Working Party on Financial Services
Digital Operational Resilience
(DORA)

Meeting 28 April 2021

Discussion note: Chapter V

0. INTRODUCTION

With this note the Presidency intends to follow up on the Partial Compromise Proposal that covered the discussions held on 21st January, 11th February and 3rd March CWP regarding Chapters I and V, in particular, regarding Section II of the latter and address remaining issues in regard to drafting therein. Below, the Presidency describes the feedback received and presents drafting proposals accompanied by relevant explanations.

The Presidency also raises some additional diverse queries that have not been previously discussed with MS in order to gather their views on a possible way forward.

1. Scope wording - Article 3

1 - Definition of ICT TPP

In their written comments, some MS referred that the current definition of ICT services does not mention cloud computing and software services, which should be encompassed in the definition of services covered by DORA.

Q.1 - Against this background, the Presidency would like to know if MS can support the following amendment to Article 3(16).

*(16) 'ICT services' means digital and data services provided through the ICT systems to one or more internal or external users, on an ongoing-basis, including provision of **cloud computing services, software,** data, data entry, data storage, data processing and reporting services, data monitoring as well as data based business and decision support services, hardware as a service and hardware services which include technical support via software or firmware updates by the hardware provider;*

2 – Definition of ICT third-party service provider established in a third country

Several MS referred that this definition should clarify that the reference to "not established in the Union" means that the ICT TPP did not set up a subsidiary, branch or representative office in the Union. MS also referred the need to align this definition with the definition of 'ICT sub-contractor established in a third country' defined in Article 3(20).

The Presidency considers that this wording may need further clarification, particularly having in mind its intersection with Article 28(9). To that end, the following amendments could be introduced:

*"3(19) 'ICT third-party service provider established in a third country' means an ICT third-party service provider that is a legal person, **that does not have a legal representative in the Union or has** not established **a branch or a subsidiary** in the Union **and** ~~that~~ has entered into a contractual arrangement with a financial entity for the provision of ICT services;*

*3(20) 'ICT sub-contractor established in a third country' means an ICT sub-contractor that is a legal person, **that does not have a legal representative in the Union or has not** established ~~**in a third-country, has not set up business/presence**~~ **a branch or a subsidiary** in the Union and has entered into a contractual arrangement either with an ICT third-party service provider, or with an ICT third-party service provider established in a third country;*

3(19x) 'ICT third-party service provider established in a third country designated as critical' means an ICT third-party service provider that is a legal person whose head office is not established in the Union and has entered into a contractual arrangement with a financial entity for the provision of ICT services;

*Article 28(9). "Financial entities shall refrain from using an ICT third-party service provider established in a third country designated as critical pursuant to point (a) of paragraph 1 that does not **have a subsidiary** established **ed** ~~a subsidiary~~ in the Union.*

The first subparagraph does not apply within 12 months following such designation."

Please find below the rationale for this approach:

1 - If an ICT TPP that has a legal representative or a branch in the Union is not considered an "ICT TPP established in a third country" in accordance with Article 3(19), the requirement concerning the establishment of a subsidiary in the Union set forth in Article 28(9) would not be applicable to this ICT TPP as it would not be considered an "ICT TPP established in a third country".

2 - Hence, one way forward could be clarifying that the requirement concerning the establishment of a subsidiary in the Union would not be applicable to any "ICT TPP established in a third country", but rather solely to "ICT TPP established in a third country designated as critical".

3 - Consequently, following the assessment in Article 28(2), if such ICT TPP is deemed critical and does not have a subsidiary, meaning a company incorporated in the Union, it would be deemed an "ICT TPP established in a third country designated as critical". Thus, would be subject to the requirement concerning the establishment of a subsidiary in the Union, even if having already a legal representative or branch in the Union.4-Indeed, this new definition might better clarify the more demanding requirements for "ICT TPP established in a third country designated as critical", as supported by the majority of MS in Article 28(9), in comparison with the overall "ICT TPP established in a third country".

Q.2 - Against this background, the Presidency would like to know if MS support the amendments proposed above in Article 3(19) and 3(20) and the inclusion of proposed new Article 3(19x).

2. Contractual arrangements for the use of ICT services - Chapter V Section I

3- Article 25 (1) and (5) – Applying specific provisions of Section I of Chapter V to all ICT services

Further to the discussion held on the CWP of 3rdMarch, the majority of MS supported narrowing the overall scope of Section I of Chapter V to the provision of ICT services concerning critical or important functions.

MS broadly supported this approach mainly in order to allow financial entities, particularly the smaller ones, to only apply the burdensome procedures established in Section I of Chapter V in relation to critical or important functions rather than all ICT services covered by DORA, which would encompass services such as accounting or HR software.

However, some MS noticed that the establishment of a linear approach in Article 25(1) could result in an excessive and undesirable limitation of financial entities' responsibility, as these should remain fully responsible for any outsourced activity, and not only for those concerning critical or important functions.

In case such approach is adopted, financial entities will have to, as established in the Commission proposal, assess whether a contractual arrangement contractual arrangement covers a critical or important function before entering into such arrangement in order to determine what would be the requirements applicable.

Q.3.1 - Against this background, the Presidency would like to know if MS support reinstating the original wording of Article 25(1):

Financial entities that have in place contractual arrangements for the use of ICT ~~concerning critical or important functions~~ services to run their business operations shall at all times remain fully responsible for complying with, and the discharge of, all obligations under this Regulation and applicable financial services legislation.

Q.3.2 - the Presidency would like to know if MS support reinstating the assessment of whether the contractual arrangement covers a critical or important function in Article 25(5):

Before entering into a contractual arrangement on the use of ICT services ~~concerning critical or important functions~~, financial entities shall

(a) assess whether the contractual arrangement covers a critical or important function;

(b) assess if supervisory conditions for contracting are met;

(c) identify and assess all relevant risks in relation to the contractual arrangement, including the possibility that such contractual arrangements may contribute to reinforcing ICT related concentration risk as referred to in Article 26;

(d) undertake all due diligence on prospective ICT third-party service providers and ensure throughout the selection and assessment processes that the ICT third-party service provider is suitable;

(e) identify and assess conflicts of interest that the contractual arrangement may cause.

Points (b) to (e) shall only be applicable in relation to contractual arrangements on the use of ICT services concerning critical or important functions.

4- Articles 25 (4) and 28(7) – Register of Information

Article 25(4) 3º subparagraph, as amended by this Presidency partial compromise proposal I (PCPI), states that financial entities should report information on their ICT-third party services concerning critical or important functions to the Competent Authorities (CAs) on an annual basis.. This shall be pursued by means of a Register of Information to be made available to the CAs upon request.

Article 28(7) requires CAs to transmit the reports referred to in Article 25(4) to the Oversight Forum but not necessarily the Register of Information. Given that this information would be essential for the designation of ICT TPPs (as well as for analytical purposes), it is important to ensure a common and harmonised reporting from the CAs to the Oversight Forum to reduce the time and complexity of analysing the data collection process for ICT TPPs.

Still in this regard, it should be noted that, when determining whether an ICT TPP should be designated as critical pursuant to Article 28(1) a), the criteria described in Article 28(2) should not be limited to critical or important functions, although those are explicitly referred in Article 28(2) c), but rather to all "ICT services provided by an ICT third-party provider" as currently referred to in Article 28(2).

Against this background, one way forward could be to amend Article 25 in order to clarify that all contractual arrangements concerning ICT services should be included in the Register of Information, thus allowing the Oversight Forum to have a comprehensive view of the overall ICT services provided by the ICT TPP when assessing its criticality. On the other hand, the provision regarding the interaction between financial entities and each ICT TPP would keep focusing on critical or important functions.

Q.4 - In light of the above, the Presidency would like to know if MS agree to explicitly require financial entities to submit, on an annual basis, to their CAs the Register of Information, which shall include the required information for the purposes of Article 28(7) to be then transmitted by CAs to the Oversight Forum?

Q.5 Would MS support clarifying that the information contained in the Register of Information should not be limited to critical or important functions, in order to ensure a comprehensive assessment of all the services provided by an ICT TPP to financial entities?

Please see below the proposed wording for Articles 25(4) and 28(7) in case Q.4 and Q.5 are supported by MS:

25(4) As part of their ICT risk management framework, financial entities shall maintain and update at entity level and, at sub-consolidated and consolidated levels, a Register of Information in relation to all contractual arrangements on the use of ICT ***services*** ~~***concerning critical or important functions***~~ *provided by ICT third-party service providers.*

The contractual arrangements referred to in the first subparagraph shall be appropriately documented, ***distinguishing between those that cover critical or important functions and those that do not****.*

Financial entities shall ~~report~~ ***transmit*** *at least yearly to the competent authorities* ***the Register of Information*** ~~*information on the number of new arrangements on the use of ICT services concerning critical or important functions, the categories of ICT third-party service providers, the type of contractual arrangements and the services and functions which are being provided*~~*.*

Financial entities shall make available to the competent authority, upon request, the full Register of Information or as requested, specified sections thereof, along with any information deemed necessary to enable the effective supervision of the financial entity.

Financial entities shall inform the competent authority in a timely manner about planned contracting of ICT services concerning critical or important functions and when an ICT service has become critical or important.

*28(7) For the purposes of point (a) of paragraph 1, competent authorities shall transmit, on a****n*** *yearly and aggregated basis, the reports referred to in Article 25(4),* ***including the Register of Information****, to the Oversight Forum established pursuant to Article 29. The Oversight Forum shall assess the ICT third-party dependencies of financial entities based on the information received from the competent authorities.*

3. Oversight framework – Article 3, Chapter V Section II and Chapter VII

5 - Article 3(50.1) Lead Overseer

During the discussion held in the CWP of 21st January, concerning the establishment of multiple Lead Overseers or a single Lead Overseer a significant majority of MS supported the latter. Conversely, while some MS supported the establishment of EBA as the single Lead Overseer due to its experience concerning digital operational matters, several MS were still forming their views on this regard.

Q.6 - Against this background, the Presidency would like to know MS preference concerning the ESA which should be appointed as Lead Overseer.

6 - Article 28(2) – Criticality assessment at group level

During the discussion held in the CWP of 3rd March and in subsequent written comments, the majority of MS favored to clarify in Article 28(2) that the criticality assessment of ICT TPPs takes place at group level.

It should be noted that, while this assessment takes into consideration all ICT services provided by the entities within a group, the designation as critical and the imposition of oversight measures described in Section II of Chapter V, such as the oversight plan and recommendations, concern each specific ICT TPP. Accordingly, the decision regarding designation as critical referred in Article 28(1)a) shall specify which specific ICT TPP(s) within the group are critical.

A coordination point amongst the several ICT TPPs within a group should be appointed with a view to ensure the practical arrangements and give effect to the conduct of the Oversight.

Q.7 - The Presidency would like to know if MS support the addition of the following wording in Article 28 (2) to better clarify the approach described above.

(*2) The designation referred to in point (a) of paragraph 1 shall be based on all of the following criteria in relation to ICT services provided by an ICT third-party provider~~'s group.~~ Where an ICT services provider belongs to a group, the criteria shall be considered in relation to the group as a whole.*

Q.8 - The Presidency would like to know if MS would support the addition of a provision stating that a coordination point should be nominated in order to allow for a better communication with the ICT TPP group.

7 - Article 28 (5a) - ICT TPPs right to be heard following the criticality assessment

While the regime established in Article 28 (5a) pursuant to PCPI was broadly supported, some MS considered that additional safeguards could be established in order to allow an ICT TPP to react to the assessment under Article 28 (2), before the designation as critical takes place in accordance with Article 28 (1) a).

To this end, one possible way forward could be to provide more time for the ICT TPP to make available all relevant additional information to challenge the assessment and determining that the Lead Overseer may subsequently interact with the ICT TPP in order to ensure a properly informed decision.

Consequently, Article 28(5a) would be amended as follows:

The Lead Overseer shall notify the ICT third-party service provider of the outcome of the assessment referred in paragraph 2.

*Within ~~30~~ **60** calendar days from the date of the notification, the ICT third-party service provider may submit to the Lead Overseer a reasoned statement on the assessment which shall contain all relevant additional information which may be deemed appropriate by the ICT third-party service provider to support the completeness and accuracy of the designation procedure. **Prior to taking a decision on designation under Article 28(1)a), the Lead Overseer shall take due consideration of this statement and may request further information to the ICT third-party service provider, to be provided within 30 calendar days from request.***

Q.9.1 - The Presidency would like to know if MS would support the extension of the deadline for the ICT TPP reaction?

Q.9.1 - The Presidency would like to know if MS would support the addition of the subsequent interaction in the final part of Article 28(5a) reflected above?

8 - Article 29(3) – ECB voting power in the Oversight Forum

Some MS considered that voting power should be granted to the ECB in the Oversight Forum since the ECB supervises significant credit institutions across the Union. In any case, it should be noted that this approach could create an unbalanced power to the MS that compose the SSM, since unlike the remaining 8 MS that would only be granted one vote through the respective NCA in the Oversight Forum, they would also be indirectly represented through their position in the Supervisory Board of the ECB[1].

Q.10 - The Presidency would like to know if MS support amending Article 29 (3) as follows in order to ensure that the ECB is a voting member in the Oversight Forum:

***(b)** **the ECB and** one high-level representative from the current staff of the relevant competent authority from each Member State who shall be voting members;*

***(c)** the Executive Directors of each ESA and one representative from the European Commission, from the ESRB~~, from ECB~~ and from ENISA, who shall be non-voting observers;*

9 - Article 31 (4) - Common reporting template on sub-contracting

For the purposes of Article 31 (d) (iv), there could be merit in revisiting the ESAs proposal regarding the establishment of a common reporting template to be submitted by the ICT TPPs to

1 According to the decision process of the ECB for banking prudential supervision matters, as defined in Article 26 (1), 26 (6) and 26 (8) of Council Regulation (EU) No 1024/2013 of 15 October 2013).

the Lead Overseer, *ex-ante*, to ensure consistent and comprehensive assessment of their sub-contracting arrangements related to services provided to the financial entities.

This information on sub-outsourcing provided by the ICT TPPs could also function as a quality assurance to the Register Information, which the financial entities will be submitting to the CAs as it will not only provide information on the main counterparties but also on the extension of subcontracting such counterparties may carry out granting an overview on who is, in fact, providing relevant services to financial entities.

Q.11 - Would MS agree with the establishment of a common template on sub-contracting as per the above?

10 - Article 32 (3) - periodic penalty payment

In accordance with Article 32(3)(e), the Lead Overseer shall impose a periodic penalty payment where the production of the required information from the ICT TPP is incomplete. The Presidency considers that this could be limiting, and also challenging in case the Lead Overseer would need to substantiate why and how the information was incomplete. The Presidency believes that this could be resolved if the penalty is also applicable in the case where the ICT TPP does not provide the required information within the time limit to be set by the Lead Overseer.

Q.12 - Would MS agree with extending the application of the periodic penalty payment in the case where the ICT TPP does not provide the required information within the time limit set by the Lead Overseer?

The wording for Article 32(3) e) in case Q. 12 is supported by MS would be the following.

(e) indicate the *periodic penalty payments provided for in Article 31(4) where the production of the required information is incomplete or* ***when such information is not provided within the time limit established in point (d).***

11 - Article 35 – Composition of the Joint Examination Team

In result of previous discussions, the current composition of the JET is the following: i) staff members from the Lead Overseer; ii) competent authorities supervising the financial entities to which the critical ICT third-party service provider provides services; iii) national competent authorities from the Member State where the critical ICT third-party service provider is established.

In what regards the members referred in point i) it should be noted that, due to the establishment of a Single Lead Overseer, only staff members from that Lead Overseer will be eligible for the JET in accordance with the current drafting. As DORA will require extraordinary cooperation between the ESAs for the purposes of the ICT TPPs' oversight, and taking into account the economies of scale that arise from sharing resources and skills among the ESAs, it could be appropriate to allow staff members from any ESAs to be eligible for the JET. This could provide for a more efficient and effective conduct of the oversight, creating more synergies concerning human resources, knowledge, experience and skills and providing greater oversight convergence.

Q.13 - Would MS agree with allowing staff members from all ESAs to be eligible to integrate the JET?

Also on the subject matter of the composition of the JET, the Presidency takes note of concerns expressed by some MS regarding the interaction between DORA and NIS 2. Following previous discussions on this regard, the composition of the Oversight Forum was amended as follows in order to encompass as non-voting observer: "*e) one representative of the national competent authorities designated under Article 8 of Directive (EU) 2016/1148 responsible for the supervision of an essential entity listed in point (8) of Annex I to that Directive which has been designated as a critical ICT third-party service providers."*

Nonetheless it should be noted that the JET, which is currently composed solely by members from the staff of the financial supervisors, has as its main attribution, to perform the oversight concerning critical ICT TPPs. In order to strength cooperation between DORA and NIS 2 authorities and to seize skills and experience of NIS 2 supervisors, one possible way forward would be to allow that the NIS 2 national competent authority (NIS 2 CA) of a critical ICT TPP, as mentioned in Article 29(3)e) is part of the JET set forth for such critical ICT TPP.

Finally, it should be noted that some MS expressed reservations regarding the inclusion of CAs from the Member State where the critical ICT third-party service provider is established, as set forth in point iii) above, because due to the financial scope of their functions, such CA may not have a specific relation with the critical ICT TPP, unlike NIS 2 CAs. In addition some MS suggested to clarify that the participation of these entities should be voluntary and that only one CA from MS referred in point iii) should participate in the JET.

Q.14 - Would MS agree to add NIS 2 CA referred in Article 29 (3) e) to the composition of the JET?

Q.15.1 - Would MS like to keep the financial CA referred in point iii) above in the composition of the JET or should it be replaced by NIS 2 CA referred in Article 29 (3) e)?

Q.15.2 - In case MS support the maintenance of the financial CA referred in point iii), should it be clarified that only one CA is eligible for this purpose and that the participation is voluntary?

12 - Article 37(1) – Timeline for comply or explain procedure

Similarly to the views presented in point 7 "*Article 28(5a) - ICT TPP right to be heard following the criticality assessment*", MS also considered that a broader deadline could be established in order to allow critical ICT TPP to present the reasons for not following a recommendation.

Subsequently, Article 37(1) would be amended as follows:

1. Within ~~30~~ 60 calendar days after the receipt of the recommendations issued by the Lead Overseer pursuant to point (d) of Article 31(1), critical ICT third-party service providers shall either notify the Lead Overseer on their intention to follow the recommendations or provid~~inge~~ a reasoned explanation for not following such recommendations. The Lead Overseer shall immediately transmit this information to competent authorities.

Q.16 - Would MS support this amendment?

13 - Article 37(1a) – References to "infringement" and "commercial interests of critical ICT third-party service providers"

The issuance of a public notice in case the critical ICT TPP fails to notify the Lead Overseer in accordance with Article 37(1) or in case the explanation provided is deemed insufficient was broadly supported by MS.

However some MS suggested improving the wording by replacing the references to "infringement" by "non-compliance" since this provision concerns recommendations. In addition, MS considered that the reference to the "commercial interests of critical ICT third-party service providers" as a reason for non publication might be excessive since other elements are already considered when deciding whether to advance with the publication or not, namely if such publication is "proportionate for the purpose of public awareness, (…) or could seriously jeopardise the orderly functioning and integrity of financial markets or the stability of the whole or part of the financial system of the Union".

Q.17 - Against this background the Presidency would like to know if MS support the following amendments to Article 37(1a)**:**

1a. *The Lead Overseer shall disclose to the public where a~~n~~ critical ICT third-party service provider failed to notify the Lead Overseer in accordance with paragraph 1 or in case the explanation provided by the critical ICT third-party service provider is not deemed as sufficient. The information published shall disclose the identity of the critical ICT third-party service provider as well as information on the type and nature of the ~~infringement~~ non-compliance and be limited to that relevant and proportionate for the purpose of public awareness, unless such publication ~~is in conflict with the legitimate interest commercial interests of critical ICT third-party service providers, or with the protection of their business secrets, or~~ could seriously jeopardise the orderly functioning and integrity of financial markets or the stability of the whole or part of the financial system of the Union.*

14 - Article 37(2a) to (4) - Suspension and termination of contracts (interaction DORA-NIS 2)

As referred above, the interaction between DORA and NIS 2 is still a concern for some MS[2].

On the CWP held in 11th February a specific topic on this subject was discussed as per the WK 1624/2021:

"*That being said, it should be taken into account that Articles 29 and 30 of the NIS 2 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, NIS 2 NCAs may, in accordance with Article 29(5)(a) NIS 2, as ultima ratio, apply the following power to essential entities:*

[2] It should be noted that DORA is *lex specialis* to NIS2 only in what regards financial entities and not ICT TPP, since Article 2(6) of NIS2 only refers to supervision and not oversight. The Presidency envisages to add a recital which clarifies this matter.

"(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 NIS 2 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".

In result, the NCA responsible for the supervision of a critical ICT TPP which is also an essential or important entity pursuant to NIS 2 was added as an observer to the Oversight Forum in accordance with Article 37 (3) e).

Without prejudice of the developments referred above, in order to foster cooperation between DORA and NIS 2 authorities an additional coordination mechanism could be added in Article 37, determining that before making a decision regarding the suspension of use of services or the termination of a contractual arrangement between a financial entity and a critical ICT TPP, DORA CAs could consult the NIS 2 CA of such critical ICT TPP.

In addition, the opinion of the NIS 2 CA could be added to the elements to be taken into account when making such decision.

Q.18 - Further to the above, the Presidency would like to know MS views on the following:

Q.18.1 - The addition of paragraph 2b.

Q.18.2 - The addition of the wording in bold in paragraph 3.

Q.18.3 - The addition of point e) in paragraph 4.

Q.19 – Do MS consider that the consultation of the NIS 2 CA responsible for the supervision of the critical ICT TPP concerned in the suspension / termination of contracts should be optional or mandatory?

The wording for Article 37 in case Q.17.1 to Q.17.3 are supported by MS would be the following:

2a. Where a competent authority deems that a financial entity fails to take into account or to sufficiently address within its management of ICT third party risk the specific risks identified in the recommendations referred to in paragraph 2, it shall notify the financial entity of the possibility of a decision being taken pursuant to paragraph 3 within 60 working days, in the absence of appropriate contractual arrangements aimed at addressing such risks.

2b. Upon receiving the assessment referred to in Article 35(5a), competent authorities, before taking any of the decisions referred to in paragraph 3 [may/shall] consult the national competent authorities designated under Article 8 of Directive (EU) 2016/1148 responsible for the supervision of an essential entity listed in point (8) of Annex I to that Directive designated as a critical ICT third-party service provider.

3. *Competent authorities may, as a measure of last resort* ***and following the notification and consultation as set out in paragraph 2a and 2b,*** *in accordance with Article 44, require financial entities to temporarily suspend, either in part or completely, the use or deployment of a service provided by the critical ICT third-party service provider until the risks identified in the recommendations addressed to critical ICT third-party providers have been addressed. Where*

necessary, they may require financial entities to terminate, in part or completely, the relevant contractual arrangements concluded with the critical ICT third-party service providers.

4. Upon receiving the assessment referred to in Article 35(5a), competent authorities, when taking the decisions referred to in paragraph 3, competent authorities shall take into account the type and magnitude of risk that is not addressed by the critical ICT third-party service provider, as well as the seriousness of the non-compliance, having regard to the following criteria:

(a) the gravity and the duration of the non-compliance;

(b) whether the non-compliance has revealed serious weaknesses in the critical ICT third-party service provider's procedures, management systems, risk management and internal controls;

(c) whether financial crime was facilitated, occasioned or otherwise attributable to the non-compliance;

(d) whether the non-compliance has been committed intentionally or negligently.

(e) [where appropriate] the opinion of the national competent authorities designated under Article 8 of Directive (EU) 2016/1148 responsible for the supervision of an essential entity listed in point (8) of Annex I to that Directive which has been designated as a critical ICT third-party service providers, provided in accordance with paragraph 2.b.

15 - Article 42 (3) – Coordination and cooperation across authorities

Still, on the matter of interaction between DORA and NIS2 CAs, effective coordination and cooperation across relevant authorities and consistency across different legislative acts could be fostered. The risks of cross-sectoral divergences should be mitigated to the extent possible in Level 1, for instance including related provisions establishing cooperation arrangements and exchange of information.

Q.20 - In light of the above would MS agree to include a new 42(3a) as follows, taking into consideration the wording currently proposed in PCP II for Article 42(3)?

(3)Competent authorities may, when deemed appropriate, request any relevant technical advice from the authorities designated in accordance with Article 8 of Directive (EU) 2016/1148 and establish cooperation arrangements to allow the set-up of effective and fast-response coordination mechanism.

(3a) Such arrangements may specify the procedures for the coordination of supervisory and oversight activities, respectively, in relation to entities listed under point (7) of Annex II of the Directive (EU) 2016/1148 designated as critical ICT third-party service providers pursuant to Article 28, including for the conduct, in accordance with national law, of investigations and on-site inspections, as well as mechanisms for the exchange of information between competent authorities and authorities designated in accordance with Article 8(1) of Directive (EU) 2016/1148 which include access to information requested by the latter authorities.

16 - Article 42a Information exchange between LO and CA

Following previous discussions, the Presidency introduced in Article 35(5a) the requirement for the Lead Overseer to inform the CA of the critical ICT TPP compliance with their respective recommendations.

Nonetheless, MS requested in their written comments to better clarify that the Lead Overseer should inform regularly all NCAs of the financial entities to whom the critical ICT TPP provides services about approaches and measures taken in relation to critical ICT TPPs.

To this end, Article 42a could be amended in the following way:

*2.Competent authorities and the Lead Overseer shall, in a timely manner, mutually exchange the relevant information concerning critical ICT third-party service provider necessary to carry out the respective duties resulting from this Regulation**, namely in relation to identified risks, approaches and measures taken as part of the Lead Overseer oversight tasks.***

Q.21 – Do MS support this addition?