Committee on Payments and Market Infrastructures

8 September 2026

# CPMI-IOSCO consultation on cyber resilience at FMIs

## Summary

The BIS Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) are today publishing for public comment the *Cyber resilience toolkit: practical considerations for FMIs* (toolkit).

The toolkit provides practical considerations to support FMIs as they seek to strengthen their cyber resilience frameworks and implement operational resilience-related components of the 2012 CPMI-IOSCO *Principles for financial market infrastructures* (PFMI),[1] as informed by the 2016 CPMI-IOSCO *Guidance on cyber resilience for financial market infrastructures* (Cyber Guidance). The intended audience for this toolkit includes FMI board members, non-board senior management and personnel with operational and cyber risk and resilience-related responsibilities.

The toolkit comprises a set of voluntary, non-binding tools which contain practical considerations across four broad topics most relevant to further enhancing the cyber resilience of FMIs, consistent with the PFMI and as informed by the Cyber Guidance: (i) governance of cyber risk and resilience; (ii) scenario identification and design; (iii) response, resumption and recovery plans; and (iv) testing and exercising. In developing the toolkit, CPMI and IOSCO have considered input from industry workshops, the findings of the 2022 CPMI-IOSCO *Implementation monitoring of the PFMI: Level 3 assessment on Financial Market Infrastructures' Cyber Resilience* (L3 assessment) and analysis of relevant industry standards.

The practical considerations in the toolkit are intended to be technology-neutral and applicable to a wide range of FMIs. They are not intended to provide exhaustive coverage of a given topic or impose additional standards on FMIs beyond those set out in the PFMI, as informed by the Cyber Guidance. The toolkit encourages viewing the practical considerations through the lens of the FMI's ecosystem as well as from the perspective of the individual FMI.

CPMI and IOSCO are also consulting on a related publication, the discussion paper *FMIs' reliance on third-party service providers: challenges and risks*. The discussion paper identifies and explores key challenges for FMIs in third-party risk management and considers cyber resilience at FMIs in the context of the ecosystem risk posed by third-party service providers.

## Background

In 2016, CPMI-IOSCO published the Cyber Guidance to enhance FMIs' cyber resilience in the context of the PFMI concerning governance (Principle 2), the framework for the comprehensive management of risks (Principle 3), settlement finality (Principle 8), operational risk (Principle 17) and FMI links (Principle 20). The Cyber Guidance provides supplemental detail related to the preparations and measures that FMIs may undertake to enhance their cyber resilience capabilities, with the objective of limiting the escalating risks that cyber threats pose to financial stability.

[1] The Committee on Payment and Settlement Systems (CPSS) changed its name to the BIS Committee on Payments and Market Infrastructures (CPMI) on 1 September 2014.

In 2022, the L3 assessment identified several issues and observations related to FMIs' implementation of the PFMI, including on scenario development, recovery and response planning, cyber testing and the governance of cyber risk and resilience.

Since then, cyber risks to FMIs have intensified in frequency and nature. For example, the volume of cyber attacks on financial institutions has increased since the publication of the Cyber Guidance, and recent developments in artificial intelligence (AI) models require firms to consider adapting their defences against the speed, volume and complexity of AI-driven threats.

The toolkit has been informed by the L3 assessment's findings and the evolving threat environment, which together highlight the need for practical, adaptable resources to support effective, real-world implementation of the Principles noted above.

## The toolkit

The toolkit contains practical considerations across four non-binding tools covering the following broad topics, which also include overarching elements such as ecosystem and AI risks:

1. **Governance of cyber risk and resilience** provides practical considerations which may assist FMIs in strengthening the governance of FMIs' cyber resilience frameworks relating to roles and responsibilities, maturity models and metrics for measuring resilience.
2. **Scenario identification and design** provides practical considerations for extreme but plausible scenario construction by outlining potential strategies and methodologies for their design using a risk-based approach.
3. **Response, resumption and recovery plans** provide practical considerations which may assist their design, including identifying critical operations, designing key scenario elements and handling disconnection and reconnection processes.
4. **Cyber resilience testing and exercising** provides practical considerations which may assist cyber resilience testing programmes at FMIs, including on categories of testing, tailoring test programmes to an FMI's requirements, conducting red team testing and learning, and evolving from testing and exercising.

The toolkit is intended to be used with due consideration to an FMI's risk profile and the scale, complexity and nature of activity undertaken. The materials in the four tools may be used individually or in combination depending on specific needs and priorities.

Recognising that cyber resilience cannot be achieved in isolation and requires FMIs to consider the bidirectional interdependencies present in each aspect of their cyber resilience frameworks, each tool also provides considerations for identifying, managing and mitigating the cyber risks that FMIs face from (and pose to) the entities in their ecosystems.

## Consultation

The CPMI and IOSCO invite comments on the content of the toolkit by 1 December 2026.

Responses should be sent via email to the Secretariats of the CPMI and IOSCO (cpmi@bis.org; cpmi-iosco@iosco.org). Responses will be published on the websites of the BIS and IOSCO unless respondents expressly request otherwise. Commercial, personal or other sensitive information should not be included in the submissions, or may be included, with redactions for publication clearly noted. After the consultation, CPMI and IOSCO will publish a final version of the report, taking into account the comments received.