Digital finance: Digital Operational Resilience Act (DORA)

2020/0266(COD) - 10/11/2022 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 556 votes to 18, with 38 abstentions, a legislative resolution on the proposal for a regulation of the European Parliament and of the Council on the digital operational resilience of the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014.

The Digital Operational Resilience Regulation (DORA) aims to achieve a high level of digital operational resilience for all regulated financial entities, such as banks, insurance companies and investment firms.

DORA creates a regulatory framework on digital operational resilience in which all firms must ensure that they can withstand, respond to and recover from all types of ICT-related disruptions and threats. The new rules will provide a strong framework to strengthen IT security in the financial sector.

The European Parliament's first reading position under the ordinary legislative procedure amends the proposal as follows:

Uniform requirements

DORA sets uniform requirements for the security of networks and information systems of companies and organisations operating in the financial sector, as follows:

- requirements for financial entities with regard to: (i) information and communication technology (ICT) risk management; (ii) reporting of major ICT incidents to the competent authorities and voluntary reporting of significant cyber threats to the competent authorities; (iii) reporting of major payment-related operational or security incidents by financial entities to the competent authorities; (iv) digital operational resilience testing; (v) information and intelligence sharing in relation to cyber threats and vulnerabilities; (vi) measures to ensure sound risk management of third-party ICT service providers;

- requirements for contractual arrangements between third party ICT service providers and financial entities;

- rules on the establishment of the supervisory framework applicable to critical third-party ICT service providers when providing services to financial entities, as well as those related to the exercise of tasks within that framework.

Scope of application

The new regulation should apply to **almost all financial entities**. It should not apply to insurance intermediaries that are micro, small or medium-sized enterprises. **Auditors** will not be subject to DORA but will be part of a future review of the regulation, where a possible revision of the rules may be explored.

Proportionality principle

The amended text clarifies that financial entities should implement risk management rules in accordance with the proportionality principle, taking into account their size and overall risk profile as well as the nature, scale and complexity of their services, activities and operations.

Governance and organisation

Financial entities should have a **governance and internal control framework** that ensures effective and prudent management of ICT risk to achieve a high level of digital operational resilience. The management body of the financial entity should define, approve, oversee and be responsible for the implementation of all provisions of the ICT risk management framework.

Critical ICT third–party service providers

The **European Supervisory Authorities** (ESAs), through the Joint Committee and upon recommendation from the Oversight Forum established pursuant to the Regulation should designate the ICT third–party service providers that are critical for financial entities, following an assessment.

In order for supervision to be properly implemented, financial entities should only be able to use the services of an ICT third-party service provider and which has been designated as critical if it has established **a subsidiary in the EU** within 12 months of the designation.

Oversight framework

Lead Overseers should be granted the necessary powers to conduct investigations, to carry out onsite and offsite inspections at the premises and locations of critical ICT third–party service providers and to obtain complete and updated information. Those powers should enable the Lead Overseer (i.e. the ESA designated in accordance with the Regulation) to acquire real insight into the type, dimension and impact of the ICT third–party risk posed to financial entities and ultimately to the Union's financial system.

To ensure a consistent approach to oversight activities and with a view to enabling coordinated general oversight strategies and cohesive operational approaches and work methodologies, the three Lead Overseers appointed should set up a **Joint Oversight Network** to coordinate among themselves in the preparatory stages and to coordinate the conduct of oversight activities over their respective overseen critical ICT third–party service providers.

The Lead Overseer should also be able to exercise its supervisory powers in **third countries**. The exercise of these powers in third countries should enable the Lead Overseer to examine the facilities from which ICT or technical support services are actually provided or managed by the critical third party ICT service provider.

Digital operational resilience testing

In order to assess preparedness to deal with ICT-related incidents, identify weaknesses, deficiencies and gaps in digital operational resilience and promptly implement corrective measures, financial entities, other than micro-enterprises, should establish, maintain and review a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk-management framework.

Under the amended Regulation, penetration tests should be carried out in functioning mode, and it should be possible to include several Member States' authorities in the test procedures. The use of internal auditors will be possible only in a number of strictly limited circumstances, subject to safeguard conditions.

Data protection

The ESAs and the competent authorities should be allowed to process personal data only where necessary for the purpose of carrying out their respective obligations and duties pursuant to this Regulation, in particular for investigation, inspection, request for information, communication, publication, evaluation, verification, assessment and drafting of oversight plans.