VISION

Cybersecurity in the financial sector

FSOR

FINANCIAL SECTOR FORUM
FOR OPERATIONAL RESILIENCE

Vision

The Danish financial sector must be able to counter the changing threat from cy-bercrime and thus continuously be able to:

- **provide a secure and efficient infrastructure**
- **maintain the Danes' trust in the digital solutions in the Danish financial sector.**

We will strengthen collaboration within the sector and ensure improved scope for action for individual sector participants

We will strengthen collaboration with relevant stakeholders both nationally and internationally

We will increase awareness and knowledge of cyber security

November 2022

Cybersecurity in the financial sector

Throughout the world, the IT systems of the financial sector and other critical sectors of society are being attacked by both criminals and state-sponsored hackers. Denmark is one of the most digitised societies in the world. Combined with the financial sector's handling of large values, this makes the financial sector in Denmark a target for cybercrime. The Centre for Cyber Security has assessed for a number of years that the Danish financial sector faces a very high risk of cybercrime.

Cyberattacks are a potential threat to financial stability

The financial sector depends on complex IT systems in order to function. At the same time, banks and mortgage credit institutions are linked across the sector via data centres as well as payment and settlement systems.

A stable financial system depends on a number of factor, including confidence in correct and confidential recording of transactions, timely settlement of payments and securities transactions and that the systems are secure and accessible. Repeated cyberattacks on companies and systems in the financial sector may weaken confidence in the financial system – even if the individual attack does not have immediate societal consequences. Individual, but large-scale, cyberattacks that compromise critical systems have the potential to paralyse the whole sector, or significant parts thereof, for a period of time. Cyberattacks in the financial system are thus a potential threat to financial stability.

The individual players in the financial sector have strong focus on IT security, including on making their systems resilient to cyber threats. However, the interconnectedness of the financial sector means that there is a need for joint and coordinated action against the rising cybercrime. Danmarks Nationalbank put the issue on the Systemic Risk Council's agenda in December 2015. There was broad agreement in follow-up discussions with the financial sector that it was expedient to establish a formalised sector collaboration. On this basis, the Financial Sector Forum for Operational Resilience (FSOR) was set up. FSOR held its first meeting in June 2016.

Financial Sector Forum for Operational Resilience

FSOR is a forum for collaboration between authorities and key financial sector participants and its objective is to increase operational resilience across the sector, including resilience to cyberattacks. The tasks of FSOR are[1] to:

- ensure a common overview of operational risks that may have a cross-sectoral impact and that could potentially pose a threat to financial stability in Denmark;

- decide on and ensure implementation of joint measures to ensure financial sector resilience to major operational incidents, including cyberattacks;

- create a framework for collaboration and knowledge sharing – within the sector, between different sectors and internationally.

FSOR regularly updates a risk analysis at sector level[2], which constitutes the fulcrum of FSOR's and Danmarks Nationalbank's initiatives aimed at increasing cyber resilience. Firstly, the risk analysis identifies risks that may threaten financial stability in Denmark and, secondly, it provides a structured basis for prioritising between measures that can reduce risks.

A number of sources are used in the risk analysis to identify the risks faced by the financial sector. This includes mapping key business processes and systemic dependencies, past incidents, threat assessments and input from FSOR members, including input from the annual survey of FSOR members' main concerns in relation to operational resilience. Key initiatives taken on the basis of the risk analysis include:

- A detailed crisis management plan at sector level to ensure coordinated action across the financial sector in the event of a systemic crisis. The plan supplements the members' own crisis management plans and the national crisis management authority, NOST. Crisis management plans at different levels are essential, as operational incidents will occur despite good preventive measures. By way of illustration, it can be mentioned that the crisis management plan at sector level during covid-19 disseminated knowledge about the situation across the financial sector based on the individual organisation's reports to the sector crisis management group. The crisis management plan is continuously tested, updated and improved based on the experience gathered.

- A TIBER test programme for key players in the financial sector, which Danmarks Nationalbank and the players have established jointly. TIBER stands for Threat Intelligence Based Ethical Red-teaming, and the Danish implementation guide for conducting the tests is based on an overall framework developed by the European Central Bank. During a test, test participants are to identify so-called ethical hacker attacks and stop/prevent these attacks from doing damage.

1 See Terms of Reference for FSOR for further details (*link*).
2 See 'Handbook of methodology for FSOR's risk analysis' (*link*).

Danmarks Nationalbank is the authority for TIBER-DK[3] and supports the performance of the tests.

- Regular examination of cyber resilience in the financial sector, including identification of general issues across the sector, linked with knowledge-sharing and individual feedback to the participants by Danmarks Nationalbank.

- Development of a joint baseline for cyber resilience that can be used on a voluntary basis by organisations in the financial sector. The baseline aims to provide tangible and measurable recommendations on cyber resilience in various areas such as data protection and governance.

- Joint focus on increasing the level of data protection for sector-critical data and the ability to ensure secure and efficient recovery following a cyberattack.

- Involvement of critical suppliers in the FSOR work aimed at bringing the suppliers closer to the players in the sector.

FSOR also has close collaboration with Risk Forum for Interdependencies (RGA)[4], which works to increase operational resilience between key infrastructure systems. Risks which are identified in RGA, but which cannot be mitigated in this forum, are passed on to FSOR.

FSOR's vision to counter the changeable threat from cybercrime shows the direction for FSOR's initiatives such as the above and the work initiated in the individual banks and mortgage credit institutions, data centres, payment and settlement systems. In this way, the work in the FSOR will contribute to ensuring that the financial sector at all times can:

- provide a secure and efficient infrastructure and

- maintain the Danes' trust in the digital solutions in the Danish financial sector.

It is essential that the customers of the financial sector have confidence in the sector and in the digital solutions used by the sector. This is a precondition for realising the growth and innovation potential offered by the digitalisation of society.

3 TIBER-DK was one of the first TIBER programmes in Europe. See Danmarks Nationalbank's website for further information about TIBER-DK (*link*).

4 See Danmarks Nationalbank's website for further information about RGA (*link*).

Action areas

In order to realise this vision, FSOR has implemented a number of initiatives in three main action areas:

Strengthened collaboration within the sector and improved scope for action for individual sector participants

FSOR should provide a framework for strengthened collaboration within the sector and improve the sector's scope for action in relation to cyber and IT security threats. Strengthened sectoral collaboration should con-tribute to improving the individual participants' ability to address cyber and IT security threats.

Stronger collaboration with relevant stakeholders, both nationally and internationally

FSOR should strengthen collaboration with relevant stakeholders, both nationally and internationally, with a view to sharing experience and best practice for countering cybercrime. This should improve the scope for specific action for FSOR members and stakeholders.

Increased awareness and knowledge of cyber security

FSOR should help to ensure that all financial sector participants have the knowledge, skills and capabilities needed to protect themselves against cyber and IT security threats. At the same time, FSOR's work should contribute to improving the efforts of individual participants' to increase their customers' awareness and competencies regarding cyber security.

FSOR participants

Banks and mortgage credit institutions

Payment and settlement systems

Insurance companies and pension funds

Data centres

Industry associations
Authorities

Other relevant organisations

Danmarks Nationalbank chairs and act as secretariat for FSOR.