Contribution ID: 7fd0b581-dee7-4670-83e6-b5846d44d0ba
Date: 04/03/2024 14:59:14

Public consultation 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

Fields marked with * are mandatory.

Intorduction

The European Supervisory Authorities (EBA, EIOPA and ESMA) have published the second batch of Consultation Papers on the mandates stemming from the Digital Operational Resilience Act (DORA) with the aim to collect market participants' feedback on the proposed 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.

Market participants are invited to provide their feedback to the draft technical standards by responding to the questions presented in this consultation paper.

The feedback received will be taken into account in the finalisation of the draft technical standards, which are due to be submitted to the European Commission by 17 July 2024.

Comments are most helpful if they:

- respond to the questions stated;
- indicate the specific point to which a comment relates; contain a clear rationale;
- provide evidence (including relevant data, where applicable) to support the views expressed;
- reflect a cross-sectoral (banking, insurance, markets and securities) approach, to the extent possible;
- and describe any alternative approaches the ESAs could consider.

To submit your comments, please click on the blue "Submit" button in the last part of the present survey. Please note that comments submitted after 4 March 2024 or submitted via other means may

not be processed.

Please clearly express in the consultation form if you wish your comments to be published or to be treated as confidential. A confidential response may be requested from the ESAs in accordance with the ESAs' rules on public access to documents. We may consult you if we receive such a request.

Any decision we make not to disclose the response is reviewable by the ESAs' Boards of Appeal and the European Ombudsman.

The protection of individuals with regard to the processing of personal data by the ESAs is based on Regulation (EU) 1725/2018 of the European Parliament and of the Council of 23 October 2018. Further information on data protection can be found under the Legal notice section of the ESA websites.

General Information

* Name of the Reporting Stakeholder

European Association of Public Banks

Legal Entity Identifier (LEI), if available

* Type of Reporting Organisation

- ( ) ICT Third-Party Service Provider
- ( ) Financial Entity
- (•) Industry Association/Federation
- ( ) Consumer Protection Association
- ( ) Competent Authority
- ( ) Other

* Financial Sector

- [x] Banking and payments
- [ ] Insurance
- [ ] Markets and securities
- [ ] Other

Jurisdiction of Establishment

Belgium

* Geographical Scope of Business

- ( ) EU domestic
- (•) Eu cross-border
- ( ) Third-country

- [ ] Worldwide (EU and third-country)

* Name of Point of Contact

Mathilde Pradeau

* Email Address of Point of Contact

mathilde.pradeau@eapb.eu

* Please provide your explicit consent for the publication of your response.

- [x] Yes, publish my response
- [ ] No, please treat my response as confidential

Questions

Question 1. Are articles 1 and 2 appropriate and sufficiently clear?

- [ ] Yes
- [x] No

* 1b. Please provide your reasoning and suggested changes.

Article 1 introduces proportionality based on features of the ICT third-part service provider, not on features of the financial entity. Proportionality at that level also makes sense.
With respect to the elements of increased or reduced risk, we would like to add the criterion whether the ICT third-party service provider is critical or not. Critical ICT third-party service providers are subject to the oversight framework. Being subject to the oversight framework informs the level of risk. More general, industry risk reducing measures such as certification are elements to be taken into account by financial entities while assessing the risk.
Moreover, Article 1 is not specific enough to understand how certain risk aspects should be applied to Articles 2-7.It would therefore be desirable to specify how points a) to i) are to be implemented in practice.
Article 2 requires clarification regarding the geographical scope. In particular whether subsidiaries in non-EU but EFTA or EEA members are concerned as well.

Question 2. Is article 3 appropriate and sufficiently clear?

- [ ] Yes
- [x] No

* 2b. Please provide your reasoning and suggested changes.

No, article 3 is not sufficiently clear.

Proportionality: No explicit proportionate and risk-based approach is applied in the RTS. The ESAs assume that: (i) all ICT services that support critical or important functions have the same level of risk (or importance) to a FE; and (ii) all subcontractors associated with an ICT service that supports a critical or important function, or supports material parts of it, are considered equivalent,
regardless of their role and potential impact on the provision of the services. Monitor the material risks of subcontractors whose disruption or failure could lead to a material impact on the provision of services.
Re Art. 3 (1):
c) Passing on the contractual conditions to the subcontractors is problematic. Proposed amendment: Check that the use of subcontractors does not impair or hinder the ICT service provider's compliance with its contractual obligations towards the FE.
e) Delete this point: This leads to a disproportionately high level of complexity at the FE for sometimes very specialized tasks. Alternatively, external audit certificates from auditors or the results of pool audits should be accepted as sufficient evidence.

Question 3. Is article 4 appropriate and sufficiently clear?

- ○ Yes
- ◉ No

* 3b. Please provide your reasoning and suggested changes.

Article 4: Implementation must be contractually agreed between the financial entity and the ICT TPP. In some cases, some points may not be fulfilled by the subcontractor in accordance with the contract: Termination of the contract with the ICT TPP solely due to individual problems with some subcontractors has huge consequences for the financial institution. Short-term implementation is not possible, for example, due to a lack of alternatives or very expensive exit plans. In these cases, risk assumption should be permitted on the basis of a risk assessment.
b) It is not clear which obligations regarding the monitoring and reporting by ICT service providers the article refers to. If this is linked to another section of this RTS or possibly referring to contractual obligations, it should be stated.

f) A completely uninterrupted provision of services will not be possible in all cases and is not absolutely necessary. Instead of "to ensure the continuous provision ...", it should read "to ensure the provision of ICT services without disruption".
g) The plans themselves cannot and must not be passed on to the subcontractor. The service level requirements from the contingency plans relevant to the UAN should be passed on, see EBA Outsourcing Guidelines, 75 g, i and l.

h) is the complete requirement for the highest security standards pursuant to Art. 28.5 DORA meant? The chain of references is not entirely clear, as only a general reference is made to Art. 28.10 DORA (and thus indirectly to Art. 7.1.a RTS 28.10 "Information security standard"). We recommend a risk-oriented assessment option for the security requirement.
i) The word "at least" is not comprehensible. Why should the FE require more extensive audit and access rights for the subcontractor than for the ICT service provider itself? We recommend deleting "at least".

Question 4. Is article 5 appropriate and sufficiently clear?

- ○ Yes

- [x] No

* 4b. Please provide your reasoning and suggested changes.

Article 5 is neither appropriate nor sufficiently clear. Monitoring the supply chain is not sufficiently defined in this context. It should at least be stipulated that it exclusively concerns the subcontractors who provide the essential part of the services. It is difficult to document the entire chain of subcontractors. In addition, it is already adequately regulated in EBA guidelines. Finally, reporting efforts should not be unnecessarily increased by the financial institution keeping unnecessary records with all possible subcontractors. The disclosure of contracts with subcontractors is neither necessary nor practicable. The contract details are subject to confidentiality and are not made available by ICT third-party service provider. These may contain content that cannot be shown to financial institutions. Disclosure also requires the consent of the subcontractor and this cannot be contractually guaranteed with ICT third-party service provider.
Article 5.1: As there is no direct contractual relationship between the financial entity and the subcontractor, the requirement for monitoring in this regard is not considered appropriate (requirement otherwise clearly formulated).
Article 5.2: We do not consider monitoring activities between the financial entity and the subcontractor to be feasible. In our opinion, the service provider must check or confirm compliance by means of a certificate. It is unclear where the boundary/difference to EBA-GL 2019/02 is with regards to onward transfers.

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

- [ ] Yes
- [x] No

* 5b. Please provide your reasoning and suggested changes.

Both articles are neither appropriate nor sufficiently clear. Changes in contracts with subcontractors do not lead to changes in the contractual relationship between the financial institution and ICT third-party provider. This documentation would lead to considerable effort, which would not lead to any improvement in monitoring. Only the changes referred to in the contracts with FE's ICT or if these changes lead to changes in the contractual relationship with FE’s ICT. FE’s ICT must also be informed of this. Checking all changes on suspicion that they could lead to changes in performance at all would result in disproportionate effort. The FE’s ICT should notify the changes that affect the contractual relationship and have an impact on the agreed service.
3) FE’s ICT should not be able to make any changes to the contract without the consent of the financial entity. Implementation of changes by the subcontractor are changes to the contract - therefore this rule is unnecessary.
4) See above
5) only if they result in changes to the contractual relationship with the financial entity
Article 6 should be limited to critical and important functions, analogous to Article 3.
In 6.1. a uniform definition of a "reasonable" lead time is needed. It is not clear whether that term corresponds to a notification period.

6. Do you have any further comment you would like to share?

The oversight framework for critical ICT third-party providers entrusts the ESAs with the lead oversight role, because (recital 88) "...the simultaneous carrying out of multiple audits and access rights, performed separately by numerous competent authorities…creating redundancy, burden and complexity for critical ICT third-party service providers if they were subject to numerous monitoring and inspection requests." Obviously, the same holds for all ICT third-party providers and as such in this context. It is highly likely that an ICT third-party provider is providing the same services to different financial entities. Because the RTS lays down the requirements at the level of an individual financial entity, every single financial entity has to apply the requirements to that ICT third-party provider creating redundancy, burden and complexity for ICT third-party providers. Therefore, we propose to, without undoing the individual responsibility of the financial entity, create room for cooperation between financial entities/enabling the use of third parties (e.g. (parts of) risk assessment regarding the use of subcontractors) in order to avoid redundancy, burden and complexity. The draft RTS do not distinguish between existing and new contractual arrangements. It will take time to amend the existing stock of contractual arrangements such that these are in line with the RTS. The time schedule is too tight: expected final RTS in July, applicable from January 2025. Moreover, it may be that the respective counterparties do not agree with the necessary amendments. This would necessitate the financial entity to replace the ICT third-party provider in this timeframe arguably resulting in a greater operational risk than having a not fully compliant contract. As such, we would propose to introduce transitional arrangements for existing contracts where the RTS would apply at the earlier of (i) the renewal of the contract and (b) x years from now.

Contact

Contact Form