JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

8 December 2023

Digital Operational Resilience Act (DORA): public consultation on the second batch of policy products

1. Information and communication technology (ICT) supports complex systems used for everyday activities of the financial sector. The extended use of ICT systems increases the efficiencies of internal process and the user experience for the customers, however it also introduces risks and vulnerabilities, which may make financial entities expose to cyber-attacks or incidents. If not managed properly, ICT risks could lead to the disruptions of financial services that are often offered across borders and can have far-reaching effects on other companies, sectors, or even the rest of the economy. The risk of such cross-border and cross-sectoral disruptions highlights the importance of digital operational resilience of the financial sector.

2. As a measure to enhance the overall digital operational resilience of the EU financial sector, on 27 December 2022, the Digital Operational Resilience Act (DORA) was published in the Official Journal of the European Union[1] and entered into force on 16 January 2023. DORA will apply from 17 January 2025.

3. 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. Furthermore, DORA is *lex specialis* to the NIS Directive[2] and to Article 11 and Chapters III, IV and VI of the CER Directive[3].

4. From the supervisory perspective, DORA aims at increasing supervisory awareness of cyber risks and ICT-related incidents faced by FEs and enhancing the cooperation among competent authorities in the financial sector, but also among authorities from different sectors and jurisdictions in relation to ICT and cyber risk management.

5. The DORA also introduces a framework to oversee the systemic and concentration risks posed by the financial sector's reliance on ICT third party service providers and an EU-level oversight framework for the critical ICT service providers that aims at ensuring that the ICT risks posed by these critical providers to financial entities are properly managed.

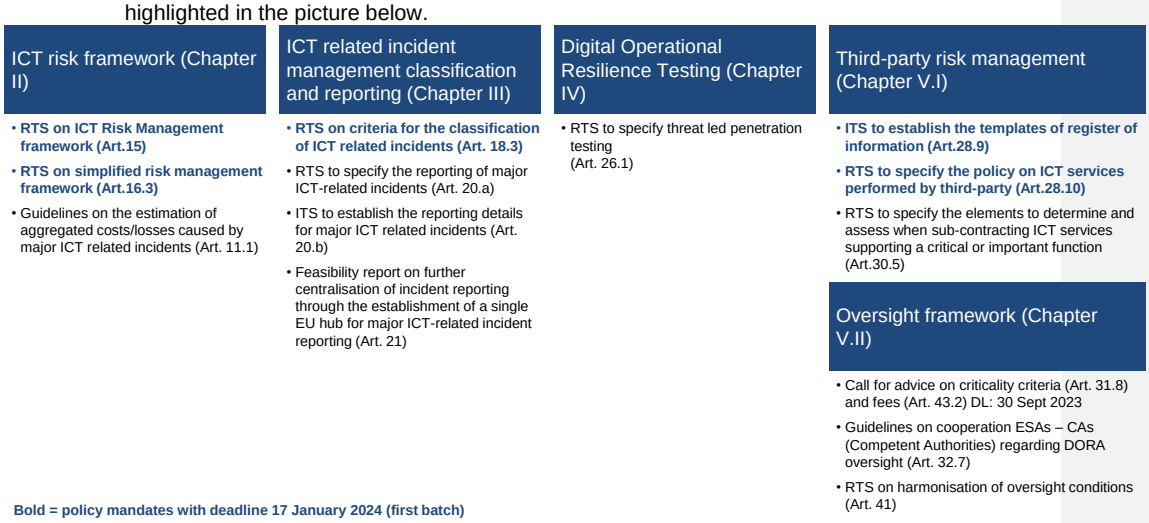
6. To operationalise the application, DORA mandates the European Supervisory Authorities (ESAs) to prepare jointly, through the Joint Committee (JC), a set of policy products with two main

[1] Regulation (EU) 2022/2554 of 14 December 2022 on the Digital Operational Resilience of the Financial Sector (DORA)

[2] See Recital 28 of Directive (EU) of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS II Directive)

[3] See Recital 21 and Article 8 of Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities (CER)

submission deadlines 17 January 2024 (first batch) and 17 June 2024 (second batch) as highlighted in the picture below.



7. In addition to the policy mandates conferred on the ESAs by DORA, the ESAs have issued on 29 September 2023 a technical advice[4] to the European Commission to respond to the call for advice[5] to support the preparation of delegated acts complementing the DORA text in relation to the criteria to designate ICT third-party service providers as critical and the fees those providers will have to pay to be overseen.

8. The timelines for the policy development of all DORA deliverables and their public consultation are summarised in the below table:

Commented [AP1]: Revised. Please check

Policy products	Public consultation	Submission to the European Commission
First batch of policy products	Completed	17 Jan 2024
Second batch of policy products	08 Dec 2023 – 04 Mar 2024	17 Jul 2024
Feasibility report on single EU Hub	TBA	17 Jan 2025

4 https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Other%20publications/2023/JC%20technical%20advice%20on%20DORA/1062226/Joint-ESAs%E2%80%99%20response%20to%20the%20Call%20for%20advice%20on%20the%20designation%20criteria%20and%20fees%20for%20the%20DORA%20oversight%20framework_final.pdf

5 ESAs launch discussion on criteria for critical ICT third-party service providers and oversight fees (europa.eu)

9. The publication of today focuses on the second batch of the policy mandates that include consultation papers on the following standards:

   i. 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) establish the content of the notification for significant cyber threats.

   The draft RTS reflects proportionality and ensures consistency with the incident reporting approach taken in Directive (EU) 2022/2555 (NIS2).

   With regard to the reporting timelines, the draft RTS proposes harmonised timelines for financial entities within the scope of DORA. Accordingly, the proposed timelines for reporting major incidents are as follows:

   - the initial report within 4 hours from the moment of classification of the incident as major, but no later than 24 hours from the time of detection of the incident.
   - an intermediate report within 72 hours from the classification of the incident as major, or when regular activities have been recovered and business is back to normal.
   - the final report shall be submitted no later than 1 month from the classification of the incident as major.

   With regard to the content of the major incident reports, the draft RTS aims at striking the right balance between allowing competent authorities to receive the essential information related to each incident but also not posing reporting burden to financial entities. In relation to the content of the notifications for significant cyber threats (which are to be reported on voluntary basis), the draft RTS introduces a short, simple and concise content of the notifications.

   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. With regard to the template, the draft ITS introduces a single template covering the initial notification, intermediate and final reports. The template and the supporting technical details are designed in a way similar to prudential reporting requirements. The draft ITS also provides data glossary, characteristics of the data fields and instructions how to populate them.

   ii. 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. The calculation of the annual costs and losses under the Guidelines is aligned with the assessment of the costs and losses of each incident under the technical standards incident reporting. In particular, the Guidelines introduce a reporting covering the gross costs and losses, financial recoveries and of the net costs and losses by major ICT-related incident.

The Guidelines also propose to focus the reference period for the aggregation to an accounting year in order to rely on available figures from the validated financial statements.

iii. RTS on thread-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.

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

Article 30(5) of DORA requires the ESAs to develop, through the Joint Committee, draft regulatory technical standards to 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 draft RTS provides further specifications on how to determine and assess when subcontracting ICT services supporting critical or important functions can be performed. In line with the mandate the draft RTS focuses on ICT services supporting critical or important functions or material parts of them provided by ICT subcontractors. The draft RTS follows the lifecycle of arrangements between financial entities and ICT third-party service providers when subcontracting ICT services supporting critical or important functions, and sets key requirements to financial entities on the use of subcontracted services supporting critical or important functions or material parts thereof, covering: 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.

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

Article 32(7) of DORA requires the ESAs to issue guidelines on the cooperation between the ESAs and the competent authorities covering:

- 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 draft guidelines cover the cooperation and information exchanges between ESAs and competent authorities only. Hence, 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.

The draft guidelines cover the following four areas:

- General considerations: this covers topics, such as language, communication means, contact points and difference of opinions between ESAs and competent authorities.
- Designation of critical ICT third-party service providers: this covers information exchanges between the Lead Overseer, competent authorities and the Oversight Forum related to the designation of critical ICT third-party service providers.
- Oversight activities: this covers procedures and information exchanges related to the annual oversight plan, general investigations and on-site inspections and competent authorities taking measures concerning critical ICT third-party service providers in agreement with the Lead Overseer.
- Follow-up of the recommendations: this covers information exchanges between the Lead Overseer and competent authorities to ensure the follow-up of recommendations and the decision of competent authorities to require financial entities to suspend / terminate their contract with the critical ICT third-party service provider.

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

Article 41(1) of DORA requires the ESAs to develop, by 17 July 2024, draft RTS to 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[6] will be finalised according to a different timeline with the involvement of the recently constituted High-Level Group on DORA Oversight (HLGO).

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.

Public consultation and next steps

10. The public consultation on all mandates included into the second batch will last until 04 March 2024. Furthermore, to present the consultation papers and their rationale, and to provide clarification to questions raised by the stakeholders, the ESAs will organise an online public hearing on 23 January 2024.

11. The details on how to provide feedback on the various policy products is included in each consultation paper.

12. Based on the feedback received to the public consultation, the legal instruments will be finalised and will be submitted to the European Commission by 17 July 2024.

Background

13. DORA is a cross-sectoral regulation applying to more than 20 different types of financial entities and to a more than double number of competent authorities (CAs), in order to ensure a cross-sectoral proportionate and harmonized approach in developing the level 2 legislation, the ESAs have decided to constitute the Joint Committee Sub-Committee on Digital Operational

[6] The empowerment reads "The ESAs shall, through the Joint Committee, develop draft regulatory technical standards to specify: (c) the criteria for determining the composition of the joint examination team ensuring a balanced participation of staff members from the ESAs and from the relevant competent authorities, their designation, tasks, and working arrangements".

Resilience (JC SC DOR)[7] to contribute and coordinate where needed, the ESAs' input to the EU regulatory process relating to digital operational resilience. More than 50 authorities including national authorities, the European Central Bank and ENISA take part in the joint work on the development of the policy products mandated by the DORA[8].

[7] Mandate of the European Supervisory Authorities' Joint Committee Sub-Committee on Digital Operational Resilience (europa.eu)

[8] The following policy products shall be developed in consultation with ENISA only: RTS on ICT Risk Management Framework (Art. 15) and Simplified Risk Management Framework (Art. 16). The following policy products shall be developed in consultation with both ENISA and the ECB: RTS on criteria for the classification of ICT-related incident (Art. 18(3)), RTS to specify the reporting of major ICT-related incidents (Art. 20.a), ITS to establish the reporting details for major ICT-related incidents (Art. 20.b) and the Feasibility report on further centralisation of incident reporting through the establishment of a EU hub for major ICT-related incident reporting (Art. 21). Finally, the ESAs shall develop in agreement with the ECB the RTS to specify threat led penetration testing (Art. 26.1)