Contribution ID: b320443b-3a7c-4c46-a701-71ffdc8653e8
Date: 01/03/2024 16:34:02

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

Deutsche Boerse Group

Legal Entity Identifier (LEI), if available

529900G3SW56SHYNPR95

* Type of Reporting Organisation

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

* Financial Sector

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

Jurisdiction of Establishment

Germany

* Geographical Scope of Business

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

- [ ] Worldwide (EU and third-country)

* Name of Point of Contact

Sujata Wirsching

* Email Address of Point of Contact

sujata.wirsching@deutsche-boerse.com

* 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.

The expected level of monitoring by the financial entity of subcontractors is too high, and we believe it is challenging to implement and somewhat disproportionate. We question the balance of these provisions as a lot of insight into the level of the third party's business set-up is expected of financial entities. The new provisions will shift the burden towards the financial entity where, currently, this level of responsibility is agreed on in the contract where financial entities are relying on the responsibility and liability of the third party to honor the terms of the agreement. This balance may be distorted by the severity of the Draft RTS provisions and may lead to a disbalance that does not represent the individual responsibility of the contracting parties.
Article 2 is (a) not sufficiently clear, and (b) establishes responsibilities which contradict company law.
Ad (a) it is unclear where the RTS applies "on a sub-consolidated or consolidated basis", as the RTS applies to financial entities and not groups of entities.
If the target of Article 2 is to establish responsibilities of a parent undertaking for its sub-consolidated or consolidated affiliates, this should be clearly stated, e.g. "Where this Regulation applies to financial entities which are consolidated or sub-consolidated by a parent undertaking, the parent undertaking that is responsible for providing the consolidated or sub-consolidated financial statements for the group shall ensure, that the conditions for subcontracting (…)".
The reference "where permitted" does not imply which permission is meant and is thus unclear. Is this a permission by a group entity provided to the parent undertaking (in case of outsourcing to the parent undertaking), or is this a reference to a permission of the parent undertaking to its subsidiary to allow its ICT third party service provider to use subcontractors? As the RTS only governs subcontracting, we deem the "where permitted" may be superfluous.
Ad (b) Article 2 assigns a responsibility to the consolidating parent undertaking for the consistent application of the Regulation in the ICT contracts of its consolidated subsidiaries. Ultimately this means assigning managerial liability to the directors of the parent company for the compliance of its affiliates in the field of ICT subcontracting.
This is not mandated by the first level regulation, DORA only entitles the ESA to "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." paragraph 2, point (a). Art. 30 paragraph 2 point (a) sets out certain requirements for ICT contracts and does not make any reference that may imply any assignment of responsibility to parent undertakings of a financial entity. Such assignment is neither an element of "assessment" by the financial entity, nor may the financial entity "determine" a third party a responsibility for its own actions (contract to the detriment of a third party).
In many cases the parent undertaking does not have any legal right or means to influence the day-to-day business of its subsidiary, e.g. if the subsidiary is a public listed company. Assigning legal responsibility to the parent undertaking for subsidiaries, that it cannot steer in their day-to-day business appears to be inappropriate.
It remains unclear how the elements of increased or reduced risk affect the requirements of Article 2 to 7.
We would like to point out that the principle of proportionality seems not applicable throughout the RTS.
We will provide further comments also on the connection and overlap with the ESAs' outsourcing guidelines.
Furthermore, we propose streamlining the Article by combing Article 1(b) and Article 1(i) as the combination is targeted to concentration risks.

Question 2. Is article 3 appropriate and sufficiently clear?

- ○ Yes
- ◉ No

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

a) Art 3 implies far reaching due diligence (DD) requirements to be fulfilled prior to agreeing to a subcontracting of critical/important functions. While DD requirements are important elements for an appropriate ICT risk management, as some are too far reaching. This is implied by the definition of ICT third party services (ICT TPS), which as per “RTS on the standard templates for the purposes of the register of information” has been broadened compared to the definition of “ICT Services” in Art 3 (21) DORA to also cover e.g. software licenses and ICT consulting services (no digital or data). As the definition of ICT Services covers almost every aspect of modern value chains, the DD requirements on ICT TPS and their subcontractors (SC) providing ICT services along the entire sub-outsourcing chain will increase the efforts to be invested by financial entities (FEs), will lead to a high financial impact and leave FEs as slow movers, strongly reducing their international competitiveness. To prohibit ICT TPS the use of SCs is not a viable alternative for FEs. We propose to limit the DD obligations to ICT TPS and SCs in a proportionate manner to those providing ICT services whose disruption would impair the security or the continuity of the service provision, as has been done by the ESAs in the RTS or to remove the DD requirement completely where the ICT TPS proves to have an effective system for monitoring SCs.
b) Art 3.c) requires that the TPS providing ICT services supporting critical or important functions must disclose its contracts with all its SCs. This means a breach of confidentiality obligations by the ICT TPS which are market standard in all ICT service agreements. Existing regulation requires the outsourcing regulated entity to contractually oblige the insourcer of critical/important functions to have its contracts with its SCs in line with the primary outsourcing agreement, which avoids pre-contractual disclosures of SC arrangements and thus breaches of market standard confidentiality obligations. We propose to use this approach also for DORA. The term “replicated” implies that the clauses of the primary ICT services agreement must be taken to the SC arrangements without any textual deviation on a 1:1 basis. This won't be possible in agreements with providers that already subcontracted services or provide services to many FEs – at least if the FEs use their own terms and don't rely on the terms of the ICT TPS. A replication will only be possible if the authority publishes binding standard clauses. The meaning of “as appropriate” following the term “replicated” is unclear as it could either refer to the choice of relevant clauses, the requirement to “replicate” the clauses or understood to soften the term “replicated”. We propose a wording that clearly implies that the SC arrangement should be in line with the clauses of the primary ICT service agreement and avoids the interpretation of “replicated”, e.g. “that the SC arrangements between the ICT TPS and its SC are in line with the clauses of the contractual arrangements between the FE and the ICT TPS to ensure that the FE is able to comply with its own DORA obligations".
c) It’s unlikely that ICT TPS, i.e. large TPS, will be willing to accept the involvement of the FE, as they usually offer their service to several FEs. It is unrealistic for the ICT TPS to involve all FEs in the decision-making.
d) Art 3.1.d) It will be impossible, especially for small ICT TPS, to set up the required structure as they might not have the required organisational structure e.g., an adequate internal control system to comply with requirements. Proportionality should consider the criticality of the services for the FE, that would only have an outside-in view on the ICT TPS’s abilities i.e. before conducting the contractual arrangement.
e) Art 3.1.e) It's unlikely to oversee the SC as no direct contractual agreement is in place with the SC concerning the term “possible”. It is hard to prove the oversight of the SC.
f) Art 3.1.f) ICT TPS are unlikely to share this information with the FE, which would not be extensive enough anyway to carry out an adequate assessment on the FE’s digital operational resilience. The reference to step-in-rights is unclear. Its presence in the ICT TPS SC chain is a drastic measure with far reaching consequences in case they are exercised, strong operational effects for the ICT TPS, which the FE may not be able to fully understand prior. If the RTS is meant to add an obligation to implement step-in-rights along the entire subcontracting chain, this should be made explicit in a separate subclause. It however has to be noted that the feasibility of this requirement along the ICT subcontracting chain is low if not even zero.
g) Art 3.1.i) It is unlikely that the FE will be aware of ‘any obstacle’, as ‘any’ is too broad.

Question 3. Is article 4 appropriate and sufficiently clear?

- ○ Yes
- ◉ No

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

Please consider that the financial entity has no contractual relationship of its own with the sub-outsourcing company. For this reason, the financial entity cannot directly influence the sub-outsourcing company. Furthermore, the financial entity does not know the contract between the outsourcing company and the sub-outsourcing company and cannot shape it. It can only contractually require the outsourcing company to enter into agreements with the sub-outsourcing company that serve to ensure compliance with regulatory requirements. The financial entity can only exert influence in the contractual relationship with the outsourcing company directly.
The initiative for further outsourcing does not come from the financial entity, but from the outsourcing company.
The requirement of Article 4 to describe in the written contractual arrangements which ICT services support critical or important functions and which are eligible for subcontracting including the respective preconditions may work for classic outsourcing arrangements. However, where ubiquitary cloud services are contracted, market standard agreements are frameworks that allows the use of a broad scale of cloud services, e.g. different compute instance types, storage instance types, specific software etc. These agreements are of general, framework-like architecture and are not specific to certain functions of the financial entity. Such market standard agreements provide the financial entity with the ability to use or refrain from the use of certain or all cloud services. Thus, the requirement of a specific identification of the respective ICT services provided under such agreement as supporting critical or important functions appears to be unrealistic.
Article 4 (a): It is difficult to agree on monitoring for all subcontracted ICT services. The experience showed that it is even difficult to monitor the first level of subcontracting. Especially in case of multi-tenant service providers this is not feasible.
Article 4 (c): It is in general not possible to assess all risks. ICT service providers using subsidiaries as subcontractors will not be willing to disclose all risks and to report them to the financial entity (conflicting interests)
Article 4 (e): Please refer to comment on Article 4 a). This kind of specification will hardly be possible over the outsourcing chain as no direct contractual relationship between the financial entity and the subcontractor exists. Could an annotation ‘if possible’ be added as this requirement is placed on the ICT service provider?
Article 4 (f) requires a “continuous provision of the ICT services” which implies an availability service level of 100 percent, which is not offered by any ICT provider. Article 4 (f) should rather be referencing the service levels agreed between the financial entity and the ICT third party service provider, e.g. “that the ICT third party service provided is required to ensure the provision of the ICT services supporting critical or important functions in line with the service levels it agreed with the financial entity, even in case of failure (…)”.
Article 4 (f) it is not clear how an ICT service provider can provide the service if, for example, a critical ICT sub-service provider fails. It would instead be better to formulate that emergency plans must be available for critical ICT sub-service providers.
Article 4 (g) stipulates that the agreement between the financial entity and the ICT third party service provider shall specify the service levels that each and any ICT subcontractor in the subcontracting chain shall meet. Given the complexity of subcontracting chains in the ICT industry, a financial entity will not be able to fulfill this requirement without suffering an unproportionate burden. It should be sufficient, that the ICT third party service provider is obliged and fulfills the service levels promised to the financial entity.

Question 4. Is article 5 appropriate and sufficiently clear?

- ○ Yes

- [x] No

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

Article 5 2) stipulates that the financial entity shall monitor the ICT subcontracting chain inter alia by reviewing the contractual documentation between ICT third party service provider and subcontractors. In order to determine if all conditions referred to in Article 4 are fulfilled.
Given the breath of what's considered ICT services, the complex ICT subcontracting chains, different jurisdictions to which the subcontracting agreements may be subjected and the cost for legal experts in such jurisdictions for reviewing such agreements, this obligation appears to be overly burdensome without having a proportionate effect on the resilience of the financial entity. It should rather be sufficient to oblige the financial entity to implement an obligation in its ICT third party service agreements requiring the ICT third party service provider to establish provisions in its agreement with its subcontractors that are in line with the primary ICT third party service agreement with the financial entity.
The financial entity should not be required to monitor key performance indicators of its ICT third party service provider's subcontractors. Given the complex outsourcing chains and the number of ICT service subcontracting agreements and subcontractors which may be involved in the provision of the ICT services, this implies a massive effort, which is not proportionate to the effect that may be derived from that monitoring.
Article 5 (1):
The requirement in Article 5 of the RTS to have every contract and the KPIs of the sub-service providers along the chain delivered and checked by the institution does not appear to us to be appropriate for achieving the objectives of the DORA. Cloud services in particular use a large number of service providers; obtaining the KPIs and the contract of each sub-service provider and having them checked again by the institution will probably not be made possible by the service providers and will lead to considerable additional work without a corresponding reduction in risk. Confirmation that the provider has passed on all clauses and regularly reviews the performance should be sufficient here, analogous to the EBA Guidelines on Outsourcing para. 80.
Article 5 (2):
ICT service providers are unlikely to share contractual documents with the financial entity. This requirement might force ICT service providers to break contractual agreements with their service providers by sending contractual documents to other third parties. NDAs of the ICT service provider and their providers might prevent ICT service providers to share contractual documents with the financial entity.
Article 5 (2) should entirely be deleted.
General comments on Article 5:
The monitoring requirements on subcontractors should not exceed the current requirements on monitoring as stated in the EBA guideline on outsourcing arrangements.

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

- [ ] Yes
- [x] No

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

Article 6 2) constitutes an obligation on the financial entity to inform the ICT third party service provider about its risk assessment results by the end of a notice period. This obligation is not parametrised, i.e. it does not apply only where the risk assessment is negative. It is not clear, how such obligation shall leverage the operational resilience of the financial entity. The financial entities should be able to act in its sole discretion to provide a (potentially confidential) risk assessment to the provider if it opines that this may be beneficial for it.
Article 6 3) stipulates, that the financial entity shall require that material changes in subcontracting are only made after approval or non-rejection. This has the effect, that the financial entities are obliged to agree on contractual arrangements with the ICT third party service provider establishing an approval/veto right. This will practically not be achievable in most ICT contracting situation. Art 7 1) stipulates a termination right in case of undue implementation of subcontractings. Such termination rights have proven to be agreeable by ICT service providers. Thus, we propose to amend Article 6 section 3) to the effect that it clarifies, that the contractual implementation of termination rights in case of undue ICT subcontracting is sufficient.
Moreover, the requirement for financial entities to inform the ICT third-party service provider of its risk assessment results by the end of the notice period, as put forward in Article 6 (2), appears contrary to our views. We believe that this requirement shall only apply if the ICT service provide is required to take actions following the financial entity's risk assessment. Where no risks are detected and no actions are required from the ICT service provider, the requirement to inform the ICT service provider shall not be mandatory as it would only create additional efforts and overhead for financial entities.
It is not clear if Article 7 requires financial entities to implement the respective termination rights in their contractual arrangements with their ICT service providers, or if Article 7 seeks to establish such termination right. If the latter is the case, this may be welcomed by financial entities, however from a legal perspective this is a massive interference in the private autonomy, which faces constitutional concerns.
Article 7(a): We suggest limiting this to critical and important functions, as it refers to all ICT services, which is not feasible
Article 8 should take into account the date of first applicability of the DORA requirements for financial entities rather than the day of its application.
While financial entities should have a right to be informed of material changes in the subcontracting chain, we do not believe it is realistic to expect them to be able to exercise a right of veto over the appointment of a new subcontractor in all but exceptional cases.
We would not assume ICT third-party service providers would change internal business setups once these are decided on and communicated. The RTS suggests a disproportionate level of influence by the FE. We would suggest a more pragmatic approach to suggest introducing termination criteria based on a change of sub-provider.

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

No further comments.

Contact

Contact Form