July 2024

Joint Statement on DORA

The financial services industry is committed to ensuring the digital operational resilience of the EU financial sector in line with DORA's objective to achieving and upholding ongoing compliance with DORA requirements.

It is within this context that the undersigned associations would like to draw attention to the challenges that industry participants, representing financial entities as well as ICT third-party service providers, are facing regarding the implementation of DORA by the 17 January 2025 deadline, and to highlight the need for coordinated supervisory action to be taken in response.

Industry would therefore appreciate further clarity from the supervisory authorities on their approach to any possible DORA enforcement actions. This could include an outline of potential supervisory priorities or areas of focus for the first year of DORA application, which would provide helpful guidance for industry participants on how to prioritize their efforts.

In addition, in order to provide guidance on ongoing compliance challenges, **we recommend ensuring a continuous and effective convergence among supervisory authorities during the implementation of DORA in the run-up to and after 17 January 2025. The working group which was set up for DORA implementation and brings several supervisory authorities together could be a helpful vehicle for this purpose** and could be used to establish a clear timetable and ensure coordination across Member States.[1]

AFME, EPIF, FIA, FIA EPTA, AmCham EU and UK AFB would welcome the opportunity to meet with relevant policymakers to discuss and further explain remaining issues ahead of DORA's implementation date.

DORA's comprehensive requirements necessitate significant changes to financial entities' risk management processes and adjustments to existing frameworks spanning multiple operational and technological domains within a firm.

[1] The importance of convergence among supervisory authorities is exemplified by the recent ECB consultation on outsourcing cloud services which may lead to possible fragmentation in the market.

Given the significant challenges regarding contract remediation, industry participants would also appreciate clarity from the regulators that applying a risk-based approach which prioritizes CIF (critical or important function) contracts with a plan to remediate other providers is acceptable to the regulators and would not trigger any supervisory enforcement measures.

These challenges relate to several key areas including:

1. **Contract management.** The required remediation of a potentially significant number of third-party contracts will not be achievable for many firms by the 17 January 2025 DORA implementation deadline. The final subcontracting technical standard has not yet been published. The final rules are not expected until early in Q3, shortening the timeframe for industry to remediate any changes reflected. Therefore, the industry emphasizes the need for transitional provisions, including a risk-based approach to remediation and supervisory enforcement.
2. **Scope.** A number of definitions in DORA are broad and the application of proportionality and risk-based principles to some of DORA's requirements falls short. This makes certain requirements more complex to implement and extends them to a broader scope of processes, third-parties, and supporting applications, ultimately leading to a greater implementation burden and potentially hindering focus and resources available for high-risk areas.
3. **Incident reporting.** The expansion of incident reporting to include all supervised activities has removed proportionality from the incident classification criteria. A lack of proportionality, alongside a strict interpretation of recurring incident notifications, has resulted in a more extensive implementation challenge across an expanded breadth of financial services and ICT infrastructure for financial entities. A significant amount of time and resources will be necessary to meet the incident reporting requirements.
4. **Third-party risk management.** The requirement to implement significant changes to existing risk management processes across a potentially large volume of in-scope ICT third-party providers and subcontractors is a challenge. In particular, the register of information, for which the technical standard remains unfinalized and the proposed expectations of enhanced subcontractor oversight.
5. **Threat-led penetration testing (TLPT).** It remains unclear whether TLPT requirements will apply to a wide range of firms' critical or important functions and how mutual recognition, or cooperation of TLPT authorities, will occur in practice. This could result in multiple TLPTs occurring across firms which have multiple financial entities. The potential inclusion of third parties, in addition, could create risks to the smooth functioning of a TLPT testing programme.

The above implementation challenges are significant and will be difficult for the industry to overcome by 17 January 2025, particularly given the short period between adoption by the European Commission of the technical standards and the delayed finalization of the implementing technical standard on the register of information. This has been acknowledged by a number of supervisory authorities.