# Digital finance: Digital Operational Resilience Act (DORA)

2020/0266(COD) - 24/09/2020 - Legislative proposal

PURPOSE: to lay down uniform requirements concerning the security of network and information systems supporting the business processes of financial entities with a view to achieving a high level of digital operational resilience for the financial sector.

PROPOSED ACT: Regulation of the European Parliament and of the Council.

ROLE OF THE EUROPEAN PARLIAMENT: the European Parliament decides in accordance with the ordinary legislative procedure and on an equal footing with the Council.

BACKGROUND: this proposal is part of the Digital Finance package, a package of measures to further enable and support the potential of digital finance in terms of innovation and competition while mitigating the risks. The digital finance package includes a new Strategy on digital finance for the EU financial sector with the aim to ensure that the Union's financial services legislation is fit for the digital age, and contributes to a future-ready economy that works for the people, including by enabling the use of innovative technologies. The Union has a stated and confirmed policy interest in developing and promoting the uptake of transformative technologies in the financial sector, including blockchain and distributed ledger technology (DLT).

This package also includes a proposal for a pilot regime on distributed ledger technology market infrastructures, a proposal on crypto-asset markets, and a proposal to clarify or amend certain related EU financial services rules.

The use of digital, or Information and Communication Technologies (ICT) has in the last decades gained a pivotal role in finance, assuming today critical relevance in the operation of typical daily functions of all financial entities. Digitalisation covers, for instance, payments, which have increasingly moved from cash and paper-based methods to the use of digital solutions.

However, digital, or Information and Communication Technologies (ICT), gives rise to opportunities as well as risks. Risks include an increased threat to cyber attacks and ICT disruptions.

ICT risks pose challenges to the operational resilience, performance and stability of the EU financial system. The absence of detailed and comprehensive rules on digital operational resilience at EU level has led to the proliferation of national regulatory initiatives (e.g. on digital operational resilience testing) and supervisory approaches (e.g. addressing ICT third-party dependencies).

This situation fragments the single market, undermines the stability and integrity of the EU financial sector, and jeopardises the protection of consumers and investors.

It is therefore necessary to put in place a detailed and comprehensive framework on digital operational resilience for EU financial entities.

CONTENT: this proposal aims to put into place a comprehensive framework which shall enhance digital risk management. In particular, it seeks to strengthen and streamline the financial entities' conduct of ICT risk management, establish a thorough testing of ICT systems, increase supervisors' awareness of cyber risks and ICT-related incidents faced by financial entities, as well as introduce powers for financial

supervisors to oversee risks stemming from financial entities' dependency on ICT third-party service providers.

***Scope of the Regulation***

To ensure consistency around the ICT risk management requirements applicable to the financial sector, the proposed Regulation shall cover a range of financial entities regulated at Union level, namely inter alia: (i) credit institutions, (ii) payment institutions, (iii) electronic money institutions, (iv) investment firms, crypto-asset service providers, (v) central securities depositories, (vi) central counterparties, (vii) trading venues, (viii) trade repositories, (ix) credit rating agencies, (x) crowdfunding service providers.

Such a coverage facilitates a homogenous and coherent application of all components of the risk management on ICT-related areas, while safeguards the level playing field among financial entities in respect of their regulatory obligations on ICT risk.

***Governance related requirements***

As this proposed Regulation is designed to better aligning financial entities' business strategies and the conduct of the ICT risk management, the management body shall be required to maintain a crucial, active role in steering the ICT risk management framework and shall pursue the respect of a string cyber hygiene.

***ICT risk management requirements***

Digital operational resilience is rooted in a set of key principles and requirements on ICT risk management framework, in line with the joint ESAs technical advice. These requirements, inspired from relevant international, national and industry-set standards, guidelines and recommendations, revolve around specific functions in ICT risk management (identification, protection and prevention, detection, response and recovery, learning and evolving and communication). To keep pace with a quickly evolving cyber threat landscape, financial entities are required to set-up and maintain resilient ICT systems and tools that minimize the impact of ICT risk.

***ICT-related incident reporting***

The proposal shall create a consistent incident reporting mechanism that will help reduce administrative burdens for financial entities and strengthen supervisory effectiveness. The reporting shall be processed using a common template and following a harmonised procedure as developed by the ESAs.

***Digital operational resilience testing***

The capabilities and functions included in the ICT risk management framework need to be periodically tested for preparedness and identification of weaknesses, deficiencies or gaps, as well as the prompt implementation of corrective measures. This proposal allows for a proportionate application of digital operational resilience testing requirements depending on the size, business and risk profiles of financial entities.

***Information sharing***

To raise awareness on ICT risk, minimise its spread, support financial entities' defensive capabilities and threat detection techniques, the proposed Regulation shall allow financial entities to set-up arrangements to exchange amongst themselves cyber threat information and intelligence. All voluntary information sharing arrangements between financial entities that this Regulation promotes would be conducted in trusted environments in full respect of Union data protection rules.

***Budgetary implications***

As the current Regulation foresees an enhanced role for the ESAs by means of powers granted upon them to adequately oversee critical ICT third-party providers, the proposal would entail the deployment of increased resources, in particular to fulfil the oversight missions (such as onsite and online inspections and audits exercises) and the use of staff possessing specific ICT security expertise.

The scale and distribution of these costs will depend on the extent of the new oversight powers and the (precise) tasks to be performed by the ESAs.

The estimated total cost impact is approximately EUR 30.19 million for the period 2022 - 2027. Therefore, no impact on EU budget appropriations is foreseen (except for the additional staff), as these costs will be fully funded by fees.