Consultation Fact Sheet

FMI's reliance on third-party service providers: challenges and risks

Body	
Committee on Payments and Market Infrastructures (CPMI), IOSCO	
Published 2026-09-08	**Consultation deadline** 2026-12-01
Scope of application Third-party risk management by financial market infrastructures (FMIs): payment systems, central securities depositories, securities settlement systems, central counterparties and trade repositories, covering both external service providers and intra-group arrangements	**Impacted / targeted stakeholders** FMIs and their participants; third-party service providers; regulatory and supervisory authorities responsible for oversight over FMIs

Synthesis

CPMI-IOSCO are seeking feedback on six risk management challenges arising from FMIs' increased reliance on third-party service providers: (1) interconnected and complex ecosystems, including cyber-related risks; (2) provider concentration; (3) complex and opaque supply chains; (4) exit planning; (5) bargaining power imbalances; and (6) variation in regulatory, supervisory and oversight expectations. The paper examines how these dependencies can amplify operational disruption across the financial system and highlights existing standards, guidance and tools that may support FMIs' risk management. It seeks views on whether the challenges are comprehensive and whether further CPMI-IOSCO support would be beneficial.

01

Purpose & rationale

FMIs' growing use of third-party services is driven by scalability needs, technological modernisation and cost efficiency. Reliance is expected to increase as FMIs modernise their information systems through cloud computing and consider emerging technologies such as artificial intelligence and distributed ledger technology. These developments can deepen operational dependencies and complicate risk management.

FMIs concentrate activity and operate within highly interconnected financial networks, while their payment, clearing and settlement services typically have limited substitutability. Disruptions can therefore transmit or amplify risks across the financial system. The paper draws on authority and FMI surveys, industry roundtables and existing international publications to examine the resulting challenges.

Specific policy objectives:

- Identify third-party risk management challenges that are particularly important for FMIs given their critical role and interconnectedness.
- Facilitate the sharing of existing practices, standards, guidance and tools.
- Gather feedback on possible solutions and where further CPMI-IOSCO engagement or policy work would be beneficial.

02

Key issues for discussion

Discussion area	Key challenges	Existing guidance and practice
Increasingly interconnected and complex ecosystem, including cyber-related risks	Links with participants, other FMIs and service providers can transmit and amplify operational disruption. Supply chain attacks may exploit weaker links through information and communication technology (ICT) connections, with monitoring particularly challenging across complex, cross-border supply chains.	PFMI Principle 17 and the Cyber Guidance require FMIs to identify, monitor and manage risks arising from participants, other FMIs and third-party service providers, including through cyber governance, scenario design, response and recovery planning and testing. IOSCO and BCBS materials further require assessment of providers' ICT and cyber controls, contractual security and incident-notification provisions, ongoing monitoring and business-continuity testing. FMIs reported maintaining rapid information-sharing channels for ICT incidents, but the L3 Cyber review found that some do not involve external parties in response, resumption and recovery testing.
Concentration of third-party service providers	At individual FMI level, dependencies may concentrate across services, geographic regions or common nth-party providers, threatening critical operations. At systemic level, reliance by multiple FMIs or financial institutions on a limited number of providers can create wider disruption. Limited interoperability and complex service relationships may cause vendor lock-in.	IOSCO's outsourcing principles require firms to identify and manage reliance on a single provider for material or critical services, including where the same provider serves multiple regulated entities, with due diligence used to assess dependency and possible diversification. FSB and BCBS materials apply comparable risk-management expectations to intra-group arrangements rather than treating them as inherently lower risk. In practice, FMIs balance diversification against additional cost, complexity and the new risks introduced by each additional provider, while authorities may collect provider data to identify concentrations that are not visible to individual FMIs.

Discussion area	Key challenges	Existing guidance and practice
Complexity and opacity of supply chains	Complex service architectures and limited access to supplier information obscure critical dependencies and hinder contingency planning. Only a small proportion of surveyed FMIs had visibility beyond fourth-party service providers; providers themselves reported that visibility degrades quickly along the supply chain.	PFMI expects contracts with critical service providers to preserve FMI and authority access to necessary information, require FMI approval before material sub-outsourcing and maintain clear communication channels. The FSB Toolkit and BCBS Principles extend this to mapping supply chains, identifying key nth parties, ongoing due diligence and monitoring, prior notification of material subcontracting changes, incident reporting and access or audit rights over relevant subcontractors. Providers reported monitoring their own critical third parties and communicating material fourth-party incidents, while FMIs expressed interest in testing across the full supply chain, including participants.
Difficulties with exit planning	Different system architectures, time- and resource-intensive switching, and service criticality can make exit impracticable, particularly during stress. Providers' planning often focuses on loss of a region or service rather than complete disengagement. FMIs may need other operational resilience options where immediate exit is unrealistic.	FMI expects contracts with critical service providers to preserve FMI and authority access to necessary information, require FMI approval before material sub-outsourcing and maintain clear communication channels. The FSB Toolkit and BCBS Principles extend this to mapping supply chains, identifying key nth parties, ongoing due diligence and monitoring, prior notification of material subcontracting changes, incident reporting and access or audit rights over relevant subcontractors. Providers reported monitoring their own critical third parties and communicating material fourth-party incidents, while FMIs expressed interest in testing across the full supply chain, including participants.

Discussion area	Key challenges	Existing guidance and practice
Imbalance of bargaining power	FMIs may be systemically important but relatively small customers from a provider's revenue perspective. Limited bargaining power can impede negotiation and enforcement of audit rights, information-sharing provisions, service-level expectations and access to testing with providers.	Existing standards do not directly address bargaining-power imbalances, but they expect contractual arrangements to give FMIs the information, access, audit, service-level, incident-reporting and resilience-testing rights needed to manage critical third-party relationships. PFMI requires access to necessary information; the FSB Toolkit covers service levels, performance expectations, audit and oversight rights and nth-party visibility; and BCBS Principle 5 covers access, audit and information rights for critical arrangements. Industry feedback indicates that these rights can be difficult to negotiate or enforce, particularly with large providers, and that participation in joint testing remains constrained.
Variation in regulatory, supervisory and oversight expectations	Differences in definitions, scope, criticality designations and data collection complicate cross-jurisdictional risk management frameworks. Some jurisdictions focus on outsourcing; others include broader third-party relationships, intra-group arrangements and subcontractors. Most data collection focuses on direct providers rather than the full supply chain.	PFMI allows jurisdictions flexibility in how its principles are implemented and permits authorities to impose higher requirements, so some variation is inherent. In practice, jurisdictions differ in the specificity of requirements for due diligence, contractual clauses, access rights, business continuity and testing; in whether authorities directly oversee service providers; and in the scope and depth of data collected on direct and nth-party providers. Providers respond by standardising contracts across jurisdictions where possible, rolling common changes across clients and, in some cases, using financial-services addenda.

03

Consultation questions & next steps

CPMI-IOSCO seek feedback on whether the identified challenges are accurate and comprehensive, possible solutions, additional contractual difficulties, and the value of further engagement or policy work. FMIs are also asked how they use other international publications and about material cross-jurisdictional issues. Service providers are asked about their understanding of service criticality; the information, tools and contractual rights they provide to support FMI risk management; conflicting regulations or guidelines; and material cross-jurisdictional developments.