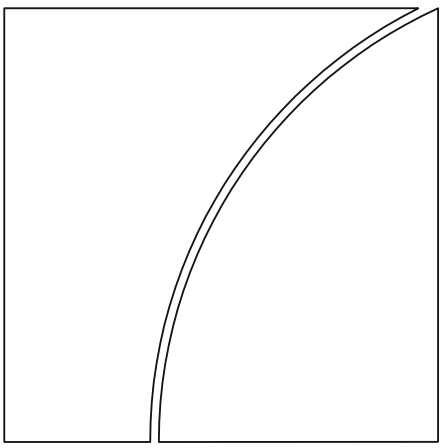
Committee on Payments and Market Infrastructures

Board of the International Organization of Securities Commissions



Discussion paper

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

September 2026

BIS

IOSCO

This publication is available on the BIS website (www.bis.org) and the IOSCO website (www.iosco.org).

ISBN 978-92-9259-969-0 (online)

Contents

Executive Summary

This paper discusses the risk management challenges associated with the increased reliance of financial market infrastructures (FMIs) [1] on third-party service providers [2] and FMIs' resulting increased operational risk exposure, particularly for the delivery of their critical services.[3] It explores where it may be particularly important to address these challenges due to FMIs' critical role and interconnectedness within the financial system. It also examines relevant work that other standard-setting and international bodies have undertaken with respect to third-party risk management in other parts of the financial sector.

The Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions (CPMI-IOSCO) have analysed the current state of FMIs' use of, and increasing reliance on, third-party service providers, with a view to identifying and understanding the key risks associated with this movement. CPMI-IOSCO are seeking industry feedback to learn whether the risk management challenges discussed are comprehensive and whether further support on this topic by CPMI-IOSCO would be beneficial to FMIs and other industry participants.[4]

In recent years, FMIs have increasingly used services offered by third parties, including for critical services, elevating the complexity of FMIs' ecosystems. This may present challenges to their operational resilience. FMIs are highly interconnected within the financial system through links with other FMIs, trading venues, market participants and third-party service providers, and many are considered systemically important. Therefore, their ability to manage third-party risks in a robust manner and recover from operational incidents that may originate from third-party service providers is vital to support financial stability and market confidence.

Against this background, **CPMI-IOSCO have identified the following key risk management challenges to FMIs' operational resilience:**

1. **Increasing complexity and interconnectedness of FMIs' ecosystems,** which increases 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.

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

[2] The CPMI Glossary defines "third-party service provider to an FMI" as "An unaffiliated entity that provides services to an FMI. This can be a utility such as electricity companies and network providers, or an entity which the FMI "outsources" part of its operations, such as IT infrastructure." (see www.bis.org/cpmi/publ/d00b.htm). However, for the purposes of this discussion paper, the term "third-party service provider" includes intra-group arrangements as well.

[3] The results of the survey of CPMI-IOSCO member authorities indicate that FMIs' use of third-party service providers has increased, particularly for cloud computing and other IT related services. Surveyed authorities consider this reliance will increase further in the next three to six years. See section 1.1 below.

[4] This discussion paper is not intended to create additional guidance for FMIs.

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.

In this discussion paper, CPMI-IOSCO refers to guidance and tools from international organisations and standard-setting bodies alongside the risk management challenges identified in order to highlight existing guidance and tools that may be relevant to FMIs. For example, the Financial Stability Board's (FSB) *Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities*[5] (FSB toolkit) is aimed broadly at the financial sector and provides additional resources that FMIs could leverage to support their third-party risk management practices. CPMI-IOSCO does not intend to provide new definitions within this paper. Where applicable, the definitions of common terms used throughout this paper, such as "third-party service relationship", "service provider", "outsourcing" and "supply chain", follow those set out on pages 4–6 of the FSB toolkit.

FMIs' unique and highly interconnected nature and the fact they may be a point of concentration in financial markets means any outage in their services could cascade risks and disruption throughout the financial system. At the same time, FMIs may be especially exposed when they procure products and services for which a small number of third-party service providers dominate the market. The effects of this may intensify as FMIs continue to transition towards cloud computing as well as other emerging technologies, such as artificial intelligence (AI), with limited major suppliers. For this reason, CPMI-IOSCO are seeking industry feedback on the materiality of these challenges, and on how CPMI-IOSCO may be able to help to address these challenges.

[5] See FSB, *Final Report on Enhancing Third-party Risk Management and Oversight – A Toolkit for Financial Institutions and Financial Authorities*, December 2023, at www.fsb.org/2023/12/final-report-on-enhancing-third-party-risk-management-and-oversight-a-toolkit-for-financial-institutions-and-financial-authorities/

1. Introduction: FMIs and the third-party risk landscape

This discussion paper aims to: facilitate the sharing of existing practices, standards, guidance, and tools related to third-party risk management; foster dialogue; and support industry efforts related to enhancing third party risk management by:

- highlighting key issues and challenges in FMIs' third-party risk management; and
- providing an opportunity for industry participants to share feedback on the analysis and identify instances where further engagement or policy would be beneficial.

CPMI-IOSCO have analysed the current state of FMIs' use of third-party service providers and their increased reliance on them, with a view to understanding the key risks associated with this trend and the challenges to managing those risks. CPMI-IOSCO conducted analysis focused on three overarching themes: (i) understanding the current landscape and trends in third-party risks and outsourcing; (ii) exploring relevant international standards, guidance, and tools as well as jurisdictional expectations; and (iii) examining challenges in FMIs' management of third-party risks and whether any further policy work may be helpful.

1.1 Background and inputs to the discussion paper

To gain an understanding of the current landscape and trends in the use of third-party service providers and the management of related risks, CPMI-IOSCO conducted a survey of CPMI-IOSCO member authorities (summarised below). CPMI-IOSCO also engaged with FMIs and third-party service providers from multiple jurisdictions conducting a survey of FMIs and holding virtual roundtables with FMIs and third-party service providers. These are summarised in Annex 1.

CPMI-IOSCO explored relevant international standards, guidance, and other publications to identify tools that could be relevant to FMIs. CPMI-IOSCO compared the *Principles for Financial Market Infrastructures* (PFMI) Principle 17 on operational risk, and Annex F on oversight expectations applicable to critical third-party service providers[6] with third-party or outsourcing guidance and tools provided by the Basel Committee on Banking Supervision (BCBS), the International Association of Insurance Supervisors (IAIS), IOSCO and the FSB. The analysis also considered the findings of CPMI-IOSCO Level 3 implementation monitoring assessments of FMIs' business continuity planning[7] and cyber resilience, [8] to understand where there may be differences in implementation of the PFMI in relation to FMIs' management of risks associated with third-party service providers.

These inputs have supported CPMI-IOSCO's analysis of challenges in FMIs' management of third-party risks, which are explored in section 2 of this paper. Section 3 concludes the analysis and section 4 sets out questions for which CPMI-IOSCO are seeking feedback.

Current landscape and trends in the use of third-party service providers

FMIs' use of third-party service providers, particularly for services such as information and communication technology (ICT), has increased over the last 10 years across many jurisdictions. This has

6 CPMI–IOSCO, *Principles for financial market infrastructures,* April 2012, www.bis.org/cpmi/publ/d101.htm and www.iosco.org/library/pubdocs/pdf/IOSCOPD377-PFMI.pdf.

7 CPMI-IOSCO, *Implementation monitoring of PFMI: Level 3 assessment of FMIs' business continuity planning*, July 2021, at www.bis.org/cpmi/publ/d197.htm and www.iosco.org/library/pubdocs/pdf/IOSCOPD680.pdf

8 CPMI-IOSCO, *Implementation monitoring of the PFMI: Level 3 assessment on Financial Market Infrastructures' Cyber Resilience*, November 2022, at www.bis.org/cpmi/publ/d212.htm and www.iosco.org/library/pubdocs/pdf/IOSCOPD723.pdf

been driven by factors such as scalability needs, technological modernisation, and cost efficiency. FMIs' reliance on third-party service providers for critical services is expected to increase as FMIs continue to modernise their information systems, such as through cloud computing, and consider the use of emerging technologies such as AI, distributed ledger technology and likely, in the medium to long term, quantum computing. Moreover, FMIs may continue to increase their reliance on third-party service provider relationships through their intra-group organisation and/or directly through an external service provider.

Jurisdictions' regulatory, supervisory and oversight expectations for third-party risk management

CPMI-IOSCO surveyed their member jurisdictions on their regulatory, supervisory and oversight expectations and supervisory practices regarding FMIs' management of third-party risks. Relevant regulations often draw on PFMI Principle 17 and Annex F. Typically, jurisdictions noted or implied that FMIs retain ultimate responsibility for managing risks from activities provided by a third-party service provider.

The survey found that requirements across jurisdictions differ in their level of specificity.[9] For instance, some jurisdictions have specific requirements for FMIs related to third-party risk management on due diligence, contractual clauses, access rights, business continuity planning and testing, whereas others prescribe more general risk management principles. CPMI-IOSCO observed variation among member jurisdictions in approaches, where some require FMIs to monitor and manage their third-party risks, whereas other authorities may also have some supervisory and oversight responsibilities over third-party providers. Similarly, data collection from FMIs also varies across jurisdictions in frequency, scope, and depth. For example, most jurisdictions require FMIs to provide data on "first level" service providers, but only some require data on nth-party service providers (ie sub-contractors along the supply chain).[10] [11]

International standards, guidance, and other third-party risk management publications by standard-setting and other international bodies

CPMI-IOSCO's work on third-party risk for FMIs is anchored in the PFMI, notably Principle 17 on operational risk and Annex F on oversight expectations for critical third-party service providers. PFMI Principle 17 states "An FMI should identify, monitor, and manage the risks that key participants, other FMIs, and service and utility providers might pose to its operations. In addition, an FMI should identify, monitor, and manage the risks its operations might pose to other FMIs." Explanatory notes 3.17.19-21 to the PFMI provide further detail on how FMIs should conduct third-party risk management, including that an FMI should identify the risks from its critical third-party service providers and have contracts with third-party service providers that allow the FMI access to necessary information. Annex F provides expectations that a regulator, supervisor or overseer of an FMI may want to establish for an FMI's critical third-party service providers in order to support the FMI's overall safety and efficiency.

[9] As noted in PFMI Responsibility D 4.4.1, "The adoption and application of [the PFMI] can greatly enhance regulatory, supervisory, and oversight efforts by relevant authorities and support the establishment of important minimum standards for risk management…the precise means through which the principles are applied will vary from jurisdiction to jurisdiction…"

[10] See FSB toolkit, p. 23. Also note that the FSB toolkit defines "Nth-party service provider" as "a service provider that is part of a third-party service provider's supply chain and supports the ultimate delivery of services to one or more financial institutions."

[11] For the purposes of this discussion paper, the definition of supply chain is consistent with the definition used in the FSB toolkit: "The network of entities that provide infrastructure, physical goods, services and other inputs directly or indirectly utilised for the delivery of a service to a financial institution. For the purposes of the toolkit, the scope of supply chain is limited to the services under a third-party service relationship."

Internationally, several organisations and standard-setting bodies have issued publications on managing third-party risk. Throughout section 2 of this paper, CPMI-IOSCO refers to relevant passages from these publications in order to highlight existing guidance and tools that may be relevant to FMIs' management of the risks highlighted. For example, the FSB toolkit is directed toward financial institutions in their management of third-party risks, and to authorities in their oversight of financial institutions. Given the FSB toolkit is aimed broadly at the financial sector, it provides additional resources that FMIs could leverage to support their third-party risk management practices. The FSB toolkit provides a lifecycle-based, risk-proportionate set of tools for managing critical third-party relationships, including definitions, methods for identifying systemic dependencies, and considerations for supply-chain (nth-party) risk.

There are also sector-specific documents. The BCBS *Principles for the sound management of third-party risk* (2025) [12] (BCBS Principles) provide granular recommendations on governance, contracting, intragroup outsourcing, supply-chain visibility, concentration risk, and emerging technologies for banking institutions. The IOSCO *Principles on outsourcing* (2021)[13] set out expectations for applicable regulated entities that outsource tasks, along with guidance for implementation. The document covers issues such as defining outsourcing, the assessing of materiality and criticality, affiliates, sub-outsourcing and outsourcing on a cross-border basis. The IOSCO principles may be used by some FMIs, though they are written to apply to a wider range of entities in securities markets. The IAIS *Application Paper on operational resilience objectives and toolkit* (2026)[14] is aimed at IAIS member insurers and covers the full breadth of operational resilience considerations. It discusses ICT third-party outsourcing and challenges around concentration of third-party service providers.

CPMI-IOSCO also drew from their Level 3 assessments on cyber resilience (L3 Cyber) and business continuity planning (L3 BCP) reviews. These reviews examined consistency in the outcomes of FMIs' implementation of the PFMI around cyber resilience (as informed by the CPMI-IOSCO *Guidance on cyber resilience for FMIs* (Cyber Guidance)) and business continuity planning. The Level 3 assessments identified observations relevant to third-party risk management and an issue of concern regarding a lack of testing coordination with critical third-party service providers and, in some cases, limited oversight of outsourced services.

[12] See BCBS, *Principles for the sound management of third-party risk,* December 2025, at www.bis.org/bcbs/publ/d605.htm.

[13] See IOSCO, *Principles on Outsourcing: Final Report,* October 2021, at www.iosco.org/library/pubdocs/pdf/IOSCOPD687.pdf.

[14] See IAIS, *Application Paper on operational resilience objectives and toolkit,* February 2026, at www.iais.org/2026/02/final-version-of-the-application-paper-on-operational-resilience-objectives-and-toolkit-published/.

2. Key challenges of FMIs' increased reliance on third-party service providers

FMIs are critical nodes in an increasingly interconnected and complex ecosystem which includes participants, linked FMIs, settlement banks, liquidity providers, third-party service providers, critical infrastructures, vendors, and vendor products.[15] As noted in the PFMI, "by performing centralised activities [...] FMIs concentrate risks and create interdependencies between and among FMIs and participating institutions." FMIs also operate in concentrated markets – the level of substitutability of FMIs' payment, clearing and settlement services is typically low. CPMI-IOSCO have identified several challenges to third-party risk management that are particularly important for FMIs given this interconnectedness and FMIs' role within the financial system, where risks may be amplified by the way that FMIs concentrate and conduct activity. These challenges are discussed further below. This discussion paper refers to the PFMI and other international standards, guidance and third-party risk management publications by standard-setting and other international bodies.

In the survey of CPMI-IOSCO member authorities, it was noted that use of third-party services is likely to increase as FMIs continue to transition towards cloud computing and consider the use of emerging technologies. Since the survey was conducted, there has been further attention on the use of technologies such as distributed ledger technology, quantum computing, and AI by standard-setting bodies. Such new technologies could heighten the challenges identified in this paper that could require proactive monitoring, including related to concentrated providers, greater interconnectedness through these technologies and exit planning and substitutability.

FMIs' increasingly interconnected and complex ecosystem, the corresponding cyber-related risk, and the concentration of third-party service providers can be characterised as structural factors which can pose challenges to FMIs' ability to effectively manage risk. Complex and opaque supply chains, difficulties with exit planning and imbalances in bargaining power may relate more to individual FMI and service provider relationships and may also make it more difficult for FMIs to effectively monitor and mitigate risks.

2.1 FMIs' increasingly interconnected and complex ecosystem

The increased reliance on third-party service providers is not unique to FMIs and widely used third-party service providers can themselves cascade risks across the financial system. However, the increased use of third-party service providers by FMIs can amplify an outage, given an FMI can transmit risk to its ecosystem. A significant outage at an FMI could affect public confidence or even pose risks to financial stability. It follows that it is important for FMIs to consider the risks to their ecosystem arising from their relationships, and the relationships of their participants, with third-party service providers.[16]

[15] Annex A in the CPMI-IOSCO Cyber Guidance defines ecosystem as "A system or group of interconnected elements, formed linkages and dependencies. For an FMI, this may include participants, linked FMIs, service providers, vendors and vendor products." Section 3.3 of the Cyber Guidance 3.3 describes the entities within an FMI's ecosystem as including "participants, linked FMIs, settlement banks, liquidity providers, service providers, critical infrastructures such as energy and telecommunications, vendors and vendor products".

[16] PFMI Principle 3, KC 3 states, "An FMI should regularly review the material risks it bears from and poses to other entities (such as other FMIs, settlement banks, liquidity providers, and service providers) as a result of interdependencies and develop appropriate risk management tools to address these risks." See also Principle 2, KC 7 and Principle 17, KC 7.

International publications highlight the importance and challenge of managing such risks. These may be relevant to considerations of how risk can arise from and be transmitted to an FMI's ecosystem. The PFMI also note that "Complex interdependencies may be a normal part of an FMI's structure or operations [...] Interdependencies, however, can also present an important source of systemic risk".[17] Further, the PFMI note "An FMI should identify, monitor, and manage the risks that key participants, other FMIs, and service and utility providers might pose to its operations."[18]

Responses to the survey of CPMI-IOSCO member authorities reinforced this theme. Authorities noted that increased interconnectedness through systemic dependencies creates pathways for risk to spread across the financial sector and that this is a prevalent risk in the current FMI operational risk landscape, supporting the need for third-party risk management. In the survey of FMIs, just under half of respondents reported explicitly considering their role in transmitting risk to the wider ecosystem as part of their risk assessment and risk management. However, in the FMI roundtable, some FMIs noted that they typically consider risks arising from their ecosystem through the lens of concentration of third-party service providers and supply chain opacity.

The FSB toolkit acknowledges that the extent and nature of financial institutions' interactions with a broad and diverse ecosystem of third-party service providers have evolved and become more complex. The FSB toolkit shares practices on managing systemic third-party dependencies, concentration risks, and interconnected critical services. It promotes holistic third-party risk management, helping financial institutions and authorities identify, monitor, and mitigate system-wide vulnerabilities arising from interconnected service provider ecosystems.

2.1.1 Cyber-related risks

Cybersecurity and data protection were the most cited operational risks in third-party relationships, both by participants in the FMI roundtable and by CPMI-IOSCO member authorities in survey responses. Although cyber risk can be considered a risk in its own right, it is also closely linked to risks arising from an FMI's ecosystem, in that cyber incidents can originate within the FMI's systems or from external sources, such as third-party service providers, and may directly or indirectly affect its operations. Third-party relationships can expose FMIs to risks and vulnerabilities as third-party service providers may be subject to "supply -chain attacks" where threat actors compromise weaker links in the supply chain to reach the target organisation through ICT interconnections. Due to the extensive and often global nature of supply chains, these cyber risks are further exacerbated by the complexity of monitoring supply chains, especially when services are delivered across borders and/or involve long and complex chains of providers. Challenges related to monitoring supply chains are discussed further in section 2.3.

FMIs have several means of monitoring and managing cyber risk, which vary depending on the third-party service provider and the FMIs' contract with that provider. For example, during the roundtable, FMIs stated that they have effective communication channels to ensure rapid and ongoing information-sharing during ICT incidents, including with other FMIs and supervisory authorities. The Cyber Guidance provides supplemental detail to the PFMI, with detail related to the preparations and measures that FMIs should undertake to enhance their cyber resilience capabilities with the objective of mitigating risks that cyber threats pose to financial stability. Principle 17 Key Consideration 7 and the Cyber Guidance stress the need to identify, monitor, and manage risks associated with external parties such as participants, other FMIs, and third-party service providers. The Cyber Guidance includes third-party service providers as part of the ecosystem of external parties that may pose risks to FMIs' operations. To help FMIs enhance their cyber resilience, CPMI-IOSCO have published *Cyber resilience*

[17] PFMI, section 2.3.

[18] PFMI, Principle17, Key consideration 7.

toolkit: practical considerations for FMIs. The toolkit comprises a set of voluntary, non-binding tools which contain practical considerations across four topics relevant to enhancing the cyber resilience of FMIs consistent with the PFMI: (i) governance of cyber risk and resilience; (ii) scenario identification and design; (iii) response, resumption and recovery plans; and (iv) testing and exercising.

The L3 Cyber review assessed FMIs' implementation of relevant PFMI Principles and was informed by the Cyber Guidance. The assessment found that a large majority of FMIs regularly review cyber risks arising from third party relationships. However, the L3 Cyber review also noted that some FMIs do not involve these external parties when testing their cyber response, resumption, and recovery plans or procedures. It also indicated that "A lack of testing coordination with external parties calls into question the overall comprehensiveness of an FMI's cyber resilience testing programme and, in particular, the ability to recover and resume operations following a cyber incident."

International publications address cyber risk in other parts of the financial sector. The IOSCO principles on outsourcing highlight that cyber vulnerabilities may arise through connections to unsecure vendors and the exploitation of information and communication platforms. Regulated entities should therefore take appropriate steps to ensure that third-party service providers have in place a comprehensive ICT security, cyber-resilience, disaster recovery and business continuity programme. The service provider should also have in place and maintain effective measures and protocols for cyber security and to protect against cyber incidents.

Principle 4 of the BCBS Principles[19] prescribes evaluating a third party's ICT security and cyber risk controls during onboarding, and Principle 5 (on contracting)[20] stipulates that contracts include security requirements and incident notification obligations for critical third-party service providers. Additionally, Principle 7 on monitoring[21] calls for ongoing monitoring of third-party service providers' risk and performance, and Principle 8 (on business continuity management)[22] requires firms and critical providers to test and maintain robust business continuity plans to ensure resilience against disruptions.

2.2 Concentration of third-party service providers

There can be benefits to having large or dominant third-party service providers, including economies of scale, which can lower the costs of bringing in expertise or specialist services. This market dynamic, however, can reduce the level of substitutability of the service provider or create risks from certain third-party service providers being used by many FMIs and financial sector firms, creating a single point of failure across a potentially significant portion of the financial sector.

Principle 5 of the IOSCO Principles on outsourcing states that a regulated entity should be aware of the risks posed and should manage them effectively, where it is dependent on a single service

19 Principle 4: "As part of the assessment of a TPSP's capacity and ability to deliver the services under the arrangement, banks should consider the TPSP's: operational and technical capability; […] effectiveness of internal controls and risk management, including its ability to manage information and communication technology, cyber and other operational risks;"

20 Principle 5: "Contractual provisions should facilitate effective risk management and oversight of the TPSPs and relevant services by the banks and specify the expectations and obligations of both the banks and TPSPs. Banks should negotiate a contract that meets their own business goals and risk management needs".

21 Principle 7: "Banks should, on an ongoing basis, assess and monitor the performance and changes in the risks and criticality of TPSP arrangements and report accordingly to board and senior management. Banks should respond to issues as appropriate."

22 Principle 8: "Banks should manage their dependencies on TPSP arrangements within their BCM processes. Banks' BCM processes should consider: development, periodic review and updating of the bank's internal BCPs and DRPs with respect to TPSP arrangements; periodic testing of the bank's BCPs and DRPs […]; lessons learned from incidents (if any) and result of the periodic testing; periodic updating of identified contingent providers."

provider for material or critical outsourced tasks or where it is aware that one service provider provides material or critical outsourcing services to multiple regulated entities including itself.

While concentration among third-party service providers is often common across the financial sector, this may be of particular concern for FMIs given their critical role in concentrating activity within the financial system, as discussed in section 2.1:[23]

a) **From the perspective of individual FMIs**: Risk arising from a dependency of an FMI (or, where relevant, on a group basis) on one or more services provided by a single third-party service provider (directly or indirectly through nth-parties) or a limited number of third-party service providers where the disruption or failure of such services has potential implications for the FMI's critical operations. Examples of situations in which concentration risk may arise include but are not limited to: (i) concentration of multiple services provided by the same service provider; (ii) concentration of services from one or multiple third-party service providers in a single geographic region; or (iii) multiple third-party service providers with a dependency on the same key nth party.

b) **From a systemic perspective**: Risk to the financial sector overall arising from a dependency of multiple FMIs or other financial institutions on one or more services provided by a single service provider or a limited number of third-party service providers

Interactions between these types of concentration, where an individual FMI is "locked in" to a relationship with a particular service provider because of the specific, unique services provided, as well as its large or dominant position in the market, are discussed in section 2.4.

2.2.1 Concentration of third-party service providers from the perspective of individual FMIs

In the FMI survey, FMIs were asked how they rated the materiality of risk, arising from both market concentration (ie, a limited number of third-party service providers in a given market for a particular service) and dependency on a single service provider for multiple services. Around three quarters of the respondents rated the risk from both types of concentration as either high or medium (on a scale of high, medium or low risk). Risk arising from market concentration is generally seen as more material by firms operating in two or more regions, while concentration by choice of provider is generally seen as more material by firms operating in only one jurisdiction. At the FMI roundtable, FMIs discussed incorporating practices to manage risk associated with concentration, and noted that reducing concentration needed to be weighed against the impact of increasing costs and administrative complexity, as every new service provider introduces new third-party risk.

If an FMI's ability and choice to move between third-party service providers is restricted as a practical matter, they may experience "vendor lock-in". Due to the lack of interoperability between providers or other practical constraints, they may be unable to switch to an alternative service provider when they want to exit the agreement (eg, once their contract ceases or in the case of unsatisfactory performance), or in the case of an outage or other stressed circumstances. The depth and breadth of the FMI's relationship with the third party may also increase the complexity and cost of switching providers at the end of a contract or bringing the provision of the service in-house. For example, one service provider could be providing multiple services such as cloud hosting and data analytics. This complexity may make it challenging to maintain backup systems or change third-party service providers in stressed circumstances or following an outage.

[23] This discussion paper considers two distinct types of concentration risk, drawing on a similar distinction made in BCBS report *Principles for the sound management of third-party risk*, 2025.

International publications highlight the importance and challenge of managing risks related to the concentration of the provision of services. Principle 5 of the IOSCO Principles on outsourcing states, "A regulated entity should be aware of the risks posed, and should manage them effectively, where it is dependent on a single service provider for material or critical outsourced tasks or where it is aware that one service provider provides material or critical outsourcing services to multiple regulated entities including itself."[24] The IOSCO Principles on outsourcing also highlight that effective due diligence enables firms to assess the extent of their reliance on individual providers and to consider mitigating actions, such as diversifying providers for different services to reduce dependencies and the risk of vendor lock in.

Services delivered through intra-group outsourcing[25] arrangements may be harder to exit or replace given that these are in-house rather than external. Analysis of the responses to the survey of CPMI-IOSCO member authorities suggests that most authorities do not have a specific policy for intra-group outsourcing arrangements but maintain similar risk management expectations as those for managing third-party risks that would arise from external providers. Section 2 of the FSB toolkit notes that, if intra-group services are not managed appropriately, they can pose risks to individual financial institutions within a group (eg, major subsidiaries) as well as to the broader financial group. The BCBS Principles similarly highlight that banks should not assume intra-group arrangements are inherently less risky than external third-party arrangements.[26]

2.2.2 Concentration of third-party service providers from a systemic perspective

Concentration of third-party service providers may have systemic implications when a single third party provides services to multiple FMIs. In such cases, an outage at that third-party service provider could have a systemic impact by disrupting the critical operations and services of multiple FMIs, potentially across different jurisdictions. For this reason, a number of authorities seek visibility into which service providers FMIs are using, given that individual FMIs are not able to gain this system-wide perspective. However, FMI supervisors may only be able to gather data limited to the FMI sector (compared with across the financial sector or broader economy) and within the jurisdiction (rather than globally).

2.3 Complexity and opacity of supply chains

FMIs' increasing use of third-party service providers can introduce supply-chain complexity, which can make identification and management of risks related to critical dependencies difficult and hinder resilience planning. FMIs may not have visibility into their third-party service providers' suppliers. During the FMI roundtable, a number of FMIs cited supply-chain visibility as a challenge. This was echoed in their responses to the survey, where approximately one-third of FMIs noted they only had visibility into third-party service providers across their supply chains. Other FMIs indicated they had visibility into

[24] IOSCO Principles on outsourcing, Principle 5, 2021, www.iosco.org/library/pubdocs/pdf/IOSCOPD687.pdf.

[25] For the purposes of this discussion paper, use of the term "outsourcing" is consistent with the definition provided in the FSB toolkit: "A category of third-party service relationships where a financial institution uses a service provider to perform, on a recurrent or an ongoing basis, services, or parts thereof, that would otherwise be undertaken, or could reasonably be undertaken, by the financial institution itself."

[26] The BCBS Principles note "Banks should not treat intragroup TPSP arrangements as if they are inherently less risky than other arrangements. Banks' risk management processes should be proportionate to the unique characteristics of intragroup arrangements (eg the bank's level of control and influence on the intragroup entity, complexities from cross-border operations and prioritisation of the bank's requirements) and the risks and criticality of the arrangements."

fourth-party service providers, but only a small portion had visibility beyond this. These limitations may obscure indirect dependencies and complicate risk management.

The lack of visibility is typically driven by data access challenges and complexity in how services and technologies are architected. In the FMI survey, a number of respondents identified that they had difficulty obtaining information relevant to enabling appropriate risk management from third-party service providers and their contractors. Third-party service providers may be unwilling or unable to share relevant information. As a result, FMIs face difficulties in identifying critical dependencies, assessing supply chain, concentration and related risks, and designing effective contingency measures.

During the service provider roundtable, participants – who in many cases are contractually required to disclose outsourcing – explained that they identify and monitor their own critical third parties (ie fourth parties for FMIs). Where any fourth-party incidents occur, third-party service providers monitor and communicate the impacts of those incidents to FMI clients. However, third-party service providers noted that visibility degrades quickly across the supply chain.

Authorities and FMIs stressed that effective supply chain management depends on supply-chain visibility and transparency. In terms of supervisory practices, some CPMI-IOSCO member authorities noted a number of expectations to help manage risk associated with complex supply chains. In survey responses, some authorities indicated that they rely on periodic surveys to understand FMIs' supply chains, while others use ongoing supervisory monitoring. Most data collection focuses on direct third-party service providers rather than nth-party service providers. Some authorities also noted that they do not have visibility into the critical providers of FMIs' critical providers. During the FMI roundtable, FMIs expressed interest in enhanced collaboration, such as through testing the whole-supply chain (including their participants) to help address these challenges.

International publications provide guidance and outline expectations for managing risk associated with the complexity and opacity of supply chains that are consistent with the points raised in the roundtable discussions. Explanatory note 3.17.20 of the PFMI states that a contractual relationship should be in place between the FMI and the critical service provider allowing the FMI and relevant authorities to have full access to necessary information. It also states "The contract should ensure that the FMI's approval is mandatory before the critical service provider can itself outsource material elements of the service provided to the FMI, and that in the event of such an arrangement, full access to the necessary information is preserved. Clear lines of communication should be established between the outsourcing FMI and the critical service provider to facilitate the flow of functions and information between parties in both ordinary and exceptional circumstances."

The FSB toolkit provides tools for managing supply chain related risks that FMIs may find relevant. Specifically, section 3.5 emphasises that financial institutions should identify and manage risks arising from third-party service providers' supply chains, including nth-party dependencies. It highlights the need for mapping supply-chain structures, performing ongoing due diligence and monitoring, ensuring visibility into third-party service providers' outsourcing arrangements, and requiring third-party service providers to maintain resilient supply chain controls. The FSB toolkit frames this as part of lifecycle risk management aimed at reducing vulnerabilities created by multi-layered dependencies. In addition, section 3.5 in the FSB toolkit provides tools that FMIs might leverage to manage risks arising in a service provider's supply chain, such as ensuring visibility into third-party service providers' key nth-party service providers.

Principle 4 (on due diligence) of the BCBS Principles[27] correspondingly advises firms to assess a service provider's ability to manage its own critical sub-contractors, and Principle 5[28] calls for contractual clauses to ensure banks (and competent authorities) retain visibility into and rights over any material sub-outsourcing by a critical service provider.

2.4 Difficulties with exit planning

Another theme that emerged from engagement with FMIs and third-party service providers was exit planning, including strategies to exit a relationship with a third-party service provider. FMIs mitigate challenges with exit planning in a number of ways. In the survey of FMIs, around two-thirds of the firms noted that they use exit planning as a way to maintain their ability to substitute third-party service providers. FMIs can build clauses into their contracts with third-party service providers to allow them to exit the relationship in the event that the third party does not meet certain contractual obligations, both under business-as-usual and crisis scenarios.[29]

Although exit planning is considered a mitigant to risks such as vendor lock-in, or as a business continuity planning tool, exit planning itself poses challenges to FMIs.[30] Under certain stressed scenarios, exiting a third-party service provider relationship may not be realistic. For example, an FMI may not be able to easily and quickly move from one service provider to another if the third-party service providers' systems have different architecture: to move providers would involve time- and resource-intensive efforts to change the architecture of the FMI's systems for the new provider, therefore disincentivising the move. Instead, the FMI may need to consider other operational resilience options. Additionally, the feasibility of exiting a service provider relationship may vary depending on the type and criticality of the service(s) provided.

Most respondents to the survey of CPMI-IOSCO member authorities reported that they do not have specific policy or regulatory, supervisory or oversight requirements around exit plans for FMIs. A few respondents distinguished between exit plans in stressed scenarios and those under business-as-usual circumstances. Some respondents noted a requirement to plan for bringing services in-house or transferring to a new provider if a service provider became unavailable.

During the roundtable with third-party service providers, attendees also discussed their engagement with FMI clients on business continuity planning and exit planning. They noted that their exit planning for FMI clients typically focuses on scenarios such as loss of a region or service, rather than full disengagement or exit from the service provider. These strategies are considered to be more realistic, given it is unlikely that an FMI would completely "switch off" all services from a service provider (which typically offers a variety of services), especially during an ongoing incident or outage. Third-party service providers noted that they are working to make their services more portable through multi-cloud and data transfer tools and recognised that FMIs must be able to exit services without disruption or

[27] Principle 4: "As part of the assessment of a TPSP's capacity and ability to deliver the services under the arrangement, banks should consider the TPSP's: […] ability to manage supply chain risks (eg identification of key Nth parties, providing relevant information to the bank when requested)"

[28] Principle 5: "Banks' contracts governing critical TPSP arrangements should include […] those listed below: conditions governing key nth parties (eg prior notification of use or change, and incident reporting); […] rights for banks to receive accurate, comprehensive and timely information […]; rights of banks to access, audit and obtain relevant information from key nth parties"

[29] In the survey of FMIs, almost all FMIs reported that they adopt pre-contract due diligence.

[30] For the purposes of this discussion paper, use of the term "exit planning" is consistent with the definition in the FSB toolkit, p 27: "identifying, documenting and, to the extent possible, testing exit strategies for their third-party service relationships involving critical services. Exit strategies can cover a range of scenarios, including normal and planned migrations of services and service providers but also adverse events,".

regulatory, supervisory or oversight non-compliance. However, third-party service providers also cautioned that it may not be realistic to immediately exit a service provider relationship in times of stress. As some third-party service providers adopt more portable technology solutions compatible with different vendors, FMIs may be better able to expand their exit strategies.

International publications highlight exit planning as a challenge that many financial sector firms face. Explanatory note 3.17.20 of the PFMI states "An FMI that relies upon or outsources some of its operations to another FMI or a third-party service provider (for example, data processing and information systems management) should ensure that those operations meet the same requirements they would need to meet if they were provided internally. The FMI should have robust arrangements for the selection and substitution of such providers, timely access to all necessary information, and the proper controls and monitoring tools."

Other international publications provide more specific suggestions for exit planning that may be relevant to FMIs. In terms of potential measures to manage this risk, the FSB toolkit discusses exit strategies to mitigate vendor lock-in, including contractual arrangements that allow for transition planning and service continuity. The FSB toolkit notes that "there is no one-size-fits-all approach to exit planning" and that "the feasibility of an exit plan may depend on the circumstances of the financial institution, the relevant critical service and the service provider". Finally, the FSB toolkit notes, "Business continuity plans should be distinguished from exit plans […] which are a distinct process with [a] different objective. However, some business continuity plans may include an exit from the third-party service relationship where feasible, practicable and usually as a measure of last resort."[31]

Similarly, Principle 9 (on termination) of the BCBS Principles provides for the design of exit approaches for both planned and unplanned scenarios.[32] It suggests that exit plans should be regularly updated where relevant and tested from both a technical and non-technical standpoint (eg availability of budget, human resources, technical infrastructure, transfer of knowledge, access to data).

2.5 Imbalance of bargaining power

FMIs participating in the FMI roundtable indicated that an overarching issue related to FMIs' relationships with third-party service providers is an imbalance of bargaining power to ensure contractual arrangements meet the expectations of FMIs' regulators, supervisors and overseers. This bargaining power imbalance may be the result of several factors, including concentration of providers which can leave FMIs with limited choices. FMIs – despite their systemic importance – may be relatively small customers from a revenue perspective. It was noted in the FMI roundtable that, beyond explicit contractual constraints, the enforcement of contractual arrangements was difficult, particularly with larger third-party service providers.

This imbalance of bargaining power may present an obstacle to FMIs securing and enforcing contractual arrangements that allow them to adequately identify, manage and monitor risks related to third-party service providers. In particular, this may affect FMIs' ability to secure contractual provisions such as a right to audit; information-sharing provisions, especially when material incidents occur; access to testing with the service provider; and the right to set service-level expectations that can be used to manage the relationship, enforce expectations, and as a benchmark to exit the contract if the service provider is not meeting those expectations.

One contractual provision that has consistently been identified as a challenge is inclusion of third-party service providers in FMIs' business continuity planning. The L3 Cyber review found that most

[31] FSB toolkit, pp 25, 27-28.

[32] BCBS (2025), Principle 9: "Banks should maintain exit plans for planned termination and exit strategies for unplanned termination of TPSP arrangements."

FMIs did not include critical third-party service providers in the testing of their response, resumption, and recovery plans and processes with respect to cyber incidents. At the FMI roundtable, FMIs noted that they have an interest in being able to undertake testing with third-party service providers and participants. Conversely, in the service provider roundtable, third-party service providers challenged the value and practicality of participating in testing with all of their clients given the scale of operations.

Imbalance in bargaining power is not explicitly mentioned in the PFMI, CPMI-IOSCO guidance, or guidance from the FSB and other standard setting bodies, but each contains expectations or examples of what the contractual relationship should deliver. Explanatory note 3.17.20 to the PFMI states that "A contractual relationship should be in place between the FMI and the critical service provider allowing the FMI and relevant authorities to have full access to necessary information".

The FSB toolkit also underscores the need for robust contractual arrangements in third-party relationships, including clear service level agreements, performance expectations and incident-reporting obligations. It emphasises ensuring rights to audit, oversee and access information, alongside visibility of sub-contractors and nth-party dependencies. The FSB toolkit also highlights the importance of testing operational resilience and business-continuity capabilities, as part of life cycle management of third-party risks, to validate providers' ability to support critical services.

Similarly, Principle 5 (on contracting) of the BCBS Principles states that financial institutions contracts with third-party service providers should consider rights to access, audit and obtain information for their critical third-party arrangements, reinforcing the importance of these provisions even when bargaining power is uneven.[33]

2.6 Variation in regulatory, supervisory and oversight expectations

The survey of CPMI-IOSCO member authorities indicated that expectations and oversight practices in relation to FMIs' management of third-party risk have some clear elements of commonality but also points of divergence. This may make it more complex for FMIs operating across jurisdictions to design their third-party risk management frameworks in a way that meets all regulatory, supervisory and oversight expectations.

CPMI-IOSCO members implement the PFMI as applicable within their jurisdictions. As noted in the introduction to the PFMI (1.19), "With a few exceptions, the principles do not prescribe a specific tool or arrangement to achieve their requirements and allow for different means to satisfy a particular principle…In addition, authorities have the flexibility to consider imposing higher requirements for FMIs in their jurisdiction either on the basis of specific risks posed by an FMI or as a general policy." Implementation may reasonably vary across jurisdictions for a number of reasons, including to reflect national and regulatory frameworks and regulators' legal authority. Some variation is therefore to be expected but nonetheless can pose challenges for FMIs who operate across borders.

Examples of variation include:

- **Definitions and scope of third-party risks and arrangements.** For instance, some jurisdictions focus only on outsourcing, while others include broader arrangements such as third-party relationships, intra-group arrangements and sub-contractors. Varying and evolving expectations from different supervisors and jurisdictions were noted as a challenge by participants during FMI industry engagement. For example, most jurisdictions differentiate the level of importance of third-party service providers by using designations such as "critical"

[33] Principle 5: "Banks' contracts governing TPSP arrangements should consider: […] rights of banks to access (including premises), audit and obtain relevant information from the TPSPs".

"essential" or "integral" when referring to the services they may provide. These designations may be made by the FMI rather than the regulatory, supervisory or oversight authority.

- **Data collection practices across jurisdictions.** These can vary in terms of frequency, scope, and methodology. Some jurisdictions rely on periodic or ad hoc surveys, while others integrate data gathering into ongoing supervisory activities. Moreover, although some frameworks aim to capture full supply chain dependencies, most jurisdictions focus only on third-party service providers. Effective data collection can be helpful for authorities to monitor FMIs' exposure to third-party risks, to the extent that domestic frameworks permit this. Data collection may help to identify operational vulnerabilities and support sector-wide analysis, including comparisons across entities and aggregation of information on key third-party service providers.

Some participants at the service provider roundtable noted that to address the regulatory variation and compliance needs of FMIs, they generally look to standardise contracts where possible, to meet all relevant jurisdictional requirements and to avoid having variation in agreements across entities and jurisdictions. When negotiating adjustments to one contract, they look to roll this change out widely. Some third-party service providers have a "financial services addendum" and noted that greater consistency of reporting requirements and risk management expectations (even at a broader level) across jurisdictions and types of financial institution would simplify their contracting approach.

3. Conclusion

While relevant to all financial entities to varying degrees, the challenges discussed in this paper have been identified as particularly important for FMIs' effective service provider risk management. FMIs serve as critical nodes within the network of the financial system. This unique degree of interconnectedness and the fact that they themselves may be a point of concentration in markets means disruptions to FMIs could cascade or amplify risks throughout the system.

FMIs may also depend on a small number of third-party service providers that support critical services. The concentration of services and functions in a small number of third-party service providers, whether by individual FMIs or at a system-wide level, may also act as an amplifier of risks. This concentration may increase as FMIs continue to transition towards cloud computing and other emerging technologies if there is concentration within service providers.

FMIs' growing use of third-party service providers has increased the interconnectivity and complexity of their supply chains, which makes supply chain visibility both more challenging and more important. Industry engagement indicates that only a small portion of FMIs have visibility beyond their fourth-party service providers. This has implications for their cyber resilience, particularly in scenarios where threat actors seek to compromise weak links in the supply chain. The difficulty of managing complex supply chains may be exacerbated by the cross-border nature of service provider services. This means that FMIs may be subject to varying regulatory, supervisory and oversight requirements across jurisdictions for managing their service provider risk, albeit some of this may be unavoidable due to national frameworks, mandates and powers.

FMIs also face challenges to their effective management of service provider risks when entering and exiting contracts. An imbalance of bargaining power, potentially owing to risk related to concentration of third-party service providers and the relative importance of the FMI as a service provider's client, may hinder FMIs' ability to secure customised contractual terms to meet certain service, information, or other needs. In addition, while exit planning is a useful tool to mitigate third-party risk, terminating an agreement with a service provider may not always be feasible in stressed scenarios, and may depend on the criticality of the service provided.

4. Discussion Questions

CPMI-IOSCO is seeking feedback from FMIs, their participants, third-party service providers, and other stakeholders on whether this paper accurately and comprehensively reflects FMIs' risk management challenges with respect to third-party service provision; and whether and how CPMI-IOSCO may help to address these challenges. Detailed questions are provided below.

Responses to the questions should be sent via email to the Secretariats of the CPMI and IOSCO (cpmi@bis.org; cpmi-iosco@iosco.org) by 1 December 2026. 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.

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?

Annex 1 Summary of industry input

FMI survey and roundtable

In May 2025, CPMI-IOSCO were joined by panellists from 12 international FMIs for a roundtable conversation focusing on how FMIs experience and evaluate the materiality of third-party risks.

Ahead of the roundtable, CPMI-IOSCO shared a preparatory survey with participants to get an initial sense of how FMIs perceive certain risks. The roundtable with the FMIs and the preparatory survey indicated wide usage of third-party service providers and a general view that the establishment and management of their third-party relationships is in line with PFMI Principle 17 and Annex F and the CPMI-IOSCO cyber guidance. The FMIs highlighted that their expectations on intragroup arrangements are the same as for other external outsourcing arrangements, and that they hold their group entities to the same standards.

Nearly all of the FMIs surveyed conduct pre-contract due diligence. A large number of firms also highlighted a proportionate approach to ongoing risk management, depending on the criticality of the third-party service provided.

It was noted that the "right to audit" clause in the contract can be difficult to enforce. In addition, certain FMIs highlighted having limited to no negotiation power and noted that they often receive pre-set contracts from the third-party service providers.

The survey found that approximately three quarters of the respondents consider both market concentration (due to a small number of providers in the market) and "concentration by choice of provider" (ie the choice to use a single provider which could lead to vendor lock-in/ contractual constraints) pose either medium or high risk. However, there are slight differences in perceptions depending on the size of FMIs. Market concentration is generally seen as posing more material risk by larger firms operating in two or more regions; concentration by choice of provider is generally seen as posing more material risk by smaller firms operating in only one jurisdiction.

The majority of the survey respondents indicated that they have visibility of their fourth party service providers, though only a few FMIs answered that their visibility extends beyond this. This visibility, however, does not necessarily translate into the ability to risk manage. During the roundtable, FMIs indicated that obtaining clarity on interdependencies and monitoring lower tier third-party service providers can be challenging and made more complex by the level of skill and understanding needed and the lack of data quality and transparency. FMIs also asked for greater collaboration at the industry level to better understand interconnectedness: limited visibility hinders the ability to design effective contingency measures.

Participants highlighted a lack of regulatory, supervisory or oversight streamlining as there are varying and evolving expectations from different regulators, supervisors and overseers across jurisdictions. Participants noted that a concentration assessment scope should be carried out not only at the FMI level but also at the ecosystem level. Participants also noted that concentration risks seem difficult to avoid not only for FMIs but also for the financial sector as a whole, due to the market structure and market dominance for certain services (eg cloud services).

Participants indicated that FMIs themselves can be treated as third-party service providers by other members of the financial sector, which creates regulatory, supervisory and oversight burden as a regulated firm and as a third party.

Third-party roundtable

Members of CPMI-IOSCO were joined by 11 third-party firms who offer services such as cloud computing, messaging, and other ICT services, for a virtual roundtable in September 2025. The roundtable explored how third-party service providers manage their operational risk and resilience and how they approach their relationships with FMIs.

Third-party service providers noted operational resilience as central to their offering. A number of third-party service providers indicated their understanding of the critical role of FMIs and accordingly their willingness to tailor contracts to suit the requirements of FMIs and the financial sector. Some third-party service providers noted having a "financial services addendum" for their contracts, but it was not clear how widely this applied to FMIs or how many third-party service providers offer it. They noted their increasing willingness to provide access for audit purposes to financial sector firms. They recognised the need to meet regulatory, supervisory and oversight requirements across financial sectors and jurisdictions, although they noted that this causes some fragmentation, so they welcomed harmonisation in requirements across jurisdictions.

Some third-party service providers indicated they have technical and account managers to ensure good communication with customers, including on changes and outages, and that they undertake testing ahead of changes. They also noted their engagement with their own third parties (FMIs' fourth parties) but did not indicate much visibility beyond this. On business continuity testing, third-party service providers cautioned against wide-scale testing given the need to tailor to FMIs' individual circumstances.

On exit planning, third-party service providers challenged the practicality of FMIs fully exiting a third-party relationship given the range of services provided. The third-party service providers noted that, in the case of an incident, their geographical diversity would typically not lead to a blanket outage. Providers also expressed scepticism about the effectiveness of lengthy exit plans, with some suggesting that such documents can be impractical in real-world scenarios. Some third-party service providers did note their work to improve and support portability of data at the end of the contract.