ESMA_QA_2292

Submission Date
27/09/2024

Status: Answer Published

Additional Information

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

Topic
ICT risk management

Additional Legal Reference
Art. 5-15, Art. 16 DORA; Art. 12 (1) IFR + Art. 12 ECSPR

Subject Matter
Obligation to apply the ICT risk managment (Art. 5-15) and/or the simplified ICT risk management framework for entities that hold two or more licences.

Question

Is a small and non-interconnected investment firm (Art. 12 (1) IFR (Regulation (EU) 2019/2033)) that also holds a licence as a crowdfunding service provider according to Art. 12 ECSPR (Regulation (EU) 2020/1503) obligated to apply Art. 5-15 DORA or is it allowed to use the simplified ICT risk management framework of Art. 16 DORA?

ESMA Answer

17-12-2025

Original language

Answer provided by the European Commission:

Articles 5-15 DORA establish obligations for financial entities to put in place an internal governance and control framework that ensures an effective and prudent management of ICT risk. Article 16 DORA introduces an exemption from the obligations laid down in Articles 5-15 enabling the design of a simplified ICT risk framework for the following categories of entities: small and non-interconnected investment firms, payment institutions exempted pursuant to Directive (EU) 2015/2366; institutions exempted pursuant to Directive 2013/36/EU in respect of which Member States have decided not to apply the option referred to in Article 2(4) DORA; electronic money institutions exempted pursuant to Directive 2009/110/EC; and small institutions for occupational retirement provision. The reason for this exemption is to ensure that the obligations are proportionate to the nature of ICT risks in view of the size and or the service they provide (see in this respect recital 42 DORA). Article 5-15 DORA cannot be derogated from, except where a financial entity benefits from the exemption laid down in Article 16 DORA (which only requests a simplified ICT risk framework). The assessment of whether an entity benefits from the simplified regime laid down in Article 16 DORA is to be done in on a case-by-case basis. In that context, if the main activity of a financial entity does not fall within the scope of the entities benefiting from Article 16 DORA, the entity must apply a full ICT risk management framework as laid down in Art 5-15. If it does, the simplified ICT risk management framework under Article 16 DORA would apply.

Disclaimer:

The answers clarify provisions already contained in the applicable legislation. They do not extend in any way the rights and obligations deriving from such legislation nor do they introduce any additional requirements for the concerned operators and competent authorities. The answers are merely intended to assist natural or legal persons, including competent authorities and Union institutions and bodies in clarifying the application or implementation of the relevant legal provisions. Only the Court of Justice of the European Union is competent to authoritatively interpret Union law. The views expressed in the internal Commission Decision cannot prejudge the position that the European Commission might take before the Union and national courts.