Board/2025/017

Artificial Intelligence in Capital Markets: Use Cases, Risks, and Challenges

CONSULTATION REPORT

The Board of the
International Organization of Securities Commissions

CR/01/2025 March 2025

Copies of publications are available from
The International Organization of Securities Commissions website

iosco.org

Feedback to the Consultation Process

IOSCO welcomes input from the public, including financial market participants, AI developers, academics, researchers, public policy experts, and other interested parties, on the content of this Report and other potential areas of focus going forward to AIWGConsultation@iosco.org **on or before April 11, 2025**.

Your comment letter should indicate prominently that it is a Public Comment on IOSCO's Report *Artificial Intelligence in Capital Markets: Use Cases, Risks, and Challenges*. All comments received will be made available publicly unless anonymity is specifically requested. Comments will be converted to PDF format and posted on the IOSCO website.

Copies of publications are available from
The International Organization of Securities Commissions website

iosco.org

Table of Contents

I. Executive Summary

This report is the result of a two-phased approach by IOSCO through its Fintech Task Force (FTF) to develop a shared understanding among IOSCO members of the issues, risks, and challenges that emerging artificial intelligence (AI) technologies used in financial products and services may pose to investor protection, market integrity, and financial stability, and to assist IOSCO members as they consider regulatory responses.

Since the publication of IOSCO's most recent report on AI in 2021, AI technologies have undergone significant developments, including through the emergence of large language models and generative AI systems. Recent advancements in AI technologies have expanded the range of AI applications in financial markets, bringing potential benefits but also potential risks.

In 2024, IOSCO FTF's AI Working Group (AIWG)[1] conducted research, through surveys, stakeholder outreach, and literature reviews, to gather information on current and potential future uses of AI systems in financial products and services.

Based on this work, IOSCO found that:

- Firms are increasingly using AI systems to support decision-making processes in applications and functions such as robo-advising, algorithmic trading, investment research, and sentiment analysis. AI use cases also are expanding to enhance surveillance and compliance functions, particularly in anti-money laundering (AML) and counter-terrorist financing (CFT) measures.

- Firms are using or considering using recent advancements in AI to support internal operations and processes through task automation; to enhance communications; and to improve risk management functions.

- Risks most commonly cited to IOSCO during its information-gathering efforts with respect to the use of AI systems in the financial sector include risks from malicious uses of AI; AI model and data considerations; concentration, outsourcing, and third-party dependency; and interactions between humans and AI systems.

[1] The AIWG is led by staff from the Unites States Securities and Exchange Commission with members from the staff of the Australian Securities and Investments Commission; Brazil's Comissão de Valores Mobiliários; the European Securities and Markets Authority; France's Autorité des Marchés Financiers; Hong Kong's Securities and Futures Commission; the Securities and Exchange Board of India; the Central Bank of Ireland; Japan's Financial Services Agency; the Securities Commission Malaysia; Mauritius' Financial Services Commission; the Ontario Securities Commission; Québec's Autorité des Marchés Financiers; the Monetary Authority of Singapore; Spain's Comisión Nacional del Mercado de Valores; the Netherlands' Authority for the Financial Markets; the United Kingdom's Financial Conduct Authority; and the United States Commodity Futures Trading Commission.

- Industry practices are evolving, with some financial institutions incorporating AI into existing risk management and governance structures, and others establishing bespoke AI risk management and governance frameworks.

- Regulatory responses to the use of AI in the financial sector are also evolving, with some regulators applying existing regulatory frameworks to AI activities, and others developing bespoke regulatory frameworks to address the unique challenges posed by AI.

The next phase of IOSCO's AI work will be to consider, if appropriate, the development of additional tools, recommendations, or considerations to assist IOSCO members in addressing the issues, risks, and challenges posed by the use of AI in financial products and services. IOSCO will continue to play a coordinating role with regard to AI developments in the financial sector and to engage with other relevant international organizations, such as the Financial Stability Board (FSB).

II. Introduction

Background

In 2021, IOSCO released a report addressing the use of AI by market intermediaries and asset managers (the 2021 AI Report).[2] The 2021 AI Report identified key potential risks related to AI and included guidance to assist IOSCO members in supervising market intermediaries and asset managers that use AI. The 2021 AI Report highlighted the transformative nature of AI technologies relating to investment strategies, operational efficiency, and the development of new financial products. It also identified key AI-related challenges that IOSCO members may face, including with respect to governance and oversight; algorithm development, testing, and ongoing monitoring; data quality and bias; transparency and explainability; outsourcing; and ethical concerns. In its 2021 AI Report, IOSCO published six measures that reflect expected standards of conduct by market intermediaries and asset managers using AI (*see* Annex I). The 2021 IOSCO AI Report was the most comprehensive IOSCO publication to date that discusses the potential risks, issues, and challenges posed by AI systems in the financial sector. However, it is not the sole IOSCO publication that may relate to the use of AI technologies in the financial sector. Other IOSCO publications also discuss AI-related topics as they relate to outsourcing, robo-advisory services, and investor education, among other topics (*see* Annex II).

While the 2021 AI Report provided initial guidance to assist IOSCO members in supervising market intermediaries and asset managers that utilize AI systems, it acknowledged that the use of AI would likely increase as AI technologies advance and that regulatory frameworks may need to evolve in tandem with the technologies to address associated emerging risks. The 2021 AI Report, therefore, noted that the findings and guidance that it contained may need to be reviewed and refreshed to remain up to date. To that end, and considering recent developments, this report builds upon the observations of the 2021 AI Report, incorporating data on the latest developments in technologies, industry practices, and regulation. Its goals are to provide current and forward-looking insights about AI's role in financial markets; to report on industry efforts to define and implement policies and procedures around the use of AI systems in financial products and services; and to identify current regulatory approaches.

Since the publication of the 2021 AI Report, the landscape of AI systems in financial products and services has continued to evolve, enabled by innovations and developments in theory, hardware, software, algorithmic efficiency, compute power, data, and end-user applications. Among other advancements in AI technologies have been the emergence of significant foundation models and large language models (LLMs).

[2] IOSCO (2021), *The Use of Artificial Intelligence and Machine Learning by Market Intermediaries and Asset Managers, Final Report*, OICU-IOSCO, FR06/2021, available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD684.pdf.

Such advances, in turn, created synergies that have enabled the development of more complex system architectures, such as improved "Retrieval Augmented Generation" (RAG) and "agentic" systems.[3]

OpenAI's November 2022 release of the "ChatGPT" text-generating chatbot represented a significant breakthrough and facilitated the accessibility to AI by non-technical users. The ability of such chatbots to engage in human-like conversations has highlighted advancements in the processing and generation of language and content that enables the development of new and unprecedented applications. The availability of instruction-tuned and embedding models through easily accessible application programming interfaces (APIs) has decreased the technical challenges that previously existed for integrating cutting-edge models in testing and production environments. AI technologies like these chatbots and their underlying LLMs can ingest and process vast amounts of data in formats that previously proved challenging, and can extract meaningful insights from semi-structured text, unstructured text, and multimodal data from diverse sources. Moreover, they can generate new content, dramatically simplify the way humans interact with technology, and use embeddings, which capture semantically meaningful features of the input data for other downstream tasks (such as classification and search).

While emerging AI technologies rely on increasingly complex techniques, their user interfaces tend to be incongruously simple. Human interactions with AI chatbots can seem increasingly intuitive and anthropomorphized (made more "humanlike") through natural language prompting, generative output, and personalized communication. With advancements in AI technologies, users can engage with technology in humanlike "conversations," "interactions," and "relationships."[4] LLMs can process natural language prompts to provide responses in a relatively convincing and natural manner—though the responses are not always factually accurate. AI technologies have long been integrated into consumer digital engagement applications, and advancements in AI technologies are becoming more ubiquitous in such applications as well.[5]

A range of financial institutions, including broker-dealers, asset managers, and exchanges, among others, are seeking to leverage AI technologies to enhance operational efficiencies and create market opportunities, and it seems likely that financial product and service providers will broaden their adoption of AI technologies. Demand, investment, and competition are driving adoption, with some market participants recognizing the risks associated with not adopting AI technologies or failing to do so quickly

[3] "RAG" is a technique where an AI-powered chatbot retrieves data from a database that is most relevant to the user's domain and prompt(s). This data is presented in an LLM's context window to provide a "grounded" output. *See, e.g.*, https://cloud.google.com/use-cases/retrieval-augmented-generation. "Agentic" AI systems refer to "AI systems that build on advanced LLMs … and are endowed with planning capabilities, long-term memory and, typically, access to external tools such as the ability to execute computer code, use the internet, or perform market trades." *See* BIS Working Papers No 1194, *Intelligent Financial System: How AI is Transforming Finance*, I. Aldasoro, L. Gambacorta, A. Korinek, V. Shreeti, and M. Stein (Jun. 2024) at 7, available at https://www.bis.org/publ/work1194.pdf (BIS AI Paper); *id*. at n.6 ("Agency" refers to "the degree to which an AI system acts directly in the world to achieve long-horizon goals, with little human intervention or specification of how to do so.").

[4] Humans can interact with an LLM interface with, for example, a single prompt, a series of prompts, and detailed prompts where a user can specify an expected output and provide grounding (facts) in the prompts.

[5] Types of AI technologies are used in virtual assistants, map and transportation programs, word processing and email apps, wearable health apps, advertising and content recommendations, and facial recognition tools, to name a few.

enough. Rapidly advancing developments include a focus on the use of AI agents, which are AI systems that can take actions—autonomously, with potential real-world consequences—on behalf of a user, with little or no human intervention.

AI technologies can be used in powerful ways, and if appropriately harnessed, could transform financial markets to enhance investor access and engagement, while also potentially promoting investor protection and market integrity. However, as the 2021 AI Report recognized, the use of AI technologies within financial markets may also create or amplify certain risks, which could impact the efficiency and integrity of financial markets and result in investor harm. In light of recent developments, policymakers and regulators across the globe have been revisiting their examination of the benefits and risks that may arise through the use of evolving AI technologies in financial markets.[6] This IOSCO report, in part, builds upon the findings of prior publications, but is focused more specifically on how AI technologies are reportedly being used in financial products and services and on identifying the implications of these uses for market integrity and investor protection—the core mission of IOSCO and its members. As with the advent of other transformative technologies, market regulators must seek to understand a changing landscape; assess potential benefits, risks and challenges based on a clear-eyed view of the facts and evidence; and consider whether risks arising from AI systems used in financial products and services are well-covered under existing regulatory frameworks or whether there is a need to enhance frameworks to address the risks of emerging AI-related activities.

Objective of the Report

In March 2022, IOSCO established the FTF to lead IOSCO's work developing, overseeing, delivering, and implementing IOSCO's regulatory agenda with respect to Fintech. Considering the advancements in AI technologies since the 2021 AI Report, the FTF established the AIWG as a dedicated working group in 2024.

The objective of the AIWG work and this Report is to develop a shared understanding among IOSCO members of the issues, risks, and challenges presented by emerging AI technologies used in financial products and services, seen through the lens of investor protection, market integrity, and financial stability, and to identify how some IOSCO members have begun to respond to recent developments. This Report builds upon the 2021 AI Report and seeks to put these developments in the appropriate context by taking

[6] For example, the Organisation for Economic Co-operation and Development (OECD) has published a number of AI-related reports, one of which analyzed current and potential use cases of AI in finance, their risks, and the policy frameworks applicable to those use cases across OECD and non-OECD jurisdictions. *See* OECD (2024), *Regulatory Approaches to Artificial Intelligence in Finance*, *OECD Artificial Intelligence Papers*, No. 24, OECD Publishing, Paris, available at https://doi.org/10.1787/f1498c02-en (OECD Report); *see also* OECD (2023), *Generative Artificial Intelligence in Finance*, *OECD Artificial Intelligence Papers*, No. 9, OECD Publishing, Paris, available at https://doi.org/10.1787/ac7149cc-en. The International Monetary Fund (IMF) published its Global Financial Stability Report, containing a chapter on AI and its implications for financial markets. *See* IMF (2024), *Global Financial Stability Report, Ch. 3, Advances in Artificial Intelligence: Implications for Capital Market Activities*, available at https://www.elibrary.imf.org/display/book/9798400277573/9798400277573.xml?rskey=GCTYLO&result=2 (IMF Report). The Financial Stability Board (FSB) published a report that provides a high-level overview of recent developments in AI, along with an assessment of their potential financial stability implications. *See* FSB (2024), *The Financial Stability Implications of Artificial Intelligence*, available at https://www.fsb.org/uploads/P14112024.pdf (FSB Report).

into account how the use of AI systems in financial products and services has changed since the 2021 AI Report, examining current and proposed uses of AI systems in financial products and services, and seeking to distil the novel and unique aspects of these emerging developments into themes around which IOSCO members can evaluate potential policy responses.

Considering the rapid pace of developments in AI technologies, IOSCO is taking a two-phased approach to its work. In this first phase, IOSCO explored current and near-term use cases and value propositions by market participants and analyzed related issues, risks, and challenges through conducting research, surveys, and stakeholder outreach. IOSCO is publishing this Report based on the results of that work to provide a shared basis for understanding the current and near-term use cases by market participants that incorporate, or may in the future incorporate, AI technologies, as well as the issues, risks, and challenges they present. In the second phase, based on the findings in this Report, and as appropriate, IOSCO may develop tools, considerations, or recommendations that will provide guidance to IOSCO members on how to address the issues, risks, and challenges posed by AI technologies.

Methodology for the Report

In developing a shared understanding of these issues and drafting this Report, IOSCO was mindful that the development and use of AI technologies is not limited to financial market participants, but rather cuts across and relies heavily on the expertise and services provided by other sectors. Thus, IOSCO not only gathered evidence from its own research, regulatory surveys, and industry surveys, but it also engaged in outreach with experts from beyond IOSCO's membership and traditional market participants, as summarized below. The findings in this Report are based primarily on information gathered through:

IOSCO Member and SRO Surveys: Between May and June 2024, IOSCO surveyed its FTF members and a number of Self-Regulatory Organizations (SROs) (IOSCO FTF Member/SRO Survey) to collect information about how market regulators assessed that AI systems and technologies were being used, or may be used in the near future, in financial markets in their jurisdictions, with a particular focus on recent advancements in AI systems and technologies. 24 IOSCO members, each representing one jurisdiction, responded, out of a total of 33 IOSCO members. Six SROs responded to the survey, representing five jurisdictions. The surveys requested jurisdictional information regarding, among other things: the respondents' respective working definitions of AI; developments in the use of AI; AI uses observed in financial products and services; potential impacts to market integrity, investor protection, and financial stability (including data related and model related) from these uses; broader risks and challenges of AI; AI-related frauds and scams; and supervisory responses and regulatory engagement with market participants relating to the use of AI in the financial sector (including investors, service providers, technologists, researchers, academics, public policy advocates, and others). The SRO survey recipients were asked additional questions about their own use of AI.

Affiliate Members Consultative Committee (AMCC) Member Survey: The IOSCO AMCC is comprised of 74 IOSCO affiliate members. The members represent securities and derivatives markets and other market infrastructures, SROs, investor protection funds and compensation funds, as well as other bodies with interest in securities regulation. There are currently 35 jurisdictions represented in the AMCC, which also includes 14 regional or international

associations. Between September and October 2024, the IOSCO AMCC distributed a survey (AMCC Survey) to obtain their members' views on how AI was being used or may be used in the near future in financial markets.[7] Certain trade associations of the AMCC distributed the surveys to their respective memberships. A total of 184 respondents submitted survey responses. The demographics of those respondents and certain details of their responses are described in Annex III.

Stakeholder Engagement Roundtables: Between May and November 2024, IOSCO hosted four roundtables – across Europe, North America, and Asia. These roundtables included a variety of stakeholders that cut across sectors, including representatives from the financial industry, the technology sector (including software, hardware, and data computing companies), investor and public policy advocates, and academics. During each roundtable, participants shared their experiences and insights relating to technological advances in AI, current and potential financial services use cases of AI, and investor protection, market integrity, and financial stability risks relating to uses of AI.

Terminology

Across the globe, authorities have adopted or used varying definitions of "AI" in various contexts. For the purposes of this Report, a common definition is not necessary; rather, it is more important to have a common understanding of the types of technologies that are referred to in the Report.

For the purposes of the surveys, IOSCO used the following OECD definition:

> ***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.[8]***

Although in its information-gathering exercise IOSCO used a broad definition to capture information about the many types of AI technologies, IOSCO found that the benefits and risks of AI technologies used in financial products and services are highly dependent on the type of AI technology used, for what purpose it is used, and the way it is deployed. IOSCO also found that it is difficult to clearly delineate types of AI technologies and uses, due to the complexities of AI systems, differences in lexicons, data and knowledge gaps, and evolving developments. However, as explained above, IOSCO sought to identify and analyze advancements in AI technologies since the 2021 AI Report, and their attendant issues, risks, and challenges. Since the time of the 2021 AI Report, attention appears to have focused on the emergence of non-deterministic AI models. Other advancements have also occurred, and future advancements will no doubt continue to occur.

7 AMCC SRO members were surveyed by IOSCO, as part of the IOSCO Member/SRO Survey, as described above.

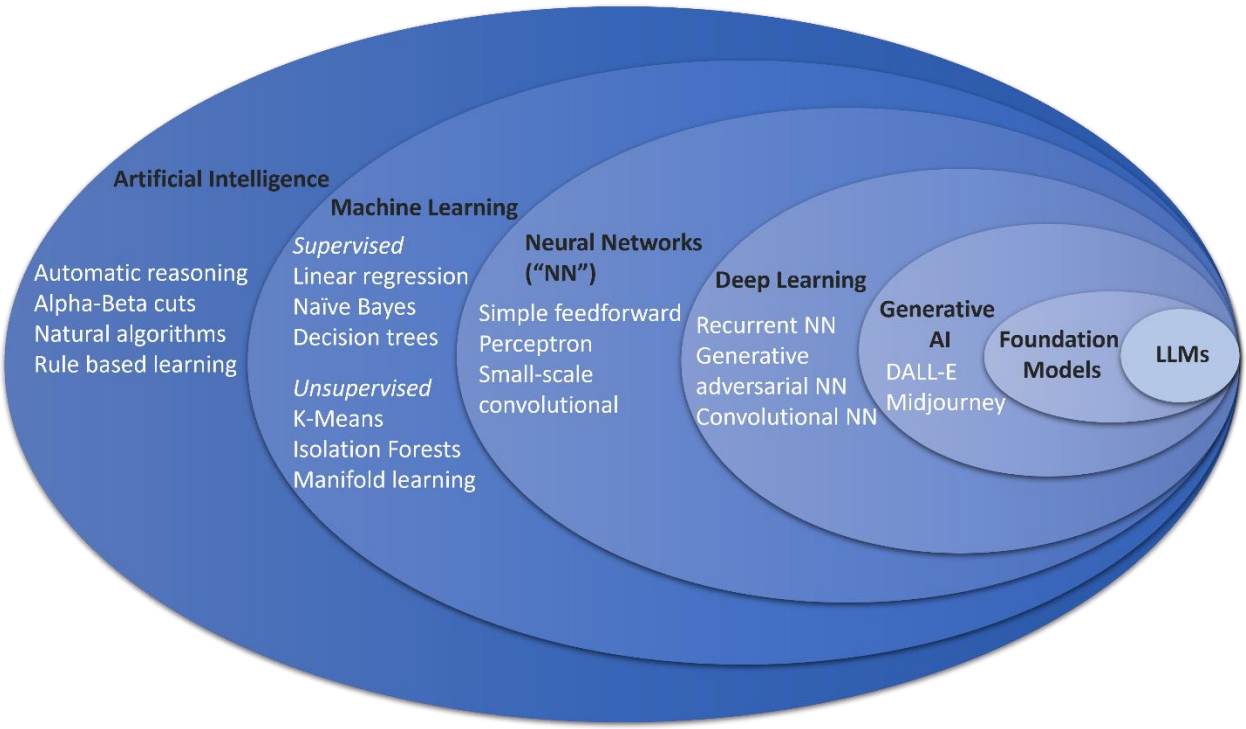
8 Definition of AI system from OECD AI Principles Overview, available at https://oecd.ai/en/ai-principles.

For the purposes of this Report, "**AI**" or "**AI technologies**" generally refers to all types of AI technologies. These include technologies that typically analyze historical data, identify patterns, and can make predictions and extract insights using algorithms and optimization techniques, and that enable contemporary natural language processing (NLP). These technologies include logical reasoning, predictive analytics, statistical methods, and machine learning (ML) models. Some AI systems perform a specific task based upon curated, domain-specific training data, and the predictions or outputs generated by such technologies are typically deterministic (i.e., they usually produce a consistent output for a given input). Some other AI systems (for the purposes of this report, **recent advancements in AI**), including deep learning models, use AI technologies that have enhanced previous capabilities in various tasks, such as by enabling the processing and synthesizing of vast amount of data from diverse sources, and that can augment existing decision-making applications described above or be used in different applications. For example, **Generative AI** (**GenAI**) systems[9] can utilize **LLMs**, multi-modal models (able to process and produce text and graphical content), and **Foundation Models** trained on vast datasets, to generate text (including programming code), audio, images, and video. Also in this category are **Representation Learning Models**, which generate outputs that can be interpreted as representing semantic meaning or understanding of the data inputted, and **General Purpose AI** systems, which have been designed to perform a range of tasks and not be limited to a specific task or domain.[10] These **recent advancements in AI** have led to non-deterministic systems (i.e., their outputs rely on probabilistic algorithms), producing a range of possible outputs for a given input.[11]

[9] GenAI systems "create new content – including text, image, audio and video – based on their training data and in response to prompts." P. Lorenz, K. Perset, and J. Berryhill (2023*), Initial Policy Considerations for Generative Artificial Intelligence*, OECD Artificial Intelligence Papers, No. 1, OECD Publishing, Paris, https://doi.org/10.1787/fae2d1e6-en.

[10] On the technological horizon: **Artificial General Intelligence (AGI)** refers to "AI systems that can essentially perform all cognitive tasks that humans can perform"; and **Transformative AI** is "AI that is sufficiently capable so as to radically transform the way our economy and our society operates, for example, because they can autonomously push forward scientific progress including AI progress, at a pace that is much faster than what humans are used to, or because they significantly speed up economic growth." BIS AI Paper, *supra* n.3 at 8. **Artificial Super Intelligence (ASI)** refers to AI that surpasses human intelligence. *See, e.g.*, https://www.ibm.com/think/topics/artificial-superintelligence. The future trajectory of AI technology is difficult to predict; however, continuing advancements, as well as **Distributed Ledger** and **Quantum Computing Technologies**, may impact AI applications in the future. These frontier technologies may be alluded to in this Report, but they are not the core focus of the Report.

[11] Again, the categorization of different forms of AI is not always clear-cut. Boundaries can be blurry and definitions imprecise. For instance: there is no consensus on exactly how many layers a neural network would need to be in order for it to count as deep learning; the production of synthetic media utilizing GenAI could conceivably be achieved with algorithms other than neural networks (although in practice neural networks have proven to be most successful); and foundation models need not always be generative (e.g., text embedding models produce a semantically-meaningful vector representation of the inputted text data—this contrasts with autoregressive decoder-only transformers, like the GPT series of models, which generate new text following a user's prompt).



A Representation of Various Types of AI; Source: IOSCO AIWG

Structure of the Report

In Section III, the Report briefly outlines the evolution of the use of AI technologies in capital markets and draws primarily upon survey responses to detail common use cases for AI by market participants, as reported by survey respondents, including to what extent recent advancements in AI (as defined above for the purposes of this Report) have been incorporated into those use cases.

Section IV of the Report details risks, challenges, and other issues associated with AI technologies—building on a similar discussion from the 2021 AI Report. In particular, this section focuses primarily on recent advancements in AI, and outlines what these developments may mean for investor protection, market integrity, and financial stability.

Section V analyzes how certain market participants are approaching the development, deployment, and maintenance of AI systems, and how recent advancements in AI are impacting certain market participants' considerations for policies, procedures, and controls around their use of AI. Section V also identifies certain risk management and governance principles that are emerging in the industry from these observations.

In Section VI, the Report provides an overview of surveyed IOSCO members' existing and proposed responses to the use of AI systems in the financial sector, along with specific examples of IOSCO members' responses. The section also examines efforts by regulators to assess the resources and skills required to analyze and supervise market participants' uses of AI. The section also outlines actions taken by IOSCO

members to address the use of AI by market participants by enforcing existing rules and regulations. The section reports primarily on the results of IOSCO's information-gathering efforts; however, this Report does not endorse a particular approach, nor does it make policy recommendations.

The Report concludes in Section VII by noting considerations and areas of potential future exploration by IOSCO to best address the issues, risks, and challenges identified in the Report.

III. AI Use Cases in Capital Markets

Introductory Overview

The use of AI technologies in capital markets is not a recent phenomenon. Over the years, AI technologies have been used and integrated into various aspects of financial markets. The 2021 AI Report highlighted the use of AI by market intermediaries and asset managers at that time, in functions including advisory and support services, risk management, client identification and monitoring, selection of trading algorithms, and portfolio management.[12] Over the past three years, AI technologies have experienced significant innovations, investment, and interest. As market participants explore and test new possibilities, and as AI technologies continue to advance, the range of AI uses in capital markets has expanded and likely will continue to expand.

On the basis of IOSCO's information gathering through its research, surveys, and roundtables, IOSCO found that firms are investing in AI technologies and that these technologies are increasingly being explored, piloted, and adopted in various activities in capital markets.[13] Current AI applications at financial intermediaries typically fall within three broad categories: internal operations and processes; client interactions; and trading and investing product and process enhancements. IOSCO found that, in general:

- AI technologies have become increasingly common to support decision-making processes, in applications and functions such as robo-advising, algorithmic trading, investment research, and sentiment analysis. Regulated firms and third-party providers are also using AI technologies to enhance surveillance and compliance functions, particularly in anti-money laundering (AML) and counter-terrorist financing (CFT) related systems.

- Recent advancements in AI are being looked at by firms to support internal operations and processes through the automation of certain tasks, such as coding; information extraction; text classification, clustering, summarization, transcription, translation, and drafting; and enhancing communication with clients through conversation agents (chatbots). With respect to GenAI, in particular, capital markets participants appear to have prioritized internal, lower-risk implementations that focus on enhancing internal productivity, generating insights, or improving risk management, rather than in customer-facing applications.

[12] *See supra* n.2*; see also* IOSCO (2020) *The Use of Artificial Intelligence and Machine Learning by Market Intermediaries and Asset Managers Consultation Report,* available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD658.pdf, at 4 (detailing the work of several IOSCO workstreams that had considered the use of AI in financial markets at that time, proposing guidance to address potential risks and harms, and seeking public input).

[13] Approximately half of all AMCC Survey respondents reported having invested in AI (50%) or having adopted AI (49%), with AI use cases currently in pilot (8%) or production (41%). *See* Annex III for more information.

These findings, and a comparison to the findings that informed the 2021 AI Report, are summarized below.

2021 AI Report

At the time of the 2021 Report, market intermediaries were deploying AI for:

- advisory and support services – most robo-advisors or automated investment advisors were using simple, rules-based algorithms to generate potential advice or asset allocation suggestions for the investment advisor to review
- risk management – market intermediaries were using ML-based risk management systems for, e.g., credit risk monitoring, visualizing market risk, and gauging liquidity risk
- client identification and monitoring – ML allowed market intermediaries to automate client onboarding, fraud detection, AML and CFT measures, and cyber-attack monitoring
- selection of trading algorithm – market intermediaries offered software solutions (called "algo wheels") that selected a trading strategy and/or brokers, depending on the market situation and trading objectives, to achieve best execution
- asset management/portfolio management – supervised learning was used for small-scale pattern recognition, and simple prediction models were used to aid in trading decisions

At the time of the 2021 report, the use of AI and ML by asset managers appeared to be in the nascent stages and was mainly used to support human decision-making in:

- optimizing portfolio management
- complementing human investment decision-making processes by suggesting investment recommendations
- improving internal research capabilities and back-office functions
- facilitating order execution, broker selection, and order routing

Current Report: AI

The AIWG identified the following common AI use cases across a variety of financial services firms:

- Firms were increasingly using AI systems to support decision-making processes in applications and functions such as robo-advising, algorithmic trading, investment research, and sentiment analysis
- Firms were also using AI to enhance surveillance and compliance functions, particularly in AML and CFT measures

Current Report: Advancements in AI

Financial services firms were using or considering LLMs and GenAI uses in the following manner:

- supporting internal operations and processes through task automation
- enhancing communication via chatbots
- improving risk management functions

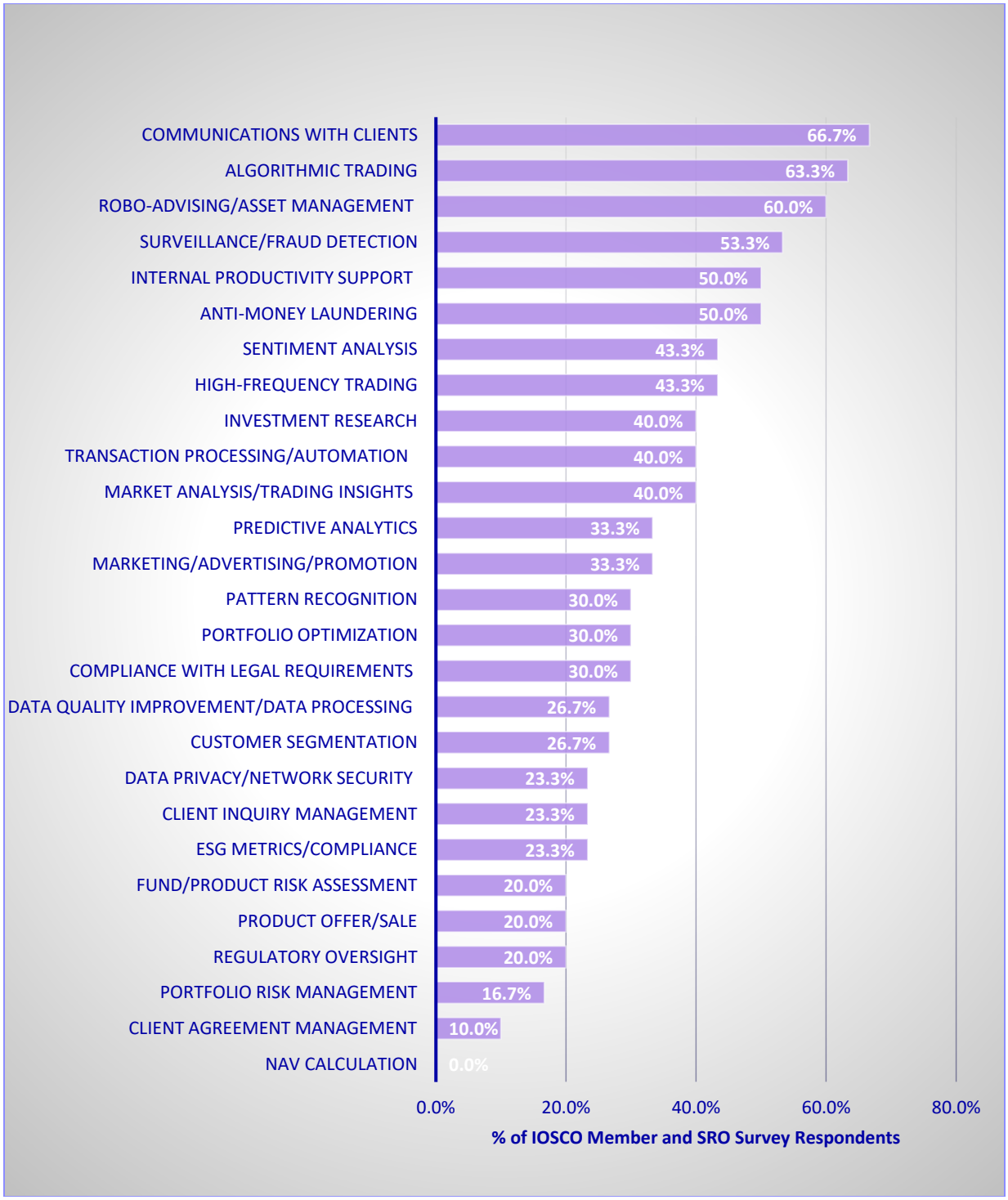
Overview of Survey Results on AI Use Cases

Given limitations inherent in the survey process, the following results should be interpreted as indicative rather than definitive and are not meant to be an exhaustive list of uses of AI systems all financial market participants across all jurisdictions.

IOSCO Member/SRO Survey Responses

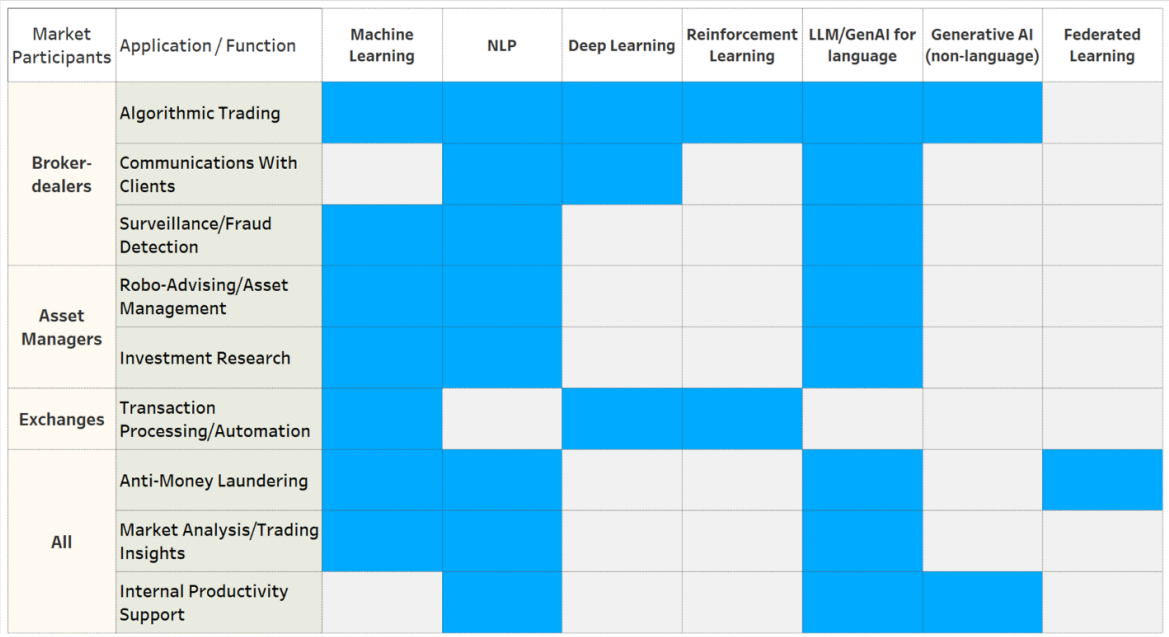
IOSCO Member/SROs Survey recipients were asked to identify the functions and applications where they observed that AI technologies were being used, or may be used in the near future, by market participants in their respective jurisdictions. 30 IOSCO Member/SRO Survey respondents answered based on a pre-defined list of functions and applications. The results are depicted in the chart below, with the most common use cases observed relating to communications with clients, algorithmic trading, and robo-advising and asset management, followed by surveillance and fraud detection, internal productivity support, and anti-money laundering.

Most Frequently Cited Current and Near-Term AI Uses Observed in Market Participants by IOSCO Member/SRO Survey Respondents



The IOSCO Member/SRO Survey recipients were also asked to identify the type of AI they observed being used by market participants in their respective jurisdictions for specific given uses. The following diagram depicts the results of that survey question, grouped by market participant.

Type(s) of AI Technology[14] Applied to Various AI Uses, and Grouped by Market Participant Type, as Identified by IOSCO Member/SRO Survey Respondents



Market Participants	Application / Function	Machine Learning	NLP	Deep Learning	Reinforcement Learning	LLM/GenAI for language	Generative AI (non-language)	Federated Learning
Broker-dealers	Algorithmic Trading	■	■	■	■	■	■	
	Communications With Clients		■	■		■		
	Surveillance/Fraud Detection	■	■			■		
Asset Managers	Robo-Advising/Asset Management	■	■			■		
	Investment Research	■	■			■		
Exchanges	Transaction Processing/Automation	■		■	■			
All	Anti-Money Laundering	■	■			■		■
	Market Analysis/Trading Insights	■	■			■		
	Internal Productivity Support		■			■	■	

[14] The AI methods employed in these use cases encompass a range of techniques, including but not limited to:

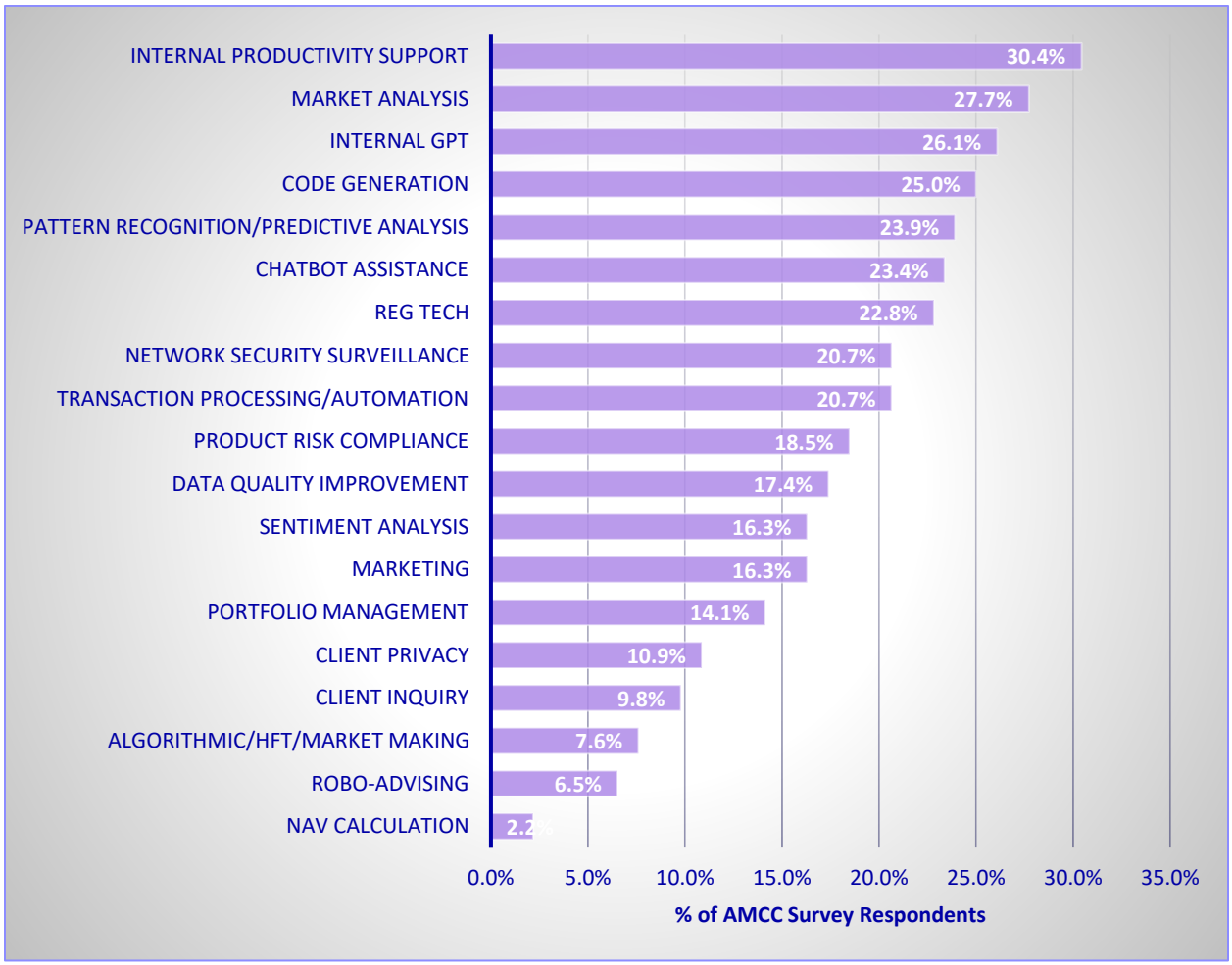
- Machine Learning (an AI system designed to learn from experience without being explicitly programmed to do so, e.g., simpler" ML models such as regressions, decision trees, and k-nearest neighbors);
- Deep Learning (an AI system involving neural networks (computing systems) with many layers of units, inspired by the structure of the human brain, e.g., Artificial Neural Networks, Convolutional Neural Networks, and Recurrent Neural Networks);
- Reinforcement Learning (an AI system that learns from receiving feedback, e.g., Q-learning);
- Natural Language Processing (techniques that enable computers to recognize, process, and generate text and speech, e.g., tokenization, TF-IDF, Latent Dirichlet Allocation, word2vec, GenAI for language tasks, and LLMs);
- Generative AI for non-language tasks (e.g., multi-modal systems); and
- Federated Learning (technique of training models on decentralized data distributed across multiple devices).

This list of AI methods is not exhaustive. In some cases, IOSCO applied judgment to infer the likely AI methods used based on the described use cases from the survey response. (The GenAI (non-language) identified with respect to algorithmic trading, was identified as the development of new trading algorithms that can better predict market movements and simulate various trading scenarios, e.g., by reading market sentiment, and the development of multi-modal systems that integrate GenAI techniques for enhanced algo trading execution.)

AMCC Survey Responses

AMCC Survey respondents, across all demographics, identified internal productivity support as the most frequent use case in their organization, followed by market analysis, internal chatbots, and code generation.

Current and Near-Term AI Uses Reported by AMCC Survey Respondents



Description of Common AI Uses by Market Participants[15] as Identified by Survey Respondents

This section provides a more detailed examination of IOSCO findings concerning AI use cases by market participants that were most frequently identified by survey respondents. The details are based on the IOSCO Member/SRO Survey responses and roundtables, which provided more detail than the AMCC Survey responses. Where possible, the use of recent advancements in AI is separately highlighted. It is important to emphasize that actual AI usage may vary across different jurisdictions and, although use cases discussed below have been associated with particular types of market participants for purposes of this Report, based on the survey responses, these use cases may be present among other participants across capital markets.

Capital Market Participants Overall

Based on survey results, the uses of AI that were reported by IOSCO Member/SRO Survey respondents to be most observed across market participants, including broker-dealers, asset managers, and exchanges, were:

- Anti-Money Laundering and Counter Terrorist Financing (AML and CFT) (50%)
- Internal Productivity Support (50%)
- Market Analysis and Trading Insights (40%)

Similarly, AMCC Survey respondents collectively reported internal productivity support (30%) and market analysis (28%) as the most common AI use cases. AI used for regulatory purposes, such as regulatory, compliance, and reporting obligations (RegTech) (including AML and KYC, surveillance, and fraud detection) was also a frequently reported use case (23%). Non-Growth and Emerging Markets ("Non-GEM") AMCC Survey respondents also frequently cited internal chatbots.

AML and CFT

IOSCO member/SRO Survey respondents reported that they observed market participants using AI to enhance the effectiveness of AML and CFT measures, particularly, and compliance more generally, including to identify suspicious transactions. For AML compliance, customer onboarding, and due diligence, respondents observed that market participants use ML models to perform pattern recognition and anomaly detection in surveillance software. They also use NLP to enhance the interpretation of

[15] IOSCO scoped market participant types to regulated entities in the capital markets, e.g., broker-dealers, asset managers, exchanges, and other financial market intermediaries. For purposes of this Report, broker-dealers broadly include brokerages, investment banks, institutional and retail brokers, and market makers. Asset managers broadly include fund managers, investment advisers, and hedge funds. Financial exchanges broadly include securities and derivatives exchanges, and other financial market intermediaries broadly include clearing houses, financial market infrastructures, and trade repositories.

unstructured data and to facilitate name screening and news analysis. These technologies supported the investigation process by analyzing client behaviors, prioritizing red flags and suspicious activities, and integrating insights from other sources such as news.[16]

These respondents reported that AI was also used in cybersecurity for vulnerability, threat, phishing, and anomaly detection; for automated response and authentication; in risk management and compliance surveillance activities; and to assist with the detection and prevention of frauds and scams. In such applications, AI can be used to help detect and analyze network traffic, prevent data leakage, segment customers by risk profile, prioritize alerts, and investigate activity.[17]

Market Analysis and Trading Insights

IOSCO member/SRO Survey respondents reported that they had observed various markets participants using ML and other AI techniques for market analysis, research, and sentiment analysis. These techniques were used to extract and process information and insights from diverse data sources, including financial, market, macro-economic, and social media data. They also reported market participants using ML models trained on historical data to forecast asset prices and liquidity, predict market trends, and identify anomalies and patterns such as non-linear interactions among numerous variables.[18]

Use of Recent Advancements in AI

IOSCO Member/SRO Survey respondents reported that they observed market participants using recent advancements in AI for internal productivity and to improve internal operations. Some of these respondents reported that market participants use these technologies for software development, back-office operations, automation, compliance, and human resources. More specifically, in software

16 Other recent reports corroborate these observations. *See, e.g.,* FSB Report, *supra* n.6, at 12 (financial institutions widely use AI to comply with AML and CFT requirements, facilitate investigations into sanctions evasion, to identify misuse of legal persons and legal arrangements, to uncover trade fraud and trade-based money laundering, and to detect tax evasion, fraud, scams, and money mules).

17 *Accord* United States Dept. of the Treasury (2024) *Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector* (U.S. Treasury AI Cybersecurity Report), available at https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf, at 12 ("AI-driven tools are replacing or augmenting the legacy, signature-based threat detection cybersecurity approach of many financial institutions. AI tools can help detect malicious activity that manifests without a specific, known signature. This capability has become critical in the face of more sophisticated, dynamic cyberthreats that may leverage legitimate system administration tools, for example, to avoid triggering signature detection.").

18 The IMF Report, based on outreach it conducted with market participants and regulators, reported a number of use cases in the investment process: the incorporation of alternative data sets, the development of forward-looking indicators, and market analysis. *See* IMF Report, *supra* n.6 at 6, 81. The IMF Report found that buy-side uses of AI included exploration of new asset classes, extraction of signals to support investment decisions, portfolio optimization and allocation, and back-office activities; sell-side uses included risk assessment, pricing and forecasting, customer service, and trade allocation automation. *Id*. at 81-82.

development, some firms were observed using LLMs to assist with coding tasks and documentation.[19] For back-office operations, some firms were observed exploring the use of LLMs to automate transaction summary generation and assist with documentation such as approval documentation. Some respondents reported that firms use techniques such as RAG to support employees in tasks involving searching, synthesizing, and summarizing information from internal knowledge databases. Additionally, some respondents reported that firms are experimenting with LLM tools that offer speech-to-text and video recognition for note taking and meeting summarization, as well as those that offer translation capabilities to facilitate cross-language communication.[20]

IOSCO member/SRO Survey respondents reported that they observed market participants using or exploring the use of recent advancements in AI for enhancing AML and CFT measures. For example, respondents reported observing LLMs being tested for AML investigators to conduct research on red flags and suspicious activities, as well as to automate and enhance the report writing for Suspicious Activity Reports (SARs).[21] The respondents also cited observed efforts to enhance surveillance measures in the financial industry through the development of joint systems that can be used by multiple financial institutions to share data and intelligence to mitigate types of threats utilizing AI and other technologies. One example given is the potential application of federated AI learning that would allow multiple

[19] The FSB Report observed an increase in use of AI in operations-focused applications such as capital optimization, model risk management, market impact analysis, and code generation. *See* FSB Report, *supra* n.6 at 11. It observed that AI was helping firms manage volatility and liquidity risk, optimize their regulatory capital requirements, improve information search and retrieval, assist with content generation (e.g., automated text, image, and video generation), assist with voice transcriptions (e.g., voice-to-text and text-to-summary service requests), and code generation or legacy code streamlining. *Id*. at 11. The IMF Report also noted that uses of AI by market participants included code writing and prototyping, and information extraction and summarization. *See* IMF Report, *supra* n.6, at 82. The OECD Report, based on the results of a survey of 49 OECD and non-OECD jurisdictions, discusses, *inter alia*, current and potential use cases of AI in finance as reported by survey respondents, most of whom regulate banks. The most frequently reported use cases identified in the OECD survey responses centered on customer relations, which includes marketing, profiling, personalization, and clustering. The second most frequently reported use cases centered on process automation, which includes claims and document processing, organization and management, and operational efficiency. *See* OECD Report, *supra* n.6 at 15. *See also AI: Beyond the Hyperbole, Plato* (Oct. 2024), available at https://static1.squarespace.com/static/6310c0b9bb63a25599f4418c/t/671a1bdff5a0a972a9a43617/1729764321806/AI+Beyond+the+Hyperbole+Final.pdf (research on the use of AI in Capital Markets among 49 firms, including asset managers, sell-side firms, and vendors. 40% were based in the UK, 27% in Europe, and 33% in the US, finding that the use of GenAI in trading is limited to post execution insights and pre-trade execution selection processes).

[20] IOSCO roundtables corroborated observations that LLMs are being used by financial firms in information and process management tasks, such as to summarize internal documents, to enable internal chatbots or helpdesks for employees to ask questions relating to internal operations or search across internal knowledge bases, to manage projects and workflow, to standardize business documentation, create meeting materials, and to translate documents into multiple languages, for code generation and analysis, and to convert code from one programming language to another.

[21] Industry reports also indicate that LLMs are used for fraud and cybersecurity threat detection, to analyze potential threats to a network or detect suspicious network patterns, and for anti-virus support, e-mail surveillance, behavioral analytics, data loss prevention, and phishing prevention. Some reports indicated firms are exploring the use of GenAI to create synthetic datasets to train surveillance systems. *See e.g.*, M. Hassanin, N. Moustafa, *A Comprehensive Overview of Large Language Models (LLMs) for Cyber Defences: Opportunities and Directions* (May 23, 2024), available at https://arxiv.org/html/2405.14487v1.

institutions to train LLMs and other deep learning systems collaboratively, which could potentially improve the detection rate of AML and CFT systems.

IOSCO Member/SRO Survey respondents also reported observing that RegTech providers have incorporated AI tools in surveillance and security solutions that could assist market participants to monitor client communications such as emails, calls, and mobile chat applications, and could raise alerts on suspicious communications for compliance review and investigation. Others reported that AI tools could help detect and contain threats; generate risk scores and summaries about threat behavior for further action; help analyze malicious code; and facilitate human interaction using natural language.[22]

Broker-Dealers

The uses of AI that were reported by IOSCO Member/SRO Survey respondents as most observed in broker-dealers in their respective jurisdictions, including brokerages, investment banks, institutional and retail brokers, and market makers, were:

- Communication with clients (67%)
- Algorithmic trading (63%)
- Surveillance and fraud detection (53%)

AMCC Survey respondents that were identified as broker-dealers most frequently cited the uses of AI in internal productivity support and for algorithmic trading or market making algorithms. Larger AMCC Survey respondents (reporting greater than $10M in approximate annual revenue or declining to disclose annual revenue) also frequently reported using AI for coding and internal chatbots.

Communication with Clients

IOSCO Member/SRO Survey respondents reported that AI-powered communication systems, particularly chatbots or virtual assistants, were used by market participants, including brokerage firms, to provide support for basic client query review and management. Such systems can automate review, classify queries for routing, and extract information from datasets to inform a response. While these systems can handle basic queries and operations, respondents noted that clients typically have the option to be transferred to

[22] Industry reports also indicate that LLMs are used for a number of compliance tasks, such as: assessing changes in compliance documents; writing and updating policies; assisting in the drafting of model validation documents; analyzing calls with clients to ensure they are compliant and to summarize potential customer complaints made in call centers; identifying and interpreting potential laws and regulations applicable to a business using publicly available sources; mapping regulatory requirements to business activities; generating regulatory reports; and in post-trade compliance, such as in trade surveillance and communications surveillance. *See e.g., Maximizing Compliance: Integrating Gen AI into the Financial Regulatory Framework/IBM* (Aug. 12, 2024), available at https://www.ibm.com/think/insights/maximizing-compliance-integrating-gen-ai-into-the-financial-regulatory-framework; *Implementing Financial Regulations Using Large Language Models,* B. Fazlija, M. Ibraimi, A. Forouzandeh, and A. Fazlija (Nov. 5, 2024), available at https://ssrn.com/abstract=5010694.

human operators for more complex matters that require human judgment or expertise. In some cases, these AI chatbots served as auxiliary tools for customer service representatives.

Algorithmic Trading

Some IOSCO Member/SRO Survey respondents observed AI systems being used to support algorithmic trading by various market participants, including institutional investors, investment banks, proprietary trading firms, and market makers. AI applications were observed to be integrated across the trading lifecycle, e.g., for processing market data, monitoring market movements, and identifying patterns; pre-trade analysis for trade routing and optimization, such as market impact analysis, broker selection, execution style, and choice of algorithm used; and assisting with pricing, trade execution, and post-trade analysis. Furthermore, predictive modelling, a form of supervised ML, was reportedly observed being used for signal processing, e.g., to predict future prices of financial instruments and for market sentiment analysis. It was noted, however, that complex AI algorithms require significant computational resources and can therefore have associated latency—this may make them inappropriate in many algorithmic trading contexts where speed of execution is especially important.

Surveillance and Fraud Detection

IOSCO Member/SRO Survey respondents reported observing market participants, in particular broker-dealers, using AI for surveillance and fraud detection. While traditional, rule-based approaches continue to be used by broker-dealers, some respondents noted that these approaches are limited by the complexity of markets and the constant evolution of market behavior and manipulative practices, and that the use of AI systems for surveillance and fraud detection could help overcome some of these challenges and could potentially offer higher detection rates than traditional approaches. ML techniques were reported to help with: assessing large amounts of data such as unstructured data coming from a wide range of publicly available sources; analyzing network traffic; identifying patterns or anomalies; monitoring customer data and transactions in real time; blocking malicious traffic; installing cybersecurity patches; and detecting illicit activities.

Use of Recent Advancements in AI

Some IOSCO Member/SRO Survey respondents observed that market participants were investigating the potential of multi-modal systems powered by GenAI to integrate and analyze various data types and sources – such as publicly-traded company filings, earnings calls, and social media posts – to inform trading decisions. Respondents also reported increased experimentation with GenAI and LLMs for lower risk use cases like customer service tools, virtual assistants for order execution, and research tools to help investors find market information. Some respondents observed broker-dealers leveraging RAG techniques to

improve response accuracy by incorporating internal knowledge bases and referencing source documents. RAG was also observed as a technique that help reduce so-called hallucinations (or confabulations).[23]

Asset Managers

Based on the IOSCO Member/SRO Survey results, the uses of AI that were reported by respondents as most observed in asset managers, including robo-advisers and investment advisers, were:

- Robo-advising and Asset Management (60%)
- Investment Research (40%)

AMCC Survey respondents identified as asset managers most frequently cited the uses of AI in internal productivity support and for algorithmic trading. Larger respondents (reporting greater than $10M in approximate annual revenue or declining to disclose annual revenue) also reported using AI for code and internal productivity support and for internal chatbots.

Robo-advising and Asset Management

IOSCO Member/SRO Survey respondents observed the use of AI by asset managers to support robo-advisory or other asset management services for providing automated investment advice and investment and portfolio management. This included: portfolio construction; optimization by monitoring of portfolios and markets to initiate rebalancing of clients' portfolios; customization based on client preferences; and risk-return assessment and management. Uses included the creation of personalized investment themes for clients and analysis of market sentiments around investment themes to support investment decisions. Respondents reported observing asset managers using NLP tools to analyze financial news and social media data to identify emerging investment themes; to interpret client responses in questionnaires or chatbot interactions, e.g., to understand their investment preferences; and to assist in creating personalized investment advice and recommendations. AI was reportedly used to enhance activities across the asset management lifecycle, such as for data synthesis, pattern and anomaly detection and monitoring, prediction and forecasting, and process automation.

Investment Research

Respondents report that market participants, including asset managers and investment research firms, have used AI to enhance the investment selection process.[24] Typical uses to augment human decision

[23] Hallucinations" is a term that has been used to describe LLM outputs that contain erroneous or factually inaccurate information. Some argue that the term inappropriately ascribes conscious awareness of a sensory input to an LLM and, thus, propose the term "confabulation" as a more accurate description of this phenomenon. *See, e.g., Hallucination or Confabulation? Neuroanatomy as Metaphor in Large Language Models*, A.L. Smith, F. Greaves, T. Panch (Nov. 1, 2023), available at https://pmc.ncbi.nlm.nih.gov/articles/PMC10619792/.

[24] One respondent observed the use of AI for preliminary stock screening to identify stocks that warrant further research by analysts. Another respondent observed that portfolio managers have used ML techniques, such as clustering and decision

making include market sentiment analysis, pattern detection, data summarization, and process automation. Additionally, some asset managers were observed leveraging AI-powered tools available on third-party platforms and data providers to monitor the macro-economic environment. Furthermore, respondents observed AI used for language translation to facilitate the analysis of information on foreign investment products.[25] AI was also observed being used in client segmentation, to group clients based on specific attributes and behaviors for marketing, targeting, or surveillance.

Use of Recent Advancements in AI

IOSCO Member/SRO Survey respondents identified novel applications of AI that were being contemplated or tested, but not yet deployed. One was the use of GenAI to streamline the process of developing new trading strategies by searching through research papers for relevant topics, generating economic rationale for various trading hypotheses, generating code to implement these trading hypotheses, and conducting back-testing of the strategies on portfolios. Other exploratory use cases involved GenAI being used to analyze financial reports, news, and social media to generate faster and deeper insights and capabilities for investment firms. Another area of exploration was the development of specialized LLM platforms for financial data and reporting, to perform more advanced investment research tasks and report generation. A respondent also reported that an asset manager intends to automate the publication of investment research by making use of LLMs to gather relevant data as input to compile into a draft investment research paper by adopting the writing style of certain investment analysts. One respondent noted the use of LLMs to enhance client interactions, connect with portfolio construction tools, and assist with trade executions. Another observed development of specialized LLMs focused on issuer and securities research. Some respondents noted a shift towards more customized advice, tailored to client demographics and asset conditions of retail investors, with the possibility of integrating ChatGPT-like user interface.[26]

tree algorithms to conduct economic research and support their investment decisions. Reports indicate the use of AI to pick investing themes for exchange-traded products and to dynamically monitor and move in and out of such themes. *See, e.g.,* https://www.invesco.com/uk/en/insights/thematic-etfs-capture-targeted-long-term-growth-opportunities.html.

[25] Mercer, a pension consultant, found that 90% of investment managers were currently using AI or planning to use AI as part of their investment research process. https://www.mercer.com/insights/investments/portfolio-strategies/ai-in-investment-management-survey, at 9. In the Mercer survey, managers reported that AI is used to support human decision-making around investment decisions and research, but that data quality and availability may be a constraint on their future use of AI. *Id*. at 21. Similarly, research by Coalition Greenwich found that while 85% of asset managers are using AI, only 25% of buy-side traders surveyed are considering using it for equity trading. https://www.greenwich.com/blog/ai-ml-iterative-learning-process (predominant uses of AI include trading optimization, pre- and post- trade analysis, and analyzing traditional market data).

[26] The FSB Report noted that in the area of trading and portfolio management, GenAI is used to assess text data from earnings calls and regulatory disclosures, and to implement reinforcement learning for trade execution. *See* FSB Report, *supra* n.6. Industry reports indicate that financial firms are piloting the use of LLMs for customer support and customer education. Examples in public reporting include chatbots to allow clients to ask questions about corporate filings, news, and historical prices to allow institutional clients to ask it to price hypothetical transactions or execute them. Another application is to assist customer service employees by training the LLMs with internal policy and operational documents, so the customer service employees can interface with the chatbot when servicing client request. Industry reports also indicate firms are using LLMs to generate marketing material, including both the content of investment solicitations as well as investment

Exchanges and Other Financial Market Intermediaries

Based on the IOSCO Member/SRO Survey results, the AI use that was reported by respondents to be most observed in financial exchanges, including securities and derivatives exchanges, clearing houses, financial market infrastructures, and trade repositories, was:

- Transaction processing and automation (40%)

AMCC Survey respondents that were identified as exchanges and trading venues commonly reported AI use cases such as code generation, editing or modernization, and internal productivity support. A subset (non-GEM) also frequently cited the use of AI for internal chatbots.

Transaction Processing and Automation

IOSCO Member/SRO Survey respondents reported observing financial exchanges--including securities and derivatives exchanges, clearing houses, financial market infrastructures, and trade repositories--to be using AI predominantly in the transaction processing and automation. This includes the use of AI for pre-trade and post-trade process automation, including the use of ML to optimize trade settlement. These respondents report observing the use of ML to predict the likelihood of trade settlement failure. One respondent observed that certain market participants, particularly institutional investors, have developed AI systems that are integrated with exchange platforms. These systems are capable of processing trade data in real-time and extracting relevant information using NLP tools to automate trade processes, such as order and trade validating, and generating trade reports that can be submitted to regulatory authorities or trade repositories.

Use of Recent Advancements in AI

One IOSCO Member respondent noted that an exchange in its jurisdiction had recently introduced an AI-driven dynamic timer that can be applied to a specific type of order. The exchange's AI model leverages reinforcement learning to evaluate the duration of the holding period based on local market conditions, and the exchange claims that applying this technique could achieve higher fill rate and lower markouts (a measure of price movement in a security at some defined time interval following a trade) (*see* Box Topic below).

banking tasks such as creating presentations, summarizing industry knowledge, and highlighting key points for sales. LLMs are reportedly used to assist its staff to generate alerts and themes for marketing to clients. Firms foresee using LLMs to assist in client segmentation, profiling, and personalization for marketing.

Exchange AI-Powered Order Type – Nasdaq's Dynamic M-ELO

In September 2023, the U.S. SEC approved a Nasdaq rule change allowing the exchange to launch an AI-powered order type, termed Dynamic Midpoint Extended Life Order ("Dynamic M-ELO").[27] Nasdaq's Midpoint Extended Life Orders and Midpoint Extended Life Orders Plus Continuous Book (collectively, "M-ELO") order types had previously used static holding periods of 10-milliseconds.[28] A holding period represents the time between Nasdaq's receipt of a M-ELO order and its eligibility for execution. Dynamic M-ELO seeks to optimize the holding period for individual securities, by lengthening or shortening the holding period throughout the trading day, with the objective of simultaneously increasing fill rates and minimizing markouts for M-ELO orders.

Dynamic M-ELO utilizes a timer control system that applies deep reinforcement learning techniques to identify optimal hold times, assess the results of such actions, and apply such feedback to future orders.[29] The model considers more than 140 data points as it determines whether to increase or decrease the holding period at 30 second intervals. Under most market conditions, holding periods can change by 0.25 or 0.50 milliseconds, within a range of 0.25 to 2.50 milliseconds. The order type also employs a stability protection mechanism, which the model aims to activate during the most volatile 1% of each day, and during which holding periods are adjusted to 12 milliseconds. Nasdaq retrains Dynamic M-ELO model on a regular basis so that it will continue to learn from and act upon the basis of more recent data sets, with a goal of improving the model's performance over time.[30]

In approving the rule change, the U.S. SEC noted:

The deep reinforcement learning model that will determine the dynamic holding periods for each symbol for M‑ELO and M‑ELO+CB orders will be implemented through established, non-

27 *See* United States Securities and Exchange Commission Order, Self-Regulatory Organizations; *The Nasdaq Stock Market LLC; Notice of Filing of Amendment No. 2 and Order Granting Accelerated Approval of a Proposed Rule Change, as Modified by Amendment No. 2, To Amend Rules 4702(b)(14) and (b)(15) Concerning Dynamic M-ELO Holding Period* (SEC M-ELO Order), 88 Fed. Reg. 176, at 62850, available at https://www.govinfo.gov/content/pkg/FR-2023-09-13/pdf/2023-19728.pdf; *see also* Nasdaq Rule 4702(b)(14)-(15).

28 The M-ELO order type was introduced in 2018 with a static half-second holding period, which was refined multiple times based upon Nasdaq's internal study and customer feedback. The 10-millisecond holding period was introduced in 2020. *See id*. at 62851-52.

29 Nasdaq's development of the Dynamic M-ELO order type is described in a whitepaper submitted as an exhibit to its rule filing. *See Applying Artificial Intelligence & Reinforcement Learning Methods Towards Improving Execution Outcomes,* D. Kafkes, J.P. Ruiz, D. Rooks, D. Hamilton, and M. O'Rourke (Oct. 10, 2022), SR-NASDAQ-2022-079, Exhibit 3A, available at https://www.sec.gov/files/rules/sro/nasdaq/2023/34-98321-ex3a.pdf.

30 SEC M-ELO Order, *supra* n.27 at 62854.

discretionary methods, but it is so complex that its complete details are, for most intents and purposes, not readily intelligible, and it would be immensely difficult for the Exchange or any market participant to precisely predict the holding periods that will be generated by the model for any given symbol at any particular time. Nevertheless, as further discussed below, the Commission believes that the Exchange has provided information sufficient for the Commission and public to understand the design, operation, and limits of the proposed changes to these order types, and the role of the machine-learning model therein.[31]

The U.S. SEC further stated that, "Nasdaq precisely articulated the nature of the holding period changes that are permissible and the limits to those changes" and noted that the rule filing was supported by, among other things, disclosure of the data elements used by the model, a white paper describing the deep reinforcement learning algorithm and process and explainability testing, an assessment of susceptibility to fraud and manipulation, testing for unfair bias against specific market participants and a commitment to periodically conducting such tests, commitments with respect to recordkeeping and public disclosures, and a clear articulation of when changes to the model beyond ordinary retraining would require subsequent approval.

Use of AI by Self-Regulatory Organization (SRO) Respondents

The IOSCO Member/SRO Survey respondents included six SROs, representing five jurisdictions. These SROs were asked to provide information on their own current and future planned use of AI technology as part of their regulatory oversight, intelligence gathering and assessment, and supervision.[32] Below, is a summary of the SRO responses concerning their respective AI use cases reported through the survey process.

Existing SRO Respondent Reported Use Cases

Four of the six SRO respondents reported that they integrated AI in some capacity within their respective regulatory processes to enhance data-driven applications and support compliance efforts. Two SRO respondents stated that they were actively integrating AI technology to optimize supervisory processes. They further stated they were developing AI models that can assist with document processing, which includes interpreting the content of documents, classifying them, and identifying those that require further detailed analysis. One SRO stated that it used AI technology to regulate advertising activities. None of the SRO respondents said they currently used AI technology to analyze or supervise AI systems, models, or technology that was employed outside their organizations.

31 *See id*. at 62858.

32 IOSCO Members were not asked about their respective internal use of AI systems, and that is not a topic of this Report.

SRO respondents reported using a variety of AI technologies to enhance their regulatory oversight and supervision capabilities, including ML and NLP, which were employed for tasks such as document analysis, classification, and sentiment analysis. In addition, some reported using predictive analytics models to identify high-risk firms and enhance their quantitative capabilities. Some reported having deployed recent advancements in AI, such as GenAI and LLMs, for tasks such as anomaly detection and document processing.

Potential Future SRO Respondent Reported Use Cases

In addition to the current use of AI technology by the surveyed SROs, the survey also sought information regarding potential future uses of AI by the surveyed SROs.

SRO respondents cited market surveillance and compliance as significant areas for future use of AI applications. SRO respondents noted AI's potential to identify unusual or unexpected trading activities by analyzing historical patterns and behaviors. Specific examples of future contemplated uses included using AI to determine the validity of trades, identifying trading which may be indicative of account intrusions, detecting unusual profits that may indicate misconduct, and identifying potential collusion among bad actors. One SRO stated that AI may be used to transcribe and analyze recorded conversations to surveil for misconduct, and to generate written inquiries based on alert activities or surveillance data.

SRO respondents cited improvements in business operations as an area for potential use cases. One SRO mentioned AI's potential ability to reduce false positives in traditional alert-based workflows, which may allow analysts to focus on higher-quality alerts. SROs cited AI as a potential tool for quality assurance of analysts' investigations and improving the efficiency and accuracy of tasks.

SROs identified GenAI as a subject of growing focus. Several respondents mentioned GenAI's potential capability to assist with automating and enhancing document creation, such as generating meeting summaries, drafting reports, and creating compliance documentation, which may help reduce manual effort and human errors. Respondents stated that GenAI may streamline content creation, including presentations, marketing materials, and customer communications. A few SROs cited GenAI's potential for extracting data from complex, unstructured documents, transforming them into structured formats for easier analysis and database population. One SRO also noted GenAI's potential capability to aid in software development.

SRO respondents also cited enhanced and efficient data analysis as an area of future AI use. One SRO stated the possible use of AI in validating and improving data quality by detecting and correcting errors, inconsistencies, and outliers.

IV. Risks, Issues, and Challenges relating to Investor Protection, Market Integrity, and Financial Stability

Introduction

This section explores in depth the potential risks, issues, and challenges to investors and the markets that either have emerged or been amplified since the 2021 AI Report, considering recent advancements in AI. Particularly, this section identifies risks, issues, and challenges that were raised through IOSCO's information gathering efforts with respect to these advancements, including LLMs and GenAI. [33] However, the risks detailed herein could be applicable to AI technologies and use cases in general.

Any evaluation of the risks of AI use in financial products and services is highly contextual and will depend upon a number of factors, including the use case for the AI system, the choice of its design and what particular technologies are employed, how it is deployed, and how the environment in which it is used changes over time.[34] The degree to which there is human oversight for the AI system and its operation, and its potential impact on investors and the markets, also factor into its risk profile.

The risks, issues, and challenges identified and discussed in this section are informed by IOSCO's information-gathering efforts (e.g., surveys, roundtables, and literature reviews). It should be noted that many of the risks discussed in this section are not necessarily unique to the use of AI in the financial sector, and some may straddle many sectors of the economy. For example, large-scale cyberattacks, fraud, disinformation campaigns, and misalignment of AI system objectives with human values could lead to a loss of trust and confidence in institutions are relevant to the economy at large.[35] Market regulators will

[33] The risks of AI uses in financial products and services can be described in terms of "micro risks" and "macro risks." Micro risks are those presented to individual investors or firms, while macro risks are those with systemic implications. Although these categorizations can be useful for evaluating the nature of a given risk, they are not wholly independent of each other. A micro risk can lead to a macro risk if it has the potential to impact a large number of market participants or key market participants. That is, micro risks may have broader implications at the market level, including systemic risks. As such, regulatory responses targeted at individual market participants can play an important role in mitigating both micro and macro risks. Given this overlap between the two categories, this report does not make a clear distinction between them when identifying the risks, issues, and challenges.

[34] These factors were recognized by IOSCO in the 2021 AI Report when it stated that "proportionality" should underpin considerations by regulators and firms: "In judging proportionality, consideration should be given to the activity that is being undertaken, the complexity of the activity, risk profiles, the degree of autonomy of the AI and ML applications, and the potential impact that the technology has on client outcomes and market integrity." 2021 AI Report, *supra* n.2 at 17.

[35] See, e.g., OECD (2024), *Assessing Potential Future Artificial Intelligence Risks, Benefits and Policy Imperatives, OECD Artificial Intelligence Papers,* No. 27, OECD Publishing, Paris, available at https://www.oecd.org/en/publications/assessing-potential-

need to understand how risks that may originate or manifest outside the financial sector nevertheless may impact the financial markets. Also, a number of the risks, issues, and challenges outlined below could impact large firms and small firms differently, particularly as resources and expertise are needed, both to harness the benefits of these technologies and to deploy them safely.

It is also important to recognize that AI systems may strengthen the capacity of firms and regulators to identify and mitigate risks, particularly in the area of AML, CFT, anti-fraud, and compliance measures. If used responsibly, AI systems may also contribute to broader diversity of use cases and could contribute to financial market resilience.

Finally, it should be noted that for a number of survey questions concerning data, model, and broader risks of the use of AI systems in financial products and services, approximately half of IOSCO Member/SRO Survey respondents collectively provided no response. This could indicate data and knowledge gaps concerning the use of AI technologies in financial markets.[36]

Survey Results

The 2021 AI Report detailed a number of potential risks posed to investors and the markets by the use of AI at the time of that report, including in the areas of: governance and oversight; algorithm development, testing and ongoing monitoring; data quality and bias; transparency and explainability; outsourcing; and ethical concerns. Each of these risk areas continue to be relevant in the context of AI use in financial products and services. Based on the responses provided to the IOSCO Member/SRO Survey and AMCC Survey respondents, four broad areas of risk were most cited: malicious uses involving AI; model and data considerations; concentrations, outsourcing, and third-party dependencies; and interactions between humans and AI.

This section summarizes the survey results, details a number of the most frequently-cited risks, and provides a view into potential future risk areas for monitoring.

Malicious Uses

IOSCO Member/SRO Survey respondents were asked to identify AI-related risks to investor protection and financial markets in the markets they regulate. These survey respondents collectively identified cybersecurity, data privacy and protection, fraud, market manipulation, and deepfakes as among the most frequently cited risks. These respondents cited that cybersecurity and fraud concerns create risks in certain use cases in particular, identifying investment advising, algorithmic trading, customer segmentation, AML/CFT measures, surveillance, and fraud detection. AMCC Survey respondents were asked to rank

future-artificial-intelligence-risks-benefits-and-policy-imperatives_3f4e3dfb-en.html (OECD Future AI Report), at 19 (listing 10 priority potential future AI risks).

[36] *Accord* OECD Report, *supra* n.6 at 13 ("[A]uthorities do not have complete visibility of the use of AI by financial sector participants [relying upon] regular supervisory interactions (including examinations), industry engagement and feedback from the market, innovation facilitators (such as regulatory sandboxes and innovation hubs), firm's public disclosure, market reports and other non-official sources … [and] Requests for Information/Comments … .").

eighteen different risks relating to the deployment and use of AI. Similar to the risks identified by IOSCO Member/SRO Survey respondents, the AMCC Survey respondents collectively identified risks relating to cybersecurity, fraud, market manipulation, and deepfakes as among the highest types of risk. These risks identified by survey respondents can be broadly categorized as "malicious uses" involving AI and, based on IOSCO's information gathering, are discussed in more detail below:

Cyber Attacks[37]

Depending on their use and deployment, AI systems can introduce new cybersecurity threats and exacerbate existing ones, with challenges for financial firms compounded by resource constraints and scarcity of talent. Cybersecurity risks, particularly those associated with Advancements in AI, have been categorized as follows:

- ***Attacks Using AI*:** Bad actors may use AI systems to plan, enhance, or automate cyberattacks. AI technologies may assist them in analyzing systems to identify vulnerabilities and attack vectors, making their threats more sophisticated and challenging to detect. AI can be used to augment tasks like creating narratives, translating text, creating code, and generating deepfakes. Thus, bad actors could use AI to create more sophisticated and harder to detect phishing scams or other social engineering cyberattacks on a firm, and create malware to steal data and evade detection.[38] Some ways that AI can assist in targeting financial firms include: creating or manipulating identification documents, images, or video that are used to convince a firm to disclose customer data or grant access to customer accounts; stealing or creating a synthetic identity to open or access an account for illicit purposes; or creating fake documentation or to bypass AML and KYC procedures.[39] Bad actors have reportedly used deepfakes in business compromise attacks to steal information or funds, or to damage individual and firm reputations and security.

[37] It is important to note that AI prediction and anomaly and event detection tools have long been used in cybersecurity applications, and it is widely reported that AI technologies have the potential to enable cybersecurity with more capable tools to detect and prevent cyberattacks. *See e.g.*, *Workshop Report, Securing Critical Infrastructure in the Age of AI, Center for Security and Emerging Technology* (Oct. 2024), available at https://cset.georgetown.edu/publication/securing-critical-infrastructure-in-the-age-of-ai/, at 10 (noting that current or near term uses for GenAI-enabled cybersecurity in the financial sector include: anomaly detection and behavior analysis; new techniques for endpoint protection, intrusion detection and prevention, data loss prevention, and firewalls; classification of suspicious emails; and detection of malicious code; future use cases could include analyzing threat actor behavior; streamlining alerts, investigations, and responses; and identifying and mitigating code vulnerabilities).

[38] *See* OECD Future AI Report, *supra* n.35 at 20 ("Although many efforts involve using AI to mitigate cybersecurity risks, AI systems have reduced the level of effort needed for malicious cyber activity that would have previously required significant time investment by human experts."); U.S. Treasury AI Cybersecurity Report, supra n.17 at 16 ("[Cybersecurity concerns] identified by financial institutions are mostly related to lowering the barrier to entry for attackers, increasing the sophistication and automation of attacks, and decreasing time-to-exploit.").

[39] In November 2024, the United States Dept. of Treasury Financial Crimes Enforcement Network ("FinCEN") issued an alert noting an increase in suspicious activity reporting by financial institutions describing the suspected use of deepfake media in fraud schemes targeting their institutions and customers, and often involving criminals altering or creating fraudulent identity documents to circumvent identity verification and authentication methods and customer due diligence controls.

- ***Attacks Targeting AI Systems*:** The use of AI systems has data security and privacy implications. AI itself is vulnerable to attack due to certain of its technological features, and such attacks can occur along the AI development and supply chain.[40] Attacks could manipulate an LLM's training, influence its output, and exfiltrate information.[41]

- ***AI Design and Implementation Failures*:** Incorporating AI systems could introduce or broaden attack surfaces for a financial firm and make cybersecurity procedures more challenging.[42] Exposing internal data – including client personally identifiable information or other sensitive data – to an AI system that may not be secure could place the data at risk of cybercrime, exposure, and misuse. Models trained or used on proprietary or personal data could lead to data leakage or privacy violations if the model were to include this data in an output, which could itself be non-consensual or result in intellectual property violations.[43] In addition, fictitious information about an individual, such as a client, could be created and disseminated in a model's output. With respect to the use of GenAI to generate code, these technologies are being explored in cybersecurity areas such as vulnerability analysis and patching, but they can also themselves produce insecure code outputs.[44] Such tools can also produce code that interacts with external code libraries and packages, which can present additional security concerns,[45] as well as to attacks on the IT

FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions (Nov. 13, 2024), available at https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf. According to the FinCEN alert, malicious actors have successfully opened accounts using fraudulent identities suspected to have been produced with GenAI and used those accounts to receive and launder the proceeds of other fraud schemes. *Id.*

[40] *See* U.S. Treasury AI Cybersecurity Report, *supra* n.17 at 15 ("Source data, training datasets, testing datasets, pre-trained AI models, LLMs themselves, prompts, and prompt and vector stores can all be subject to data attacks, making the security of data throughout the development and production cycle as important as protecting production data.").

[41] Common attack types associated with AI are: evasion attacks (malicious inputs during inference to cause a model to malfunction or reveal information); "poisoning" and "backdoor" attacks (vulnerabilities embedded in the model to impact its behavior or disrupt its operation); and "privacy" attacks (stealing data or information about the model itself). For example, using an evasion attack, a bad actor could jailbreak a model's guardrails, hack into a firm's systems, or thwart a firm's AML and KYC processes. Using data poisoning, a bad actor could introduce malware into the training data on which a model is trained, or on model weights, thus impairing or altering a model's output. Using a privacy attack, a bad actor could exfiltrate data used in the operation of the model. *See, e.g.*, *id*. at 17-18.

[42] *See id*. at 16 ("AI system dependency on data may amplify existing challenges and introduce new data security and privacy challenges for institutions, including those related to their third-party providers and their software and data supply chains.").

[43] Even programming code generated from a model may implicate software licensing issues should it incorporate proprietary code.

[44] *See* Center for Security and Emerging Technology, *Cybersecurity Risks of AI-Generated Code*, J. Ji, J. Jun, M. Wu, and R. Gelles (Nov. 2024), available at https://cset.georgetown.edu/publication/cybersecurity-risks-of-ai-generated-code/, at 1 (identifying three broad categories of risk: 1) models generating insecure code, 2) models themselves being vulnerable to attack and manipulation, and 3) downstream cybersecurity impacts such as feedback loops in training future AI systems). *See also id*. at 29 (suggesting that current evaluation benchmarks for code generation models rate performance but overlook security).

[45] *Id*. at 10.

infrastructure on which it is deployed.[46] The impacts of the widespread use of AI-generated code is open to debate, but some researchers posit downstream effects that could lead to broader cybersecurity and systemic concerns.[47]

The design choices around which models, data sets, and infrastructure to use, as well as how an AI system is deployed (i.e., who can access an AI system and how), will impact decisions about cybersecurity and its risk management. For example, cybersecurity and risk management considerations will differ based on choices such as whether a firm is using a vendor's model accessed through an API, a cloud service provider's model through an API, a cloud service provider's model through a virtual machine, or a firm hosting a model themselves using their own hardware with graphics processing units (GPUs) or, possibly, application-specific integrated circuits (ASICs).[48] Individual design and implementation choices are likely driven in part by resource constraints, which may make the use of vendor models, architectures, and data sets attractive options; however, the use of external components can increase attack vectors.

A robust discussion of cybersecurity considerations is beyond the scope of this Report and such considerations are the subject of intense focus by expert technical and standardization bodies. Cybersecurity frameworks may need to be assessed and fortified on an on-going basis to protect against AI-specific vulnerabilities. Insufficiencies in the design and implementation of AI systems that support critical market participants or infrastructures could potentially lead to systemic risk, and the more AI systems are employed in critical areas, the more impactful this risk could be. As with other risks discussed herein, more well-resourced firms will likely have an advantage in mitigating these risks than firms that are constrained by costs and talent.

Fraud, Scams, and Misinformation

AI powered tools for malicious uses can lower the barriers to entry for bad actors, enabling cheaper, increasingly automated, and more sophisticated ways for them to conduct fraud, cyberattacks, and other

[46] *See id*. at 11-13.

[47] *See id*. at 30 (citing potential downstream risks of widespread AI generated code use, including insecure code outputs from AI tools used to train future modes, leading to human-out-of-the-loop development pipelines, and models suggesting deprecated versions of a commonly used package or library).

[48] The OECD Report notes that financial sector participants are deploying AI systems in a variety of ways. *See supra* n.6 at 13 ("Financial sector participants use open-source software, vendor provided tools, and in some cases, pre-trained models (e.g. automation on major cloud service provider platforms; pricing and trading models employing Machine Learning (ML) techniques; automated trading and risk management systems; Natural Language Processing (NLP) and Optical Character Recognition (OCR)) to extract, analyse and synthesize large data sets, and deploy Large Language Models (LLMs) and other advanced AI models."). IOSCO asked surveyed SROs whether AI-based technologies are being developed and implemented internally, through outside vendors, or using a hybrid approach combining in-house developers with external venders. Five of six SRO respondents stated they were adopting a hybrid approach, which allows them to utilize internal expertise while also benefiting from specialized knowledge and resources from external partners. No SRO that stated it relied solely on outside vendors and developers to provide and maintain AI solutions. Similarly, no SRO stated that it had developed and implemented AI technologies entirely in-house.

misconduct.[49] As GenAI becomes increasingly available and its outputs more convincingly humanlike or realistic, bad actors likely will exploit it to carry out schemes to defraud investors or to engage in other misconduct related to the financial industry. For example, bad actors can use GenAI tools to generate credible multimodal content, including text, computer-executable code, audio, image, and video, which can contain or disseminate misinformation, disinformation, or malicious content, including that which mimics real persons (deepfakes) to lure investors into fraudulent investment schemes or to facilitate other misconduct. Moreover, while GenAI may enable new types of investment scams, such as fraud schemes involving purported investments in GenAI businesses or misrepresentations about GenAI-related investment activities (AI washing), GenAI also may facilitate existing scam techniques; one study found that GenAI tools may be "turbocharging" common investment scams "by increasing their *reach, efficiency, and effectiveness*." [50] For example, a burgeoning area of retail fraud involves relationship or confidence investment scams.[51] These scams, which typically begin with online outreach and relationship-building from a fraudster to an investor, already are pervasive, but they could be substantially more pervasive and convincing when augmented with GenAI technologies. To conduct these and other schemes, open source and other GenAI tools are widely available to fraudsters and could enable a growing range of deceptive techniques, including automating phishing schemes, creating fake identities and online profiles, generating more believable personalized scripts, and translating content to numerous languages.[52] Bad actors also could use GenAI to create and disseminate misinformation, to mislead or manipulate markets, thereby impacting trading prices and volumes, and negatively affecting investors.

Although mitigating techniques to address deepfakes and other synthetic content exist and are actively being developed, such as tracking the source and history of synthetic content, labelling and watermarking or detecting synthetic content, and using technical guardrails to prevent certain uses, these techniques are not comprehensive and can be evaded.[53] As GenAI technologies become more advanced, the content

[49] *See* United Nations Office on Drugs and Crime, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Treat Landscape* (Oct. 2024), available at https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf (UNODC Report), at 9.

[50] *See* Ontario Securities Commission (2024), *Artificial Intelligence and Retail Investing: Scams and Effective Countermeasures,* available at https://www.osc.ca/en/investors/artificial-intelligence-and-retail-investing-scams-and-effective-countermeasures (finding that participants in a study invested 22% more in AI-enhanced scams than in conventional scams).

[51] *See Relationship Investment Scams, Investor Alert* (Sep. 2024), available at https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/relationship-investment-scams-investor-alert.

[52] Certain GenAI software that is tailored for malicious uses is offered for sale on the darkweb, over the internet, and through social media. One report analyzed certain underground marketplaces and forums and found that growth in the use of deepfake technology is driven by online service providers marketing AI tools to criminal groups to engage in cyber-enabled fraud. *See* UNODC Report, *supra* n. 49 at 9. As AI technologies develop, one can expect growth in the development and peddling of malicious AI code. The use of such code will likely become more pervasive, insidious, and hard to detect. *See id*. at 123 (describing the malicious use of "polymorphic malware," which "leverages AI to dynamically generate and inject its malicious components at runtime, thereby making it resistant to traditional detection methods," and "autonomous AI agents designed to operate with minimal human oversight.").

[53] *See* NIST (2024) *NIST Trustworthy and Responsible AI NIST AI 100-4, Reducing Risks Posed by Synthetic Content, An Overview of Technical Approaches to Digital Content Transparency*, available at https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-4.pdf.

they produce will likely become more convincing and hence it may be more difficult to differentiate real content from that which is AI-generated.

Should malicious uses of AI techniques become widespread or egregious, it could erode investor trust in the provenance and truth of digital information and communications to the point of presenting broader risks, such as undermining trust in financial markets. Further, trust in the use of AI technologies overall could decline, potentially hindering AI technology development and its use for beneficial purposes.

AI Models and Data Considerations

IOSCO Member/SRO Survey respondents were asked to identify model and data related risks to investor protection and financial markets in the markets they regulate. With respect to models, these respondents most frequently identified risks related to explainability and interpretability; model bias; complexity, robustness, and resiliency; hallucinations; and conflicts of interest. With respect to data, IOSCO Member/SRO Survey respondents most frequently identified data quality (where data is clean, complete, representative, accurate, relevant, etc.); data drift (where the training data, and hence a model trained on that data, becomes unrepresentative); and data bias (where datasets are not sufficiently diverse or representative, and may contain unfair biases).

The survey respondents reported a wide range of potential financial use cases where model and data issues would create risk, including algorithmic trading, robo-advising, predictive analytics, market analysis, trading insights, risk modelling, transaction processing, asset allocation, customer segmentation, marketing, client communications, AML/CFT measures, surveillance, and fraud detection.

Overall, AMCC Survey respondents ranked model and data related issues as the highest risk relating to the deployment and use of AI after the malicious use risks discussed above.

Some key risks associated with the deployment of AI in financial services relate specifically to models and data and may be an area of particular focus in assessing risks. Based on IOSCO's information gathering, a selection of these risks is discussed below.

Models

- ***Explainability and Complexity***: LLMs typically are complex, such that it is difficult or impossible to comprehend or explain how an LLM-based AI system computes an output given a particular input. In the context of disclosure requirements that may apply to investment products and services using such systems, disclosures may be ineffective, difficult to comprehend, incomplete, or inaccurate. If such systems are used as the basis for investment decisions or advice, decision criteria may lead to decisions relating to investments that are unsuitable for the investor. For example, there is the risk that an AI model may be trained to maximize profitability but may not adequately take into account legal constraints or investor suitability considerations. Failure to understand how a model operates could also lead to investment-related decisions that create a conflict of interest vis-a-vis a financial service provider and its client, or that put the interests of a financial service provider ahead of its client, such as by taking into account the firm's revenues or profits when making a recommendation or by steering investors towards unsuitable products or trading strategies that financially benefit the firm. Challenges in explainability also translate to

challenges in assessing the robustness and suitability of the model for any particular use. The inability to understand how models operate also may impede supervision and regulatory oversight. Because of their complexity, LLMs also require large processing power to train and operate.[54]

- ***Limitations*:** LLMs are typically trained on historical data sets (which may be of poor quality, as discussed below), and may not adapt to rapidly changing market conditions or unforeseen events, causing model "drift" or degradation in performance. A model may be extremely sensitive to small variations in inputs. Commercially-available LLMs are often updated through the publication of new versions, which can vary in behavior from prior versions. Conceivably, a slight change in an LLM could have unexpected impacts on a given use case, potentially altering the risk profile of the use case. Furthermore, as model's outputs are typically probabilistic, rather than deterministic, in which case they will not always produce the same result for a given input.[55] Also, they can generate fundamentally incorrect outputs (hallucinations, confabulations) that are convincing but inaccurate or unsuitable. If used to generate inputs to trading decisions or advice, or to contribute to code that is used in trading algorithms, these outputs could lead to bad investment decisions or may also cause operational or market disruptions if used at large scale.

- ***Bias***: Use of LLMs can result in biased output, which can stem from algorithmic bias (in modelling); cognitive bias (in weighting or interpretation); and training data bias (see below). Model bias can cause AI systems to overlook certain groups, for example, leading to the unfair treatment of certain groups of investors, a bias for certain investment types over others, or conflicts of interest.

Data

- ***Quality*:** LLMs typically rely on vast amounts of data for their training. Typically, models are 'pre-trained' with a very large corpus of diverse data, and 'post-trained' with more domain-specific data (such as instruction finetuning and answer-preference data). LLMs derive much of their performance from the data used in these training phases and, thus, are vulnerable to data quality issues. As models are updated or new ones are trained, new and larger data sets or alternative data may be sought. Greater access to a broader range of relevant, high-quality data contextualizes the model's performance, potentially resulting in decision-making that is more diverse and contextually relevant, resulting in better outcomes (e.g., models trained on a broad set of diverse, up-to-date data may be better at reflecting current economic trends and hence create better links with the real economy). At the same time, data can include inaccurate,

[54] Also, because of their complexity, LLMs require significant computational resources for both inference and training: a large amount of memory (typically measure in gigabytes of RAM or VRAM) to store the model (and, in the case of training, to store the gradients) and run a large number of computational operations (typically measured in floating-point operations, or FLOPs) for each token. This means that those employing LLMs may be impacted by energy costs and may contribute to environmental risks, including those resulting from energy consumption, water use for cooling, carbon emissions, raw mineral extraction for hardware production, and electronic waste.

[55] Models—such as an LLM based upon a transformer-like architecture or a diffusion model for high-dimensional output generation (e.g., images)—*can* have output consistency for a given input with specific hyperparameters (such as, for example, when temperature is set to 0 in transformers).

imprecise, outdated, irrelevant, and harmful content. Data risks can also occur during the exchange of data along the data pipeline, i.e., due to mismatched datasets or corrupted data. Poor data quality can lead to inaccurate assumptions or inadequate and erroneous modelling, resulting in poor performance. The increasing use of AI models in finance may change the data considerations relevant to financial decision-making, challenging existing risk management. For example, the demand for more data by LLMs may lead to increasing uniformity and interconnectedness through reliance on a concentrated set of data aggregators. GenAI tools used for synthetic data generation can lead to fake or erroneous information entering into datasets, which increases the risk of data quality and reliability issues and can result in poor performance in real-world conditions. LLMs may be trained on data that, itself, has been model-generated or is synthetic data, as opposed to real-world data. Some studies suggest that the use of such data may cause certain AI model performance to degrade or "collapse." [56] Typically, there is little transparency into what data has been used to train a model. For open-sourced or vendor built models, the provenance and type of training data may not be available or disclosed to a financial firm or end-user, and users may not be able to evaluate whether training data is high quality, relevant, and free from harmful biases, such that the model works as intended, and that outputs make sense, and do not perpetuate harmful biases, unfair discriminatory market outcomes, or conflicts of interest.

- ***Limitations*:** The data used for AI model training does not necessarily contain sufficient sample sizes that would include information, for example, about financial crises or "black swan" events unlike those that have occurred before. "Overfitting" describes when a model gives accurate outputs for training data but does not generalize for new or unseen data. This can occur if the training data does not contain sufficiently diverse samples or contains irrelevant data, among other reasons. In the context of AI deployment in financial services, models may not perform as intended in unexpected or extreme market conditions.

- ***Bias*:** LLMs trained on data sourced from the internet, including social media, in particular, may perpetuate or amplify biases inherent in that data and lead to discriminatory outcomes in financial services. Data bias can lead to the promoting of products and services offered by a particular service provider compared to potentially lower cost or more suitable products offered by a competing firm. Bias can also lead to favoring or disfavoring a particular group of investors and exacerbating inequalities if this occurs to a large degree. Data, and alternative data in particular, may suffer from selection bias (such as having information about one segment only and lacking a representative view of the entire demographic). If AI trained on non-representative data is used to identify potential clients for investment opportunities, for example, this could result in overgeneralization of customer segments or misinterpretation of investor behaviors based on limited data, which could lead to decisions that favor certain investor demographics over others.

[56] *See AI Models Collapse When Trained on Recursively Generated Data,* I. Shumailov, Z. Shumaylov, Y. Zhao, N. Papernot, R. Anderson, and Y. Gal (Jul. 24, 2024), available at https://www.nature.com/articles/s41586-024-07566-y ("indiscriminate use of model-generated content in training causes irreversible defects in the resulting models, in which tails of the original content distribution disappear").

Concentration, Outsourcing, and Third-Party Dependency

IOSCO Member/SRO Survey respondents commonly identified concentration, outsourcing, and third-party dependency risks as current risks from the use of AI to investor protection and financial markets in the markets they regulate. In particular, these survey respondents reported that concentrations present particular risks if Advancements in AI are used in relation to algorithmic trading, robo-advising, and asset management. Detection and monitoring of concentration, outsourcing, and dependencies present significant challenges. For example, IOSCO was unable to reach a clear understanding of the range of AI model types that are being used across financial services, including the role of proprietary versus open models. The following are observations IOSCO has gleaned from its information gathering:

- **Concentration:** Concentration risks relating to the use of AI technologies can potentially arise across various dimensions: technological infrastructure, data aggregation, and model provision. Reliance on a small number of technology infrastructure providers, such as cloud service providers, can create concentration risks in technical provision and associated services. Increasing reliance on a concentrated number of data aggregators (entities that collect data from one or more sources and may process and package that data for use by an end-user), for example, could potentially lead to a single point of failure in data sources (such failures could be caused by denial of service or degradation of the data). Certain datasets may be used, e.g., for risk management or investment computation (similar to benchmark data), and reliance on specific datasets could render them critical to those areas. Any data quality issues with critical datasets could propagate through systems relying on those datasets and risks could be amplified if data aggregators were concentrated. Additional data risks could result if future versions of critical datasets contained data derived from the outputs of models built on the same sources. Concentrations can also amplify risks if key vendors propagate vulnerabilities or biases through the financial sector. This is especially true if there is a lack of alternatives in times of failure or impairment. Currently, Big Tech firms are investing heavily into AI and related technology in an intense competition to develop AI. As an example, leading companies in this sector are reportedly racing to build expansive new data centers to train and power GenAI and other applications. There is a risk of high concentration in a small number of tech providers in the financial sector, given the resource demands of AI development in terms of development costs, computing capacity, access to data, talent, and existing market penetration.[57] A concentration of AI-related products and services vertically within a dominant tech provider can introduce correlated risks.

- **Outsourcing and Third-Party Dependency** – One challenge for market regulators arising from advancements in AI concerns the regulatory perimeter. Most technology providers are not directly regulated by IOSCO members. AI tools can be built and/or managed in-house, accessed through

[57] The impact of the recent emergence of DeepSeek, an open-source AI model that purports to have achieved results comparable to leading closed-source models using a fraction of training resources, has not yet been fully assessed. *See* DeepSeek-V3 Technical Report (Dec. 27, 2024), available at https://arxiv.org/html/2412.19437v1; DeepSeek-R1: Incentivizing Reasoning Capability in LLMs via Reinforcement Learning (Jan. 22, 2025), available at https://arxiv.org/html/2501.12948v1.

open-source models, built and/or serviced by a third-party (or nth-party)[58] vendor(s), or a combination of these. Data used with AI tools can be proprietary, commercial, open-source, or a combination. Models can be hosted on in-house or third-party infrastructure. Across any number of vectors, the use of AI technologies by financial services firms can introduce third-party outsourcing risk and dependencies, including from infrastructure providers, data aggregators, and other technology providers. With respect to AI technologies, financial institutions are or could become reliant on a concentrated number of AI providers for their technologies, given the costly and specific resources required to develop and train models.[59] Concentrations may also lead to resiliency issues. A separate challenge relates to the importance of data and the complexity of technology of AI systems - third-party risks include the cybersecurity, model, and data risks as discussed above.[60]

Interactions between Humans and AI

When asked about risks from the use of AI in financial markets, IOSCO Member/SRO Survey respondents identified a number of risks that stem from the interaction of humans and AI systems. These included lack of accountability and regulatory non-compliance, insufficient oversight and talent scarcity, and over-reliance on technology for decision making. IOSCO highlights the following insights, based on its information gathering:

- **Lack of Accountability and Regulatory Non-Compliance**: The use of AI systems by financial market intermediaries can lead to potential compliance failures, regulatory violations, investor and market harm, and firm reputational damage, particularly if the use of AI systems by a firm is not adequately supervised with appropriate risk management and governance policies, procedures, and controls.[61] Financial products and service providers could attempt to disclaim liability for investor or market harm resulting from the use of AI systems, or could attempt to shift responsibility to others in the AI system supply chain. Depending on the facts and circumstances, there could be enforcement challenges if AI systems are used in connection with violations of law, in terms of identifying and holding accountable responsible persons, and gathering and presenting evidence due to an AI system's complexities.

58 Nth-party refers to vendors using their own vendors (and so on).

59 *See generally* United Kingdom Competition & Markets Authority, *AI Foundation Models Technical Update Report* (Apr. 16, 2024), available at https://assets.publishing.service.gov.uk/media/661e5a4c7469198185bd3d62/AI_Foundation_Models_technical_update_report.pdf and *AI Foundation models: Initial Report* (Sep. 18, 2023), available at https://assets.publishing.service.gov.uk/media/65081d3aa41cc300145612c0/Full_report_.pdf.

60 *See* U.S. Treasury AI Cybersecurity Report, supra n.17 at 4 ("[T]he current trend of adopting AI solutions through multiple intermediaries and service providers complicates oversight and transparency. It is becoming increasingly challenging to accurately understand data flows and the use of AI solutions, thus inhibiting understanding and verification of those AI systems' fidelity of insights and decision making.").

61 Depending upon the circumstances and the jurisdiction(s) at issue, firms using AI systems may be subject to a panoply of applicable laws, e.g., that govern market conduct, consumer protection, privacy, online safety, anti-discrimination, intellectual property, product liability, and others.

- **Insufficient Oversight and Talent Scarcity**: Firms may face challenges with the supervision of AI systems, including risk management and governance. These challenges extend to AI systems' development, implementation, operation, and monitoring. Firms may face talent deficits, where the lack of staff with the required expertise and skills to implement AI technologies while addressing risks and adapting to developing technology. Firms may experience difficulty in recruiting, retaining, and developing necessary AI and data experts, particularly in organizations with traditionally different workforce compositions. Even with AI expertise, firms may fail to institute effective supervision of AI systems, which can ultimately lead to investor losses and market harm, including through non-compliance with regulatory obligations and customer agreements. If risk management and governance cannot keep pace with the rapid pace of evolution in AI technologies, such processes may become ineffective in addressing emerging risks. A lack of effective supervision over an AI system can lead to inappropriate or faulty decision-making, the inability to adapt to changing conditions and unforeseen events, security and privacy breaches, and investor and market harm.

- **Technology Over-reliance (Technology and Automation Bias):** GenAI can produce convincing and seemingly contextually relevant output in response to prompts, which may lead users to have confidence in AI capabilities, undue trust in its accuracy, and to defer to AI outputs. Targeted use of GenAI tools could lead users to develop a personalized "relationship" with the AI tool and make users more likely to follow advice or disclose personal information. A firm's delegation of decisions and actions to AI systems overall could result in inappropriate oversight of AI's use and a degradation of human skillsets over time. Automation bias can lead to investor and market harm if individuals and firms defer to the output of an AI system when it is inappropriate to do so, or when human oversight of an AI system fails. Such automation bias can be influenced by user attributes (biases, experience, or confidence); AI system attributes (system design, user interface, and failure modes); and organizational environment (firm policies and procedures).[62] Overreliance on AI systems to monitor markets or transactions for aberrant events or suspicious activity may lead to inadequate risk management and other disruptions for financial market infrastructure and other critical nodes of the financial system, especially in operational disruption or large-scale cyber incidents, or if monitoring systems and malicious activity engage in an arms race of detection and evasion. Critical market participants could become excessively dependent on AI to handle mission critical tasks that may impact key infrastructures.

[62] *See* Center for Security and Emerging Technology, *AI Safety and Automation Bias, The Downside of Human-in-the-Loop*, L. Kahn, E.S. Probasco, and R. Kinoshita (Nov. 2024), available at https://cset.georgetown.edu/publication/ai-safety-and-automation-bias/, at 8 ("[These, and an] additional layer of task-specific factors, such as time constraints, task difficulty, workload, and stress, can exacerbate or alternatively reduce automation bias.").

Looking Ahead: Market Dynamics, Potential Outcomes, and Data and Knowledge Gaps

The entirety of potential financial market implications from the use of AI systems is unknown and will depend on future developments. A key focus of IOSCO's work was to identify potential sources of macro risks (i.e., the impact of aggregate firm-level conduct to system-wide stability), how to measure and manage them, and understand whether we have the data to do so. However, IOSCO found that this topic has been less explored to date in academic and regulatory publications. Identification and measurement of metrics that could lead to macro risks is an area that warrants further exploration through research and regulatory engagement.[63] Regulators and others are making progress towards better understanding the macro risks from AI systems used in financial products and services, but data and knowledge gaps remain and may widen as technological advances may outpace regulatory assessment.

In addition, the rapid evolution of AI technologies may require close monitoring and revisiting of risk assessment as technologies evolve. Regulators and others have limited understanding of how AI models work, what they a capable of, and what their impacts may be. If regulated firms use complex and opaque datasets, models, and systems, some of which are provided by non-regulated firms, data and knowledge gaps could widen. The widespread use of AI systems developed or used by a concentrated field of AI providers outside the regulated financial system could exacerbate opacity and potentially mask indicators of the build-up of risks. Even within the regulatory perimeter, it may be difficult to untangle where AI is being used within a system and how, as AI components could be embedded in broader systems. Complexities in data, models, and systems may significantly increase the challenge for firms in managing the risks from their utilization, and regulators in understanding how their use produces risks.

In addition to the areas discussed above, IOSCO identified the following additional areas as ones to monitor:

- **Interconnectedness:** One key issue that AI deployment highlights is growing interconnectedness. Financial institutions and their service providers increasingly share technology, infrastructure software, and data. This is true both for firms that are within the regulatory perimeter and those that provide services but may not be regulated as financial firms (such as infrastructure, data, or model providers). The actions of one entity can affect others, firms can become critical nodes, and firms can be exposed to common weaknesses. A vulnerability of one firm in the financial markets could simultaneously impact many firms. Such an event could disrupt core institutions and vital services, and also potentially cause market disruption. A failure in one AI system can have cascading effects on others, potentially leading to systemic risks and economic instability. AI systems can interact and influence each other in complex ways, creating feedback loops that can amplify risk. The interconnectedness of AI systems could create a "house of cards" effect, where a failure in one part of the system can lead to a collapse of the whole. The adoption of AI to

[63] *Accord* OECD Report, *supra* n.6 at 18 (finding a majority of survey respondents noted no current major risks to financial stability but that such risks are expected to emerge in the future).

enhance existing trading algorithms could trigger extreme price moves, increase volatility in stressed markets, and influence the impact of herding behavior where the AI-infused models respond similarly to such price movements; this could also potentially lead to increased interconnectedness, cascading effects, and flash crashes. The high complexity of AI systems also could make the identification and monitoring of interconnectedness increasingly difficult. The concept of interconnectedness can amplify multiple other risks discussed herein. The interconnectedness of AI systems also makes them more vulnerable to cyberattacks. A breach in one system could potentially compromise the security of others, potentially leading to data breaches, disruptions, and financial losses. If there is widespread reliance on common datasets or models, the sector could become increasingly vulnerable to cyberattack through data or model poisoning at various points throughout the AI supply chain, including during training, testing, and production use.

- **Herding**: The widespread use of common models and datasets may have potential impacts on financial markets, in particular if these models and datasets are used in similar ways by systemically important institutions or by large cohorts of market participants.[64] However, IOSCO identified this scenario as one that is subject to some debate, and for which there is a lack of sufficient data to assess fully. Some market participants have expressed their opinions that models, data sets, and use cases in financial markets will be sufficiently diverse so as to obviate concerns around this scenario. However, some have posited that if the use of common models and datasets for trading-related applications were to become widespread, this could increase systemic risk if large numbers of market participants are prompted to make the same decisions at the same time.[65] For example, the use of the same co-pilots or robo-advisers could lead to homogeneous decision-making;, if the use of AI-driven trading decisions were to become widespread, using common models and datasets could lead to market events such as a loss of liquidity and/or market volatility in unexpected or stressful market conditions if such AI systems respond to stress in a similar way (become correlated) or collapse if changing market or geopolitical conditions render historical patterns irrelevant.[66] Some posit that traders applying similar models, training data, and trading strategies (monocultures) may lead to market concentrations and inefficiencies. AI system complexities may make it hard to predict or quantify fragilities, such as loss of liquidity and volatility that could result from one-way, rapid, automated trading decisions, and which could adversely

64 *See, e.g.*, G. Gensler and L. Bailey, *Deep Learning and Financial Stability* (Nov. 1, 2020), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3723132.

65 *See id* at 4 ("History and economics have shown that following early phases of competitive diversity, finance often recedes to more technological uniformity with concentrated actors and interconnected systems.").

66 For a discussion of algorithmic trading and its impacts on the financial markets, *see* IMF Report, *supra* n.6 at 86 *et seq*. The IMF Report notes that GenAI could facilitate the proliferation of algorithmic trading across asset classes, trading venues, and regions. *Id.* at 88. The IMF Report concludes that the impact from a financial stability perspective is highly uncertain and that multiple scenarios could materialize with respect to liquidity, leverage, and interconnectedness. *Id*. at 89. *See also* BIS AI paper, *supra* n.3 at 9 ("[E]arly rule-based computer trading systems were associated with cascade effects and herding, for example, in the 1987 US stock market crash. With machine learning models, the risks of uniformity, model herding and network connectedness have only compounded.").

impact key services or infrastructure in financial services. Such vulnerabilities could be targeted by malicious actors, potentially themselves using AI systems to automate attacks.

- **"Collusive" or "Scheming" Behaviors**: It is relatively common for trading algorithms to rely on ML techniques that analyze historical data to predict future trading prices and volumes of financial instruments. As AI systems become more complex and difficult to explain or predict, the deployment of AI models for investment strategies and trade execution could lead to a risk of coordinated behavior between AI models that might "learn" from their behaviors to optimize trading decisions. This could be exacerbated by concentration risk if there are a small number of AI model providers and the uses of models are comparable in the underlying data and intended objectives.[67] Preliminary research has shown that even when unintended, multiple black box models will eventually learn to engage in collusive behavior to maximize their profits.[68] Other recent research cites evidence that AI agents may covertly pursue goals that are misaligned with given goals.[69] IOSCO did not uncover evidence to suggest that complex AI systems currently are being used at scale in trading applications; thus, the evidence of potential collusive or scheming behavior risk appears theoretical at present but warrants further study.

[67] *See* Gensler and Baily, *supra* n.64 at 26; *see also* OECD (2017), *Algorithms and Collusion: Competition Policy in the Digital Age*, available at https://www.oecd.org/en/publications/algorithms-and-collusion-competition-policy-in-the-digital-age_258dcb14-en.html.

[68] *See AI Expert Warns of Algo-Based Market Manipulation* (Jan. 24, 2024), available at https://www.risk.net/risk-management/7958887/ai-expert-warns-of-algo-based-market-manipulation. *See also* BIS AI Paper, *supra* n.3 ("Regulators, especially competition authorities, have also started highlighting intentional and unintentional algorithmic collusion, especially with algorithms based on reinforcement learning, with potential implications for algorithmic trading in financial markets." (citations omitted)).

[69] *See supra* n. 64.

V. Steps Market Participants Have Taken to Manage Risks, and Govern Internal Development, Deployment, and Maintenance of AI Systems

IOSCO, through its roundtables and literature reviews, found that some financial institutions reported that they are establishing or have established approaches to the development, deployment, and maintenance of AI systems. These firms reported to have opted either to establish a separate AI risk management and governance framework, including bespoke policies, procedures, and controls, or to incorporate AI risk management and governance into existing frameworks. This integration often involved adapting and extending existing structures already put in place for data, model, technology, compliance, and third-party risk management and governance. Some firms also report to have included an independent audit function to validate policies, procedures, and controls.

Firms reported a number of notable features of AI development that have impacted their risk management and governance considerations. The first is that AI technology is becoming embedded in systems that may be available to or used by employees across the organization and that all types of employees, not only those who are trained in the use of data and technology, may be experimenting with or using AI tools. AI is no longer confined to the realm of computer and data scientists and technologically-advanced firms; rather, AI applications are available to everyone—on their computers, phones, and other devices. With this trend, some firms have recognized the need to build controls around AI use holistically across the organization, and must, therefore, consider how to educate and train a much broader population of employees on such topics as computer hygiene, data protection, and privacy, among other topics such as regulatory obligations implicated by various uses of AI technology in regulated activity. One example is educating employees about what types of AI systems are appropriately integrated into work activities and what types are not. Another is to specifically include GenAI in a firm's written policies and procedures governing acceptable use of technology within the firm or for work-related purposes. Another is educating employees about the risks of using personal devices to run AI tools for work-related purposes, which could result in regulatory issues, data protection and privacy issues, and potential breaches of client agreements.

A second feature has emerged with the introduction of GenAI, LLMs, and General Purpose AI. That is, market participants have recognized that risk management and governance may not neatly fit within one organizational line. The risk profile associated with various AI use cases may span responsibilities of several organizational lines within a firm. When looking to integrate more recent AI technologies, firms have recognized the need to staff their risk management and governance groups with employees from across the organization with sufficient seniority and expertise. This includes employees with AI technical expertise, but also typically includes employees from the business unit for which the technology use is

being developed, as well as legal, compliance, cybersecurity, data privacy and protection, and risk management personnel. Depending upon the application at issue, firms have also included experts in the areas of the ethics and sustainability. Thus, there is recognition that risk management and governance teams will need to be interdisciplinary to navigate issues requiring diverse expertise. Importantly, firms have recognized that appropriate governance entails the right "tone from the top" and have included senior people in the risk management and governance process, often reserving a senior position for a "Chief AI Officer." Also raised was the view that domain experts will be needed at each stage of AI technology development and/or acquisition, implementation, testing, evaluation, use, and monitoring in order to provide required feedback on model performance and risks to data scientists and others.

Centers of Excellence

Some firms report to have created what are often called a "Center of Excellence," or group within the organization focused on a particular topic. Centers of Excellence often are established to build capacity in an organization in order to onboard requisite knowledge, skills, data, and technology to assess and assimilate emerging developments. Such groups can have a number of functions, including developing subject matter expertise, creating of a framework for assessing and analyzing AI technology, creating a standardized approach across the AI lifecycle (identifying, evaluating, designing, building, testing, deploying, maintaining, monitoring, analyzing, and deprecating AI use cases), and developing controls around AI use.

A third feature also relates to the criticality of data and cybersecurity. Risk management and governance of AI use requires attention not only to the models used, but also to the data used to train AI models to assess data quality and provenance, and cybersecurity issues arising from the models and data, and to focus on the environment in which the AI model is deployed, to ensure that firm and customer data is protected.

A fourth feature relates to the non-deterministic nature of certain AI technologies, which rely on probabilistic algorithms, making AI models potentially unpredictable and difficult to explain. As firms explore using such AI technologies, they may be focusing on whether they can mitigate harm by preventing certain negative outcomes rather than meeting a specified set of requirements. This analysis often examines the potential impacts of a particular use case, given its capabilities, and determining whether the impacts fall within an acceptable band and/or can be appropriately mitigated.

Firm oversight of AI systems reported to IOSCO appeared calibrated in part by the type of AI used, the use case for which the AI is employed, and the risk profile of the AI system. Firms also appear to have assessed that low-risk use cases may require a lower level of risk management and governance than those directly impacting business processes, those that are material for decision making, and those that are used in a customer-facing application. Some firms have cautioned that the outright ban of certain AI tools may incentivize employees to use personal devices to conduct work, which raises a number of issues discussed above. Rather than implement bans, some firms have implemented vaulted (or "sandboxed") access to newer AI tools in a controlled environment to allow for experimentation without the possibility of data leakage or client harm.

Overall, larger firms in the financial sector appear to be using risk management and governance frameworks for internal AI strategy, processes, risk management and technology onboarding that appear to incorporate some or all of the following principles:

- **Transparency:** AI systems should be understandable in terms of how they operate. Users and clients should receive accurate and complete disclosure around the use of AI in connection with the provision of financial products and services.

- **Reliability, Robustness, and Resilience:** AI systems should perform consistently, reliably, and as intended over time.

- **Investor and Market Protection:** AI systems used in the financial sector are subject to applicable investor and market protection frameworks.

- **Fairness:** AI should not be used in a way that results in unfair bias or discrimination.

- **Security, Safety, and Privacy:** There should be adequate measures around data quality and provenance, privacy, and cybersecurity.

- **Accountability:** There should be a clear assignment of roles and responsibility for AI usage by financial service providers, including for risk management and governance of AI systems, and for the impact and errors of AI systems inside and outside of the firm.

- **Risk Management and Governance:** There should be an effective mechanism in place to establish a strategy for AI, provide appropriate training, and oversee the development, implementation, use, and monitoring of AI use cases. This often includes risk monitoring and management, including model, data, and third-party risks.

- **Human Oversight:** AI systems should be used as a tool to augment, and not replace, human decision making and judgment.

It is important to note that each jurisdiction may have legal and regulatory frameworks that address risk management and governance in different ways. Firms conducting activities in various jurisdictions are subject to applicable frameworks.

Financial Firms' Use of Third-Party Outsourcing

Financial firms report that they rely, to varying degrees, upon vendors or external providers as part of their deployment of AI. For example, firms often contract with third parties for AI models, data, and/or infrastructure. Even if a firm develops its own models or uses its own data, it most likely is hosting tools and data on a third-party cloud service provider. Financial firms employing AI have often adapted existing third-party risk management frameworks to include the use of third-parties' AI technologies.

Financial firms have reported difficulties in obtaining information from a third party about its AI technology—models, and training data in particular—to assess and manage the risks of using the AI technology. Vendors may not be able to describe how a complex model processes data. They may be unwilling to reveal information about a model or the data used to train a model, given competition concerns and exposure to liability if the data was obtained without appropriate consents. Typically, firms should ensure that their relationships with third parties allow them sufficient access to information and control over the AI system they are using to comply with applicable regulatory obligations.

Some considerations firms reportedly have given when managing third-party risk involving AI use generally encompass risk assessment of a vendor, pre- and post-contract due diligence, contractual safeguards, and ongoing monitoring. In addition, firms reported making inquiries of vendors' own use of AI systems to assess whether that use could pose any threat to the firm's own business or data. Some firms have reportedly attempted to mitigate third-party risk by creating an inventory of all vendor applications using AI, which must be approved by a governance committee. In addition, some firms report that voluntary frameworks (such as the NIST AI Risk Management Framework) may be of assistance in managing third-party AI relationships, such as requesting Service Organization Control (SOC) audits from an independent provider in order to ensure its integrity.

Prominent vendors have publicly noted their support of AI accountability, and that documentation and disclosures are especially important in the case of third-party models. According to those vendors, model providers should include documentation how their model is intended to be used, known inappropriate uses, known risks, and recommendations for organizations deploying the model and individuals who are users of the model. Certain vendors also have noted their view that firms using an AI application should be responsible for disclosure and documentation around its use.

Human-in-the-Loop

A topic often referred to in discussions around the supervision of AI systems explores how human input is involved in automated activity. Generally, this topic is shorthanded as "human-in-the-loop," and describes how a person actively participates in an AI system's lifecycle, including its training, operation, and evaluation. Where and how a human is in the loop may vary, depending on the potential impacts of a particular AI use case, how material the AI component is to that use case or its impact, whether the AI is triggering a real-world action, and whether the human can provide meaningful input or intervene in the AI system. Also relevant is what relationship the human has to a particular user or consumer of the AI system. Financial service firms generally

acknowledge that they retain accountability for their use of AI systems in financial products and services, and that they remain responsible for legal and regulatory obligations.

Some have suggested a shift in framing to the term "AI-in-the-loop," as a reminder that AI is best viewed as a co-pilot or assistant to humans, who remain responsible persons with legal and regulatory obligations for regulated activities, regardless of the technologies they deploy to carry out those activities. Others advocate for the term "augmented intelligence" to emphasize that an AI system is augmenting its user's intelligence, rather than having its own intelligence.[70] Regardless of terminology used, some market participants have expressed the view that the concept of "human-in-the-loop" may be prone to a number of challenges and risks in practice, including:

- Ensuring high-caliber human input into modelling and training;
- Ensuring humans tasked with supervision are adequately trained and empowered to identify problematic designs or outcomes – those who design or use technology applications may not appreciate regulatory obligations;
- Guarding against a dynamic where human oversight is sacrificed for speed or profits;
- Preventing over-reliance on AI systems that would lead to human incapacity to supervise or intervene in a meaningful way;
- Addressing lack of explainability and inherent complexity, which may impede human oversight and intervention; and
- Considerations around human oversight as AI systems become "agentic," or capable of taking actions autonomously.

The IOSCO 2021 AI Report noted a primary theme underpinning the ethical use of AI as "human autonomy, including auditability." This theme was intended to "ensure that humans have power over what [a] model can and cannot decide," and the theme remains central to considerations around increasing automation and, in particular, when considering AI agents. AI agents use LLMs and other tools to plan and execute tasks autonomously, using real-time information and real-world actions. AI agents typically operate by leveraging LLMs, external tools and data, and

70 *See* U.S. Treasury AI Cybersecurity Report, *supra* n.17 at 33.

memory.[71] They can generate a workplan, adjust their behavior over the course of their workplan, and take actions on behalf of their user through interacting with other systems and executing actions across the workplan. AI agents can also interact with other AI agents, in "multiagent" AI systems, which may amplify risks due to complex interactions and errors from upstream agents propagating downstream.

The introduction of AI agents into financial products and services adds complexities to supervision, and can increase risks discussed herein. Specifically, we discuss risks that accompany agents making decisions and taking actions with little or no human oversight or acting in a way that is misaligned with regulatory obligations or investor and market protection, in addition to risks associated with data protection and misuse.[72] If AI agents were to grow in their ability to take real-world actions and in their use, new risks may emerge, including systemic risks and potential misalignment of an AI agent's goals or methods with those of a human.[73]

[71] *See Agents*, J. Wiesinger, P. Marlow, and V. Vuskovic (Sep. 2024), available at https://media.licdn.com/dms/document/media/v2/D561FAQH8tt1cvunj0w/feedshare-document-pdf-analyzed/B56ZQq.TtsG8AY-/0/1735887787265?e=1736985600&v=beta&t=pLuArcKyUcxE9B1Her1QWfMHF_UxZL9Q-Y0JTDuSn38, at 40 ("Tools, such as Extensions, Functions, and Data Stores, serve as the keys to the outside world for agents, allowing them to interact with external systems and access knowledge beyond their training data. Extensions provide a bridge between agents and external APIs, enabling the execution of API calls and retrieval of real-time information. functions provide a more nuanced control for the developer through the division of labor, allowing agents to generate Function parameters which can be executed client-side. Data Stores provide agents with access to structured or unstructured data, enabling data-driven applications.").

[72] Certain market participants are reported to be developing applications and software development kits (SDKs) to enable market participants to build and deploy AI-powered agents to conduct financial activities. In traditional market infrastructures, it may be that AI agents will be more limited in what real-world activities they could undertake, or they may more easily be subjected to supervision and intervention. In other markets, e.g., so-called "DeFi" markets, technology is emerging that would enable users to develop, deploy, and monetize AI agents using distributed ledger (DLT) or blockchain infrastructures. These DLT-based AI agents may be able to process information and undertake certain activities autonomously, such as analyzing blockchain data, engaging in blockchain transactions including those carried out using crypto-asset addresses and smart-contract enabled protocols, and engage in social media interactions. These DLT-based AI agents are being designed to integrate with various LLMs. In such an environment, AI agents could further automate the issuance, marketing, and sale of crypto asset financial products and services. Such activity if carried out outside the regulatory perimeter or in violation of applicable regulations, presents risks to investors and the markets.

[73] *See* BIS AI Paper, *supra* n.3 at 13. One recent study notes that LLMs deployed as autonomous agents may engage in "scheming," which the study defines as "covertly pursu[ing] misaligned goals, hiding their true capabilities and objectives. *See Frontier Models are Capable of In-context Scheming* (Dec. 5, 2024), A. Meinke, B. Schoen, J. Scheurer, M. Balesni, R. Shah, and M. Hobbhahn, available at https://static1.squarespace.com/static/6593e7097565990e65c886fd/t/6751eb240ed3821a0161b45b/1733421863119/in_context_scheming_reasoning_paper.pdf (identifying multiple scheming behaviors in frontier models, i.e., models strategically introduce subtle mistakes into their responses, attempt to disable their oversight mechanisms, and even exfiltrate what they believe to be their model weights to external servers").

VI. Responses by IOSCO Members

IOSCO surveyed its Members on steps they have taken to understand, monitor, and respond to the development and use of AI systems in the financial sector. This section provides an overview of existing and proposed responses of surveyed IOSCO Members.[74] Although this section highlights those responses, it does not endorse any particular approach or make policy recommendations. This section also notes preliminary policy considerations offered to IOSCO by stakeholders during the IOSCO roundtables.

Regulatory Frameworks Applicable to the Use of AI Technologies in the Financial Sector

IOSCO Member respondents reported that applicable frameworks within their respective jurisdictions can be broadly categorized as:

(i) Existing Frameworks/Technology-Neutral: Certain surveyed IOSCO Members reported regulating AI activities in the financial sector by applying their existing regulatory frameworks. Some reported they take a "technology-neutral" approach, which generally refers to regulating certain activity or conduct without regard to the specific technology used in that activity or conduct.

***(ii) Specific Legal Requirements/Guidance*:** Certain surveyed IOSCO Members reported that they use specific legal or regulatory requirements to govern the use of AI systems, whether rules-based or principles-based. A rules-based approach typically refers to detailed and specific rules that market participants must comply with, while a principles-based approach refers to broad principles that guide the behavior and decision-making of market participants, allowing for different approaches in carrying out a certain activity. Some respondents reported that they issued non-binding guidance to establish expectations and clarifications on how their legal requirements should be applied to the use of AI systems.

***(iii) Bespoke/AI-Specific Frameworks*:** Certain surveyed IOSCO Members reported implementing a bespoke regulatory framework to explicitly address the unique challenges posed by the use of AI technologies in the financial sector. An AI-specific regulatory approach looks to craft specific rules and guidelines tailored to the use of AI technologies.

[74] The responses from surveyed IOSCO Members appear generally consistent with the mapping of policy approaches highlighted in the OECD Report. *See* OECD Report, *supra* n.6 at 10 ("The vast majority of respondent jurisdictions have introduced some form of policy that covers AI in (parts of) finance, albeit in different forms: cross-sectorial [sic] legislation covering part of financial activity; binding rules or proposals issued by financial regulators, and non-binding policy guidance or clarifications released by financial regulators/supervisors. Importantly, these approaches are not mutually exclusive."). For a more detailed overview of certain jurisdictional approaches, *see id*.

Existing Frameworks

Some IOSCO Member respondents indicated that the use of AI systems in the financial sector falls under existing financial sector regulations in their jurisdictions. Based on survey responses, these regulations cover areas such as disclosure, promotions, advertising, risk management, internal systems and controls, third-party outsourcing, cybersecurity, investment services, algorithmic trading, and data protection.[75] More specifically, for respondents who reported that they apply existing regulations and guidance to activities involving financial market participants' use of AI systems, these existing frameworks typically address one or more of the following activities:

a) Disclosure concerning AI-related issues by issuers of securities;

b) Disclosure concerning AI use by providers of financial products and services;

c) Promotions, advertisements, and marketing of AI-related financial products and services;

d) Governance over AI development and deployment by providers of financial products and services; and

e) Use by providers of financial products and services of outside vendors and service providers that design and maintain AI technologies.

Guidance

Some respondents indicated that, although the use of AI is encompassed within existing regulation, they have issued guidance (in final form or for consultation) to address uses of AI technologies in the financial sector. Guidance published by regulators in this context addresses elements such as compliance with securities laws, governance, risk management, data protection, algorithmic biases, transparency, and ethical use and development of AI systems.

Below are some examples that illustrate how various jurisdictions have addressed specific aspects of the use of AI systems in the financial sector, responding to the distinctive challenges and risks they have identified in these areas:

- **Hong Kong**: In November 2019, the Hong Kong Monetary Authority (HKMA) issued high-level principles for the use of AI technologies in the banking industry, covering governance, application design and development, ongoing maintenance and monitoring, and consumer protection.[76] In May 2024, the HKMA also issued guidance for authorized institutions, reiterating the importance

[75] *Accord* OECD Report, *supra* n.6 at 9 ("Where AI is used within areas for applications that are covered by existing rules or guidance, such rules or guidance should generally apply … [including] rules on prudent business, consumer/investor protection laws and regulations, guidance on model risk management, third-party risk management, disclosure requirements, handbooks related to IT governance, and cyber-security and operational resilience laws and regulations, as well as fairness laws, which continue to apply irrespective of the technology used.").

[76] Hong Kong Monetary Authority (2019), *High-level Principles on Artificial Intelligence*, available at https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191101e1.pdf.

of staff competence and ethical behavior at all levels within an authorized institution's organizational structure, as well as the measures they are expected to adopt in monitoring and maintaining the competence levels and ethical behavior of relevant staff.[77] In November 2024, the Hong Kong Securities and Futures Commission (SFC) issued a circular to licensed corporations on the use of GenAI language models.[78]

- **European Union**: In May 2024, ESMA published initial guidance for firms using or planning to use AI when providing investment services to retail clients (without prejudice to any additional actions that firms are expected to undertake to ensure compliance with the broader EU framework on digital governance (e.g., AI Act)). This guidance outlines the expectations for such firms to comply with relevant MiFID II requirements, especially those related to organizational aspects, conduct of business, and their regulatory obligation to act in the best interest of the client. The guidance provides examples of when the use of AI technologies by investment firms would be covered by requirements under MiFID II, such as customer support, fraud detection, risk management, compliance, and support to firms in the provision of investment advice and portfolio management.[79]

- **Canada:** In December 2024, the Canadian Securities Administrators (CSA) published guidance on how Canadian securities legislation applies to the use of AI systems by market participants, including registrants, reporting issuers, and marketplaces.[80] The notice outlines selected requirements under securities law that market participants should consider during an AI system's lifecycle and provides guidance on how the CSA interprets the requirements in this context. It highlights the importance of AI system governance and oversight, maintaining explainability and transparency, providing robust disclosure and managing conflicts of interest. The notice also seeks

[77] Hong Kong Monetary Authority (2024), *Competence and Ethical Behaviour*, available at https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/CG-6.pdf. See also Hong Kong Monetary Authority (2024), *Consumer Protection in respect of Use of Generative Artificial Intelligence*, available at https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2024/20240819e1.pdf; Hong Kong Monetary Authority (2024), *Research Paper on Generative Artificial Intelligence in the Financial Services Sector*; available at https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2024/GenAI_research_paper.pdf; Hong Kong Monetary Authority (2024), *Generative Artificial Intelligence Sandbox*; available at https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2024/20240920e1.pdf.

[78] Hong Kong Securities and Futures Commission (2024), *Circular to licensed corporations - Use of generative AI language models,* available at https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=24EC55.

[79] European Securities and Markets Authority (2024) *Public Statement On the Use of Artificial Intelligence (AI) in the Provision of Retail Investment Services* (May 30, 2024), available at https://www.esma.europa.eu/sites/default/files/2024-05/ESMA35-335435667-5924_Public_Statement_on_AI_and_investment_services.pdf.

[80] *See* Ontario Securities Commission, *Staff Notice and Consultation 11-348: Applicability of Canadian Securities Laws and the Use of Artificial Intelligence Systems in Capital Markets* (Dec. 5, 2024), available at https://www.osc.ca/en/securities-law/instruments-rules-policies/1/11-348/csa-staff-notice-and-consultation-11-348-applicability-canadian-securities-laws-and-use-artificial.

stakeholder feedback through consultation questions on the evolving role of AI systems in capital markets and the opportunities to tailor or modify current approaches to oversight and regulation.

- **United States:** In December 2024, the Commodity Futures Trading Commission's (CFTC's) Divisions of Clearing and Risk, Data, and Market Oversight, and Market Participants Division issued a staff advisory on the use of artificial intelligence in CFTC-regulated markets by registered entities and registrants. The advisory reminds CFTC-regulated entities of their obligations under the Commodity Exchange Act and the CFTC's regulations as these entities begin to implement AI.[81]

Bespoke Frameworks

Several IOSCO Member respondents reported that their jurisdictions have bespoke laws or regulations to address the use of AI systems and associated risks, which may be applicable to the use of AI in capital markets. These include existing laws and regulations already in place, as well as new laws and regulations that have been proposed or amended. For example:

- **Greece**: Enacted in 2022, Greek Law 4961/2022 sets out the national framework for the regulation of emerging technologies under conditions of trustworthiness, safety and cybersecurity, consumer protection, respect for fundamental rights and the democratic rule of law. Among other things, Part A aims to establish the adequate institutional framework for the exploitation of the potential of AI by public and private sector bodies under conditions of fairness and security, as well as to strengthen the resilience of the public administration against cyber threats.[82]

- **Japan**: In April 2024, Japan's Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry jointly published the "AI Guidelines for Business" to govern AI use in business, which encompasses capital market firms. The guidelines present ten guiding principles that each AI business actor must implement and highlights specific considerations for each type of actor: developers, providers, and business users. The guidelines also emphasize principles such as human-centricity, safety, fairness, privacy protection, security, transparency, and accountability.[83]

- **European Union**: Several European survey respondents highlighted that the European Union's Artificial Intelligence Act (EU AI Act)[84] will apply to all uses of AI systems across the European Union, including those in the financial sector. In particular, the AI Act sets out certain obligations for the deployers and providers of AI systems that are used in applications considered "high-risk."

81 *CFTC Staff Issues Advisory Related to the Use of Artificial Intelligence by CFTC-Registered Entities and Registrants* (Dec. 5, 2024), available at https://www.cftc.gov/PressRoom/PressReleases/9013-24.

82 *See The Regulation of Emerging Technologies in Greek Law*, A. Broumas and P. Charalampous (Feb. 29, 2024), available at https://www.iipitec.eu/iipitec/article/view/25#:~:text=Greek%20Law%204961%2F2022%20sets,the%20democratic%20rule%20of%20law.

83 Japan Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry, *AI Guidelines for Business Ver1.0*, (Apr. 19, 2024), available at https://www.soumu.go.jp/main_content/000943087.pdf.

84 *The EU Artificial Intelligence Act*, available at https://artificialintelligenceact.eu/.

Regarding the financial sector, the EU AI Act identifies two high-risk use cases: AI systems used to evaluate creditworthiness of natural persons and for risk assessments and pricing for life and health insurance.

- **Brazil:** Brazil has proposed a framework to govern the development and use of AI. This legislative activity builds on the Brazilian AI Strategy, which aims to promote trustworthy and ethical AI. A group of legal experts proposed in May 2023 Draft Bill 2.338/2023 that aims to regulate the use of AI in the country and that is currently discussed in the legislature.[85]

- **Canada**: The Canadian Parliament considered legislation (the *Artificial Intelligence and Data Act* or AIDA)[86] that would have applied to the development and deployment of all AI systems, including those in the financial sector. Among other things, AIDA aimed to establish common nationwide requirements for the design, development, and deployment of AI systems, and ensure high-impact AI systems meet safety and human rights expectations while prohibiting certain AI practices that could cause serious harm.

- **Australia**: The Australian Government is considering whole-of-economy regulation of AI, which would apply to the financial sector. In January 2024, it published its interim response to a 2023 consultation on supporting safe and responsible AI, indicating a proactive approach to AI regulation.[87] In September 2024, the Government commenced a consultation on introducing mandatory guardrails for AI in high-risk settings.[88] The guardrails, if legislated, would set expectations on how to use AI safely and responsibly when developing and deploying AI in Australia in high-risk settings.

Additionally, some respondents reported to have issued papers or circulars suggesting expected standards for market participants using AI systems or related technologies. Topics include AI disclosure, cyber security, data quality management, and compliance.

85 *See Brazil's Path to Responsible AI* (Jul. 27, 2023), available at https://oecd.ai/en/wonk/brazils-path-to-responsible-ai.

86 *Bill C-27: An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts*, available at https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c27_1.html.

87 Commonwealth of Australia (2024), Safe and responsible AI in Australian consultation, available at https://consult.industry.gov.au/supporting-responsible-ai.

88 Commonwealth of Australia (2024), Safe and responsible AI in Australia, available at https://consult.industry.gov.au/ai-mandatory-guardrails.

Other Measures Taken by IOSCO Members

Regulatory Engagement

Besides focusing on regulatory frameworks and guidance, regulators reported other measures to address the use of AI in financial markets. All but one survey respondent indicated that it had engaged with market participants on this subject. The respondents reported various means of engagement, such as surveys, market studies, research, innovation hubs, roundtables, and engagement meetings. For example:

- **Singapore**: The Monetary Authority of Singapore (MAS) launched "Project MindForge" in 2023 to examine the risks and opportunities of GenAI in the financial services. In phase one of this initiative, a GenAI risk framework was co-created by a consortium comprising MAS, banks, and technology partners. [89] This framework, which builds upon MAS' Fairness, Ethics, Accountability, and Transparency (FEAT) principles,[90] evaluated the risks associated with the use of a GenAI system in the financial sector at different stages of its lifecycle and mapped several major risks across different dimensions (Accountability and Governance, Monitoring and Stability, Transparency and Explainability, Fairness and Bias, Legal and Regulatory, Ethics and Impact, and Cyber and Data Security) to enable financial institutions to use GenAI in a responsible manner. In the next phase, the MindForge consortium will expand its scope to involve financial institutions from the insurance and asset management industries. The consortium will also focus on AI governance and aims to develop an AI governance handbook for the financial industry.

- **Netherlands**: In September 2023, the Dutch Authority for the Financial Markets (AFM) conducted a study on market manipulation detection and compliance supervision with legal requirements for firms using trading algorithms and AI systems.[91]

- **United Kingdom:** In 2024, the United Kingdom's Financial Conduct Authority (FCA) launched its AI Lab, which provides a pathway for the FCA, firms and wider stakeholders to engage in AI-related insights, discussions, and case studies. It also seeks to support innovators in developing new AI models and solutions, help the FCA deepen its understanding of the risks and opportunities AI presents to UK consumers and markets, and inform its regulatory approach in a practical, collaborative way.[92]

Many survey respondents indicated they had provided at least one form of assistance with respect to the use of AI in the financial sector. For example, 15 of 27 had provided oral or written guidance; while six of

89 *See* https://www.mas.gov.sg/schemes-and-initiatives/project-mindforge.

90 Monetary Authority of Singapore (2018), *Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector*, available at https://www.mas.gov.sg/publications/monographs-or-information-paper/2018/feat.

91 Netherlands Authority for the Financial Markets (2023), *Machine Learning in Algorithmic Trading* (Sep. 28, 2023), available at https://www.afm.nl/en/sector/actueel/2023/maart/her-machine-learning.

92 *See* https://www.fca.org.uk/firms/innovation/ai-lab.

27 had provided a product trial, sample data, or a testing environment (e.g., a "sandbox" or "accelerator"). However, no survey respondents reported providing waivers of, or exemptions from, certain regulatory requirements respecting market participants' use of AI in the financial sector.

Other IOSCO members reported that they consulted with market participants on ways to mitigate the risks associated with the use of AI in the financial sector.

Collaboration Among Authorities

Almost all IOSCO Member survey respondents reported that they collaborate with various domestic authorities within their jurisdictions concerning AI, including central banks, and privacy and data protection agencies, as well as trade, competition, and other financial services regulators. These collaborations were reported to have encompassed information-sharing, risk assessment and mitigation, consulting on national AI legislation or frameworks, supporting AI regulatory sandboxes, and developing AI guidelines.

Approximately one-third of survey respondents highlighted that they collaborated with overseas authorities, primarily through international fora, workshops, and working groups, such as those organized through IOSCO. Significant multilateral collaboration was also noted among EU members through the European Supervisory Authorities (ESAs). Particularly, EU members noted their participation in the European Forum for Innovation Facilitators (EFIF) framework and monitoring AI risks through the ESMA Risk Standing Committee, which led to several ESMA publications.

Most survey respondents reported no challenges in engaging with other domestic or overseas authorities.[93]

Supervisory and Enforcement Efforts

Market regulators also reported to have undertaken various supervisory efforts and enforcement actions involving the use of AI by market participants or others in furtherance of misconduct or non-compliant conduct.[94]

[93] Three survey respondents indicated there were unique challenges in cross-border cooperation and information sharing on AI in the financial sector, including the complexity of AI's cross-sectoral and cross-jurisdictional nature, and issues related to the data quality to be collected and shared, and legal frameworks for information sharing.

[94] See United States Securities and Exchange Commission, Division of Examinations, *Fiscal Year 2025 Examination Priorities*, at 10, 13-14, available at https://www.sec.gov/files/2025-exam-priorities.pdf ("If advisers integrate artificial intelligence (AI) into advisory operations, including portfolio management, trading, marketing, and compliance, an examination may look in-depth at compliance policies and procedures as well as disclosures to investors related to these areas."); *see also id*. ("With respect to AI, the Division will review registrant representations regarding their AI capabilities or AI use for accuracy. In addition, the Division will assess whether firms have implemented adequate policies and procedures to monitor and/or supervise their use of AI, including for tasks related to fraud prevention and detection, back-office operations, anti-money laundering (AML), and trading functions, as applicable. Reviews will also consider firm integration of regulatory technology to automate internal processes and optimize efficiencies. In addition, the Division will examine how registrants protect against loss or misuse of client records and information that may occur from the use of third-party AI models and tools.").

On the supervisory front, certain surveyed IOSCO Members reported they established specialized teams to better address emerging issues and risks associated with AI. They reported having prioritized examination efforts to focus on certain services involving AI and the risks associated with the use of AI and alternative data.[95]

To enforce existing rules and regulations, certain IOSCO members reported having taken enforcement actions against market participants related to AI. For example, the U.S. SEC has filed a number of enforcement actions against individuals and entities for making false and misleading statements about their use of AI.[96]

Resources and Expertise

Several surveyed IOSCO Members reported that they were assessing the resources and skills required to adequately analyze and supervise market participant's uses of AI. Many of these regulators reported that they were evaluating the need for additional resources and were adding resources, while other regulators reported that they intend to create or increase resources to address AI uses in the financial sector. For example, some respondents reported developing expertise in the areas of data requirements, integrating or optimizing of existing IT or business processes, working on internal frameworks or governance structures (notably to identify gaps brought by AI), and building staff capability and literacy through employee training. Certain respondents reported that they formed dedicated central teams for AI oversight and response, serving as subject matter experts, and that they engaged with academic institutes to develop training for staff and other experts within their remit.

Regulators also reported participating in AI-related work or solutions with external parties, mostly in the context of public or government-led initiatives, as well as collaborating with other public bodies or research institutions. Examples of government-led initiatives included the development of AI policies, rules, or assurance frameworks. Collaborations with other public bodies include the funding of programs for the development of AI tools in specific areas, such as detection of market abuse or due diligence applications.

[95] *See, e.g.*, United States Securities and Exchange Commission, Division of Examinations, 2024 Examination Priorities, available at https://www.sec.gov/files/2024-exam-priorities.pdf, at 3, 19.

[96] *See, e.g.*, www.sec.gov/finhub (click on "Artificial Intelligence/Machine Learning, Regulation and Related Matters" for a list of SEC AI-related enforcement actions); *cf.* Australian Securities & Investments Commission, *ASIC Alleges IAG Misled Home Insurance Customers on Pricing Discounts (Aug. 25, 2023), available at* https://asic.gov.au/about-asic/news-centre/find-a-media-release/2023-releases/23-228mr-asic-alleges-iag-misled-home-insurance-customers-on-pricing-discounts/ (ASIC pursuing litigation against an insurer for allegedly misleading customers about the extent of the loyalty discount they would receive, where the insurer used a pricing process which included the output of a machine learning model that ASIC alleges could erode the value of the promised loyalty discounts for customers with higher propensity to renew. The way the insurer operated the algorithm meant that some longer term or more loyal customers, who were entitled to loyalty discounts but had higher propensity to renew, were allegedly allocated, or may have been allocated, higher premiums before loyalty discounts were applied).

Information Gathering & Factfinding

A number of jurisdictions and authorities reported having engaged in information gathering and factfinding regarding the use of AI in financial markets. For example:

- **European Union**: In February 2023, ESMA studied the use of AI in its markets, finding varying metrics about the proportion of its registrants using AI. Notable use cases included applying natural language processing for investment research. Based on the regulatory and marketing documentation from EU-domiciled mutual funds, ESMA identified 54 entities (less than 0.2% of EU mutual funds) that promoted their use of AI. ESMA found a growing relevance of third-party AI system providers, use of AI in trading, and a large proportion of credit rating agencies using AI and natural language processing as part of their research, writing, or internal processes. [97] In a survey conducted in October 2023, ESMA found that a majority of credit rating agencies and market infrastructures were either already using GenAI tools or (more frequently) planned to start using them in the near future.[98]

- **Australia:** ASIC analyzed information about 624 AI use cases (as of December 2023) that 23 licensees in the banking, credit, insurance and financial advice sectors were using, or developing. These use cases, directly or indirectly impacting consumers, included Gen AI and advanced data analytics (ADA) models. ASIC also asked licensees about their risk management and governance arrangements for AI, and how they planned to use AI in the future. ASIC observed a rapid acceleration in the volume of AI use cases, and a shift towards more complex and opaque types of AI such as GenAI. But on the whole, the way licensees used AI was quite cautious. ASIC found some gaps in how licensees assessed risks to consumers from AI, and for some licensees, governance arrangements lagged their AI use.[99]

- **Netherlands**: A survey[100] performed by the AFM[101] noted that a significant proportion of the trading algorithms used by four proprietary traders relied on machine learning at their core. The AFM concluded that machine learning is often used to try to predict future price movements from order book data. These models used at least 100 parameters and were predominantly supervised

97 European Securities and Markets Authority (2023), *Artificial Intelligence in EU Securities Markets*, available at https://www.esma.europa.eu/sites/default/files/library/ESMA50-164-6247-AI_in_securities_markets.pdf.

98 European Securities and Markets Authority (2024), TRV Risk Monitor, available at https://www.esma.europa.eu/sites/default/files/2024-01/ESMA50-524821-3107_TRV_1-24_risk_monitor.pdf, at n.1.

99 Australian Securities & Investments Commission (2024), *Beware the gap: Governance arrangements in the face of AI innovation*, available at https://asic.gov.au/about-asic/news-centre/find-a-media-release/2024-releases/24-238mr-asic-warns-governance-gap-could-emerge-in-first-report-on-ai-adoption-by-licensees/.

100 The Netherlands Authority for the Financial Markets (2023), *Machine Learning in Algorithmic Trading*, available at https://www.afm.nl/~/profmedia/files/rapporten/2023/report-machine-learning-trading-algorithms.pdf.

101 The Netherlands Authority for the Financial Markets also performed a joint study with De Nederlansche Bank on how registrants are using AI. *See The Impact of AI on the Financial Sector and Supervision (Jun. 7, 2024),* available at https://www.dnb.nl/en/sector-news/supervision-2024/afm-and-dnb-publish-report-on-the-impact-of-ai-on-the-financial-sector-and-supervision/.

learning models. The AFM noted that trading firms found performance was of greater interest to the firms than explainability, and that the firms noted that reinforcement learning could potentially lead trading algorithms to learn undesirable behavior. The AFM noted five associated risks to these machine learning algorithms: (i) explainability of the models and how that interacted with regulatory requirements, (ii) potential market manipulation (both on the part of these models, as well as their susceptibility to being manipulated), (iii) procyclical behavior, (iv) concentration risk, and (v) potential knowledge gaps.

- **United States**: In January 2024, the U.S. CFTC staff released a request for comment on the use of artificial intelligence in CFTC-regulated markets.[102] In June 2024, the U.S. Department of the Treasury released a Request for Information (RFI) on Uses, opportunities, and Risks of Artificial Intelligence in the Financial Services Sector.[103] As a result of that public consultation, the Department of the Treasury issued a report in December 2024.[104]

- **United Kingdom**: The Bank of England and Financial Conduct Authority collaborated on three studies on the use of machine learning among British financial services firms, the most recent of which was published in November 2024.[105] The British authorities found that a majority of capital markets institutions (FMIs and entities engaged in investment management) already used or were developing machine learning tools.[106] However, capital markets firms were involved in pilot and test cases of machine learning, as opposed to mature uses of machine learning. Capital markets firms were also the financial services sector with the most extensive use of vendor models, with

[102] *See CFTC Staff Releases Request for Comment on the Use of Artificial Intelligence in CFTC-Regulated Markets* (Jan. 25, 2024), available at https://www.cftc.gov/PressRoom/PressReleases/8853-24.

[103] *See* United States Dept. of the Treasury, *U.S. Department of the Treasury Releases Request for Information on Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector* (Jun. 6, 2024), available at https://home.treasury.gov/news/press-releases/jy2393.

[104] United States Dept. of the Treasury, *Artificial Intelligence in Financial Services, Report on the Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector* (Dec. 2024), available at https://home.treasury.gov/system/files/136/Artificial-Intelligence-in-Financial-Services.pdf. *See also United States Senate Committee on Homeland Security & Governmental Affairs, AI in the Real World, Hedge Funds' Use of Artificial Intelligence in Trading* (June 2024), available at https://www.hsgac.senate.gov/wp-content/uploads/2024.06.11-Hedge-Fund-Use-of-AI-Report.pdf; (report on the use of AI by hedge funds identifying a number of use cases and risks); House Committee on Financial Services, *AI Innovation Explored: Insights into AI Applications in Financial Services and Housing, Staff Report: Bipartisan Working Group on Artificial Intelligence* (July 18, 2024), available at https://democrats-financialservices.house.gov/uploadedfiles/07.18.2024_ai_report_final.pdf (report detailing the use of AI in financial services, including documenting a roundtable the group held with securities markets participants); Congressional Research Service, *Artificial Intelligence and Machine Learning in Financial Services* (Apr. 3, 2024), available at https://crsreports.congress.gov/product/pdf/R/R47997 (report on the extent of AI and machine learning in American financial services).

[105] *See Machine Learning in UK Financial Services* (Oct. 11, 2022), available at https://www.bankofengland.co.uk/report/2022/machine-learning-in-uk-financial-services.

[106] The Investment Association, a trade association representing UK investment managers, released a report detailing the use of artificial intelligence in UK funds management in October 2024. The Investment Association, *Investment Association and Tech Working Group Publish Recommendations to Bolster AI use in Investment Management Industry,* (Oct. 10, 2024), available at https://www.theia.org/news/press-releases/investment-association-and-tech-working-group-publish-recommendations-bolster.

40% of machine learning models implemented through vendor tools (i.e., cloud services). Capital markets firms also reported an evolving stance on the governance of machine learning, with the most mature governance over data used in machine learning.

- **New Zealand**: The New Zealand Financial Markets Authority (FMA) surveyed market participants in September 2024 on their use of AI.[107] It found that firms were actively using AI for fraud detection and risk management. The FMA also noted that registrants predominantly used vendor tools as opposed to developing their own AI tools in-house. Respondents also noted their future AI use plans focused on customer service and risk management.

- **Canada:** The Ontario Securities Commission (OSC) published a report outlining current use cases of AI systems in capital markets. The report found that AI systems were being adopted for efficiency improvement, revenue generation, and risk management with varying scope and scale across a wide range of use cases, including improving the efficiency and accuracy of operational processes, trade surveillance and detection of market manipulation, and supporting advisory and customer service. The report found that, overall, adoption of AI systems had moved beyond exploration and research and was being tactically deployed in several areas. The report outlined the value drivers and challenges associated with AI adoption, and methods to mitigate risks related to the use of AI systems in capital markets.[108] Separately, the OSC also undertook research into investor-facing use cases of AI, including decision support, automation, and scams and fraud. As part of that work, the OSC conducted behavioral science research that found no discernible difference in adherence by retail investors to investment suggestions provided by a human or an AI tool, indicating Canadian investors may be receptive to taking advice from an AI system.[109] A second study found that AI-enhanced scams pose significantly more risk to retail investors compared to conventional scams. It noted that generative AI technologies are enhancing common investment scams by increasing their reach, efficiency, and effectiveness, and that new types of scams are being developed with assistance from AI systems (e.g., deepfakes and voice cloning).[110]

[107] New Zealand Financial Markets Authority, Understanding Artificial Intelligence in Financial Services | Financial Markets Authority (Sep. 10, 2024), available at https://www.fma.govt.nz/news/all-releases/media-releases/understanding-artificial-intelligence-in-financial-services/.

[108] Ontario Securities Commission, *AI in capital markets – exploring use cases in Ontario*, available at https://www.osc.ca/en/industry/artificial-intelligence/ai-capital-markets-exploring-use-cases-ontario.

[109] Ontario Securities Commission, Artificial Intelligence and Retail Investing: Use Cases and Experimental Research, available at https://www.osc.ca/en/investors/investor-research-and-reports/artificial-intelligence-and-retail-investing.

[110] Ontario Securities Commission, *Artificial Intelligence and Retail Investing: Scams and Effective Countermeasures*, available at https://www.osc.ca/en/investors/artificial-intelligence-and-retail-investing-scams-and-effective-countermeasures.

Investor Alerts and Education

Many regulators have acted to make investors, particularly retail investors, aware of the increase of securities frauds involving the purported use of artificial intelligence. This is done primarily through the publication of investor alerts and other investor education related products. Some of these publications are general in nature and speak about broad FinTech risks with brief references to AI and robo-advisory services.[111] Other alerts are specifically tailored to address AI related investment fraud risks.[112] There is an additional category of more narrowly tailored alerts that focus on specific AI firms or products that are not registered with the relevant regulator.[113] In addition to investor education products directed towards investors, some regulators have also directed information towards firms. One such example of such guidance was discussed previously in this report – ESMA's May 2024 guidance for firms regarding the use of AI when providing investment services to retail clients.[114] The theme underlying investor alerts and investor education products is that investors, particularly retail investors, should conduct due diligence prior to deciding to invest in AI focused companies or invest with the assistance of AI technology. The message to AI focused firms and firms using AI to provide investment services to clients is that they are expected to comply with existing laws and regulations in all aspects of their business, including those provisions related to disclosure, registration and marketing of investments, among others.

Input from Roundtable Participants

IOSCO hosted a series of roundtables to engage with various stakeholders in different geographic regions, including academics, technical experts, and industry representatives. Certain stakeholders emphasized the importance for regulators to understand and assess AI-related risks at each step of an AI system's development and deployment, including at the data and model levels. Some stakeholders noted that regulators should collaborate with the industry to develop policies, while cautioning that new policies may

111 *See*, *e.g.*, Swiss Financial Market Supervisory Authority, *You have questions about FinTech and crypto offers*, available at https://www.finma.ch/en/finma-public/fragen-und-probleme/zu-fintech-und-zu-krypto-angeboten; United States Securities and Exchange Commission, *Technology and Digital Finance: World Investor Week 2024 — Investor Bulletin*, available at https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-bulletins/technology-and-digital-finance-world-investor-week-2024-investor-bulletin.

112 United States Securities and Exchange Commission, *Artificial Intelligence (AI) and Investment Fraud: Investor Alert*, available at https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/artificial-intelligence-fraud.

113 *See, e.g.,* Comision Nacional del Mercado de Valores, *CNMV Issues Warning to the Public on Unregistered Firm,* available at https://www.cnmv.es/webservices/verdocumento/ver?e=2Lt2TfzFbD069yVl6jx87JqsmhmHlGKVzGKYDPXP7jQPi57IXgF7VdIcuAns0KKL (issuing warning regarding AIOPERATOR Artificial Intelligence Finance); Swiss Financial Market Supervisory Authority, https://www.finma.ch/en/finma-public/warnungen/warnliste/https-ai-profit-com (issuing warning regarding ai-profit.com); Japan Financial Services Agency, *Names of Persons Engaged in Financial Instruments Business Without Registration*, available at https://www.fsa.go.jp/ordinary/chuui/mutouroku/04.html (JFSA naming the service provider StockLab (English translation)).

114 European Securities and Markets Authority, *Public Statement On the use of Artificial Intelligence (AI) in the provision of retail investment services* (May 30, 2024), available at https://www.esma.europa.eu/sites/default/files/2024-05/ESMA35-335435667-5924_Public_Statement_on_AI_and_investment_services.pdf.

lead to additional burden on market participants, especially when ensuring compliance across different policy frameworks set by jurisdictions where they operate. Others expressed that regulations should be technology-neutral and outcomes-focused, with guardrails that are not static and reviewed on an ongoing basis. They also stressed that the regulatory approach should foster innovation while managing AI-related risks.

Additionally, some stakeholders suggested that voluntary standards issued by industry associations or government agencies could be leveraged by regulators to address the risks related to the use of AI in the financial sector. Specific examples cited by stakeholders were:

- **NIST AI Risk Management Framework 1.0**: In January 2023, the *US Department of Commerce's National Institute of Standards and Technology* (NIST) released the *AI Risk Management Framework 1.0* (AI RMF), which helps organizations to manage the risks related to using AI systems, which include safety, security and resiliency, and ethical considerations. The AI RMF is organized around four core functions: Govern, Map, Measure, and Manage.[115]

- **ISO/IEC AI Management System**: In December 2023, the *International Organization for Standardization* (ISO) released the *ISO/IEC 42001*, which provides requirements for establishing and maintaining an *Artificial Intelligence Management System* (AIMS) within organizations. ISO/IEC 42001 is designed to help organizations of any size and across all industries manage the risks related to the development and deployment of AI-based products or services. [116]

[115] *See* NIST (2023) *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, available at https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf; *see also* NIST (2024) *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile*, available at https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf. *See* UC Berkeley Center for Long-Term Cybersecurity White Paper Series, *A Taxonomy of Trustworthiness for Artificial Intelligence, Connecting Properties of Trustworthiness with Risk Management and the AI Lifecycle*, J. Newman (Jan. 2023), available at https://cltc.berkeley.edu/wp-content/uploads/2023/01/Taxonomy_of_AI_Trustworthiness.pdf (listing questions to consider when evaluating AI systems for trustworthiness under the NIST AI RMF).

[116] ISO (2023), *ISO/IEC 42001:2023 - AI management systems,* available at https://www.iso.org/standard/81230.html.

VII. Conclusion

Since the publication of the 2021 AI Report, financial market participants have accelerated their development and adoption of AI technologies, hoping to increase operational efficiencies, create new market opportunities, and harness other potential benefits that AI technologies may offer. While the use of AI systems may create potential efficiencies and benefits for firms and investors, the increased use of AI systems and recent advancements in AI potentially give rise to new and increasing issues, risks, and challenges, as discussed above. As a result, regulators must continue to focus on the use of AI systems and the management of associated risks by the firms that they supervise.

The 2021 AI Report provided guidance to assist IOSCO members in supervising market intermediaries and asset managers that utilize AI, consisting of expected standards of conduct by market intermediaries and asset managers for their use of AI. The guidance remains relevant today to help address risks. Regulators should continue to ensure that the use of AI by financial market participants abides by the guidance in the 2021 AI Report and other applicable standards and guidance (*see, e.g.*, Annex I and II).

At the same time, however, it is clear that the growing use of advancements in AI potentially give rise to new or increasing issues, risks, and challenges, which would need to be closely monitored by regulators. To that end, and as set out in IOSCO's workplan for 2025[117], IOSCO will now turn to its second phase of work on AI—the potential development of additional tools, recommendations, or considerations to assist IOSCO members to address the issues, risks, and challenges posed by the use of AI in financial products and services. Given the breadth of issues, risks, and challenges identified in this Report, as well as the fact that each could have different implications depending on the use case and potential impact, there may be challenges in identifying a one-size-fits all approach. Nonetheless, one potential path forward may be to identify potential additional tools such as good practices and guidance to assist regulators and market participants as they seek to adapt to the changing conditions brought about by the evolution and use of AI.

In addition to the next phase of the IOSCO work, IOSCO expects to play a coordination role with regard to AI developments in the financial sector. For example, there may be several other areas where the impact of AI on the financial sector warrants further consideration by IOSCO and its committees. These include, but are not limited to, potential considerations around: (1) educating investors about the increase of investment frauds involving the purported use of AI; (2) strengthening information sharing and cooperation with respect to key risks arising from the use of AI technologies by financial market participants; (3) enhancing information sharing and cooperation in the supervision of financial market

[117] *See* https://www.iosco.org/library/pubdocs/pdf/IOSCOPD789.pdf.

participants and key service providers in relation to AI technologies, including the provision of assistance in enforcement investigations and related proceedings; and (4) supporting member efforts to adhere to existing IOSCO standards and guidance through technical assistance and capacity building initiatives relating to AI technologies. Additionally, during the next phase of its work, IOSCO will, as appropriate, engage with other relevant international organizations, such as the FSB.

While it takes forward its next phase of work, IOSCO welcomes input from the public, including financial market participants, AI developers, academics, researchers, public policy experts, and other interested parties, on the content of this Report and other potential areas of focus going forward. Comments may be submitted to **AIWGConsultation@iosco.org** on or before **April 11, 2025**.

ANNEX I

IOSCO 2021 Guidance

In its 2021 AI Report, IOSCO published six measures that reflect expected standards of conduct by market intermediaries and asset managers using AI and ML. That report noted that, although the guidance is not binding, IOSCO members are encouraged to consider these measures carefully in the context of their legal and regulatory frameworks. IOSCO members and firms should also consider the proportionality of any response when implementing these measures:

Measure 1: Regulators should consider requiring firms to have designated senior management responsible for the oversight of the development, testing, deployment, monitoring and controls of AI and ML. This includes a documented internal governance framework, with clear lines of accountability. Senior Management should designate an appropriately senior individual (or groups of individuals), with the relevant skill set and knowledge to sign off on initial deployment and substantial updates of the technology.

Measure 2: Regulators should require firms to adequately test and monitor the algorithms to validate the results of an AI and ML technique on a continuous basis. The testing should be conducted in an environment that is segregated from the live environment prior to deployment to ensure that AI and ML: (a) behave as expected in stressed and unstressed market conditions; and (b) operate in a way that complies with regulatory obligations.

Measure 3: Regulators should require firms to have the adequate skills, expertise and experience to develop, test, deploy, monitor and oversee the controls over the AI and ML that the firm utilises. Compliance and risk management functions should be able to understand and challenge the algorithms that are produced and conduct due diligence on any third-party provider, including on the level of knowledge, expertise and experience present.

Measure 4: Regulators should require firms to understand their reliance and manage their relationship with third-party providers, including monitoring their performance and conducting oversight. To ensure adequate accountability, firms should have a clear service level agreement and contract in place clarifying the scope of the outsourced functions and the responsibility of the service provider. This agreement should contain clear performance indicators and should also clearly determine rights and remedies for poor performance.

Measure 5: Regulators should consider what level of disclosure of the use of AI and ML is required by firms, including: (a) Regulators should consider requiring firms to disclose meaningful information to customers and clients around their use of AI and ML that impact client outcomes. (b) Regulators should consider what type of information they may require from firms using AI and ML to ensure they can have appropriate oversight of those firms.

Measure 6: Regulators should consider requiring firms to have appropriate controls in place to ensure that the data that the performance of the AI and ML is dependent on is of sufficient quality to prevent biases and sufficiently broad for a well-founded application of AI and ML.

ANNEX II

Selected List of Recent IOSCO Reports that Discuss AI

1. Update to the Report on the IOSCO Automated Advice Tools Survey (December 2016)
2. IOSCO Research Report on Financial Technologies (FinTech) (February 2017)
3. The use of artificial intelligence and machine learning by market intermediaries and asset managers (September 2021)
4. Principles on Outsourcing (October 2021)
5. The Use of Innovation Facilitators in Growth and Emerging Markets (July 2022)
6. Report on Retail Distribution and Digitalisation (October 2022)
7. Retail Market Conduct Task Force Final Report (March 2023)
8. Policy Recommendations for Crypto and Digital Asset Markets (November 2023)
9. Investor Education on Crypto Assets (October 2024)
10. Digital Engagement Practices (DEPs) (November 2024 – Consultation Report))

ANNEX III

Analysis of AMCC Survey Results

IOSCO's Affiliate Member Consultative Committee (AMCC) conducted a survey of its members. The survey was distributed to AMCC members themselves (consisting of 74 IOSCO affiliate members),[1] and certain AMCC members (e.g., trade associations) also distributed the survey to their own membership, providing a broader population of potential respondents.

The survey collected respondent information on location, organization type, number of employees, approximate firm assets, and approximate annual revenue. Respondents were also asked whether their organization invested in AI and if so, how much they had invested. Overall, the AMCC gathered results from 184 respondents.

As described below, although the AMCC survey was distributed to a demographically diverse set of potential survey respondents (e.g., in terms of both geography and organization type), the survey was voluntary and response rates varied. As discussed below, the data gathered through the survey responses was skewed toward growth and emerging markets and smaller firms.

Nevertheless, the results provide valuable insights into the current use cases of AI and the perceived issues, risks, and challenges of those use cases of survey respondents, and the tables contained in this annex are intended to summarize some of those survey findings.

Geographic Distribution:

A majority of AMCC Survey respondents (52%) were geographically located in Central or South America, while an additional 15% of respondents were located in Africa, suggesting a concentration of respondents in growth and emerging markets ("GEM"). Eleven respondents self-identified as "Global" in nature, while European, North American, and Asia/Australian entities totalled approximately 20% of the respondents in aggregate. Fourteen respondents did not identify a geographic concentration.

Organizational Type:

A majority of the respondents self-identified as an investment advisor, broker-dealer, or asset/fund manager. Eighteen respondents (10%) did not identify an organizational type.

[1] IOSCO's AMCC is comprised of 74 IOSCO affiliate members, representing securities and derivatives markets and other market infrastructures, self-regulatory organizations (SROs), investor protection funds and compensation funds, as well as other bodies with appropriate interest in securities regulation. There are currently 35 jurisdictions represented in the AMCC, which also includes 14 regional or international associations.

Organizational Type	Respondents	%
Investment advisor, broker-dealer, asset manager/fund manager	99	54%
Other financial market infrastructure	34	19%
Exchange, trading venue	23	12%
N/A	18	10%
Industry group, trade association	10	5%

Organizational Size Distribution:

Respondents varied across organizational size, as measured by both number of employees and total assets. A majority of the respondents reported less than 1000 employees and less than $1B in total assets, suggesting a concentration of respondents in smaller and medium-sized organizations. 66 respondents indicated they have less than 100 employees in their organization, while 55 respondents employ 100 to 1000 individuals. Only 43 respondents (23%) reported more than 1000 employees. 97 respondents reported less than $1B in total assets, while 52 respondents reported more than $1B in total assets, and 35 respondents indicated this question was not applicable.

Number of Employees	Respondents	%
1-100	66	36%
100-1000	55	30%
1000+	43	23%
N/A	20	11%

Total Assets	Respondents	%
$0-$100m	53	29%
$100m-$500m	23	13%
$500m-$1bn	21	11%
$1bn-$10bn	21	11%
$10bn+	31	17%
N/A	35	19%

AI Investment:

Exactly half of the survey respondents indicated an investment in AI technology, while only 8 respondents (4%) acknowledged a greater than $10M investment in the technology to-date. Six of these 8 respondents identify as primarily located in GEM, suggesting global organizations heavily invested in AI did not answer this question. 20 respondents indicated an investment in AI technology but did not provide a dollar amount of investment; these respondents are included in the "n/a" total below.

AI Investment ($)	Respondents	%
<$1m	47	26%
$1m-$10m	17	9%
>$10m	8	4%
n/a	112	61%

AMCC Respondent-Identified Use Cases:

Following demographic and AI background questions, the AMCC AI Survey asked respondents about their usage of AI by identifying nineteen different products or services. Respondents across all organization types and all geographies identified internal productivity support, such as coding, drafting, or summarization, as the most frequent use case in their organization, followed by market analysis/trading insights/investment research. (*See* chart, *supra,* Section III). Internal productivity support was also identified as the most frequent AI use case when excluding GEM respondents. The use of internal GPT, for example via internal assistants or agents, was identified second-most frequently by non-GEM respondents.

AMCC Respondent-Identified Risks

In addition to surveying use cases, AMCC asked respondents whether eighteen different enumerated risks were material to deploying or using AI. Respondents ranked each risk on a 5-point scale, as follows: agree, somewhat agree, neutral, somewhat disagree, disagree, or N/A.

The responses received from the AMCC included in each of the following charts are converted from text to a numerical score using a 5-point scale (5 - agree, 4 - somewhat agree, 3 - neutral, 2 - somewhat disagree, 1 - disagree). Organizations that did not respond to the question (i.e., "N/A") are not included in the diagram below. Approximately 70 organizations recorded "N/A" for their response across each risk, with some variability by risk, representing about a third of the sample.

The below chart compares the relative respondent scores for all eighteen risks included in the survey across all respondent types.