SUERF
The European Money and Finance Forum

SUERF Policy Brief
No 1605, October 2026

Operational resilience and financial stability: Exploring a stress test perspective

Neha Gupta | De Nederlandsche Bank
David-Jan Jansen | De Nederlandsche Bank, Vrije Universiteit, Tinbergen Institute

Keywords: Operational resilience, critical infrastructure, financial stability, stress tests

JEL codes: G20, G32

Abstract

Operational resilience is a growing financial stability concern amid geopolitical tensions and cyber threats. We discuss a stress testing approach in which operational shocks to critical infrastructure generate systemic risk through four channels: common exposures, interconnectedness, loss of trust and macroeconomic feedback loops. Applying this approach across scenarios can help policymakers anticipate transmission, strengthen safeguards and promote system wide resilience.

Disclaimer: The views expressed here are those of the authors and do not necessarily represent the views of De Nederlandsche Bank or the Eurosystem. We thank Remco van der Molen and Anne-Clarine Prosman for feedback on a draft version of this policy brief. Any errors remain our own.

Introduction

Operational resilience has moved steadily up the financial stability agenda. Geopolitical tensions have heightened concerns about cyberattacks and sabotage (IMF, 2024). Episodes such as the 2025 Iberian power blackout show how operational disruptions to non-financial critical infrastructure can also affect the financial system (Cremades et al., 2025). Emerging AI technologies may further accelerate the exploitation of operational vulnerabilities (ESRB, 2026; Crisanto et al., 2026). In short, both the likelihood of operational shocks and their potential to spread across financial institutions and markets are increasing.

Considering these rising challenges, policymakers need to understand how operational disruptions can threaten financial stability in a timely manner. A better level of understanding will then guide efforts to build resilience. All this requires tools that connect the initial operational shock to its propagation across the financial system (Bank of England, 2024; ESRB, 2026). Existing stress tests often assess whether individual institutions can withstand disruption. The macroprudential challenge is to identify when operational disruptions across institutions interact and become systemic. This brief describes such an approach linking disruptions in financial and non-financial critical infrastructure to systemic risk.

A stress test perspective

Our framework traces the transmission from an operational shock to systemic risk in five steps (Figure 1). Conventional financial stress tests typically begin with macro-financial shocks, such as higher interest rates or falling house prices. In the present context, the stress test begins with an operational shock. This shock may take different forms, including infrastructure sabotage, a cyber incident or an extreme weather event.

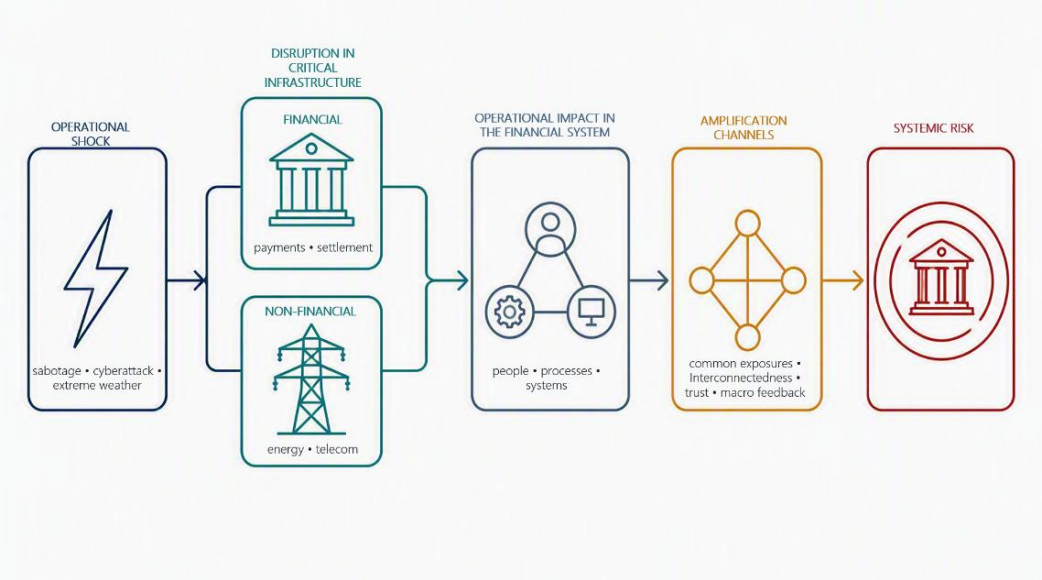
Second, the operational shock affects critical infrastructure. This may involve core financial infrastructure, such as payment or securities settlement systems, or non-financial infrastructure, such as energy, rail or communications networks.

Third, the shock directly affects financial institutions through familiar operational risk channels: people, processes and systems. Customer services may become unavailable, trading may be interrupted or employees may lose access to IT systems. These disruptions can severely affect individual financial institutions without becoming systemic.

The fourth step is where the initial operational disruption can potentially amplify within the financial system and start having systemic implications. We see four possible amplification channels:

- **Common exposures**: Financial institutions often depend on the same systems, software or service providers. An incident at a shared third-party provider — such as a cloud or data provider, or an open-source software component — can therefore disrupt multiple institutions at once.
- **Interconnectedness, particularly through liquidity channels**: Disruptions to payment and securities settlement systems can create liquidity strains for financial institutions. For example, Eisenbach et al. (2022) estimate that the failure of one large US bank could affect 31% of the wholesale payment system, while an outage at a shared third-party provider could increase this share to more than 60%.
- **Loss of trust**: Operational incidents can undermine trust in individual institutions and the wider financial system. Jamilov et al. (2026), for example, show that a cyber incident can lower the share prices of other firms in the same sector. A loss of trust can, in some cases, increase run risk.
- **Macroeconomic feedback loops**: Stress in the financial system can raise risk premia, constrain credit provision and slow economic growth. These second-round effects can, in turn, place additional pressure on the financial system.

Figure 1. From operational disruption to systemic stress



Quantifying operational resilience: A work in progress

In the end, policymakers need to assess whether the financial system can absorb the shock without systemic consequences. For this fifth and last step in our approach, quantification is essential. However, such quantification is not always straightforward, for instance due to data challenges.

To further our understanding, policymakers could consider developing system wide models, collect data on operational dependencies and embed operational scenarios in stress tests. The framework could, for example, assess vulnerabilities arising from shared ICT third-party dependencies using information available under the Digital Operational Resilience Act (DORA). It could also examine operational disruptions following extreme weather events, such as the transmission of flood risk to lenders' credit risk (Caloia et al., 2026). Applying the framework across these and other scenarios would help policymakers identify vulnerabilities and strengthen resilience early on.

References

Bank of England (2024), Operational resilience in a macroprudential framework.

Caloia, Francesco G., Kees C.H. van Ginkel and David-Jan Jansen (2026), Floods and financial stability: Scenario-based evidence from below sea level. *Journal of Financial Stability*, 84, 101545.

Cremades, Lourdes, Álvaro Esandi and Miguel Pérez (2025), The impact of the 28 April 2025 blackout on Spain's payment systems. *Financial Stability Review* - Banco de España, 49, Autumn.

Crisanto, Juan Carlos, Adrien Currat, and Jeffery Young (2026), When machines attack: frontier AI cyber threats and policy responses in the financial sector. FSI Occasional Paper No. 28.

Eisenbach, Thomas M., Anna Kovner and Michael Junho Lee (2022), Cyber risk and the U.S. financial system: a pre-mortem analysis. *Journal of Financial Intermediation*, 100971.

European Systemic Risk Board (ESRB) (2026), Addressing frontier AI models with cyber capabilities from a financial stability perspective.

International Monetary Fund (IMF) (2024), Cyber risk: a growing concern for macrofinancial stability. *IMF Global Financial Stability Report*, April.

Jamilov, Rustam, Helene Rey, and Ahmed Tahoun (2026), The anatomy of cyber risk. *Journal of Finance*, forthcoming.

About the author(s)

Neha Gupta is an economist at De Nederlandsche Bank. She worked on operational resilience and stress testing during her time at the Financial Stability division. She received an MSc in Econometrics and Operations Research from the Vrije Universiteit Amsterdam.

David-Jan Jansen is an economist working on central bank communication, stress testing and financial stability. He holds a PhD and an MSc in Economics from the University of Groningen and a BA in History from Utrecht University. He currently works at De Nederlandsche Bank and the Vrije Universiteit Amsterdam.

SUERF Policy Notes and Briefs disseminate SUERF Members' economic research, policy-oriented analyses, and views. They analyze relevant developments, address challenges and propose solutions to current monetary, financial and macroeconomic themes. The style is analytical yet non-technical, facilitating interaction and the exchange of ideas between researchers, policy makers and financial practitioners.

SUERF Policy Notes and Briefs are accessible to the public free of charge at https://www.suerf.org/publications/suerf-policy-notes-and-briefs/

The views expressed are those of the authors and not necessarily those of the institutions the authors are affiliated with.

© SUERF – The European Money and Finance Forum. Reproduction or translation for educational and non-commercial purposes is permitted provided that the source is acknowledged.

Editorial Board: Ernest Gnan, Jakob de Haan, David T. Llewellyn, Donato Masciandaro

Designed by the Information Management and Services Division of the Oesterreichische Nationalbank (OeNB)

SUERF Secretariat
c/o OeNB, Otto-Wagner-Platz 3A-1090 Vienna, Austria
Phone: +43 1 40 420 7206 E-mail: suerf@oenb.at Website: https://www.suerf.org/
ISSN 2791-5395 (Online)