High-Level Principles on the Implementation of the Digital Operational Resilience Act (DORA)

7th June 2024

The European Association of CCP Clearing Houses (EACH), the European Central Securities Depositories Association (ECSDA), and the Federation of European Securities Exchanges (FESE) (the Associations) fully support the objective of the Digital Operational Resilience Act (DORA) to deliver clear, resilient, and proportionate ICT cybersecurity rules. Following the recent European Supervisory Authorities' (ESAs) consultations on policy mandates under DORA, we would like to provide further suggestions on the DORA implementation. Financial Market Infrastructures (FMIs) play an important role in supporting the financial system's stability and are taking several measures to build upon their cyber resilience to protect their systems. We remain committed to contributing to a workable framework that is fit for purpose for both the industry and supervisors.

1. Proportionality

- DORA Recital (7) recognises a need for a proportional approach to strengthen the industry's digital resilience. It also needs to form the basis of the Level 2 approach. Based on the recent Level 2 draft requirements, we believe ESMA and the national competent authorities (NCAs) can better apply this principle for trading venues/CCPs/CSDs.
- An overly detailed approach by the ESAs in the Level 2 drafting – as shown in the batches of consultations published so far – would not only have a significant impact in terms of cost but would also significantly hamper the possibility of complying with all such requirements within the expected deadline.
- For example, the requirements for external testers on thread-led penetration testing are too detailed, which makes them difficult to comply with in practice. Similarly, the expected level of monitoring by the financial entity of sub-outsourcing companies is too high, and we believe it will be challenging to implement. The draft RTS provisions will shift the burden of legal liability towards the financial entity, while currently the responsibility to honour the contractual requirements lies with the third party. It seems inappropriate to shift the legal responsibility of the subsidiary's actions to the parent undertaking.
- Overall, we would urge regulators to ensure that the volume of testing in DORA and other legislative requirements do not result in a constant testing in progress, diverting cyber teams from the need to address the risk of real events.
- Assessing the batches of consultations issued so far, the risk of over-reporting further undermines the Commission's objective to minimise the administrative reporting burden for relevant stakeholders, as recently underlined in the progress report on the EU Supervisory Data Strategy (here). For example, in the context of consultation on Draft RTS and ITS on major incident reporting under DORA[1], the list of data fields to be

[1] ESAs Consultation on RTS and ITS on content, format, timelines and procedures for reporting of major incidents and significant cyber threats under DORA, available here.

reported for the initial, intermediate and final reports is excessively burdensome and potentially counterproductive. Certain information, e.g., an assessment of the full impact of an incident on other entities and/or third-party providers, is likely unavailable at an early stage as requested in the consultation; providing premature information could subsequently be misleading.

2. Providing enough time for safe implementation

- Current publication schedules for DORA RTS and ITS may not allow financial entities adequate time to safely comply with DORA in January 2025 and might even decrease the level of cyber resilience in the financial sector. RTS/ITS clarify a significant number of the requirements under DORA. The ESAs will publish many of the final RTS/ITS only in the coming months and the Commission will adopt them shortly before the end of the year. This leaves the industry with very little time to adjust to the new requirements. In various instances, these RTS and ITS cover highly technical areas such as requirements related to cryptographic techniques. It is highly unlikely that financial entities will be able to safely make such technical changes in the short timelines allowed.
- It should also not be underestimated that detailed RTS requirements will lead to significant repapering/re-negotiating of ICT contracts with ICT third-party service providers (including subcontracting arrangements). DORA's aim to foster digital operational resilience might be severely compromised if ICT services of ICT third-party service providers cannot be provided by the beginning of 2025 as corresponding contractual arrangements have not been finalised in time. To guarantee safe implementation without disruption, the Commission and the ESAs should consider granting supervisory forbearance for the first months of application.

3. Clear transitioning from existing regulations to DORA

- As recognised in DORA Recital (102), with the application of the DORA Level 1 and 2 framework, redundant, equivalent, and/or obsolete sector-specific ICT risk management regulations and guidelines, such as the ESMA Guidelines on outsourcing to cloud service providers[2] or the EBA Recommendations on outsourcing to cloud service providers[3] should be repealed or reviewed. This supports the aim of building a flexible and proportionate common framework, which improves the resilience of the financial sector.
- Although DORA is categorised as *Lex Specialis* and would have primacy over other rules as in the case of the updated Network and Information Security Directive (NIS2), it would be necessary to delimit this prevalence in a more concise way (e.g., in cases such as incident reporting, DORA and NIS2 have different approaches both in their form and in the recipients of the reporting information). In our opinion, it would be necessary to clearly define the prevalence to avoid ambiguity and legal uncertainty.
- The ESAs' guidance on the supervisory approach is necessary to identify sector-specific rules that will be repealed and/or adapted. This is particularly relevant in the interim period where the industry is moving towards compliance with DORA and existing regulations and guidelines still apply. The industry needs guidance regarding the breaches and cases of non-compliance in the interim period and the potential regulatory actions from supervisors.

[2] ESMA Final Report on Guidelines on Outsourcing to Cloud Service Providers, available here.
[3] EBA Final Report on Recommendations on Outsourcing to Cloud Service Providers, available here.

4. Building upon existing practices to implement DORA

- It is important to build on existing registers, frameworks, and practices to ease the compliance burden. Imposing a one-size-fits-all approach would unnecessarily disrupt existing practices that already work properly.
- Firms will have different approaches to applying responsibilities across their business lines, depending on the corporate model in play. Therefore, uniformity across the industry should not be an objective in and of itself. Instead, entities should have the option to build on their existing practices, reviewing to what extent they need to be updated or adapted.
- For example, FMIs operate under a 2-hour Recovery Time Objective (RTO) guidance, as per CPMI-IOSCO Principles of Financial Market Infrastructure. The 2-hour RTO guidance works well under operational disaster recovery plans. Therefore, recommending additional prescriptive requirements related to RTO would be counterproductive as it may limit flexibility to adapt to new types of situations and cyber threats. Similarly, the RTS on thread-led penetration testing (TLPT) should sufficiently align with the existing TIBER-EU framework for threat intelligence-based ethical red-teaming.

5. Effective coordination among the ESAs and NCAs

- DORA introduces additional layers of coordination between financial sector supervisory authorities, both at the level of ESAs and NCAs. Clear, transparent, and effective arrangements among the ESAs and NCAs are needed for monitoring activities, strengthening the objective of supervisory convergence.
- While ensuring a common approach across the financial sector is the ultimate goal, this should not alter the timeliness and effectiveness of interactions between supervised entities with their own NCAs responsible for supervising trading, settlement and clearing.
- The DORA cross-functional approach should stimulate other forms of cooperation among different NCAs supervising financial entities in the scope of DORA. This is especially important for FMI groups that require a clear and coordinated supervisory approach applied to different entities in the same group.

6. Protection of sensitive business data

- Business-relevant data that is sensitive should be protected. The integrity and confidentiality of such information need adequate guarantees when shared between financial entities and the Lead Overseer.
- Some Level 2 draft requirements under the recent policy batches are too far-reaching and might undermine the principles of confidentiality. For example, the RTS on oversight harmonisation in Article 3(2)(f) requires ICT third-party providers to disclose meeting minutes. However, such minutes may contain sensitive business data and would therefore infringe on confidentiality.
- As outlined in Recital (9) of the RTS on TLPT, testing in a live environment poses significant risks such as denial-of-service incidents and unexpected system crashes. Beyond increased costs due to such testing, it might also lead to the loss and disclosure of sensitive information. As such, it is crucial to mitigate these risks during the DORA implementation.

About EACH

The European Association of CCP Clearing Houses (EACH) represents the interests of Central Counterparties Clearing Houses (CCPs) in Europe since 1992. EACH currently has 18 members from 14 different European countries and is registered in the European Union Transparency Register with number 36897011311-96. The list of EACH members is available here.

If you have any questions on EACH, please contact EACH Secretariat at info@eachccp.eu or +32(0)22061260.

About ECSDA

The European CSD Association represents 40 Central Securities Depositories (CSDs) headquartered in 36 countries across geographical Europe. In pursuit of an efficient and risk-averse infrastructure for European financial markets, the Association has as its ethos to provide a forum that aims to increase dialogue and intellectual exchange on common topics of interest among CSDs and relevant external stakeholders. For more information regarding the role and activities of ECSDA, we invite you to consult the following link.

About FESE

The Federation of European Securities Exchanges (FESE) represents 35 exchanges in equities, bonds, derivatives and commodities through 16 Full Members and 1 Affiliate Member from 30 countries.

At the end of April 2024, FESE members had 6,222 companies listed on their markets, of which 8% are foreign companies contributing towards European integration and providing broad and liquid access to Europe's capital markets. Many of our members also organise specialised markets that allow small and medium-sized companies across Europe to access capital markets; 2,021 companies were listed in these specialised markets/segments in equity, increasing choice for investors and issuers. Through their RM and MTF operations, FESE members are keen to support the European Commission's objective of creating a competitive and efficient Capital Markets Union.

For more information, visit www.fese.eu. Follow FESE on LinkedIn.