# 5. Digital operational resilience

Thomas Plomteux

The European regulation on digital operational resilience for the financial sector (the Digital Operational Resilience Act or DORA) entered into effect on 16 January 2023.[1] The provisions of DORA will apply as of 17 January 2025.

The impetus for this regulation was the industry's ever-increasing dependence on digital assets and processes. As a result, ICT risks pose a growing challenge for the operational resilience, performance and stability of the European financial system. In addition, the European Commission considered that previous legislation did not address this issue in a sufficiently detailed and comprehensive manner, did not provide financial supervisors with the most adequate tools to fulfil their mandate, and left too much room for divergent approaches within the EU single market. The European Supervisory Authorities (ESAs) had also issued joint technical advice calling for a more coherent approach to the management of ICT risks in the financial sector.

DORA is based on five pillars:

- The first pillar consists of key principles and requirements on ICT governance and risk management, inspired by relevant international and sectoral standards, guidelines and recommendations. These requirements concern specific functions in ICT risk management (identification, protection and prevention, detection, response and recovery, training and development, and communication) and underline the importance of an adequate policy and organisational framework. This pillar also covers the crucial and active role to be played by the management body in driving forward the ICT risk management framework and assigning clear roles and responsibilities for ICT-related functions.
- The second pillar contains requirements related to the management and classification of ICT-related incidents as well as provisions to harmonise and streamline the reporting of major incidents to the competent authorities. In addition, this pillar addresses the responsibility of competent authorities to provide feedback and guidance to financial entities and to transmit relevant data to other authorities with a legitimate interest. The aim is for financial entities to have to report major incidents to a single competent authority. In this context, the feasibility of an EU hub will also be examined by the ESAs, the ECB and the European Union Agency on Cybersecurity (ENISA). Last but not least, the incident reporting obligations under PSD2 will be fully integrated into this new reporting framework.
- The third pillar concerns the requirements for testing digital operational resilience, i.e. periodically assessing resilience to cyber-attacks and identifying weaknesses, shortcomings, or gaps, as well as the rapid implementation of corrective measures. While all financial entities are required to subject their ICT systems to testing, which can range from scanning for vulnerabilities to analysing software, only those entities identified by competent authorities will be required to perform advanced threat-led penetration testing (TLPT).
- Fourth, the regulation contains provisions to ensure proper management of third-party ICT risks. On the one hand, this objective will be achieved by imposing rules on how financial entities should monitor these risks and by harmonising key elements of the provision of services and the relationship with external ICT service

1 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

providers. On the other hand, the regulation aims to promote convergence in supervisory approaches to third-party ICT risks in the financial sector by establishing an EU oversight framework for critical third-party ICT service providers.

- The fifth and final pillar aims to increase awareness of ICT risks and related aspects. This pillar focuses on limiting the spread of these risks and supporting defensive capabilities and threat detection techniques, while explicitly allowing financial entities to establish mutual arrangements for information exchange on cyber threats.

With a view to achieving maximum harmonisation in the financial sector, DORA targets a wide range of financial entities, including central securities depositories, credit institutions, insurance and reinsurance companies, stockbroking firms, payment institutions and electronic money institutions.

DORA should be considered a *lex specialis* with regard to the EU directive on measures to ensure a high common level of cybersecurity in the Union (also referred to as the NIS 2 Directive).[1] This means that DORA's requirements, for example regarding ICT security or incident reporting, are at least equivalent to those of the NIS2 Directive and that institutions falling under DORA need only comply with the provisions of this regulation unless – which is not expected – the national legislation transposing the NIS2 Directive explicitly extends the directive's scope or provisions.

Given the strong link between the digital and physical resilience of financial entities, the obligations set out in Chapters III and IV of the Critical Entities Resilience Directive (CER)[2] do not apply to financial institutions covered by DORA either. Here, too, though, the national legislation transposing the CER Directive could expand the scope or provisions of the same.

The Bank is committed to ensuring the successful implementation of DORA:

- On the one hand, the Bank is actively contributing, under the auspices of the ESAs, to the creation of level 2 standards to clarify DORA in many areas. A first set of draft standards covering the ICT risk management framework, the criteria for classifying ICT-related incidents, the policy regarding ICT services offered by third parties that support critical or important business functions, and the templates to be used when reporting ICT third-party dependencies to the competent authorities has already been released. Most of these standards have since been adopted by the European Commission via delegated acts (not yet published in the Official Journal).[3] A second set of draft standards should be finalised by 17 July 2024 and will include provisions related to the reporting of major ICT-related incidents, advanced threat-led penetration testing, subcontracting of ICT services supporting critical or important business functions, and the oversight of critical third parties. The public consultation on this second set of standards ran until 4 March 2024.[4] More information on DORA-related policy mandates and instruments can be found in Box 9.
- On the other hand, the Bank is strongly committed to the successful implementation of DORA through increasing awareness in the sector by means of various seminars, communications and surveys; facilitating the integration of DORA into the Belgian legal order; developing the necessary ICT tools and processes for data collection and dissemination; adapting existing supervisory methodologies; and anticipating, insofar as possible, the impact that the oversight of critical third parties will have on its activities.

1 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.

2 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

3 See https://www.eba.europa.eu/publications-and-media/press-releases/esas-publish-first-set-rules-under-dora-ict-and-third-party.

4 See https://www.eba.europa.eu/publications-and-media/press-releases/esas-launch-joint-consultation-second-batch-policy-mandates.

BOX 9

# DORA policy instruments

DORA lays down several mandates for the European Supervisory Authorities (ESAs), in some cases in consultation or in agreement with the European Union Agency on Cybersecurity (ENISA) and/or the European Central Bank (ECB), to give form to the Level 1 text through common draft regulatory or implementing technical standards (RTS or ITS), guidelines and a report. Moreover, the European Commission has called on the ESAs for advice on two Commission delegated acts under DORA. The table below presents an overview of these mandates.

| ICT risk management (chapter II) | ICT-related incident management, classification and reporting (chapter III) | Digital operation resilience testing (chapter IV) | Management of ICT third-party risk (chapter V, section 1) |
|---|---|---|---|
| RTS on ICT risk management framework (Art. 15) | RTS on criteria for the classification of ICT-related incidents (Art. 18(3)) | RTS to specify threat-led penetration testing (Art. 26(11)) | ITS to establish the templated for the register of information (Art. 28(9)) |
| RTS on simplified ICT risk management framework (Art. 16(3)) | RTS to specify the reporting of major ICT-related incidents (Art. 20(a)) | | RTS to specify the policy on ICT services provided by third parties (Art. 28(10)) |
| Guidelines on the estimation of aggregated costs/losses caused by major ICT-related incidents (Art. 11(11)) | ITS to establish the reporting details for major ICT-related incidents (Art. 20(b)) | | RTS to specify the elements to determine and assess when subcontracting ICT services supporting a critical or important function (Art. 30(5)) |
| | Feasibility report on further centralisation of incident reporting through the establishment of a single EU hub for major ICT-related incident reporting (Art. 21) | | |
| | | | Managing of ICT third-party risk (chapter V, section 2) |
| | | | Call for advice on criticality criteria and oversight fees |
| | | | Guidelines on cooperative ESAs-NCA regarding DORA oversight (Art. 32(7)) |
| | | | RTS on harmonisation of oversight conditions (Art. 41) |

| Policy mandates with the deadline of 17 January 2024 (first batch) | Policy mandates with the deadline of 17 July 2024 (second batch) |
|---|---|

Source: NBB.

The remainder of this box describes these policy mandates and their current status in more detail. This overview is based on the DORA Level 1 text, [1] the draft policy instruments, and information published on the websites of the ESAs [2, 3, 4] and the European Commission. [5]

***Call for advice on criticality criteria and fees***

In December 2022, the Commission issued a call for advice to the ESAs in relation to two delegated acts under DORA, in order to specify further the criteria to designate critical ICT third-party service providers (subject to the EU oversight mechanism) and to determine the fees levied on such providers and the way in which they are to be paid. The ESAs published their joint response to the Commission on 29 September 2023. [6] In turn, the Commission published draft acts for public consultation (between 16 November and 14 December 2023). [7] The final acts were adopted by the Commission in the first quarter of 2024.

Quantitative and qualitative indicators have also been proposed in relation to criticality criteria, along with the necessary information to build up and interpret such indicators using a two-step approach. Minimum relevance thresholds have been put forward for the quantitative indicators, to be used as starting points in the assessment process to designate critical third-party providers.

In addition, the proposals clarify the types of estimated expenditures to be covered by oversight fees, the information to be used to determine the applicable turnover of CTPPs, the calculation basis and method, and practical issues relating to fee collection. Provision is also made for a financial contribution for voluntary opt-in requests.

***First batch of regulatory and implementing technical standards***

The technical standards mandated by DORA can be grouped into two batches depending on their deadline for submission to the European Parliament, the Council and the Commission. The first batch of final reports on proposed draft regulatory technical standards and implementing technical standards was published by the ESAs on 17 January 2024 and submitted to the European Commission, which has adopted most of these documents (i.e. the regulatory technical standards) via delegated acts.

The *RTS on ICT risk management framework and on simplified ICT risk management framework* identify further aspects related to ICT risk management with a view to harmonising tools, methods, processes and policies, complementary to those identified in the DORA Level 1 text. They further identify the key elements that financial entities subject to the simplified regime and of lower scale, risk, size and

1 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

2 See https://www.eba.europa.eu/publications-and-media/press-releases/esas-publish-first-set-rules-under-dora-ict-and-third-party.

3 See https://www.eba.europa.eu/publications-and-media/press-releases/esas-launch-joint-consultation-second-batch-policy-mandates.

4 See https://www.esma.europa.eu/press-news/esma-news/esas-specify-criticality-criteria-and-oversight-fees-critical-ict-third-party.

5 See https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13980-Critical-ICT-third-party-service-providers-criteria-fees_en.

6 See https://www.esma.europa.eu/press-news/esma-news/esas-specify-criticality-criteria-and-oversight-fees-critical-ict-third-party

7 See https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13980-Critical-ICT-third-party-service-providers-criteria-fees_en.

complexity will need to have in place and set out a simplified ICT risk management framework. There are a number of changes to the text as compared with the version that underwent public consultation, primarily relating to the introduction of further proportionality and, where possible, a risk-based approach; the removal of an article on governance and information security awareness from the general regime requirements (as a mandate for this was considered not to be included in the DORA Level 1 text); and the clarification of certain provisions, especially those in the articles on network security, encryption, access control and business continuity.

The *RTS to specify the policy on ICT services supporting critical or important functions* specify certain aspects of the governance arrangements, risk management and internal control framework that financial entities should have in place when working with ICT third-party service providers. They aim to ensure that financial entities remain in control of their operational risks, information security and business continuity throughout the lifecycle of contractual arrangements with ICT third-party service providers. The proposal submitted for public consultation was only amended to a limited extent. For example, it was clarified that the policy will apply to subcontractors for ICT services that support critical or important functions or material parts thereof, and financial entities will be given more leeway in updating their contractual arrangements with third-party service providers when review of this policy requires such updates.

The *RTS on classification of major incidents and significant cyber threats* specify the criteria and approach for the classification of major ICT-related incidents, the materiality thresholds of each classification criterion, the criteria and materiality thresholds for determining significant cyber threats, the criteria for competent authorities to assess the relevance of incidents for competent authorities in other Member States, and the details of the incidents to be shared with the latter. Compared with the version that was submitted by the ESAs for public consultation, significant changes have been made to the classification approach, the specification of the classification criteria and their thresholds, and the reporting requirements for recurring incidents, to introduce more proportionality, address issues raised by the financial sector and cover relevant cyber incidents.

The draft ITS on the register of information set out the templates to be maintained and updated by financial entities in relation to their contractual arrangements with ICT third-party service providers. The register of information will play a crucial role in the ICT third-party risk management framework of financial entities and will be used by competent authorities and ESAs in the context of supervising compliance with DORA and to designate critical ICT third-party service providers subject to the DORA oversight regime. Compared with the version that formed the object of public consultation, the information to be registered has been reduced and templates have been streamlined, financial groups will be allowed to use a single register as long as they are capable of fulfilling their reporting requirements to the competent authorities, and it has been clarified that financial entities will be required to document in the register those subcontractors that effectively underpin ICT services supporting critical or important functions or a material portion thereof.

***Second batch of regulatory and implementing technical standards***

A second batch of technical standards is due to be submitted to the European Parliament, the Council and the Commission by 17 July 2024. Proposals for these policy instruments were subject to public consultation from 8 December 2023 until 4 March 2024. This batch includes the following mandates.

The *draft RTS on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents* cover the content of major incident reports, the time limits for their submission and the content of the notification of significant cyber threats. They also ensure consistency with the incident reporting approach of the NIS2 Directive. With regard to the content of major incident reports, the draft RTS aim to strike an appropriate balance between providing competent authorities with essential information about each incident and not imposing a reporting burden on financial entities. With regard to the notification of significant cyber threats (to be reported on a voluntary basis), the draft RTS provide for short, simple and concise content.

The *draft ITS on the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat* cover aspects related to general reporting requirements and introduce the format and templates for reporting major incidents and significant cyber threats under DORA. With regard to the template, the draft ITS provide for a single template covering the initial notification as well as intermediate and final reports. The draft ITS also provide a data glossary, characteristics of the data fields and instructions on how to populate them.

The *draft Guidelines on aggregated costs and losses from major incidents* specify the estimation of aggregated annual costs and losses caused by major ICT-related incidents. They introduce reporting on gross costs and losses, financial recoveries and the net costs and losses caused by such incidents. The guidelines also propose basing the reference period for aggregation on an accounting year in order to rely on available figures from validated financial statements.

The *draft RTS on threat-led penetration testing (TLPT)* further specify the criteria to be used to identify financial entities required to perform TLPT, the requirements and standards governing the use of internal testers, the requirements in relation to scope, the methodology and approach for each testing phase, the results, the closure and remediation stages, and the type of supervisory and other relevant cooperation needed for implementation of TLPT and the facilitation of mutual recognition.

The *draft RTS on subcontracting of critical or important functions* specify the points that need to be determined and assessed when outsourcing ICT services supporting critical or important functions (or material parts thereof). The draft RTS follow the lifecycle of arrangements between financial entities and ICT third-party service providers when subcontracting ICT services supporting critical or important functions and set key requirements for financial entities in this regard, covering the risk assessment before ICT services supporting critical or important functions can be subcontracted, the contractual arrangements, the monitoring of subcontracting arrangements, information on material changes, and exit and termination rights.

The *draft Guidelines on oversight cooperation between ESAs and competent authorities* cover the detailed procedures and conditions for the allocation and execution of oversight tasks between competent authorities and the ESAs and details on the exchange of information (for instance regarding the designation of critical ICT third-party service providers or to ensure the follow-up of recommendations addressed to such providers).

The *draft RTS on oversight harmonisation* specify the information to be provided by ICT third–party service providers when making a voluntary request to be designated as critical; the content, structure and format of the information to be disclosed or reported by ICT third-party service providers; and the

details of the competent authorities' assessment of the measures taken by critical ICT third-party service providers based on the oversight recommendation. The mandate for the joint examination teams will be finalised in accordance with a slightly different timeline.

***Feasibility report on an EU hub***

Finally, the ESAs are tasked with assessing, in consultation with the ECB and ENISA, the feasibility of and conditions for the potential centralisation of ICT-related incident reporting at EU level. Such centralisation could take the form of a single EU hub for major ICT-related incident reporting, which could either receive relevant reports directly and in turn automatically notify national competent authorities or merely centralise relevant reports forwarded by national competent authorities, thus performing a coordinating role. A report on this topic will be submitted to the European Parliament, the Council and the Commission by 17 January 2025. With that in mind, the proposed EU hub will not, in any case, be operational at the time DORA becomes applicable to financial entities.