BERNITSAS briefing

January 2024

FINANCIAL SERVICES BRIEFING: Special Edition

The DORA Framework: Preparation for the Digital Operation Resilience in the EU Financial Sector

This Briefing provides an introduction to the Digital Operational Resilience Act (DORA), the new EU cyber security regulatory framework for the financial sector, and the related compliance obligations of financial entities.

In This Issue

A. Introduction and Scope
B. Achieving Digital Operational Resilience
C. What does DORA Mean for Financial Entities?
D. Workplan for Financial Entities: When and How Should We Act?

A. Introduction and Scope

1. The Digital Operational Resilience Act (DORA)[1] is the regulatory framework for cyber security in the EU financial sector. Given the pivotal role of Information and Communication Technologies (ICT) in the provision of financial services and the increased digitalisation and interconnectedness, the Regulation introduces harmonised rules for the prevention and mitigation of ICT-related operational risk.
2. DORA is part of the EU Digital Finance Package, which also includes the Digital Finance Strategy, the EU Pilot Regime for DLT Market Infrastructures[2], the Regulation on Markets in crypto assets[3] and the amending Directive 2022/2556.
3. Unlike the NIS2 Directive[4], which provides legal measures to enhance the overall level of cybersecurity in the EU, DORA concentrates on the financial sector. Its scope covers a wide range of financial entities including, in general[5], the following:
   a. banks;
   b. payment institutions or e-money institutions;
   c. investment firms (private equity / venture capital firms);
   d. insurance or reinsurance undertakings or intermediaries;
   e. crypto-asset service providers; or
   f. crowdfunding service providers.
4. DORA also applies to ICT third-party service providers (for example cloud platforms).

B. Achieving Digital Operational Resilience

1. Digital operational resilience, according to DORA, is the ability of financial entities to build, assure and review their operational integrity and reliability. This is achieved by ensuring the ICT-related capabilities needed to address the security of the network and

[1] Regulation (EU) 2022/2554.
[2] Regulation (EU) 2022/858.
[3] Regulation (EU) 2023/1114.
[4] Directive 2022/2555.
[5] The list is not exhaustive, and exceptions may apply.

information systems that they use to support their activities. To obtain such resilience, financial entities must comply with detailed requirements concerning:

a. the management of ICT risk;
b. the management, classification and reporting of ICT-related incidents;
c. the regular testing of digital operational resilience; and
d. the management of ICT third-party risk.

C. What does DORA mean for Financial Entities?

1. Although financial entities already have security protection measures and systems in place, it is advisable that they perform a gap analysis to ensure compliance with DORA and detect the areas in which further action must be taken. For example, existing procedures for incident reporting will most probably have to be updated while security testing in accordance with the DORA criteria will become mandatory. In particular, financial entities[6] will have to ensure that they comply, among others, with the following obligations:

a. **ICT risk management** - Financial entities are required to:
   i. have in place an internal governance and control framework ensuring an effective and prudent management of ICT risk; management bodies must define, approve and oversee the implementation of all arrangements related to the ICT risk management framework;
   ii. have a sound, comprehensive and well-documented ICT risk management framework, that includes at least strategies, policies, procedures, ICT protocols and tools.
   iii. assign the responsibility for managing and overseeing ICT risk to an independent control function and take all appropriate measures to avoid conflicts of interest;
   iv. have a digital operational resilience strategy as part of their ICT management framework.
   v. use and maintain updated ICT systems, protocols and tools;
   vi. identify, classify and adequately document all ICT supported business functions, roles, and responsibilities and identify, on a continuous basis, all sources of ICT risk;
   vii. continuously monitor and control the security and functioning of ICT systems and tools and deploy adequate ICT security tools, policies and procedures;
   viii. have mechanisms to promptly detect anomalous activities and identify potential material single points of failure. All detection mechanisms must be regularly tested;
   ix. have a comprehensive ICT business continuity policy as well as response and recovery plans. ICT business continuity plans will be periodically tested;
   x. develop and document backup policies and restoration and recovery procedures and methods; set up backup systems; and
   xi. have in place crisis communication plans.

b. **ICT-related incident management, classification and reporting -** Financial entities are required to:
   i. define, establish and implement an ICT-related incident management process;
   ii. record all ICT-related incidents and significant cyber threats;
   iii. classify ICT-related incidents and determine their impact following the criteria of DORA;
   iv. report major ICT-related incidents to the competent authorities.

c. **Digital operational resilience testing -** Financial entities must:
   i. establish a sound and comprehensive digital operational resilience testing program,

[6] The obligations mentioned constitute a general framework for financial institutions, the components of which are, however, diversified depending on the type of financial entities (for example, financial entities qualifying as microenterprises are typically subject to less obligations).

which will include a range of assessments, tests, methodologies, practices and tools;

ii. carry out, at least every three years, threat-led penetration testing (TLPT), following the criteria outlined in the Regulation;

iii. adopt a strategy for ICT third-party risk, including a policy on the use of ICT services which support critical or important functions provided by ICT third-party service providers.

iv. maintain, both at entity and consolidated levels, a register in relation to all contractual arrangements on the use of ICT services provided by third parties;

v. report to the competent authorities on the number of new contractual arrangements; inform the authorities about any planned contractual arrangement on the use of ICT services supporting critical or important functions;

vi. undertake appropriate due diligence and assessments of any contractual arrangements they plan to enter into;

vii. assess whether an envisaged agreement in relation to ICT services supporting critical or important functions would lead to dependencies with service providers;

viii. ensure that certain key provisions are included in the contract.

2. DORA amends existing financial services legislation[7] to align it with its requirements. It is also accompanied by Directive (EU) 2022/255 amending existing legislation like CRD IV, MiFID II, PSD II etc., as regards digital operational resilience.

D. Workplan For Financial Entities: When and How Should We Act?

1. DORA will become applicable with a direct effect on Member States on 17 January 2025. By the same date, Member States must have introduced national legislative measures; in the meantime, the European Supervisory Authorities are working for the adoption of regulatory technical standards (RTSs) and Guidelines as well as the adoption of delegated Regulations to complement DORA.
2. Financial entities that fall within the scope of the Act should be compliant on the date of applicability (17 January 2025). To achieve this goal, they must prepare well in advance on both a technical level and a corporate governance level. This requires that they start familiarising themselves with the DORA obligations as early as the beginning of 2024, while actual preparation should start by the end of June 2024 or earlier, depending on the structure of each entity. Preparation should entail the internal cooperation of various departments while managing bodies should oversee the progress made. During the phase of preparation, the financial entities should also closely follow the related regulatory developments, that will shape the final framework for digital operational resilience, aligning their preparatory actions accordingly.

Contact

Anastasia Mallerou
Counsel
E amallerou@bernitsaslaw.com

[7] Regulations (EU) 1060/2009, 648/2012, 909/2014, 600/2014, 2016/1011.