DANMARKS NATIONALBANK

ANALYSIS | Emergency preparedness
1 December 2025 | No. 29

Emergency preparedness for critical financial sector activities in extreme scenarios

Written by

Frederik Kaae Jorst
Principal Expert, Recovery Taskforce
frjo@nationalbanken.dk
+45 3363 6412

Gustav Kaas-Jacobsen
Recovery Taskforce Lead
joj@nationalbanken.dk
+45 3363 6240

Kristine Rasmussen
Advisor, Recovery Taskforce
krr@nationalbanken.dk
+45 3363 6117

20 pages

The threat landscape is complex and the risk of severe operational disruptions due to cyberattacks or physical sabotage cannot be ruled out. With the support of FSOR – a sectoral collaboration between key companies and authorities in the financial sector – Danmarks Nationalbank has analysed the operational emergency preparedness of financial sector activities most critical to society. The focus is on ensuring that citizens and businesses can continue to make payments and transfer money, even if key systems or data are unavailable. The analysis has led to a number of recommendations from Danmarks Nationalbank to key financial companies, aimed at enhancing emergency preparedness by adding an extra safety net.

The complex threat landscape requires further strengthening of operational contingency measures

The financial sector plays a critical role in society and operational resilience is crucial. Although the maturity level in the financial sector is generally high, the complex threat landscape underscores the need for an extra safety net in the event of a severe incident. It should cover the activities that are most critical for citizens and businesses.

The financial sector is highly interconnected, making comprehensive overview, coordination and action essential

Financial companies are highly interconnected across activities. It has been important to create a coherent picture of dependencies to assess the need for additional emergency measures. Coordination across the sector is also crucial for ensuring that emergency solutions work in practice. Resilience is only increased when emergency solutions are implemented, tested and functional.

Emergency solutions should be established to handle severe, prolonged disruptions, including in banks

Danmarks Nationalbank has identified recommendations for key financial companies to ensure the continuation of activities critical to society, even in an extreme scenario where data or key systems are unavailable. This includes a bank emergency solution so that citizens can use payment cards, receive salaries and transfer money, and where businesses can receive customer payments and pay bills.

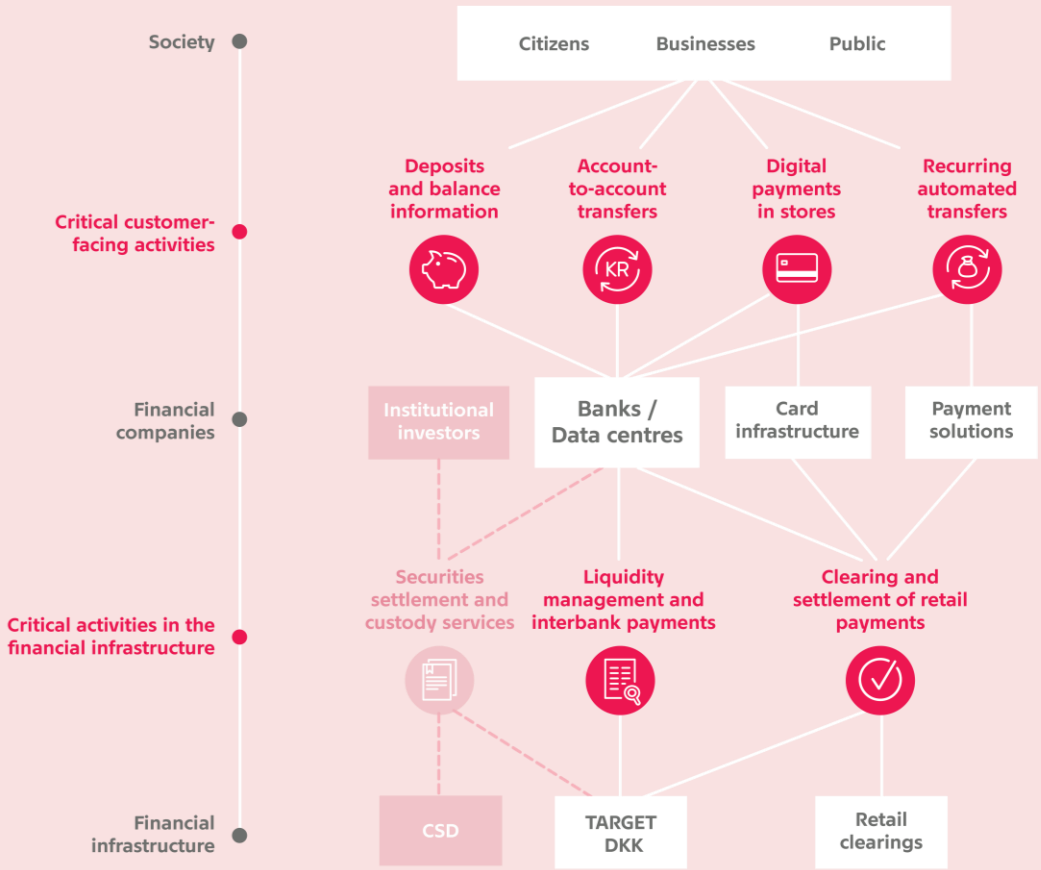
Why is this important?

Actors in the financial sector are responsible for operating the financial infrastructure that is critical to society. The financial infrastructure ensures, among other things, that financial transactions can be processed, that citizens can make payments in stores and that businesses can pay salaries.

The operation of critical financial infrastructure may be exposed to serious cyberattacks or other operational incidents that could cause disruptions and outages. In particularly critical situations, this may pose a threat to both the continued operation of individual financial companies and overall financial stability. It is therefore essential that the companies continuously work to handle both technical issues and attacks and that they have emergency solutions in place to handle severe, prolonged outages.

Main chart

Connection between key financial companies and activities critical to society





Keywords

Emergency preparedness | Cyber security | Financial sector | Payments | Financial stability | Digitalisation | Financial Sector Forum for Operational Resilience (FSOR) | Financial regulation

01
Introduction and summary

Citizens, businesses and public authorities depend on a range of activities in the financial sector, such as access to deposits and balance information, salary payments and the use of payment cards in stores. A severe operational outage that disables these services could have negative consequences for financial stability and the economy. If a key financial company, e.g. a bank, card company, payment service provider or financial market infrastructure, suffers a prolonged outage, it could affect other companies in the financial sector due to the interconnections of systems and processes. The consequences of an outage therefore cannot be managed in isolation. This analysis provides an overview of the consequences of a prolonged outage at a key financial company and identifies the need for further initiatives.

Geopolitical situation has made the threat landscape more complex

The threat landscape for Denmark has become more complex. The Danish Defence Intelligence Service, DDIS, assesses that Russia is waging a hybrid war against NATO and the West and that it is highly likely that the hybrid threat from Russia against NATO will increase in the coming years[1]. Examples include cyberattacks, drone activity, influence campaigns, GPS jamming and sabotage of critical infrastructure, such as the cutting of submarine cables. In addition, the Danish Resilience Agency, SAMSIK[2], assesses that the cyber threat against the financial sector. The threat from cybercrime remains very high. As a result of increased risk appetite from Russia, the threat level for destructive cyberattacks has been raised to moderate. This means there is capacity for harmful activity and intent to do harm, but no indications of specific planning.

The financial sector is constantly affected by operational incidents, which are typically handled without customers noticing. The sector has a resilient setup with dual-site operations, mirrored systems and redundant networks. Since 2016, Danmarks Nationalbank has launched several initiatives to strengthen operational resilience. These include, among others, the establishment of the Financial Sector Forum for Operational Resilience (FSOR) in 2016, semi-annual risk analyses, and since 2018, ongoing threat-led red team testing of individual financial institutions, see box 1. In 2023, the Danish Financial Supervisory Authority conducted a cyber stress test focusing on retail payments to assess preparedness and crisis management in the event of a prolonged outage in key systems. Participants have since worked on lessons learned and recommendations from the stress test. The sector is also working with the Digital Operational Resilience Act, DORA[3], which from January 2025 imposes requirements regarding policies and procedures for backup, recovery and testing thereof. Danmarks Nationalbank's latest survey of the financial sector's resilience against cyberattacks[4] and other operational incidents shows high resilience among key companies in the sector, albeit with variations across companies and areas. Although the resilient operational setup mitigates

[1] See The Danish Defence Intelligence Service, *Vurdering af den hybride trussel mod Danmark* (assessment of the hybrid threat against Denmark, in Danish only), 3 October 2025 (*link*).
[2] The Danish Resilience Agency assesses that the threat of cybercrime against the financial sector is *very high*, the threat from cyberactivism is *high* and the threat from both cyber-espionage and destructive cyberattacks is *moderate*. For an explanation of the threat assessment, Cybertruslen mod finanssektoren (cyber threat to the financial sector, in Danish only), 1 November 2024 (*link*).
[3] See Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (*link*).
[4] See Danmarks Nationalbank, *The threat landscape requires continuous efforts to strengthen cyber resilience*, 25 November 2025 (*link*).

problems in a range of scenarios, in light of the complex threat landscape, it is relevant to strengthen emergency preparedness by adding an extra safety net.

The financial sector is highly interconnected, making comprehensive overview, coordination and action essential

Responsibility for operational resilience lies with the individual financial companies, but the interconnection and complexity of the financial sector make cross-sector collaboration necessary. As previously mentioned, the sector's joint work on operational risks primarily takes place in the public-private collaboration forum Financial Sector Forum for Operational Resilience, FSOR. In 2023, Danmarks Nationalbank, with the support of all members of FSOR and relevant authorities, decided to initiate an analysis of the continuity of critical business activities at sector level in the event of especially serious attacks or outages. The starting point for the work was to create a comprehensive picture of activities, companies, dependencies and existing contingency measures to assess the need for further initiatives if a key company suffers a prolonged outage or where critical data are compromised or destroyed. Developments in the threat landscape since 2023 further highlight the relevance of this work.

Danmarks Nationalbank's analysis focused on emergency solutions for critical customer-facing activities, so that citizens can continue to use their payment cards, receive salaries and transfer money, and businesses can receive customer payments and pay bills. This also requires that critical activities in the financial infrastructure function, so that retail payments can be settled and banks can manage their liquidity and make payments between each other. Due to the interconnection and complexity of the financial sector, another focus was on measures that can be supported by a common approach across the sector or shared infrastructure. Activities in focus for recommendations include:

- access to deposits and balance information
- account-to-account transfers
- digital payments in stores
- recurring automated transfers, such as bill payments and payments of salaries, pensions and public benefits
- liquidity management and interbank payments
  clearing and settlement of retail payments

Emergency solutions should be established to handle severe, prolonged disruptions, including in banks

Necessary features for emergency solutions in the financial sector activities most critical to society include, for example, that the solution should, to the greatest extent possible, be agnostic to the type of incident and independent of the affected company's normal systems. The emergency solution must also be able to continue the activities within an ambitious but realistic timeframe. For some activities, an emergency solution must function within a few hours, while for others that are less time-critical, it must function within a few days.

Danmarks Nationalbank has identified recommendations for a number of key companies in the financial sector to enhance emergency preparedness for activities critical to society. As banks play a key role in society, Danmarks Nationalbank recommends, among other things, an emergency solution that can serve as a safety net to continue access to critical customer data and essential payment activities, independently of the banks' normal systems. The emergency solution should comprise central data collection to ensure that data on Danes' deposits are always available and consistent, even if data at banks have been compromised. It should also include emergency platforms that make it possible for a bank to re-establish critical activities and enable customers to continue to view their accounts, use payment cards, receive salaries and transfer money, independently of the bank's normal systems. Danmarks Nationalbank

recommends that these emergency platforms are established by the banks in a decentralised manner. Comparable emergency platforms exist in a few other countries.

A bank emergency solution requires resources for development, establishment and operation for both authorities and banks. In the case of emergency platforms, Danmarks Nationalbank assesses that banks can, to some extent, build on ongoing initiatives already under development in some banks. Regarding central data collection, it would be natural – in order to ensure cost-effectiveness – to build on existing reporting to the authorities. Danmarks Nationalbank therefore assesses that the costs of establishing central data collection with a limited number of data points, including customers' accounts, balances and information on associated payment cards, will be manageable.

To establish a bank emergency solution, there is a need to develop a legal framework that regulates data collection and specifies clear minimum requirements for the decentralised emergency platforms that banks must meet.

In addition to a bank emergency solution, Danmarks Nationalbank is in dialogue with a number of key financial companies about the remaining targeted recommendations for the critical activities where there is a need to further enhance emergency preparedness. The work will continue into 2026. Increased operational resilience requires that emergency solutions are implemented, tested and functional. This will require coordination across companies and authorities.

BOX 1

Financial Sector Forum for Operational Resilience, FSOR, and organisation of the analysis project

Since 2016, the Danmarks Nationalbank and financial sector have worked together in FSOR and shared knowledge about operational risks, including cyber threats. One of the first initiatives in FSOR was the establishment of a joint risk analysis, which identifies the greatest operational risks that have the potential to threaten financial stability. The risk analysis is updated semi-annually and provides a structured basis for prioritising joint initiatives to reduce the identified risks. Another example of a joint initiative is the establishment of sector-level crisis management in 2017, which supplements members' own crisis plans and the National Operational Staff, NOST, and aims to ensure coordinated action and communication across the financial sector in the event of a systemic crisis. A third example is threat-based red team tests of companies in the financial sector under the TIBER-DK programme, launched by Danmarks Nationalbank in 2018. In a TIBER test, the participant must identify, prevent and respond to advanced cyberattacks from ethical hackers – a so-called red team – to gain insights on how to protect activities critical to society against cyberattacks and prevent the attacks from causing harm. Another initiative is Danmarks Nationalbank's recurring cyber survey, which, through self-assessment among FSOR members, contributes important learning and knowledge sharing about cyber resilience among the members. For more on FSOR's work and initiatives, see Danmarks Nationalbank's website (*link*).

Work on business continuity measures at sector level and organisation of this analysis

During the work on the risk analysis in 2019, Danmarks Nationalbank and FSOR identified a need to strengthen the capability for data protection and business continuity at both individual and sector level. A number of initiatives were subsequently implemented to address several of the most severe risks. In 2023, Danmarks Nationalbank, with the support of FSOR and relevant authorities, decided to initiate an analysis of continuity of critical business activities at sector level.

Continues …

... continued

The analysis of business continuity at sector level was anchored in a taskforce set up by Danmarks Nationalbank. In addition to representatives from Danmarks Nationalbank, the taskforce included members from e-nettet and Finansiel Stabilitet participating in the project from September 2023 to September 2025. A reference group for the project was also established, with representatives from the Ministry of Industry, Business and Financial Affairs, Euronext Securities, Finance Denmark, e-nettet, the Danish Financial Supervisory Authority, Finansiel Stabilitet and Danmarks Nationalbank.

The work was initiated with the support of FSOR's members, who were involved throughout. Expert knowledge from the FSOR members' and the reference group's organisations were crucial to carrying out the analysis. The analysis work involved all relevant companies and authorities, with more than 100 meetings held in this context.

The work included a review of work in other comparable countries and ongoing dialogue with the respective authorities.

02
Critical financial sector activities and key companies

In this section, the financial sector activities critical to society and key companies included in the scope of this analysis are identified.

Identification of the critical financial activities included in the scope of the analysis

The focus of the analysis was to identify the financial activities that are most important to continue from a customer perspective and are most critical on a societal level, i.e., for citizens, businesses and the public authorities. Due to the interconnection and complexity of the financial sector, another focus was on initiatives where cross-sector collaboration is advantageous.

In summary, identification was based on three main considerations:

- **Customer-facing activities or activities supporting these:** The focus is on financial business activities carried out for or by citizens, businesses and authorities. This includes both activities performed directly for or by customers, as well as activities necessary to support customer-facing activities end-to-end.
- **Critical business activities on a societal level:** The focus is on business activities that are, on a societal level, most critical to continue within a relatively short period of time in the event of an extreme operational scenario where a key financial company is cut off from data or systems for an extended period.
- **Activities that can be supported by a common approach or infrastructure:** The focus is on critical financial business activities where continuity can be supported by a common approach across different companies in the financial sector or by shared infrastructure. Common initiatives are relevant where several companies use the same infrastructure and where a uniform approach can create tangible advantages in terms of effective coordination and mutual dependency management.

Based on these main considerations, the financial activities critical to society that must be able to continue in the event of a prolonged operational outage are:

- access to deposits and balance information (including access to credit and liquidity facilities)
- account-to-account transfers
- digital payments in stores
- recurring automated transfers, such as bill payments and payments of salaries, pensions and public benefits
- liquidity management and interbank payments
- clearing and settlement of retail payments
- securities settlement and custody services

The scope is shown in chart 1 in the red area.

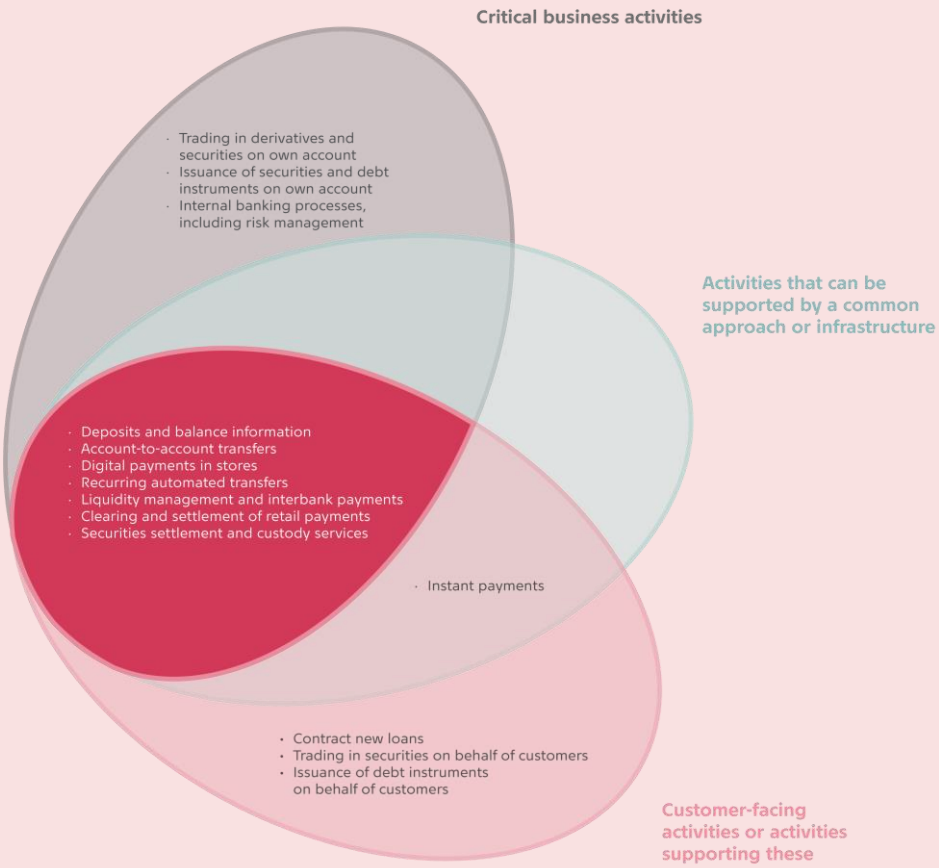
The purpose of the analysis is to add an extra safety net for the critical customer-facing activities and thus not to continue all critical activities for individual companies in the event of a prolonged operational outage. Consequently, there will be critical financial sector activities that are not included in the scope of the

analysis, as they do not meet the criterion of being able to be supported by a common approach or infrastructure. There are also customer-facing activities which, although they are aimed at citizens, businesses or authorities, are not considered among the most critical to continue in an extreme scenario and are therefore not included in scope of the analysis.

With regard to securities settlement and custody services, the Danish Financial Supervisory Authority and Danmarks Nationalbank conducted a sector-wide operational resilience stress test in 2025. The results of the stress test will be available in 2026, after which further work in this area will be initiated.

CHART 1

Financial business activities that are critical on a societal level in the event of a prolonged outage



Identification of key companies included in the scope of the analysis

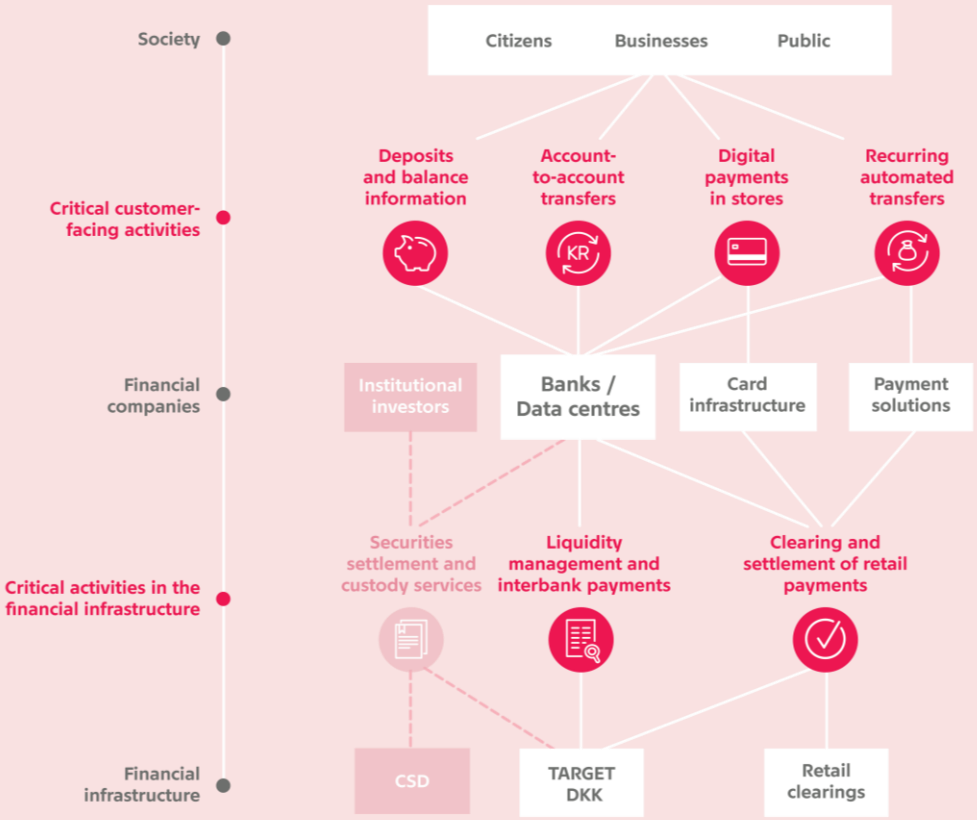
A number of companies in the financial sector are key to delivering the business activities outlined above. The key companies included in the scope of the analysis are:

- **Banks:** Provide deposits, payment services, etc.
- **Data centres:** Provide IT operations and IT services to banks.
- **Card infrastructure:** Enables digital payments with payment cards.
- **Payment solutions:** Systems for recurring transfers, such as bill payments and salary payments.
- **Financial infrastructure:** Responsible for clearing and settlement of transactions.
- **Financial networks:** Connect financial companies and enable data exchange and transactions.

The connection between the key actors in the financial sector and activities critical to society included in the scope of this analysis is shown in chart 2.

CHART 2

Connection between activities critical to society, key companies and infrastructure in the financial sector



03
Critical customer-facing financial sector activities

This chapter reviews the three customer-facing financial activities identified as critical to continue for citizens, companies and public authorities: 1) access to deposits, balance information and account-to-account transfers, 2) digital payments in stores and 3) recurring automated transfers.

Access to deposits, balance information and account-to-account transfers

Banks play a key role in supporting a range of critical activities for both citizens and companies. Among the most fundamental activities are the ability to access account information, make payments and for citizens to receive salaries, pensions, and social benefits. The financial sector is subject to extensive requirements regarding data protection and emergency preparedness and invests significant resources in protecting critical functions and data. The implementation of the Digital Operational Resilience Act, DORA, requires enhanced resilience against serious incidents.

In the event of a major system failure, data compromise or physical destruction, it is crucial that access to critical customer data and basic payment activities can be continued, independently from the banks' normal systems. It is therefore relevant to ensure alternative solutions that can function as a safety net, activated only if normal systems and backups cannot be restored within a short timeframe.

A few countries have already developed models to ensure access to balance information and payments in such situations, via so-called emergency platforms. In the United States, the Sheltered Harbor initiative was established in 2015 as a voluntary, decentralised solution where banks store their own data and can activate emergency platforms independent of their normal systems. In response to changes in the threat landscape, legislation was introduced in Finland in 2022 to establish centralised data collection and a shared emergency platform managed by authorities. Both approaches are built around three main elements: Secure storage of critical customer data, access to basic functions via an emergency platform and a clear contingency plan for activation and operation, see box 2.

A hybrid model, where critical customer data are continuously collected and validated centrally, while emergency platforms and contingency plans are established decentrally by individual banks, combines key elements from both approaches.

Central data collection ensures that the most critical customer data are available and consistent, even if the bank's own systems are unavailable. Ongoing validation boosts confidence that data can be used in practice. In addition, authorities can help maintain public confidence in a crisis by clearly communicating that critical data are secured. A data format based on common reporting standards also increases flexibility, as data can be transferred to another bank's emergency platform if its own platform fails.

Decentralised emergency platforms and contingency plans mean that responsibility for operations, activation and customer management remains with

the banks. This supports rapid response and integration with existing processes. An emergency platform must provide customers access to view their accounts, use their payment cards, receive salaries and pay bills. The solution can be adapted to the individual bank's technical and organisational circumstances and integrated with existing contingency procedures. Most banks, including the largest, are already working to expand and adapt their contingency solutions to continuously address risks arising from the heightened threat landscape. The banks' focus is on securing their most critical business activities and it is important that this also includes the activities considered most critical for society. Common minimum requirements for functionality and activation time must ensure that the activities that are the most critical to society can continue within an ambitious but realistic timeframe. It is also important that the banks' own contingency measures and emergency solutions can use data from the central data collection. As previously mentioned, this increases flexibility at sector level and enables the continuation of critical functions, even if a bank's own emergency platform fails.

In a Danish context, Danmarks Nationalbank recommends a hybrid model, with central data collection and decentralised emergency platforms and contingency plans. Such a model will require resources for development, establishment and operation for both authorities and banks. Danmarks Nationalbank assesses that, regarding the development of emergency platforms, banks can to some extent build on ongoing initiatives already under development in some banks. Regarding central data collection, it would be natural, to ensure cost-effectiveness, to build on existing reporting solutions, where banks already report customer data to the authorities. Danmarks Nationalbank therefore assesses that the costs of establishing central data collection with a limited number of data points, including customers' accounts, balances and information on associated payment cards, will be manageable.

A bank emergency solution will require close cooperation between authorities and the sector regarding governance, standards and ongoing testing to ensure that the solution works in practice. In this context, there will also be a need to develop a legal framework that regulates data collection and specifies clear minimum requirements for the decentralised emergency platforms and contingency plans that banks must meet.

BOX 2

Key elements of and international experiences with bank emergency solutions

Key elements of a bank emergency solution

- ***Data vault***: Ongoing collection and secure storage of critical customer data, physically and logically separated from the banks' primary systems. This ensures that necessary data can be restored if local backups are compromised.
- ***Emergency platform:*** A technical solution that can be activated quickly and independently of the affected bank's normal infrastructure. The emergency platform must provide access to basic functions such as account balance information and account-to-account transfers, based on data from the data vault.
- ***Contingency plan:*** Clear procedures for activation, operation and deactivation of the emergency solution, including objective criteria for activation and governance for interaction with the surrounding financial infrastructure.

International experiences
The United States and Finland have each established a decentralised and a centralised model based on the above elements, both of which are described in more detail below. In Norway, work is ongoing to investigate the possibilities of establishing an independent data repository and independent contingency solutions for card and account administration at banks. Conclusions from the Norwegian project are expected by the end of January 2026.[1]

United States – Sheltered Harbor
Sheltered Harbor is a private initiative run by the US financial sector.[2] It was established in 2015 in response to increasing cyber threats and the need for greater operational resilience. The model is based on a decentralised approach, where financial entities, including banks, continuously secure critical customer data in an encrypted and immutable data vault separated from normal systems, including backups. In the event of a severe outage, data can be restored and customers gain access to basic functions via emergency platforms, which are operated decentrally by the individual financial entities. The model is based on voluntary participation and common technical and organisational standards and has been developed to support the sector's own contingency needs and risk assessments. Certification with audit requirements and ongoing testing are part of the scheme to ensure that data and platforms comply with the standards.

Finland – National Emergency Account System
Authorities in Finland have established a central emergency system to ensure that citizens and companies can continue to access basic account functions and payments if severe disruptions occur. The system is anchored in legislation adopted in 2022, which regulates the National Emergency Account System, NEAS.[3] Responsibility for administering NEAS lies with the Finnish Financial Stability Authority, FFSA. Banks in Finland must regularly report necessary customer data to the authority. If a major disruption occurs, where one or more banks' normal systems are affected by outages, the authorities can activate NEAS. The emergency system gives customers access to transfer money to and from their accounts, pay with a debit card and withdraw cash. FFSA is responsible for data collection, validation, testing and operation of the emergency account system.

Possible implementation models

	United States	Finland	Hybrid
Data vault	*Decentralised at private financial companies*	*Centralised at an authority*	*Centralised at an authority*
Emergency platform and contingency plan	*Decentralised at private financial companies*	*Centralised at an authority*	*Decentralised at private financial companies*

[1] See Mandat for prosjekt om uavhengig bankberedskap, Justis- og beredskapsdepartementet, 6 June 2026 (*link*).
[2] See Sheltered Harbor - How it Works (*link*)
[3] See Lag om vissa arrangemang för tryggande av försörjningsberedskapen inom finansbranschen (666/2022), 8 July 2022 (*link*).

Digital payments in physical stores

Digital payments are crucial for citizens' ability to purchase goods and services. Approximately 90 per cent of all payments in physical stores in Denmark are made digitally, and most of these are made with payment cards and card-based wallets. Payments with Dankort, Visa/Dankort and international debit cards from Visa and Mastercard together make up around 97 per cent of these card payments.

Banks issue the payment cards and the money is withdrawn from the cardholder's bank account and deposited into the store's bank account after a payment is completed. The infrastructure behind card payments is complex. The card payment process occurs in several stages and involves, among others, the store's card acquirer, a card scheme owner and a data processor. Each stage is a prerequisite for card payments to be completed at the point of sale. The Danish market is characterised by high concentration, with a few companies handling several of the key stages. A prolonged outage at a key company could therefore result in significant disruptions to digital payments in physical stores.

There are currently several emergency solutions in place. These include offline payments with payment cards, which can be used in the event of outages at key companies in the card infrastructure or in case of unavailability of an internet connection. There is also STIP (stand-in processing), which enables continued payment with international debit cards within certain amount limits in the event of an outage at the card-issuing bank.

Danmarks Nationalbank recommends further strengthening the resilience for card payments by having key companies in the card infrastructure implement individual measures and by having banks adjust amount limits for STIP so that cardholders can maintain normal consumption during an outage.

Recurring automated transfers

Recurring automated transfers include a range of regular payments handled via key solutions in the financial sector. These transfers include bill payments, salary payments, payments of public benefits and pensions, where banks act as both sender and recipient on behalf of their customers. A high degree of automation and dependence on key solutions and/or companies means that critical payments or transfers could be significantly delayed if a key solution or company is affected by a severe and prolonged outage.

In particular, the payment of salaries, pensions, public benefits and time-critical bill payments, including, for example, mortgage payments from homeowners to mortgage credit institutions, are considered high priority. Other types of bill payments are considered less critical and, in the event of an outage, can be handled via alternative solutions, such as manual account-to-account transfers between debtor and creditor.

The solutions supporting these recurrent automated transfers are managed by both private financial companies and public authorities. There is awareness of the importance of these solutions and of contingency across the respective system owners and their suppliers. Danmarks Nationalbank recommends that all key companies and public authorities have emergency solutions in place that ensure the payment of salaries, benefits and pensions, as well as bill payments, can continue independently of normal automated processes within an ambitious but realistic timeframe. Danmarks Nationalbank will continue the dialogue with the relevant parties in 2026.

04
Critical activities in the financial infrastructure

This section reviews the two activities in the financial infrastructure identified as critical to support customer-facing activities end-to-end: 1) Liquidity management and interbank payments, 2) Clearing and settlement of retail payments.

Liquidity management and interbank payments

Interbank payments are payments and transfers between financial institutions, typically banks and mortgage credit institutions. These include both internal settlements and customer payments, which go through the banks' own systems and the central bank's infrastructure. On an average banking day in 2024, banks and mortgage credit institutions in Denmark conducted interbank payment transactions with a total value of approximately kr. 100 billion.

Banks depend on being able to manage their liquidity in order to continue critical customer-facing business activities during a prolonged outage and to ensure liquidity for interbank payments, CLS payments, retail clearing and securities settlement. Liquidity management includes planning and managing cash flows, access to market funding and access to eligible liquid assets. This is particularly critical towards the end of the monetary policy day or on days with large draw on liquidity, such as at the end of the month.

Liquidity management and interbank payments take place in Danmarks Nationalbank's system TARGET DKK, which includes the pan-European platform TARGET Services and Danmarks Nationalbank's own system for Collateral Management and Monetary Policy Instruments. Danmarks Nationalbank migrated its payment systems to TARGET Services in April 2025 and is now working with other European central banks to protect key systems against persistent cyber threats. TARGET Services is built on a resilient operational concept that allows operations to be moved to alternative sites in the event of severe and prolonged outages. In extreme scenarios where the key system is unavailable, an independent emergency solution has been established.

Danmarks Nationalbank is reviewing existing emergency solutions to ensure they address risks arising from the heightened threat landscape. Danmarks Nationalbank will continue this work in 2026.

Clearing and settlement of retail payments

Clearing and settlement of retail payments is a critical activity in the financial infrastructure, as it enables the correct calculation, exchange and accounting of payments between citizens, companies and public authorities. The systems include handling account-to-account payments, card transactions and bill payments between banks. An outage in a system for clearing and settlement of retail payments may mean that payments cannot be completed as planned.

The Danish clearing infrastructure is facing an expected change, where clearing of account-to-account transfers will migrate to a pan-European clearing platform. This means that resilience and contingency measures for clearing and settlement are assessed both in relation to the current and the future infrastructure. This also includes the parts of the infrastructure that are not migrating, such as the clearing of card and bill payments. The network infrastructure is a key

dependency for clearing and settlement, where redundancy and alternative communication channels are essential if normal networks are unavailable. Focus on network redundancy is part of the work on migrating to an international clearing platform, including assessing the need for increasing redundancy in the communication with international systems.

Danmarks Nationalbank recommends that the owners of the various clearing systems establish emergency solutions that ensure clearing and settlement of critical payments and transfers can take place independently of normal processes, systems and networks. Danmarks Nationalbank will follow up with the owners of the clearing systems in 2026 regarding the establishment of emergency solutions.

05
Prerequisites for enhancing emergency preparedness

The Danish financial sector generally has a high level of maturity and thus a good starting point for mitigating operational risks across a range of parameters. However, the geopolitical situation underscores the need to focus on emergency solutions to continue activities critical to society in scenarios involving severe, prolonged operational outages. This section outlines the key characteristics that are considered necessary for emergency solutions to continue the most critical activities.

The purpose of the analysis was to assess how financial business activities critical to society can be continued if one of the key financial companies is affected by a severe and prolonged outage. The analysis considered whether independent emergency solutions already exist and assessed whether these will be sufficient or enhancing them where relevant. The aim has been to assess where there may be a need to further strengthen emergency preparedness.[5]

In the analysis, the need for additional emergency solutions is assessed based on a set of characteristics considered necessary to strengthen contingency measures for the most critical activities in the financial sector.

A key characteristic is that emergency solutions must be able to be initiated and function independently of the affected company's normal operational setup and processes, regardless of which company is impacted. There is a residual risk that otherwise resilient contingency elements, including redundancy, backups, mirroring and dual-site operations, are not sufficient in an extreme scenario. It is therefore necessary to consider how an alternative setup can ensure the continuation of activities critical to society within an ambitious but realistic timeframe, even if key parts of the normal operational environment are compromised[6].

Another important characteristic is that the alternative emergency solution should, as far as possible, be agnostic to the type of incident, so that it can be activated regardless of whether the outage is due to a targeted attack or another severe systemic incident affecting critical systems, networks or data[7]. However, the analysis does not cover war-like incidents with broad, cross-sectoral impact.

[5] In the analysis, Danmarks Nationalbank also focused on the sector's dependence on telecommunications and engages in ongoing dialogue with relevant parties. Based on the dialogue with electricity and telecommunications authorities, it is assessed that a scenario in which the Danish financial infrastructure is completely cut off from neighbouring countries is not plausible in the current threat landscape. Such a scenario is relevant in other countries, including as part of the background for the emergency account system established by the Finnish authorities.

[6] International legislation and guidelines such as BIS/CPMI-IOSCO Guidance on Cyber Resilience for FMIs (*link*), the Digital Operational Resilience Act (*link*) and EBA Guidelines on ICT and security risk management (*link*) highlight that contingency plans should take into account extreme, plausible scenarios.

[7] The European Systemic Risk Board (ESRB) report *Advancing macroprudential tools for cyber resilience,* April 2024 (*link*) highlights the need for systemic backup solutions that can be activated regardless of the nature of the incident. The report points out that the cause of an incident cannot necessarily be identified and that solutions should therefore be resilient to different types of outages. The report focuses primarily on cyber threats, but it also notes that other types of failures may have similar consequences, supporting the need for flexible and technically independent contingency solutions.

Other characteristics include timeframe, flexibility and capacity, as outlined below:

Necessary features for emergency solutions

- *Agnostic to incident type:* The solution should, as far as possible, be able to handle different types of incidents, such as loss of functionality or unavailability of systems and data.
- *Independence from affected companies' normal operational systems:* The emergency solution must be sufficiently able to be initiated and function independently of the affected company's normal operational systems, processes, and networks, so that the solution can be activated even if key parts of the normal operational environment are compromised.
- *Timeframe:* The emergency solution must be able to be activated and put into use within a short period of time, so that critical financial sector activities can continue within an ambitious but realistic timeframe. Furthermore, the emergency solution must be able to remain operational until normal systems, processes or networks are restored and the transition from emergency to normal operation can be made.
- *Flexibility:* Sufficient flexibility must be built into the emergency solutions so that future adjustments to the surrounding system landscape are considered, such as upcoming changes in infrastructure, technology or the use of payment solutions.
- *Capacity:* Emergency solutions for activities that require processing of large volumes of transactions or large amounts of data must be automated and IT-supported to ensure that the solution is comprehensive and does not have unnecessary capacity constraints.

In addition to the above features for an emergency solution, it is also important to ensure *clear communication* both on the part of the individual key companies and across the sector. Furthermore, *clear coordination, roles and responsibilities* are crucial, so that all organisations and systems in the emergency solution know their role and responsibility and can act accordingly. There must be *clear procedures* for activation, operation, testing and maintenance of the emergency solution and there must be ongoing updates and learning based on experiences and tests of both the emergency solution and the ability to return to normal operations.

The work on the analysis has involved ongoing dialogue where key financial companies, relevant authorities and business associations have contributed with knowledge about systems, dependencies and emergency solutions. Based on this dialogue, the above features and existing emergency solutions, Danmarks Nationalbank has identified a number of recommendations for the key companies in the financial sector with a view to continuing activities critical to society in serious scenarios involving prolonged outages. Danmarks Nationalbank is in dialogue with the key companies on more targeted recommendations for activities where a need to enhance emergency preparedness has been identified. The work will continue into 2026. Increased operational resilience requires that emergency solutions are implemented, tested and functional. This will require coordination across financial companies and authorities.

Må vi sende dig *nyheder* fra Nationalbanken?

Få besked om vores nyeste udgivelser direkte i din indbakke.

Læs mere om vores nyhedsservice
og tilmeld dig på *nationalbanken.dk/da/nyhedsservice*,
eller *scan QR-koden*.

Du kan også få vores nyheder som RSS-feeds.
Læs mere på nationalbanken.dk/da/rss-feeds.

Publications



NEWS

News may be a news article or an appetiser offering quick insight into one of Danmarks Nationalbank's more extensive publications. The series is targeted at people who need an easy overview and like a clear angle.



STATISTICAL NEWS

Statistical news focuses on the latest figures and trends in Danmarks Nationalbank's statistics. Statistical news is targeted at people who want quick insight into current financial data.



REPORT

Reports consist of recurring reports on Danmarks Nationalbank's areas of work and activities. Here you will find Danmarks Nationalbank's annual report, among other documents. Reports are targeted at people who need a status and update on the past period.



ANALYSIS

Analyses focus on current issues of particular relevance to Danmarks Nationalbank's objectives. The analyses may also contain Danmarks Nationalbank's recommendations. They include our projections for the Danish economy and our assessment of financial stability. Analyses are targeted at people with a broad interest in economic and financial matters.



ECONOMIC MEMO

Economic Memos provide insight into the analysis work being performed by Danmarks Nationalbank's employees. For example, Economic Memos contain background analyses and method descriptions. Economic Memos are primarily targeted at people who already have a knowledge of economic and financial analyses.



WORKING PAPER

Working Papers present research work by both Danmarks Nationalbank's employees and our partners. Working Papers are primarily targeted at professionals and people with an interest in central banking research as well as economics and finance in a broader sense.

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
Langelinie Allé 47
2100 Copenhagen Ø
+45 3363 6363

This edition closed for contributions on 20 November 2025

DANMARKS NATIONALBANK