

Question ID

2024_7047

Legal act

Regulation (EU) No 2022/2554 (DORA)

Topic

ICT-related incidents (management / classification / reporting)

Article

18

Paragraph

3

COM Delegated or Implementing Acts/RTS/ITS/GLs/Recommendations

Not applicable

Article/Paragraph

Article 6 of Delegated Act on Classification of Major Incidents

Name of institution / submitter

AFME

Country of incorporation / residence

Belgium

Type of submitter

Industry association

Subject matter

Critical Services Affected

Question

Article 6 of the Delegated Act on the Classification of Major Incidents states that:

"For the purpose of determining the criticality of the services affected as referred to in Article 18(1), point (e), of Regulation (EU) 2022/2554, financial entities shall assess whether the incident:

- (a) affects or has affected ICT services or network and information systems that support critical or important functions of the financial entity;
- (b) affects or has affected financial services provided by the financial entity that require authorisation, registration or that are supervised by competent authorities;
- (c) constitutes or has constituted a successful, malicious and unauthorised access to the network and information systems of the financial entity."

Can you confirm please that ALL three of the components are cumulatively required to trigger the criteria on Critical Services Affected?

Background on the question

It is not clear whether ALL three of the components are required or whether ANY of the components would be sufficient to trigger the criteria. If the latter, we have major concerns that the second component will result in almost every incident at a regulated entity being classified as major, with the subsequent overreporting obscuring sight of those incidents which may have systemic impact.

Submission date

03/04/2024

Final publishing date

11/12/2024

Final answer

Article 6 of Commission Delegated Regulation (EU) 2024/1772 provides that *'financial entities shall assess whether the incident:*

(a) affects or has affected ICT services or network and information systems that support critical or important functions of the financial entity;

(b) Affects or has affected financial services provided by the financial entity that require authorisation, registration or that are supervised by competent authorities;

(c) constitutes or has constituted a successful, malicious and unauthorized access to the network and information systems of the financial entity.'

In accordance with Article 8 of the Commission Delegated Regulation, an incident shall be considered major, and therefore be reported to the national competent authority, when it has affected critical services under Article 6 and when the additional specific conditions in Article 8 are met.

Accordingly, for the purpose of classification of major ICT incidents under the Delegated Regulation and Article 19(1) of Regulation (EU) 2022/2554, an impact on any of the components listed in Article 6 of the Delegated Regulation should be considered as affecting critical services.

Status

Final Q&A

Answer prepared by

Answer prepared by the Joint ESAs Q&A