EUROFI VIEWS MAGAZINE - BERLIN SEPTEMBER 2020

Leena Mörttinen

Director General, Financial Markets Department, Ministry of Finance, Finland

Effective digitalization of financial services requires a comprehensive approach to systemic risk

Digitalization of financial services continues to benefit the economy through provision of competitively priced innovative services to customers. Covid-19 has shown that digital services can also contribute to resilience of societies in times of crisis. However, the digitalization also brings new risks. The reliance on digital infrastructure coupled with collection and processing of masses of highly sensitive data through complex value chains with multiple service providers, high speed of innovation and growing pressures to reduce costs create new vulnerabilities and risks on the level of the societies.

There is a growing awareness that these risks need to be properly managed by the financial institutions and their service providers. Requirements for risk management should be further enhanced in the legislation and supervisors should have adequate powers to enforce them. In addition, attention should be given on how to deal with the systemic nature of these risks as operational incidents involving financial services can quickly hamper normal functioning of the society. Financial markets are strongly interlinked with other critical sectors such as telecommunications and energy networks. Preparing for large scale incidents requires more than financial buffers. Contingency arrangements and redundancy capacities need to be in place, supported by a "whole-of-government-and-society" approach, taking into account also considera-tions of national security.

The "Digital Operational Resilience Act" currently prepared by the Commission provides a good starting point to deal with risks brought about by digitalization. However, the following areas should also be covered to provide a comprehensive approach to address also the systemic nature of the risks:

Legislative framework should provide for a clear and unquestionable obligation for cooperation and immediate infor-mation exchange between all relevant EU and national authorities: financial supervisors, central banks, cyber and other security authorities and government ministries. Provisions on professional secrecy or proprietary information should not impede on the information flow.

Operational incidents have a local impact and may threaten national security, which is why they require action by the relevant national authorities. This implies that these authorities need to have adequate influence on both incident preven-tion and incident handling. National authorities also need to have powers to deal directly with third party service provid-ers (TPPs).

In addition to legislative action the Commission should further non-legislative actions to bolster the operational prepared-ness in the financial sector. These actions could involve joint exercises, operational "playbooks", secure collaboration tools and investments in reinforcements of critical infrastructures and European redundancy capacities. Financial sector should be fully integrated into existing EU cross-sectoral crisis management arrangements. These actions should be re-flected also in the Digital Financial Services Strategy/Fintech Action Plan currently being prepared by the Commission.

In many Member States the core financial services have been designated as critical functions and financial infrastructure is considered as part of national arrangements on Critical Infrastructure Protection. However, such designation has not been made at the EU context. Consequently, the EU legislative framework on Critical Infrastructure Protection, which is currently under review, should be amended to include also financial services as discrepancies in definitions may lead into lack of cooperation and information sharing. Common cross-sectoral EU framework should be complimentary to the existing regulation in financial services. It would contribute to better understanding of interdependencies between differ-ent critical functions and services, including financial services, the changing security environment and emerging risks, in both the physical and in the cyber domains. ●