EFAMA
European Fund and Asset Management Association

CONSULTATION RESPONSE

Brussels, 4 March 2024

EFAMA response to the Consultation Paper on draft regulatory technical standards on subcontracting of ICT services supporting critical or important functions.

General remarks

EFAMA, the voice of European investment management industry, has long recognised the importance of operational resilience in the financial market and supported the introduction of a framework that would foster cybersecurity across sectors. At the same time, since the beginning of these discussions, we have highlighted a need for an approach which would not pose challenges to firms' divergent organisational arrangements, nor impose barriers to growth and innovation by setting the bar too high, in particular for smaller entities or those that do not provide critical IT infrastructure. This approach emanates from the principle of proportionality being widely applied to the provisions of DORA[1] by virtue of its Art. 4.

In our response to this Draft RTS[2], we would:

- Draw the ESAs' attention in particular to the proper and comprehensive incorporation of the proportionality principle as established in Art. 4(2) of DORA,
- Question the mandate and rationale behind the obligation to monitor the entire ICT subcontracting chain, including through the review of contractual arrangements,
- Question the ESAs' assessment that the costs and overall effort involved in implementing the RTS are low, and
- Call for standard contractual clauses to be developed at EU level in cooperation with the financial industry.

[1] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance)(DORA) .

[2] ESAs, Consultation Paper on Draft Regulatory Technical Standards to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Article 30(5) of Regulation (EU) 2022/2554 (Draft RTS).

Rue Marie-Thérèse 11 | B-1000 Bruxelles | T +32 2 513 39 69 | info@efama.org | www.efama.org | EU transparency register: 3373670692-24

Response to the ESAs' Questionnaire

Q1: Are articles 1 and 2 appropriate and sufficiently clear?

☐ Yes

☒ No

Q1b: Please provide your reasoning and suggested changes.

According to Art. 4(2) of DORA, the application by financial entities of Section I in Chapter V od DORA "*shall be proportionate to their size and overall risk profile, and to the nature and complexity of their services, activities and operations (...)*". Article 30(5) of DORA, which establishes the mandate for the ESAs to develop this Draft RTS, is included in Section I in Chapter V of DORA. Nevertheless, in EFAMA's opinion, the principle of proportionality was not reflected comprehensively in the provisions on the assessment of subcontracting ICT services.

Article 1 of the Draft RTS provides a list of elements that shall be taken into account by financial entities, and which speak of increased or reduced risks. They, however, do not refer to all the characteristics of the entity described in Art. 4(2) of DORA. They concentrate exclusively on the properties of the ICT subcontractor or the ICT service. We believe that the other elements such as size, overall risk profile of the financial entity etc. should also be taken into consideration and embedded not only in Art. 1 but in the whole Draft RTS.

EFAMA is also of the opinion that the elements included already in the Art. 1 do not have a sufficient influence on the obligations vested upon financial entities in Art. 2-7 of the Draft RTS. In our opinion, the analysis conducted by the financial entity should have a much broader impact, allowing entities for which it is justified to adhere to simplified rules or to limit the scope of obligations to the elements that are relevant to their situation. Otherwise, a question would arise whether the principle of proportionality was applied in preparing the Draft RTS.

We would also like to highlight that this Draft RTS would bring a significant change to the existing practice of subcontracting, as based on the sector-specific outsourcing and delegation rules and further explained in the ESMA Guidelines on outsourcing to cloud service providers[3] and EBA Guidelines on outsourcing arrangements[4]. As will be described in responses to Questions no. 2 and 4, we challenge the proposed approach which significantly shifts the weight of obligations from ICT TPPs to financial entities. We question whether it will lead to the best outcome in terms of the selection of subcontractors and their oversight, and whether it justifies the additional workload and expenditure that financial entities will have to bear.

To comment on Art. 1 of the Draft RTS in more detail, we would like to highlight that letter (f), which addresses the issue of transferability, covers only the relocation of the ICT service to another ICT TPP, leaving out the possibility of this service being moved to the financial entity itself. For example, in case of an incident, it is often also possible to support some services "in house", and that option should also be recognised in the Draft RTS.

Moreover, even though the aim of the Draft RTS is to specify issues around subcontracting, Art. 1(f) refers only to the transferability of the ICT service supporting critical or important functions in its entirety. EFAMA is of the opinion that, to properly assess elements of increased or reduced risks in case of subcontracting, the transferability of the subcontracted service to another subcontractor should also be taken into account. This is also the case for Art. 1(g) of the Draft RTS, where only the impact of disruptions on services provided

[3] ESMA, Guidelines On outsourcing to cloud service providers, 10 May 2021.
[4] EBA, EBA BS 2019 xxx (EBA Draft Guidelines on outsourcing arrangements).docx (europa.eu), 25 February 2019.

by the ICT TPP is to be analysed. We are of the opinion that the impact of disruptions on the part of the service that is subcontracted could also be taken into account.

Q2: Is article 3 appropriate and sufficiently clear?

☐ Yes

☒ No

Q2b: Please provide your reasoning and suggested changes.

We would refer to the response to Question no. 1 and the need to thoroughly implement the principle of proportionality into the Draft RTS. We are of the opinion that all elements listed in Art. 3 should be assessed in accordance with Art. 4(2) of DORA. Therefore, the fulfillment of particular obligations should be subject to the condition "where appropriate".

We would also caution against the proposed radical shift from ICT TPP to financial entities when it comes to the assessment of possible subcontractors. We are of the opinion that this is and should remain the primary obligation and responsibility of the direct ICT TPP. Through their immediate contractual arrangements, the direct ICT TPPs are much more capable to control and demand certain actions from subcontractors. A proposed transfer of due diligence obligations to financial entities may in fact create a notion of relieving ICT TPPs from their responsibilities, which would be counterproductive to the objectives of DORA.

For example, the obligation of the financial entity to assess whether the relevant clauses of the contractual arrangements between the financial entity and the ICT TPP are replicated as appropriate in the subcontracting arrangements (Art. 3(1)(c) of the Draft RTS) should remain the responsibility of the direct ICT TPP. For this obligation to be exercised by the financial entity, it would require the entity to analyse the contractual arrangements between ICT TPP and its subcontractors, which we believe would be excessively burdensome. We would suggest this obligation to be deleted from Art. 3 of the Draft RTS and instead be included as one of the conditions for subcontracting, which the ICT TPP is obliged to fulfill under Art. 4 of the Draft RTS.

Q3: Is article 4 appropriate and sufficiently clear?

☐ Yes

☒ No

Q3b: Please provide your reasoning and suggested changes.

EFAMA would like to comment in particular on the Art. 4(f) of the Draft RTS, which regards the obligation of the ICT TPP to ensure the continuous provision of ICT services, even in case of failure by the subcontractor, to meet its service levels or any other contractual obligations. The way this provision was phrased suggests the need for back-up options that would replace the service provided by one subcontractor with another and on a one-to-one basis. We are of the opinion that the security of operations, even critical or important ones, can be also reached on a comparable level of service, especially on an interim basis. Therefore, we deem it sufficient to refer to the level of service agreed between the financial entity and ICT TPP, or an obligation to provide suitable contingency measures.

Moreover, according to our understanding, Art. 4 of the Draft RTS lists elements which must be included in the contractual arrangement between the financial entity and the direct ICT TPP for the subcontracting of critical or important functions to be possible. As the financial entity does not have a direct contractual relationship with subcontractors, any obligations can be imposed on them only by the direct ICT TPP and not by the financial entity. Therefore, we would suggest for the wording in Art. 4(i) of the Draft RTS to be amended in order to express directly that this is the obligation of the ICT TPP:

"*i) that **the ICT third-party service provider is required to ensure that the** subcontractor shall grant to the financial entity and relevant competent and resolution authorities at least the same audit, information and access rights as granted to the financial entity and relevant competent authorities by the ICT third-party service provider;*"

Q4: Is article 5 appropriate and sufficiently clear?

☐ Yes

☒ No

Q4b: Please provide your reasoning and suggested changes.

EFAMA is strongly against the obligation of the financial entity to monitor the ICT subcontracting chain, as proposed in Art. 5 of the Draft RTS. Firstly, we would like to highlight that this obligation goes beyond the ESAs' mandate established in Art. 30(5) of DORA. It is clearly provided there, that the aim of the draft RTS to be developed by the ESAs is to further specify elements referred to in Art. 30(2)(a). To recall, Art. 30(2) of DORA specifies elements of contractual arrangement on the use of ICT services, with the letter (a) concentrating on the description of those services, whether they can be subcontracted, and the conditions of said subcontracting. We are of the opinion that the monitoring established in Art. 5 of the Draft RTS, creates an entirely new obligation of the financial entity, which is outside of the scope of the contractual arrangement with the ICT TPP. If such monitoring obligation was intended by EU policymakers, it should have been established in the provisions of DORA. It was, however, not included in Art. 30 of DORA, even though paragraph 3(e) refers specifically to financial entities' right to monitor the ICT TPP's performance. We also do not find ground for this obligation in other provisions of DORA, including Art. 28(3) and (9) which mandate the ESAs to develop an ITS to establish templates for the purpose of the register of information in relation to contractual arrangements.

Secondly, this obligation would bring a significant change to the existing practice, which was based on the existing sector-specific outsourcing and delegation rules, which were further explained in the ESMA Guidelines on outsourcing to cloud service providers[5] and EBA Guidelines on outsourcing arrangements[6]. Both documents oblige only the cloud service provider or the service provider to monitor the subcontractor, and not the financial entity. As a result, monitoring of a subcontractor by a financial entity is not included in currently binding contractual arrangements and would require conducting a review of every one of them.

Moreover, as the obligation of the direct ICT TPP to monitor its subcontractors is already included in Art. 4(e) of the Draft RTS, imposing it also on financial entities, that do not have a direct contractual arrangement with the subcontractor, seems duplicative and excessive. Therefore, we would call for the removal of Art. 5 from the Draft RTS.

[5] ESMA, Guidelines On outsourcing to cloud service providers, 10 May 2021.
[6] EBA, EBA BS 2019 xxx (EBA Draft Guidelines on outsourcing arrangements).docx (europa.eu), 25 February 2019.

The enforcement of the monitoring obligation is also practically impossible as it requires monitoring of the entire ICT subcontracting chain and conditions, including through the review of contractual arrangements, which also doesn't follow the principle of proportionality, as described in Art. 4(2) of DORA.

Q5: Are articles 6 and 7 appropriate and sufficiently clear?

☐ Yes

☒ No

Q5b: Please provide your reasoning and suggested changes.

Firstly, EFAMA would like to highlight that Art. 4 of the Draft RTS, which stipulates the conditions for subcontracting, does not include any rules on the direct ICT TPP dealing with material changes, as provided further in Art. 6 and 7 of the Draft RTS. Lack thereof might be an impediment to the further enforcement of said requirements.

Secondly, we are of the opinion that Art. 6(2) of the Draft RTS, which includes the obligation to inform the ICT TPP of the risk assessment results done by financial entity on the planned material changes to the subcontracting arrangements, should be deleted. We believe it is repetitive and point 4 of Art. 6 regulates this issue in a clear enough way.

We are also of the opinion that Art. 6(3) addresses the same issue as Art. 7 of the Draft RTS and therefore is also of a repetitive nature.

Q6: Do you have any further comment you would like to share?

EFAMA would like to share its impression that the limitation of the Draft RTS to cases of subcontracting of ICT critical, or of other important functions, is not comprehensively reflected throughout the entire document. In particular, Art. 1 does not refer at all to these types of ICT services. It also seems that Art. 7 would have a broader effect.

We also strongly disagree with the ESAs assessment that the costs and overall effort involved in implementing the RTS are low. We see significant amendments to the contractual arrangements to be negotiated and a much broader scope of monitoring of ICT services, which would result in the need for extra staff and higher costs, to name the few.

In order to reduce the burden and costs of amending the contractual arrangements with ICT TPPs, it would be beneficial if standard contractual clauses were developed at EU level, as already foreseen in Art. 30(4) of DORA. This would strengthen the bargaining power of financial entities in negotiations with ICT TPPs. To guarantee the best outcome, said clauses should be developed in cooperation with the financial industry.

*****

ABOUT EFAMA

EFAMA is the voice of the European investment management industry, which manages about 28.5 trillion of assets on behalf of its clients in Europe and around the world. We advocate for a regulatory environment that supports our industry's crucial role in steering capital towards investments for a sustainable future and providing long-term value for investors.

Besides fostering a Capital Markets Union, consumer empowerment and sustainable finance in Europe, we also support open and well-functioning global capital markets and engage with international standard setters and relevant third-country authorities. EFAMA is a primary source of industry statistical data and issues regular publications, including Market Insights and the EFAMA Fact Book.

More information is available at www.efama.org

Contact:

Zuzanna Bogusz
Regulatory Policy Advisor
zuzanna.bogusz@efama.org | +32 456 16 58 67