To:
Mr. Klaas Knot
Chair
Financial Stability Board

Mr. Pablo Hernández de Cos
Chair
Basel Committee on Banking Supervision

Mr. Erik Thedéen
Incoming Chair
Basel Committee on Banking Supervision

Mr. Jean-Paul Servais
Chair
International Organization of Securities Commissions

Mr. Fabio Panetta
Chair
Committee on Payments and Markets Infrastructures

Mr. Carmine Di Noia
Director for Financial and Enterprise Affairs
Organisation for Economic Co-operation and Development

CC:
Mr. John Schindler
Secretary General
Financial Stability Board

Mr. Neil Esho
Secretary General
Basel Committee on Banking Supervision

Mr. Tajinder Singh
Acting Secretary General
International Organization of Securities Commissions

Ms. Tara Rice
Head of Secretariat
Committee on Payments and Market Infrastructures

Mr. Serdar Çelik
Head of the Capital Markets and Financial Institutions Division
Organisation for Economic Co-operation and Development

28 May 2024

Re: Key Considerations for Artificial Intelligence in Capital Markets

Dear Sirs and Madam,

The Global Financial Markets Association ("GFMA")[1] welcomes the continued leadership of the G20 on artificial intelligence ("AI"), as demonstrated by the Organisation for Economic Co-operation and Development ("OECD"), the Financial Stability Board ("FSB"), the International Organisation of Securities Commissions ("IOSCO"), the Basel Committee on Banking Supervision ("BCBS"), and the Committee on Payments and Market Infrastructures ("CPMI") as they collaborate and coordinate to evaluate the impact of AI in capital markets. The FSB and IOSCO recently released updated work programmes for 2024 adding focus on AI. We look forward to supporting these efforts and value the role the Financial Stability Engagement Group ("FSEG") may play in supporting consistency of regulatory developments, including supervisory oversight, due to the inherent cross sectoral nature of this technology. AI has been used in the financial services industry for many years, but there has been increased focus on AI recently due to advancements in generative AI ("GenAI") and predictive AI ("PredAI").

As the authorities commence new workstreams on this topic for 2024, including review of potential financial stability risk implications, GFMA would like to share industry views concerning key considerations regarding the use of, and regulatory approach to, AI in capital markets. The financial services industry has been one of the earliest and most prominent industry adopters of AI; it has "decades-long history […] with long-standing applications in financial services."[2] Firms have utilized "traditional" forms of AI and machine learning for many years, and consequently have developed governance processes to oversee, manage and monitor their application of AI, in accordance with their existing

[1] The GFMA represents the common interests of the world's leading financial and capital market participants, to provide a collective voice on matters that support global capital markets. We advocate on policies to address risks that have no borders, regional market developments that impact global capital markets, and policies that promote efficient cross-border capital flows, benefiting broader global economic growth. The Global Financial Markets Association ("GFMA") brings together three of the world's leading financial trade associations to address the increasingly important global regulatory agenda and to promote coordinated advocacy efforts. The Association for Financial Markets in Europe ("AFME") in London, Brussels and Frankfurt, the Asia Securities Industry & Financial Markets Association ("ASIFMA") in Hong Kong and Singapore, and the Securities Industry and Financial Markets Association ("SIFMA") in New York and Washington are, respectively, the European, Asian and North American members of GFMA.
[2] Ostmann, F., and Dorobantu C., The Alan Turing Institute, AI in Financial Services, 2021.

regulatory obligations. Specifically, these established governance processes cover a wide set of functional policy areas, examples of which are contained in the attached appendix I. These functional policy areas also may be used to assess and address potential impacts from AI to overall financial stability risk; additional AI-specific capital markets regulation, therefore, may be redundant.

AI has the potential to transform financial services and capital markets to make them safer, more efficient, accessible, and tailored to consumer needs. This, in turn, brings important benefits to consumers and the wider global economy. However, there is a real concern that a fragmented regulatory approach, with overlapping regimes mandating different requirements, could end up being a major risk for financial entities when using AI, and could prevent stakeholders from realizing the genuine benefits of this technology. This risk is reflected in recent calls from multiple world leaders for collaborative international approaches to establishing AI governance standards, in order to promote safe, secure, trustworthy, and sustainable AI while maximizing the potential benefits of AI to our economies and societies[3].

A summary of the key considerations and industry views can be found on the following pages of this letter.

We appreciate the OECD, FSB, IOSCO, BCBS, and CPMI's consideration of our views and hope they serve as an aid in guiding your analysis on the role of AI in capital markets. GFMA would welcome the opportunity to further participate in this valuable process. Please feel free to contact the undersigned to further discuss these considerations or any other questions regarding this topic.

Sincerely,

Leonardo Arduini
Chair
Global Financial Markets Association

[3] *See* the Seoul Ministerial Statement for advancing AI safety, innovation and inclusivity: AI Seoul Summit 2024 (May 2024).

Key Topics for Considerations on AI in Capital Markets

GFMA would like to share industry views concerning key considerations regarding the use of, and the regulatory approach to, AI in capital markets.

It is not necessary to define "Artificial Intelligence."

At this time, GFMA does not endorse a specific definition of AI since it is neither a narrow nor static technology. Additionally, GFMA believes that if global standards setters utilize a principles-based and outcomes-focused approach by referring to AI characteristics, it may be less necessary to develop a consensus single, specific definition of AI, particularly since many jurisdictions have recently adopted, or are in the process of adopting, region specific AI definitions. We equally caution regional authorities from producing specific and prescriptive definitions.

However, GFMA understands that in order to comment on considerations relating to this topic, it may be necessary to refer to a common definition. For this reason, GFMA will utilize the OECD definition of AI systems[4] as a reference definition for all considerations outlined in this letter.

> *OECD definition of AI systems – An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.*

The OECD definition is not overly broad as to capture systems that are not considered AI today. Additionally, definitions in many major jurisdictions have followed the OECD definition or have proposed similar definitions based upon the one developed by the OECD. Notably, in May 2024, the OECD Ministerial Council Meeting ("MCM") adopted the latest revisions to the OECD Principles on Artificial Intelligence, which include 47 state adherents and continues to reference this definition of AI systems[5]. The European Union's AI Act also utilizes this definition[6].

Existing standards and frameworks sufficiently cover current and future AI use cases.

Artificial intelligence is an established technology utilized by the financial services industry. New advancements, such as GenAI and PredAI, have led to increased focus on the potential opportunities of use cases, for example, to serve clients directly or indirectly. As AI technology evolves and new use cases continue to develop, it is integral that a technology-neutral, principles-based, and outcomes-focused approach is prioritized. Global authorities can apply and adapt existing standards and frameworks where applicable, rather than create new AI-specific standards that could lead to conflicts of law for technology solutions implemented by financial services firms, or create undue costs and burden for implementing and monitoring AI use cases. Existing standards have proven effective, while remaining technology-neutral, and promote outcomes-based regulation[7].

Should gaps in existing standards be identified as new AI use cases gain prominence, from a financial stability perspective, standard setters should explore whether it would be sufficient to update existing governance frameworks or if new guidance may be necessary to fill in any gaps. After such analysis, if these options are insufficient, only then should new standards be considered, provided that they complement existing processes and procedures for technological innovations.

GFMA appreciates the global standard setters' time and effort that is necessary to review existing standards. The cross sectoral perspective of the FSB could also support the G20 in identifying where alignment is necessary to avoid potential unintended consequences from other sector regulations impacting the ability of financial services firms to innovate and continue to serve their clients with fit for purpose technology solutions.

[4] The OECD definition of AI system was last amended November 2023 – with Explanatory Memorandum published March 2024.

[5] The OECD published revisions to their AI Principles on 5 May 2024 (see adherents section of the revisions for a list of all states).

[6] *See* Article 3(1) of the EU AI Act (corrigendum).

[7] Examples include the FSB's "Final report on enhancing third-party risk management and oversight – a toolkit for financial institutions and financial authorities" (December 2023), IOSCO's "Principles on Outsourcing" (October 2021), and the BCBS's "Principles for operational resilience" and revisions to the "Principles for the sound management of operational risk" (March 2021).

Further, we would call upon the G20 to endorse a technology-neutral, principles-based, and outcomes-focused approach for AI consistent with the goals outlined in paragraph 61 of the New Delhi Leader's Declaration Statement:

> "To unlock the full potential of AI, equitably share its benefits and mitigate risks, we will work together to promote international cooperation and further discussion on international governance for AI. To this end, we:
>
> i. Reaffirm our commitment to G20 AI Principles (2019) and endeavour to share information on approaches to using AI to support solutions in the digital economy.
>
> ii. Will pursue a pro-innovation regulatory/governance approach that maximizes the benefits and takes into account the risks associated with the use of AI…."

The following two sections on model risk and third-party risk management serve as specific examples of how existing standards sufficiently apply to AI. Additionally, appendix I is included as a resource to broadly demonstrate how existing functional policy areas are applicable to current and potential future applications of AI in capital markets.

Model risk standards apply to AI applications and models used by financial institutions.

Capital markets firms are subject to comprehensive model risk standards and frameworks. AI applications and models that are used by firms are already subject to these requirements. These frameworks are regularly reviewed on a risk-based and outcomes-based approach. As indicated above, if there are gaps identified in the future where risks are not properly accounted for, GFMA would welcome working with authorities to help design updates to these frameworks as needed, or to promulgate necessary guidance or best practices.

One example of a potential model risk standard gap for additional review by authorities is basic linguistics. Currently, many leading GenAI models are predominantly trained in English/Latin-based languages. When evaluating model risks, it is important to consider training with relevant local language data and the need to appropriately test large language models ("LLMs") for accuracy in the markets where they are being utilized. It is these types of gaps where public and private collaboration can help identify some of the practical factors and steps that could be employed to significantly mitigate potential risks.

Third-party risk management standards apply to AI.

FSB, IOSCO, BCBS, and others have recently implemented robust third-party risk management standards that are technology-neutral, principles-based, and outcomes-focused. As a result, these standards are flexible enough to cover the evolution of AI and demonstrate how a technology-neutral, principles-based, and outcomes-focused approach has proven practicable for firms to manage new AI use cases.

As global standard setters and regulators further consider third-party risks related to AI, GFMA recommends they be cognizant of all the actors and their accompanying responsibilities in the AI supply chain. Vendor intellectual property protection can limit firms' ability to fully review third-party solutions, but clearly defining the roles of all actors in the AI supply chain can help increase transparency and facilitate application of existing risk-based standards on this topic.

New AI-specific regulation has the potential to stifle innovation in the financial sector.

AI-specific regulation has the potential to stifle innovation for financial services, as well as other sectors, globally. This risk is heightened if local jurisdictions enact AI legislation and regulations that are inconsistent, unclear, or unnecessarily prescriptive. Such requirements would lead to fragmentation and would also deter innovation which, in turn, would stunt necessary technological advancement. In particular, many jurisdictions already have passed, or are in the process of enacting, their own AI-specific regulations, legislation, and frameworks (*see* appendix II), yet the scope and content of these requirements can vary significantly by regime. These difficulties may be further exacerbated if regulators introduce additional AI-specific regulations for the financial services or capital markets sectors. Local jurisdictions therefore should be dissuaded from enacting new standards specifically aimed at AI to avoid detrimentally impacting their own constituents.

Instead, and as outlined in the above sections, regulatory focus should be on the application of existing technology-neutral and outcomes-based frameworks to AI use cases. Notably, many recent AI-specific initiatives at the jurisdictional level have highlighted the need for this approach[8]. The need for cohesive international regulatory alignment is also reflected by recent calls by multiple world leaders for collaborative international approaches to establishing AI governance standards, in order to promote safe, secure, trustworthy, and sustainable AI while maximizing the potential benefits of AI to our economies and societies[9].

Finally, as an alternative to new regulation, GFMA encourages collaboration between the official sector and industry to develop risk frameworks and toolkits. Examples of recent successful collaborative efforts on this include the Monetary Authority of Singapore ("MAS") Veritas Consortium, the MAS Project MindForge, the Model AI Governance Framework for GenAI in Singapore, and the FSB FIRE initiative. The private and public sector collectively can help foster innovation and at the same time mitigate unintended impacts to financial stability by working together as technology evolves.

[8] For example, the UK FCA "*is technology neutral and pro-innovation [for AI regulation.] We expect firms to be fully compliant with the existing framework, including the Senior Managers & Certification Regime (SM&CR) and Consumer Duty.*" [FCA, AI: Flipping the coin in financial services, October 2023]; the UK "*Bank [of England] and PRA adopt a technology-agnostic approach to supervision and regulation of AI/ML*" [Bank of England & PRA, The Bank and the PRA's response to DSIT/HMT: update on our approach to AI, April 2024]; In Canada, "*According to the Competition Bureau Canada regulation should […] be technology neural and device agnostic. Rules that a financial entity must comply with often refer to the technology used at the time of the development of the rules […] Although such regulation may have been effective in the past, rules that can foster innovation and the development of yet-to-be developed technologies are necessary.*" [OECD, Digital Disruption in Banking and its Impact on Competition, 2020]; Commissioner Kristin N. Johnson has stated that the U.S. CFTC's "*approach to mitigating the risks associated with the use of AI in our markets should be principles-based, retaining adaptability and remaining technology neutral.*" [CFTC, Statement of Commissioner Kristin N. Johnson: Articulating an Agenda for Regulating AI, May 2024]; Monetary Authority Singapore "*requires regulated financial institutions (FIs) to have controls in place to avoid or mitigate conflicts between their interests and those of their customers. This approach is technology-neutral and is applied across all regulated FIs.*" [MAS, Written reply to Parliamentary Question on impact of artificial intelligence on trading platforms in financial markets, August 2023]; and in Hong Kong, "*The HKMA adopts a risk-based and technology-neutral approach in its supervision.*" [HKMA, Risk-based and technology-neutral – the HKMA's supervisory approach to financial technology (Fintech), March 2016].

[9] *See* the Seoul Ministerial Statement for advancing AI safety, innovation and inclusivity: AI Seoul Summit 2024 (May 2024), and the Seoul Declaration for safe, innovative and inclusive AI by participants attending the Leaders' Session: AI Seoul Summit (May 2024).

Appendix I – Existing Technology-Neutral Functional Policy Areas Applicable to AI

This appendix serves to illustrate the wide range of existing functional policy areas, sorted on a thematic basis, that already apply to financial entities. **This list is by no means exhaustive**; all technology-neutral functional policy areas in any jurisdiction already apply to the use of AI[10]. However, it serves as a snapshot of some existing areas that clearly also may be used to assess and address potential impacts from AI to overall financial stability risks, for illustrative purposes.

Since GFMA is a global capital markets trade association, this table is limited to capital market specific functional areas and the corresponding regulations being managed by global capital markets participants. Please note that GFMA's regional affiliate trades (AFME, ASIFMA, and SIFMA) are all continuing efforts on this topic at the regional and jurisdictional levels[11].

No.	Functional Policy Area	Application to AI
1.	Market Protection	Financial firms that use AI systems in connection with providing services to investors may find that their AI systems are subject to the requirements of various market protection legislation, such as MiFID II, the Dodd-Frank Act, the Securities and Futures Act, and the Financial Instruments and Exchange Act. For example: • Financial entities using AI systems for trading or investment decision-making must ensure that they produce detailed and interpretable logs and records of all decisions and transactions to help meet transparency and reporting obligations under certain of these laws. • AI systems used in trading must be designed to operate in a way that complies with market abuse requirements and are auditable. • Certain market-specific regulations require financial firms to take all sufficient steps to obtain the best possible result for their clients when executing orders. AI systems used in automated trading must therefore be designed to consistently consider multiple factors (such as price, cost, speed, and likelihood of execution) to ensure compliance with such a best execution requirement. • Market-specific regulations, that apply to general obligations and trading practices regardless of whether AI is used, would also continue to apply. • There are various existing controls that are designed to mitigate the impact of volatility in the markets.
2.	Governance Structures[12]	Firms need to have effective risk governance structures in place to identify, understand and manage risks associated with applications of AI systems. This includes having oversight of the full model development cycle, from proposal to deployment and ongoing monitoring. While the risks stemming from AI can be novel, the need for effective governance structures is not a new concept. In many jurisdictions, specific requirements already exist to ensure that management have full coverage of the firm's activities, as well as the appropriate skillsets to perform their oversight roles.
3.	Risk Monitoring and Management	There are a wide range of risks that can arise from an application of AI; it is important to have an effective risk monitoring and management framework in place to help ensure that such risks are identified and addressed accordingly. However, while there are potentially some novel risks to consider from the use of AI, identifying, addressing, and monitoring AI-related risks need not be fundamentally different to firm's existing risk management frameworks.
4.	Cybersecurity[13]	As firms consider integrating AI systems into their business practices, they must consider the cybersecurity of their valuable data and operational significance. In particular, data poisoning, data leakage, and data integrity attacks are particularly important risks to be mindful of given AI systems' dependency on the data used to train and test it. In addition to the cybersecurity risks presented from the use of AI, financial institutions also need to be aware of how threat actors may use AI to increase the propensity and sophistication of existing cybersecurity threats. For example, AI-generated spearfishing messages, social

[10] Please note that GFMA-affiliate trades (AFME, ASIFMA, and SIFMA) can provide more details on the suites of existing principles-based, technology-neutral, outcomes-focused financial services regulations in their jurisdictions.

[11] *See*, for example, ASIFMA's "Practical Considerations for Generative AI" (January 2024) and "Enabling an Efficient Regulatory Environment for AI" (June 2021), AFME's "AI: Challenges and Opportunities for Compliance" (September 2023), and SIFMA's Response to "Request for Comment on the Use of AI in CFTC Regulated Markets" (April 2024).

[12] We flag that the Basel Committee on Banking Supervision ("BCBS") has published Corporate Governance Principles for Banks (revised April 2023).

[13] We flag that the International Organisation of Securities Commissions ("IOSCO") has published Fundamental Elements of Cybersecurity for the Financial Sector (October 2016).

		engineering attacks that are executed through AI-generated deep-fakes, and using GenAI to conduct parallel disinformation campaigns alongside a targeted cybersecurity attack.
5.	Model Risk Management	Traditional model-risk management frameworks are applicable to the development, validation, implementation, and use and governance of models, including AI systems, and which consider model explainability and data integrity as key considerations.
6.	Third Party Risk Management[14]	Third-party risk management is of high importance for AI as many financial institutions are electing to purchase AI systems (either in part or in whole) from third-party vendors versus building the AI system in-house. There are broadly three categories of AI-related third parties: (1) vendors providing AI software; (2) vendors of software that includes AI features; and (3) other traditional vendors who may use AI in connection with their provision of services to the client. The risks and requirements are slightly different for each category.
7.	Data Privacy	Due to the broad definition of 'personal data' under many jurisdictions' data privacy laws, the data entered into or associated with AI systems (as training, prompt or reference data) may involve personal data that is subject to, and protected by, such laws. Additionally, AI systems may be used to collect and use the personal data of individuals, or monitor their behaviour for customer service or fraud detection purposes, for example. This could involve monitoring websites or app usage, geolocation, or voice data. Again, such activities would likely be subject to the requirements of applicable data privacy laws.
8.	Transparency	Transparency in AI is important to help facilitate confidence and trust in AI. There are broadly three categories of transparency considerations: (1) requirements to disclose when individuals are interacting with an AI system, or output created by and AI system; (2) in certain circumstances, requirements to disclose where an individual is subject to a decision created by an AI system; and (3) requirements for developers of AI systems to disclose certain information to the users and deployers of those systems.
9.	Operational resilience & business continuity[15]	Operational resilience requirements help improve the stability and reliability of services, including those that are completed by, or in connection with, AI systems so firms can continue to operate in the event the AI system is disrupted, becomes un-operational, or otherwise stops operating as intended. As firms consider deploying AI systems, firms' operational resilience posture in connection with those AI systems is gaining increasing importance.
10.	Stress Testing[16]	Stress tests are already a key part of financial entities' training and testing toolkit; they allow firms and regulators to identify and test a range of risk-based scenarios over time to improve resilience. As firms consider deploying AI systems, it is correspondingly important for AI systems to be tested to both assess their performance, and to better understand the reaction functions of AI systems. While the scope and content of the rules vary by regulator, broadly speaking, stress-testing enables regulators *inter alia* to probe the resilience of financial systems to emerging threats to financial stability and individual firms.

[14] We flag that the International Organisation of Securities Commissions ("IOSCO") has published Guidance on Cyber Resilience for Financial Market Infrastructures (June 2016).

[15] We flag that the Basel Committee on Banking Supervision ("BCBS") has published Principles for Operational Resilience (August 2020).

[16] We flag that the Basel Committee on Banking Supervision ("BCBS") has published Stress Testing Principles (October 2018).

Appendix II – Jurisdictions with AI-Specific Regulations, Legislation and Frameworks

Below is a non-exhaustive list of jurisdictions that have enacted, or are in the process of enacting, AI-specific regulations, legislation, and frameworks. In addition, several other jurisdictions are anticipated to introduce similar AI-specific legislation in the future, such as India, Indonesia, Taiwan, and Thailand.

GFMA considers that the extensive body of existing technology-neutral, principles-based, outcomes focused regulations and guidance that apply to financial entities are sufficient to address the use of AI in capital markets. However, to the extent that there are concerns around the ability of such existing requirements to address any potential novel AI-related risks, there is a relatively new body of overarching AI-specific regulations, legislation, and frameworks that also apply[17]. **If local jurisdictions also enact new standards specifically aimed at AI, it will only introduce a third layer of legal requirements that constituents would have to address when using this technology, which could detrimentally impact their ability to realize the benefits of AI**.

Further, financial entities already face challenges in navigating these overlapping regimes, as the scope and content of these overarching AI requirements vary - sometimes significantly - by jurisdiction. **Introducing additional AI-specific regulations for capital markets could cause further fragmentation if they are inconsistent with, or rendered redundant by, such existing requirements.**

Jurisdiction	AI-Specific Regime
Brazil*	Bill No. 2338/2023 to regulate Artificial Intelligence
Canada*	Bill C-27 – the Digital Charter Implementation Act, 2022
Chile*	Exempt Resolution No. 33 – Law to Regulate Artificial Intelligence System, Robotics and Similar Technologies (2023)
China	Administrative Measures for Generative Artificial Intelligence Services (2023)
EU	Regulation 2024/… laying down harmonized rules on artificial intelligence (the Corrigendum – the "EU AI Act")
Hong Kong	HKMA's High-level Principles on Artificial Intelligence (2019)
Japan	AI Guidelines for Business Ver 1.0 (2024)
Mexico*	Law for the Ethical Regulation of Artificial Intelligence for the Mexican United States (2023)
Philippines*	Bill 7396 - Artificial Intelligence Development Authority Bill
South Korea*	Act on Promotion of AI Industry and Framework for Establishing Trustworthy AI (2023)
U.S.	NIST AI Risk Management Framework

** Denotes countries whose AI legislation is in proposal stage (as of the date of this letter) and has not passed through the respective legislative or parliamentary process.*

[17] That some of these are only non-binding frameworks (including principles and guidance) suggests that certain regulators consider that existing technology-neutral laws already sufficiently address AI-related risks such that additional binding legislative measures are not required.