

23 February 2023

FSOR 2022

FSOR
FINANCIAL SECTOR FORUM
FOR OPERATIONAL RESILIENCE

Danmarks Nationalbank chairs the Financial Sector forum for Operational Resilience (FSOR), which is a public-private forum for collaboration aimed at increasing cyber resilience in the financial sector in Denmark. In addition to Danmarks Nationalbank, the key players in the financial sector in Denmark participate in this forum. In 2022, the ordinary meetings of FSOR were held in May and November. MasterCard joined FSOR as a member in 2022.

Risk analysis guides the work in FSOR

The FSOR members and Danmarks Nationalbank, which acts as secretariat of FSOR, collaborate on identifying and addressing operational risks that could affect the entire sector and potentially threaten financial stability. In 2022, FSOR had a strong focus on the risks in the wake of Russia's invasion of Ukraine. It also focused on shedding light on any risks associated with the use of cloud services. The risk analysis has identified a total of 41 risks, including several risks related to data protection and the ability to ensure quick and safe recovery following a cyberattack.

FSOR's risk analysis is updated every six months. Based on the results, FSOR assesses the need for further initiatives aimed at mitigating the identified risks. In 2022, FSOR decided to initiate a number of measures, including knowledge sharing on data protection and recovery and on the use of cloud services.

In addition to FSOR's risk analysis, risks in the central infrastructure are analysed by the Risk Forum for mutual Interdependencies (RGA). RGA is a forum for collaboration between Euronext Securities Copenhagen, Finance Danmark, e-nettet and Danmarks Nationalbank. FSOR's and RGA's risk analyses are coordinated on an ongoing basis.

Crisis management ensures cross-sectoral coordination in case of a crisis situation

The crisis management secretariat in Danmarks Nationalbank maintains a detailed crisis management plan established by FSOR to ensure coordinated action across the financial sector in the event of a crisis that may potentially threaten financial stability. The plan supplements the members' own crisis management plans and is coordinated with the national crisis management of the National Operative Staff (NOST).

In 2022, FSOR's crisis management was on heightened alert following Russia's invasion of Ukraine and coordinated with NOST regarding the energy situation and the risk of brown-outs.

FSOR's crisis management plan was tested twice. On 14 June 2022, a partial test was carried out with the aim of practising an 'unannoun-

ced' activation of the crisis management plan. On 10 November 2022, a comprehensive test of the entire plan was carried out. The goal was to practise the execution of the crisis management plan and to work in depth with a selected scenario. FSOR's crisis management plan is updated on a quarterly basis, e.g., on experience from crisis management tests.

During 2022, FSOR's crisis management secretariat visited all members of the crisis management collaboration. The visits focused, among other things, on the interaction between FSOR's crisis management plan and the members' local crisis management plans.

Tool to increase the sector's cyber maturity

Based on the risk analysis, FSOR has developed a tool that enables companies to self-assess their cyber maturity. The first version of the tool, called FSOR baseline, was launched in early 2022 and has been used to collect data in relation to Danmarks Nationalbank's survey of cyber resilience among FSOR members. e-nettet is the system owner, and a working group under FSOR is developing the tool further.

TIBER-DK tests critical financial sector players

Since the beginning of 2019, Danmarks Nationalbank has coordinated threat-based testing of cyber resilience among critical players in the financial sector under the TIBER-DK programme. TIBER testing simulates advanced cyberattacks in actual production environments. In 2022, the programme continued according to plan.

In 2022, learnings from the TIBER tests was analysed and shared through recommendations to the participants and FSOR. The annual threat landscape report, prepared by Nordic Financial CERT with the involvement of relevant parties for use in the TIBER tests, was published in December 2022. NFCERT has subsequently presented the report to FSOR. General experience from the tests has been shared with TIBER-EU and has also played a role in the work on the details of the Digital Operational Resilience Act (DORA), under which threat-based testing similar to TIBER will be a future requirement.

Peter Ejler Storgaard

Chair of FSOR

Director and Head of Financial Stability in Danmarks Nationalbank