DORA (Digital Operational Resilience Act)

Updated in April 2023

The Crypto-Asset Markets Regulation (MiCA), the Pilot Regime and the Digital Operational Resilience Regulation (DORA) are key elements of the EU's Digital Finance Package published on 24 September 2020. MICA forms with the Pilot Regime the two major legislative proposals on digital assets proposed by the European Commission. The Commission's objective, through these proposals, is to encourage innovation based on the technology underlying this device, namely the "Distributed Ledger Technology" (DLT) while preserving financial stability, market integrity and investor protection.

The Regulation on digital operational resilience for the financial sector, also known as the Digital Operational Resilience Act or DORA, was published in the Official Journal of the European Union on 27 December 2022**. The Regulation entered into force on 16 January 2023 and will apply from 17 January 2025**. As DORA is a Regulation and not a Directive, it is binding in its entirety and directly applicable in all EU Member States.

The EU's Digital Operational Resilience Act (DORA) will have significant implications for financial services firms. Its main objective is to establish harmonised regulations at European level to ensure operational Resilience against cyber-attacks. DORA contains detailed lists of requirements designed to improve operational and security capabilities of financial entities but also to their critical **Information and Communication Technologies** "ICT" third-party providers, operating within the European Union.

Before DORA, financial institutions managed the main categories of operational risk mainly with the allocation of capital, but they did not manage all components of operational resilience. After DORA, they must also follow rules for the protection, detection, containment, recovery and repair capabilities against ICT-related incidents. This Regulation acknowledges that ICT incidents and a lack of operational resilience have the possibility to jeopardise the soundness of the entire financial system, even if there is "adequate" capital for the traditional risk categories.

1. Overview

This new regulatory framework includes two legislative acts:

- The Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on Digital Operational Resilience (so-called DORA Regulation) which defines uniform requirements to strengthen and harmonize the management of risks related to information and communication technologies (ICT) and the security of networks and information systems at EU level.
- The Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022 which amends existing directives such as CRD IV, PSD2, BRRD, Solvency2, IORP2, MiFID2, AIFM, ... in order to make them consistent with the new provisions of the DORA regulation.

a. Large scope of application

DORA covers all financial actors from credit institutions to **UCITS and AIFM management companies**, Crypto-asset service providers, Central Securities Depository, payment institutions, insurance companies and statutory auditors. It would also regulate critical third-party ICT providers operating within the European Union in financial services: they will each have a Lead Overseer (either EBA, ESMA or EIOPA) supervising the provider's procedures and arrangements to manage the ICT risks they could pose to financial actors.

For the record, ICT third-party service provider means an undertaking providing digital and data services, including providers of cloud computing services, software, data analytics services, data centres, but excluding providers of hardware components and undertakings authorised under Union law which provide electronic communication services as defined referred to in point (4) of Article 2 of Directive (EU) 2018/1972 of the European Parliament and of the Council.

b. Key aspects of the Regulation

- **ICT risk management**

Main target of DORA is to harmonize the rules on ICT risk management. The management body of the financial entity carries the ultimate responsibility for managing ICT risk, in that perspective the regulation sets out a list of duties and obligations to which management is subject.

Dora requires that firms conduct business impact analyses of their exposure to severe disruptions. Firms are required to identify their ICT risk environment and implement a comprehensive ICT risk management framework that guides and directs all ICT risk management work.

- **ICT incident reporting requirements**

ICT incidents should be categorized based on factors described in the regulation, such as the geographic extent of the incident, the criticality of the departments involved, and the duration of the incident. Major incidents must be reported to the relevant competent authority according to a three-tier procedure defined in the regulation.

Financial actors are required to put in place an ICT-related incident management process and develop capabilities to monitor, handle and follow-up on such incidents.

- **Digital Operational Resiliency Testing**

DORA outlines an obligation to implement a proportional and risk-based digital operational resilience testing programme. The programme must provide for the execution of a full range of appropriate tests, such as vulnerability assessments and scans, open source analyses and network security assessments. Critical ICT systems and applications must be tested annually, and some financial entities are required to perform so-called advanced threat-based penetration testing once every three years.

- **Third-party ICT service providers risk management**

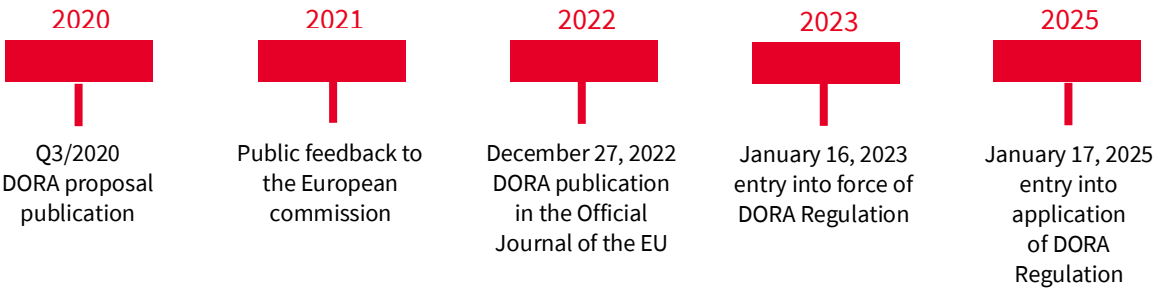
DORA also defines key milestones for acquiring new ICT services, requirements for terminating them, and specific contractual provisions to be included in contracts with third-party ICT service providers. DORA further requires financial entities to assess ICT concentration risk before entering into new contractual arrangements.

Third-party ICT risk is considered an integral part of the ICT risk management framework. Financial entities are therefore required to adopt and regularly review a third-party ICT risk strategy and maintain an information register describing all contractual arrangements with third-party ICT service providers.

- **Third-party ICT risk and exchange of information**

Financial entities may share information and cyber threat intelligence with each other, provided that such exchange of information is aimed at improving the digital operational resilience of financial entities, takes place within the trust of the communities of and that it is carried out in accordance with local legislation.

2. Chronology of events: key dates



The DORA regulation will apply directly to all EU member states from January 17, 2025. Over the next two years, the European Commission will issue delegated acts based on the final draft technical and implementing regulatory standards (RTS and ITS) to be submitted jointly by the European Supervisory Authorities (EBA, EIOPA, ESMA). These texts will clarify certain requirements of the DORA regulation (level 1) and will constitute level 2 of this new unified regulatory framework aimed at strengthening the digital operational resilience of the financial sector.

Directive 2022/2556 will have to be transposed by Member States by January 17, 2025.

3. Reference texts

- **Digital Operational Resilience Act (DORA)**
  - **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 (Text with EEA relevance): EUR-Lex - 32022R2554 - EN - EUR-Lex (europa.eu)
  - **Directive** (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022 amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards **digital operational resilience for the financial sector** (Text with EEA relevance) PE/42/2022/REV/1: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2556&from=EN

Christian.de-beaufort@sgss.socgen.com