Contribution ID: 416f7d71-ec1a-40fb-b17f-93c1798ca84f
Date: 08/09/2023 22:27:42

Public consultation 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

Fields marked with * are mandatory.

Introduction

The European Supervisory Authorities (EBA, EIOPA and ESMA) have published the first 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 further specify the detailed content of the policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers under 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 January 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 11 September 2023 or submitted via other means may not be processed.

Please clearly express in the consultation form if you wish your comments to be disclosed 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 Börse 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 and Luxembourg

* 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

Questions

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

- Yes
- (•) No

* 1b. If not, please provide your reasoning and suggested changes.

We support the recognition within Article 1 of the Delegated Regulation 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, “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. The current wording of Article 1 could however be read to mean that intra-group providers are in fact higher risk.

The following clarification is therefore recommended: “whether the ICT third-party service providers are part of the same group of the financial entity whether the ICT service provider is a third party, as opposed to being part of the same group of the financial entity.”

Further, more clarification is needed on the consistent application of the proportionality principle is required, currently it is mentioned at certain places and the detailed requirements are way specific to apply to the proportionality principle.

We need more clarity what is meant with location.

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

- Yes
- (•) No

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

General thoughts on Article 3.1 the effectiveness of multi-vendor strategies:

The establishment of multi-vendor strategies can be used in individual cases to mitigation of risks of individual outsourcing. However, the full implementation will not be successful in terms of risk reduction,

despite exorbitant financial commitment.

This thesis is based primarily on the following scenarios:
The range of applications is distributed across the entire manufacturing depth (IaaS to SaaS) and increases complexity compared to traditional IT systems:
o IaaS and PaaS-based applications can be designed to be multi-vendor-enabled through smart architectural choices
o SaaS service, on the other hand, can only be relocated via migrations
o A multi-cloud strategy therefore primarily pursues the goal of distributing risk across multiple vendors
The multi-vendor strategy cannot address geographical and political concentration:
o Hyperscalers are currently exclusively US-American suppliers
o Functionally comparable offers can only be consumed by Chinese service providers
o 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. This type of strategy can be used in part to mitigate it. An obligation must therefore be avoided.

Whether a multi-vendor-strategy is an effective approach against resilience, availability, and vendor lock-in etc. should be decided by the respective organization. To mention such a strategy already in the DORA act, could encourage auditors to exactly ask for such a solution, disregarding other effective options like contractual guaranties or technical provisions. Also, 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.

We notice that Art. 3(8), 9(2) and 10 each require that the 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.

Further on Article 3.4: The allocation of responsibilities should not only focus on the contractual aspects, but also the service description and delivery. We suggest to change this as follows: “The policy referred to in paragraph 1 shall clearly assign the internal responsibilities for the approval, management, control, and documentation of relevant contractual arrangements (including service descriptions and service levels) and shall ensure that appropriate skills, experience and knowledge are maintained within the financial entity to effectively oversee relevant contractual arrangements and service delivery.”

DORA requires financial entities to take a holistic approach to the management of ICT policy across the business and supply chain. This conflicts with the proposed approach in article 3, which is in effect to delineate ownership of governance. By extension we are concerned that article 3.4 appears to imply specific individuals be designated for internal responsibilities: we would welcome clarification this is in terms of broader functions.
Article 3.5 obligates financial entities to assess whether and how the third-party provider has allocated sufficient resources to comply with all legal and regulatory requirements. This fails to recognize the difficulties facing financial entities in going beyond a third party’s assurances. We suggest the wording is amended to: “the policy referred to in paragraph 1 shall foresee that the financial entity has sought assurances that the ICT third-party service does not endanger the financial entity to comply with all its legal and regulatory requirements.”
In article 3.6 the term 'member of senior management' should be clarified by the ESAs. Should this in all cases be an individual reporting directly to the CEO of the financial entity?

Article 3.6 also appears more prescriptive than the existing EBA Guidelines, where the Delegated Regulation frames these as policy requirements. We seek clarity on whether this is intended and if so, why the supervisors are diverging.

We also note that the Delegated Regulation fails to make direct reference to other incoming DORA provisions, for example the Register of Information under Article 3.3. We are concerned that the ICT policy would therefore be duplicative, in the event that firms are unable to point towards and leverage other processes.

Question 3: Is article 4 appropriate and sufficiently clear?

- ○ Yes
- ◉ No

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

Article 4.1: We strongly recommend that the inclusion of subcontractors within Article 4 is removed. Firstly, financial entities may struggle in practice to obtain all the relevant information, and secondly subcontracting is already addressed under article 30 of DORA, with a separate draft RTS (Regulatory Technical Standard) due later in 2023 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 the following amendment in article 4.1: “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?

- ○ Yes
- ◉ No

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

Article 5: We have no objections, but we require clarity that the requirements are only for all ICT services supporting critical or important functions. Also, subject to the assumption that there is no expectation on firms to seek fresh/renewed management body approval for previously approved contractual arrangements. Similarly, we would object to any expectation that approval by the management body would need to be regranted in the event that the service provider makes changes as permitted by the contractual arrangement, for example changing a subcontractor.

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 article 30 of DORA. 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 all the required contractual terms, leading to extended renegotiation periods, which could be challenging within the implementation period. One potential way to address this would 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?

- ○ Yes

- [x] No

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

Article 6: The risk assessment under article 6 aligns with the existing requirements under paragraph 68 of the EBA Outsourcing Guidelines. Confirmation is though sought on whether the existing risk assessment can be relied upon for the purposes of DORA. We are strongly 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.

Question 6: Is article 8 appropriate and sufficiently clear?

- [ ] Yes
- [x] No

* 6b.Please provide your reasoning and suggested changes.

Article 8(2) requires that intra-group ICT providers have “to be on arms’ length terms”. This is not normally the way it works for intra-group matters and we would recommend deleting this unless there are specific terms that explains “to be on fully arms’ length terms”.
Article 8.2 appears to suggest that an intra-group provider has been selected by virtue of it being “set at arm’ s length”, whereas the decision to use an intragroup provider may in fact be due to the financial entity wanting to have greater control over a service, as compared to a third-party provider. To avoid any perception that supervisors are expecting intra-group providers to be treated as ringfenced entities, we recommend amending the proposed wording to “shall specify the conditions, including any financial conditions, for approving the use of an intra-group provider.”

Question 7: Is article 9 appropriate and sufficiently clear?

- [ ] Yes
- [x] No

* 7b. If not, please provide your reasoning and suggested changes.

In regard to the selection of Option A for the Policy Issue 7 on contractual clauses (i.e., page 25), 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.

Article 9: 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 article 30 of DORA. While this approach does work across most of the Delegated Regulation, there is duplication when adopting such an approach with regards to Article 9, in particular between Art 9.2 of the delegated regulation, and Article 30.2 (d) and 30.3 (c, 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.

Article 9.2 and 9.3: The ESAs should clarify what is meant by requirement third-party certifications and reports as referred to in paragraph 9.2 (c) are adequate and sufficient to comply with their regulatory obligations and shall not rely solely on these reports over time.

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.

Question 8: Is article 10 appropriate and sufficiently clear?

- ○ Yes
- ◉ No

* 8b. Please provide your reasoning and suggested changes.

Article 10: 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 is not seen as appropriate in this context and should be replaced with “measures”: penalty would be more appropriate for a supervisory authority.

Regarding cloud service providers it is not possible to fulfil these requirements on contractual arrangement level as they reside on service functional level and are subject to customer configuration. It should also be noted again that financial institutions do not have an equal bargaining power when negotiating contractual terms with CSPs; it is not possible to change the standard cloud service provider agreements. Standard EU contractual terms for cloud services would be highly appreciated.

Question 9: Is article 11 appropriate and sufficiently clear?

- ○ Yes
- ◉ No

* 9b. Please provide your reasoning and suggested changes.

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 (page 23), 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.

The requirement for exit plans on each ICT service to be periodically tested under article 11 has caused considerable concern in that this marks a considerable uplift in required resourcing from the current market practice and may also be impractical depending on the service in question, for example as with Cloud. We propose the following wording as an alternative: "shall include requirements for a documented exit plan for each ICT service supporting critical or important functions provided by an ICT third-party service provider taking into account possible service interruptions, inappropriate or failed service delivery or the unexpected termination of a relevant contractual arrangement. The exit plan shall be realistic, approved at a high level (in case of critical services), tested by the different lines of defense of the organization, and include analysis of possible risk scenarios".

We also 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. Supervisors should take this into account when reviewing the exit plans developed by financial entities.

Regarding cloud service providers - it is not a realistic requirement to periodically test exit plans as scenarios for exit can be very many and many 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 clear what the requirements regarding the timeframe for exit plan are under this Article (should it be 1, 6, 12 or 24 months)?

Contact

Contact Form