FSOR

FINANCIAL SECTOR FORUM
FOR OPERATIONAL RESILIENCE

15 April 2020

Annual report 2019

In 2019, the Financial Sector forum for Operational Resilience (FSOR) continued the work to improve the operational resilience of the sector. During the year, a number of new measures were launched, including an update of the FSOR's risk analysis for the financial sector as a whole, review of the crisis management plan, increased focus on the involvement of the sector's vendors, and cooperation across critical sectors in Denmark. In addition, the defence against cyber attacks in the major banks and the vital parts of the financial infrastructure are tested within the framework of TIBER-DK.

The FSOR was established in 2016 with the aim of increasing the financial sector's resilience to operational incidents. The work also comprises cyber attacks that could threaten financial stability and the real economy.

Members are the key players in the financial sector. These include the systemically important banks, data centres that store and process parts of the sector's data and the companies that own the financial infrastructure.

The FSOR is setting the agenda for the joint work on operational resilience in the Danish financial sector.

New measures resulting from COVID-19

In the first months of 2020, COVID-19 has challenged the financial sector, Denmark and the rest of the world. Since the beginning of the crisis, members of the FSOR have focused on ensuring staffing for the sector's critical business functions – also in case the crisis worsens.

The financial institutions have been quick to implement measures to protect critical business functions and employees. This includes implementation of split teams, virtual meetings and working from home.

The operation of the sector's critical functions has so far been stable, and there are currently no systemic issues in the financial sector. Therefore, the FSOR's crisis management plan has not been activated as a result of COVID-19.

The FSOR is collecting structured information on the current situation on a daily basis across the financial sector. Data are processed and are disseminated through regular virtual meetings with members.

The FSOR also acts as the link between the financial sector and the national crisis response, NOST. The data collected by the FSOR from the financial sector are included in the national situational picture.

New initiatives as a result of an updated risk analysis

The FSOR's work on operational risks is based on an analytical foundation. A risk analysis is performed at sector level to identify operational risks that could potentially threaten financial stability.

The risk analysis is a corner stone in FSOR's work. It provides a structured basis for a targeted prioritisation of future initiatives to make the sector more resilient. In this way, the FSOR ensures that it is targeting its efforts to what is most valuable both for the sector as a whole and for the Danish society.

In 2019, FSOR prepared a new risk analysis for the financial sector. The risk analysis comprises a comprehensive mapping of the most critical business activities, including the systems and vendors used. The analysis also includes information on historical incidents, vulnerabilities and threats. The identified operational risks are assessed

in terms of probability and impact – and for the most critical risks, mitigating actions are initiated.

Going forward, the FSOR's risk analysis will be structured according to an annual wheel, and will be updated at regular intervals.

Increased cooperation with vendors on cyber resilience

In previous risk analyses performed by the FSOR, it was identified that vendors are important to the sector's operational resilience, including cyber resilience. This has given rise to a dialogue with critical vendors, and in February and May 2019, workshops were held with the participation of FSOR members and the critical vendors.

The FSOR considers it important that dialogue and cooperation with critical vendors continue. In 2020, vendors will be further involved in the financial sector's efforts to increase cyber resilience.

TIBER-DK gives focus on cyber resilience at senior management level

Danmarks Nationalbank is the authority for the TIBER-DK programme (Threat Intelligence Based Ethical Red-teaming) and has developed the Danish TIBER-DK framework based on the European TIBER-EU in close cooperation with the Danish financial sector.

The TIBER-DK programme tests the largest financial institutions, infrastructure companies and data centres. In these tests, an ethical hacker team tries to gain access to pre-specified functions and data that are critical both to the participant being tested and to society.

TIBER-DK tests aim to make the sector better at identifying and stopping attacks. The test is based on the tactics, techniques and procedures considered the most realistic formed on intelligence-based threat information. Testing the institutions will strengthen cyber resilience and promote financial stability.

In 2019, TIBER-DK started testing the participating institutions. Danmarks Nationalbank facilitates the tests and the knowledge-sharing among the participants of TIBER-DK. Lessons learned from the the first TIBER-DK tests have given rise to an update of the TIBER-DK framework.

The 2020 report on the generic threat landscape on which the TIBER-DK test is based was prepared by Nordic Financial CERT, NFCERT, with input from the TIBER-DK participants, the Centre for Cyber Security, the Security Alliance and Danmarks Nationalbank. The NFCERT presented the report and the current threat scenario to the FSOR at a meeting on 16 December 2019.

It is still too early to extract any general results from the tests. However, TIBER-DK has already put a spotlight on cyber resilience in the sector. There are several participants who conduct pre-testing of TIBER-DK or projects in preparation for the actual TIBER test. For the participants who have completed the TIBER-DK test or are in the process, the TIBER framework has provided a focus at the highest management level. Participants are also inspired by the TIBER-DK framework in their own tests and use, for example, the current threat scenario in their own red team tests.

Crisis management plan provides a strong foundation

In connection with its establishment in 2016, the FSOR established a crisis management plan at sector level which supplements its members' own crisis plans and the national crisis response, NOST. The crisis management plan is regularly tested to ensure that the plan works in practice in the event of a serious incident in the sector.

It is no longer a question if cyber criminals have the capacity to penetrate central systems. We know they can. It is therefore essential to have a detailed plan to ensure coordinated action across the financial sector in the event of a crisis.

In 2019, the FSOR crisis management plan was updated with a focus on making it more operational. At the same time, the possibility of virtual gatherings and partial activation of the FSOR's crisis response was introduced.

As part of the roll-out of the updated crisis management plan, Danmarks Nationalbank held bilateral meetings with all FSOR participants in 2019. The purpose of the meetings was, among other things, to ensure that the crisis response plan is properly linked to the local plans.

In 2019, the sectors crisis management plan was tested several times. In June 2019, a test of a virtual communication platform was conducted. In September 2019, the activation of the crisis response

was tested. And in the most recent test in November 2019, 22 organisations and about 100 people from the financial sector participated in a comprehensive test of a ransomware attack.

The test in November confirmed that the crisis response plan is a well-functioning tool for structuring and managing a crisis situation, and that the virtual communication platform can be used to share material and to host meetings.

The ongoing tests ensure that we are standing on a strong foundation. We cannot predict exactly what will happen if the financial sector is hit by a major operational incident. But the more we have practiced and know the workings and dependencies of the sector, the better we can deal with a crisis when it hits us.

FSOR collaborates with other critical sectors

In 2018, the national cyber strategy was launched. The strategy identifies six critical sectors in Denmark, including the financial sector.

In connection with the roll-out of the strategy, a decentralised cyber and information security unit, DCIS, was established for each sector, and a sub-strategy for each sector's cybersecurity was developed.

Danmarks Nationalbank, which chairs and provides secretariat services to the FSOR, works closely with DCIS-Finans, which is headed by the Danish Financial Supervisory Authority, in an effort to increase operational resilience in the financial sector. Danmarks Nationalbank and the Danish Financial Supervisory Authority also participate in the cooperation across the critical sectors under the auspices of the Centre for Cyber Security (CFCS). One of the tasks in this context is to map interdependencies between the critical sectors.

Increased involvement of the insurance and pension industry

In 2019, the FSOR's membership was expanded with two representatives from the insurance and pension industry: PensionDanmark and Codan. Together with the trade association Insurance & Pension Denmark, they represent the insurance and pension industry in the FSOR.

In 2019, the insurance and pension industry was also enrolled in the FSOR's crisis management plan and has begun work on designing a risk analysis for the industry based on the same principles as the risk analysis covering the rest of the financial sector.

As a new member of the FSOR, NFCERT can provide insight on threats

At least once a year, it is assessed whether all relevant actors are represented in the FSOR. At the FSOR meeting in November, it was decided to invite NFCERT into FSOR. NFCERT plays a major role in the knowledge-sharing of incidents, threat assessments and international cooperation on incidents. NFCERT accepted the invitation.

Thank you to the FSOR members for a fruitful cooperation.

Karsten Biltoft
Chairman of FSOR, Head of Financial Stability
15 April 2020