



Press release

14 February 2023

ESRB publishes report on advancing macroprudential tools for cyber resilience

The European Systemic Risk Board (ESRB) has today published a [report](#) aimed at advancing macroprudential tools for cyber resilience.

The report, which was prepared against a geopolitical backdrop of heightened cyber risk, highlights the need to boost cyber resilience. To this end, authorities across the EU are encouraged to make progress on three elements:

1. **Cyber Resilience Scenario Testing** is an analytical tool designed to assist authorities in (i) testing the response and recovery capacity of the financial system in severe but plausible scenarios involving a cyber incident, (ii) evaluating the impact of these scenarios on financial and operational stability, and (iii) identifying areas where further work is required to mitigate cyber risk. The ESRB encourages authorities to pilot system-wide cyber resilience scenario testing as soon as possible. Such pilots can complement other analytical tools that the authorities might be using and deepen their understanding of the risks to system-wide cyber resilience.
2. **Systemic Impact Tolerance Objectives** is a further analytical tool developed to identify and measure the impacts of cyber incidents on the financial system, and to evaluate when they are likely to breach tolerance levels and cause significant disruption. Defining such objectives can help authorities to assess their own coordination and action capabilities.
3. **Financial crisis management tools**, which the report considers in terms of how well they deal with system-wide cyber incidents. The report finds that the effectiveness of existing financial crisis management tools in responding to a cyber incident depends on the severity of the impact on the financial system and on how fast it spreads.

This report builds on previous work by the ESRB to prevent and mitigate risks to financial stability in the event of a cyber incident. This includes the 2022 ESRB [Recommendation](#) for the establishment of a pan-European systemic cyber incident coordination framework and the

accompanying report, entitled “[Mitigating systemic cyber risk](#)”, which describes how this framework would facilitate an effective response to a major cyber incident. The ESRB’s work focuses on the financial system as a whole. It complements the work of the Joint Committee of the European Supervisory Authorities undertaken within the framework of the Digital Operational Resilience Act (DORA), which aims to improve cyber resilience at the level of individual entities.

The ESRB will continue to work on an EU-wide strategy to help mitigate systemic cyber risk.

The ESRB will act as a hub to share progress reports and good practices, and update the conceptual approach to Cyber Resilience Scenario Testing and Systemic Impact Tolerance Objectives to integrate the experience and insights gained from pilot projects. Its future work will also include analysing operational financial crisis management tools for systemic cyber crises.

For media queries, please contact William Lelieveldt, tel.: +49 69 1344 7316.

European Systemic Risk Board

Directorate General Communications

Sonnemannstrasse 20, 60314 Frankfurt am Main, Germany

Tel.: +49 69 1344 7455, email: media@esrb.europa.eu, website: www.esrb.europa.eu

Reproduction is permitted provided that the source is acknowledged.