



## TOPICS:

ITC risk

## SOURCE

European Central Bank

## ECB: Cyber Resilience Stress Testing from a Macroprudential Perspective

- This ECB document, published in the Macroprudential Bulletin (March 2025), examines **the growing systemic risk posed by cyber threats** to financial stability.
- **Contagion Mechanisms in Cyber Stress Testing - Operational Contagion:** Cyber incidents affecting financial market infrastructures, third-party providers, or payment systems can create widespread disruptions. Examples include the 2023 ransomware attack on ION, which halted financial trading services; **Financial Contagion:** Cyberattacks can erode liquidity, trigger counterparty credit risks, and disrupt market stability. The 2023 attack on the Industrial and Commercial Bank of China (ICBC) impacted the U.S. Treasury market, highlighting the interconnectedness of financial institutions; **Confidence Contagion:** Cyber-induced loss of trust in financial institutions can trigger "cyber runs," fire sales, and market volatility.
- **Approaches to Cyber Resilience Stress Testing - Bottom-Up Approach:** Individual institutions assess their resilience to cyberattacks, simulating response and recovery strategies.

The ECB's 2024 stress test on 109 banks followed this model, focusing on operational recovery rather than capital adequacy; **Top-Down Approach:** Supervisory authorities model systemic cyber risk, assessing second-round effects, financial interlinkages, and behavioral responses. This method helps quantify broader financial stability implications.

- **Principles for Effective Cyber Stress Testing** - Clearly define objectives and institutional scope; Incorporate all contagion channels and focus on tail risks; Consider behavioral responses, such as market panic and liquidity hoarding; Integrate bottom-up and top-down methodologies to provide a comprehensive view of systemic resilience.
- **Policy and Regulatory Implications** - The European Systemic Risk Board (ESRB) emphasizes the need to integrate cyber resilience into macroprudential frameworks. The Digital Operational Resilience Act (DORA), effective January 2025, mandates resilience testing for financial institutions and critical third-party service providers.

FOLLOW US!

