Digital operational resilience act (DORA)

The Single Rulebook – encompassing all EU legislation governing financial institutions – barely touches on operational risks relating to information and communications technologies (ICT). In September 2020, the Commission tabled a proposal for a regulation on the digital operational resilience of the financial sector (DORA), to introduce and harmonise key digital operational requirements across the EU, so as to make ICT operations resilient in the face of severe operational disruption and cyber-attacks.

Background

The EU's financial sector is regulated by a harmonised Single Rulebook, but it barely addresses digital operational resilience or ICT security. The current legislative framework is incomplete or inconsistently harmonised, obstructing the single market in financial services. The way in which ICT-risk related provisions have been addressed at EU level to date shows gaps or overlaps in important areas such as ICT-related incident reporting and digital operational resilience testing.

European Commission proposal

The proposed digital operational resilience act (DORA) has been designed to ensure that EU financial sector operations can withstand operational disruption and cyber-attacks. It offers a regulatory framework for digital operational resilience, obliging all firms to make sure they can withstand, respond to and recover from all types of ICT-related disruptions and threats. The proposed regulation covers a wide range of financial institutions, including credit institutions, payment and electronic money institutions, crypto-asset service providers, central securities depositories, trading venues and trade repositories. If the DORA proposal is formally adopted, the relevant European Supervisory Authorities (ESAs) will develop technical standards to govern all financial services institutions. Implementation will be supervised and enforced by the national competent authorities. The package aims to support innovation and the uptake of new financial technologies while providing an environment with an appropriate level of protection.

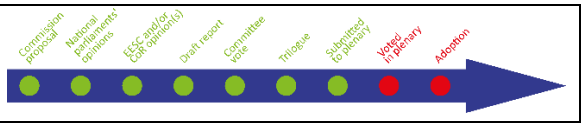
European Parliament position and provisional agreement

The Committee on Economic and Monetary Affairs (ECON) adopted its report on 1 December 2021. The Committee's decision to enter into interinstitutional negotiations was confirmed by plenary on 15 December 2021. The report recommended that the scope of the proposal be extended to insurance intermediaries that are not micro-, small or medium-sized enterprises (with some exceptions). It suggested that every financial entity should establish a control framework to ensure prudent management of all ICT risks. The report's amendments also introduced provisions relating to the proportionality principle.

Parliament and the Council reached a provisional agreement on 10 May 2022. The compromise text retains Parliament's recommendations, in particular the differentiated approach to the regulation of small, micro- and interconnected entities. Rapporteur Billy Kelleher stated that the provisional agreement was a 'key step in building up the EU's cyber resilience at the point where financial services and ICT interact', adding that the compromise was 'strong, progressive, yet future proofed'.

The ECON committee voted in favour of the provisional agreement on 12 July 2022. The text is due to be put to the vote during the November I plenary session.

First-reading report: 2020/0266(COD); Committee responsible: ECON; Rapporteur: Billy Kelleher (Renew, Ireland).



EPRS | European Parliamentary Research Service
Author: Issam Hallak, Members' Research Service
PE 738.197 – November 2022