DANMARKS NATIONALBANK

28 AUGUST 2020 — NO. 14

How can joint measures to manage cyber risks be prioritised?

- Some systemic risks can best be addressed jointly. The Danish financial sector has developed a methodology for prioritising the joint work on cyber risks.
- The sector works together to identify and address systemic risks on a structured basis. The methodology increases cyber security both for the individual institution and for society as a whole.
- The methodology may also be used in sectors other than the financial sector.

The financial sector in Denmark has a strong focus on countering the increasing risk of cyber attacks. Work is being undertaken to manage cyber risks both in the individual institutions as well as at sector and national level, see Box 1.

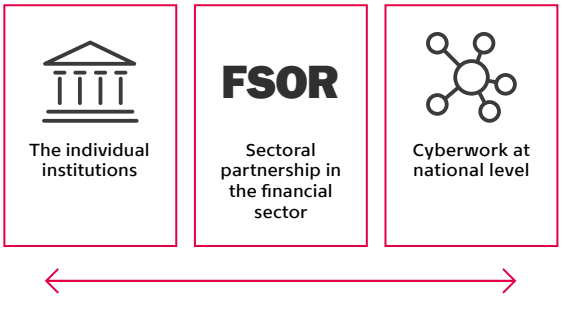
Each institution is responsible for ensuring a stable operation and operational resilience of its own systems. However, the technical and financial interconnectedness can cause cyber attacks to spread across

Key players in cyberwork Box 1

The individual institutions are working on cyber resilience and are using considerable and necessary ressources to manage cyber risks. In addition, the Danish Financial Supervisory Authority supervises financial institutions and data centres, while Danmarks Nationalbank monitors the payments infrastructure.

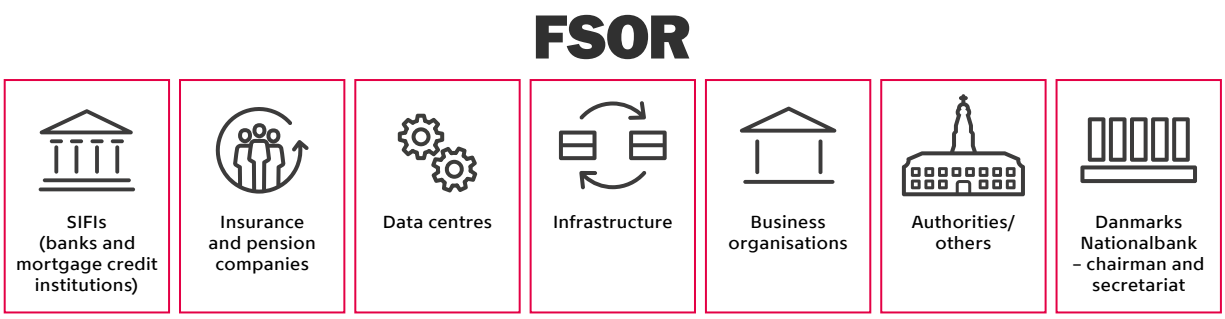
Financial Sector Forum for Operational Resilience, FSOR, is also a key player in cyberwork in the financial sector. See Box 2 for a description of FSOR.

At national level, the government in 2018 published a national cyber and information security strategy (*link*), which defined six sectors critical to society, here among the financial sector. The strategy includes cross-sectoral initiatives aimed at increasing cyber resilience, which are coordinated by the Danish Centre for Cyber Security, CFCS. In the event of a national crisis, activities are coordinated by the National Operational Staff, NOST.



FSOR brings together private and public players from the financial sector Box 2

The financial sector in Denmark has established a private-public partnership forum, the Financial Sector Forum for Operational Resilience, FSOR, to increase the sector's operational resilience to, among other things, cyber attacks. FSOR is a voluntary, yet binding, collaboration forum, and the members are the core participants of the financial sector. The FSOR members are: 1) the largest and systemically important financial institutions, SIFIs, insurance and pension companies, 2) data centres operating critical systems as well as storing and handling parts of the sector's data, 3) the companies that own the infrastructure – including financial transaction platforms, 4) financial business groups, and 5) central authorities. Danmarks Nationalbank chairs FSOR and acts as its secretariat.



institutions and systems. Therefore, it makes sense both for the individual institutions and for society to address several of the operational risks, including cyber risks, jointly.

But how can you identify key issues across institutions and prioritise what needs to be done jointly? The financial sector's work to design a joint risk analysis offers a possible take on this challenge!

Below follows a presentation of the structured risk analysis methodology prepared and applied by the Danish financial sector. The methodology is generic and may also be used in sectors other than the financial sector. The results of the analysis are sensitive and confidential and are therefore presented as general examples only. In the text below, focus is on the methodology itself.[1]

How to design a risk analysis at sector level – step by step

The financial sector in Denmark has established a private-public partnership forum (the Financial Sector Forum for Operational Resilience, FSOR) to increase the sector's resilience to, among other things, cyber attacks, see Box 2. A central feature of the partnership is the design of a risk analysis. The risk analysis contributes to identifying the operational risks that could potentially threaten the stability of the financial system, and provides a structured basis for prioritising measures aimed at reducing such risks.

The methodology applied to prepare a risk analysis at sector level comprises four main steps:

1. The scope of the analysis is defined
2. Risks are identified
3. Risks are assessed in terms of probability and consequence
4. Mitigating measures for the most important risks are identified.

1 For further details on the method, see *Handbook of methodology for FSOR's risk analysis*, August 2020 (*link*).

FSOR has set up a working group responsible for the practical preparation of the risk analysis, which comprises a wide range of participants from the financial sector. Based on the analysis, FSOR decides what measures to implement, when and how.

1. The scope of the analysis is defined
The first step of the risk analysis is to identify the so-called crown jewels of the sector. A full list of the sectors business activities is prepared. Based on this list, the most critical business activities are identified, i.e. activities where breakdowns, breaches of confidentiality or loss of integrity could potentially have systemic implications and threaten financial stability.

Among the crown jewels, FSOR's risk analysis initially focuses on business activities where breakdowns etc. quickly become critical, see Chart 1. Focus is currently limited to activities deemed to be critical within a time frame of up to one week. It is essential to have a deep understanding of these activities in advance as they must be handled urgently.

By identifying the most critical business activities, the focus is narrowed down to addressing the most important risks. Deciding on the priorities in this way also means accepting that not everything is equally important and that all functions of the financial sector cannot enjoy the same high level of protection. Often, however, a high level of protection for critical functions will also reduce the risk for a number of less critical functions.

2. Risks are identified
Risks occur when vulnerabilities can be exploited by threats. The purpose of collecting information about threats and vulnerabilities is to be able to make a broad identification of the risks that could potentially threaten critical business activities and thus financial stability.

The critical business activities falling within the scope of the analysis are mapped. An overview of systems, networks, suppliers and their interconnectedness is created. The mapping provides input on possible vulnerabilities, for instance as a result of interdependencies between and a concentration of suppliers of critical systems and networks.

In addition, information about threats and vulnerabilities is collected from a number of other sources, including information on:

Scope of risk analysis Chart 1

	≤ ½ day	≤ 1 day	2 days	> 1 week
Business activity 1	(X)	X		
Business activity 2			(X)	X
Business activity 3			X	
Business activity 4			X	
Business activity 5		(X)	X	
Business activity 6				X
Business activity 7				X
Business activity 8				X

Note: (X) = for particularly critical days. The red line separates business activities that become critical within less and more than one week, respectively.

- historical events
- threat assessments
- vulnerabilities identified by FSOR's cyber stocktake, which is a questionnaire-based survey of the cyber resilience of FSOR's members
- knowledge of future system changes etc.

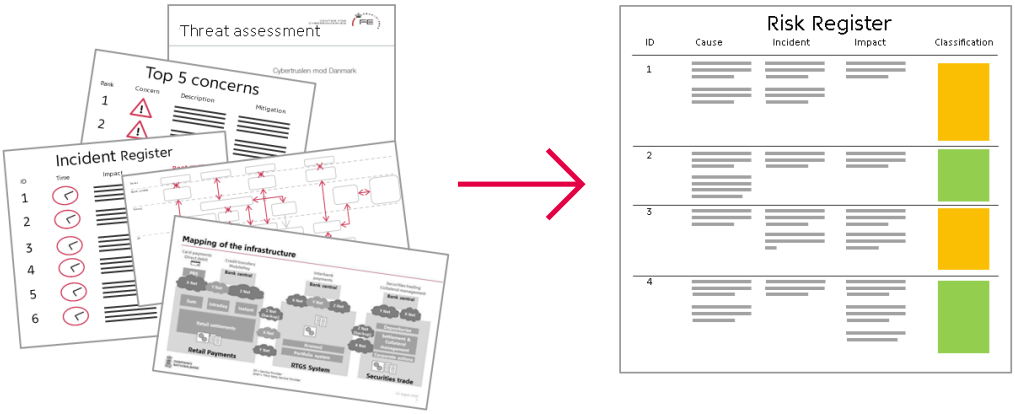
FSOR conducts regular surveys among its members to identify their top 5 concerns in relation to the stable operation of critical business activities. This provides input on the vulnerabilities and threats to operational resilience which are top of mind in the sector.

In addition, the working group members constitute a key source when it comes to identifying and reporting new vulnerabilities, threats and risks. In this way, it is ensured that the risks that are of most concern to the individual institutions are included in the risk analysis.

Based on the above-mentioned sources, a list of systemic risks is drawn up, and each risk is described in terms of cause, event and effect, see Chart 2. The risk descriptions form the basis for assessing the probability and consequence of the risk.

As of July 2020, FSOR has identified 36 operational risks with the potential to threaten financial stability. One general example of a risk is a cyber attack destroying critical data belonging to a key player in the financial sector. Another example is the siloing of risk management in key parts of the financial infrastruc-

Risks are identified Chart 2



Note: Systemic risks are collected from different sources and compiled into a list describing the cause, the incident and the effect of the risk.

ture to an extent that complicates the handling of events.

3. Risks are assessed in terms of probability and consequence

Each of the risks identified are assessed in terms of probability and consequence on the basis of a number of different criteria, see Chart 3.

The assessment of probability is usually based on how often an event is expected to occur, but other factors may also influence the scoring, for instance a lack of insight into the issue. The assessment of consequence is based on the extent to which financial stability is potentially threatened.

FSOR uses a scale of 1-5 to assess probability and consequence. Risks are plotted in the risk matrix, which is divided into four colours, see Chart 4. The colour distribution of the matrix is not symmetrical as events with high consequence but low probability (black swans) also have focus with respect to financial stability.

4. Mitigating measures for the most important risks are identified

For the most important risks, a working group proposes mitigating measures, which are then discussed by FSOR. The measures decided on must then be implemented. This work follows separate tracks, and progress is continuously monitored. Other risks are accepted – and thus not addressed.

One of the mitigating measures which has come about as a result of the risk analysis work is TIBER-DK[2], for which Danmarks Nationalbank is the author-

Criteria for assessing probability and consequence Chart 3

PROBABILITY

- Frequency
- Threat scenario after mitigating actions
- Knowledge-sharing and cooperation
- Sharing of information about threats
- Traceability
- Supplier complexity
- Maturity and control environment
- Lack of understanding of risk
- Business activity and IT architecture complexity

CONSEQUENCE

- Impact on critical business activities
- Public focus and impact
- Loss of confidence in the financial system
- Integrity of critical data and confidentiality

2 Threat Intelligence Based Ethical Red-teaming in Denmark, TIBER-DK.

ity. As part of the TIBER-DK programme, the major players of the financial sector perform threat-based red team tests, whereby the procedures, techniques and tactics of real hacker groups are mimicked by ethical hackers trying to access the systems critical to society (crown jewels). The aim is to strengthen cyber resilience and financial stability based on the learning derived from the tests.[3]

Other examples of mitigating measures include cooperation on protecting the sector's critical data, cooperation on stricter requirements for and closer dialogue with suppliers, closer risk cooperation between owners of the sector's key infrastructure and a cross-sector crisis response plan to be activated when systemic events occur.

Some mitigating measures cannot be implemented by the sector itself, but are better handled at national level. Consequently, FSOR proposes mitigating measures to, for example, the national cyber strategy and engages in dialogue with relevant authorities. One example is the need to ensure sufficiently precise time reference, which is relevant to several sectors.

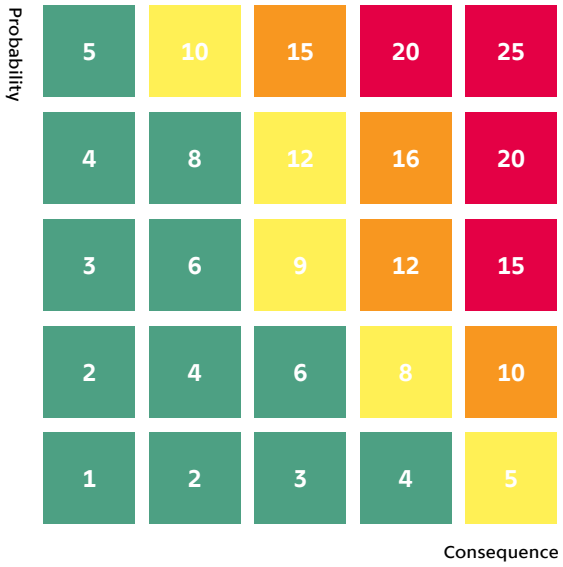
The risk analysis is updated according to an annual work cycle to ensure the continuous appraisal of the risks identified. The update also ensures consideration of any need to adjust the actual scope of the analysis.

Experience and additional reflections

Risk analysis at sector level is useful both for individual institutions, for the sector and for society as a whole, as it identifies key risks and ensures coordination, knowledge-sharing and an appropriate division of responsibilities when addressing risks. The risk analysis also ensures that the Danish financial sector works in a structured, in-depth and prioritised manner to maximise return on both the work done and the resources used.

In order for a cross-sectoral risk analysis to provide added value, it is important that

Risk matrix Chart 4



- the analysis is anchored in a credible institution with sufficient analytical capacity, knowledge and ability to complete the analysis;
- a secretariat facilitates a trusting, confidential and close collaboration between the parties, building a foundation for sharing insights and experience – both good and bad;
- the working group's competences are diverse to ensure that both the technical and business functions of the institutions are represented;
- the sector is represented at a level high enough to ensure the necessary decision-making power – also when it comes to resources.

The individual institutions are working on cyber resilience and are using considerable and necessary ressources to manage cyber risks. By comparison, the costs of cross-sectoral collaboration are limited – however, with a significant return. In most cases, it would not be possible for the individual business or institution to address the risks that are identified by FSOR. It therefore makes sense to work together as a sector to identify and address systemic risks.

3 See Danmarks Nationalbank, *TIBER-DK General Implementation Guide*, 18 April 2020 (*link*).

PUBLICATIONS

NEWS

News offers a quick and accessible insight into an Analysis, an Economic Memo, a Working Paper or a Report from Danmarks Nationalbank. News is published continuously.

ANALYSIS

Analysis from Danmarks Nationalbank focuses on economic and financial matter. Some of the analyses are published with a regular frequency e.g. *Outlook for the Danish economy and Financial stability*. Other analyses are published continuously.

REPORT

Report comprises recurring reports and reviews of the functioning of Danmarks Nationalbank. For instance Report includes the *Annual report* and the annual publication *Danish government borrowing and debt*.

ECONOMIC MEMO

Economic Memo is a cross between Analysis and Working Paper and it often shows the ongoing study of the authors. The publication series is primarily targeted at professionals. Economic Memo is published continuously.

WORKING PAPER

Working Paper presents research projects by economists in Danmarks Nationalbank and their associates. The series is primarily targeted at professionals and people with an interest for academia. Working Paper is published continuously.

The analysis consists of a Danish and an English version. In case of doubt regarding the correctness of the translation the Danish version is considered to be binding.

DANMARKS NATIONALBANK
HAVNEGADE 5
DK-1093 COPENHAGEN K
WWW.NATIONALBANKEN.DK

This edition closed for contributions on 24 August 2020

Mette K. Petry
Senior Advisor,
FSOR Secretariat
mpk@nationalbanken.dk

Lone Natorp
Head of Oversight
ln@nationalbanken.dk

Katrine Skjærbæk Rasmussen
Infrastructure Advisor
ks@nationalbanken.dk
FINANCIAL STABILITY

DANMARKS NATIONALBANK

CONTACT

Mette K. Petry
Senior Advisor,
FSOR Secretariat

mpk@nationalbanken.dk
+45 3363 6170

FINANCIAL STABILITY