ESMA_QA_2646

Submission Date
18/09/2025

Status: Answer Published

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
ICT third-party risk management

Additional Legal Reference
28(6), 30(3)(e)

Subject Matter
Audit frequency limitations

Question
As DORA requires financial entities to pre-determine the frequency of audits and inspections on the basis of a risk-based approach, are financial entities not permitted to agree on a

maximum audit frequency (e.g. once per year) with their ICT third-party service providers?

ESMA Answer

18-09-2025

Original language

DORA does not limit the financial entities in the way to implement the relevant audit requirements, including regarding the audit frequency. In case the contracts between the financial entities and their ICT third-party service providers would refer to a (maximum) audit frequency, the frequency shall be agreed by the financial entities (i.e., not imposed by the ICT third-party service providers) and shall not prevent the financial entities to implement the DORA audit requirements on a risk-based approach.

Therefore, financial entities shall also ensure that the contractual arrangements grant them the ability to carry out an audit on an ad-hoc basis when they find it necessary to comply with the DORA requirements (for example, in the event of doubts regarding the proper performance of the contract), without the clause on the audit frequency preventing it. If such conditions are met, the financial entities and their ICT third-party service providers may agree on an audit frequency in their contracts.