Digital finance: Digital Operational Resilience Act (DORA)

2020/0266(COD) - 07/12/2021 - Committee report tabled for plenary, 1st reading/single reading

The Committee on Economic and Monetary Affairs adopted the report by Billy KELLEHER (Renew Europe, IE) on the proposal for a regulation of the European Parliament and of the Council on the digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648 /2012, (EU) No 600/2014 and (EU) No 909/2014.

The Commission's proposal for a legislative act on digital operational resilience in the financial sector (DORA) aims to establish uniform requirements for the security of networks and information systems to provide a comprehensive framework that will improve the management of digital risks by financial entities.

The committee responsible recommended that the European Parliament's position adopted at first reading under the ordinary legislative procedure should amend the proposal as follows:

Uniform requirements

The requirements for financial entities will concern: (i) information and communication technology (ICT) risk management; (ii) reporting of major IT-related incidents to the competent authorities; (iii) reporting of major payment-related operational or security incidents by credit, payment and electronic money institutions to the competent authorities; (iv) digital operational resilience testing; (v) information and intelligence sharing in relation to cyber threats and vulnerabilities; and (vi) measures to ensure sound risk management of third-party ICT service providers by financial entities.

This Regulation would be without prejudice to the competences of Member States concerning the maintenance of public security, defence and national security.

Scope of application

The proposal should apply to insurance intermediaries, that are **not micro, small or medium-sized enterprises**, with the exception of undertakings which rely exclusively on organised automated sales systems. Statutory auditors and small and medium-sized audit firms would also be excluded from the scope of the Regulation, with some exceptions. The Regulation would apply to ICT intra-group service providers, with the exception of the supervisory framework in Chapter V.

Proportionality principle

The amended text clarifies that financial entities should implement the rules introduced by Chapters II (risk management), III (management, classification and reporting of IT incidents) and IV (resilience testing) in accordance with the principle of proportionality, taking into account their **size, the nature, scale and complexity** of their services, activities and operations and their overall risk profile.

The Regulation should not apply to small non-interconnected investment firms, credit institutions and electronic money institutions exempted under the relevant EU directives. It should also not apply to small institutions for occupational retirement pensions. However, these exempted firms and entities would have to put in place a sound and well-documented ICT risk management framework, which would be reviewed at least once a year.

Governance and organisation

Financial entities should have in place an **internal governance and a control framework** that ensures an effective and prudent management of all ICT risks, with a view to achieving a high level of digital operational resilience. The management body should bear the ultimate responsibility for managing the financial entity's ICT risks and put in place procedures and policies that aim to ensure the maintenance of high standards of security, confidentiality and integrity of data.

Risk identification, protection, prevention, detection

Financial entities should, *inter alia*, (i) review as needed, and at least yearly, the criticality or importance of ICT-related business functions; (ii) ensure that data is protected from internal ICT risks, including poor administration, processing-related risks and human error; (iii)

record all ICT-related incidents that have an impact on the stability, continuity or quality of financial services, including where the incident has or is likely to have an impact on such services.

The purpose of the **ICT business continuity policy** should be to manage and mitigate risks that may adversely affect the ICT systems and services of financial entities and to facilitate their rapid recovery if necessary.

ICT security awareness programmes should apply to all staff, while the digital operational resilience trainings should apply to, at least, all employees with rights of direct access to the ICT systems and to senior management staff.

Reporting major ICT-related incidents

Financial entities could notify, on a **voluntary basis**, significant cyber threats to the relevant competent authority where they deem the threat to be of relevance to the financial system, service users or clients.

The competent authority should be informed in any event within **24 hours** of becoming aware of an incident in respect of incidents that significantly disrupt the availability of services provided by the entity or that affect the integrity, confidentiality or security of personal data held by the financial entity. For incidents that have a significant impact other than on the availability of services provided by the financial entity, the competent authority should be informed within 72 hours.

Upon receipt of the incident report, the competent authority should provide details of the major IT incident to EBA, ESMA or EIOPA, and the ECB, as appropriate, as soon as possible. The Single Resolution Board (SRB) should be informed where the affected financial entity falls under the Single Resolution Mechanism Regulation, while the CSIRTs should be notified where the affected entities fall under the CRS Directive.

Testing

Threat led penetration testing should cover at least the critical or important **functions and services of a financial entity**. In addition, the text has been amended with regard to the involvement of an ICT third-party service provider. Where the involvement of ICT third-party service provider could potentially have an impact on the quality, confidentiality or security of the ICT third-party provider's services to other customers, the ICT third-party service provider may contractually agree that the ICT third-party service provider is permitted to enter directly into contractual arrangements with an external tester. ICT third-party service providers may also enter into such arrangements on behalf of all their financial entity service users in order to conduct pooled testing.

At the end of the test, once the reports and remediation plans have been approved, the financial entity and the external testers should provide the single public authority designated under the Regulation with a confidential summary of the test results and documentation confirming that the threat led penetration test was conducted in accordance with the requirements.

Sound management of ICT third-party risks by financial entities

Financial entities should maintain and update a register of information relating to all contractual arrangements for the use of IT services provided by third-party IT service providers that support critical or important functions. Contractual arrangements for the use of ICT services should allow financial entities to take appropriate remedial action, which could include wholly terminating the arrangements, if no rectification is possible, or partially terminating the arrangements, if rectification is possible, under applicable law.

With a view to reducing the risk of disruptions at the level of the financial entity, in duly justified circumstances and in agreement with its competent authorities, the financial entity may decide not to terminate the contractual arrangements with the ICT third-party service provider until it is able to switch to another ICT third-party service provider or change to in-house solutions consistent with the complexity of the service provided.

Lastly, where contractual arrangements for the use of ICT services that support critical or important functions are entered into with a **third-party ICT service provider established in a third country**, financial entities should also take into account compliance with data protection and the effective enforcement of the rules set out in this Regulation.