ANALYSIS

Financial sector contingency planning will help ensure continued functioning of society in all circumstances

Financial stability | 09.06.2023 | Päivi Tissari, Terhi Wathén

AUTHORS

Päivi Tissari
Senior Adviser

Terhi Wathén
Head of Division

The prevailing geopolitical uncertainties have brought an increase in operational risks and in threats to the financial infrastructure, which has heightened the need to be prepared for severe infrastructure disruptions. Against this background, the Finnish authorities put in place a backup system for everyday payments in 2022, the EU drafted legislation intended to bolster the resilience of financial services, and the European Systemic Risk Board (ESRB) assessed cyber risks facing the financial system.

Russia's war in Ukraine and Finland's NATO membership process have contributed to an increase

in the threats to Finland's critical financial infrastructure. In addition, financial sector digitalisation and the more widespread use of third-party services are adding to the risks affecting the technical systems of financial sector entities. More determined action must be taken to prepare for contingencies such as cyberattacks. If a severe cyberattack renders a bank unable to perform its functions, the problems will spread to other banks, possibly resulting in a loss of depositor and investor confidence in the banking sector.

In Finland, banks and other individual actors have long taken measures to improve their preparedness for various contingencies. The Bank of Finland, too, has made preparations for dealing with disruptions in the financial infrastructure and is able to support the financial sector's preparedness work, for instance within the framework of the National Emergency Supply Organisation and through participation in TIBER-FI[1] testing.

In 2022, the authorities put in place a backup system for safeguarding daily payments in situations where normal European payment systems or systems of specific banks would be unavailable due to a severe disruption or emergency in society.[2] If a Finnish bank or a significant branch of a foreign bank operating in Finland were to suffer a severe and prolonged disruption, the national emergency account system maintained by the Financial Stability Authority could, as necessary, be deployed to provide account and card services to the customers of that bank. The Bank of Finland, in turn, is responsible for safeguarding domestic interbank payments.

Finland has a collaborative system of preparedness in which the safeguarding of society's vital functions involves action from the authorities, the private and third sectors, and the general public. In September 2022, the first Government report[3] on security of supply was submitted to Parliament. The report notes that the Finnish financial markets' level of preparedness does not at present fully meet the principles of the Security Strategy for Society or the preparedness aims set by the Government, because the regulations concerning the contingency planning obligation of financial corporations are general in nature. This will be addressed in the future development work mentioned in the report.

The EU has also adopted regulations that will in future have a bearing on the work undertaken in Finland to ensure security of supply and preparedness. Major new directives include the Critical Entities Resilience Directive (CER Directive) and the Network and Information Security 2 Directive (NIS2 Cybersecurity Directive), which both entered into force on 16 January 2023.

The purpose of the CER Directive is to improve the resilience of services vital to the EU, while the NIS2 Cybersecurity Directive aims to strengthen the level of both the EU's and member states' national cybersecurity in respect of sectors and actors identified as critical. The two directives are

currently being transposed into Finnish law. The Digital Operational Resilience Act (DORA) is an EU Regulation that will enter into force in January 2025 and is designed to enhance the ICT risk management and system testing of financial market participants and raise supervisors' awareness of the cyber risks faced by supervised entities.

Preparedness for cyber threats and other operational risks requires that central banks devote continuous efforts to stress testing and training, among other things. The ESRB recommends that the authorities develop approaches to evaluating the impact of cyber incidents on financial stability under various scenarios and assess which measures are the most effective in responding to the incidents.[4] Building preparedness for threats helps to support financial stability and the continued functioning of society in both normal and extreme circumstances.

Notes

1. See: https://www.suomenpankki.fi/en/money-and-payments/tiber-fi-implementation-guideline/ ↑
2. Act on Certain Backup and Emergency Arrangements in the Financial Sector (666/2022). ↑
3. See: http://urn.fi/URN:ISBN:978-952-383-803-1. ↑
4. See: Advancing macroprudential tools for cyber resilience, ESRB, 2023. ↑

Key words

contingency planning, cyber risks, geopolitics, maintenance support performance