19 January 2021

Annual report 2020

FSOR

FINANCIAL SECTOR FORUM FOR OPERATIONAL RESILIENCE

Annual report 2020

In 2020, the coronavirus dominated conversations in the public space, in the workplace and around the dining table at home – and the pandemic has demanded focus from public authorities, corporations and the individual citizen. Naturally, the coronavirus has taken some focus away from other important agendas – including cybersecurity. Before the coronavirus outbreak, cyber attacks were one of the biggest concerns for the stability of the financial sector, and this is still the case. According to the Centre for Cyber Security, more phishing emails were sent to Danish authorities and corporations than usual during the coronavirus pandemic. Despite the current challenges posed by the coronavirus situation, it is therefore important to continue to keep a strong focus on the key risks in the sector.

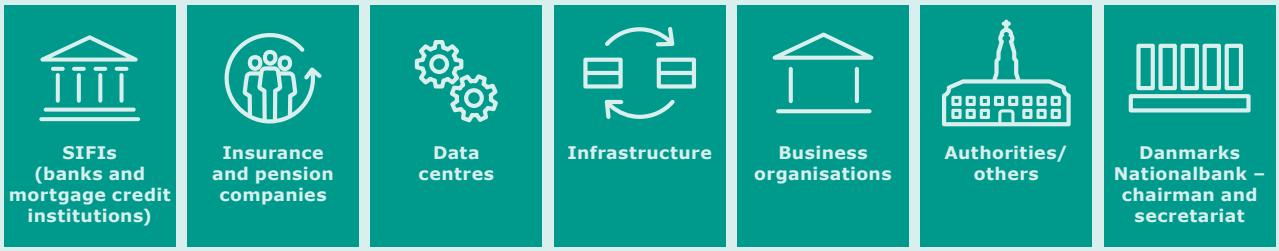
FSOR has managed to focus both on handling the special situation during the coronavirus outbreak and on driving the operational resilience agenda forward.

In 2020, the members of the Financial Sector Forum for Operational Resilience, FSOR, have managed to focus both on handling the special situation during the coronavirus outbreak and on driving the operational resilience agenda forward.

During 2020, FSOR's risk analysis has been updated twice and the risk analysis methodology has been published. Based on the results of the risk analysis, new measures have been initiated, including the preparation of a joint baseline for managing cyber risks, which will contribute to increasing the maturity level across the sector. The insurance and pension industry has also prepared a risk analysis of its operational risks. This means that the whole financial sector is now covered by a risk analysis.

In 2020, Danmarks Nationalbank has examined the cyber resilience in the financial sector based on the organisations' self-assessment. The survey provides the individual organisations with an opportunity to benchmark themselves against the rest of the sector. Furthermore, the testing of safeguards against cyber attacks has continued in the individual organisations via threat-based red team testing within the framework of TIBER-DK.

In 2020, based on reports from the sector, the Crisis Management Team has continuously formed situational overviews in connection with the coronavirus outbreak, and the critical functions of the sector have not been affected by the outbreak. At the same time, the crisis management plan has been tested twice, including for the first time as part of a cross-sectoral crisis management exercise orchestrated by the Centre for Cyber Security and with the participation of Denmark's six critical sectors.



Financial Sector Forum for Operational Resilience

In 2016, the financial sector in Denmark established a private-public partnership called the Financial Sector Forum for Operational Resilience, FSOR, to increase the sector's operational resilience to cyber attacks, among other threats.

FSOR is a voluntary, yet binding, partnership whose 25 members are the core players of the financial sector. The FSOR members are:

- The largest and systemically important financial institutions, SIFIs and insurance and pension companies.
- Data centres that operate critical systems and store and handle parts of the sector's data.
- The corporations that own the infrastructure, including financial transaction platforms.
- Financial business organisations.
- Central authorities. Danmarks Nationalbank chairs FSOR and provides secretariat services.

FSOR focuses on the systemic risks that can threaten financial stability and the real economy, and sets the current agenda for the joint work with operational resilience in the Danish financial sector.

The FSOR members are represented in a number of forums in which knowledge sharing is a key element. This is the case in the sector, where NFCERT plays a key role in knowledge sharing about incidents and threat assessments. This also applies between the six critical sectors in Denmark under the auspices of the Centre for Cyber Security as well as internationally, for example under the auspices of Nordic collaboration and collaboration in the European Central Bank, ECB.

The Coronavirus outbreak has not affected critical functions in the sector

With the coronavirus outbreak at the beginning of 2020, FSOR's members have focused on ensuring staffing of the critical tasks that the sector performs. In general, the sector has not been challenged in terms of its ability to perform the functions that are critical to society. Consequently, the crisis management plan has not been activated during the pandemic, but the situation has been monitored closely. The sector has submitted ongoing situational awareness reports to the FSOR Crisis Management Secretariat, which has structured the information across the financial sector. This information is shared with the National Operative Staff, NOST, which is responsible for the national crisis response.

The risk analyses sets agenda for joint actions in FSOR

The sector works together to identify and address systemic risks on a structured basis. A central element in this collaboration is the preparation of a risk analysis, which contributes to identifying the operational risks that could potentially threaten the stability of the financial system and which provides a structured basis for prioritising measures aimed at reducing such risks.

The risk analysis uses a number of sources to identify the risks that the financial sector faces. This includes an analysis of systemic dependencies and key business processes, past incidents, threat assessments and multiple questionnaires.

In 2020, Danmarks Nationalbank published the methodology of the risk analysis on the website *(link)*, so that others can benefit from it. The methodology is generic and can also be used in sectors other than the financial sector.

The risk analysis is updated every six months. Seven new risks have been identified in connection with the updates in 2020, and the existing risks have been re-assessed in terms of probability and consequence. By end of 2020, FSOR has identified 39 operational risks with the potential to threaten financial stability.

During 2020, the insurance and pension industry has also prepared a risk analysis based on the same methodology as the rest of the financial sector. This means that the whole financial sector is now covered by a risk analysis.

FSOR has identified 39 operational risks with the potential to threaten financial stability, and the members work together to mitigate the key risks.

VP Securities, Finance Denmark, e-nettet and Danmarks Nationalbank work closely together to identify and manage risks and incidents arising from interdependences between the VP settlements, retail payment systems and Kronos2.

Baseline will be a powerful tool to improve cyber resilience

Based on the risk analysis conclusions, FSOR started in 2020 to develop a joint *baseline* for the cyber resilience work across the sector's critical organisations and suppliers.

Baseline will formulate specific and measurable recommendations for cyber resilience in various areas, such as data protection or governance, in accordance with the existing legislation and established international standards. The aim is to develop an IT platform in which each organisation can "measure" its current cyber resilience on a voluntary basis and receive specified concrete actions that can be taken to achieve a desired level.

The work with *baseline* began in 2020. The areas to be covered by *baseline* have been decided, and the future work process has been established. In addition, an external consultant has been employed to facilitate the process and contribute to setting up the platform. A cost financing distribution has also been approved by FSOR. The first parts of *baseline* are expected to be ready around summer 2021.

Survey of cyber resilience shows progress since 2018, but there is still work to be done

In the summer of 2020, Danmarks Nationalbank conducted the third survey on the cyber resilience of the operational participants in FSOR. Similar surveys were conducted in 2016 and 2018. However, the bar is raised in the surveys in line with the current development in risks. As something new, a group of insurance and pension companies and several key suppliers also participated.

Based on the organisations' self-assessment, the survey provides a comprehensive overview of cyber maturity in the financial sector. The survey for 2020 indicates a significant improvement relative to the surveys in 2016 and 2018, but also highlights specific areas in which the level can still be raised both individually and jointly. The overall results were discussed at the FSOR meeting in November to identify joint focus areas. Danmarks Nationalbank has also provided

individual feedback for use in each FSOR member's further work to increase cyber resilience in its own organisation.

TIBER-DK tests the sector's safeguards to achieve learning and strengthen cyber resilience

TIBER-DK was formally established in December 2018 as one of the very first TIBER programmes in Europe and followed the established test plan in 2020.

A TIBER test simulates the advanced attacks from organised criminal cyber groups or state-sponsored groups in live production environments. Danmarks Nationalbank supports these tests and facilitates knowledge sharing among the participants in TIBER-DK. TIBER 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 in relation to intelligence-based threat information.

After each test, a test report is prepared as well as a plan for remedying the weaknesses and vulnerabilities found at the individual participants. Workshops are also held to anchor the valuable learning and results from the test.

The experience is that TIBER makes a difference and provides value because the test creates attention at all levels in the tested organisation, including at senior management level. In addition, the results and learning from the tests provide the basis for the implementation of specific improvements that increase cyber resilience, for example when the security of the systems is strengthened or processes are improved.

It is a great strength of TIBER that the learning lies in the defence against "real" threats and the most realistic methods of attack in relation to the participants' own business activities and functions that are critical to society. Each year, a threat landscape report is prepared for use in connection with the TIBER tests. This year, the report has been prepared by NFCERT with involvement of relevant parties.

The crisis management team monitors the coronavirus situation and ensures coordination across the sector in the event of a crisis

Despite the good preventive measures, operational incidents may occur. It is therefore essential to have a detailed plan to ensure coordinated action across the financial sector in the event of a systemic crisis.

In connection with its establishment in 2016, FSOR set up a crisis management plan at sector level which supplements its members' own crisis plans and the national crisis response under the National Operative Staff, NOST.

The crisis management plan is tested twice a year to ensure that the plan works in practice in the event of a serious incident in the sector. A crisis management exercise was held on 26 August. During the exercise, several crisis scenarios were successfully managed simultaneously, as well as switching from partial to full activation, and handling of replacement of the crisis management. On 19 November, coordination across the six sectors that are critical to society was tested in connection with a fictitious phishing attack. The Centre for Cyber Security orchestrated the exercise, and this was the first time that a test was held across the critical sectors. The exercises confirm that the financial sector's crisis management plan is a well-functioning tool for structuring and managing a crisis situation, and important knowledge was obtained in relation to improving operational coordination across the six critical sectors. Virtual crisis management was used in this year's exercises, and the use of the virtual platform as a communication tool has matured significantly in the course of the year.

In 2020, coordination of an incident across the six critical sectors in Denmark was tested for the first time.

In 2020, the coronavirus situation also contributed to learning points which have resulted in updates to the FSOR crisis management plan, which is now available in version 3.6. In addition, a workshop was held in Vejle on 5 March and a webinar was held on 27 October aimed at maintaining the FSOR members' crisis management knowledge.

The Secretariat has prepared an updated plan for the FSOR crisis management 2021-2023 which focuses on maturation and cross-sectoral collaboration.

FSOR collaborates with other critical sectors in Denmark

As part of the national cyber strategy, six critical sectors have been identified in Denmark. A decentral cyber and information security

unit, DCIS, has been established for each of these sectors. The Danish Financial Supervisory Authority handles the function as DCIS for the financial sector.

Danmarks Nationalbank, which chairs and provides secretariat services for FSOR, participates in the DCIS Forum together with the Danish Financial Supervisory Authority. The six critical sectors participate in the network, which is facilitated by the Centre for Cyber Security. The object of the DCIS forum is to increase knowledge sharing, strengthen coordination across the sectors that are critical to society and initiate and implement joint actions. One of the purposes of the joint crisis management exercise in November was to meet this object. In addition, the focus is on knowledge sharing about alerts, incident management and crisis management. The DCIS forum has set up a working group aimed at ensuring effective sharing of knowledge about threats across sectors. NFCERT participates in this work on behalf of the financial sector.

CIISI-EU has established a common knowledge sharing platform

In 2017, the ECB decided to establish a public-private collaboration between the most important European financial players known as the Euro Cyber Resilience Board, ECRB. At the beginning of 2020, the ECRB adopted a so-called "Cyber Information and Intelligence Sharing Initiative", CIISI-EU, under which a common platform has been established for knowledge sharing at strategic, tactical and operational levels between the participants in the EU. Danmarks Nationalbank is formally a member of CIISI-EU and will look at how threat information can be exchanged for the benefit of more parties.

Thank you to the FSOR members

A big thank you to the FSOR members for their good collaboration and for contributing to improving cyber resilience across the sector. A warm thank you is also extended to the participants in the working groups for their great commitment to producing these tangible results to the benefit of the overall financial sector.

Karsten Biltoft
Chairman of FSOR, Head of Financial Stability
19 January 2021