

Digital operational resilience: Addressing risks of the digital transformation

Contribution by Ana Teresa Moutinho to the Eurofi
Magazine - September 2021

SPEECH

DATE:

08 Sep 2021

Digital operational resilience is essential for a well-functioning financial services sector. As the digital transformation of the sector accelerates, addressing the risks of digital innovation becomes increasingly important.

The proposal for a Digital Operational Resilience Act – or DORA, as part of the European Commission’s digital finance strategy, sets out to establish a comprehensive framework enabling a stronger supervision of the digital dimension of the sector. The proposal builds on work already conducted by the European Insurance and Occupational Authority (EIOPA), the European Banking Authority and the European Securities and Markets Authority (making up the European Supervisory Authorities, or ESAs).

EIOPA welcomes the overarching principles of the proposal. The proliferation of digital technology across the entire insurance value chain increases the exposure of insurers to the risk of a major disruption if technology fails whether through deliberate attack or system flaw. Similar risks can be identified for insurance intermediaries and in the occupational pensions sector. Regulatory requirements are therefore needed to ensure a proper management of such risks and capture the use of different technological solutions used.

The proposal aims to ensure that market participants have sufficient safeguards in place to protect against cyber attacks and other risks.

There are some clear benefits of such a framework, notably in terms of enhanced supervisory convergence across financial sectors and an overall stronger, more resilient financial sector. The implementation of DORA should improve the management of ICT risk by the financial sector, including improving testing of undertakings' ICT systems. It should also increase awareness of threats and risks among supervisors.

All three ESAs are in firm agreement with the main principles of DORA, in particular as it will help to close the gap in terms of oversight of critical third party providers. Nonetheless, the ESAs believe that, in its current form, the proposal warrants some further reflection. In particular, there is scope for more streamlined and effective governance; a need for more coherence between oversight recommendations and follow-up; and the need for more proportionality considering the wide scope of the Regulation.

One measure of a regulation's success is the effectiveness of implementation. For DORA to work effectively, the ESAs – who will bear the most responsibility for its implementation – must be appropriately empowered – in terms of both resources and regulatory powers. In EIOPA's view, the current proposals have not yet sufficiently considered this point, with regard to both the quantity and quality of resources needed.

An effective framework should bring confidence to the market and act as an enabler of the digital economy.

A sound cyber insurance market is also an enabler of the digital economy. From raising awareness of the risks and losses that can result from cyber attacks to facilitating responses and recovery, a well-developed cyber insurance market can play a valuable role in risk management across the economy.

The European cyber insurance market is growing rapidly. This is in part due to the overall increase in written contracts offered by insurers, but also because of the growing number of insurers providing cyber insurance. In addition, the increasing frequency of cyber attacks, coupled with stricter regulation regarding

cyber security as well as continued technological developments are all expected to increase demand for cyber insurance in the near future.

In the context of its cyber underwriting strategy, EIOPA has identified a number of conditions that are essential for a resilient cyber insurance market. These include the presence of appropriate cyber underwriting and risk management practices; adequate assessment and mitigation tools to address potential systemic and extreme risks; a mutual understanding between policyholders and insurers of contractual definitions, conditions and terms; and an adequate level and quality of data on cyber incidents available at European level. This last point has clear synergies with DORA, which also calls for the collection of data on cyber incidents. It is fundamental that a centralised collection of such cyber incidents is considered from the beginning and have in mind a potential wider use in the future. Ultimately, the access to cyber incident data, potentially a European Database, could be seen as a public good and underpin the further development of the European cyber insurance industry and act as an enabler of the digital economy.

As part of its work to support the market supervisory community through the digital transformation, EIOPA will therefore continue to implement its cyber underwriting strategy as well as standing ready to play an active role in the implementation of DORA.

LAST UPDATED ON:
8 Sep 2021