EUROPEAN ASSOCIATION OF CO-OPERATIVE BANKS
The Co-operative Difference : Sustainability, Proximity, Governance

Brussels, 1 March 2023
FINAL

EACB comments on the ESAs'

Draft RTS 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

March 2023

Question 1 - Are Articles 1 and 2 appropriate and sufficiently clear?

We would suggest to modify the wording of Article 1(e) to better reflect the definition of intragroup providers in the level 1 DORA text.
The DORA definition includes intragroup providers owned by financial entities within the same institutional protection scheme, in line with a risk-based approach reiterated Recital 6 of the RTS. In fact, the risks posed by ICT intragroup subcontractors, including the ones fully or collectively owned by financial entities within the same institutional protection scheme, may differ.
Art.1(e) should read: "whether the ICT subcontractors are ~~part of the same group of the financial entity;~~ an ICT intragroup subcontractor."

Question 2 - Is Article 3 appropriate and sufficiently clear?

Article 3(1)(c)
This requirement may prove to be exceptionally challenging. Due to confidentiality requirements, financial entities typically do no not have full visibility of contractual documentation between ICT third-party service providers and subcontractors. Requiring such access conflicts with common market practices and established legal norms.

Rather, the RTS could require that the agreement between the financial entity and the ICT third party service provider must clearly state that the ICT third party service provider shall ensure, by way of contract, that the subcontractor undertakes to comply with all applicable contractual obligations set out in the agreement.

In any event, the subcontractor's services generally only cover parts of the contractually agreed services with the ICT TPP. It would therefore be more appropriate to tailor contractual agreements to the specific services being subcontracted rather than to replicate all contractual agreements.

As the very least, we would propose to adapt the wording of Article 3(1)(c) as follows:
"that the relevant clauses of the contractual arrangements between the financial entity and the ICT third-party service provider are replicated as appropriate ***according to the type, scope and complexity of the services and the data being processed by the subcontractor*** in the subcontracting arrangements between the ICT third-party service provider and its subcontractor to ensure that the financial entity is able to comply with its own obligations under Regulation (EU) 2022/2554"

Article 3(1)(e)
It should be specified that external audit certificates issued by auditors, or the results of pool audits, can also constitute adequate evidence, aside from direct monitoring of the subcontractor, aside from direct monitoring of the subcontractor or the development of in-house expertise by the financial entity.

As an example, banks belonging to institutional protection schemes have set up preventative measure to avoid undesirable developments in their member institutions, including central outsourcing management providing technical support in monitoring central ICT service providers.

Article 3(2)
The wording in Article 3(2) ("possible changes in business environment, including but not limited to changes in the supported business function") appears unclear. We would suggest to adapt is as follows:

"Financial entities that use ICT third-party service providers that subcontract ICT services supporting critical or important functions shall periodically carry out the assessment referred to in paragraph 1) against possible changes in their business environment ***that are supported by the ICT third party service provider***, including but not limited to changes in the supported business functions, in risk assessments including ICT threats, concentration risks and geopolitical risks."

Question 3 - Is Article 4 appropriate and sufficiently clear?

It is not entirely clear what Article 4(c) achieves in addition to the requirements set out in Articles 1 and 3 – whether the responsibility of the financial entity is also affected (responsibility to conduct its own assessment or whether the third-party provider should provide the results of its risk assessment to the financial entity.

Regarding Article 4(j) on termination, we are concerned with the termination rights for any deviation from agreed service levels regardless of severity. This would deviate from common market practice. Such situations

are typically addressed through service credits, other contractual remedies, and termination rights are exercised only in cases of material breaches.

The termination of a contract with an ICT third-party service provider may have far-reaching consequences for the financial entity. If such a contract is terminated due to a single problem with certain subcontractors, this effect would be disproportionate. Short-term implementation would not be possible in practice, in the absence of alternatives or exit strategies that would be very expensive. A risk assumption should be allowed in certain cases on the basis of a risk assessment.

We take the view that ICT third-party provider and the subcontractor should themselves establish exit plans to ensure the provision of the services agreed with the financial entity.

Alternatively, the requirement set out in DORA Chapter V, Section I, article 28(7)(a) is sufficient to ensure the appropriate termination rights for the financial entity in this regard. The reservation of termination rights for cases of repeated or material/significant breaches would provide a more objective basis for termination, ensuring that the financial entity retains termination rights only in situations that significantly impact critical or important functions or overall service quality.

Regarding Article 4 more generally, it is not entirely clear what are the objectives of the requirements compared to similar ones set out in DORA (eg. in subsection b) RTS / Chapter V, Section I, Art 30(3)(b) DORA).

It is also unclear how certain requirements are to be incorporated in agreements. For instance, Article 4(j) of the draft RTS do not state whether the requirement in question can be modified in the agreement or whether it should be incorporated as such.
Regarding the requirement to specify the service levels to be met by the subcontractors in Article 4(g), it is not clear how this should be incorporated into the agreement.

According to existing common market practice, the ICT third party service provider, i.e. the contracting party to the agreement, bears the direct and legal responsibility for compliance with all contractual obligations, irrespective of the involvement of subcontractors. Explicitly stipulating that certain requirements must be met by subcontractors could potentially introduce ambiguity and complicate the contractual framework.

Instead of listing requirements in detail in Article 4 (b), (e), (g), (h) and (i), it could be stated that:

- the ICT third-party service provider shall ensure, by way of written contract, that the subcontractors undertake to comply with all applicable contractual obligations set out in the agreement, including, but not limited to, by way of undertaking to grant the same audit and access rights as set out in the agreement and to comply with the security requirements set out in the agreement. (covering subsection e, g, h and i)
- the duties and responsibilities of the ICT third-party service provider under the agreement shall remain unaffected by any subcontracting, and the ICT third-party service provider shall retain full accountability for the subcontracted services and its subcontractors' performance as for its own. (covering subsections e, f and g)

Question 4 - Is Article 5 appropriate and sufficiently clear?

Article 5(1) is clearly formulated, however we take the view that the requirement for the financial entity to fully monitor the ICT subcontracting chain is not appropriate, given that there is no direct contractual relationship between the financial entity and the subcontractor.

Similarly, we do not consider it feasible for financial entities to monitor the subcontracting activities as set out in Article 5(2). We take the view that it must be up to the service provider to verify and confirm compliance by means of an audit certificate (see our comments on Article 3(1)(c).

Question 5 - Is Article 4 appropriate and sufficiently clear?

It is our understanding that the requirements under these RTS apply to critical and important functions, as explicit in other articles. This should also be specified in Articles 6 and 8.

Under Article 6(1), we would welcome clarifications on what constitutes a "sufficient advance notice period" and whether a reference can be made to existing guidance.

Under Article 6(2), it is unclear why the financial entity should inform the third-party provider of the results of the risk assessment. There is the valid option under Article 6(3) that where the financial entity does not object to the changes by the end of the notice period. In this case, there should no obligation to forward the result of the risk assessment to the third-party provider.
Article 6(2) could instead read: ***Where t***he financial entity ***does not approve the changes, it*** shall inform the ICT third-party service provider of its risk assessment results as referred to in paragraph 1) by the end of the notice period."

Finally, we consider that Article 7 should include the right of the financial entity to require the third-party provider to terminate its contract with a subcontractor in case service levels are not met due to failures on the side of the subcontractor.

For further information or questions on this paper, please contact:

- Mr Marco Mancino, Lead Prudential matters (Marco.mancino@eacb.coop)
- Ms Pauline Hascoët, Adviser Corporate Governance (Pauline.Hascoet@eacb.coop)