FESE Position Paper on the proposal for a Digital Operational Resilience (DORA) Regulation

Brussels, 14th December 2020

FESE fully supports the work of European regulators aimed at making Europe fit for the digital age and developing a harmonised regulatory regime. Exchanges play an important role in supporting the stability of the financial system and are taking several measures to build upon their cyber resilience to protect their systems.

We welcome the recent proposal, by the European Commission, for a Regulation on Digital Operational Resilience for the Financial Sector (DORA). We believe that the new regulatory framework should be structured along the following lines.

Clarity on compliance with other Regulations/Directives

Compliance with the existing sectoral/horizontal legislation, such as the Network and Information Security (NIS) Directive, European Critical Infrastructure Directive, MiFID II/R, CSDR, and GDPR, has increased cyber resilience measures across the financial sector. However, the inclusion of digital operational resilience and/or cyber resilience in most recent legislative measures has led to a cumulation of requirements.

We support the move to use DORA as the reference legislation for ICT security for the financial sector and, therefore, welcome recital 16 which recognises that DORA constitutes *lex specialis* to the NIS Directive. However, we would recommend consistency when streamlining all files. It is important to harmonise these two legislations, *inter alia* the classification of incidents to avoid further duplication of efforts upon compliance and reporting.

In addition, many of these legislative frameworks are rather high level. The proposed Regulation should ensure that the goals of innovation friendliness and security are achieved without conflict between them. Companies might otherwise struggle to comply with the rules.

Flexible and proportionate measures

In general, FESE would caution against overly prescriptive technological measures which would rapidly be outdated due to technological evolution. While there is a need for a coordinated approach on cyber-resilience, when considering further regulatory requirements in this space it is important that flexible innovation is safeguarded, as “one-size-does not fit-all”. Hence a risk-based and proportionate approach is needed. With respect to the level of resilience, we would support a clear European framework on the measures to be taken.

Any requirement to disclose details on cyber resilience should be conducted carefully. A potential approach should be sufficiently broad to encompass multiple cyber risks, avoid recommending technology-specific parameters. Nevertheless, compliance with some sectoral requirements can be challenging, as these are formulated in an excessively broad language, especially when several European and national supervisors are involved. More detailed, but not technology-prescriptive, requirements would be helpful from an operational perspective and would foster supervisory convergence by creating a clear baseline framework.

The size of a financial entity should not be the most relevant metric when determining what cybersecurity requirements ought to apply. Rather, entities should be subject to similar requirements if they have similar risk profiles, including their systemic impact, and whether they conduct similar activities.

Regulatory alignment with global standards would also be valuable. Currently, several industry-led initiatives and solutions work through sharing experiences, cooperating, and collaborating with industry groups. Any proposed security risk management framework should be based on internationally developed standards (e.g. the National Institute of Standards and Technology Cybersecurity Framework (CSF)). Against this background, we would support an approach where certified measures are deemed to be sufficient. That way, a clear harmonised baseline would be defined, acknowledging state of the art internationally agreed solutions, thereby improving the overall level of resilience. Also, acknowledging certified measures as being compliant would set a clear level of expectation for both industry and competent authorities, and would promote a harmonised cross border approach. This would, in turn, allow room for technology to innovate and develop, regardless of regulatory requirements becoming outdated.

Open to third-party service providers

We would caution against setting excessively burdensome requirements for the sub-outsourcing provisions for third countries providers, as is the case currently (Art. 31(1)(iv)). The current wording allows financial entities to outsource critical functions to ICT providers only if these would not further sub-outsource to providers not located in the EU. We would like to flag, however, that in today's practice, financial entities use third-country service providers as a common practice. Further, Art. 26(2) mandates financial entities to assess whether and how complex chains of sub-contracting may impact their ability to fully monitor the contracted functions, and the ability of competent authorities to effectively supervise the financial entity in that respect. We would suggest deleting this requirement as operationally it would not be possible to implement it.

Balanced measures for Cloud Services Providers

Cloud services are becoming increasingly important for exchanges. While we acknowledge the limited offer of EU Cloud Services Providers (CSPs), we believe that to favour innovation it is crucial that the EU market remains open to non-EU CSPs.

We would like to stress the current asymmetries of power in negotiation between customer and CSPs, i.e. the extraordinary efforts and time required to agree on regulatory compliant contracts with CSPs in the financial sector. Therefore, we actively support the EU´s work to design "Voluntary Standard Contract Clauses" to facilitate future negotiations (as mentioned in recital 55 and Art. 27). Compliance to the General Data Protection Regulation (GDPR) by ICT-third party service providers or sub-contractors should be mentioned as a requirement in the Key Contractual provisions (Art.27).

Also, it is still problematic to procure/adopt new and innovative cloud solutions as it takes a long time to ensure that these new services are regulatory compliant. Some provisions for CSPs might be too prescriptive and would inevitably lead to regulatory obstacles for these companies. Policymakers should carefully balance obligations, especially for third country CSPs.

Adequate testing and reporting requirements

Financial Markets Infrastructures (FMIs) are subject to strict and detailed incident reporting requirements, which are mandated by their primary regulator in the jurisdiction they operate in. This regime has been in place for many years and has worked well so far. Changing the approach to create a centralised reporting structure, while seemingly an attractive option because of the uniformity, might, in reality, introduce issues due to lack of familiarity with and understanding of local markets. Primary financial regulators should remain responsible for FMIs in the jurisdiction they operate in.

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

We agree that templates and formats need to be harmonised and support the approach taken in Art. 18. Furthermore, regulators across multiple jurisdictions should work to harmonise their testing requirements (such as threat-led penetration testing), and then develop principles and requirements that firms should meet when conducting such tests. It should be left to the firms to conduct the tests, whereas regulators should ensure that their principles are met and that findings are remediated promptly, without having to be involved in every phase of the testing. As local authorities should remain close to market participants, we support the proposal to report incidents on a local level.

Overall, the EU should have clear, resilient, and proportionate ICT cybersecurity rules. FESE fully supports the objective of DORA to deliver this outcome with the suggestions outlined above. We remain committed to finding a workable framework which would suit both the industry and supervisors.

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80