JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

19 June 2023

Digital Operational Resilience Act (DORA): public consultation on the first 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 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.

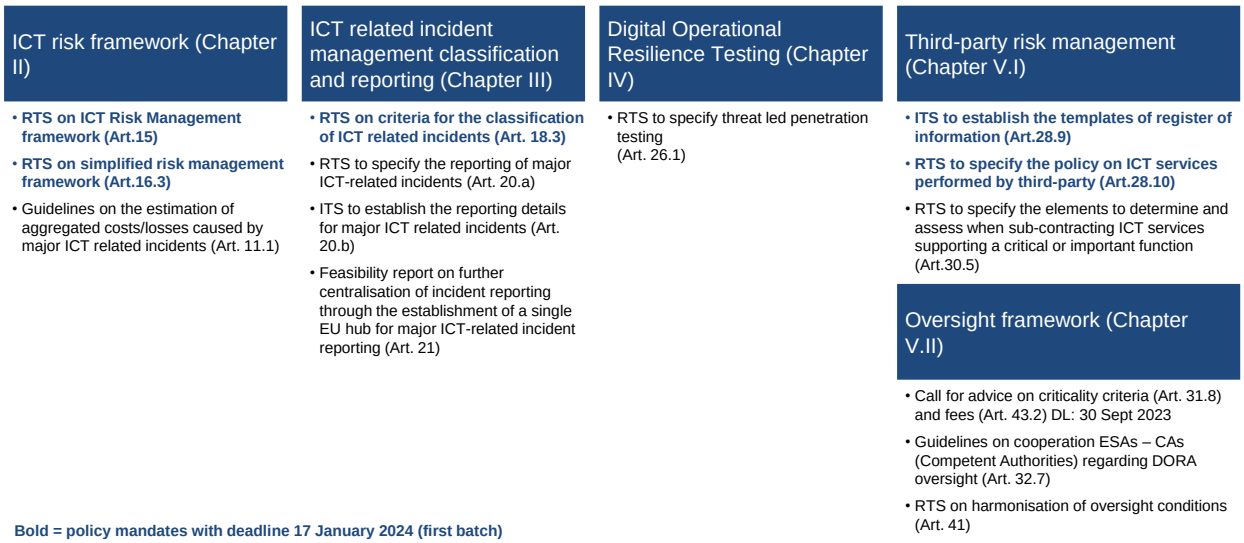
6. To operationalise the application, DORA mandates the European Supervisory Authorities (ESAs) to prepare jointly, through the Joint Committee (JC), a set of policy products with two main

[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 been asked by the European Commission to respond to a call for advice[4] 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 service providers will have to pay to be overseen. A discussion paper aiming at preparing the joint advice of the ESAs has been publicly consulted between 26 May and 23 June 2023. The final report is due by 30 September 2023.

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

Policy mandates	Public consultation	Finalise
Call for advice on criticality criteria and fees	**26 May – 23 Jun '23**	**30 Sep '23**
1st batch of mandates (Art. 15, 16(3), 18(3), 28(9) and 28(10) DORA)	**16 Jun – 11 Sep '23**	**17 Jan '24**
2nd batch of mandates (Art. 11(11), 20a, 20b, 26(11), 30(5), 32(7) and 41 DORA)	**Nov/Dec '23 – tbc**	**17 Jul '24**

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

    i. RTS on ICT risk management framework (Article 15) and RTS on simplified ICT risk management framework (Article 16(3))

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

Due to the interlinkages of the topics, the two mandates have been bundled together into single draft technical standards to comprehensively address the topic of ICT risk management.

The standards set out requirements for all financial entities with respect to: (i) ICT security policies, procedures, protocols and tools (including requirements on: governance, ICT risk management, ICT asset management, encryption and cryptography, ICT operations security, network security, ICT project and change management, physical security, ICT and information security awareness and training); (ii) Human resources policy and access control; (iii) ICT-related incident detection and response, (iv) ICT business continuity management, (v) Report on the ICT risk management framework review; and (vi) Proportionality.

In accordance with the mandate, the requirements set out in the standards are complementary to the requirements for the ICT risk management framework already set out in DORA and therefore should be read in conjunction with the DORA related articles (Articles 5-16).

The RTS further specifies simplified ICT risk management framework that applies only to five categories of smaller/less interconnected financial entities[5] and complements the requirements set out in Article 16 of DORA in the following areas: ICT risk management framework, Further elements of systems, protocols, and tools to minimise the impact of ICT risk, ICT business continuity management and Report on the ICT risk management framework review.

ii. <u>RTS on criteria for the classification of ICT-related incidents (Article 18(3))</u>

The draft RTS set out harmonised requirements for financial entities on: (i) the classification of ICT-related incidents by financial entities, (ii) the classification approach and materiality thresholds for determining major ICT-related incidents to be reported from financial entities to competent authorities, (iii) the criteria and the thresholds to be applied when classifying significant cyber threats, and (iv) the criteria to be applied by competent authorities for the purpose of assessing the relevance of major ICT-related incidents to relevant competent authorities in host Member States and the details of the information to be shared with them.

iii. <u>ITS to establish the templates for the register of information (Art.28(9))</u>

[5] Smaller less interconnected financial entities are: (i) small and non-interconnected investment firms, (ii) payment institutions exempted pursuant to Directive (EU) 2015/2366; (iii) institutions exempted pursuant to Directive 2013/36/EU in respect of which Member States have decided not to apply the option referred to in Article 2(4) of this Regulation; (iv) electronic money institutions exempted pursuant to Directive 2009/110/EC; and (v) small institutions for occupational retirement provision

The draft ITS establish harmonised templates for the register of information to be maintained by financial entities covering all contractual arrangements on the use of ICT services provided by ICT third-party service providers at individual, consolidated, and, sub-consolidated level (Article 28(3)).

The templates have been designed taking into account the threefold purpose of the register of information: (i) the register of information is part of the ICT risk management framework of financial entities (Article 28(1)); (ii) the register of information enables the effective supervision of financial entities' (Article 28(3)), including (iii) the designation of third-party service providers as critical at the level of the EU by the ESAs in the context of the oversight framework (Chapter V, Section II).

To simplify setting out the registers by the financial entities, the draft ITS contains two different set of templates for the registers at an individual entity level and at the sub-consolidated and consolidated level.

iv. <u>RTS to specify the policy on ICT services performed by ICT third-party providers (Article 28(10))</u>

The draft standards set out the requirements for all phases that should be undertaken by financial entities regarding the life cycle of ICT third-party arrangements management. In particular, the draft RTS specify the content of the policy regarding the use of ICT services supporting critical or important functions by dealing with the following aspects: (i) the pre-contractual phase (i.e. planning of contractual arrangements including the risk assessment, the due diligence and the approval process of new or material changes to those third-party contractual arrangements); (ii) the implementation, monitoring and management of contractual arrangements for the use of ICT services supporting critical or important functions; (iii) the exit strategy and the termination processes. The standards have been developed leveraging on the experience with management outsourcing arrangements.

Public consultation and next steps

10. The public consultation on all mandates included into the first batch will last until 11 September 2023. 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 13 July[6].

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

[6] Further details on the online public hearing will be made available on the websites and the social media channels of the three ESAs by 19 June.

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 January 2024.

13. As presented during the Joint-ESAs public event on DORA in February[7], the public consultation on the second batch of policy products is expected by end-2023.

Background

14. 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 Resilience (JC SC DOR)[8] 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[9].

[7] Joint ESAs DORA event - presentation (europa.eu)

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

[9] 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)