ESMA_QA_2107

Submission Date
12/02/2024

Status: Answer Published

Additional Information

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

Topic
ICT third-party risk management

Subject Matter
Application of DORA for outsourced critical services that are not ICT

Question
My questions relate to the scenario where a UK financial services firm, or an offshore financial services firm (e.g. in Guernsey), provides services to an EU financial services firm. For example, in the scenario where an EU financial services firm outsourced its fund management to a UK asset management firm to manage a fund. Would the EU firm be expected to have sought reassurance from the UK fund manager that the UK firm is also

compliant with DORA?
Thanks in advance for your help.

ESMA Answer

12-02-2024

Original language

A financial entity in the EU is subject to DORA and must ensure it operates DORA-compliant, which includes their third-party relationships.

Therefore, it follows that if an EU financial entity makes use of a non-EU third-party provider for a function or activity, independently of whether this function is considered as critical or important or not by the financial entity and this service provider in turn makes use of ICT services to support its function or activity, the responsibility to ensure the operational resilience of the function or activity that has been entrusted to the non-EU third-party provider remains with the financial entity.

The EU financial entity is expected to validate that the non-EU third-party provider does not prevent it to be compliant with DORA.