ESAs 2021 07

9 February 2021

Irene Tinagli MEP
Chair of the Committee on Economic and Monetary Affairs (ECON)
European Parliament

Joao Leão
President of the ECOFIN Council
Council of the European Union

Mairead McGuinness
Commissioner in charge of Financial stability, financial services and Capital Markets Union European Commission

Subject: Legislative proposal for a regulation on digital operational resilience for the financial sector

Dear Ms Tinagli, dear Mr Leão, dear Ms McGuinness,

We are writing to you in our individual capacities as the Chairs of the ESAs, on the important topic of the proposed Digital Operational Resilience Act (DORA).[1] Since the publication of the proposal on 24 September 2020, which builds on the 2019 ESA Joint Advice,[2] the staff of the ESAs have been working together to analyse the proposed provisions and to constructively assess their implementation and impact.

We are in firm agreement with the main principles of DORA. We fully support the aim of establishing a comprehensive framework on digital operational resilience for EU financial entities by streamlining and strengthening the existing patchwork of relevant provisions across EU financial services legislation. We support the call for enhanced collaboration and cooperation among authorities within the EU and internationally.

As emphasised in the ESAs Joint Advice, the operational resilience of Critical Third Party Providers (CTPPs) is a key concern for an EU financial sector that increasingly makes use of them. Given the absence of an overarching regulatory and supervisory framework to

[1] COM (2020) 595

[2] Joint Advice on the need for legislative improvements relating to Information and Communication Technology (ICT) risk management requirements in the EU financial sector, 10 April 2019.

monitor the digital operational resilience risks stemming from CTPPs from an economy-wide perspective, we strongly support the establishment of an oversight framework to cover the ICT services that CTPPs provide to the financial sector.

The proposed oversight framework is the first concrete initiative to address the complex issue of the dependencies on CTPPs in the financial sector, including monitoring third party concentration risks. This is imperative in its own right and should provide a pathway to any broader oversight in the future. At the same time, to manage public expectations, it is important to clearly communicate that the proposed oversight role for the ESAs is limited to the ICT risks which CTPPs may pose to financial entities, and that the oversight currently envisaged will not amount to full supervision of CTPPs across their full range of activities. To ensure the credibility of this new oversight activity, also in the context of the envisaged powers and resources, it is essential to clearly communicate that its scope is limited to the CTPPs' activities related to financial entities.

Another structural challenge for the role of the ESAs in the oversight framework is that individual CTPPs may serve entities across the entire financial sector, just as they may serve businesses across the wider economy. Unlike the established remits of the ESAs, where specialisation by sub-sector offers natural advantages, an ESAs-led oversight model for CTPPs will need to be carefully crafted to address coordination and consistency challenges.

With these constraints in mind, we are writing to express our views on how to most efficiently take forward important aspects of the governance and operational processes of the oversight framework for CTPPs and the application of the proportionality principle in DORA.

Challenges for the governance and operation of the proposed sectoral oversight framework

Successful implementation of this EU-wide oversight framework requires granting the appropriate powers and mandate, along with the necessary resources and expertise. It is essential for the oversight framework to clearly attribute the legal responsibilities that arise. Equally, the framework should sufficiently enlarge the scope of action of the ESAs by directly assigning them the necessary legal mandate in the legislative text. We are writing to you to highlight the challenges we have identified in these respects and to suggest ways to address them.

1. *Need for more streamlined and effective governance*

Firstly, the current proposal raises challenges on the practical functioning of the oversight framework, especially the complexity of the governance and decision-making process between the Oversight Forum, Joint Committee and the Boards of Supervisors of the ESAs. The size of the proposed Oversight Forum appears to contribute towards this complexity.

At the same time, considering the highly technical nature of the entities falling under the scope of the oversight, the proposed composition of the Oversight Forum may face challenges from a technical capacity and expertise perspective as it will need to be competent to discuss and address quite technical IT issues related to the oversight activities.

Secondly, we have identified challenges on the legal and operational applicability of recommendations addressed by one ESA to a cross-sectoral CTPP (i.e. a CTPP providing services to entities across the remit of more than one ESA). In particular, in cases where the Lead Overseer will be overseeing a CTPP, who will be providing ICT services to the entire financial sector, it might be questionable how and whether all the relevant competent authorities would act on the Lead Overseer's recommendations (which would be approved only by the Lead Overseer's Board of Supervisors). Moreover, there may be challenges on the operational implementation of the proposed governance in the oversight framework, which could benefit from a more responsive and better-informed decision-making process.

In light of the above, we propose the co-legislators consider a model that permits stronger ESAs cooperation through the creation of a joint-ESAs executive body which would integrate the role of the Oversight Forum and be responsible for the overall oversight work for cross-sectoral CTTPs. Necessary powers could be allocated to this executive body by the legislation to enhance its decision-making role and to ensure a unified and harmonised approach across the ESAs. In addition, the legislation could clarify the potential designation of CTPPs providing services to financial entities across the remit of a single ESA (i.e. sector-specific CTPPs), along with the governance model to be applied in these cases.

The executive body should be small and functional and with appropriate technical capacity and expertise. Membership from the ESAs would be limited to Executive Directors and some senior staff. Membership among NCAs should also be limited to few nominated representatives from the Board of Supervisors from each ESA. Therefore, among the membership, it would be essential to ensure a sufficient level of expertise on technology and information security risks in an effort to gather the necessary specialised expertise in the executive body and to bring important efficiency to the oversight framework.

The ESAs' Boards of Supervisors would periodically review the work of the executive body and its composition to ensure full accountability.

Furthermore, as DORA would require unprecedented cooperation between our authorities in the oversight of cross-sectoral CTPPs, and taking into account economies of scale of sharing resources and skills among the ESAs, we propose that the co-legislators consider establishing a cross-ESAs team to work on the oversight of CTPPs.

2. *Need for coherence between oversight recommendations and follow-up*

Another significant challenge in the current DORA proposal is the mismatch between the powers given to the ESAs to conduct their oversight work and the lack of powers relating to the follow-up process of their own recommendations. In particular, once the recommendations will be issued by the ESA Lead Overseer to the CTPP, the competent authorities will be responsible to follow them up and to take actions against their supervised financial entities where the recommendations will not be addressed by the CTPP. In this case, the proposal gives the competent authorities the right to require their supervised financial entities to temporarily suspend the CTPP services or to terminate the contracts with that CTPP. This follow-up process raises a number of significant challenges in relation to the effectiveness and soundness of the enforcement mechanism. On the one hand, it is not clear whether a supervised financial entity will be able to easily suspend or terminate a contract with one of the CTPPs, who could possibly be a major provider for that financial entity. On the other hand, the current mismatch between EU-level recommendations and follow up at entity level may lead to inconsistent approaches across the Member States and therefore put the effectiveness of the entire oversight framework at risk.

To the maximum extent compatible with existing frameworks, enforcement should be done at EU level, mirroring the oversight and promoting a coherent approach. To this end, we propose far greater involvement for the ESAs in the follow-up process and the introduction of effective enforcement measures at EU level that can be applied directly to CTPPs. Enforcement actions against a CTPP could be endorsed by competent authorities through the Board of Supervisors of one or more of the ESAs.

Moreover, DORA could allow for market transparency tools to strengthen the oversight framework and to encourage CTPPs to adhere to recommendations. For example, the ESAs could publish high-level information on the number and types of recommendations issued to each CTPP (acknowledging that the publication of the full recommendations could raise significant competition and confidentiality issues), along with the respective intention of each CTPP to follow those recommendations.

Furthermore, as the recommendations will affect CTPPs servicing the wider economy, DORA should set out in detail how the ESAs should interact with the range of relevant EU authorities and bodies (such as the data protection authorities) that perform analogous oversight tasks. This will also help ensure that CTPPs adhere to the recommendations issued.

3. Need for adequate resources

Thirdly, we reiterate our major concerns about the level of resources that the ESAs will receive to carry out their new tasks and responsibilities under DORA.

The proposal envisages important one-off policy work for the ESAs to produce jointly (at least 10 regulatory technical standards, two implementing technical standards, one set of guidelines and several recurring reports) in addition to policy work for the ESAs individually. Most of these are to be delivered within 12 months. However, no resources have been allocated for this purpose, and after careful analysis we believe that our existing resources will not be sufficient to allow the ESAs to complete these deliverables within the proposed deadlines, even with some redeployment. We strongly recommend that additional resources be allocated to this end as part of the legislative negotiations. Furthermore, we suggest to discuss in detail (at staff level) the timelines and sequencing of the deliverables.

DORA envisages significant new ongoing work. It proposes ongoing policy-related work in the form of regular reporting and several tasks relating to ICT-related incident reporting, cooperation with structures and authorities established by the NIS Directive, financial cross-sector exercises, communication and cooperation. Additionally, the proposed oversight framework will give the ESAs new roles and new tasks, including the need to address the potentially significant legal implications across the sectors. We strongly believe that the proposed new resource demands have been significantly underestimated.[3] As a result, the allocated resources are insufficient to meet the scale and complexity of the new ongoing tasks, risking the effectiveness of the oversight framework. We strongly recommend a significant increase to the allocation of new resources, including more senior roles, for the new ongoing tasks proposed under DORA.

4. Need for a more proportionate DORA

The current DORA proposal excludes only micro-enterprises from the application of certain requirements and does not make any reference to sectoral legislation when defining the financial entities in scope.

Given this, we would like to suggest a more comprehensive inclusion of the principle of proportionality in a more flexible way across the legal act.

We would like to conclude by re-emphasising our support for the objectives and principles of DORA. The proposed modifications we have set out aim to improve the current legislative proposal and achieve its objectives in an effective manner. To take forward our suggestions,

[3] For comparison, it is understood that 5 FTEs are assigned by the National Bank of Belgium to perform the oversight of SWIFT (i.e. only one CTPP in DORA terms), along with support from G10 central banks for the performance of the fieldwork, which indicatively amounts to additional 3 FTEs.

ESAs staff remain at your disposal to provide any clarification and to discuss the issues in greater detail.

Yours sincerely,

Steven Maijoor	José Manuel Campa	Gabriel Bernardino
Chair, ESMA	Chairperson, EBA	Chair, EIOPA

CC: John Berrigan, DG FISMA, Director General
Marcel Haag, DG FISMA, Director Directorate B
Billy Kelleher, Rapporteur to the Committee on European and Monetary Affairs, European Parliament
Jeppe Tranholm-Mikkelsen, Secretary-General of the Council of the European Union