FOLKETINGET
STATSREVISORERNE

FOLKETINGET
RIGSREVISIONEN

May 2024
– 14/2023

Extract from Rigsrevisionen's report
submitted to the Public Accounts Committee

The Danish FSA's IT-supervision

1. Introduction and conclusion

1.1. Purpose and conclusion

1. In Denmark, almost all financial transactions, from salary payments, loans and general shopping to trading in securities, are conducted digitally. IT breaches and hacker attacks in the financial sector can therefore have far-reaching practical and financial consequences for citizens as well as companies. By virtue of their size or the nature of their services, certain financial companies are so important for the financial sector and the national economy that IT security breaches can threaten the overall financial stability. These companies are referred to as *systemically important financial institutions*.

The risk of IT security breaches is high. Since 2018, the Danish Financial Supervisory Authority (the FSA) has assessed that IT security is one of the most significant risks facing the financial sector, and in its strategy for the cyber and information security of the financial sector, the Danish Cyber Security Centre assesses that the level of threat against the Danish financial sector is very high. Furthermore, a survey from 2023, commissioned by the FSA and carried out in the financial sector, shows that the risk of IT security breaches is a major concern to the financial institutions and a concern they find it very difficult to address.

2. The Danish Ministry of Industry, Business and Financial Affairs is responsible for the regulations that govern the financial sector. The legislation gives the FSA relatively much leeway to organise IT supervision. Firstly, the FSA has the authority to establish IT security rules that the financial institutions must adhere to and which will be supervised by the FSA. Secondly, it is up to the FSA to determine the level of supervision within the legal framework that prescribes that the supervision should be based on materiality and risk. Lastly, the FSA is independent of the Ministry of Industry, Business and Financial Affairs in conducting the supervision. According to the ministry, this means that the ministry has no powers of direction over the FSA, neither in relation to the specific processing of supervisory cases nor in relation to the overall organisation of the supervisory activities pertaining to IT security.

IT security requirements in the financial sector
Within the framework of the guidelines of the European Banking Authority, the FSA has set the requirements that apply to the IT security of the financial sector. The requirements define how the financial institutions must manage their business operations to mitigate incidents most effectively, reestablish operations as quickly as possible and minimize the impact of data breaches.

3. The purpose of the study is to assess whether the FSA has conducted its supervision of the IT security of the financial sector in a satisfactory manner. The report answers the following questions:

- Has the FSA organised the IT supervision in a satisfactory manner?
- Has the FSA conducted the IT supervision in a satisfactory manner?
- Has the FSA supported the effectiveness of the IT supervision?

4. Rigsrevisionen initiated the study in April 2023 upon a request from the Danish Public Accounts Committee.

Conclusion

The FSA's supervision of the IT security of financial institutions is not satisfactory. This entails a risk that the institutions' IT security is inadequate to prevent IT security breaches that could harm their clients and society.

The FSA's organisation of the IT supervision is not entirely satisfactory

Since 2019, the FSA has assessed the IT risks facing systemically important companies, however, the selection of institutions for inspection has only to some extent been based on the risk assessments. Furthermore, the FSA has generally not assessed the IT security risk of investment management companies as well as e-money and payment institutions and data centers that are not systemically important, which make up approx. 50% of the financial institutions that are not systematically important.

The FSA has not conducted the IT supervision in a satisfactory manner

In accordance with the objectives of the legislation, the FSA has inspected systemically important companies more frequently than the other companies. However, the FSA has not inspected the IT-security of one third of the systemically important companies within the four-year interval, as it is required to according to the guidelines. On average, four years and six months have passed between inspections, and some companies have not been inspected for seven years or more. This means that vulnerabilities in the IT security of the systemically important companies, including the shared data centers that are responsible for running the IT services of almost all banks, may remain undetected by the FSA for several years.

Since 2021, the FSA has narrowed the scope of its inspections in order to allocate more time towards conducting more frequent inspections of the systemically important companies. As a consequence of this shift in focus, certain areas of IT security, such as *access management and physical security* have not been subjected to inspection by the FSA for several years despite being deemed high-risk areas in several financial institutions by the FSA.

Because the FSA has estimated the risk associated with this type of companies to be low, the FSA has only to a limited extent inspected systemically important financial institutions and e-money and payment institutions. However, the FSA has not made any risk assessments of the IT security risk of the companies and therefore has no basis for knowing whether abandoning the inspections of IT security is appropriate.

The FSA is not adequately supporting the effectiveness of the IT supervision

Following their inspections, the FSA has instructed the majority of the systemically important companies to reduce their IT security vulnerabilities. The FSA has also set deadlines for the companies' compliance with the injunctions and has systematically followed up on the companies' compliance with the instructions. However, the companies have exceeded the deadlines set for compliance by two years, on average. Rigsrevisionen has noted that the FSA has never used its authority to impose sanctions on companies failing to comply with the instructions.

IT supervision
The FSA's IT supervision includes several activities. A significant portion of the supervision entails inspections within companies, however, it also encompasses meetings, risk assessments, monitoring, and follow-up on injunctions, among other things.

The term inspection refers to physical visits to the companies, whereas the term supervision refers to the comprehensive supervision or other activities beyond the inspections.

Shared data center
A facility that runs and develops IT solutions for banks and mortgage credit institutions.