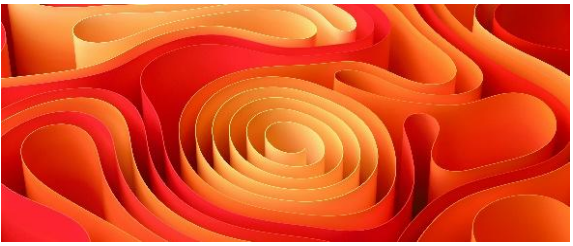
Pills

Regulatory/Supervisory Pills | N.64 April 2026

Author: Dario Esposito



TOPICS:

Stress Test

SOURCE:

Bank for International Settlements

BIS: Cyber Risk Stress Testing for Banks

- **Cyber stress tests** have emerged in response to the increasing frequency and sophistication of cyber incidents, which pose significant operational and systemic risks to banks. Unlike traditional solvency or liquidity stress tests, **these exercises focus** primarily **on operational resilience**, assessing how institutions respond to and recover from disruptions once preventive controls have failed.
- They are typically qualitative, scenario-based exercises rather than metric-driven or pass/fail assessments. There are **two principal approaches**: (i) **firm-focused tests**, which evaluate individual institutions' response and recovery capabilities, and (ii) **system-focused tests**, which assess broader financial stability implications, including contagion and interdependencies across institutions. The choice between these approaches should align with the authority's mandate and objectives, as it shapes scenario design, firm participation, and supervisory follow-up.
- **Designing** a cyber stress test involves defining **scope, selecting participants and constructing realistic but severe scenarios**. System-wide exercises often include banks, financial market infrastructures and critical service providers to capture interconnections, while firm-level tests typically cover a wider population of supervised banks to enable benchmarking. Scenario narratives are deliberately high-level to reflect uncertainty and avoid exposing vulnerabilities, while still enabling firms to test internal processes.
- **Execution** relies on iterative engagement with firms, often **through questionnaires**, **workshops and phased simulations**. Authorities assess capabilities such as incident response, communication, contingency planning and recovery time. Findings are largely qualitative but may incorporate indicators of operational continuity.
- **Post-exercise**, authorities provide confidential firm-specific feedback and **may integrate findings into supervisory processes** (eg SREP), although capital implications are generally absent. **Public disclosure is limited** to aggregated insights due to confidentiality and security concerns.