King Yew Choo

London
kingyewchoo.co.uk

CPMI Secretariat and IOSCO Secretariat
By email to cpmi@bis.org and cpmi-iosco@iosco.org

2 November 2026

CPMI-IOSCO DISCUSSION PAPER, SEPTEMBER 2026 · THIRD-PARTY SERVICE PROVIDERS

Information an FMI can use in an incident

Response to questions 1, 2 and 5, on information access and contractual enforceability

Respondent	King Yew Choo, London, United Kingdom
Capacity	Personal capacity
Interest	Founder, True Primary; declared at paragraph 15
Contact	Contact details are in the covering email, and at kingyewchoo.co.uk
Publication	No part is confidential. It may be published in full, with my name.
Questions	1, 2 and 5, from the questions for all stakeholders
Structure	Numbered paragraphs 1 to 15, with a summary above and references below

WHAT I PROPOSE

1. **Test that the information right works.** The PFMI already call for timely access to all necessary information. A review of each critical contract should check three things separately: the right, the provider's ability to deliver the records, and the FMI's ability to use them before its decision falls due (paragraphs 1 to 3).
2. **A service-specific information schedule.** For each critical service, the FMI and its provider agree which records are needed, who holds them, their form and route, and three deadlines: acknowledgement, first usable records and a full account (paragraphs 4 and 5).
3. **Retrieval drills.** Exercises test retrieval through the agreed route, through subcontractors and while the provider's normal support channel is unavailable. A shared exercise can stand in for one per client where it tests the same service and deadlines (paragraphs 7 and 8).
4. **Four further contract terms.** Preservation of records on notice of an incident; delivery that continues through a fee or liability dispute; access duties that can be enforced down the subcontracting chain; and access that survives termination and the provider's insolvency (paragraphs 11 to 14).

Question 1: accuracy and completeness

Question 1 asks whether the challenges are accurate and comprehensive, and what is missing or incomplete.

1 I agree with the paper's analysis of the six challenges. The discussion of information access is incomplete. Section 2.5 lists, among the provisions FMIs find hard to secure, "information-sharing provisions, especially when material incidents occur".[1] It also records that "the enforcement of contractual arrangements was difficult, particularly with larger third-party service providers". Three things need to be kept apart: a right written into a contract, the provider's ability to deliver the information, and the FMI's ability to use it before an operational decision falls due. A contract review should examine each of them, and a retrieval exercise is the evidence for the second and third.

2 The existing standard provides the starting point. Explanatory note 3.17.20 of the PFMI asks for "timely access to all necessary information" and a contract allowing the FMI and relevant authorities "to have full access to necessary information".[2] Where a critical provider outsources material elements, the contract should ensure that "full access to the necessary information is preserved", with lines of communication that work "in both ordinary and exceptional circumstances". I propose specifying the evidence that shows those rights can be exercised. The FMI should identify the record holder, the contractual route to that holder and the means of obtaining an intelligible copy. It should then test that route under disruption. The schedule, deadlines and drills proposed below are practices an FMI can adopt under the PFMI as they stand.

3 Consider a hypothetical payment system that uses an external messaging service, a type of service offered by firms at the paper's provider roundtable.[1] After an interruption, a participant and the system hold different accounts of whether an instruction was delivered. A service-availability report does not settle that question. The agreed record should identify the instruction, its receipt time, delivery status, acknowledgement and any retry. The test should establish whether these records can be reconciled with the system's own records before it decides how to resume processing. The list fits this service; other services need their own.

Question 2: possible solutions

Question 2 asks, for each challenge identified (and any others considered relevant), what the possible solutions are.

4 **Information access (sections 2.3 and 2.5).** I propose a service-specific information schedule agreed between the FMI and its provider. For each critical service, it should name the records needed for incident assessment, reconciliation and transfer, who holds them and who can request them. It should specify their format, time references, identifiers, retention period and delivery route. Access for relevant authorities should be addressed expressly. Each record requested should serve an identified risk-management purpose, with controls on access and onward disclosure.

5 The schedule should set separate deadlines for acknowledging a request, supplying the first usable records and completing the full account of the incident. The FMI should derive these deadlines from the decisions it must make to continue or resume its critical services. Principle 17 expects critical IT systems to "resume operations within two hours following disruptive events". The Cyber Guidance asks FMIs to "exercise judgment in effecting resumption so that risks to itself or its ecosystem do not thereby escalate".[3] The FMI should identify which provider records that judgement needs inside the two hours, and hold its own copy of any it cannot rely on receiving in time (paragraph 9). The full account of the incident can follow later. The deadlines should be agreed before the service starts, checked after material changes, and tested while the provider's normal support channel is unavailable. The test should record missing fields and discrepancies as failures to correct.

6 **Interconnectedness and systemic concentration (sections 2.1 and 2.2.2).** The paper notes that "individual FMIs are not able to gain this system-wide perspective". To expose shared dependencies, each FMI should record the legal entity supplying each critical component and its role in the service. Section 3.4 of the FSB toolkit suggests identifying each provider by a unique identifier such as its Legal Entity Identifier; the same practice fits here.[4] The FMI should check whether two direct suppliers depend on the same subcontractor. It should supply this information to its relevant authorities through agreed confidential channels. Authorities can then match submissions within their own jurisdiction. Matching across jurisdictions depends on the cooperation "both domestically and internationally" that Responsibility E of the PFMI calls for, and on legal gateways for sharing the data. A common identifier lets authorities match records once those gateways exist.

7 **Opaque supply chains (section 2.3).** The direct provider should be responsible for obtaining the agreed records from its subcontractors. Before accepting a material subcontracting change, the FMI should see evidence that the information route works. A refusal or legal restriction should be documented, with the affected service and its practical consequence. If the information cannot be obtained, the FMI should record the resulting limitation and its mitigation. The inventory should mark each access route that has not yet been tested.

8 **Testing with providers (sections 2.1.1 and 2.5).** Joint exercises should concentrate on evidence retrieval and the hand-offs between firms. Section 2.5 records that providers "challenged the value and practicality of participating in testing with all of their clients given the scale of operations". A shared exercise or independent assurance should count where the FMI judges that it tests the relevant service, access route and deadlines. The FMI should receive the results and test any gaps specific to its configuration. The exercise should also check how the provider handles simultaneous requests from several affected FMIs, which tests its capacity during a common outage.

9 **Concentration and exit (sections 2.2.1 and 2.4).** Providers told the roundtable that exit planning for FMI clients "typically focuses on scenarios such as loss of a region or service". For those scenarios, the FMI should keep a tested copy of the minimum records needed for continuity outside the affected service, where lawful, technically practicable and proportionate to the service's criticality. The copy should have a stated update interval and recovery procedure. Planned transfer should include a test that a replacement provider or the FMI can interpret the exported records. Whether the service itself can be replaced, including capacity, dependencies and the time required, is a separate assessment.

10 **Bargaining power and regulatory variation (sections 2.5 and 2.6).** Some providers already offer a "financial services addendum" and roll negotiated changes out widely. The information schedule should be reusable and fit such an addendum, with a service annex and a jurisdiction annex. It should state the common evidence requirements and identify local restrictions, responsible entities and routes for authorities to obtain records. Unresolved terms should go to the FMI's responsible decision-maker before renewal, with their operational consequences recorded. Where a provider offers only pre-set terms, as some FMIs reported, the FMI should record the gap and raise it with its relevant authority in ordinary oversight, so that a refusal repeated across several FMIs becomes visible to authorities. A common form makes differences visible; legal review must still establish whether each arrangement works under the applicable law.

Question 5: further contractual aspects

Question 5 asks whether any contractual aspects, in addition to those addressed in the paper, are particularly relevant or challenging in the context of FMI third-party risk management.

11 The paper, with the BCBS and FSB provisions it cites, already covers rights to access, audit and obtain information, including from key nth parties, and exit planning. The BCBS Principles also cover data transfer and audit trails at termination.[5] Four further terms govern how the information right in paragraph 2 holds up under stress. First, the contract should require preservation of the agreed records once an incident or investigation is notified. It should specify the ordinary retention period by record type, who can trigger a preservation request, and when preservation ends. Preservation should keep the relevant version, its time reference and any corrections, with safeguards against alteration and unnecessary disclosure.

12 Second, the contract should separate an urgent request for records from any later allocation of responsibility for the incident. Delivery should continue during a fee or liability dispute, subject to applicable law. Agreed charges, and any limits on them, should be settled in advance. The contract should name an operational escalation contact and a senior contact, each with a response deadline. It should state the consequences of a missed delivery and preserve the FMI's ability to seek available remedies. Service credits alone leave the immediate need for information unmet.

13 Third, the direct provider's obligation should extend to the necessary subcontractor arrangements. Legal review should establish which entity owes each duty, who can enforce it, and where. Where the FMI needs direct access to a subcontractor, the arrangement should secure that access expressly. A promise by the direct provider is insufficient evidence that the subcontractor has agreed to cooperate. Confidentiality provisions should name the permitted recipients and secure disclosure routes for the FMI and relevant authorities, within applicable legal powers and restrictions.

14 Fourth, preservation, access and assistance obligations should run for a stated period after termination. Before deleting records, the provider should deliver the agreed export and allow the FMI to check that it is complete and usable. Legal review should examine the effect of the provider's insolvency, conflicting disclosure obligations and limits on remedies. Where those conditions put access at risk, the FMI needs an operational safeguard, such as the separate copy in paragraph 9. The FMI should test that safeguard without depending on the departing provider's ordinary support service.

Capacity and interest

15 I respond in a personal capacity. I founded True Primary, which builds infrastructure for the agent-initiated purchase of expert work, and declare its commercial interest in the safe adoption of agentic payments.

King Yew Choo

London, United Kingdom

REFERENCES

Web addresses were accessed on 2 November 2026.

1. CPMI-IOSCO, FMIs' reliance on third-party service providers: challenges and risks, discussion paper, September 2026, section 2.1, page 6; section 2.2.2, page 10; section 2.4, page 12; section 2.5, pages 13 and 14; section 2.6, page 15; Annex 1, pages 17 and 18. https://www.bis.org/publications/cpmi-iosco-fmis-reliance-third-party-service-providers-challenges-and-risks.pdf
2. CPSS-IOSCO, Principles for financial market infrastructures, April 2012: Responsibility E, page 4; Principle 17, key consideration 6, page 94; explanatory note 3.17.20, page 99. https://www.bis.org/cpmi/publ/d101.htm
3. CPMI-IOSCO, Guidance on cyber resilience for financial market infrastructures, June 2016, paragraph 6.2.2, page 16. https://www.bis.org/cpmi/publ/d146.htm
4. FSB, Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities, 4 December 2023, section 3.4, page 21. https://www.fsb.org/uploads/P041223-1.pdf
5. BCBS, Principles for the sound management of third-party risk, December 2025, paragraphs 63 and 64, page 17. https://www.bis.org/bcbs/publ/d605.htm