Digital finance: Digital Operational Resilience Act (DORA)

2020/0266(COD) - 27/12/2022 - Final act

PURPOSE: to strengthen the IT security of financial entities such as banks, insurance companies and investment firms to enable the European financial sector to maintain resilient operations in the event of a serious operational breaches.

LEGISLATIVE ACT: Regulation (EU) 2022/2554 of the European Parliament and of the Council 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.

CONTENT: the Digital Operational Resilience Regulation (**DORA Regulation**) **uniform requirements** for the security of network and information systems of companies and organisations operating in the financial sector as well as critical third parties which provide ICT (Information Communication Technologies)-related services to them, such as cloud platforms or data analytics services.

DORA creates a **regulatory framework on digital operational resilience** whereby all firms need to make sure they can withstand, respond to and recover from all types of ICT-related disruptions and threats. These requirements are homogenous across all EU member states. The core aim is to prevent and mitigate cyber threats.

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 in relation to the **contractual arrangements** concluded between ICT third-party service providers and financial entities;

- rules for the establishment and conduct of the **Oversight Framework** for critical ICT third-party service providers when providing services to financial entities;

- rules on **cooperation** among competent authorities, and rules on supervision and enforcement by competent authorities in relation to all matters covered by this Regulation.

Scope of application

The new Regulation will **apply to almost all financial entities**. It will 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 efforts asked from financial entities will be proportional to the potential risks. The Regulation states that financial entities will implement the rules on the principle of proportionality, taking into account their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations.

Governance and organisation

Financial entities will:

- 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;

- have a robust, comprehensive and well-documented **ICT risk management framework** that enables them to respond to ICT risk in a timely, efficient and comprehensive manner and to ensure a high level of digital operational resilience;

- put in place mechanisms to **promptly detect anomalous activities**. All detection mechanisms will be regularly tested.

Framework for the supervision of critical third-party ICT service providers

Critical third-country ICT service providers to financial entities in the EU will be required to establish a **subsidiary within the EU** so that oversight can be properly implemented.

To ensure that critical ICT third-party service providers are appropriately and effectively overseen on a Union level, this Regulation provides that any of the three European Supervisory Authorities (ESAs) will be designated as a Lead Overseer.

Lead Overseers will 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.

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 will 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 will also exercise its supervisory powers in third countries.

Digital operational resilience testing

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, will 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 Regulation, **penetration tests** will be carried out in functioning mode, and it will 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.

ENTRY INTO FORCE: 16.1.2023. The Regulation will apply from 17.1.2025.