Danish Financial Supervisory Authority

DANMARKS NATIONALBANK

Stress Test of Operational Resilience

Report

July 2026

Table of Contents

Stress Test of Operational Resilience

This report presents the results of a sector-level stress test of operational resilience, conducted by the Danish Financial Supervisory Authority and Danmarks Nationalbank in 2025, together with 11 key actors in the financial sector; Danske Bank, Jyske Bank, Nykredit-koncernen, Sparekassen Kronjylland, SEB, Nordea, JN Data, BEC, Bankdata, Netcompany Banking Services og VP Securities A/S[1].

The test focused on the securities area and aimed to examine how the sector as a whole can manage an extreme yet plausible ICT incident affecting critical societal functions. The report describes the test's methodology, scenario, and key learnings. Appendix 1 provides a more detailed description of the methodology behind the test, which can serve as inspiration for other sectors with complex dependencies and critical societal functions wishing to try this tool. Appendix 2 contains questions for reflection that other financial firms and sectors can be inspired by and use to further develop their contingency plans, without necessarily engaging in a large-scale test exercise.

Perspectives and Learning Opportunities

Firms that are part of Denmark's critical infrastructure must recognize that operational resilience is not only about their own systems and contingency plans. Most contingency plans are based on the assumption that the rest of the sector operates normally when a crisis occurs. But what happens when this assumption does not hold?

When the entire sector is affected, it becomes crucial to have joint, well-prepared, and tested plans for crisis management, recovery, and continuity of critical functions. The stress test of operational resilience has provided valuable insight into how individual firms and the sector can strengthen their ability to manage crises.

A stress test of this nature provides the opportunity to:

- Test and challenge existing contingency plans under realistic and complex scenarios
- Examine how cooperation, communication, and decision-making processes function when no single actor can resolve the crisis alone
- Create a shared understanding of roles, responsibilities, and decision paths, so all parties know who should do what - and when- during a crisis
- Identify strengths and weaknesses in information sharing and coordination, and where there is a need to implement measures to ensure that both internal and external parties receive clear and coordinated messages
- Identify where there is a need to further develop common standards and procedures for business continuity, recovery, and reopening, which strengthen the sector's ability to maintain critical business processes and ensure effective and reliable restoration of operations

[1] The participants in the test were divided into two categories. In addition to the shared findings summarised in this report, the seven Category 1 participants also received individual reports containing specific lessons learned.

In summary, the experiences from the stress test show that it is necessary to continuously challenge one's own assumptions and practices for cooperation. It is important to have robust contingency plans, but also to be aware that continuity, recovery and crisis management in some scenarios require joint, well-prepared, and tested plans across the sector.

Purpose of a Sector-Level Stress Test of Operational Resilience

Threats to the financial sector are evolving rapidly, and in recent years, cyber threats, ransomware, and AI have created a more complex and unpredictable risk landscape. AI can be used both to strengthen defenses and to carry out more advanced attacks, and automation enables threat actors to target multiple firms simultaneously and more efficiently. Overall, this means that it is increasingly important not only to be able to defend against attacks. The sector must also be able to maintain and restore critical business processes during and after an operational incident. In other words, firms and the sector must be prepared and practice the continuity of their critical functions during prolonged disruptions and the return to normal operations across various disruption scenarios.

The sector-level stress test of operational resilience is the first of this kind in the EU. It is a new approach, where a large part of the financial sector is tested over an extended period in a combination of real-time crisis exercises and tabletop exercises. The first cyber stress test in Denmark in 2023 focused on individual firms, while the latest test focused on how actors cooperate and manage a joint, prolonged ICT incident across the financial sector.

An individual firm can test its own preparedness, but due to the high degree of interconnectedness in the financial sector, it cannot uncover how its shortcomings or actions affect others, or how others' shortcomings or actions affect the individual firm. Therefore, both authorities and firms have a shared incentive and responsibility to test and strengthen the sector's resilience, so that critical functions can be maintained during serious incidents. Authorities and firms have a shared interest in investing resources for the testing of the sector's resilience: both want the sector as a whole to be able to maintain critical societal functions during serious operational incidents.

A sector-level stress test is a tool that makes cooperation operational: in the shared exercise space, real dependencies and points of failure become visible. The test is not about finding faults, but about creating shared learning and development.

Test Scenario

The scenario in the stress test was developed in close collaboration with the participating firms to challenge fundamental assumptions about availability and stability in the sector.

The securities area was chosen because this area - securities trading and the underlying infrastructures - forms a central foundation for the sector's business processes and functions. Here, a technical or data-related disruption can quickly have consequences for the entire sector - not only for the directly affected firms, but also for their customers, partners, and society as a whole. Under normal

circumstances, these dependencies are often invisible precisely because they function stably and efficiently.

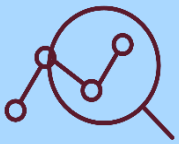
The scenario in the test involved an attack where trading data was gradually manipulated over weeks before being discovered. This meant that both response and recovery became more difficult, as the manipulation could also have affected backups. The scenario thus provided an opportunity to examine three central areas:

1. How are business continuity and recovery processes managed when even backups may be compromised by a prolonged attack?
2. How does cooperation function in restoring shared and critical data, especially when participants have different methods for maintaining their business processes during a crisis?
3. How do firms balance and integrate the sector's joint contingency with their own local contingency plans, when both must function simultaneously under pressure?

The scenario was designed to test cross-sector cooperation in practice and focus on the preparations and interaction necessary for the sector to manage a crisis collectively.

Test Methodology

The test was conducted as a combination of written tabletop exercises, live real time scenario management both online and in person, and structured questionnaires. The combination of methods allowed for both in-depth reflection and real-time collaboration. The methodology is detailed in Appendix 1.



The Difference Between Testing Fast and Testing Slow

There is a significant difference between a standard crisis exercise and a stress test of operational resilience, and the two types of tests have different advantages and limitations. A standard crisis exercise typically lasts about a day. It is a compressed exercise, where a game master usually controls the process, and participants must quickly respond to new clues and challenges. This provokes realistic stress and provides resource-efficient learning, but at the same time limits the opportunity to delve into decision-making processes, as the focus is on testing the organization's immediate reactions.

A stress test of operational resilience functions more as an exploratory exercise over a longer period. Participants have the opportunity to work thoroughly with cooperation, reflection, and decision-making. This strengthens the organization's ability to manage complex and prolonged crisis situations, because participants can try out different approaches in their own organization, test them in real-time crisis exercises together with other participants, and afterwards reflect on whether things could have been managed better or differently as a group, learning from the experiences along the way. At the same time, this type of test requires considerable resources spread over a longer period and can therefore be difficult to conduct frequently. The choice of test format will thus depend on, among other things, the purpose and resource consumption.

The participating firms helped develop and prioritize scenarios in a series of workshops, where both technical and business experts contributed experiences and solutions. During the test itself, cooperation was put to the test. Participants had to manage data corruption and coordinate communication and decisions across their organizations. In this way, both local and joint contingency plans were tested simultaneously. The sector's joint crisis management (FSOR Crisis Management Plan) was used actively. After the test, participants shared their experiences and learning points in evaluations and workshops.

The collective test and experience of where challenges arise in cooperation, and where individual firms are less robust, create strong motivation for all parties to address weaknesses and work together on solutions. The stress test thus strengthens both the shared understanding and the ability to act collectively.

Key Learnings from the Test

With this test, the financial sector has for the first time examined how local and joint contingencies function together during an extreme but plausible incident over an extended period. Some of the test's learning points are scenario-specific, while others are more general. It is important to emphasize that the understanding of a test's learnings must be seen in light of the fact that the test's design and organization affect results and learning points.

The most central learning points from the test, which form the basis for further work, are summarized below:

1. Learning Point: Effective Coordination Between Local and Joint Contingencies

In a major crisis, both the individual firms' local contingency and the sector's joint crisis management, FSOR Crisis Response Group, are activated. The test showed that, in practice, it is a complex and resource-intensive task for both firms and authorities to manage their own internal processes and crisis con-tingency while actively participating in the sector's coordinating contingency. Participants found that it requires significant capacity and overview to inves-tigate the incident, make decisions locally, and at the same time contribute to joint sector coordination - especially under time pressure and with limited information.

It can be challenging to make local and sector-based contingencies work effectively together. A learning point to be followed up on is that roles, responsibilities, and decision-making powers must be clearly prepared when both local and sector-based processes are running simultaneously.

2. Learning Point: Joint Crisis Communication

Effective internal and external communication is crucial for maintaining overview and trust during a crisis. The test prompted reflections on how variations in firms' choices of crisis management and communication - a natural result of different business models - can potentially lead to confusion among customers, the public, and employees. Media coverage and public debate can quickly amplify this effect, and trust or mistrust can spread across actors, including firms inside and outside the sector that are not directly affected. It is therefore worth considering in advance how different measures affect communication, and whether and when it is possible and appropriate to aim for coordinated messaging to customers and the public to avoid unnecessary escalation.

3. Learning Point: Cooperation on Continuity, Recovery, and Prioritization During Crises

When a major incident affects many actors simultaneously, continuity and recovery of critical functions become a complex and joint task. In a sector where many firms are connected through central infrastructures and depend on shared data, it is rarely possible for a single actor to restore normal operations or gain an overview. Recovery instead becomes a puzzle, where each participant has a part of the solution, and where cooperation and coordination are necessary to form a complete picture.

The solution therefore depends on firms pooling their knowledge and data to establish a common basis for reopening the market. This process requires technical insight, trust, and agreement on how information is validated and compared across organizations. The test provided insight into how these approaches and priorities materialize, and how the process is defined by each firm's business needs, technical solutions, and assessments of when their part of the infrastructure is ready. This may mean that recovery occurs in stages, and that there is a need for further dialogue and ongoing alignment on the next steps in the recovery phase.

4. Learning Point: Reopening Normal Business Processes - Balancing Security and Speed

Reopening and the transition to normal operations after a major incident present the sector with complex trade-offs. In cooperating to reopen critical business processes, the sector must balance the desire for rapid reopening to minimize negative consequences and the need to ensure that data and systems are reliable. The firms in the test were exposed differently in the scenario, and it was therefore not clear from the outset when and how operations should be resumed.

A prolonged shutdown of critical services can have far-reaching consequences - not only for the directly affected firms, but also for the national economy and trust in the sector. It is therefore crucial that firms make reopening decisions on an informed basis, considering both risks and societal concerns. A key learning point in the test was that when the sector has discussed and tested principles and processes for reopening in advance, it is better equipped to make quick and well-founded decisions that balance technical security with societal needs.

Forward-Looking Initiatives

The stress test of operational resilience has provided insight into how the sector reacts when multiple actors are simultaneously affected by a serious but plausible incident. The test has made it clear that resilience is about both technical solutions and individual contingency plans for business continuity and technical recovery, and to a large extent about the ability to cooperate, share information, ensure the continuity of critical functions collectively, and make difficult decisions under pressure.

Based on the test, three new initiatives have been launched:

- Development of a joint playbook with practical guidelines for a scenario involving a breakdown in the securities area
- Strengthening coordinated external crisis communication across the sector and authorities
- Strengthening collective contingency across relevant scenarios

These measures are intended to ensure that the sector is even better prepared if a major incident occurs.

The purpose of the initiatives is thus to supplement and support the operational resilience and contingency responsibility of individual system actors at the sector level - not to replace it.

The methodology and potential for learning extend beyond the financial sector and can inspire other sectors with complex dependencies between critical functions. By continuously challenging one's own assumptions and testing contingency in practice, also at the sector level, organizations can strengthen their ability to continue critical functions during disruptions and quickly recover after serious incidents.

Appendix 1: If You Wish to Work Further with Some of the Identified Themes in Your Own Organization

This section is written for those working in a firm in the financial sector or another critical sector, and who wish to know how to use the insights from the stress test in their own organization. The section contains concrete reflection questions that can be used to further develop your existing contingency plans and cooperation practices, both internally and in interaction with other actors in the sector.

The questions are based on experiences from the sector-level stress test of operational resilience in the financial sector and point to areas where it is particularly important to think beyond your own organization. They can be used as a starting point for dialogue in the board, crisis management team, between ICT and business, and in cooperation with suppliers.

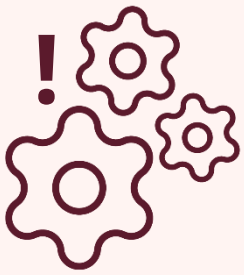
The section is intended as a practical tool to:

- Test and further develop your contingency plans
- Strengthen cooperation and communication across organizations
- Identify and manage mutual dependencies
- Prepare for complex crisis scenarios that affect the entire sector

1.

Assumptions in Your Contingency Plans

Your contingency plans are based on assumptions about the external environment: that suppliers are available, that counterparties can receive, and that the infrastructure is functioning. These assumptions are reasonable for creating concrete and action-oriented plans, but are you aware of the risks these assumptions entail, and in which scenarios they may be challenged?



1. Which of your contingency plans assume that other actors, such as suppliers, counterparties, and infrastructure, are operating normally? Are these assumptions documented?

2. Have you considered what to do if critical suppliers or partners are also affected, and whether your company is able to implement alternative solutions or procedures for cooperation under pressure?

3. Have you tested what happens if the assumptions in the identified plans do not hold?

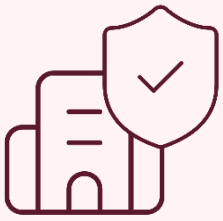
2. Communication and Coordination

When several actors are affected by the same incident, communication becomes a shared task. What one organization communicates affects all others, and it can be difficult to coordinate who says what and when.

1. Has your communication plan taken into account that other affected actors may communicate before you, and that you may then be forced to respond to their statements?
2. Does your communications department know whom to coordinate with if an incident affects the entire sector? Have you agreed on a process for this?
3. Are you familiar with the existing mechanisms for coordination in the sector, such as crisis management and authority channels, and are these integrated into your own communication plan?

3. Sector Cooperation and Activation of Contingency Plans

Your contingency plans are continuously tested and improved through internal exercises with realistic scenarios and tabletop exercises. However, it is a different task to participate in a larger sector contingency test in cooperation with other companies, each of which has its own way of building contingency plans and its own considerations.



1. Does your crisis management team know when and how the sector's joint contingency is activated, and what is expected of you, e.g., in terms of staffing?
2. Have you tested how your local contingency functions in the context of sector-wide incidents?
3. Have you considered how your sector as a whole manages an incident that affects shared infrastructure? And whether there is a plan for this that goes beyond the individual organization's contingency plan?

4.

Recognition and Planning of Mutual Dependencies

Most organizations primarily consider crisis management from their own perspective: What do we do when we are affected? However, in a sector-wide incident, you are potentially not the only ones impacted. Others depend on you, just as you depend on others. Your decisions affect the options available to others - and vice versa.

1. Have you assessed when an operational incident in your organization can affect other actors, and conversely, when an incident at others can affect you?

2. Have you considered how your own crisis measures – such as shutting down access, prioritizing certain customers, and limiting services – affect other actors' ability to continue and restore their business? And have you considered that similar crisis measures by other actors can affect you in the same way?

3. Do you have an agreement on prioritization if you depend on a supplier who also serves many others in the sector? And have you considered that the rest of the sector is likely to have the same needs?

Appendix 2: Methodology for Sector-Level Stress Test of Operational Resilience

Introduction

This appendix describes the methodology used to conduct the sector-level stress test of operational resilience in the Danish financial sector. The methodology is inspired by international experiences, including from the Bank of England and the ECB, and is adapted to Danish conditions. The approach can serve as inspiration in other sectors with complex dependencies and critical societal functions.

Core Principles

- **Cooperation:** The test is based on active involvement of all participants in design, execution, and evaluation.
- **Realistic Scenarios:** Scenarios are technically detailed and tailored to the sector's actual risks and dependencies.
- **Mix of Methods:** Combination of tabletop exercises, real-time crisis exercises, and structured questionnaires.
- **Learning:** Focus on identifying strengths, weaknesses, and development opportunities, not on finding faults.

Overall Process

1. Preparation and Design

- **Initial Meetings:** Initial dialogue with key actors to identify relevant risks and possible scenarios
- **Working Groups:** Establishment of technical and business working groups with participants from all relevant firms
- **Scenario Development:** Collaboration to prioritize and refine scenarios based on the sector's risk profile
- **Data Sets:** Development of data sets to simulate technical incidents (e.g., data corruption)

2. Test Structure and Phases

The stress test itself was conducted in three phases:

Phase 1: Preparation and Scenario Building

- Tabletop exercises: Individual preparation and scenario building
- Distribution of test materials and internal consultation in participating organizations

Phase 2: Crisis Management and Cooperation

- Live elements: Focus on critical moments where cross-sector cooperation is necessary
- Crisis management at sector level: The sector's joint crisis management (FSOR Crisis Response Group) is used for communication, reporting, and test injections

- Ongoing contact: Participants must coordinate between live sessions and local crisis management setups

Phase 3: Recovery and Reopening

- Tabletop exercises: Reflection and documentation of the recovery process
- Live recovery workshop: Coordination of recovery and reopening of critical functions
- Evaluation: Workshop on experiences and learning points

3. Method Elements

A. Tabletop Elements

- Semi-structured questionnaires to document decisions, processes, and consequences
- Data set exercises as preparation for live elements
- Individual and collective reflections

B. Live Elements

- Real-time scenario management (online and in person)
- Focus on cooperation, communication, coordination, and decision-making under pressure
- Testing both local and joint contingency plans

C. Interactive Scenario Adjustment

- Ongoing adaptation of the scenario based on participants' input and reactions
- Updating the timeline and progression to ensure relevance and realism

4. Resource Allocation

- Involvement of business, ICT, legal, and communication functions for a comprehensive perspective
- Dedicated resources for both internal and sector-based crisis management activities
- Special focus on data analysis, business continuity, recovery, and assessment of consequences

5. Impact Assessment and Second-Order Effects

- Description and, where possible, quantification of consequences from the start of the incident to the restoration of normal operations
- Assessment of both direct and indirect (second-order) effects, e.g., on customers, counterparties, and the sector as a whole
- Structuring of questionnaires focusing on assumptions, uncertainties, and professional judgment

6. Evaluation and Learning

- Individual reports with learning points for participating firms
- Joint evaluation and workshops to share experiences and identify sector initiatives
- Follow-up on sector learning in relevant forums

Procedure: How a Sector-Level Stress Test Can Be Conducted

1. **Identify Relevant Actors and Risks**
    a. Initiate dialogue with key actors

   b. Map critical dependencies and possible scenarios
2. **Establish Cooperation Structure**
   a. Set up technical and business working groups
   b. Plan design workshops and consultations
3. **Develop and Adapt Scenarios**
   a. Prioritize and refine scenarios in collaboration with participants
   b. Prepare technical data sets for simulation
4. **Plan Test Phases**
   a. Prepare tabletop exercises and live elements
   b. Allocate resources and roles internally and at sector level
5. **Conduct the Test**
   a. Start with tabletop exercises and individual preparation
   b. Hold live elements focusing on cooperation and decision-making
   c. Adjust the scenario continuously based on participants' input
6. **Document and Assess Consequences**
   a. Use questionnaires to collect data on decisions, processes, and effects
   b. Assess both direct and indirect consequences, e.g., the ability to continue the most critical functions
7. **Conduct Recovery Workshop and Evaluation**
   a. Coordinate recovery and reopening of critical functions
   b. Share experiences and learning points in joint workshops
8. **Follow Up on Learning and Initiatives**
   a. Prepare individual and sector-based reports
   b. Identify and launch relevant initiatives to strengthen resilience