



TOPICS:

Cyber risk

SOURCE:

Committee on Payments and Market Infrastructures & International Organization of Securities Commissions

BIS/CPMI-IOSCO: Third-Party Risk & Cyber Resilience for FMIs

- The two CPMI-IOSCO publications provide a complementary framework for strengthening the **operational and cyber resilience of financial market infrastructures (FMIs)**, with particular emphasis on dependencies across the wider FMI ecosystem. Both build on the "Principles for Financial Market Infrastructures (PFMI)" and **do not establish additional binding standards**.
- The **third-party risk discussion paper** identifies **six key challenges**: increasing ecosystem complexity and interconnectedness; concentration among service providers, potentially creating vendor lock-in and systemic dependencies; complex and opaque supply chains; difficulties in exit planning and provider substitution; bargaining-power imbalances that may constrain contractual protections; divergent regulatory expectations across jurisdictions. These vulnerabilities are expected to become increasingly important as FMIs further outsource critical services and adopt technologies such as AI and distributed ledger technology.
- The **cyber resilience Toolkit** complements this analysis through **four practical areas**: cyber governance; identification and design of extreme-but-plausible scenarios; response, resumption and recovery planning; and cyber resilience testing and exercising.

It emphasises end-to-end mapping of critical operations, information assets, service providers and wider supply-chain dependencies, alongside Board and senior management oversight, maturity models, resilience metrics and ecosystem-wide testing. It also considers safe disconnection and reconnection of ecosystem entities following cyber incidents.

- Taken together, the publications signal a shift towards an **ecosystem-wide approach to operational resilience**. The discussion paper identifies **where third-party dependencies may create or amplify operational and systemic risks**, while the Toolkit provides practical approaches for **incorporating those dependencies into cyber resilience frameworks**. Governance, provider concentration, contractual arrangements, scenario analysis, recovery capabilities and testing should therefore account not only for the individual FMI but also for participants, linked FMIs, third-party providers and nth-party dependencies. Feedback on the third-party risk discussion paper is due by **1 December 2026**.

