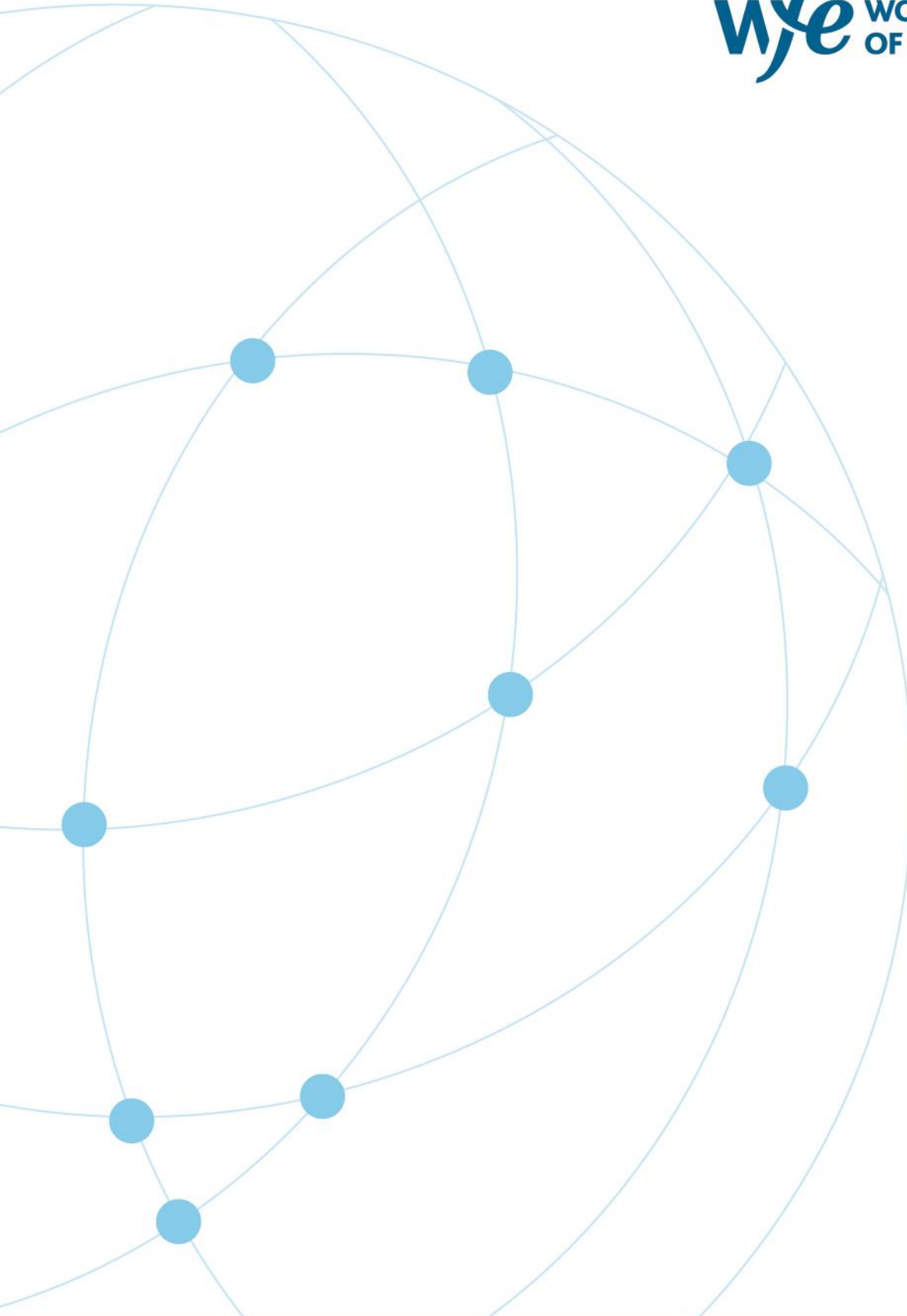




WFE Response to the FSB's consultation on Sound Practices for the Responsible Adoption of Artificial Intelligence (AI) in Financial Services.

22 July 2026

Summary

This response sets out World Federation of Exchanges' (WFE) views on the Financial Stability Board's consultation on [*Sound Practices for the Responsible Adoption of Artificial Intelligence \(AI\) in Financial Services*](#).

The WFE's response is broadly supportive of the FSB's proposed sound practices and its principles-based, proportionate approach to responsible AI adoption. It highlights the growing use of AI across exchanges and CCPs, including market surveillance, listing and issuer services, trading and market operations, while emphasising the importance of robust governance, high-quality data, human oversight and effective risk management. The response also draws attention to key issues for the industry, including third-party dependencies, AI-enabled cyber risks, and the need for a coordinated approach to operational resilience.

WFE Response to the FSB Consultation on Sound Practices for the Responsible Adoption of Artificial Intelligence in Financial Services

The World Federation of Exchanges (WFE) welcomes the opportunity to respond to the Financial Stability Board's consultation on [Sound Practices for the Responsible Adoption of Artificial Intelligence \(AI\) in Financial Services](#).

The WFE represents exchanges and central counterparties (CCPs) globally and supports the development of resilient, innovative, and well-governed financial markets. We welcome the FSB's efforts to identify practical and proportionate approaches that can support the responsible adoption of AI across the financial sector. The WFE also welcomes the FSB's explicit invitation for broader representation beyond banking and insurance, including non-bank financial institutions and financial market infrastructures (FMI). As exchanges and CCPs are already adopting AI across core market functions, their experience can provide important case studies and practical insights into the responsible use of AI outside traditional banking and insurance contexts.

General observations

The WFE broadly agrees with the consultation's assessment that AI adoption in financial services presents opportunities to enhance efficiency, resilience, innovation, and risk management, while also introducing important risks that require careful governance and oversight.

Opportunities

AI is actively transforming operations, driving efficiencies, reducing costs, and delivering tangible results for our members. Like most industries, exchanges and CCPs are adopting enterprise-wide tools, coding tools, and cybersecurity tools.

Beyond these general applications, exchanges are exploring several use cases directly related to their core market functions. The three most common markets functions members are using AI for are:

- 1. Market surveillance:** AI is increasingly being used by exchanges to enhance market surveillance capabilities. Advanced analytics and machine learning techniques can assist in identifying anomalous trading behaviour, detecting potential market abuse, and prioritising alerts for human review. Such tools can improve efficiency and effectiveness by enabling surveillance teams to process large volumes of market data more rapidly while maintaining appropriate human oversight.
- 2. Listing and issuer services:** Some exchanges are exploring AI applications that can streamline listing processes, improve issuer engagement, and facilitate access to market information. AI tools may assist with document analysis, disclosure review, information retrieval, and investor communications, helping to reduce administrative burdens and improve service delivery for issuers and market participants.
- 3. Trading and market operations:** A small number of FMIs are also evaluating the use of AI within trading and market operations. Potential applications include optimising market design features, developing new order types, enhancing operational workflows, and refining trading tools. These initiatives remain subject to extensive testing, governance controls, and regulatory oversight.

AI-enabled tools should be viewed as an enhancement to, rather than a replacement for, existing operational resilience, cybersecurity, governance, and human oversight arrangements. In this context, human oversight should be accompanied by clear human accountability. Responsibility for decisions should remain with appropriately authorised individuals or governance bodies, regardless of the degree of AI involvement in decision-support processes.

Risks & Risk Management

While AI presents ample opportunities for growth and innovation, a number of risk factors require consideration. Some of the most pertinent AI related risks reported by the exchange industry include **data security/confidentiality, model inaccuracies/hallucinations, and operational/data quality risks**. While data security and confidentiality are important, AI outcomes are often heavily dependent on the quality, lineage, completeness, and governance of the underlying data, rather than the model alone. Greater emphasis on data quality and data governance would therefore support more reliable, explainable, and well-controlled AI deployment. Its widespread use in both development (like coding agents) and everyday operations introduces broader resiliency and operational risks. In that regard, AI risk is multifaceted.

Privacy and cyber threats focused on data security and cyber exposure are seen as key areas of focus, particularly with smaller institutions, while larger institutions are also focused on model accuracy and hallucination risk.

There is also a strategic risk in **not using AI**. If exchanges and market infrastructure providers move too slowly, they may lose competitiveness in areas where organisations expect AI to deliver benefits, such as **market surveillance, fraud detection, trading operations, risk management, market data services, and regulatory compliance**. In that sense, the risk is two-sided: using AI without adequate controls creates operational and conduct risks, but failing to adopt it may reduce efficiency, innovation capacity, and competitive positioning.

Risk management and techniques

Risk management should, therefore, focus on proportionate governance, clear accountability, and controls across the AI lifecycle. AI risk can be managed through formal documentation and policies that address the use of AI, including as it relates to governance, risk management, model approval processes, human oversight, documented use cases, and clear escalation routes for high-risk applications. A baseline for AI risk management exists in the form of recognised international standards, such as NIST and ISO.¹ Stronger alignment with these established standards and comparable national standards would support consistency across jurisdictions, reduce duplication, and help avoid regulatory fragmentation where firms are required to map similar AI risks against multiple, slightly divergent frameworks. Other relevant guidance, such as the OECD AI Principles and jurisdiction-specific frameworks, may also provide useful reference points where applied in a proportionate and interoperable manner.

Practical techniques include data classification and access controls, privacy impact assessments, vendor due diligence, model validation and testing, hallucination monitoring, audit trails, cyber

¹ National Institute of Standards and Technology (NIST) AI Risk Management Framework and ISO/IEC 42001 on AI management systems.

controls, and ongoing performance monitoring. For higher-risk use cases, firms should apply stronger controls such as human-in-the-loop review, explainability checks, bias testing where relevant, incident response playbooks, and regular review by risk, compliance, legal, information security, and technology teams.

Given the increasing use of AI in critical business processes, AI governance should also be explicitly linked to existing operational resilience frameworks. For FMIs, the key consideration is often not simply whether a process uses AI, but whether the associated service remains resilient, recoverable, and subject to appropriate oversight. This would reinforce the consultation's message that AI should be managed within existing risk management and resilience frameworks, rather than treated as a wholly separate risk category.

Responsible AI adoption allows financial institutions to harness opportunities and benefits while minimising associated risks. This means that financial institutions need to understand and remain updated on the opportunities and risks of AI and respond with the appropriate adoption strategy and guardrails to manage evolving associated risks.

Across all use cases, human accountability, transparency, validation, and appropriate governance remain critical safeguards.

AI-related risks may arise not only within FMIs themselves, but also from AI systems used by participants, intermediaries, and third-party service providers connected to them. Weak governance or poorly performing AI in the wider ecosystem could have ecosystem-wide impacts, even where FMIs have strong internal controls—for example through flawed AI-driven order execution, client onboarding, or transaction validation processes that increase erroneous flows or operational risk. This can place additional strain on surveillance, risk management, and operational functions, with potential implications for market integrity and resilience. The FSB may therefore wish to acknowledge AI risk from a broader ecosystem perspective, recognising the importance of consistent governance and controls in mitigating ecosystem wide operational risk.

Third-party AI risk management

The WFE strongly supports the consultation's emphasis on third-party risk management as this is one of the most important areas requiring continued supervisory attention particularly regarding critical third-party providers.

As AI adoption grows, financial institutions are becoming increasingly reliant on third-party providers for AI models, data services, and related technology solutions. While these arrangements can deliver significant benefits, they also emphasize the importance of focusing on operational resilience, particularly where there is a relatively small number of service providers.

WFE members have reported challenges that are consistent with several observations highlighted in the consultation. One area that WFE members have reported needing help navigating with the adoption of AI is the visibility into proprietary third-party AI systems and datasets. This has presented opportunities to develop creative approaches for due diligence and independent validation. Additionally, navigating standard contractual frameworks with global technology providers can sometimes limit traditional negotiations, which may compound visibility limitations. However, use of

these providers offers stable, industry-tested environments where organizations can focus on optimizing operational and risk management practices.

The WFE recognises that reliance on a limited number of technology providers may raise operational resilience and concentration considerations. As AI adoption grows, financial institutions may become dependent on a relatively small number of providers for core AI capabilities, including large language models, market surveillance tools, cybersecurity solutions, fraud detection platforms, and other AI-enabled services. This further reinforces the importance of transparency, visibility, resilience testing, and effective oversight across the AI supply chain, particularly where critical market functions rely on a limited number of providers.

The WFE recognises that recent initiatives by authorities to establish oversight frameworks for Critical Third Parties (CTPs) and other systemically important technology service providers, including those already being implemented in some jurisdictions, such as the EU's DORA Critical Third-Party Provider (CTPP) framework and similar emerging international approaches, can mitigate some of the aforementioned concerns.

Given the growing dependence of financial institutions on AI providers, the WFE encourages the FSB to continue facilitating international dialogue and coordination in this area. In particular, further work could help address longstanding challenges relating to transparency, contractual leverage, oversight, and concentration risk.

Emerging developments Concerning Cybersecurity

The recent developments in AI-enabled cybersecurity tools, including so-called “Mythos-class” models, also known as Frontier models, should be considered. These models do not appear to constitute a “doomsday” scenario or a fundamentally new threat category but rather ***accelerate and scale existing cyber techniques***.² Therefore, our members are treating these models with measured seriousness rather than alarm.

The rapid evolution of these models reinforces the need for financial market infrastructures and others to closely monitor capability developments, maintain strong cyber hygiene and core resilience controls, and periodically reassess vulnerability management and response frameworks. This also highlights the value of a ***coordinated industry approach***, including through international forums such as ***WFE's Cybersecurity Working Group (GLEX)***, to support shared understanding and more efficient vulnerability assessment practices.

Approach to Sound Practices

We support the FSB's principles-based and proportionate approach in the consultation. The “Sound Practices” on AI governance and management of the relevant stages of AI development and deployment (AI lifecycle) offer valuable items for consideration and include ideas that our members are already pursuing.

The WFE believes that AI does not necessitate a fundamental overhaul of existing financial regulatory frameworks, as regulatory frameworks should be technology neutral. As covered above, many of the

² [July 1, 2026, WFE: Mythos Beyond the Headlines](#)

risks associated with AI are not entirely new. Rather, AI may accelerate, amplify, or change the scale of existing risks relating to operational resilience, model governance, third-party risk management, market conduct, and cybersecurity. Existing regulatory frameworks, when applied in a technology-neutral manner, already provide a strong foundation for addressing these risks.

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](https://twitter.com/TheWFE)

Follow the WFE on LinkedIn: [linkedin.com/world-federation-of-exchanges](https://www.linkedin.com/company/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

James Auliffe, Senior Manager, Regulatory Affairs: jauliffe@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