Procedure for reporting major ICT-related incidents to the CNMV and voluntary notification of significant cyber threats

20 February 2025

Introduction

Financial entities, in order to comply with their obligations under Article 19 of Regulation (EU) 2022/2554 (on Digital Operational Resilience or DORA), shall notify major ICT-related incidents in compliance with the content and timelines specified in the RTS[1][2] and ITS[3] to their corresponding authority.

CNMV is implementing a system for the collection of said notifications through its Virtual Office by introducing a certificate of a legal person.

Notification procedure

The procedure to notify the CNMV of major incidents as well as significant cyber threats is, temporarily, as follows:

1. The entity must download the following template completing the required information:
    - To notify a major incident: https://www.cnmv.es/DocPortal/Ciberseguridad/Plantilla_DORA_IR.xlsx
    - To notify a significant cyber threat: https://www.cnmv.es/DocPortal/Ciberseguridad/Plantilla_DORA_SCT.xlsx

2. The entity will send an e-mail to the CNMV's cybersecurity mailbox to inform of its intention to send a notification. This email shall have the following requirements:

    To: ciberseguridad@cnmv.es

    Subject: DORA, Major Incident/Cyber Threat Report.

[1] Commission Delegated Regulation (EU) 2024/1772 on criteria for the classification of ICT-related incidents
[2] Commission Delegated Regulation (EU) 2025/301 on the content, format and timelines for reporting major ICT-related incidents and significant cyber threats
[3] Commission Implementing Regulation (EU) 2025/302 on standard templates for reporting major ICT-related incidents and significant cyber threats

Message:

- Name and Legal Entity Identifier (LEI code) of the affected financial entity (or more than one entity in the case of an aggregate report).
- Reference code of the incident assigned by the financial entity.

3. CNMV will register the entity in its exchange system. The entity will receive an e-mail, to the address provided in the previous step, to complete its registration in said exchange system.
4. Once the entity gains access to said exchange system, the notification may be submitted to the CNMV with the template with the required information attached therein, along with additional information deemed important.
5. The CNMV will provide an acknowledgement of receipt of said notification.

Additional observations:

If the reporting entity to the CNMV is not that affected by the incident[4], said entity must make a notification in advance[5] to ciberseguridad@cnmv.es (stating the name of the entity to be notified, the contact details and the identification code of the corresponding entity). Likewise, when said entity fails to report incidents on behalf of the financial institution, the latter must notify the CNMV following the same instructions.

If the entity has previously reported an incident and remains registered in the CNMV exchange system, step number 3 would not be necessary.

Only financial entities subject to the CNMV's supervisory authority, in line with Article 46 of DORA, shall submit the incidents to the CNMV[6].

Entities may use either Spanish or English when completing the template, an Excel file, except in the case of specific fields.

Should the financial entity be unable to submit any of the notifications with the content and within the timelines specified in the RST and ITS, according to Article 5(3) of said RTS, the CNMV must be informed thereof without undue delay, but no later than the respective deadlines for the submission of the notification. To do so, please send an email to the CNMV's cybersecurity department: ciberseguridad@cnmv.es justifying the delay.

For any questions, please contact the CNMV's cybersecurity department: ciberseguridad@cnmv.es (confidential information should not be disclosed through this channel).

Notwithstanding reporting to the CNMV, INCIBE-CERT provides technical support to assist in the resolution of cybersecurity incidents:

https://www.incibe.es/en/incibe-cert/incidents/incident-handling

[4] Article 19.5 of DORA.
[5] Article 6 of the final draft of the ITS on the reporting of major ICT-related incidents.
[6] Article 46 of DORA.