Council of the European Union
General Secretariat

Interinstitutional files:
2020/0266(COD)

Brussels, 20 May 2021

WK 6712/2021 REV 1

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:	DORA: Presidency discussion note - General Issues

Working Party on Financial Services
Digital Operational Resilience
(DORA)

Meeting 26 May 2021

Discussion note: General Issues

0. Introduction

With this note, the Presidency intends to follow up on the written comments to the fourth Partial Compromise Proposal (PCP 4).
Below, the Presidency describes the feedback received and presents drafting proposals accompanied by relevant explanations.
The Presidency also raises some additional queries that have not been previously discussed with Member States (MS) in order to gather their views on a possible way forward.

1. ICT risk management

The Presidency has taken good notice of MS comments and suggestions on the proposed amendments to Chapter IV, several of which will be incorporated in the second Global Compromise Proposal (GPC 2) to be circulated in the end of May. On the contrary, other possible amendments, as the ones presented below, could merit additional assessment from MS:

1 - Legacy ICT system (Article 3)

Q.1 - Would MS support the following replacement, in line with MS suggestion?

Article 3 (2a) "Legacy ICT system" means an ~~out of date~~ ICT system that has reached the end of its lifecycle (end-of-life), that it is unsuitable for upgrades and fixes or no longer supported by its vendor or an ICT third-party service provider, but is still in use and supports the business functions of the financial entity~~, but that is unsuitable for upgrades and fixes or no longer supported by its vendor nor an ICT third-party service provider~~.

2 - Governance and organisation (Article 4)

Q.2 - Would MS support the following amendment, related to the second line of defence for ICT risk of financial entities, which seeks to reflect MS expressed views?

Article 4(1) – "*Financial entities shall have in place internal governance and control frameworks that ensure an effective and prudent management of all ICT risks. Within the internal governance and control framework, financial entities should assign the responsibility for managing and overseeing ICT risks to a control function that is independent and segregated from ICT operations processes".*

Q.3 - Would MS support the following amendment, to reflect MS suggestion that this requirement should be made general and not focus on ICT-related incidents?

Article 4(2)b) – "*set clear roles and responsibilities for all ICT-related functions and establish appropriate governance arrangements to ensure effective communication, cooperation and coordination among them~~, in particular in case of an ICT-related incident~~;*"

3 - Backups (Article 11)

In their comments, MS mostly agreed with the compromise proposal on Articles 11(2) and 11(3), dealing with backup data, backup systems and general restoration requirements. However, some MS also argued that i) backup policy/policies might not be appropriate; ii) segregation between the processing and backup sites could be hard to accomplish; and iii) the wording used might need improvement. The Presidency believes that the backup and restoration of data and ICT systems backup is a key component of ICT risk management for operational resilience and deems that further discussion is necessary

Q.4 - Against this background, the Presidency would like to know if the following compromise proposal for Article 11(2) would be acceptable for MS:

2. *Financial entities shall set up backup ~~policies~~ systems that operate according to the backup policies and processes~~. which shall ensure that backup systems are operating accordingly to the backup processes~~.*

The setting up ~~activation~~ of backup systems, and especially the initiation of backup restoration procedures, shall not jeopardize the security of the network and information systems or the integrity, availability or confidentiality of data.

3.When restoring backup data ~~and restoring systems using backup data~~, financial entities shall use ICT systems which are segregated (both physically and logically) from the primary processing site and ensure that these ICT systems are not directly connected, but allows for the transfer of data as necessary for the backup restoration.

4 - Further harmonisation of ICT risk management (Article 14)

Several MS considered important to take into consideration the sector-specific reality when drafting this RTS. This is in line with the MS preference to have a single RTS for this matter instead of three separate RTS. At the same time, the concern that this might hinder the appropriateness of such single RTS to different types of financial entities should be considered. In light of this, the Presidency would propose the amendment below:

Q.5 - Would MS support the following amendment?

Article 14 2º subparagraph - "*When developing those draft regulatory technical standards, the ESAs shall take into account the size, nature, scale, complexity and overall risk profile of the financial entities~~.~~, while giving due consideration to any specific feature arising from the distinct nature of activities across different financial services sectors.*"

2. Oversight framework

1 - Information concerning the (non-)compliance with recommendations

Article 31(1)c) of DORA, as proposed by the Commission, allows the Lead Overseer (LO) to request reports to the critical ICT TPP specifying the actions that have been taken or the remedies implemented in order to address the recommendations issued by the LO.
While Article 31(2) determines that the LO shall consult the Oversight Forum before requiring such reports to the critical ICT TPP, no requirements are established concerning the transmission of such information to the relevant competent authorities (CA).
In this regard, it should be noted that following the discussion in the 11/02 WP and the support in the subsequent written comments, PCP1 included the following requirement for the transmission of information to relevant CA concerning ongoing oversight: "*5a.The Lead Overseer, assisted by the joint examination team, shall assess the compliance with the recommendations referred to in paragraph 4. The Lead Overseer shall, without undue delay, inform the competent authorities of the financial entities using that critical ICT third-party service provider of the result of such assessment.*"
Moreover, in coherence with the abovementioned addition, Article 37(2b) and (4) currently refer that the suspension of use of services / the termination of contractual arrangements should only take place after CA receiving the information referred to in Article 35(5a).

Q.1 – Do MS consider that an approach similar to the one established in Article 35(5a) should be established for the reports referred to in Article 31(1)c)[1]?

In an affirmative case, the following amendment would be inserted:
Article 31(2a) - "***The Lead Overseer shall, without undue delay, transmit to the competent authorities of the financial entities using that critical ICT third-party service provider the reports referred in point (c) of paragraph 1.***"

Article 37(2b) – "*Upon receiving the **reports referred to in Article 31(2a) and the** assessment referred to in Article 35(5a), competent authorities, before taking any of the decisions referred to in paragraph 3, may 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."*

Article 37(4) – "*Upon receiving the **reports referred to in Article 31(2a) and the** assessment referred to in Article 35(5a), competent authorities, when taking the decisions referred to in paragraph 3, 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*:"

1 The Presidency would like to mention that these reports should explain in details the actions and approaches taken by CTPPs as follow-up of the oversight measures. Hence, in order to allow for CAs to take an informed decision the full report should be provided and this information sharing should be subjected to the safeguards established in Article 49 and 49a, amongst others.

2 - Cross-ESAs team

During the discussion on 28/04 WP, as well as in their subsequent written comments, MS supported the clarification that staff members from all ESAs should be eligible to be part of the joint examination team (JET) established in Article 35 of DORA.
The reason for this approach arises mostly from the willingness to foster ESAs cooperation for the purposes of the oversight tasks concerning critical ICT TPPs that may provide ICT services to financial entities across all sectors. Moreover, closer cooperation amongst ESAs and the sharing of resources, skills and experience could create economies of scale.
Against this background, the Presidency sees merit in requesting MS views on the establishment of a cross-ESAs team. While the presence of staff members from all ESAs in the JET aims at seizing the sectorial expertise from all ESAs when executing oversight measures, the cross-ESAs team could provide similar benefits during the planning of the oversight measures.
It should be noted that the competences and tasks of Lead Overseer and the JET would remain unchanged and the cross-ESAs team would not be involved in activities attributed to the JET, such as on-site inspections.
Indeed, the key change would be to establish that, when determining oversight measures, cross-sectoral coordination amongst all ESAs should be pursued and the Lead Overseer should take into consideration the risks posed by the critical ICT TPP to financial entities in all sectors.

Q.2 - Would MS support the following addition?

Article 29(a) Cross-ESAs team

1. A permanent cross-ESAs team with dedicated staff members from ESAs shall be set up to support and assist the work of the Lead Overseer in relation to the management of the oversight framework.
2. The cross-ESAs team shall support the Lead Overseer in the execution of the following tasks:
i) the follow up activities according to paragraph Article 28(5a) following the Lead Overseer notification to a ICT third-party service provider of the outcome of the assessment defined at Article 28(2);
ii) the assessment of the request submitted to the Lead Overseer in accordance with paragraph Article 28(8) by ICT third party service providers that are not included in the list referred to in Article 28(6);
iii) the tasks assigned to the Lead Overseer by in accordance with paragraphs 1 to 3 of Article 30;
iv) the drafting of the recommendations referred to in Article 31(1)d);
v) the assessment of the relevant information and documentation requested to the critical ICT third-party service provider according to Article 32;

3. Sectorial approach on credit, payment, e-money institutions and AISPs

1 – Exempted payment institutions (PIs) and e-money institutions (EMIs)

In the comments to PCP4, one MS referred that PIs and EMIs locally exempted from PSD2 and EMD2, respectively, are already out of the scope of DORA since the definitions of PIs and EMIs under DORA imply that they are authorised under PSD2 /EMD2. In this MS view, PSD2/EMD2 foresee an exemption from the authorization process and, consequently, these exempted entities are not subject to the EU passporting regime and are thus excluded from the scope of the Union Law.

The PCY would like to clarify that the exempted PIs and EMIs, referred respectively under Article 32(1) of PSD2 and Article 9 of EMD2, may (depending on the national transposition of said Directives) be exempted from the application of all or part of the requirements of the respective Directives, meaning that they will not necessarily be exempted from authorisation.

Additionally, the PCY would like to clarify that all locally exempted PIs and EMIs (even if exempted from authorisation) have to deal with ICT risk. In addition, in principle, they have to comply with some PSD2/EMD2 requirements and are required to have a CA designated in accordance with Article 22 of PSD2.

Given the above, the PCY would like to present two options to MS on how to treat PIs and EMIs locally exempted under PSD2/EMD2 in DORA:

Q.1 – What is MS preferred option to clarify the issues described above?

Option 1: Adding PIs and EMIs locally exempted, referred respectively under Article 32(1) of PSD2 and Article 9 of EMD2, to the scope of DORA (Article 2), ensuring that even those PIs/EMIs that are exempted from authorisation under PSD2/EMD2, but are subject to supervision, are subject to DORA requirements. In addition, adding also the following recital:

(33a) Payment institutions and e-money institutions exempted as referred to in Article 32(1) of Directive (EU) 2015/2366 and Article 9(1) of Directive 2009/110/EC, respectively, should be included in the scope of this Regulation even if they have not been granted authorisation in accordance with Article 11 of Directive (EU) 2015/2366 to provide and execute payment services throughout the Union or if they have not been granted authorisation under Title II of Directive 2009/110/EC to issue electronic money, respectively.

Article 2 – Personal scope

"(b) payment institutions***, including payment institutions exempted in accordance with Article 32 (1) of Directive (EU) 2015/2366,***

(c) electronic money institutions***, including electronic money institutions exempted in accordance with Article 9 (1) of Directive 2009/110/EC,***"

Option 1 would imply that all PIs and EMIs locally exempted from PSD2/EMD2, even those exempted from authorisation but still subject to supervision under the respective Directives, are subject to DORA under the sectorial proportionality approach (i.e. subject to Article 14a).

Option 2: Adding PIs and EMIs locally exempted, referred respectively under Article 32(1) of PSD2 and Article 9 of EMD2, to the scope of DORA (Article 2) and clarifying, both in Article 2 and recitals, that those exempted from authorisation under PSD2/EMD2 are out of the scope of DORA.

(33a) Payment institutions and e-money institutions exempted in accordance with Article 32(1) of Directive (EU) 2015/2366 and Article 9(1) of Directive 2009/110/EC, respectively, are included in the scope of this Regulation except if they have not been granted authorisation in accordance with Article 11 of Directive (EU) 2015/2366 to provide and execute payment services throughout the Union or if they have not been granted authorisation under Title II of Directive 2009/110/EC to issue electronic money, respectively.

Article 2 – Personal scope

"(b) payment institutions***, including payment institutions exempted in accordance with Article 32 (1) of Directive (EU) 2015/2366, except if they have not been granted authorisation in accordance with Article 11 of Directive (EU) 2015/2366,***

(c) electronic money institutions***, including electronic money institutions exempted in accordance with Article 9 (1) of Directive 2009/110/EC, except if they have not been granted authorisation under Title II of Directive 2009/110/EC***"

Option 2 would imply that PIs/EMIs with an ICT risk profile similar to other PIs/EMIs, subject to supervision by a PSD2/EMD2 CA, would not be subject to DORA just because they are exempted from authorisation under PSD2/EMD2.

2- Competent authorities for AISPs and exempted credit, payment and e-money institutions (Article 41)

With the introduction in the scope of DORA of new types of financial entities taking into account sectoral exemptions, some MS questioned who will be the CA, under DORA, for these entities, namely accordingly to Article 41.
For credit institutions, the referred exemption excludes them from the scope of application of the Directive, and thus there is no designated authority under that Directive - neither under DORA, by consequence.
For exempted payment institutions and electronic money institutions, the issue is rather related to the fact that in PSD2/EMD2 they are treated as PIs/EMIs but not *per se* payment service providers, as referred to in Article 41(b), and therefore clarification on their respective CA under DORA could be beneficial. Furthermore, with the inclusion of AISPs in the scope of DORA, it should also be clarified that their CA for DORA purposes is the one defined in Article 41(b).
The Presidency believes the question is worth discussing and thus would like to know MS views on the following:

Q.2 - Would MS support the following clarification regarding the CA for credit institutions exempted by Directive 2013/36/EU?

Article 41 - "*(a) for credit institutions~~,~~:*

i) the competent authority designated in accordance with Article 4 of Directive 2013/36/EU~~,~~ including for credit institutions exempted by Directive 2013/36/EU;

ii) in the case of credit institutions classified as significant, in accordance with Article 6(4) of Regulation (EU) No 1024/2013, the ECB in accordance with the powers and tasks conferred by Regulation (EU) No 1024/2013~~,~~.

Q.3 - Would MS support the following clarification, both in recitals and in Article 41, regarding the CA for exempted PIs/EMIs and AISPs?

In addition to the recital proposed in **Q1**, adding the following paragraph:

(33a) (…) The competent authority for payment institutions exempted by Directive (EU) 2015/2366, electronic money institutions exempted by Directive 2009/110/EC and account information service providers as referred to in Article 33(1) of Directive (EU) 2015/2366, is the one designated in accordance with Article 22 of Directive (EU) 2015/2366.

Article 41 – "(b) for payment service providers*, payment institutions exempted by Directive (EU) 2015/2366, electronic money institutions exempted by Directive 2009/110/EC and account information service providers as referred to in Article 33(1) of Directive (EU) 2015/2366,* the competent authority designated in accordance with Article 22 of Directive (EU) 2015/2366;"

Additionally, the Presidency would like to raise MS attention to another topic in this regard.

Article 41(c) intends to designate the CA for EMIs. However, EMIs are also payment service providers, already mentioned under Article 41(b). In addition, EMIs CA is designated by Article 22 of Directive (EU) 2015/2366 (according to Article 3 of Directive 2009/110/EC) and therefore, its CA is already designated under Article 41(b). Taking this into account, the presidency proposes to delete Article 41(c).

Q.4 - Would MS agree with the deletion of Article 41(c)?