

30 January 2026

FSOR 2025

FSOR
FINANCIAL SECTOR FORUM
FOR OPERATIONAL RESILIENCE

The Financial Sector forum for Operational Resilience, FSOR, is a public-private collaborative forum that aims to increase operational resilience in the financial sector in Denmark. FSOR is chaired by Danmarks Nationalbank, and comprises the key actors in the Danish financial sector. In 2025, the ordinary meetings of FSOR were held in May and November.

Risk analysis guides FSOR's work

The FSOR members and Danmarks Nationalbank identify and address operational risks that could impact the sector and potentially threaten financial stability. FSOR's risk analysis addresses a number of cyber and supply chain risks. In 2025 FSOR also assessed risks associated with hybrid threats, quantum-safe encryption, and stable supply of electricity, telecoms and IT infrastructure. By the end of 2025, the analysis had identified 29 risks, including several related to cyberattacks, data protection and business continuity in the event of operational incidents.

FSOR's risk analysis is updated every six months. Based on the results, FSOR assesses the need for additional measures to reduce the risks identified. The measures focus on different elements such as sector crisis management plan, stress testing of the sector's operational resilience, cyberresilience survey among key actors, threat-based testing and the ability to continue critical activities in extreme but plausible scenarios.

Crisis management plan ensures cross-sectoral coordination in the event of a crisis situation

FSOR has established a crisis management plan at sector level. Danmarks Nationalbank act as chair and secretariat. Crisis management planning ensures coordination between organisations in a crisis where vital parts of the sector are affected by an operational incident. FSOR's crisis management plan complements the local crisis response plans of its members and also coordinates with the national operational staff, NOST. The crisis management plan is continuously developed and updated, and members are responsible for ensuring consistency with their own response plans.

In September 2025, an announced and comprehensive test of the plan was conducted as part of the Danish Financial Supervisory Authority's and Danmarks Nationalbank's stress test of operational resilience. In addition, an unannounced test was carried out in March to test the ability of crisis response members to assemble at short notice, and a smaller test was carried out in November to assemble the team via an alternative communication channel. Test reports have been prepared for the exercises, identifying possible points for improvement.

FSOR's crisis management plan was briefly escalated to Level 2, 'Monitoring' twice during the year. The first time was in connection with the migration of Danish Kroner to TARGET Services in April to ensure that crisis management could be activated quickly in the event of a disruption. Migration went according to plan and there was no need for further activation of the crisis response team. The second time was during the drone flights over Denmark in September-October. In this instance, the escalation level was raised as a result of the activation of the National Operative Staff, NOST. During the incidents, no further activation of the FSOR crisis management plan was required.

Survey of resilience against cyberattacks and other operational incidents in the financial sector

In 2025, Danmarks Nationalbank worked on a questionnaire survey of operational resilience based on responses from the private actors in FSOR. Similar surveys have been conducted in 2016, 2018, 2020 and 2022. Participants in the survey self-report their level and there is no verification of the responses given.

The purpose of the survey is to provide a picture of the current level of resilience among key actors in the Danish financial sector. The results were discussed in FSOR and respondents have received individual reports.

Danmarks Nationalbank has published the overall results, which indicate that the resilience of key financial actors is generally high.¹ The analysis also shows that there are variations across financial companies and room for improvement in several areas. The complex risk outlook also increases the demands on resilience and emphasises the need for continuous work to maintain high resilience.

Recommendations for crisis response for critical activities

Danmarks Nationalbank published a number of recommendations in December 2025 for financial companies aimed at enhancing emergency preparedness by adding an extra safety net.² The process was initiated in 2023 with the support of FSOR, which has been continuously involved in and contributed with expert knowledge. The process was fronted by a task force which, in addition to representatives from Danmarks Nationalbank, consisted of employees from Finance Denmark and Financial Stability. The focus was on ensuring

1 See Danmarks Nationalbank, The threat landscape requires continuous efforts to strengthen cyber resilience, *Danmarks Nationalbank Analysis*, no. 26, November 2025 ([link](#)).

2 See Danmarks Nationalbank, Emergency preparedness for critical financial sector activities in extreme scenarios, *Danmarks Nationalbank Analysis*, no. 29, December 2025 ([link](#)).

that citizens and businesses can continue to make payments and transfer funds even if central systems or data become unavailable.

Based on the task force's analysis, Danmarks Nationalbank continued working on recommendations for key financial companies to maintain critical activities. The recommendations target both banks and payment solution and infrastructure owners. Among other things, Danmarks Nationalbank recommends an emergency banking solution with centralised data collection in a 'data vault' and decentralised emergency platforms at banks so that the public can use payment cards, receive salaries and transfer money, and where businesses can receive customer payments and pay bills – bypassing the banks' normal systems.

Threat-based testing generates learning on countering advanced cyber threats

TIBER-DK was introduced in December 2018 with testing from January 2019. Danmarks Nationalbank was among the first central banks in Europe to establish a TIBER programme and conduct tests. Threat-based testing became part of the Digital Operational Resilience Act, DORA, from January 2025, which makes the TIBER testing methodology mandatory for significant financial companies across the EU. Danmarks Nationalbank has contributed to European and Danish legislation in this area and to the pan-European framework, TIBER-EU, in close collaboration with the European Central Bank, ECB. Danmarks Nationalbank is the designated authority for threat-based testing in Denmark.

The Danish TIBER-DK implementation is used in the individual tests, generating learning that strengthens the cyberresilience of the companies tested for the benefit of financial stability. Such learning is an important tool to mitigate the cyber risks identified in FSOR's risk analysis.

December 2025 saw the release of the annual threat landscape report produced by Nordic Financial CERT, NFCERT, with the involvement of relevant parties for the TIBER tests. NFCERT presented the report to FSOR members.

Operational resilience stress test

Danmarks Nationalbank and the The Danish Financial Supervisory Authority conducted a stress test of operational resilience at sector level in 2025. The purpose of the test was to examine how each company handles a large-scale and long-term operational incident in interaction with other financial organisations, FSOR's crisis response team and authorities.

The scenario was based on an incident involving a breach of data integrity in the central securities depository that affected trading and settlement of Danish securities with spillover effects on critical business processes across the sector. Due to the systemic effects of the scenario, FSOR's crisis management plan was activated as part of the test. Results from the stress test will be ready in 2026.

The conducted stress test has contributed to learning about the sector's resilience during complex operational incidents, which is utilised in the FSOR collaboration's continued work to increase resilience in the financial sector.

Peter Ejler Storgaard

Chair of FSOR

Deputy Director and Head of Financial Stability at Danmarks Nationalbank