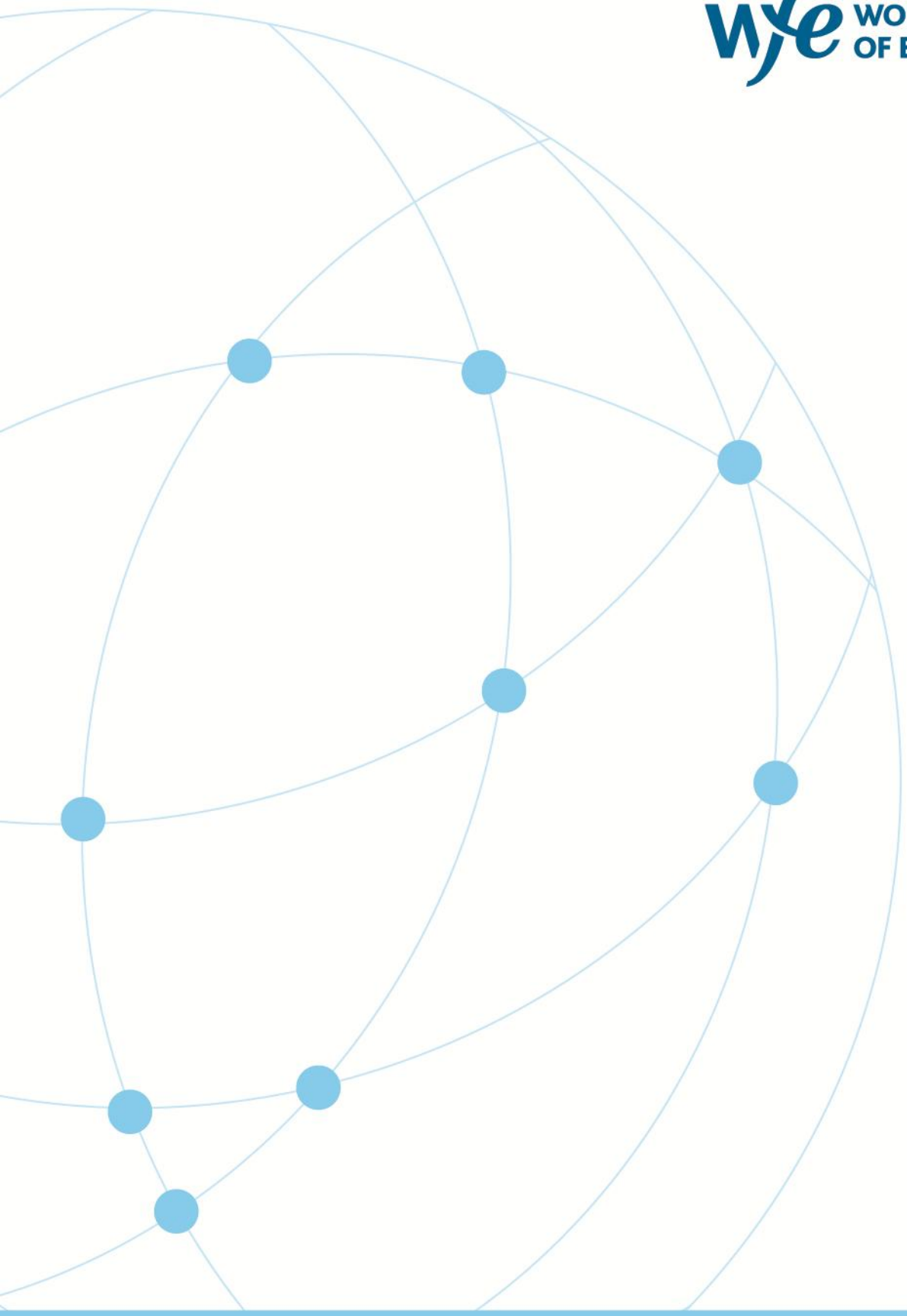
WORLD FEDERATION OF EXCHANGES



WFE Position on Third-Party Risk Management (TPRM)

November 2026

Summary

This paper sets out the WFE's position on third-party risk management (TPRM), informed by a meeting with IMF staff and member input through the Enterprise Risk Working Group. Its purpose is to provide a clear, practical and proportionate perspective on how exchanges, CCPs and other financial market infrastructures identify, assess and manage third-party dependencies in an increasingly digital and interconnected operating environment. The WFE position highlights the growing importance of third-party resilience for market integrity and continuity, while emphasising a risk-based approach to critical services, enterprise-wide risk assessment, proportionality, nth-party dependencies, concentration risk, regulatory fragmentation, information asymmetry and the operational challenges associated with oversight of major cloud, technology and service providers. Overall, the paper supports internationally coordinated, principles-based frameworks that strengthen resilience without creating unnecessary duplication, prescriptive requirements or disproportionate burdens for MIs.

WFE Position on Third-Party Risk Management (TPRM)

This paper presents the WFE's position on third-party risk management (TPRM), which was initiated after members of the Enterprise Risk Working Group (ERWG) had good discussions with IMF staff.

Drawing on members' contributions, the WFE prepared a position paper on some of the key questions discussed. The paper was subsequently presented to, discussed with and endorsed by the ERWG, and reflects the practical experience of WFE members in managing TPRM within operational resilience and enterprise risk frameworks.

Key Questions

i. **Whether your members are placing greater importance on third parties, and the reasons behind this?**

ii. **How they understand the third-party landscape, and how this is incorporated into enterprise-wide risk assessments?**

iii. **How is proportionality applied throughout the process?**

iv. **How are 4th, 5th, and nth party risks addressed?**

v. **How is concentration risk in service provision managed?**

vi. **What challenges they face in managing third-party risks?**

(i) Whether WFE members are giving higher importance to third parties, and what are some of the reasons?

Yes. WFE members are placing greater emphasis on third-party risk management due to the increasing reliance of exchanges, CCPs, and other Market Infrastructures (MIs) on external technology and service providers.

For MIs, third-party resilience has particular significance because it is closely connected to market integrity and the orderly functioning of financial markets. Given the role of trading venues and CCPs in trading, clearing, settlement, and risk management, disruptions to critical third parties may have consequences that extend beyond individual firms.

Key drivers include:

- Increased dependence on cloud service providers and digital infrastructure;

- Interconnectedness across financial ecosystems regarding service providers;
- Increased outsourcing of certain operational functions;
- Growing regulatory expectations relating to operational resilience and outsourcing oversight;
- Heightened awareness of concentration risk among major technology providers;
- The continued importance of maintaining market integrity, availability, and continuity of critical market services.
- Rapid proliferation of third-party AI offerings, including frontier models.

(ii) How do they understand the third-party landscape? And how do they consider this as part of enterprise-wide risk assessment?

WFE members generally adopt a risk-based and enterprise-wide approach to understanding third-party dependencies.

This typically includes:

- Mapping critical services and operational dependencies;
- Identifying providers and maintaining an inventory of those supporting critical business services and market operations;
- Assessing the criticality and substitutability of providers;
- Evaluating cyber, operational, legal, geopolitical, and concentration risks;
- Conducting scenario testing against severe but plausible disruption scenarios;
- Conducting due diligence and ongoing monitoring throughout the vendor lifecycle.
- Integrating third-party risk into broader operational resilience, cyber resilience, business continuity, and enterprise risk management frameworks.

Third-party risks are not viewed in isolation. Instead, they are increasingly incorporated into holistic enterprise-wide risk assessments alongside:

- Technology risk,
- Operational risk,
- System-wide risk,
- Business continuity risk,
- Reputational risk,

- Legal and regulatory compliance risk,
- Financial risk,
- and cyber risk.

(iii) How is proportionality applied in the whole process?

The WFE consistently supports a proportionate and principles-based approach to TPRM.

In the case of MIs, proportionality also reflect third parties' overall importance and the potential downstream effects of disruption on clients, and broader market functioning.

Proportionality is typically applied based on factors such as:

- Criticality of the outsourced service;
- Potential system-wide impact of disruption;
- Degree of substitutability;
- Sensitivity of data involved;
- Connectivity to critical market functions;
- Size and complexity of the institution;
- Nature of the service provider relationship.

Higher-risk or critical providers are generally subject to:

- Enhanced due diligence,
- More frequent monitoring,
- Resilience testing,
- Incident escalation requirements,
- and Stronger exit planning.

The WFE has also consistently emphasised that regulatory frameworks should avoid one-size-fits-all obligations and should recognise the differing risk profiles of institutions and services.

(iv) What are ways in which 4th, 5th, and nth parties are addressed?

WFE members increasingly recognise the importance of subcontracting chains and "nth-party" dependencies, particularly in cloud and technology ecosystems.

Approaches may include:

- Requiring disclosure of material subcontractors in contractual arrangements;
- Seeking transparency regarding critical downstream dependencies;
- Including audit, notification, and incident reporting clauses covering subcontractors;
- Assessing concentration and system-wide dependencies across supply chains;
- Conducting scenario analysis and resilience testing involving key subcontractors;
- Reviewing providers' own vendor risk management frameworks.

Third parties remain liable for the provision of services under contractual agreements, regardless of the use of sub-contractors. Therefore, MIs can enforce contractual provisions that hold the direct third party fully accountable for the performance and security failures of its subcontractors helps ensure that responsibility is not diluted across the supply chain. However, securing such provisions can be challenging in practice where firms may have limited negotiating leverage. Greater regulatory recognition of the principle of direct third-party accountability would help reinforce these discussions and support MIs in obtaining appropriate contractual protections.

In relation to critical providers, firms would typically seek greater assurance over material subcontractors and aim to ensure appropriate flow-down of resilience, audit, and incident management obligations through the subcontracting chain.

However, although firms would typically seek appropriate visibility over material subcontracting arrangements, complete transparency across all nth-party relationships may not be feasible in practice.

Accordingly, supervisory expectations should remain realistic and proportionate, recognising that regulated entities may not always have direct control over deep subcontracting chains.

The WFE therefore supports collaborative approaches involving:

- Regulated entities,
- Critical providers, and
- Regulators.

(v) How is concentration of service provision handled?

WFE members recognise concentration risk as a continued area of focus, particularly in relation to major cloud and technology providers that support MIs. In practice, multiple MIs, along with their critical service providers, often rely on common cloud and technology providers, which can create broader system-wide considerations. In this context, the role of authorities (such as the introduction of emerging critical third-party regimes) in addressing this issue could be helpful.

Current MI's approaches generally focus on:

- Concentration risk assessments;
- Cloud strategy assessments and Identification of single points of failure;
- Business continuity and contingency planning;
- Exit and transition strategies;
- Multi-region or resilience architecture approaches;
- Enhanced oversight of critical providers;
- Contractual safeguards (typically with limited bargaining power) and resilience obligations;
- Ongoing resilience testing and monitoring.

At the same time, the WFE has cautioned against overly prescriptive or mandatory diversification requirements.

The WFE position is that:

- Resilience outcomes are more important than arbitrary diversification mandates;
- Forced diversification may introduce additional operational complexity and risk;
- In some cases, concentration may reflect market realities, scale efficiencies, and security capabilities of leading providers.

As such, concentration risk should be managed through robust governance, resilience planning, and supervisory coordination rather than simplistic numerical diversification requirements.

(vi) What are some of the challenges they face in managing third-party risks?

WFE members identify several key challenges in managing third-party risks, including:

1. Limited Visibility into Nth-Party Dependencies

- Understanding deep subcontracting chains and indirect dependencies remains difficult. The tension between enhanced regulatory expectations (e.g. audit, testing, transparency) over limited leverage over large global providers exists. Third and fourth parties are rapidly adding emerging technologies, like Generative AI, to their services. This introduces new data privacy and security risks that are very difficult for MIs to track and assess.

2. Regulatory Fragmentation

Divergent national and regional outsourcing and operational resilience rules create:

- Duplicative compliance obligations,
- Inconsistent supervisory expectations, and
- Operational inefficiencies.

3. Concentration Risk

The limited number of globally significant cloud and technology providers creates industry-wide dependencies that warrant close attention and raise questions regarding substitutability.

4. Information Asymmetry

Financial institutions may face challenges obtaining:

- Sufficient transparency,
- Suitable contractual arrangements,
- Audit access,
- Incident information,
- Testing visibility from large providers or
- Crisis synchronization: receiving timely, specific updates during a live outage is incredibly difficult because global cloud and technology providers typically use automated ticketing systems that may not provide information needed for MIs to meet strict, fast-paced timelines to declare market halts and notify regulators.

5. Resource and Operational Burden

Increasing due diligence, monitoring, testing, and reporting expectations can create significant operational and compliance burdens for both firms and providers. The practical difficulty of executing exit strategies for critical services is also challenging.

6. **Assessment Pushback and Vendor Fatigue**

Some members have reported difficulties in getting information from large providers, who try to limit them to standard disclosures

7. Cross-Border Coordination

Global providers operate across multiple jurisdictions, making coordinated oversight and supervisory cooperation increasingly important. The need to align with evolving regulatory and supervisory expectations relating to outsourcing, third-party risk management, operational resilience, and critical service providers can be challenging. Data sovereignty conflicts may also arise. MIs may face conflicting rules when using global cloud providers. While cloud service relies on borderless, distributed infrastructure, local regulatory frameworks frequently require data to remain under sovereign legal control. This creates difficult compliance and architecture challenges when leveraging global cloud service providers.

The WFE therefore continues to support internationally coordinated, principles-based, and proportionate TPRM frameworks that strengthen resilience while avoiding unnecessary duplication and fragmentation.

WORLD FEDERATION OF EXCHANGES

About the World Federation of Exchanges (WFE):

Established in 1961, the WFE is the global industry association for exchanges and clearing houses. Headquartered in London, it represents the providers of over 250 pieces of market infrastructure, including standalone CCPs that are not part of exchange groups. Of our members, 39% are in Asia Pacific, 42% in EMEA and 19% in the Americas region. The WFE's 74 member CCPs and clearing services collectively ensure that risk takers post some USD 1.4 trillion (equivalent) of resources to back their positions, in the form of initial margin and default fund requirements. WFE exchanges are home to over 41,000 listed companies, and the market capitalization of these entities is over $137 trillion; around $198.5 trillion in trading annually passes through WFE members (at end-2025).

The WFE is the definitive source for exchange-traded statistics and publishes over 350 market data indicators. Its free statistics database stretches back 50 years and provides information and insight into developments on global exchanges. The WFE works with standard-setters, policy makers, regulators and government organisations around the world to support and promote the development of fair, transparent, stable and efficient markets. The WFE shares regulatory authorities' goals of ensuring the safety and soundness of the global financial system.

With extensive experience of developing and enforcing high standards of conduct, the WFE and its members support an orderly, secure, fair and transparent environment for investors; for companies that raise capital; and for all who deal with financial risk. We seek outcomes that maximise the common good, consumer confidence and economic growth. And we engage with policymakers and regulators in an open, collaborative way, reflecting the central, public role that exchanges and CCPs play in a globally integrated financial system. If you have any further questions, or wish to follow-up on our contribution, the WFE remains at your disposal.

Website: www.world-exchanges.org

Follow the WFE on X: @TheWFE

Follow the WFE on LinkedIn: linkedin.com/world-federation-of-exchanges

If you have any further questions, or wish to follow-up on our contribution, the WFE remains at your disposal. Please contact:

Chhavi Sinha, Manager, Regulatory Affairs: csinha@world-exchanges.org

Richard Metcalfe, Head of Regulatory Affairs: rmetcalfe@world-exchanges.org

or

Nandini Sukumar, Chief Executive Officer: nsukumar@world-exchanges.org.

EU Transparency Register number – 973382524675-69