

## Question ID

2026\_7779

---

## Legal act

Regulation (EU) No 2022/2554 (DORA Reg)

---

## Topic

ICT-related incidents (management / classification / reporting)

---

## Article

18

---

## Paragraph

1

---

## Subparagraph

(e)

---

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

Regulation (EU) 2024/1772 - RTS on the classification of ICT-related incidents and cyber threats

---

## Article/Paragraph

Articles 6

---

## Type of submitter

Competent authority

---

## Subject matter

Scope of Article 6 lit. c RTS

---

## Question

Is the criticality of the services affected pursuant to Article 6 (c) RTS to be assumed for every successful, malicious and unauthorised access to the network and information systems of the financial entity, regardless of whether the affected systems support critical or important functions?

---

## Background on the question

The question concerns the reporting obligations for successful, malicious and unauthorised access and the requirements of Article 6 (c) RTS.

According to the wording of Article 6 (c) RTS, financial entities determine criticality of services affected based on whether the incident "constitutes or has constituted a successful, malicious and unauthorised access to the network and information systems of the financial entity."

Strictly according to the wording, criticality is to be assumed for each successful, malicious and unauthorised access to network and information systems of the financial entity. The network and information systems do not have to support critical or important functions of the financial entity.

However, the definition of a major ICT-related incident according to Article 3 (10) DORA suggests that it only applies to network and information systems that support critical or important functions of the financial entity. Article 6 (a) RTS reiterates the requirement to support critical and important functions, whereas Article 6 (c) RTS does not. This raises question of why this is not the case in Article 6 (c) RTS.

The question formulated above is accompanied by the question of whether successful, malicious and unauthorised access to network and information systems by third parties is exempt from Article 6 (c) RTS. According to the wording of Article 6 (c) RTS corresponding accesses to the network and information systems of third parties are not included. The wording explicitly states that access must be gained to the "systems of the financial entity".

---

#### **Submission date**

18/03/2026

---

#### **Final publishing date**

02/10/2026

---

#### **Final answer**

Under Article 6(c) of Commission Delegated Regulation (EU) 2024/1772 ("the RTS") read in conjunction with Recital 5, an incident that constitutes or has constituted a successful, malicious and unauthorised access to the network and information systems of the financial entity must be assessed independently for the purpose of determining the criticality of the services affected, as referred to in Article 18(1)(e) of Regulation (EU) 2022/2554 ("DORA"), regardless of whether the compromised network and information systems support critical or important functions or whether the access to the financial entity's network or systems was gained through the network and information systems of an ICT third-party service provider.

Then, as per the article 8(1) of the RTS, such an incident is classified as a major ICT-related incident as per the definition of DORA article 3(10) whenever it has affected critical services as referred to in Article 6 together with the materiality threshold referred to Article 9(5)(b) of the RTS (where any successful, malicious and unauthorised access are considered as well), or with two or more of the other materiality thresholds referred to in Articles 9(1) to (6) of the RTS. Further clarifications about Article 6 of the RTS can be read in DORA Q&A 2024\_7047

---

#### **Status**

## Final Q&A

---

### **Answer prepared by**

Answer prepared by the Joint ESAs Q&A

---