EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Press release

26 July 2024

ECB concludes cyber resilience stress test

- Stress test gauged how banks would respond to and recover from severe but plausible cybersecurity incident
- 109 banks tested, of which 28 underwent more extensive testing
- Results to feed into ECB's 2024 Supervisory Review and Evaluation Process

The European Central Bank (ECB) today concluded its cyber resilience stress test, which gauged how banks would respond to and recover from a severe but plausible cybersecurity incident. Overall, the stress test showed that banks have response and recovery frameworks in place, but areas for improvement remain. The results will feed into the 2024 Supervisory Review and Evaluation Process (SREP) and have helped increase banks' awareness of the strengths and weaknesses of their cyber resilience frameworks.

The exercise was launched in January 2024 and featured a fictitious stress test scenario under which all preventive measures failed and a cyberattack severely affected the databases of each bank's core systems. The stress test therefore focused on how banks would respond to and recover from a cyberattack, rather than on how they would prevent it.

Detecting and addressing deficiencies in supervised banks' operational resilience frameworks, including those stemming from cyber risks, is one of the ECB's SSM supervisory priorities for 2024-2026. This reflects the recent surge in cyber incidents that supervised banks have reported to ECB – an increase that partly stems from rising geopolitical tensions and challenges posed by the digitalisation of the banking sector.

The stress test involved 109 banks directly supervised by the ECB. All banks had to answer a questionnaire and submit documentation for the supervisors to analyse, while a sample of 28 banks was chosen to undergo more extensive testing. The latter were asked to perform an actual IT recovery test and provide evidence that it had been successful, in addition they were also visited on site by

European Central Bank
Directorate General Communications
Sonnemannstrasse 20, 60314 Frankfurt am Main, Germany
Tel.: +49 69 1344 7455, email: media@ecb.europa.eu, website: www.bankingsupervision.europa.eu

supervisors. The sample covered different business models and geographical locations to reflect the wider euro area banking system and ensure sufficient coordination with other supervisory activities.

To test their response to the scenario, banks had to show their ability to:

- activate their crisis response plans, including internal crisis management procedures and business continuity plans;
- communicate with all external stakeholders such as customers, service providers and law enforcement agents;
- run an analysis to identify what services would be affected and how;
- implement mitigation measures, including workarounds that would help the bank to operate during the time needed to fully recover IT systems.

To test their ability to recover from the scenario, banks had to show they could:

- activate their recovery plans, including restoring backed-up data and aligning with critical third-party service providers on how to respond to the incident;
- ensure that affected areas were recovered and up and running;
- implement lessons learnt, for example by reviewing their response and recovery plans.

The ECB is committed to continuing to work with the banks it supervises to strengthen their cyber resilience framework. To this end, it will further encourage banks to keep working on meeting supervisory expectations by, among other things, ensuring they have in place adequate business continuity, communication and recovery plans, which should consider a wide enough range of cyber risk scenarios. Banks should also be able to meet their own recovery objectives, properly assess dependencies on critical third-party ICT service providers, and adequately estimate direct and indirect losses from a cyberattack.

The outcome of the exercise will feed into the 2024 SREP, which assesses banks' individual risk profiles. The cyber resilience stress test is not focused on banks' capital, so its results will not affect banks' Pillar 2 Guidance. Supervisors have provided individual feedback to each bank and will follow up with them accordingly. In some cases, banks have already improved or plan to remedy the shortcomings pinpointed during the exercise.

For media queries, please contact Clara Martín Marqués, tel.: +49 69 1344 17919.

Notes

European Central Bank
Directorate General Communications
Sonnemannstrasse 20, 60314 Frankfurt am Main, Germany
Tel.: +49 69 1344 7455, email: media@ecb.europa.eu, website: www.bankingsupervision.europa.eu

- The ECB conducts supervisory stress tests on an annual basis in line with Article 100 of the Capital Requirements Directive, and every two years participates in an EU-wide stress test coordinated by the European Banking Authority. In those years where there is no EU-wide stress test, the ECB conducts a targeted stress test exercise which focuses on a specific topic of interest, such as the sensitivity analysis of interest rate risk in the banking book in 2017, the sensitivity analysis of liquidity risk in 2019, and the climate risk stress test in 2022.

- The ECB currently directly supervises 113 banks. The 109 banks that participated in the cyber resilience stress test were those under direct ECB supervision at the time the exercise was launched, with a few exclusions for bank-specific reasons such as restructuring or change of significance status.

European Central Bank
Directorate General Communications
Sonnemannstrasse 20, 60314 Frankfurt am Main, Germany
Tel.: +49 69 1344 7455, email: media@ecb.europa.eu, website: www.bankingsupervision.europa.eu