European Association of CCP Clearing Houses

EACH views on the European Commission's proposal on digital operational resilience for the financial sector (DORA)

December 2020

Introduction

The European Association of CCP Clearing Houses (EACH) represents the interests of Central Counterparties (CCPs) in Europe since 1992. CCPs are financial market infrastructures that significantly contribute to safer, more efficient and transparent global financial markets. EACH currently has 19 Members from 15 different European countries. EACH is registered in the European Union Transparency Register with number 36897011311-96.

With this note, we would like to express our views on the Proposal on digital operational resilience for the financial sector ("DORA")[1] that the European Commission published on 24th September 2020 as part of the Digital Finance Package.

EACH welcomes the European Commission's proposal's aim to further harmonize operational resilience rules and extend them to other financial entities and third-party providers to increase the resilience of the financial system as a whole. As highly regulated and supervised entities, European CCPs have acquired in-depth experience and practice in developing and applying risk management requirements, including to address operational and ICT risks.

We particularly welcome the broad principles established in this Regulation including those of proportionality and lex specialis, as well as the European Commission's intention to streamline reporting requirements and avoid overlaps. Overall, we find that the present proposal strikes the right balance between the necessity to preserve financial stability and financial innovation, and have made some further suggestions to support this goal.

Key points

Harmonization of Digital Operational Testing

We appreciate the European Commission's efforts in DORA Article 23 to harmonise the minimal requirements of advanced testing, e.g. requirements on periodicity of advanced tests

[1] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN

(three years), minimal coverage (critical functions) and other organisational requirements and requirements for testers.

However, we note that DORA does not specify the type of advanced testing that will be required from financial entities. Hence, we would encourage the European Commission to clarify that the DORA testing regime does not come *in addition* to and is not *independent from* the **requirements on advanced testing** included in the existing frameworks such as the TIBER-EU framework[2]. This would help avoiding any additional compliance costs that firms would incur as a consequence of having to fulfil duplicative requirements on testing. We believe that, ideally, DORA should state the requirements on how testing should be performed, and then it would be up to regulated entities to conduct the testing, with regulators having the right to review findings – if they wish to do so – and track remediation. This is what, for instance, the CFTC Systems Safeguards Regulation[3] mandates.

EACH would also welcome a clarification from the European Commission that a financial entity is allowed to perform thread lead penetration tests by itself, if certain criteria are met (e.g. Art 24 a) and b)). As financial entities' IT architectures are very heterogenous and sometimes very complex, it would be inefficient to rely solely on external service providers. Also, such requirements might not be possible to fulfil in every case, due to a lack of appropriate external providers. While we note that the European Commission's proposal does not exclude this possibility, a clarification that it is indeed allowed would provide more certainty.

In addition, we also encourage **cooperation with international regulatory authorities on harmonising requirements and guidance on advanced testing frameworks**, which would enable a smooth implementation for firms that operate different entities across borders and in different jurisdictions.

Scope of the proposal

As currently drafted, an intra-group relationship could be included into the scope of DORA and thereby be deemed a (critical) third-party provider. EACH would argue that **intra-group relationships should not be classified as third-party relationships for the purpose of the DORA requirements**. In an intra-group relationship, the economic interests are aligned and managed at group level; ultimately the shareholders are the same, thereby mitigating many risks that arise out of traditionally outsourcing relationship. Additionally, CCPs retain full responsibility, legal liability and accountability to the regulator for all tasks. Therefore, EACH would suggest that intra-group relationships should be excluded from the scope of DORA, when the majority of shareholders are the same.

Clarity on definition of critical services

EACH is of the opinion that the **designation of critical ICT third-party service providers** as specified within Article 28 is **not fully defined**. Article 28 indeed states that the ESAs, through

[2] TIBER-EU FRAMEWORK – How to implement the European framework for Threat Intelligence-based Ethical Red Teaming: https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

[3] CFTC System Safeguards Testing Requirements for Derivatives Clearing Organizations https://www.cftc.gov/sites/default/files/idc/groups/public/@newsroom/documents/file/federalregister121615b.pdf

the Joint Committee and upon recommendation from the Oversight Forum shall designate the ICT third-party service providers that are critical for financial entities, and such designation has to be based on a series of criteria, among which the "*number of global systemically important institutions (G-SIIs) or other systemically important institutions (O-SIIs) that rely on the respective ICT third-party service provider*". However, we believe that such definition is not precise enough and would request the Commission to provide clarifications.

Conditions on sub-sourcing in third countries

EACH appreciates that DORA foresees dedicated rules for "critical ICT third-party service provider" including cloud service providers (CSPs), which will lead to a more harmonized approach. This is an important step to mitigate national measures on outsourcing hindering the usage of this technology and the respective services.

However, **conditions on third-country service provisions**, including sub-outsourcing to CSPs established in third-countries, are **disproportionate and could hinder global operations**. A strict reading of Article 31(1)(iv) would mean financial entities cannot outsource any critical or important functions to ICT providers if they cannot ensure that the sub-contractor is *not* an ICT third-party service provider or an ICT sub-contractor established in a third-country. This is not proportional and would effectively rule out use of certain ICT service providers, including CSPs, for critical functions.

Flexibility on termination of contractual arrangements

The provisions of **Article 25.8 impose requirements on firms which terminate arrangements with their respective providers** in circumstances where there are "*material changes that affect the arrangement or the situation of the ICT third-party service provider*", as established in point 8(b), where the provider shows "*weaknesses in its overall ICT risk management*" as defined in point 8(c), or where "*the competent authority can no longer effectively supervise the financial entity*" as define in point 8(d).

EACH would recommend **providing some flexibility** to the regulated financial entities instead of mandating the termination requirements, as well as harmonising such requirements with the existing EBA Outsourcing Guidelines[4].

Requirements on copies of high-risk evidence

ICT third-party providers should not be obliged to let financial entities take copies of high risk evidence, but make these **available in a secure, non-proliferating way** (Article 27(2)h-i): for high risk evidence, e.g. non remedied vulnerabilities, ICT third-party providers have a legitimate interest to avoid clients making copies. However, ICT third-party providers should be obliged to make them available e.g. by means of a secure reading room that customers can access whenever required. Additionally, if authorities would see the need to inspect sites of CSPs, this would reduce the burden for financial entities to visit the CSPs themselves.

[4] EBA Guidelines on Outsourcing Arrangements: https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf

Back-up requirement

Art.11(3) requires that the backup system needs to be directly connected to the main system in order to, for example, replicate data. We believe that the **wording "operating environment different from main one" is very vague** and should be clarified in order for second geography/location from the same CSP to fulfil this requirement.

Penalties and measures on breaches

We would encourage the Commission to take into consideration the **proportionality of the breaches** before imposing some of the penalties and remedial measures that the competent authorities have the power to apply for breaches of the Regulation as per Article 44, e.g. the issue of "*public notices, including public statements indicating the identity of the natural or legal person and the nature of the breach*" (Article 44.4(e)).