Council of the European Union
General Secretariat

Interinstitutional files:
2020/0268(COD)

Brussels, 04 February 2021

WK 1624/2021 INIT

LIMITE

EF
ECOFIN
CODEC
TELECOM
CYBER

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	Presidency
To:	Working Party on Financial Services (Digital Operational Resilience)
Subject:	PRESIDENCY DISCUSSION NOTE - Oversight Framework

Working Party on Financial Services
Digital Operational Resilience
(DORA)

Meeting 11 February 2021

Oversight Framework

1. Designation of critical ICT TPPs

During the last WP meeting, the majority of MS supported introducing a provision allowing critical ICT TPPs to react to recommendations issued by the Lead Overseer. Nonetheless, it is the Presidency's view that additional procedural rights of critical ICT TPP in such context should be discussed.

An ICT TTP designated as critical can challenge such designation through an administrative and judicial process. Indeed, once a definitive decision is adopted, it is challengeable before the Board of Appeal of the ESAs. Subsequently, once such administrative appeal takes place, it would still be possible to challenge the decision before the General Court.

It should be noted nonetheless that DORA does not foresee the possibility of ICT TPPs expressing their views in the course of the designation procedure mentioned in Article 28(1)(a) nor in relation to the adoption of its respective oversight plan referred in Article 30(3).

One possibility to address the issues raised above would be ensuring the involvement of ICT TPP at an earlier stage of the designation as critical and adoption of the oversight plan procedures, hence granting ICT TPPs a right to be heard previously to the definitive decision.

Q.1 - Do MS see the need to amend DORA to ensure the right of the ICT TPP to be heard in the assessment of its criticality?

Q.2 - Do MS see the need to amend DORA to ensure the right of the ICT TPP to be heard before the adoption of their oversight plans?

2. Oversight plan – Oversight Forum engagement

Pursuant to Article 31(2), the exercise of the Lead Overseer's powers, such as the conduction of investigations or the issuance of recommendations, must be preceded by consultation of the Oversight Forum. No similar provision is established for the adoption of the oversight plan mentioned in Article 30(3) and (4).

The discussion of the oversight plan within the Oversight Forum could foster NCAs knowledge regarding the supervisory actions needed in relation to critical ICT TPPs and allow for their views to be taken into consideration in the design of the oversight plans.

While Article 30(3) establishes that the oversight plan is adopted by the Lead Overseer, having in mind that the respective critical ICT TPP could provide services to different sectors in

different MS, the advantages referred above could increase in case the draft oversight plan was to be prepared by the Oversight Forum, rather than the Oversight Forum being only consulted.

Q.3 - Do MS support the oversight plan being subject to discussion by the Oversight Forum?

Q.3.1 - If yes, do MS support to add the oversight plan to the list of acts to be adopted by the Joint Committee following a recommendation of the Oversight Forum established in Article 28(1)?

Still in this regard, it should be noted that Article 30(3) and (4) do not provide details on the content of the oversight plan. For the benefit of legal certainty, the key elements of the oversight plan could be further detailed in DORA.

Q.4- Would MS consider useful to specify that the oversight plan shall contain the assessment referred in Article 30(2), the annual oversight objectives and the main oversight actions foreseen for the respective critical ICT TPP?

3. Follow up by competent authorities

3.1. Information concerning the (non-)compliance with recommendations

Pursuant to Article 37(4), competent authorities shall take into account the "type and magnitude of the risk that is not addressed" and the "seriousness of the non-compliance" by critical ICT TPPs when taking the decisions referred to in Article 37(3). However, the powers to obtain such information are attributed to the Lead Overseer and the joint examination team in charge of such specific critical ICT TPP (Articles 31 to 35).

In this context, Article 29(4) states that "the ESAs shall issue guidelines on the cooperation between the ESAs and the competent authorities for the purposes of this Section on the detailed procedures and conditions relating to the execution of tasks between competent authorities and the ESAs and details on exchanges of information needed by competent authorities to ensure the follow-up of recommendations addressed by Lead Overseers pursuant to point (d) of Article 31(1) to critical ICT third-party providers."

Q.5. Do MS consider the guidelines referred to in Article 29(4) sufficient to ensure supervisory convergence?

Q.6 - If not, do MS consider necessary to include an explicit reference to the transmission of information, by the Lead Overseer to Competent Authorities concerning the compliance with the Lead Overseer's recommendations, in order to allow competent authorities to make informed decisions regarding the suspension of use of services / the termination of contractual arrangements in accordance with Article 37(3) and (4)?

Q.6.1 - If yes, should a reference to the need of competent authorities taking into consideration such information be added in Article 37(4)?

3.2. Suspension of the use of services / termination of contracts between a financial entity and a critical ICT TPP

The suspension of services / termination of contractual arrangements with a critical ICT TPP can only be required to a financial entity pursuant to Article 37 (3) in case the following cumulative conditions are met (Article 37(2) and (3)):

i) the critical ICT TPP does not adequately address the risks identified in the Lead Overseer recommendations; and

ii) a financial entity to whom such critical ICT TPP provides services does not take into account the risks identified in the recommendations.

However, Article 37 does not detail the procedure to require said suspension / termination to a financial entity.

In case where two or more financial entities subject to the supervision of the same competent authority resort to the services of the same critical ICT TPP, such competent authority could have the view that one financial entity adequately takes into account the risks identified in the recommendations is addressed to the critical ICT TPP, while the other financial entity does not. As a result, only the latter would be required to suspend the use of services / terminate contractual arrangements with that critical ICT TPP.

Article 37(5) determines that competent authorities shall inform the Lead Overseer on the supervisory and contractual measures taken where the critical ICT TPP has not (in part or entirely) endorsed the recommendations addressed to critical ICT TPP by the Lead Overseer.

Q.7 - In case the relevant competent authority considers that a financial entity has not adequately taken into account the risks identified in the recommendations to the critical ICT TPP, do MS consider that, before being able to require the financial entity to suspend the use of services / terminate contractual arrangements with such critical ICT TPP, there should be an initial communication from the competent authority to the financial entity informing of the intention to require said suspension or termination in case due measures are not taken by the financial entity within a reasonable timeframe?

Q.8 - To foster convergence of competent authorities' decisions without affecting competent authorities exclusive competence to take them, should they be required to consult the Oversight Forum before making a decision regarding the suspension of use of services / termination of a contractual arrangement between a critical ICT TPP and a financial entity?

3.3. Cooperation with NIS2 National Competent Authorities responsible for the supervision of essential and important entities

NIS2 Directive proposal attributes supervisory powers to National Competent Authorities (NCAs) over "Essential" or "Important" entities[1]. Such entities spread across a variety of sectors, such as energy, health, public administration and, more importantly for this discussion, digital infrastructure and digital providers.

Some of the digital infrastructure and digital providers entities at stake, such as cloud computing service providers, are also covered by the definition of ICT TPP in Article 3(15) of

[1] Referred to in Annexes I and II of the Commission proposal.

DORA, while others, such as providers of electronic communications services, are excluded from DORA's scope and covered by the NIS2 proposal only.

The divergent scope and powers described are justified, since DORA and NIS2 pursue parallel objectives and establish different requirements: DORA seeks to ensure digital operational resilience on a specific and very interlinked sector, while NIS2 aims at establishing a minimum common level of cybersecurity amongst a broader and diversified set of sectors.

That being said, it should be taken into account that Articles 29 and 30 of the NIS2 proposal attribute supervisory and enforcement powers to NIS NCAs, such as the power to issue warnings and binding instructions or to order the implementation of recommendations. In case those powers are deemed ineffective, NIS2 NCAs may, in accordance with Article 29(5)(a) NIS2, as *ultima ratio*, apply the following power to essential entities:

"*(a) suspend or request a certification or authorisation body to suspend a certification or authorisation concerning part or all the services or activities provided by an essential entity*".

Consequently, there is the possibility of the abovementioned suspension of a certification or authorisation being exercised in relation to essential entities in NIS2 which are simultaneously critical ICT TPPs pursuant to DORA, thus subject to the suspension of use of services or termination of contracts by financial entities in accordance with Article 37(3) and (4) of DORA.

Against this background, it could be appropriate to establish coordination mechanisms aimed at ensuring information sharing, coordination and cooperation between DORA and NIS competent authorities. A possible mechanism could be to attribute to the NCA responsible for the supervision of critical ICT TPPs, which are also essential or important entities pursuant to NIS2 the statute of observer in the Oversight Forum foreseen in DORA.

Q.9 - Would MS support the attribution of the statute of observer in the Oversight Forum to the NCA responsible for the supervision of a critical ICT TPP which is also an essential or important entity pursuant to NIS2?