VOICE OF AMAC

（2025 年第 2 期，总第 199 期）

中国证券投资基金业协会　　2025 年 5 月 28 日

人工智能在资本市场中的应用、风险与应对

——国际证监会组织（IOSCO）相关调查报告观点摘编

【编者按】2021 年 9 月，国际证监会组织（以下简称 IOSCO）发布《市场中介机构和资产管理机构使用人工智能和机器学习技术情况》报告（以下简称 2021 年报告），指出市场参与者对人工智能（AI）的使用正处于萌芽阶段，技术主要用于辅助人工决策方面，协会对该报告进行了摘编[1]。

时隔四年，金融产品和服务中的 AI 在理论、硬件、软件、算法效率、计算能力、数据和最终用户应用等方面的创新和发展推动下，不断发展。近期，IOSCO 通过问卷调查的方式调研了 24 家辖区成员及 6 家行业自律组织，并于 2025 年 3 月发布最新报告《资本市场中的人工智能：使用案例、风险及挑战》，梳理不同辖区市场参与者的使用场景，旨在了解金融产品和服务中使用 AI 可能对投资者保护、市场诚

[1] 参见中国证券投资基金业协会《声音》2022 年第 1 期《市场中介机构和资产管理机构使用人工智能和机器学习技术情况、潜在风险、应对措施及监管建议》，https://www.amac.org.cn/hyyj/sy/。

信和金融稳定带来的风险和挑战。总体来看，全球监管机构正在积极应对 AI 的快速发展，在确保市场稳定的同时促进技术创新，并加强投资者保护。

协会对此最新报告观点进行了摘编，主要分为人工智能的定义及分类、AI 技术在资本市场领域的应用场景不断拓展、投资者和市场面临的风险和挑战、全球主要司法辖区监督应对等四部分，供读者参考。

一、人工智能的定义及分类

（一）IOSCO 的定义

2021 年，人工智能（AI）在金融服务行业的应用，仍处于早期阶段。当时，IOSCO 采用的定义是由数据科学家约翰·麦卡锡（John McCarthy）于 1956 年提出的“制造智能机器的科学和工程”，指通过计算机模仿人类的学习、推理、规划、感知和语言理解能力，做出决策并解决问题。

IOSCO2025 年的最新报告采用了经合组织（以下简称 OECD）对 AI 的定义，指基于机器的系统，根据收到的输入信息推断并生成输出结果，如预测、建议或决策等，不同的人工智能系统在部署后的自主性水平和适应性程度各不相同。OECD 的定义从系统行为角度描述 AI 在金融领域的应用，更贴合技术发展和行业实际。

（二）目前 AI 技术的分类

近年来，AI 技术呈现快速演进态势。主要涵盖：一是传统 AI 技术，包括规则引擎、逻辑回归、决策树等早期模型；二是机器学习（ML）与深度学习（DL），包括神经网络、

强化学习、卷积神经网络等；三是自然语言处理（NLP）与大语言模型（LLM），包括文本生成、语义理解与自动对话；**四是**生成式人工智能（GenAI），能够使用 LLM 训练的基础模型来生成文本（包括编程代码）、图像和视频等。

二、AI 技术在资本市场领域的应用场景不断拓展

2021 年报告提出，当时市场参与者对 AI 和 ML 技术的应用处于起步阶段，主要用于咨询和风险管理，作为人工决策的辅助工具。

根据 IOSCO2025 年报告，随着技术进步，市场参与者[2]应用 AI 常见的场景包括：

一是反洗钱和反恐怖融资（50%[3]）。市场参与者在监控软件中使用 ML 进行识别和异常检测、使用 NLP 加强对非结构化数据的解释，辅助进行人名筛选和新闻分析等。AI 还被用于网络安全中对漏洞、网络钓鱼和异常的检测；以及身份验证、风险管理、合规监督及预防诈骗等。

二是内部生产力支持（50%）。市场参与者利用 AI 进行软件开发、后台操作、自动化和人力资源管理等方面的应用。例如，在软件开发中使用 LLM 协助编程和文档编制、尝试使用语音转文本功能和视频识别功能用于记录笔记和会议总结，以及利用具有翻译功能的工具辅助跨语言交流等。

三是市场分析和交易洞察（40%）。市场参与者运用 ML 及其他 AI 手段，提取并处理来自金融、市场、宏观经济和社交媒体等渠道的信息与见解。

---

[2] IOSCO 将市场参与者类型界定为资本市场中受监管的实体，如经纪商、资产管理机构、交易所和其他金融市场中介机构等。

[3] 本文中百分比的调研范围是 IOSCO 成员机构及行业自律组织辖区的市场参与者、以及下文提到其辖区的经纪商、资产管理机构及交易所。

（一）经纪商使用 AI 的主要场景

2021 年，经纪商使用 AI 已经开始应用于提供咨询服务和执行简单的交易命令，适用于辅助场景，设有人工干预流程。

随着技术发展，经纪商更广泛地应用 AI 与客户沟通、进行算法交易和监控与欺诈监测。一是与客户沟通（67%），其使用 AI 驱动的通信系统（如聊天机器人或虚拟助理）向客户提供咨询分析和管理支持。二是算法交易（63%），AI 涵盖了整个交易生命周期，包括交易前分析、协助定价、交易执行和交易后分析。此外，预测建模技术（一种受监督的机器学习）还被用于市场信号处理，如预测金融工具的未来价格和市场情绪分析。三是监控与欺诈监测（53%），ML 有助于评估数据、分析网络流量、识别异常行为、实时监控客户数据和交易、阻止恶意流量、安装网络安全补丁以及检测非法活动等。

（二）资产管理机构使用 AI 的主要场景

2021 年，资产管理机构对于 AI 和 ML 已经开始用于优化投资组合管理、提升内部研究能力以及后台支持工作，辅助人工决策方面。

当前资产管理机构使用 AI 场景更进一步拓展：一是更广泛地使用机器人顾问（60%）。AI 根据客户的风险偏好和财务目标，构建和优化投资组合。例如，一些公司利用 NLP 分析新闻和社交媒体数据，识别新兴投资主题，并将其整合到个性化的投资建议中。二是投资研究（40%）。资产管理机构借助第三方平台和数据提供商的 AI 工具监控宏观经济

环境，获取市场信息。此外，资产管理公司还积极探索 GenAI 和 LLM 的前沿应用，如利用 GenAI 优化交易策略的开发过程，包括搜索相关研究论文、生成经济理论基础、编写实现交易假设的程序代码以及对投资组合策略进行回溯测试。

（三）交易所开始探索应用 AI 技术

2021 年，IOSCO 成员辖区的交易所尚未应用 AI 技术。IOSCO 的最新调查显示，目前部分交易所已经开始探索利用 AI 来提高运营效率，主要集中在交易处理和自动化流程。AI 被用于优化交易前和交易后的流程，包括利用 ML 预测交易结算失败的可能性。美国证监会（以下简称 SEC）辖区的一家交易所最近引入了 AI 驱动的动态计时器，应用于特定类型的订单，SEC 还允许纳斯达克用 AI 自动调整股票订单的“等待时间”，旨在让交易更快成交，减少价格波动带来的损失。

（四）行业自律组织应用 AI 的场景

IOSCO 调查的 6 家行业自律组织中，4 家已经在监管流程中整合 AI 技术，用于增强数据驱动类应用程序和辅助合规工作。其中，ML 和 NLP 主要用于文档分析、情绪分析以及量化分析等。GenAI 和 LLM 主要用于异常事件检测和文档处理等任务。未来潜在应用方面，行业自律组织反馈，AI 可以在多方面提供支持，一是市场监控和合规管理，AI 有潜力通过分析历史规律和行为来识别异常的交易活动，如账户入侵、不当行为等。二是提高业务运营水平，AI 可以减少传统风险预警流程中的误报情况。三是工作流程的自动化，AI 可以减少人工工作量与错误，提升文档创建效率。

三、投资者和市场面临的风险和挑战

2025 年调查报告与 2021 年报告提及的 AI 风险相似，主要涉及治理和监督、算法开发、测试和持续监控、数据质量和偏见、透明度和可解释性、外包以及伦理等方面问题。最新报告中，问卷反馈最常提及的风险集中在恶意使用 AI、模型和数据质量不高、技术过度依赖、内部监督及人才缺失五方面，AI 在金融领域的风险本质未发生根本变化。

（一）AI 被恶意利用

恶意使用 AI 存在多方面风险：一是网络攻击风险，不法分子可利用 AI 强化攻击能力，自动化分析系统漏洞、生成攻击路径，增加攻击复杂性和隐蔽性；二是数据安全和隐私保护受影响，攻击者可能操纵 LLM 训练结果、泄露信息，且 AI 与其他系统整合时，可能扩大攻击范围，导致数据泄露或隐私侵犯；三是欺诈、骗局和错误信息风险，AI 工具降低不法分子入侵网络门槛，可生成虚假身份和新型投资骗局，提升传统骗局传播效率和迷惑性，随着 GenAI 生成内容逼真度提高，区分真实信息与合成内容难度加大，欺诈识别难度增加。

（二）模型和数据质量不高

人工智能模型和数据可能产生偏见，对投资者和市场构成重大风险。一是 LLM 通常较为复杂，LLM 通常使用历史数据进行训练，可能无法适应快速变化的市场状况或不可预见的事件。二是模型偏见可能导致 AI 系统忽视某些群体，如不公平对待某些投资者群体或对某些投资品类型有偏见。

三是数据质量问题也可能影响模型性能，GenAI 的合成数据可能引入虚假或错误信息，增加数据质量和可靠性风险。

（三）技术过度依赖

一方面，金融机构可能会高度依赖技术基础设施提供商（如云服务商），形成技术供应瓶颈；另一方面，大型科技公司主导 AI 研发资源，导致金融领域技术供应商高度集中。此外，风险管理、投资计算基准数据等关键信息过度集中化也可能放大数据质量问题或模型偏差风险。外包化与第三方依赖风险方面，大多数开源模型开发商等不受金融监管机构直接管辖，导致模型透明度、数据安全及合规性难以有效监督。

（四）监督不足

对于使用者而言，AI 的风险可能会贯穿于开发、实施、运营和监控等。一是问责机制缺失与合规困境。市场参与者使用 AI 时若缺乏健全的治理框架，可能导致合规失效，如部分机构可能将 AI 引发的损害责任转嫁给技术供应链中的第三方。二是技术依赖导致自动化偏见，如交易监控、风控系统等过度依托 AI，可能会因算法漏洞、网络攻击引发市场中断。三是由于 AI 的复杂性，执法部门在识别、追究违法行为责任人以及收集证据时也可能面临挑战。

（五）人才缺口

市场参与者在 AI 的监督、风险管理和结构治理方面面临人才短缺挑战，缺乏复合型人才，难以招聘、留住和培养必要的人工智能和数据专家，传统人才结构难以适配技术迭代。这种短缺可能导致上述提到的监督不足，进而引发投资

者损失、市场损害以及合规风险。目前，监管机构虽在积极了解 AI 的相关风险，但数据和知识方面的缺口依然存在且有扩大的趋势。鉴于 AI 的复杂性，监管机构需要对其持续进行监测，并不断更新风险评估。然而，监管机构对 AI 的理解有限，特别是当被监管机构使用复杂且不透明的数据时，这些缺口可能会进一步扩大，增加了监管的难度。监管机构应持续关注 AI 系统间的互联性、模型和数据集可能引发的群体效应，以及 AI 模型潜在的共谋行为。

四、全球主要司法辖区监督应对

2021 年报告向 IOSCO 成员提出六项监管建议，为监管机构有效监督市场参与者使用 AI 和 ML 树立了行为标准。四年来，各司法辖区通过调整现有监管框架、加强监督执法、开展研究和政府间合作、投资者教育、增加资源配置和人才能力建设等措施规范 AI 的应用。具体措施如下：

（一）调整涉及 AI 的监管框架

一方面，部分监管机构在现有框架下发布指导意见，如欧洲证券市场管理局（以下简称 ESMA）强调，投资者需进行尽职调查后才能投资 AI 相关公司或借助 AI 进行投资。美国商品期货交易委员会（CFTC）则提醒监管实体在使用 AI 时遵守相关法规。另一方面，部分辖区制定专门的法律法规管理金融领域应用 AI，如 ESMA 于 2024 年发布了关于企业使用或计划使用 AI 向零售客户提供投资服务的初步指导意见，旨在帮助企业遵守《金融工具市场指令 II》（MiFID II）的相关要求，涵盖了组织结构、业务行为以及以客户最佳利益等；日本发布了《商业中的人工智能指导原则》，要求包

括资本市场企业在内的 AI 使用者遵守以人为中心、安全、公平等原则。

（二）加强针对 AI 的监督执法

部分监管机构已开展多种监督工作和执法行动，应对市场参与者使用 AI 从事不当或不合规行为。一些 IOSCO 成员已经成立专业化团队，优先检查涉及 AI 的服务及相关风险。为执行现有法规，部分成员对相关市场参与方采取执法行动，如 SEC 会对虚假陈述 AI 的个人和实体提起执法行动。例如，由于虚假和误导性的陈述，SEC 已经对多个个人和实体提起多项执法行动。

（三）开展项目研究及政府间合作

为应对金融市场的 AI 使用问题，监管机构采取了多种措施。新加坡金融管理局（MAS）2023 年启动“MindForge 项目”，研究 GenAI 在金融服务领域风险和机遇，创建公平、道德、问责和透明度（FEAT）原则。英国金融行为监管局（以下简称 FCA）2024 年推出 AI 实验室，为 FCA、企业及相关方提供参与 AI 洞察、讨论和案例研究途径。合作方面，多数 IOSCO 成员机构还与其他国内机构合作监管 AI，涵盖信息共享、风险管控、立法咨询等；部分成员通过国际论坛、工作组等与海外机构合作。约三分之一成员参与国际合作，如欧盟成员经由欧洲监管机构组织展开多边合作。绝大多数成员表示与国内外机构沟通顺畅，合作无显著障碍。

（四）加强对投资者的风险提示与教育

为了提高投资者对 AI 相关风险的认识，IOSCO 的成员机构通过发布投资者提示和教育产品，使投资者尤其是零售

投资者，能够识别涉及使用 AI 的欺诈行为，并要求企业遵守现行法律法规。例如，ESMA 发布了关于使用 AI 提供投资服务的指导原则，强调了企业在向零售客户提供服务时的合规要求。

（五）增加资源配置以及人才能力建设

为应对金融行业的 AI 使用，IOSCO 的成员机构采取了多项措施。一些成员正在评估所需的资源和专业技能，已增加或计划增加资源，如发展数据获取、整合和优化 IT 流程、评估内部框架和治理结构以及通过培训提升员工能力等。部分成员机构还成立了专门的 AI 监督团队，与学术机构合作培训人员，为其工作人员和其他专家提供培训。

【本文摘编自国际证监会组织（IOSCO）于 2025 年 3 月发布的报告《资本市场中的人工智能：使用案例、风险及挑战》】