WORLD FEDERATION OF EXCHANGES

# The WFE advises US Treasury that an AI regulatory framework needs to be outcomes-based

**20th August 2024**

**Summary**

The World Federation of Exchanges (WFE) welcomes the opportunity to comment on the US Treasury's approach to AI. As the global industry association for exchanges and clearing houses, we represent the providers of over 250 pieces of market infrastructure that see more than $124tr in trading pass through them annually (at end-2023).

Exchanges and CCPs' extensive experience with technology makes them well-placed to offer views on the development of AI. While these technological innovations and the associated concerns about managing generative AI are significant, it is important to remember that, as trusted third parties providing secure and regulated platforms for trading securities, our members are already carefully scrutinising tools and establishing controls to govern AI use.

The WFE advises the Treasury that:

- The definition of AI should be precisely tailored to avoid including more than what is necessary. A broad definition would create onerous restrictions and not be proportionate to the risks that different tools have.
- A definition of AI should focus on computer systems with the ability to make decisions or predictions based on automated, statistical learning.
- AI deployment by malicious actors is an emerging type of risk associated with this technology which financial services firms are well aware of and are tackling.
- Whilst traditional risk management techniques can be used to manage risk of AI systems, more work needs to be done to develop AI specific risk management tools.
- Third parties will be valuable to help develop AI tools and risk management tools, but Treasury is right to be cognisant of the risks around big tech firms utilising their market dominance.
- Regulatory uncertainty is a key concern amongst our members. Regulators should focus on outcomes and use sound judgment, fostering collaboration to support innovation and competitiveness in financial markets.
- Our members favour a principles and risk-based approach to developing a regulatory framework, where requirements are proportional to the level of risk associated with AI applications. This needs alignment among the various financial regulators and must be compliant with international standards.
- Ultimately, government policy should encourage modernisation by promoting the use of cutting-edge technologies like AI, cloud computing, and machine learning in capital markets. This enhances market dynamics, and provides better services to consumers.

AI use cases amongst our members are numerous and varied. Among these, AI can help exchanges and CCPs to:

  - detect fraud,
  - undertake market surveillance,
  - facilitate trade execution,
  - manage risk,
  - optimise settlement,
  - provide customer support, and enhance compliance.

**Detailed Response**

AI encompasses a wide array of technologies designed to perform tasks that typically require human intelligence, such as behaviour analysis, problem-solving, and decision-making. Recent advances, particularly in generative AI, have spurred widespread adoption across various industries. This surge has pushed AI into the spotlight, prompting extensive discussions on its applications and the need for regulation, capturing the interest of developers, industry stakeholders, and policymakers.

While these technological innovations and the associated concerns about managing generative AI are significant, it is important to remember that AI has been in use in financial services for at least twenty years. Financial institutions have been using machine learning (ML), a subset of AI that focuses on the development of algorithms and statistical models that enable computers to perform tasks, for a long time. As such, firms have carefully scrutinised tools and established controls to govern AI use.

Despite the challenges, the potential for AI to significantly boost market efficiency is especially beneficial in the financial services sector. Here, the ability to rapidly analyse data is crucial for enhancing productivity, efficiency, and competitiveness. Although the advantages are considerable, there are valid concerns about the uncertainties surrounding the evolving landscape of AI technologies. Therefore, we appreciate the Treasury's efforts to understand the industry's perspective on this technology.

**Definition and Scope**

Defining artificial intelligence is difficult. Psychologists have been debating how to define human intelligence for at least a hundred years and no standard definition exists. The same is true for technologists who have not been able to reach consensus on what constitutes artificial intelligence. The reason for this is that there is no definitive boundary, but rather a spectrum of features that define what we understand as artificial intelligence. Moreover, as AI becomes increasingly sophisticated and varied, technologies which were once widely regarded as AI, are no longer seen as such, despite using standard AI methods.

Defining AI will have real implications for its trajectory and utility in financial markets. Therefore, the definition must be intentionally crafted to recognise both current and potential technologies in use. It should be precisely tailored to avoid including more than necessary. An overly broad definition could create unnecessary complexity by imposing extensive compliance obligations. Therefore, the Treasury and US regulators should be careful to avoid this while still accommodating the diverse and evolving nature of the technology.

In our view, the definition of AI in the President's Executive Order is overly broad and could lead to AI being defined as any computer system. At least in financial services, it would be better to adopt a definition of AI that focuses on computer systems with the ability to make decisions or predictions based on automated, statistical learning. Such a definition would more accurately capture what we understand to technologies currently employed in the industry.

**Benefits of AI**

AI can help increase economic growth by enhancing productivity through automation and innovation and by driving advancements in various sectors, leading to new products, services, and markets. In financial services, AI can help deliver better outcomes for the market, end users and the real economy.

AI can reduce costs for financial services firms by automating routine tasks and improving operational efficiency. It can create innovative products through advanced data analytics and personalized services. Additionally, AI-driven insights and decision-making can boost revenues and employment by identifying new opportunities and optimising investment strategies.

Technological advancement and automation have typically provided benefits for humanity and increased economic growth. Technology can reduce the need for human labour in certain areas and allow humans to focus on more productive or innovative tasks. AI is merely the next step in automation rather than a radical departure from the norm

**Use Cases**

AI brings valuable contributions in various ways. First, it can identify intricate patterns within data that humans might overlook, aiding in accurately identifying and mimicking behaviours more accurately. Second, AI's ability to handle repetitive tasks can outpace human capabilities, boosting overall efficiency. Furthermore, AI systems ensure consistent task performance without succumbing to fatigue or distractions ensuring reliable results over time. Additionally, AI's ability to manage large datasets without demanding excessive resources highlights its scalability and resourcefulness, further enriching its value.

Our members generally see AI use cases in three broad categories:

1. Individual productivity – tools designed to improve the output of individual employees. Examples could include using generative AI to help develop code, virtual assistants to help staff or automated data entry.
2. Operational efficiency – tools designed to improve the efficiency of the overall operation of exchanges and CCPs. Examples include predictive tools to identify hardware that requires maintenance, automation of repetitive processes or fraud detection and prevention.
3. New product developments – these would be products and services that an exchange or CCP could offer to market participants or the broader market. Examples could include market data offerings and regulatory compliance solutions.

AI has many potential use cases for exchanges and CCPs:

- Fraud and money laundering detection: AI can be used to identify potential fraud due to its ability to analyse vast amounts of data, identify patterns, and detect anomalies.
- Market Surveillance: AI can be used to monitor financial markets for suspicious activities, detect market manipulation and fraud, ensure compliance with regulations, and maintain the integrity of the market.
- Risk Management: AI can be used to manage risk by analysing data, simulating models and monitor operational activities.
- Customer Support: AI can enhance customer support and provide efficient, responsive, and personalised services.
- Trade Execution & Settlement Optimisation: AI can be used to help optimise execution and settlement.
- Regulatory Compliance & Regulatory Filings: AI can enhance regulatory compliance by helping to monitor changes, provide audit trails and automate reporting requirements.

- Cybersecurity: AI can enhance cybersecurity defences by detecting threats, anomalies and phishing attempts.

**Cybersecurity, Market Manipulation and Fraud**

Given the concerns raised around the world, it is worth digging a little deeper into criminal activities using AI. Here, AI will be an asset for both the "good guys" and the "bad guys." The financial services industry has already witnessed how deep fakes can be used to trick unwitting employees to erroneously send payments. In addition, generative AI and Large Language Models (LLMs) allow for better phishing emails to increase the impact and success of these attacks. Meanwhile, phishing attacks continue to be a primary method for threat actors to gain initial access to a financial institution's systems.

To counter malicious actors, AI is currently being used by cyber professionals primarily through their use of cyber vendors. AI/ML is used by advanced intrusion detection systems to not only detect known malicious activity but also to identify variants of this activity and disrupt these attacks. Similarly, AI is used by network monitoring tools to identify changes in network traffic behaviour that may, for example, signal an intrusion looking for new hosts. Given that numerous malware strains attempt to do similar actions to gain access to the underlying operating system and the growing number of clients using advanced intrusion detection systems, the ability of these vendors to provide holistic protection across its customer base is greatly benefited by AI technology and the financial institutions that utilize them.

AI is also one of the most effective tools for combating fraud. As previously mentioned, AI excels when analysing large, representative datasets. Utilising AI to detect and prevent fraud is likely the most effective way to counteract malfeasance by bad actors. AI can scrutinise extensive databases of financial transactions to pinpoint unusual and anomalous activities that may suggest fraudulent trading or other nefarious actions.

This helps demonstrate the earlier point on the definition and scope of this exercise. An overly broad definition of AI could hamper exchanges' ability to utilise AI tools to prevent malicious activity if it leads to excessive regulatory burden.

**Risks related to AI**

While AI brings numerous benefits to financial services, the industry is cognisant of the importance of managing potential risks and ensuring that AI applications align with ethical and regulatory standards. Exchanges and CCPs are already incentivised to have the strongest possible risk management because any failures could harm their reputations as trusted venues delivering market integrity.

**Risk Management of AI**

Financial institutions are currently using existing risk management frameworks to manage AI risks. Risk management techniques, such as those involved in identifying risk or analysing the impact or likelihood of an event remain relevant to managing AI risks.

In many ways some AI risks are similar to more traditional risk. For example, discrimination and bias in decision-making by humans are longstanding risks across all business sectors. Nevertheless, due to

its capabilities, AI may amplify these risks if the training data is biased or the opacity of the AI system prevents explainability and accountability.

Furthermore, some of the concerns around explainability are mistaken. Most AI models are based on a set of predefined rules, so they are highly transparent and interpretable. These older, more classical machine learning models use decision trees, linear regression and support vector machines that are more interpretable than complex deep learning models.

Nevertheless, as more complex forms of AI emerge, we need more comprehensive and developed risk management techniques. Emerging standards, such as NIST's AI Risk Management Framework,[1] have recently been introduced to provide pillars for the comprehensive management of AI risks. Currently, the NIST AI Risk Management Framework provides a framework to manage risks identified through the AI development process. However, this and other frameworks do not provide any detail on 'how' to identify potential risks to AI models. This framework will evolve with this information over time to be a critical piece in the consistent application of AI risk management.

**Third Parties**

Third parties bring great value to financial services and will likely play a pivotal role in the development of AI technologies within financial markets. Technology companies will develop AI tools for financial services and those that have a general level of applicability across the whole economy. The latter can then be tailored to the regulated environment in financial services. Those AI tools developed with a more general level of applicability will benefit from being exposed to various sectors of the economy and bring great value to the sector.

Where our members use third parties, the third parties will be subject to vendor risk management. Depending upon the type of tool and the impact and likelihood of failure, they may be subject to enhanced vendor risk management. As explained above, risk management techniques for AI are still developing so our members are generally cautious when engaging with AI developed by third parties.

*Concentration*

Market concentration can contribute positively to economic growth and industry development when it facilitates efficiency gains and innovation. The potential for AI to create large economies of scale is not much different from the potential of any technological advancements to create economies of scale. This may be done with third parties that specialise in technology and AI, working with other industries to deliver large economies of scale and significant expertise.

With the exception of LLMs, there is not currently a significant level of concentration of AI models among a small number of firms. While there are a limited number of cloud providers and open-source projects that provide the software and hardware tools used to train and serve AI models, the models themselves use diverse data inputs, proprietary knowledge and bespoke guardrails that vary as much by development group as by firm.

Nevertheless, regulators should monitor market concentration in AI to prevent market dominance from hindering regulatory compliance or risk management. AI systems may require large computational power with large data sets to produce expected and accurate results. The ability to

[1] https://www.nist.gov/itl/ai-risk-management-framework

provide the computational power necessary for complex models may reside with a handful of large technology companies which may drive further concentration and interconnectedness with these providers. Furthermore, firms often need to understand AI models to meet their regulatory obligations, but AI companies may claim proprietary restrictions.

Regulators are correct to be cognisant of the risks of AI to competition and market concentration. Regulators should be aware of these pressures on regulated firms, often by companies much bigger than them, and monitor the issue in case of negative outcomes.

**Barriers to AI**

Our members are experiencing a number of the more generic barriers. AI solutions are very costly and require sufficient skilled workers. The projects often involve high sunk costs without guarantee of success.

Regulatory uncertainty is a key concern for our members. As these systems can be costly to develop, members want to ensure that they are compliant with regulations. Clear statements of support for the development of AI systems by the Treasury and other regulators can help remove this uncertainty.

Regulators should prioritise outcomes and exercise reasonable and sound judgement when overseeing AI use in financial markets. Whilst becoming reliant on enforcement to maintain compliance can be a successful strategy, it can also foster an adversarial relationship with industry and capture technical infringements that do not necessarily result in poor outcomes. Instead, regulators can build a collaborative relationship with those that they regulate to ensure that only the most serious events are punished. This, in turn, will help deliver an internationally competitive financial sector by allowing market participants to take risks with innovation Regulators can exercise sound and reasonable judgement, taking into consideration the nascent nature of some AI techniques, to determine where these failings are small or where enforcement is a more appropriate tool for supervision.

**Recommendations**

Designing an effective AI regulatory framework requires a nuanced approach that balances robust oversight with the promotion of innovation.

First and foremost, AI regulations should be **principles based.** Principles-based regulation is essential for maintaining flexibility and encouraging innovation. Instead of rigid, prescriptive rules, this approach focuses on achieving desired outcomes, giving organisations the freedom to determine the best methods to meet these standards. Principles enshrined in law and regulatory rules remain valid regardless of the technology used.

Secondly, an **incremental approach** to AI regulation would be desirable. This method allows for gradual adjustments and learning, ensuring that regulations do not hinder technological progress. By evolving alongside AI advancements, the regulatory framework can remain relevant and effective.

Regulators should also apply a **risk-based approach** to regulating AI. This means that requirements should be proportional to the level of risk associated with AI applications. Regulators should evaluate each AI system based on its unique characteristics and intended use. The scrutiny should correspond to factors such as the intended use-case, the sophistication of end-users, the level of risk posed by the

system, and the degree of autonomy it exercises independent of rules or guidance. The risk associated with an AI application capable of generative outputs, allowing it significant freedom in decision-making, far exceeds that of an AI system constrained to a limited dataset and narrow range of actions. Consequently, these systems should not be subject to identical regulatory assessments. This approach mirrors that of the National Institute of Standards and Technology (NIST) in crafting its AI Risk Management Framework.

Collaborative oversight among regulatory agencies will be vital to avoid unnecessary complexity. By leveraging existing frameworks and aligning with international standards, regulators can create a cohesive and effective oversight environment. Global standards alignment will facilitate easier compliance for multinational companies and foster international trust and collaboration. Treasury can play a vital role by providing oversight to the federal regulatory agencies in this regard.

Finally, government policy should encourage modernisation by promoting the use of cutting-edge technologies like AI, cloud computing, and machine learning in capital markets. This can drive efficiency, enhance market dynamics, and provide better services to consumers. Additionally, policies should support skills development and professional standards in AI, ensuring that the workforce is prepared to manage and innovate within the evolving technological landscape.

By integrating these principles, the AI regulatory framework can achieve a balance between ensuring robust oversight and fostering innovation. This approach not only protects public interest and safety but also encourages the growth and beneficial application of AI technologies across various industries.

## Background

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, 36% are in Asia-Pacific, 43% in EMEA and 21% in the Americas. The WFE's 87 member CCPs and clearing services collectively ensure that risk takers post some $1.3 trillion (equivalent) of resources to back their positions, in the form of initial margin and default fund requirements. The exchanges covered by WFE data are home to over 55,000 listed companies, and the market capitalization of these entities is over $111tr; around $124tr in trading annually passes through WFE members (at end-2023).

The WFE is the definitive source for exchange-traded statistics and publishes over 350 market data indicators. Its free statistics database stretches back more than 40 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 policy makers 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. Please contact:

James Auliffe, 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.