WORLD FEDERATION OF EXCHANGES

WFE Response to the Bank of England/PRA/FCA Operational Resilience Consultations

September 2020

www.world-exchanges.org

Introduction

We are grateful for the opportunity to respond to the Bank of England, PRA and FCA's consultations regarding *Operational Resilience: Impact tolerances for important business services*.

The World Federation of Exchanges (WFE) is the global trade association for regulated exchanges and clearing houses. We represent over 200 market-infrastructures, spread across the Asia-Pacific region (~37%), EMEA (~43%) and the Americas (~20%). with everything from local entities in emerging markets to groups based in major financial centres. Collectively, member exchanges trade some $95 trillion a year; while the 50 distinct CCP clearing services (both vertically integrated and stand-alone) collectively ensure that traders put up $1 trillion of resources to back their risk positions.

With extensive experience of developing and enforcing high standards of conduct, WFE members support an orderly, secure, fair and transparent environment for all sorts of investors and companies wishing to invest, raise capital and manage financial risk.

We seek outcomes that maximise financial stability, consumer confidence and economic growth. We also engage with policy makers and regulators in an open, collaborative way, reflecting the central, public role that exchanges and CCPs play in an internationally integrated financial system.

In the face of the considerations arising from the pandemic in the operation of critical market infrastructures, exchanges and CCPs promptly triggered continuity plans (involving, for example, remote working) to maintain their operational resilience against the backdrop of social-distancing policies that governments around the world are adopting.

Market infrastructures recognise their responsibilities as critical elements of the financial system, supplying finance to real economy firms and providing a platform for investors even in times of market stress. Accordingly, they already had developed business continuity plans, which in recent months have been executed as necessary. This has underpinned what have proved to be record volumes of trading.

In line with its membership criteria and its members' own desires, the WFE has long supported the need for market infrastructures to be prepared and as resilient as possible in the face of a wide range of contingencies. For that reason, over the years the WFE has created working groups, consisting of exchange and CCP experts from across the globe, focused on enterprise and operational risk, as well as on cybersecurity. Operational resilience has been – and continues to be – a priority issue for our membership, and one in which significant time, effort and money has been invested. We therefore welcome the opportunity to offer our perspectives and further contribute to the dialogue, in order to secure the shared objectives of fair and orderly markets that promote the safety and resilience of the financial system.

Market infrastructures are implementing advanced and embedded enterprise and operational risk management right across their organisations with measures which are tailored to deliver on the rigorous requirements and regulatory expectations (eg, stress testing scenario planning on a weekly basis) that apply to them as national critical infrastructures. This is necessary to ensure market integrity and systemic stability. The advanced work being undertaken by the WFE's membership has been highlighted in a study[1] outlining the organisational structures and practices being employed – including the creation of dedicated in-house teams focused on developing and delivering high standards of operational resilience, which has the ability to be scaled-up in managing incidents. Operational resilience naturally includes a number of strands, such as the protection of an organisation's cyber infrastructure –

[1] WFE, A WFE Benchmarking Paper Organisational Structures for Enterprise and Operational Risk, February 2020

and the type of preparations and existing measures that have been undertaken by the membership have been publicly detailed by the WFE[2]. These investments in operationally resilient resources and practices[3] supported a well-functioning[4] marketplace with fair and orderly markets operating to the benefit of their local economies. Embedded and resourced operational resilience in market infrastructures supports the prevention of threats from disrupting operations. During the pandemic this included significant steps such as moving, as necessary, from open-outcry to electronic trading. However, operational resilience threats remain constant and evermore resourced, as was witnessed with the recent DDoS cyber-attack targeted at exchanges and other financial services firms. It is for this reason that continuing collaboration and co-operation between all parties (standard-setters, regulators and across industry) is necessary in delivering resilience objectives.

Indeed, ensuring that all market participants[5] ingrain such resilience-based measures in their organisations is part of the need for an ecosystem-wide approach to operational resilience. Longstanding resilience measures were also integral in shielding market infrastructures in relation to pandemic related threats, such as those from phishing emails which fundamentally did not represent a new form of attack but simply had altered content or 'bait' relating to Covid-19 related matters. In other words, whilst Covid-19 has been a practical, *specific* example of why good operational resilience is important, it highlights that operational resilience measures are a prerequisite to ensuring the continued functioning of an organisation, following an incident or event, and that the pandemic in itself should not radically alter the general approach to managing resilience. Achieving the end outcome of operational resilience, and recognising the existing measures in place, should both be kept in mind when considering any additional or further guidance that policy makers may wish to pursue in the wake of the analysis of the impact of the pandemic.

If you have any further questions, or wish to follow-up on our contribution, the WFE remains at your disposal. Please contact:

Jonathan Pallant: jpallant@world-exchanges.org
Richard Metcalfe: rmetcalfe@world-exchanges.org

[2] The World Federation of Exchanges publishes update on industry cyber efforts during the pandemic, WFE, May 2020
[3] Business Continuity Planning at Resilient Market Infrastructures, WFE, March 2020
[4] A well-functioning exchange is one that facilitates continuous trading in securities and derivatives, and which provides for the transfer of risk and maximises the incorporation of new information in the value of financial instruments. This foundation allows market participants to make informed choices placing their orders; confident that executed trades will then be cleared and settled.
[5] Stock market was not closed. It was not possible to open it, Interview with Sri Lankan Securities and Exchange Commission (SEC) Chairman Viraj Dayaratne, Daily Mirror Sri Lanka, May 2020

Overview

The WFE welcomes the onus being placed on the importance of operational resilience within the financial services ecosystem. In a pandemic environment with market volatility and atypical operational practices, it is only natural that there will be growing scrutiny on the prevention, response and recovery of financial services to operational failures. It is essential that financial services firms seek to protect their ability to serve their customers – thereby avoiding disruption to the wider economy. To this end, the WFE has sought to assist the sector in convening and conveying the work they are already doing, and are continually enhancing, in this space through working groups consisting of specialist risk management experts from market infrastructures around the world.

These working groups are dedicated to generating best practices and benchmarking the sector, in order to raise standards for the industry as a whole, as well as addressing specific operational resilience threats – for example, sharing cyber threat intelligence related to common risks. Addressing operational resilience requires our members to confront those common threats that could affect any one of them and the safe and efficient operation of the systems they run as critical national infrastructures. As a result, it is appropriate that entities work collectively on such issues, in order to best harness the expertise and perspectives available across the WFE membership, in combating these challenges and the threats they pose to global financial stability.

In seeking to enhance the operational resilience of financial services firms, the WFE would encourage the UK regulatory authorities and international standards-setting bodies (ISSBs) to consider operational resilience in terms of the whole ecosystem, rather than just firm by firm or sector by sector. Operational risks, while not necessarily generating financial loss, do have the potential to inflict serious service-delivery issues right across the financial services sectors and are rarely siloed incidents. The Covid-19 pandemic is a case in point. Whilst this is undoubtedly an objective supervisory authorities are seeking to address, the WFE recommends that a broader 'bird's eye' perspective should be considered, within reasonable expectations, with supervisory authorities preparing, testing and regulating the whole financial services community to ascertain how resilient they are as an eco-system, given their interconnectedness and common exposures.

It is important that any proposed operational resilience framework can be implemented, or is compatible (as far as possible), globally and by all sectors in the ecosystem. Such an approach would also help to avoid inadvertent fragmentation and needless differing/conflicting regulatory expectations and requirements applying in different jurisdictions. To ensure these aims, the WFE encourages the UK supervisory authorities to continue to co-ordinate with their peers across jurisdictions and the ISSBs, as well as with their public and private sector stakeholders, to enable a globally coordinated and consistent approach. Ensuring that the proposals are informed by and aligned with important international guidance that has emerged since the publication of the Bank/FCA's consultation should be given particular consideration, eg IOSCO's *Principles on Outsourcing*. A harmonised and coherent approach is particularly relevant for future operational resilience initiatives, given the potential for additional jurisdiction specific legislation and regulatory requirements to emerge in response to the pandemic. Conflicting practices risk regulated entities needing to implement multiple sets of requirements, adding to the risk of confusion and inefficient implementation (especially when the pandemic threat is still live).

The role of appropriate regulatory deference in laws and rules related to operational resilience is worthy of careful consideration. The UK supervisory authorities are among the first to progress specific operational resilience requirements. However, the proposals include thorough, resource intensive work to be undertaken to satisfy the requirements outlined. Further, if each national jurisdiction were to make analogous requirements for slightly differentiated work, to achieve similar outcomes, the result would be unduly burdensome for globally active firms.

Therefore, we believe consideration ought to be given to how these requirements might operate in terms of deference and mutual recognition for cross-border arrangements.

A common lexicon is also important so that there is consistent agreement on the foundational aspects of operational resilience. There are existing potential discrepancies in the use of terminology between key supervisory authorities. For example, there have already been differences in the use of terminology from the Monetary Authority of Singapore and UK regulators' definition of 'business services'. This type of conflicting terminology could cause additional confusion and artificial barriers in cross-border trading and in the understanding and implementation of operational resilience requirements. Where possible, the adoption of terminology defined by the ISSBs may assist in addressing this and provide greater commonality. Ensuring commonality in terminology also naturally benefits and supports efforts for achieving, and the use of, appropriate regulatory deference and mutual recognition.

The WFE also believe that in general, the proposals should not only follow the *do no harm principle* but also follow a *rapid but safe principle,* so that, for example, in relation to recovery-time objectives, firms are not incentivised to bring up services and systems within impact tolerances at the expense of market contagion. Risk to the industry should be minimised through careful actions that are dependent on the facts and circumstances of the event.

With these points in mind, the WFE is broadly supportive of the overarching objectives and outcomes-based approach of the proposals outlined by the Bank of England/PRA/FCA, as reflected in our 2018 response to the Bank's consultation. In responding to the consultation, there are key areas around scenarios, recovery time objectives, testing and (the management of) outsourcing that members of the WFE would seek to highlight in reacting to the latest proposals.

Specific Commentary

Severe/Extreme but Plausible Scenarios

The continuous learning[6] that market infrastructures undertake in relation to types of operational risk reflects the fact that threats are continuously evolving. To have static requirements for ostensibly static threats undermines this learning. The proposals by the Bank of England[7], PRA and FCA[8] are an example of the more outcomes-focused design of regulation (in its stated broad ambition), which is welcome. We welcome, for example, the statement that: "It's the resilience outcome that's most important to the supervisory authorities, not simply a firm's ability to demonstrate compliance"[9].

In discussing the importance of considering the scenarios that may affect operational resilience and a firm's ability to remain within its 'impact tolerances', it is important that there is commonality in approach, whilst being tailored in certain details, to reflect the needs/services provided by each organisation. It is noteworthy that the proposals include the requirement for an organisation to give consideration to 'extreme but plausible' scenarios. Without specified parameters, there is the potential for organisations which offer the same or similar services, and conduct the same or similar operations, to have great disparity in the scope of those scenarios, and the associated testing. In paragraph 4.9 of *Building Operational Resilience: Impact tolerances for important business services* paper[10], it is stated that firms and FMIs should consider failures within their control as well as those outside of their control. Whilst that remains an important set of considerations, there is a potential danger that a regulatory requirement to consider such scenarios on the basis of mere 'plausibility' could lead to the aforementioned disparate set of scenarios and associated planning for those scenarios. This could give rise to an unclear picture of the positioning of firms' general operational resilience for such scenarios, as well as a distorted and confused picture of what that resilience looks like across the financial services ecosystem as a whole. In line with the concept of principles and outcomes-based regulatory oversight, developing incident and crisis management *abilities* may be a better solution. In other words, it is the process and capability that matters most.

In light of the pandemic, with market volatility and atypical operating practices, it is apparent that incident and crisis management *capability*[11] is key. Working on the premise that it is counterproductive to assume that every eventuality can be identified in advance, there needs to be an acceptance that, on occasion (hopefully rare occasion), something will fail and that, while planning and testing for identified scenarios clearly remains valuable, so are procedures for detecting and reacting to new contingencies.

From a practical perspective, failures are more straightforward to plan for and recover from (eg, using contingency network equipment, parallel utilities services, secondary data centres). The real challenge for incident management is, arguably, partial failure or service degradation where teams are dealing with novel (or previously unknown) issues with only partial or emerging information. It is in these situations that an organisation's incident response capability

[6] BIS-IOSCO, Guidance on cyber resilience for financial market infrastructures, June 2016
[7] BoE, Bank of England Consultation papers: Operational Resilience of FMIs, December 2019
[8] FCA, Building operational resilience: impact tolerances for important business services and feedback to DP18/04, December 2019
[9] Speech by Megan Butler, Executive Director of Supervision: Investment, Wholesale and Specialist, The view from the regulator on Operational Resilience, December 2019
[10] Paragraph 4.9 of the BoE, PRA, FCA, Building Operational Resilience: Impact tolerances for important business services paper, 2019
[11] "Effective crisis management extends beyond preparing for any specific event to development of broad, flexible capabilities that enable response to a wide range of events along various dimensions". Cyber crisis management: Readiness, response, and recovery, Deloitte 2016

proves itself. Rather than dealing only with that which is known, the incident teams need the ability to triage and address unknowns – in effect, the ability to rapidly, and as efficiently as possible, manage any such scenario. This is crucial from a business resilience perspective and potentially more so than the more obvious 'failover' scenarios. Greater emphasis could, instead, be focused on understanding how firms are setup to respond, and how entities consider and determine their approach, to novel risk management to achieve the end outcome of operational resilience.

Service Performance Metrics and Inter-dependencies

We believe the papers could potentially go further to require the establishment of service-failure criteria. This is linked to the regrettably confused discussion of what constitutes fair and orderly markets that took place during the height of volatility experienced as a result of the pandemic. It is crucial, for example, to understand where a service is degraded but still operating. At a certain point a decision needs to be made that a service has been impaired to the point of failure (or 'failover'). In the context of exchanges and CCPs, there are important questions over how these critical services are linked to each other and the point at which service degradation and/or failure feeds into the market suspension criteria and decision point. For instance, the consequences of a failure in a market infrastructure's equity/cash market and the potential implications on the derivatives market or the degradation and/or failure of electronic disclosure services and how that impacts markets given the requirement for maintaining 'fair and orderly' markets. So, given the inter-connectedness between critical services, it is not just outage, but also service degradation thresholds which are relevant, and indeed could be more prominently discussed in these papers/requirements.

As alluded to, this recommendation should not be confused with some of the inaccurate discussions around 'fair and orderly' markets which appeared in some quarters during the pandemic. The surge in pandemic-related volatility provoked some public discussion about the meaning of fair and orderly markets. When investors and issuers of securities see steep declines in the value of assets, it is understandable that they should closely monitor the effectiveness of the price-formation process. However, falling (or, rapidly rising and falling) asset prices do not imply a lack of integrity in the market on which those assets are traded and the WFE welcomed the publicly stated approach that the FCA took in relation to the market volatility witnessed earlier in the year and the judicious approach to short-selling bans, for instance.

Recovery Time Objective (RTO)

The WFE welcomes the recognition[12] that there are incidents in which the resumption of the provision of an 'important business service' should *not* be conducted, because further risk or issues would be introduced to the system or marketplace. In particular, the supervisory authorities' desire not to create 'perverse incentives' and enabling firms and FMI to consider the "particular circumstances of a disruption" to influence whether it is "appropriate to exceed their impact tolerances" is an important inclusion. We support this nuanced approach to the resumption of important business services – the same considerations, in seeking to avoid perverse incentives, should be recognised in the application of EMIR[13] and its requirements for critical business functions.

To expand on why this is a concern, it is important to consider that the CPMI-IOSCO *Principles for Financial Market Infrastructures* express a 2-hour RTO as guidance. Guidance works well under operational disaster-recovery plans.

[12] Paragraph 4.7, Ibid.
[13] Article 17 (6) of RTS 153/2013

However, we believe that mandating a hard recovery time, as required under EMIR, for extreme scenarios is counterproductive. While we recognise and support the intention behind a 2-hour target, we remain convinced that there needs to be some flexibility, to take into account particular facts and circumstances – in the same manner recognised in the Bank/FCA proposals regarding important business services. In the wake of a cyber incident, for instance, firms may find themselves stretched between a commitment to deliver availability for customers, completing a thorough investigation of the extent of the compromise, and ensuring the integrity of seemingly untouched systems. In an ecosystem of interconnected entities, the risk of contagion should not be underestimated. Mandating a 2-hour recovery runs the risk of inadvertently creating the wrong incentives for the resumption of operations, at the expense of due diligence over data completeness, accuracy and validity, therefore risking contagion to other firms and potentially even causing a systemic event.

Mapping and Testing - Outsourcing/Use of Third-Party Service Providers

Referenced within the papers are proposals around outsourcing and the impact of third-party service providers. Whilst covered elsewhere in the PRA paper, the WFE would like to submit its views about some of the proposals being made, given the potential scope of firms who may be subject to the requirements both now or in the future.

The WFE recognises that there is growing use of third-party providers by market infrastructures. This is often to improve efficiencies, to reduce exposures via specialist/expert providers, to better serve customers by employing new technologies provided by third-parties and to enable service provision which would not otherwise be feasible or viable. Often the reasoning behind the use of third-parties is to address those objectives that this consultation is seeking to address – ie, updating infrastructure with new solutions to make it more resilient and/or efficient and effective. It is, of course, only right that appropriate governance arrangements should be placed around the use of such providers and this remains a priority for the WFE's membership.

It is also widely understood that where a third-party is providing a 'critical or important operational function'[14] , on which an organisation is in practice reliant, that there are appropriate due diligence and governance arrangements in place. However, it might not be possible for a regulated entity to test the response of a third-party provider to severe/extreme but plausible scenarios. This is not to advocate the notion of 'outsourcing your responsibilities' but rather to flag that there is potentially a heavy resource implication associated with such additional legal contractual requirements needing to be embedded for the testing processes and the audit. These may be sizeable and may have implications for the firms in the aggregate cost benefit analysis. The use of 'pooled audit', for example, may lower the operational overhead experienced by these providers (especially for firms with many counterparties or clients).

There may also be cross-border implications resulting from rules or restrictions imposed by a host country or host country regulator. For example, it may not be possible or advisable for on-site audits to be conducted at the third-party and there may be instances where certain reports include confidential supervisory information that could not be shared externally without approval. Where a vendor is regulated (either directly or as part of a corporate family), information necessary to evaluate the third-party should also be permitted to come from the vendor's home country regulator. This may be particularly relevant following the experiences between firms and their vendors over the pandemic, where there is an extent to which an individual firm is necessarily limited in how it can oversee its third-parties and be privy to all apposite information. For instance, this may have arisen when on-site inspections could not occur due to social-distancing restrictions and remote working arrangements. A supplementary approach to issues concerning the testing of multiple vendors and managing extreme scenarios may be to give greater focus

[14] PRA, Consultation Paper, CP30/19 *Outsourcing and third-party risk management, 2019*

(whilst recognising its existing inclusion in the proposals) to ensuring that the contingency planning process incorporates appropriate exit strategies as outlined and in harmony with international standard-setting bodies.

The proposed use of 'outsourcing registers' gives rise to concerns about the potential concentration of information in a 'single point of vulnerability'; and how the application of the 'registered providers' would operate – extending from the recommendations and requirements detailed under the EBA's paper[15]. In addition to the risks that could be incurred by a single, large scale data loss event, vendor contracts typically prohibit sharing information about the nature of their relationship outside the two parties. There may also be cross-border implications resulting from data privacy rules or other restrictions imposed by a host country or host country regulator.

[15] EBA, Final Report EBA Guidelines on outsourcing arrangements, 2019