CNMV
COMISIÓN NACIONAL DEL MERCADO DE VALORES

ESAs joint consultation on second batch of policy mandates under the Digital Operational Resilience Act

ESAs joint consultation on second batch of policy mandates under the Digital Operational Resilience Act

1. – Target participants

The public consultation is addressed to market participants.

2. - Information Note

DORA brings harmonisation of the rules relating to operational resilience for the financial sector applying to 21 different types of financial entities, covering important topics such as: ICT risk management; ICT incident management and reporting; testing of the digital operational resilience of ICT systems; and the management of ICT third party risks.

To operationalise the application, DORA mandates the European Supervisory Authorities (ESAs) to prepare jointly, through the Joint Committee (JC), a set of policy products. For the first batch of mandates, the deadline for submission to the European Commission is set for 17 January 2024 and the public consultation has already been completed.

This publication focuses on the **second batch** of the policy mandates to be submitted by 17 June 2024 and include consultation papers on the following standards:

1) RTS and ITS on content, timelines and templates on ICT-related incident reporting (Article 20)

The draft RTS on reporting details for major incidents under DORA covers three distinct aspects:

a) the content of the major incident reports for major ICT-related incidents;

b) the time limits for the submission of an initial notification, intermediate and final reports for each major incident;

c) the content of the notification for significant cyber threats.

The draft ITS covers aspects related to general reporting requirements and introduces the format and templates for reporting major incidents and significant cyber threats under DORA

Consultation Paper on draft RTS and ITS on major incident reporting under DORA.

RTS and ITS on major incidents reporting response form.

2) Guidelines on aggregated costs and losses from major ICT-related incidents (Article 11(1))

The draft Guidelines specify the estimation of aggregated annual costs and losses caused by major ICT-related incidents.

Consultation Paper on draft GL on costs and losses.

GL on costs and losses caused by major ICT-related incidents response form.

3) RTS on threat-led penetration testing (Art.26(11))

Article 26 of DORA requires certain financial entities to carry out at least every 3 years advanced testing by means of TLPT. Article 26(11) of DORA mandates the ESAs, 'in agreement with the ECB' to develop draft regulatory technical standards 'in accordance with the TIBER-EU framework' to specify further the criteria used for identifying financial entities required to perform TLPT, the requirements and standards governing the use of internal testers, the requirements in relation to scope, testing methodology and approach for each phase of the testing, results, closure and remediation stages and the type of supervisory and other relevant cooperation needed for the implementation of TLPT and for the facilitation of mutual recognition.

Consultation Paper on draft RTS on TLPT.

RTS on threat-led penetration testing (TLPT) response form.

4) RTS on subcontracting of critical or important functions (Art.30(5))

The draft regulatory technical standards specify further the elements referred to in Article 30(2) point (a), which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions or material parts thereof. The RTS cover requirements regarding: the risk assessment before allowing ICT services supporting critical or important functions to be subcontracted; requirements on the contractual arrangements; on the monitoring of subcontracting arrangements; on information of material changes; and on exit and termination rights.

Consultation Paper on draft RTS subcontracting.

RTS on subcontracting ICT services response form.

5) Guidelines on oversight cooperation between the ESAs and competent authorities (Article 32(7))

The guidelines cover: the detailed procedures and conditions for the allocation and execution of tasks between competent authorities and the ESAs; and the details on the exchanges of information which are necessary for competent authorities to ensure the follow-up of recommendations addressed to critical ICT third-party service providers.

The cooperation with financial entities, critical ICT third-party service providers, competent authorities under Directive (EU) 2022/2555, among competent authorities, among the ESAs and with other EU institutions is outside the scope of the guidelines.

Consultation Paper on draft Guidelines on oversight cooperation.

GL on oversight cooperation and information exchange between ESAs and CAs response form.

6) RTS on oversight harmonisation (Art.41(1))

The primary goal of the draft RTS is to bring harmonization of requirements across regulations and instore efficient oversight conditions vis-à-vis critical third-party service providers, financial entities, and supervisory authorities across the Union in order to avoid legislative fragmentation, all while ensuring the stability of the financial sector. They specify:

a) the information to be provided by an ICT third–party service provider in the application for a voluntary request to be designated as critical;

b) the content, structure and format of the information to be submitted, disclosed or reported by the ICT third–party service providers to the Lead Overseer (LO) pursuant to Article 35(1), including the template for providing information on subcontracting arrangements;

d) the details of the competent authorities' assessment of the measures taken by critical ICT third–party service providers (CTPPs) based on the recommendations of the LO pursuant to Article 42(3).

It is noted that the mandate of the Joint Examination Team will be finalised according to a different timeline with the involvement of the recently constituted High-Level Group on DORA Oversight (HLGO).

Consultation Paper on draft RTS on oversight harmonisation.

RTS on oversight harmonisation response form.

3. - Submission of comments

The deadline for submitting comments is **4 March 2024**.

Respondents may send their comments through ESMA's website: **www.esma.europa.eu.** Both the paper of this consultations and the response forms are available on ***ESMA's website*** (place the cursor on the word to obtain the link).

Likewise, please send a copy of your answers to the CNMV to the following email address: **documentosinternacional@cnmv.es**

Dirección de Asuntos Internacionales
CNMV
c/ Edison 4
28006 Madrid