Consultation Fact Sheet

Cyber resilience toolkit: practical considerations for FMIs

Body	
Committee on Payments and Market Infrastructures (CPMI), IOSCO	
Published 2026-09-08	**Consultation deadline** 2026-12-01
Scope of application Cyber resilience frameworks of FMIs, covering governance, preparedness, response and recovery, and testing	**Impacted / targeted stakeholders** FMIs and their participants; linked FMIs and third-party service providers; regulatory and supervisory authorities responsible for oversight over FMIs

Synthesis

The Committee on Payments and Market Infrastructures (CPMI) and the Board of IOSCO are consulting on a voluntary, non-binding cyber resilience toolkit intended to provide financial market infrastructures with practical, technology-neutral support for strengthening their cyber resilience frameworks and implementing operational resilience-related components of the Principles for financial market infrastructures, as informed by the 2016 CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures. The toolkit is organized around four areas: (1) governance of cyber risk and resilience, including board and senior management capabilities, ecosystem risk management, maturity models and resilience metrics; (2) identification and design of extreme but plausible cyber scenarios, including scenario scope, threat intelligence, emerging risks and ecosystem dependencies; (3) response, resumption and recovery planning, covering critical operations and information assets, infrastructure and data resilience, third-party dependencies, contingency arrangements, safe resumption and the disconnection and reconnection of ecosystem entities; and (4) cyber resilience testing and exercising.

01

Purpose & rationale

Cyber risks to FMIs are intensifying, while AI is increasing the speed and sophistication of attacks. CPMI-IOSCO's 2022 implementation assessment identified scope to improve cyber response and recovery plans and resilience planning and testing. Although the PFMI and Cyber Guidance remain fit for purpose, these findings and the evolving threat environment indicate a need for practical, adaptable implementation support. FMIs' interconnectedness also requires measures addressing contagion and coordinated recovery across their ecosystems.

Specific policy objectives:

- Strengthen governance and assessment of the adequacy and effectiveness of cyber resilience frameworks.
- Improve preparedness for extreme but plausible scenarios and capabilities for safe response, resumption and recovery.
- Limit ecosystem contagion through coordination, testing and continuous improvement.

02

Key issues for discussion

The toolkit comprises four complementary tools with practical considerations for each. The considerations are voluntary options, to be selected according to an FMI's needs rather than applied as an exhaustive checklist.

Dimension	Practical considerations
Tool 1: Governance of cyber resilience at FMIs	
Board capabilities	▪ Build a baseline level of cyber knowledge through workshops, briefings, case studies, training and cyber security simulations. ▪ Cover current and emerging threats, including the FMI's AI deployments, AI provider concentration and AI-enabled adversary capabilities. ▪ • Supplement board expertise through continuing professional education, experienced staff or independent external advice.
Ecosystem oversight	▪ Incorporate ecosystem-related risks into the cyber resilience strategy and framework from an end-to-end perspective. ▪ Involve the board and senior management in oversight and exercises assessing ecosystem interdependencies and response coordination. ▪ Integrate the cyber resilience framework with the broader enterprise-wide risk management framework.
Benchmarking and metrics	▪ Use maturity models to assess the adequacy and effectiveness of the cyber resilience framework, identify gaps and prioritize improvements. ▪ Tailor strategic, operational and control-effectiveness metrics to the information needs of the board, senior management and control functions. ▪ Use historical and predictive metrics to monitor performance against cyber resilience and risk tolerance thresholds and inform decision-making.
Tool 2: Extreme but plausible cyber scenario identification and design	
Scenario development process	▪ Define scenario objectives, scope and boundaries, formulation procedures, governance and independent review or challenge. ▪ Map information assets, ICT infrastructure and ecosystem dependencies, including critical third-party dependencies. ▪ Incorporate previous incidents and testing, business impact analysis, threat intelligence and horizon scanning. ▪ Assess critical assets, vulnerabilities, emerging threats, trends and uncertainties relevant to the FMI.
Realism and complexity	▪ Develop diverse "what-if" scenarios tailored to the FMI's environment, threat landscape and role in the financial system. ▪ Incorporate complexity through factors such as simultaneous attacks, multiple control failures, disruption at critical cut-offs, impacts across multiple sites and supply-chain or nth-party dependencies. ▪ Consider hybrid threats, disinformation and concurrent events such as market stress or energy and telecommunications outages. ▪ Include scenarios where the two-hour resumption objective cannot be achieved, particularly where data integrity is affected.

Dimension	Practical considerations
Validation and updating	▪ Assess scenario impacts and back-test scenarios against past cyber or operational incidents. ▪ Test strategies and response, resumption and recovery plans against the scenarios and identify vulnerability gaps. ▪ Conduct root cause analysis and use lessons learned to refine scenarios, response strategies and recovery measures. ▪ Regularly update scenarios as threats and the FMI's broader context evolve, and share relevant findings through trusted channels.
Tool 3: Developing response, resumption and recovery plans	
Critical operations, assets and dependencies	▪ Identify and document critical operations, systems, information assets, key roles and internal and external dependencies. ▪ Maintain current inventories and network diagrams covering critical assets, interconnections and third-party dependencies. ▪ Integrate asset and dependency management with acquisition, change management and related processes.
Resilience and recovery capabilities	▪ Strengthen infrastructure resilience through measures such as infrastructure as code, layered architectures and non-similar facilities. ▪ Support data recovery through reconciliation, an uncorrupted "golden point", protected backups and isolated recovery environments. ▪ Build application resilience through backup or degraded operating modes, event-driven architectures, transaction replay and dependency mapping.
Contingency and safe resumption	▪ Agree contractual and operational arrangements in advance, including for third-party dependencies. ▪ Establish and test pre-authorized emergency procedures and non-standard settlement arrangements for severe disruptions. ▪ Base safe resumption on eradication of the root cause, system functionality, data integrity, absence of contagion and effective communication.
Disconnection and reconnection	▪ Define objective criteria, governance and documented processes for disconnecting and reconnecting ecosystem entities. ▪ Apply a staged reconnection process covering assessment, remediation, assurance, reconnection and recovery/resumption, with verification where appropriate. ▪ Maintain clear communications and regularly test and review the arrangements.
Tool 4: Cyber resilience testing and exercising	
Testing program design and coverage	▪ Develop a risk-based testing program with clear objectives, scope and scheduling, proportionate to system criticality and cyber maturity. ▪ Combine vulnerability assessments, penetration and red team testing, backup and failover testing, business continuity testing and crisis exercises. ▪ Include ecosystem, cross-sectoral and cross-border exercises where relevant, with clear governance, responsibilities and resources.
System changes and advanced testing	▪ Identify significant system changes through structured change management and test before and after implementation according to risk. ▪ Embed automated security testing and centrally track, prioritize and validate remediation of identified vulnerabilities. ▪ Tailor red team and AI-assisted testing to the FMI's risk profile and critical dependencies, with appropriate safeguards and human oversight.

Dimension	Practical considerations
Learning, remediation and continuous improvement	▪ Assess outcomes against measurable detection, response and recovery criteria and analyze findings and root causes. ▪ Assign remediation actions, owners and timelines and validate fixes through follow-up testing. ▪ Incorporate lessons from tests, exercises and real incidents into the cyber resilience framework and future testing.