European Association of CCP Clearing Houses

EACH Response to the ESAs' consultation paper on Draft RTS to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554

September 2023

European Association of CCP Clearing Houses AISBL (EACH), Avenue des Arts 6, 1210 Brussels

Introduction

The European Association of CCP Clearing Houses (EACH) represents the interests of Central Counterparties (CCPs) in Europe since 1992. CCPs are financial market infrastructures that significantly contribute to safer, more efficient and transparent global financial markets. EACH currently has 19 members from 15 different European countries. EACH is registered in the European Union Transparency Register with number 36897011311-96.

EACH appreciates the opportunity to provide feedback to the consultation paper on Draft Regulatory Technical Standards to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554[1].

Questions

Question 1: Are the articles 1 and 2 regarding the application of proportionality and the level of application appropriate and sufficiently clear?

We **support the recognition within Article 1** of the proposed RTS that there is a **difference in risk profile between a third-party provider and an intra-group provider**. As noted **within recital 31 of DORA[2]**, *"when ICT services are provided from within the same financial group, financial entities might have a higher level of control over intra-group providers, which ought to be taken into account in the overall risk assessment"*.

However, we would kindly request to better clarify:

- The fact that a ***consistent* application of proportionality principle is required**, as the detailed requirements indicated are very specific to be suitable for the application of a proportionality principle.
- What the ESAs precisely **mean with *"location"***.

Question 2: Is article 3 regarding the governance arrangements appropriate and sufficiently clear?

The establishment of **multi-vendor strategies can be used in individual cases** to mitigate the risks of individual outsourcing. However, we believe that the **full implementation would not be successful in terms of risk reduction**, despite exorbitant financial commitment.

[1] https://www.esma.europa.eu/sites/default/files/2023-06/CP_-_Draft_RTS_on_policy_on_the_use_of_ICT_services_regarding_CI_functions.pdf

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554&qid=1694432731023

This thesis is based primarily on the following scenarios:

1. The **range of applications is distributed across the entire manufacturing depth** (IaaS to SaaS) and increases complexity compared to traditional IT systems:
    - IaaS and PaaS-based applications can be designed to be multi-vendor-enabled through smart architectural choices;
    - SaaS service, on the other hand, can only be relocated via migrations;
    - A multi-cloud strategy therefore primarily pursues the goal of distributing risk across multiple vendors.
2. The **multi-vendor strategy cannot address geographical and political concentration**:
    - Hyperscalers are currently exclusively US-American suppliers;
    - Functionally comparable offers can only be consumed by Chinese service providers;
    - There are no European providers above IaaS that offer internationally competitive PaaS and SaaS.

For these reasons, the **multi-vendor strategy should not be manifested as a comprehensive and mandatory part of DORA and the upcoming RTS**. Whether it is an effective approach against resilience, availability, and vendor lock-in etc. should be decided by the respective organization, and it should be taken into account that the monetary implications of multi-vendor-strategies in all its aspects are usually underestimated, hence a positive business case would be impossible and as a result public adoption is hampered. **An obligation should therefore, in our opinion, be avoided.**

We also notice that **Articles 3(8), 9(2) and 10** each require that ICT services need to be subject to "independent review" and included in the audit plan. However, we have identified two issues:

- it is not clear if internal audit would qualify as an "independent review" or if a third party would need to conduct such an audit, which would imply considerable costs;
- there is no indication on the frequency that such review needs to be done.

We would therefore **kindly request clarification** in this regard.

Furthermore, **Article 3(5)** mandated financial entities to assess whether and how the third-party provider has allocated sufficient resources to comply with all legal and regulatory requirements. This however **fails to recognize the difficulties facing financial entities in going beyond a third party's assurances**. We suggest the wording is amended as follows: *"Without prejudice to the final responsibility of the financial entity to effectively oversee relevant contractual arrangements, the policy referred to in paragraph 1 shall foresee that the financial entity* ***has sought assurances*** ~~***assesses***~~ *that the ICT third party service provider* ***does not endanger*** ~~***has sufficient resources to ensure that***~~ *the financial entity* ***to complyies*** *with all its legal and regulatory requirements".*

We also note that the **proposed RTS do not make direct reference to other incoming DORA provisions**, for example the Register of Information under Article 3(3). We would like to express our concern towards the fact that the **ICT policy would end up being duplicative**, in the event that firms are unable to point towards and leverage other processes.

Question 3: Is article 4 appropriate and sufficiently clear?

We would like to kindly recommend **removing the inclusion of subcontractors within Article 4**. First of all, financial entities may struggle in practice to obtain all the relevant information and, secondly, subcontracting is already addressed under DORA Article 30, with a separate draft RTS[3] to provide further information on the conditions which should be attached to subcontracting of services relating to critical and important services. To avoid confusion and unnecessary overlap, we advise **amending Article 4(1) as follows**: *"[…] the policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers shall differentiate~~, including for sub-contractors,~~ between: […]"*.

Question 4: Is article 5 appropriate and sufficiently clear?

Concerning **Article 5**, we have no objections but would nevertheless kindly require **clarity that the requirements are only for all ICT services supporting critical or important functions**. Also, subject to the assumption that there is only an expectation on firms to seek fresh/renewed management body approval for previously approved contractual arrangements or changes as permitted by the contractual arrangement, for example changing a subcontractor, where this is warranted on a risk-based approach.

This raises a related broader point, on **how financial entities must renegotiate existing contractual arrangements with third-party providers** to incorporate the contractual provisions set out within DORA Article 30. While we recognize the provisions themselves are not within the scope of this consultation, we flag that some tech providers may be reticent to agree with all the required contractual terms, leading to extended renegotiation timelines, which could be challenging within the implementation period. One potential way to address this could be the **adoption of a grace period for the renegotiation of legacy contracts**, allowing these provisions to be implemented as contracts mature and come up for renegotiation.

Question 5: Are articles 6 and 7 appropriate and sufficiently clear?

The **risk assessment under Article 6 aligns with the existing requirements under paragraph 68 of the EBA Outsourcing Guidelines**[4]. Confirmation is though sought on

[3] *5. The ESAs shall, through the Joint Committee, develop draft regulatory technical standards to specify further the elements referred to in paragraph 2, point (a), which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions*

[4] https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1

whether the existing risk assessment can be relied upon for the purposes of DORA. We are in fact of the opinion that there should be no expectation on firms to operationally establish a separate risk assessment, or to put in place a sub-set of metrics specifically aimed at ICT services

We also would like to kindly flag the following issues:

- **Article 7(1e)** requires financial entities to assess whether the ICT-service provider *"acts in an ethical and socially responsible manner and adheres to human and children's rights, applicable principles on environmental protection, and ensures appropriate working conditions including the prohibition of child labour"*. We would like to point out that CCPs, because of their nature focused on providing clearing services to their members, **do not have exposure to human rights and environmental law violations. The requirements included in Article 7(1e) appears therefore out of the scope of CCP activities**.
- **Article 7(2)** requires that a risk assessment be done at group level on the ICT Services and the ICT provider. This requirements appears however very broad for a large groups like those some CCPs belong to. The current wording of this proposed RTS broadens the scope of DORA Level 1 to include group level considerations and appears to apply to non-EU parents as well. We would therefore kindly **recommend providing a clarification that this does not apply to entities outside of the EU**.

Question 6: Is article 8 appropriate and sufficiently clear?

Article 8(2) requires that intra-group ICT providers have to be on arms' length terms. We would like to flag that this is not normally the way intra-group matters work and would respectfully **recommend deleting this provision unless there are specific terms that need to be on fully arms' length terms**.

Question 7: Is article 9 appropriate and sufficiently clear?

We understand that the policy on use of ICT services supporting critical and important functions is to be read as an extension of the provisions on contractual arrangements, as set out within DORA Article 30. While this approach does work across most of the proposed RTS, there is **duplication when adopting such an approach with regards to Article 9, in particular between Article 9(2) of the proposed RTS and Articles 30(2d) and 30(3c), (d) & (e) of DORA**. The current partial overlap has also created uncertainty as to why the ESAs have doubly focused on auditing provisions, as opposed to any of the other contractual provisions listed within Article 30.

Due to unequal negotiation power regarding contractual terms on the cloud services use, there may be difficulty to implement some of these requirements in practice.

In regard to the selection of **Option A for the Policy Issue 7 on contractual clauses**, we would like to highlight the **difficulty that ICT service providers of standard IT services** (e.g., hardware maintenance, software development tools, etc.) may encounter to implement this requirement.

Question 8: Is article 10 appropriate and sufficiently clear?

Article 10(1) currently states that "*The policy [on monitoring of the contractual arrangements] should also specify measures that apply when service levels are not met including, where appropriate penalties".* The use of the **word "penalty" does not appear appropriate in this context and should be replaced with "measures"**: "penalty" would indeed be more appropriate for a supervisory authority.

Question 9: Is article 11 appropriate and sufficiently clear?

When considering the exit and termination of contractual arrangements for the use of ICT services supporting critical or important functions, as outlined in **Article 11, we support and agree with the exit plan periodic review requirement**. However, we emphasize that the **periodic testing of the exit plan would be hardly feasible from an execution perspective** (i.e., conducting the actual testing and not only analyzing if testing is still possible).
Moreover, considering the statements made in Policy issue 3, item 27, for existing contracts where such exit plans do not already exist, we suggest that a **certain adjustment period shall be granted in order to establish and implement those required exit plans**.

We also would like to flag that, **in certain areas of the digital services market, there are in practice few or at times no feasible alternatives**. The related exit plan could therefore amount to a firm ceasing the service completely, given it is unlikely they will be able to provide such services in-house. We encourage **supervisors to take this into account when reviewing the exit plans developed by financial entities**.

Finally, regarding **cloud service providers**, we do **not believe it is it a realistic requirement to periodically test exit plans** as scenarios for exit can be multiple and several of those would require an active contractual arrangement with another ICT service provider (it would mean that every solution needs to have a developed and testable alternative solution). It is also **not precisely clear**, in our opinion, **what the requirements regarding the timeframe for exit plan are under this Article.**