Three Takeaways from the IOSCO Report to Securities Regulators on Artificial Intelligence

October 14, 2021

On September 7, 2021, the Board of the International Organization of Securities Commissions ("IOSCO") issued a final report entitled "The Use of Artificial Intelligence and Machine Learning by Market Intermediaries and Asset Managers" (the "Report"), which aims to assist IOSCO members in supervising their regulated entities over the use of AI and ML.

While non-binding, the Report is likely to serve at least as a key frame of reference—if not as a benchmark—for the development of more tailored supervisory approaches by securities regulators around the globe. While the concepts in the Report are not new, they reflect an acknowledgement that existing regulations may not be sufficient to mitigate the wide variety of AI-risks, and that new and tailored regulations targeting asset managers and market intermediaries' use of AI may be needed.

We discuss IOSCO's recommendations below, and also share some concrete steps companies can take in anticipation of heightened regulatory scrutiny of AI in the securities industry. Hedge Fund Law Report's recent coverage, with comments from Avi Gesser and ConsenSys' Lex Sokolin, provides additional insights on the Report, including its genesis and evolution from prior drafts.

THE IOSCO REPORT

The IOSCO Board is the governing and standard-setting body of IOSCO with membership comprising of securities regulatory authorities around the world, including the U.S. Securities and Exchange Commission ("SEC"), U.S. Commodity Futures Trading Commission ("CFTC"), and the UK Financial Conduct Authority ("FCA"), among others. The Report is the culmination of IOSCO's multiyear effort engaging with market intermediaries and asset managers to identify real-life artificial intelligence ("AI") and machine learning ("ML") use cases and their associated risks, and incorporates the feedback IOSCO received on its June 2020 Consultation Report.

AI Use Cases and Risks for Market Intermediaries and Asset Managers

Like in many industries, the securities industry is increasingly leveraging AI. Through its market participant engagement efforts, the Report identifies the following major use cases for market intermediaries and asset managers.

Market Intermediary AI Use Cases

- Advisory and support services;
- Risk management;
- Client identification and monitoring;
- Selection of trading algorithm; and
- Asset management/ Portfolio management.

Manager AI Use Cases

- Optimize portfolio management;
- Complement human investment decision-making processes by suggesting investment recommendations;
- Improve internal research capabilities, as well as back office functions;
- Order execution, broker selection, and order routing/algo-wheels (which the Report notes is a burgeoning use).

According to IOSCO, based on its industry engagement findings, these AI uses raise concerns in the following areas:

- Governance and oversight;
- Algorithm development, testing and ongoing monitoring;
- Data quality and bias;
- Transparency and explainability;
- Outsourcing; and
- Ethical concerns.

IOSCO's Emphasis on Proportionality

IOSCO's Report recognizes that, given the wide variety of ways that firms are using AI, they carry different risks and require different controls. For example, the testing, oversight and transparency required for AI that is being used for things like anti-money laundering, sanctions compliance, or cybersecurity is very different than for investment products or robo-advising. This is why the Report talks a lot about "proportionality"—or a risk-based approach—to AI regulation. In particular, risk-reduction measures will need to be tailored to the risks of the specific AI use cases and the specific firm. To be able to

assess those risks, the legal and compliance departments at regulated entities will want to be aware of the full complement of AI applications used by their firms, so they can assess which ones carry the most risk, and therefore, which need the most oversight and controls.

IOSCO's Six Recommendations to Regulators

IOSCO calls upon its member regulators to consider the following six measures in developing their own regulatory frameworks:

1. Senior-level Oversight and Internal Governance Framework

The Report encourages regulators to consider requiring firms to designate responsible senior management and create a documented internal governance framework for the oversight of the development, testing, deployment, monitoring and controls of AI. Where senior management does not have the appropriate technical knowledge to effectively discharge this oversight role, they should designate one or more appropriate senior personnel to support in this function, but would remain ultimately responsible. According to IOSCO, this measure addresses the need for accountability over the entire lifecycle of AI/ML models. In addition, the Report also encourages regulators to consider requiring firms to:

- Understand how AI is being used in the firm and the intended outcomes of the models;
- Implement appropriate controls and governance frameworks over data quality and data sources (for both internal and external data), as well as model outcomes;
- Create and document AI methodology and maintain an audit trail of how AI is used across the business; and
- Assess whether the models are applied in accordance with the firm's broader risk assessment frameworks and ethical principles.

Given the variety of AI uses and risks, regulators may be disinclined to create prescriptive and generally applicable rules for AI. Rather, they are likely to focus on a regulated entity's AI governance process, including whether it has a designated person or group at the senior management level responsible for managing regulatory and reputational risks. Among other responsibilities, this person or committee could be responsible for briefing the board on AI and overseeing the alignment of the company's AI development, testing, deployment, and monitoring with regulatory expectations and industry standards.

2. Model Validation and Ongoing Monitoring

As a second recommended measure, the Report emphasizes that AI models should be tested, both before and throughout deployment, in light of their risks (including privacy, cybersecurity, and market abuse), and that firms' risk and compliance functions should be involved in this process.

Consistent with its proportionality principle, the Report clarifies that continuous monitoring does not need to be real-time, given the potentially prohibitive cost for smaller firms. Nevertheless, firms should build into their control framework, as appropriate, a "kill-switch" functionality for their AI, which should be tested and contain back-up capabilities. IOSCO notes that it is not enough for the kill-switch to exist, but rather it should be deployable if the need ever arises.

3. Personnel Knowledge and Skills

The third recommended measure highlights IOSCO's view that *internal* skills and expertise are needed to properly oversee AI development and deployment. Moreover, an appropriate AI governance scheme should be multi-disciplinary—involving not only compliance and risk management functions, but also their close coordination and collaboration with business units and technical functions. In a way, this is reminiscent of the shifting paradigm in the cybersecurity realm in the past five years: to properly manage AI risks, companies need to move away from thinking of them as purely technological and toward treating them as risks with critical business, regulatory, and reputational import.

In addition, the Report points out the importance of institutional knowledge building and the need for redundancy with respect to personnel expertise. The Report underscores the importance of ensuring AI model continuity and mitigating the risk of operational disruptions, for example, in light of key personnel departures. We have all learned the criticality of operational resiliency in the past year in light of the global pandemic; regulators across industries, including the SEC, are also increasingly viewing this as a priority—a concern that is not unique to AI, but perhaps especially critical in this realm.

4. Third-Party Vendor Management

The Report also focuses on the need to ensure adequate third-party vendor management, given the increasing reliance on external parties for AI model development. Not unlike cybersecurity, firms need to perform initial and ongoing due diligence on AI vendors, and have contractual provisions in place to delineate accountability, allocate risks, and determine available recourses in accordance with the firm's AI or other vendor management frameworks. The Report also urges firms to consider the IOSCO outsourcing principles in developing risk-based vendor governance frameworks.

5. Transparency and Meaningful Disclosures

With respect to transparency and disclosure, IOSCO appears to have incorporated substantial input from its public consultation process. Again, advocating for a proportionate or risk-based approach, the Report notes that regulators should consider requiring firms to disclose *meaningful* information about their use of AI with the objective of enabling clients to understand: "(1) the nature of, and (2) key characteristics of the products and services they are receiving, and (3) how they are impacted by the use of the technology." Ultimately, the focus is on whether clients have sufficient information in particular contexts to evaluate both the benefits and the risks of AI, so that they can make informed decisions. Adequate disclosures have been a longstanding focus of SEC's enforcement actions and were at the center of its action against BlueCrest Capital Management in December 2020. SEC's 2017 Guidance for robo-advisers also contains very specific disclosure requirements for that context. According to the Guidance, robo-advisers should disclose, in addition to other required information under the Advisers Act Rule 204-3(b), information regarding its AI-driven business model and related risks, including (non-exhaustive list below):

- The fact that an algorithm is used to manage individual client accounts;
- A description of the algorithmic functions used to manage client accounts, and the assumptions and limitations underlying the algorithms;
- A description of the particular risks inherent in the use of an algorithm, and circumstances that might cause the robo-adviser to override the algorithm;
- A description of any involvement by a third party in the development, management, or ownership of the algorithm used to manage client accounts, including an explanation of any conflicts of interest such an arrangement may create; and
- An explanation of the degree of human involvement in the oversight and management of individual client accounts.

The Guidance also emphasizes the importance of accurately disclosing the scope of advisory services provided and ensuring the effectiveness of disclosures by taking into account factors such as plain language and presentation so as to minimize the risk of misleading clients.

6. Bias Testing and Data Quality Assurance

Algorithmic bias and its potential for discrimination and unfairness are a key concern for many regulators, including the FTC. According to IOSCO, this is an area ripe for additional personnel training, including for the more technically oriented personnel. The Report calls on firms to ensure that data used for AI is relevant, complete, and representative of the target population, so as to not lead to biased outcomes.

KEY TAKEAWAYS

1. Training on AI Uses, Risks, and Mitigation Options: The IOSCO Report suggests that regulators have started to expect that companies will have *effective* senior management and board oversight over AI, with governance structures that enable accountability over the full model lifecycle. This means companies should consider having targeted trainings for their senior leaders on the uses, operational and regulatory risks, as well as monitoring and risk management around both in-house and third-party models. This also means that to the extent the day-to-day oversight function will be delegated to management, companies should consider cultivating or hiring the appropriate talent—including in the key roles played by both risk and compliance functions.

2. Testing the Plan, Including for AI Incidents: AI controls, governance frameworks, and policies should aim to be useful in practice. As in the cyber context, companies should consider running scenario-based tabletop exercises to stress-test what they would do if their AI models act unexpectedly or are discovered to have flawed outcomes. Should a kill-switch be deployed, who decides, and what is the business continuity plan if that happens? What are the associated regulator or consumer communications needs, if any? Does the issue need to be escalated to senior management or the board? Creating an incident response plan for AI, and pressure-testing that in a tabletop scenario, can provide valuable insights, which companies can proactively address *before* an incident arises.

3. Providing Clear Disclosures: Given the recent BlueCrest enforcement action, under certain circumstances, inadequate AI-related disclosure not only could lead to regulatory scrutiny, but also result in significant reputational damage. Depending on the context, companies should consider what consumers, investors, or other relevant stakeholders might need to know in order to make informed decisions with respect to the company's AI-driven services and products. Public disclosures around AI should also be reviewed for accuracy, and to ensure they represent up-to-date information on the company's risks.

To subscribe to the Data Blog, please click here.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Avi Gesser
agesser@debevoise.com

Anna R. Gressel
argressel@debevoise.com

Mengyi Xu
mxu@debevoise.com