Contribution ID: c39fc300-0599-4555-85e4-7cf4001c5deb
Date: 04/03/2024 22:14:22

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

Electronic Money Association

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

Judith Crawford

* Email Address of Point of Contact

judith.crawford@e-ma.org

* 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
- (•) No

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

We propose that the list of risk factors to be assessed by FEs in relation to the use of sub-contractors by ICT third-service providers in Art.1 of the draft RTS is expanded to consider the size (market capitalisation /financial resources, use by other FEs, international/global presence) and company profile of the ICT sub-contractor(s). We perceive these to be relevant factors that a FE should consider in its risk assessment over the potential use of an ICT sub-contractor to support the delivery of a Critical function.

Question 2. Is article 3 appropriate and sufficiently clear?

- ( ) Yes
- (•) No

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

We do not perceive the reference to “replication of the relevant clauses” in the contractual agreement between the FE and the ICT third-party service provider in the separate agreement that the ICT 3rd-party service provider establishes with sub-contractor(s) to be appropriate. The scope (and type) of services that the ICT third-party service provider receives from any subcontractor may well be very different than the services it delivers to the FE; the commercial/power relationship may also be very different. In this context, we are sceptical that the proposed condition can be enforced.

There are also already appropriate conditions included in Art. 3 (on effective monitoring of sub-contractors by the third-party ICT service providers, participation of the third-party ICT service provider in operational testing of sub-contractors etc.) to provide confidence to the financial entity on the effectiveness of the subcontractors’ controls used by a third-party ICT service provider. In this context we propose that the ESAs withdraw this condition from Art. 3(1)c of the draft RTS.

We are also concerned about the scope of the exercise of rights of audit, information and access referenced in Art. 3(1)i of the draft RTS. As stated above, the scope of services that the ICT third-party service provider receives from any subcontractor may well be very different than the services it delivers to the FE. We perceive it is not realistic to expect the ICT third-party service provider to secure rights of audit/information /access for the FE to any sub-contractor ICT assets or resources that are not involved in the delivery of sub-contracted services. We propose that the relevant qualifying language is introduced in this section of the draft RTS.

We also encourage the ESAs to afford FEs the ability to leverage sub-contractor audit reports compiled by (or on behalf) of the ICT third-party service providers to satisfy this condition.

Question 3. Is article 4 appropriate and sufficiently clear?

- ○ Yes
- ◉ No

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

We are puzzled by the requirement for contractual agreements with ICT-third party service providers to record (i) Incident responses, business continuity plans and service levels to be met by ICT sub-contractors and (ii) the ICT security standards and any additional security features to be met by the subcontractors recorded in Art. 4(g) and 4 (h) of the draft RTS.

In many instances, the FE will not be able to identify the relevant service levels/KPIs for services the ICT third-party service provider subcontracts. Such KPIs will be set by the direct customer of the subcontractor (ICT third-party service provider or even a higher-level subcontractor) and reflect its own ICT infrastructure requirements. Subcontractors are also very likely to be reticent to share details of their business continuity plans and of their security controls framework with any commercial entities that are not their direct clients.

It is more appropriate to require the FE to document in its service delivery agreement the responsibility of the ICT third-party service provider to ensure that subcontractors' security controls, BCM framework and service delivery capabilities support the delivery of outsourced services at agreed levels. In this context, we propose that these requirements are withdrawn from Art. 4 of the draft RTS.

As stated in our response to Question 2 above, we remain concerned about the scope of the exercise of rights of audit, information and access referenced in Art. 4(i) of the draft RTS. As stated above, the scope of services that the ICT third-party service provider receives from any subcontractor may be very different than the services it delivers to the FE. We perceive it is not realistic to expect the ICT third-party service provider to seek to secure identical/equivalent rights of audit/information/access to any sub-contractor ICT assets or resources that are not involved in the delivery of sub-contracted services. We propose that the relevant qualifying language is introduced in this section of the draft RTS.

Question 4. Is article 5 appropriate and sufficiently clear?

- ○ Yes
- ◉ No

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

We are concerned by the references to the FE "fully monitoring" the ICT subcontracting chain in Art. 5(1) if the draft RTS. We note the requirement for FEs to document the ICT sub-contracting chain in the relevant Register of Information. However, it not clear what further subcontractor monitoring FEs are required to carry out when they do not have a direct commercial relationship with such sub-contractors. We encourage the ESAs to provide further clarity on FE sub-contractor monitoring requirements.

Building on our comment above, we fail to understand the rationale of the requirement for FEs to review contracts established between ICT third-party service providers and sub-contractors and the KPIs listed in such contracts in Art 5(2) of the draft RTS. It is not clear why ICT third-party service providers would allow FEs to review commercially sensitive agreements established with subcontractors. As noted above, the scope of services that the ICT third-party service provider receives from any subcontractor may be much wider than the services it delivers to the FE. We propose that this requirement is removed from the draft RTS.

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

- ○ Yes
- ◉ No

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

It is not clear whether the ESAs expect the Termination triggers listed in Article 7 to be introduced in outsourcing agreements that the FEs establish with 3rd-party ICT service providers that use subcontractors to support the delivery of Critical business functions. The ESAs are encouraged to provide further clarity on this topic.

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

We encourage the ESAs to take into account “the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations” in identifying the FE management requirements of relevant sub-contractors detailed in this draft RTS per the parameters of the RTS Mandate stated in Art 28(10) of DORA.

Contact

Contact Form