Committee on Payments and Market Infrastructures | BIS | IOSCO

08 September 2026

CPMI-IOSCO consultation on third-party risk 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 discussion paper *FMIs' reliance on third-party service providers: challenges and risks*.[1]

The discussion paper identifies and explores the risks and challenges associated with the increased reliance of financial market infrastructures (FMIs)[2] on third-party service providers, in particular for the delivery of critical services. The paper examines six key challenges and discusses how they may amplify risks, noting the particular importance of FMIs' management of these risks due to their unique and highly interconnected role in the financial system. The paper aims to facilitate sharing of existing practices and views on third-party risk management at FMIs, by highlighting key issues and providing an opportunity for industry participants to submit feedback on its findings and identify opportunities for further engagement.

CPMI-IOSCO's development of the discussion paper has been firmly anchored in the 2012 CPMI-IOSCO *Principles for financial market infrastructures* (PFMI), specifically Principle 17 (Operational risk) and Annex F (Oversight expectations applicable to critical service providers). These elements were compared with third-party and outsourcing guidance published by other international standard-setting bodies and international organisations.[3]

The discussion paper also incorporates input from industry workshops with FMIs and third-party service providers as well as the results of surveys of member authorities and FMIs. It also draws from the findings of the 2022 CPMI-IOSCO *Implementation monitoring of the PFMI: Level 3 assessment on Financial Market Infrastructures' Cyber Resilience* and 2021 CPMI-IOSCO *Implementation monitoring of PFMI: Level 3 assessment of FMIs' business continuity planning*.

CPMI-IOSCO are seeking industry feedback on the discussion paper, with the aim of understanding whether the challenges to third-party risk management it identifies are comprehensive and whether further support on this topic by CPMI-IOSCO would be beneficial to FMIs and other industry participants.

CPMI-IOSCO are also consulting on a related publication, *Cyber resilience toolkit: practical considerations for FMIs*. The toolkit comprises a set of voluntary, non-binding tools across four key topics relevant to enhancing the cyber resilience of FMIs consistent with the PFMI.[4] It is designed to be viewed

1 The discussion paper is not intended to impose additional standards beyond those set out in the PFMI.

2 FMIs play a critical role in the financial system and the broader economy. For the purposes of the discussion paper, the term FMI refers to payment systems, central securities depositories, securities settlement systems, central counterparties and trade repositories.

3 These include IOSCO, *Principles on outsourcing, final report*, 2021; FSB, *Toolkit for Enhancing Third-Party Risk Management and Oversight*, 2023; Basel Committee on Banking Supervision, *Principles for the sound management of third-party risk,* 2025; and International Association of Insurance Supervisors, *Application Paper on operational resilience objectives and toolkit,* 2026.

4 As informed by CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures*, 2016.

not just from the perspective of an individual FMI but also through the lens of the FMI's ecosystem, a key risk area identified in this discussion paper.

Background

The FMI ecosystem is growing more complex. This is demonstrated by the interconnected nature of FMIs within the financial system, through links to other FMIs or trading venues, market participants and critical service providers. FMIs' ability to manage third-party risks in a robust manner and recover from operational incidents, including those that may originate from third-party service providers, is vital to support financial stability and market confidence.

Using services offered by third parties, including for critical services, may present challenges to FMIs' operational resilience. FMIs' use of third-party service providers, particularly for services such as information and communication technology, has increased significantly over the last 10 years across multiple jurisdictions. This has been driven by factors such as scalability needs, technological modernisation and cost efficiency.

CPMI-IOSCO expect FMIs' reliance on third-party service providers for critical services will continue to increase as they modernise their information systems and consider the use of emerging technologies such as artificial intelligence and distributed ledger technology. Moreover, FMIs may continue to increase their reliance on third-party service relationships in both intragroup and external arrangements.

Against this background, CPMI-IOSCO have analysed the current state of FMIs' use of and reliance on third-party service providers, with a view to understanding the key risks associated with this trend. The discussion paper sets out the findings of this analysis.

Discussion paper

The discussion paper identifies and explores six categories of challenges identified by CPMI-IOSCO that contribute to increased risk.

1. **Increasing complexity and interconnectedness of FMIs' ecosystems,** which increase their exposure to and ability to transmit risk, including **cyber risk.**
2. **Concentration of third-party service providers**, including (i) where individual FMIs depend on one or more services provided by a single or limited number of third-party service providers (this may lead to a lack of substitutability and vendor lock-in, where the disruption or failure of such services has potential implications for the FMI's critical operations); and (ii) where the FMI ecosystem depends on one or more services provided by a single third-party service provider or limited number of third-party service providers, the disruption or failure of which may have systemic implications.
3. **Complex and opaque supply chains**, which can make identification and management of risks related to critical dependencies difficult and hinder resilience planning.
4. **Difficulties with exit planning,** reflecting the potential inability to substitute or terminate contracts with third-party service providers, particularly for critical services. Even where substitute providers are available, high switching costs and complex system architectures may make exit impracticable, especially in stressed scenarios.
5. **Imbalances in bargaining power** driven by concentration of third-party service providers which can leave FMIs with limited choices, constraining FMIs' ability to negotiate contractual terms that may be needed to support effective risk management.

6. **Variation in regulatory expectations,** which occurs across jurisdictions due to differences in national regulatory frameworks, mandates and legal authority, may create challenges for FMIs managing third-party risks. Variations in scope, definitions and data requirements may complicate the design of consistent risk management frameworks, increase compliance burden and hinder contract standardisation.

The discussion paper then sets out a number of questions for feedback from different stakeholders on identified risks.

For all stakeholders

1. Are the challenges identified in this discussion paper accurate and comprehensive? Are there any challenges that are missing or discussion that is incomplete?
2. For each challenge identified in this discussion paper (and any others considered relevant), what are possible solutions?
3. For any of these challenges, would further engagement or policy from CPMI-IOSCO be helpful? Please explain your answer.
4. Would further discussion with CPMI-IOSCO on third-party risk management be helpful and, if so, are there any specific areas that would be beneficial to discuss? Please explain your view.
5. Are there any contractual aspects, in addition to those addressed in this paper, that are particularly relevant or challenging in the context of FMI third-party risk management?

For FMIs

6. Does your organisation use any international publications, in addition to those published by CPMI-IOSCO, to inform the design of your third-party risk management framework (for example, the FSB toolkit, the IOSCO Principles on outsourcing, the BCBS Principles)? If yes, please explain how these documents are used (eg with respect to risk management models, roles and responsibilities, the types of risk controlled and solutions/measures)?
7. From an FMI perspective, should authorities be aware of any current or emerging topics associated with the provision of third-party services across jurisdictions that have a material impact on FMIs' third party risk management?

For third-party service providers

8. Does your organisation have insight into the extent to which your service(s) are critical to the FMIs you serve, so they are able to meet applicable jurisdictional regulatory, supervisory or oversight requirements in relation to their operational resilience? If yes, please explain how.
9. What information, tools and contractual rights do you provide to your FMI customers to support their ability to manage risk, including cyber risks and other risks arising in the supply chain?
10. Is your organisation subject to any regulations or guidelines that may conflict with those that your FMI clients are required to follow?
11. From a third-party service provider perspective, should authorities be aware of any current or emerging topics associated with the provision of third-party services across jurisdictions that have a material impact on FMIs' third party risk management?

Consultation

The CPMI and IOSCO invite feedback on the questions in the discussion paper by 01 December 2026.

Responses to the questions 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.