WORLD FEDERATION OF EXCHANGES

WFE Response to the EU Commission's Proposals for Digital Operational Resilience for the Financial Sector (DORA)

February 2021

www.world-exchanges.org

Introduction

We are grateful for the opportunity to respond to the EU Commission's Proposals for Digital Operational Resilience for the Financial Sector (DORA).

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.

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

Overview

The WFE welcomes the ambition and overarching objective of the EU Commission in seeking to harmonise operational resilience requirements and to extend the application of those rules across a greater number of financial entities, especially those operating in new digital-based environments.

The WFE believes that principles, guidance or regulatory requirements, relating to issues such as operational resilience should be all-encompassing of the whole financial services industry rather than aimed at individual sectors within it; and, where possible, guided by international standard-setting bodies (ISSB). To that end, the WFE supports the EU's ambition of 'levelling-up' the financial ecosystem, as such an approach has clear benefits in terms of reducing the risk of there being a weak link in the chain from end-investor to central market infrastructure.

Market infrastructures have embedded advanced enterprise and operational risk management across their organisations, with measures which are tailored to deliver on the rigorous requirements and regulatory expectations (eg, stress testing on a regular basis) that apply to them as national and international 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] that outlined the organisational structures and practices that are being employed – including the creation of dedicated in-house teams focused on developing and delivering high standards of operational resilience.

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

Specific Commentary

Definitions and use of ICT third-party service providers established in a third-country

It is equally important that a 'tailored' and proportionate approach is proposed in the application of regulation across financial entities and ICT service providers to ensure that those requirements can be met and that they deliver enhanced resilience from their implementation. The WFE represents a number of exchanges who are market data service providers (MDSPs), as well as providing other associated data tools and services.

Those market infrastructures could potentially be included under the definitions and criteria employed to categorise 'ICT third-party service providers' (Article 3 (15)), given the reference to data services[2]. They may also be classed as a 'critical ICT third-party service provider' (Article 3 (18)). However, as those services are not "material outsourcing", they are, in our view, out of the scope of the definition.

The WFE is concerned that, should MDSPs fall, by default or otherwise, into such a category, they would be unfairly and inappropriately subject to the most severe aspects of the requirements and restrictions imposed by the new legislation. This is with particular reference to proposals to prohibit (under Article 28 (9)) the use of an 'ICT third-party service provider established in a third country' (Article 3 (19), if deemed 'critical' under Article 28(2)). The WFE requests greater clarity on the definition of 'critical ICT third-party service provider' to understand exactly what the proposal is seeking to capture.

Under its current guise, the criteria (and subsequent restrictions) appear to be too broad and sweeping in scope and would be disproportionate to the actual risk profile of many of those captured under the proposed definition. Even where not deemed 'critical', application of the proposals, including the imposition of contractual clauses and onsite inspection rights, may be inappropriate or prohibitive to third-country providers (as further addressed later in this response). Indeed, the extension of the prohibition to the use of ICT sub-contractors established in a third-country where the sub-contracting 'concerns a critical or important function of the financial entity' (Article 31(IV)) may also create unnecessary and disproportionate obstructions to firms using certain ICT service providers.

The WFE recognises the Commission's desire to ensure accountability and to have appropriate oversight capabilities. However, greater specificity concerning the ICT service providers which would be captured (regarding the definitions employed, especially those deemed 'critical') is required for the proposals to be properly understood in terms of their potential impact. For example, also providing the exact meaning of what constitutes a 'business/presence in the Union', in relation to ICT third-party service providers, would be beneficial in resolving ambiguity and potentially enabling a better understanding of whether the requirements of the Commission can be met[3].

Reducing access to MDSPs and other aspects of ICT service provision could, in this context, unfairly and unnecessarily promote market fragmentation; with improving the efficiency of markets, reducing risk and consumer choice affected by the proposals. In an age in which the ambitions of the Capital Markets Union can be promoted and achieved through harnessing the best service provision available to EU firms, deliberately creating barriers could be at odds with realising that goal.

[2] ICT services defined under Article 3 (16), "including provision of data, data entry, data storage, data processing and reporting services, data monitoring as well as data based business and decision support services".

[3] Eg if the requirement is for a 'legal construct' to be established within the Union in order not to be classed as a 'third-country provider', what the detailed expectation of the European Commission is for that construct.

Avoiding unnecessary and disproportionate restrictions to access such service provision is integral to encouraging cross-border trade and promoting the EU as a business-friendly environment with safe and efficient markets. Markets are increasingly global and regulatory architecture and practices should reflect this fact in a manner that supports the objectives of economic policy and financial supervision. We believe society derives significant benefits from integrated financial markets. It is therefore important to have strong common principles and co-ordinating mechanisms to promote financial integration and market integrity. This is fundamental to well-functioning and safe markets at local and global levels. We believe that the G20-endorsed approach of regulatory deference should be a guiding principle in the area of cross-border supervision.

Concentration risk

It is understandable that avoiding concentration risk and enabling greater scrutiny of critical (third-party) ICT service providers is desired by the EU. However, prohibiting access to third-country providers may instead create more risk and reduce the resilience of EU firms. ICT third-party service providers often provide specialist software or infrastructure that has been tested and developed to a much greater degree than individual firms would be able to replicate for 'in-house' purposes. Outsourcing, or employing third-parties, in this context, can reduce risk for firms and instead enable access to expertise and levels of resilience that would not otherwise be available to them. Given the 'niche', highly specialised services that market infrastructure (or other elements of the financial services ecosystem) can require, there is often limited service provision that can meet the stringent high standards of resiliency that market infrastructure demands of the third-party service providers they employ. By reducing access to that list of service providers, greater concentration risk could occur and less tested and robust service providers might instead be used, out of a lack of choice rather than on the basis of resiliency, suitability and merit.

The WFE is conscious of the challenges in striking a balance that enables firms to safely employ third-party, critical, ICT service providers and enabling strong and effective supervision to take place to ensure financial stability of the Union and the Member States. However, we believe that instead of prohibition of such services, other tools and requirements could be selected, under the guidance of international standard-setting bodies[4]. This would enable ICT service providers to provide those services across borders in a safe and resilient manner. This approach also avoids unintentionally impeding the options for firms to harness the most resilient and safe service providers, whilst enabling regulatory coherence.

Data localisation (Restrictions)

The WFE would also highlight the potential for the proposals to inadvertently create data localisation requirements. This could arise due to data centres not established in the EU (classed as 'ICT third-country service providers') being unable to meet requirements such as on-site inspections of premises. They may even be totally prohibited from providing services if deemed to be a 'critical' ICT service provider established in a third-country. By requiring critical ICT service providers to establish a local entity in the EU, or without appropriate measures to enable third-country providers to meet the requirements, this would in effect introduce data localisation. Aside from the negative impact of such a policy in terms of additional resource implications and reduction of choice, it could also potentially propel international market fragmentation, with similar approaches developing from other jurisdictions to data matters.

[4] Eg, IOSCO, Principles on Outsourcing, May 2020

Proportionate requirements

Aspects of DORA appear prescriptive and disproportionate to the risk (with the associated unnecessarily burdensome implications for resources) in its proposed application of the requirements. For example, Article 7 (*Identification)*, outlines a series of measures, relating to identification, documentation, risk assessments and mapping – which would apply to *all* ICT assets, processes and third-parties. DORA Articles also extend onerous mandatory measures across incident reporting, prevention and protection requirements, contractual arrangements, testing and a number of other areas, without any nuancing for the risks posed in actuality or the specific scenario. Instead, especially given the breadth of entities and providers captured by the proposed definitions, the WFE would support enabling an approach that follows the principle of proportionality in the application of the proposals, and which accommodates a more enhanced risk and outcomes-based approach across the board (as touched upon in paragraph 46 of the introduction of DORA and in some other Articles). For instance, the extent of the depth to which the application of the measures in Article 7 is required could be aligned with whether their application relates to ICT assets, processes, third-party services or functions that deliver (or support the delivery of) regulated activities by a financial entity (ie, reflecting the degree of criticality or dependency of the ICT systems or providers to the financial entity's operation of its critical functions).

Another example would be when dealing with a third-party service *provider* that is a regulated entity (eg, an exchange, CCP, trade repository, a data reporting service provider, an index provider, benchmark administrator, investment firm or a CSD). In this situation, the provision of regulated services ought not to fall within the scope of third-party regulatory oversight requirements — irrespective of whether the provision of that specific *activity* requires explicit authorisation. This approach should also apply when the provision of that activity could be performed by the regulated entity itself. Such dedicated service providers are subject to supervision by regulators and therefore do not pose risks comparable to the use of third-parties/outsourcing to unregulated service providers. It would be unrealistic for financial institutions to conduct comprehensive oversight of such regulated entities, especially where they are a necessary part of a regulated value chain (sometimes under other regulatory requirements).

Alignment with international standards and enabling appropriate deference

Further, many firms that will fall within the proposed scope of DORA are already subject to other regulation relating to operational resilience (inclusive of cybersecurity), whether within or outside the EU. We encourage the Commission to further consider overlapping requirements, including the role of international standards (eg, ICO or NIST cyber security framework) and international guidance (eg, IOSCO Principles on Outsourcing, 2020) and national regulatory requirements (eg, Bank of England Operational Resilience proposals, 2019) in other (home) jurisdictions for those firms. The Commission may also want to consider how it enables suitable flexibility in its proposal to accommodate future guidance from the international standard-setters. For example, the FSB is due to consider "the scope for convergence in the regulatory reporting of cyber incidents and the need for revisions to the FSB Cyber Lexicon" as part of its 2021 work programme[5]. This exercise would help to identify where the EU's proposals may differ from international norms and necessitate clear reasoning to be outlined behind adopting a different approach. It would also encourage further alignment of the proposals with those existing regulations.

In order to pave the way to regulatory deference, it is important to have an efficient and proportionate process for recognising where third-country jurisdictions have legal regimes and market structures and practices that, while different in some respects from those of the EU, are consistent with internationally agreed standards and core

[5] FSB, 2021 work programme, January 2021

principles of 'DORA'. We recommend that formal arrangements are instead brought forward to enable sharing of information and co-operation between third-countries to facilitate the evaluation of ICT service providers established outside of the EU. When evaluating the comparable compliance processes more broadly, the WFE would encourage the EU to adhere more closely to the principle of regulatory deference by taking a truly outcomes-based approach, as opposed to line-by-line, requirement-by-requirement, and determine if requirements between jurisdictions are instead comparable (ie, similar). 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 or potentially conflicting rules, and therefore impacting implementation.

Achieving a common, outcomes-focused approach, via mutual recognition or other forms of deference (as far as possible, whilst recognising that local authorities are most familiar with the unique characteristics of the firms they supervise and the legal framework under which they operate), should obviate an uncoordinated regulatory environment developing but with appropriate accountability remaining with market infrastructures as regulated financial institutions.

Entity and group application

The WFE would also commend the notion of enabling a group-wide approach to meeting the proposed requirements, where it is appropriate. Often operational resilience and security standards are set centrally by reference to many existing legal and regulatory requirements, security standards and guidance. Similarly, risk assessments are typically undertaken centrally, with firms applying a holistic view of risk across their operations. If DORA is interpreted as being applicable to individual legal entities within the same group, with the accompanying delineated processes needing to be undertaken separately for each entity, this potentially could *de*-crease resilience and security by increasing complexity and driving a fragmentation of requirements.

Third-party contracts

In relation to contractual arrangements with ICT third-party service providers, DORA necessitates the mandatory termination of contracts in particular circumstances (Article 25 (8)). Mandating the requirement to terminate contracts in specific situations may not only be inappropriately inflexible for financial entities to navigate whatever the scenario in which the ICT third-party service provider might be operating, but may also have significant consequences in terms of creating operational risk. More broadly, the contractual requirements should be aligned with existing European Supervisory Authorities' (ESAs) positions on contractual requirements and with the guidance of international standard-setting bodies.

Many service providers, especially for cloud-based services, will also only offer a "one-to-many" service model, meaning service is provided in the same way to many different customers. As a result, service providers generally offer the same or substantially similar contract terms to those different customers without the flexibility to have bespoke arrangements. In addition, many requirements – particularly technical, operational, and functional requirements – are not addressed in the terms of the contract, but in the service provider's policies and procedures, third-party audits, certifications, and governance practices. Thus, a financial entity must consider and address the elements of third-party service provision/outsourcing not only by way of the contract with the service provider, but also through a review of those policies, and procedures, third-party audits, etc.... For example, a firm may decide not to outsource certain obligations related to records management or encryption-key management. In these situations,

the written legal agreement would not directly address those functions, as required in a single contract (Article 27 (1)), though, importantly, it would remain the regulated entity's responsibility to explain its arrangements to competent authorities.

Recovery time objectives

Separately, the WFE also welcomes the nuanced approach, indicated in the proposals, to the application of set recovery-time objectives (RTOs) and would encourage the Commission, and in turn the ESAs, to consider a formal change to the more prescriptive requirements for RTOs pertaining to EMIR. Given the constant threat posed by cyber attackers, accelerating such a change would be particularly welcome and supportive for market infrastructure operators.

To expand on that point, we believe that mandating a hard recovery time is counterproductive. While we recognise and support the intention behind a 2-hour target[6], we remain convinced that there needs to be some flexibility, to take into account particular facts and circumstances – in the same manner recognised by the Commission in attributing greater autonomy to the financial entity to determine its recovery time objectives (paragraph 41 of the introduction). In the wake of a cyber incident, for instance, firms may find themselves conflicted 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 recovery time 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.

[6] CPMI-IOSCO, Principles for Financial Market Infrastructures, 2012