Deloitte Audit SRL
The Mark Tower, 84-98 Grivitei Road,
8th Floor
Bucharest, District 1, Romania, 010735
Tel: +40 21 222 16 61
Fax: +40 21 222 16 60
www.deloitte.ro

Deloitte Banking Alert

September 2020

The European Commision takes steps to enhance financial services' digital operational resilience

The European Commission published its draft Digital Operational Resilience Act (DORA). The legislative proposal builds on existing information and communications technology (ICT) risk management requirements already developed by other EU institutions and ties together several recent EU initiatives into one Regulation.

The DORA aims to establish a much clearer foundation for EU financial regulators and supervisors to be able to expand their focus from ensuring firms remain financially resilient to also making sure they are able to maintain resilient operations through a severe operational disruption.

The context of the proposal

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 arising from it.** It is in line with the Commission priorities to make Europe fit for the digital age and to build a future-ready economy that works for the people. Digitalisation and operational resilience in the financial sector are two sides of the same coin. **Digital, or Information and Communication Technologies (ICT), gives rise to opportunities as well as risks. These need to be well understood and managed, especially in times of stress.**

ICT risks nevertheless continue to pose a challenge to the operational resilience, performance and stability of the EU financial system. The reform that followed the 2008 financial crisis primarily strengthened the financial resilience of the EU financial sector, only addressing ICT risks indirectly in some areas, as part of the measures to address operational risks more broadly. While the post-crisis changes to the EU financial services legislation put in place a Single Rulebook governing large parts of the financial risks associated with financial services, they did not fully address digital operational resilience. **It is therefore necessary to**

Deloitte.

put in place a detailed and comprehensive framework on digital operational resilience for EU financial entities.

What is the DORA focussing on?

The DORA proposal comes as regulators around the world have been looking more closely at how they can strengthen the operational resilience of the financial sector and of the individual firms within it. **Most important aspects of the new act include:**

- **Bringing 'critical ICT third party providers' (CTPPs), including cloud service providers (CSPs), within the regulatory perimeter**. These would be supervised by one of the European Supervisory Authorities (ESAs), who would have the power to request information, conduct off-site and on-site inspections, issue recommendations and requests, and impose fines in certain circumstances.
- **Setting EU-wide standards for digital operational resilience testing**, with a view to harmonising local rules across the EU, but leaving out automatic cross-border recognition of threat-led penetration testing (TLPT) for the time being.
- Harmonising **ICT risk management rules** across financial services sectors, based on existing guidelines.
- Harmonising **ICT incident classification and reporting**, and opening the door for the establishment of a single EU-hub for major ICT-related incident reporting by financial institutions.

How will DORA impact firms?

Although the DORA is expected to be negotiated by EU institutions over the next 1-2 years and further secondary legislation needs to be developed, we believe that **firms should be pro-active and consider the following actions:**

- **ICT third party providers will need to evaluate whether they will deemed 'critical'.** Those who are may need to establish new regulatory teams and analyse how they can best comply with the oversight framework being developed.
- **Larger firms should closely follow the ESAs as they flesh out the criteria requiring firms to carry out threat-led penetration testing**. Those newly in scope will need to develop a strategy to make the best use of these advanced tests.
- While large firms will already be applying many of the DORA's ICT risk management requirements, they should **assess whether their response and recovery strategies and plans respond appropriately to the expanded rules in these areas.**
- **All firms will need to develop or amend their incident reporting processes in line with the new rules.** In addition, firms may consider aligning these to their internal reporting processes to optimise resource allocation.

Deloitte.

Conclusions

The DORA legislation proposed by the Commission is an important first step in creating a regulatory framework for financial services operational resilience in EU law. This proposal will now have to be negotiated by the European Parliament and European Council. **The initiative would be consistent with the European Critical Infrastructure (ECI) Directive**, which is currently being reviewed in order to enhance the protection and resilience of critical infrastructures against non-cyber related threats.

Based on the past precedent of how similar FS legislative files have progressed in the EU, we can expect a final version of the primarily legislation to be agreed in the next 12 to 18 months, with further secondary legislation and technical standards fleshing out the specific application of the rules being developed thereafter by the ESAs.

For further questions regarding the aspects mentioned in this alert, please don't hesitate to contact us.

Dimitrios Goranitis
FSI Risk & Regulatory Advisory
Partner, Deloitte Central Europe
Tel: +40 751 250 884
Email: **digoranitis@deloittece.com**

Full document:

https://ec.europa.eu/transparency/regdoc/rep/1/2020/EN/COM-2020-595-F1-EN-MAIN-PART-1.PDF