated by the DP will be new and will require careful and measured introduction to ensure it is correctly understood and adopted alongside currently understood risk management frameworks without conflating the concept with risk appetite.

UK Finance observes that the industry has already incorporated many of the core concepts found in the DP, and that these could be implemented in a better and more integrated manner. However, we believe it will be important to ensure that the direction the regulators are taking is done in a measured way that takes into account and avoids conflicting with the currently embedded practices. UK Finance stands ready to support the regulators and the industry in this.

[1] https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf

Business Services

UK Finance agrees that approaching operational resilience from the perspective of business services is a pragmatic way to prioritise improvements, including to systems and processes. Many members already make infrastructure investment decisions on this basis, while also planning their return to BAU following operational incidents along business lines. With 'critical economic functions' (CEFs) a core tenet of the UK's recovery and resolution framework and featuring significantly in UK Finance's systemic members' and GSIB's recovery and resolution plans (RRPs) the DP's use of 'business services' rather than CEFs for operational resilience is an important development. The Bank of England has in the past referred to CEFs for some of its cyber resilience work (the CBEST testing framework for example) but that was only as a means of selecting appropriately critical systems to test, and it was primarily used due to a lack of a widely used and commonly accepted term.

We make the below recommendations for consideration:

- For systemic firms, UK Finance expects that the critical services previously identified as part of the CEF analysis[2] should be the main focus from an operational resiliency perspective for systemic firms, with the existing governance reporting, and metrics being complemented by devising impact tolerances and mapping all underlying processes from an end-to-end business perspective. **UK Finance recommends that the regulators consider both CEFs and 'business services' alongside each other and provide explicit gap analysis of where the current frameworks do not meet the emerging expectations around operational resilience.** This should include creating a universally understood and accepted taxonomy, to avoid two entirely separate concepts which do not align, with in-built flexibility to accommodate market participants which have different approaches and will have developed different levels of maturity with regards to operational resilience.

- For many of our members, the introduction of a framework based on business services will take time to fully embed and mature, particularly in terms of changes to process, methods, accountabilities and culture. **We recommend that the regulators recognise this in setting expectations of implementation timelines**. Although frameworks exist for business continuity or operational continuity in resolution, the creation of an overall business service view will require analysis of existing frameworks, data sources and dependencies. The switch to a business services approach will also require mapping of end-to-end processes, applications and people processes. This will require significant effort to develop and maintain, including updating policies and management information tools. Even for firms which have mapped this for Operational Continuity in Resolution (OCIR) their focus would have been only CEFs, so an entire codification of a firm is not going to be commonly available.

- Whilst 'business services' does provide a more focused approach, the inclusion by smaller firms of all components of the business service's process chain may not be appropriate or proportionate. As illustrated in Fig 3 (page 12), a business service would include all elements from sales through to payment. For a smaller firm operating across a diverse spread of markets, the disruption to the sales process may be less significant in comparison to being unable to fulfil the payment stage for an agreed commitment, for example. **UK Finance recommends allowing a firm to differentiate and prioritise those components that are most critical to its financial viability and/or its customers**. This is important to ensure a proportionate approach can be adopted for smaller firms. Given most smaller firms do not currently, on an individual basis, have CEFs according to their RRP definition, UK Finance is conscious that these firms would also likely not consider they provide a critical or vital business service, which might distort the aggregate risk that a number of these firms together might pose to the operational resilience of the financial sector. Therefore, the regulators will need to carefully consider how to agree an appropriate approach for these firm types.

- Approaching operational resilience from the perspective of business services could result in potential inconsistencies as firms define what constitutes their business services according to their own business models and customer service needs. Overlying this complexity is the fact that regulators and supervisors are themselves likely to form a view as to what constitutes a business

[2] http://www.fsb.org/wp-content/uploads/r_130716a.pdf

service. **We therefore recommend that the regulators engage with industry on how 'business services' are to be understood, and at which level they should be defined.** This will help firms make more informed choices between the approach in the DP and current practices, which will often be at different stages of maturity depending the extent to which they have already been assessed by the regulators under the current frameworks.

- We believe the regulators should consider existing guidelines when considering how firms should prioritise and/or determine the criticality of various business service lines. Some firms may identify a multitude of business service lines, which in some cases intersect with each other. **UK Finance recommends an effective approach would be to prioritise business services such that lower risk/lower impact services are not required to be separately inventoried.** Enabling tiering of business services, according to the relative criticality of each service would ensure investment (and board attention) focussed on the higher-risk critical services. Systemic firms will have already identified their CEFs and consequently a material reassessment of the critical services they provide to the UK economy should not be required.

In summary the core question for the regulators should be to what extent firms will have flexibility to design their own methodologies and taxonomy in order to determine their own business services, taking into account the systemic risks that they pose on an individual and aggregate basis. Viewed alongside the regulators' ambition to introduce an operational resilience stress testing regime, it may be inevitable – especially if the system is designed on a 'pass/fail' basis, as with financial stability stress testing – that in order to pass, firms are driven to adopt common approaches to determining what constitutes a 'business service'. As this outcome may be contrary to the interests of individual firms and their customers, we encourage the regulators to further engage with the industry in order to come to a consensus on the appropriate methodology.

Impact Tolerances

UK Finance is concerned that 'impact tolerances' is yet another term for boards and firms to understand and incorporate into their risk management decision making processes. There is the potential for confusion with this because impact tolerances, as described in the DP, does not align with currently accepted concepts found in a firm's enterprise risk framework. We believe this term will need to be refined in order to be more naturally understood within firms' risk lexicons. In order to address these concerns, the regulators should provide more detail on their expectations around the relationship between a business service and impact tolerances.

As regulators refine approach, the following issues should be considered:

- The DP suggests that each business service line has an associated set of impact tolerances. This has the potential to create a multitude of impact tolerances that a board will need to calibrate, monitor and review. If elevated to board level, as currently suggested in the DP, this may result in an oversight regime which runs the risk of becoming very challenging to manage and contrary to good risk management principles. **UK Finance recommends that the regulators ensure that the impact tolerance framework is designed in such a way that the number of impact tolerances is manageable and focused on those most important considerations**.

- The definition of impact tolerances, as currently written in the DP, is potentially confusing. We note that while most firms currently use the terminology of 'tolerances' as a stage before limit/appetite breaches, the DP suggests that 'impact tolerances' are upper limits where a breach is to be avoided in all but the most extreme scenarios. This is more akin to recovery indicators compared to how the phrase 'tolerance' is commonly used today. **We recommend the regulators work with industry further on an appropriate definition.**

- **UK Finance recommends the regulators provide clarity where a supervisor might also consider setting their own impact tolerances for firms.** The expectation that firms will be able to set a tolerable level of disruption will be challenging as, even with existing risk events, it is challenging to determine the exact number of related data, e.g. exact number of complaints, lost business, operational activity resulting from a disruptive event. Benchmarking and peer analysis will be important to ensure a level playing field, but UK Finance would like to ensure that supervisors

do not create an escalating target that would undermine competition in the market, particularly for smaller firms where the costs of matching a target may be disproportionate to the risks that they pose to the UK's real economy.

- We draw the regulators' attention to the Internal Capital Adequacy Assessment Process (ICAAP), which considers likelihood and impact, and some degree of diversification, when setting capital aside to account for operationally disruptive events. With the DP adopting an approach that specifies an operational disruptive event *will* occur – regardless of likelihood – this could result in firms having to account for more extreme (yet less likely) events than under ICAAP. **We recommend that these scenarios be aligned to the ICAAP and RRP scenarios.** This is to ensure that efforts are not unnecessarily multiplied at significant disproportionate cost to the industry. **Furthermore, we recommend that in the event that a firm meets operational resilience expectations, there is an explicit offset made in their Pillar 2 requirements.**

We agree that impact tolerances should consider criteria including time, number of customers affected and nature of impact and be considered for change as well as operational services. Specific consideration should also be afforded to types of customer (e.g. vulnerable customers), the impact on wholesale markets and more broadly trust in the financial services sector in order to create a methodology that does not set the benchmark for mitigating disruption disproportionately high.

Stress testing

UK Finance believes there are two possible approaches to designing an effective operational resilience stress testing regime. One approach is to design a framework that tests a firm's response to a sector-wide disruption, while another is a framework that tests a firm's response to a disruption that has arisen from within the firm itself. With the DP stating that the starting point when considering operational resilience is that failures are inevitable, both of these approaches should be designed to test people, processes, and infrastructure in the lead-up to an operational failure and their ability to recover from it.

As a general observation, the UK's financial sector has significant experience of sector or sub-sector business continuity testing, having been regularly exercised by the UK authorities since the early 2000s. Equally, many firms regularly subject themselves and their recovery processes to comprehensive internal testing. It should be noted that in these exercises, the cause of the event has traditionally been considered less important than a firm's ability to recover from it. This is different from financial stability stress testing which tends to be scenario-driven.

This stress testing framework is important when considering the question of impact tolerances and how to set them. Questions to consider include how a firm should set its impact tolerance to systemic operational incidents (over which it may have relatively little control) compared to how it should set its impact tolerance to more isolated and/or internal operational disruptions. An important consideration will be the cause of the disruption itself. A tolerance for a cyberattack will be different to that for an internal hardware or software-driven outage. Also, we would like to highlight that impact tolerances may need to consider further dimensions such as the 'layered' nature of disruption (i.e. tolerance may be higher/lower depending on how many areas are being disrupted at once).

There is some concern that market-wide stress scenarios could drive adverse real-world outcomes. A regime that models specific stresses on specific firms or narrowly defined non-financial services sectors may drive adverse outcomes in real-world purchasing decisions. For instance, a scenario of the top 3 cloud providers being unavailable could drive marginal investment to smaller, less robust, and/or less transparent providers who are not in scope for such a scenario. This diversification may be a regulator-desired outcome for the market, but it may be an unintended consequence and could also be negative for specific firms.

We also believe that it is important to consider whether the concept of a 'return to BAU' should be defined. This is because recent examples of operational disruption have shown that while processes or infrastructures may be returned to normal, customers may continue to be harmed by the consequences of the incident either through fraud or some other form of financial detriment or residual risk (e.g. following an identity theft incident).

In terms of sector wide operational resilience testing, CMORG is useful for sector wide exercises but it involves large firms and infrastructure providers and the increasing diversity of financial services means that this, whilst key, may not be where issues are experienced in the future. There would also be further learnings from such sector-wide testing to strengthen collective responses. **UK Finance recommends the regulators create an environment for safe testing that would incorporate non-financial services firms relevant to the continued operation of the sector. We further recommend that, as standard practice, the lessons learned from operational resilience stress test events be made public.**

'Harm' to both consumers and market participants

What constitutes 'harm' is an important concept when designing impact tolerances. UK Finance notes that there is no current definition of the concept of 'harm'. We note that GDPR goes some way in defining the term from a data subject perspective, and we suggest that this be considered as part of defining 'harm' for operational resilience. Existing Conduct Risk practices and Regulatory requirements already ensure firms manage and consider the effectiveness of their services in relation to preventing 'consumer harm'. Furthermore, EBA final guidelines on major incident reporting under PSD2 includes impact thresholds regarding reportable events. **UK Finance recommends that the regulators align the definition of 'harm' to these existing practices.**

Of equal importance is scaling the extent of the consumer harm in the context of operational resilience, both in terms of the volume of consumers and the significance of any 'harm'. To illustrate using the example in the DP, the resilience of underwriting services, where there are numerous alternative providers available within the market, would be less harmful than consumers being unable to access deposit monies, for example. Equally, a service supporting a hundred clients that could equally be operated through manual intervention is likely to cause significantly less harm than the failure of an automated service, with no contingency, servicing thousands/millions of consumers.

Outsourcing and third parties

Firms already widely use outsourcing arrangements as part of their BAU operations. This can be with third parties, across business units or subsidiaries of a firm. It is also used in multiple domains, from technology to legal services.

A robust framework exists today for managing and overseeing inter-affiliate service and advisory support relationships. These have been vetted and approved by regulators across the globe. Firms' outsourcing models are often linked to global operating models, and analysis has been performed by their second and third lines of defence between the outcomes delivered by onsite vs. outsourced coverage of relevant functions. As part of their wider risk management and operational resiliency arrangements, organisations will use a range of metrics to measure and manage risk. In technology, key performance indicators will often be included in contracts, governing BAU operating levels, key performance indicators, and recovery times. Hosting arrangement will also often include load balancing and redundancy measures.

Resiliency of services that use outsourced arrangements are becoming a focus of regulators globally**. UK Finance recommends that approaches to operational resilience are aligned to approaches to outsourcing.** There are multiple mature, internationally established risk controls frameworks for outsourcing, and the regulators should draw on lessons from existing best practice rather than invent something new.

The regulators should also bear in mind that some third parties are unlikely to be open about their internal operating model, because it is part of their proprietorial offering. As such, the regulators will need to take into account this emerging development and set out ways in which the growing systemic risk could be managed and mitigated in as efficient a way as possible. For example, regulators could help develop approaches and methods that help firms achieve visibility of risks that third party providers present.

Given the trends of how many customers now interact with financial services, firms are becoming increasingly reliant on technology companies, such as cloud providers, that are currently outside of the UK's regulatory perimeter. Although each firm will review their individual resilience of providing an omni channel presence, it would be helpful to understand how the regulators will seek to also incorporate an industry-wide operational resilience viewpoint wider than consumer facing technology challenges. In this context, it will be important in the case of a key outsourced provider to understand the role they or even

the regulators play in looking across the industry to see if impact tolerances are set consistently. It might be that differing impact tolerances for the same service provider disruption could create a systemic risk.

For firms that are heavily reliant on clearing banks, UK Finance would welcome further indication from the regulators what the approach to a clearing bank facing an operational disruption might be. It will be very costly for smaller members to build in redundancy for such an eventuality, especially so as the Bank of England could itself step in and facilitate this critical service.

Third parties may also not disclose where they themselves have outsourced sub-components of a service. As such, the regulators should use a proportional view of requirements relating to how organisations map their direct and indirect supply chain. Some of our members have highlighted that they do not have contractual rights to engage directly with a supplier's material subcontractor(s). As such, they rely on their suppliers to engage on their behalf, and to share outputs with them – which clearly exacerbates the noted challenges around third party transparency. **UK Finance strongly agrees with the need for proportionality in mapping the supply chain and recommends the regulators provide further clarity in respect of how the challenges posed by direct and indirect suppliers are expected to be managed**.

The nature of the function provided by trading venues and other FMIs to financial markets participants is such that there is a level of market concentration which in many instances results in reliance on a single provider, without available alternatives. Trading venues and other FMIs (with international customer bases) often find it challenging to adjust their rule books and contractual arrangements without regulatory guidance or requirements. As such, it is difficult for individual firms to ensure that trading venues and other FMIs will allow a firm to continue utilising the trading venue during or following a severe stress or resolution event. Individually, firms do not have the power to influence trading venue rules or to negotiate trading venue contracts unilaterally as a means of ensuring that the individual firm can rely on trading venue operations continuing during or following an adverse event. This is partly because of the lack of bargaining power of individual firms and partly because trading venues and other FMIs are prevented from entering into different terms because of rules on competition and on equal and open access. In particular, firms do not have the ability, and are in any case not best placed, to agree terms in a manner that is consistent across the industry (providing a base understanding of minimum PRA expectations on continuity of market access). **In view of this concern, UK Finance recommends that the PRA collaborate with trading venues and other regulated FMIs to ensure that the terms necessary to support the operational resiliency of individual firms, FMIs, and the financial system as a whole are incorporated into trading venue rules and contracts as an industry standard.**

Management and Governance

We note that the DP considerably expands the scope of the board's involvement in what have been hitherto operational decisions for senior executives in many firms. UK Finance believes that the intent should not be to raise these operational decisions to boards, but that there is appropriate leadership oversight and decision taking at suitably senior levels. It should be made clear that there is a distinction to be made between reporting to board for BAU, crisis reporting and decision-making reasons.

UK Finance is conscious that these issues have historically been considered at executive committees, as the relevant expertise lies here, with the senior management body receiving reports from these committees. As such, it will be important to achieve the right balance between ensuring the board is equipped to carry out its oversight role with sufficient information to reach informed decisions, and allowing the deeper executive management the ability to assess and implement a robust operational resilience environment. **UK Finance recommends that the regulators ensure that appropriate discretion is given to the management of financial services firms to delegate responsibility for operational resilience to appropriate committees with the technical knowledge and skill to manage the risk.**

Communication Plans

Member firms acknowledge the need for clear, relevant and timely communications with customers, business partners and stakeholders throughout and following operational disruption. Further to this, UK Finance already provides a single, unified voice to a crisis specific to the banking sector and its members. UK Finance's communications function in the case of an operational event that threatens resilience is to

prepare media briefings, coordinate cross-industry messaging, and if necessary act as the voice of the UK banking industry for the media and the public during a crisis.

UK Finance would only assume this role when the consequences of an incident became systemic; that is, when an incident negatively affected either a significant portion of the membership or the sector as a whole. It would not be initiated if only a single member suffered a business continuity event, or if members felt that the event did not have systemic consequences.

Where incidents are not systemic, but idiosyncratic, UK Finance recognises that there may be competitive advantages to have differing communication quality levels and that, as long as minimum standards of consumer communication are met, we recommend that this should be left to firms to decide as a commercial decision.

Conclusion

UK Finance is widely supportive of improving the capabilities of the industry to withstand operational disruption and welcomes further engagement on this important topic, particularly around refining the definition of 'impact tolerance', the stress testing framework, and the gap analysis of regulatory expectations and what the industry does today.

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

Responsible Executives

Andrew Rogan

✉ andrew.rogan@ukfinance.org.uk

☎ 020 3934 0263

Nicholas Edge

✉ nicholas.edge@ukfinance.org.uk

☎ 020 3934 1023