

ESMA_QA_2159

Status: Question Rejected

Additional Information

Level 1 Regulation

Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic

ICT risk management

Historic Question Reference

Clarification Request on Preliminary Assessment of ICT Concentration Risk submitted via DORA's consultation papers.

Additional Legal Reference

Art.1(i) of the 'Draft RTS to specify the elements that 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

Subject Matter

Intragroup ICT service providers consideration regarding the preliminary assessment of ICT concentration risk.

Question

When conducting the preliminary assessment of potential ICT concentration risk associated with an ICT service provider, as stipulated in Regulation 2022/2054 and its corresponding draft RTS on subcontracting ICT services supporting critical or important functions, what treatment should be applied to ICT intra-group service providers? In other words, are financial entities (FEs) required to consider this concentration risk for ICT intra-group service providers? Alternatively, would the exemption outlined in Regulation 2022/2054 article 31.8(iii) apply, thereby meaning that this risk should not be considered for intra-group service providers?

REGIS-TR SA seeks further clarification on this matter, given that the DORA Regulation establishes that

- 'While intra-group provision of ICT services entails specific risks and benefits, it should not be automatically considered less risky than the provision of ICT services by providers outside of a financial group and should therefore be subject to the same regulatory framework. However, 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'.

Similarly, article 28.4(c) states that

- 'Before entering into a contractual arrangement on the use of ICT services, financial entities shall: (c) identify and assess all relevant risks in relation to the contractual arrangement, including the possibility that such contractual arrangement may contribute to reinforcing ICT concentration risk as referred to in Article 29'.

Furthermore, the aforementioned article 29 covers the considerations and risks to take into account in relation to ICT service providers supporting critical or important functions, when performing the preliminary assessment of ICT concentration risk.

Additionally, the draft RTS on 'the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions' also explains that

- 'ICT intragroup subcontractors, including the ones fully or collectively owned by financial entities within the same institutional protection scheme, providing ICT services supporting critical or important functions should be considered as ICT third-party services providers. Intragroup ICT subcontracting should not be treated differently from subcontracting outside of the group. The risks posed by those ICT intragroup subcontractors may be different but the requirements applicable to them are the same in accordance with Regulation (EU) 2022/2054. When the use of ICT subcontractors is permitted, then those also include ICT intragroup subcontractors', thereby making no distinction between intra-group and external service providers.

Due to these reasons, we are uncertain about whether the exemption outlined in Regulation

2022/2054 article 31.8(iii) would apply; or if exposure to a ICT intragroup service providers should also be considered during the preliminary assessment of ICT concentration risk.