Date: March 31, 2025

To: British Columbia Securities Commission
Alberta Securities Commission
Financial and Consumer Affairs Authority of Saskatchewan
Manitoba Securities Commission
Ontario Securities Commission
Autorité des marchés financiers
Financial and Consumer Services Commission, New Brunswick
Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island
Nova Scotia Securities Commission
Office of the Superintendent of Securities, Service Newfoundland and Labrador
Northwest Territories Office of the Superintendent of Securities
Office of the Yukon Superintendent of Securities
Nunavut Securities Office

Delivered to:

The Secretary Ontario Securities Commission 20 Queen Street West 22nd Floor, Box 55 Toronto, Ontario M5H 3S8 Fax: 416-593-2318 comments@osc.gov.on.ca	Me Philippe Lebel Corporate Secretary and Executive Director, Legal Affairs Autorité des marchés financiers Place de la Cité, tour PwC 2640, boulevard Laurier, bureau 400 Québec (Québec) G1V 5C1 Fax: 514-864-8381 consultation-en-cours@lautorite.qc.ca

Dear Sirs/Mesdames:

Re: CSA Staff Notice and Consultation 11-348 - Applicability of Canadian Securities Laws and the use of Artificial Intelligence Systems in Capital Markets (the "**Consultation Paper**")

The Private Capital Markets Association of Canada ("**PCMA"**) appreciates the opportunity to participate in this consultation regarding the use of artificial intelligence ("**AI"**) systems in the capital markets. The PCMA commends the CSA for its forward-thinking approach in the Consultation Paper and for recognizing the transformative potential of AI while addressing its unique challenges.

As the voice of exempt market dealers ("**EMDs"**), issuers, and industry professionals in Canada's private capital markets, the PCMA believes AI presents significant opportunities to enhance market efficiency, improve compliance, and better serve investors.

About the PCMA

The PCMA is a not-for-profit association founded in 2002 as the national voice of the EMDs, issuers and industry professionals in the private capital markets across Canada.

The PCMA plays a critical role in the private capital markets by:

- assisting hundreds of dealers and issuer member firms and individual dealing representatives ("**DRs"**) to understand and implement their regulatory responsibilities;
- providing high-quality and in-depth educational opportunities to the private capital markets professionals;
- encouraging the highest standards of business conduct amongst its membership across Canada.
- increasing public and industry awareness of private capital markets in Canada;
- being the voice of the private capital markets to securities regulators, government agencies and other industry associations and public capital markets;
- providing valuable services and cost-saving opportunities to its member firms and individual DRs; and
- connecting its members across Canada for business and professional networking.

Additional information about the PCMA is available on our website at www.pcmacanada.com.

The PCMA has also established our Fair and Balanced Regulation Advocacy Website which is available at: https://fairandbalancedregs.com. This Advocacy Website is a platform for commentary and analysis on regulatory proposals, consultations, and requests impacting capital raising, securities registration and compliance in Canada's private capital markets, examining their implications for issuers, exempt market dealers and DRs. The PCMA is committed to supporting fair and balanced regulations in the financial sector and this is our resource to the public to share our views and for education and training purposes.

PCMA's responses to the Consultation Paper and general comments are set out below for your review and consideration.

GENERAL COMMENTS - AI AND THE PRIVATE MARKETS

The private capital markets ecosystem operates through a well-established framework where various participants fulfill distinct but interconnected roles.

Many private market issuers devote significant resources to creating comprehensive offering memoranda, term sheets, investor presentations, and marketing collateral. These documents must balance compelling investment narratives with regulatory compliance, requiring legal and financial expertise. The preparation process traditionally involves multiple stakeholders, numerous drafting cycles, and rigorous internal reviews.

EMDs serve as gatekeepers within this ecosystem, conducting thorough reviews of issuer offering documents for regulatory compliance, where required, factual claims and appropriate disclosures for investors. Additionally, EMDs are responsible for suitability assessments where they evaluate whether specific investment opportunities align with individual investor profiles, including factors like risk profile, investment objectives, time horizon, and financial circumstances.

Emerging AI Integration Strategies

Private market participants are beginning to explore AI solutions, primarily focused on internal operational efficiencies rather than client-facing applications. For example, EMDs are increasingly using AI to summarize and explain information contained in issuers' offering documents to support their Know Your Product ("**KYP"**) processes. These AI-powered outputs help EMDs quickly identify key risk factors, investment terms, and potential regulatory concerns, allowing for more efficient and thorough reviews.

In addition, some issuers are leveraging AI tools for industry research and as assistants in preparing offering documents. These applications focus on ensuring better wording, information synthesis, and data extraction which can help issuers create more comprehensive disclosure documents while reducing the time required for initial drafts.

Many issuers and EMDs are experimenting with large language models ("**LLMs"**) such as ChatGPT, Microsoft Co-Pilot, Gemini, and Claude to support specific internal processes including:

- *Document preparation and review.* Using AI to draft initial versions of certain sections in offering documents, marketing materials, compliance checklists, and disclosure statements;
- *Information extraction.* Implementing AI tools to analyze financial data and extract relevant metrics from complex documents;
- *Research synthesis.* Leveraging AI to aggregate market research and compile industry trends for investment analysis;
- *Compliance reviews and monitoring*. Utilizing AI to flag potential regulatory issues in draft documents as part of its human review by compliance officers; and
- *Workflow automation tools.* Using tools like Zapier and Make.com to streamline repetitive processes, including document routing, compliance deadline notifications, and automated report generation.

As these technologies mature, they will likely extend to more complex applications. The PCMA believes there are significant competitive advantages for registrants, including EMDs, that effectively implement AI tools in their workflows. As EMDs and issuers gain experience with these technologies, they may develop more specific use cases tailored to their unique needs. The PCMA believes early adopters will seeing benefits in:

- Accelerated workflow processes, reducing time spent on routine tasks;
- More efficient compliance reviews of offering documents and KYC documentation;
- Enhanced data analysis capabilities for investment research; and
- Improved document quality and consistency.

The relatively low cost of entry for many AI tools means that even smaller market participants can access these capabilities, potentially helping to level the competitive landscape.

While public markets have seen AI adoption in areas like algorithmic trading and large-scale data analysis, private markets face different considerations. Public markets benefit from standardized disclosure requirements and greater data availability, making large-scale AI implementation more straightforward.

However, private markets have less standardized offering documents which require more nuanced AI applications. However, this presents opportunities for targeted solutions that address specific pain points in the private capital raising process.

While the PCMA believes current AI adoption focuses primarily on internal processes, there is future potential for client-facing applications, such as AI-powered chatbots that could allow investors to ask questions about offerings. EMDs are also exploring using AI tools for education and training of their DRs for both offering information and compliance functions.

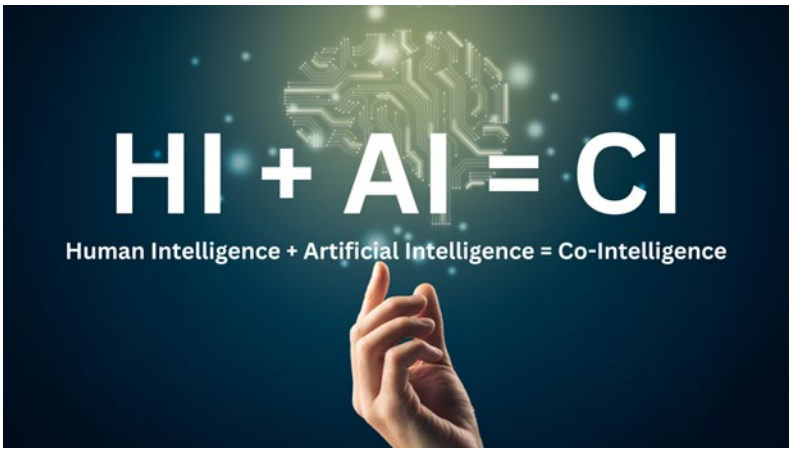
The PCMA acknowledges that such applications currently face challenges regarding reliability and accuracy of responses. Until these technologies mature further, the PCMA believes human interaction will remain central to investor communications in the private capital markets.

Human-AI Collaboration Model: HI + AI = CI

The PCMA believes the current implementation paradigm typically positions AI as an assistant rather than a replacement. In instances where AI streamlines workflow by assuming routine tasks, producing preliminary drafts, and flagging compliance concerns, it allows compliance professionals and document preparers to focus their expertise on higher-value activities requiring judgment, context-awareness, and stakeholder communication.

Despite AI technological advancements, the current adoption of AI in the private markets remains measured and subordinate to human oversight. The industry is largely relying on "*human-in-the-loop*" processes, particularly for high-stakes functions like final compliance reviews, suitability determinations, and investment recommendations.

Presently, the PCMA advocates for an approach based on the following: HI + AI = CI. This means Human Intelligence plus Artificial Intelligence equals Co-Intelligence.



First, Human Intelligence represents the unique cognitive and emotional capabilities that people bring to decision-making and analysis. This includes creativity, empathy, ethical judgment, intuition, contextual understanding, critical thinking, and the ability to interpret nuances in human behavior and societal values.

Second, Artificial Intelligence includes technologies and algorithms capable of analyzing vast quantities of data rapidly, identifying patterns and trends, making predictions, automating routine tasks, and enhancing efficiency and accuracy. AI excels at repetitive, high-volume data processing tasks, real-time analytics, pattern recognition, and quantitative reasoning.

Lastly, Co-Intelligence is the outcome when human intelligence and AI are effectively integrated. In contrast to the perspective of AI as a substitute, the co-intelligence paradigm presents AI as a collaborative partner, enhancing human capacities through the automation of data-intensive, repetitive processes, thereby enabling human experts to concentrate on higher-level tasks involving judgment, strategic planning, and complex interpersonal dynamics.

The PCMA acknowledges that AI is evolving at a very rapid pace. The PCMA recognizes that certain AI functions may not require human intelligence or a human in the loop. However, for many private market participants, applications have not reached this stage, and human oversight is still required. Accordingly, the PCMA advocates for a balanced approach to utilizing AI, emphasizing that AI tools should enhance rather than replace human expertise. Human oversight is crucial to ensure reliability, accuracy, ethical integrity, and compliance. While AI significantly boosts analytical capabilities, the PCMA believes human review, remains essential for interpreting data accurately, ensuring trustworthiness, managing risks, and maintaining transparency and accountability. The PCMA acknowledges the rapid advancement of AI tools in compliance and anticipates assisting EMDs and issuers in integrating AI into their policies and procedures to maintain regulatory compliance.

AI Use and Change in Business

The PCMA acknowledges that certain AI use cases by an EMD may trigger a regulatory filing involving Form 33-109F6 *Firm Registration*, if AI use results in a change in business based on certain circumstances including the following:

- *Direct Impact on Registerable Services*. If the use of AI directly affects registerable services provided to clients. The PCMA understand this includes circumstances where AI is used for investment advice, trade execution involving suitability determinations, or client onboarding processes. If AI fundamentally changes how these services are delivered, it will constitute a change in the EMD's primary business activities.
- *Material Change to Business Plan or Operating Model*. Any significant use of AI that alters an EMD's business plan or operating model should be disclosed where, for example, AI integration poses new risks to an EMD's business or its clients or where AI significantly impacts core functions.
- *Introduction of New Products or Material Changes to Existing Ones*. If the AI system is integral to the delivery or nature of new services, or significantly changes existing services, such as launching a new AI-driven suitability determination tool; and
- *Outsourcing Registerable Activities to AI Providers*. Where AI systems are used in a manner that effectively outsources core compliance or registrable functions, it would represent a fundamental change to the business model, warranting regulatory review.

The PCMA understands the need for filing requirements in cases where AI fundamentally changes core business functions or client-facing activities. However, in many cases firms are not changing their business model, only the tools used to carry out those activities. Accordingly, the PCMA respectfully requests further CSA clarification and guidance regarding the specific thresholds and examples where AI would trigger a change in business filing.

The PCMA believes using AI for administrative or operational tasks that are not client-facing or where AI is used as a support tool with a human-in-the-loop, should not automatically trigger a regulatory filing. Examples of such applications might include:

- Using generative AI to draft internal documents or marketing materials;
- Automating data entry or reconciliation tasks;
- Employing AI-based risk screening tools that are then reviewed by a human compliance officer.

The PCMA recommends that the CSA develop clear, practical examples that differentiate between:

- AI as a supportive tool versus AI as a core service delivery mechanism;

- Administrative uses versus client-facing, decision-making applications; and
- Minor operational adjustments versus significant business model changes.

This additional guidance would help EMDs better assess when a change in business filing is necessary, fostering responsible AI adoption while reducing unnecessary compliance burdens for EMDs.

Need for Accelerated CSA Responses to AI Developments

As the CSA acknowledges, AI is evolving at a rapid pace. In response, the PCMA believes CSA members need to substantially accelerate their response times to AI innovations in the financial sector. As discussed in the Consultation Paper and the OSC's report on *Artificial Intelligence in Capital Markets*, the rapid innovation in AI has increased the scope and scale of what can be accomplished using AI systems. The PCMA believes unprecedented pace of technological advancement demands a corresponding increase in regulatory agility.

With AI adoption at an "intermediate stage,"[1] the PCMA believes this represents a critical juncture where timely regulatory guidance can significantly influence the trajectory of responsible AI implementation across the industry. The CSA's stated commitment to deliver smart and responsive regulatory actions in anticipation of significant emerging issues, trends, technologies and business models necessitates additional regulatory guidance on AI.

The PCMA believes delayed regulatory guidance creates an uncertain operating environment that may inadvertently stifle innovation or allow unaddressed risks to accumulate. Accordingly, the PCMA believes CSA members need to develop specialized AI teams that have both AI knowledge, skills and expertise in addition to those involving securities regulation and compliance.

Concerns with Uncooperative Third-Party AI Vendors

As AI technologies become increasingly prevalent in the capital markets, it is vital to ensure that registrants can meet their compliance obligations while leveraging innovative solutions. PCMA members have concerns in circumstances where third-party vendors may not cooperate in providing necessary information to registrants regarding their use of AI.

Registrants are required to conduct thorough due diligence when outsourcing services, including those enhanced by AI. Due diligence involves assessing the functionality, risks, and operational transparency of the AI systems provided by vendors. However, a third-party AI vendor may be reluctant to share critical information, such as model functionality, training data, and risk management protocols. The PCMA understands that a registrant may then choose not to work with such a vendor at first instance. However, the PCMA is concerned about situations where the implemented technology is hard to replace or where there is a limited number of vendors, many of whom use AI. In particular, the PCMA is concerned where a lack of cooperation hinders a registrants' ability to adequately evaluate and monitor ongoing risks to ensure they are functioning as intended.

The PCMA is concerned that a third-party vendor's non-cooperation may result in what regulators believe to be inadequate due diligence or supervision, which could result in a registrant facing

[1] "*intermediate stage*" in the context of AI adoption in the capital markets signifies a level of implementation that is beyond initial exploration but not yet fully mature or widespread across all potential applications.

enforcement actions, including fines and reputational damage. The inability to demonstrate adequate oversight of AI systems places the registrant at risk, both legally and operationally.

Based on the foregoing, the PCMA recommends that the CSA introduce mandatory disclosure requirements for third-party vendors using AI. These should include information about model functionality, training data, risk assessment protocols, and potential biases. Such disclosures would enable registrants to perform their due diligence and maintain ongoing oversight.

The PCMA also believes the CSA should issue detailed guidance on how registrants can perform thorough due diligence when engaging AI vendors. For instance, guidance could include sample questions or criteria for evaluating AI-driven services. This guidance should cover best practices for evaluating AI-driven services and verifying outputs through ongoing sampling and monitoring.
In sum, the PCMA strongly urges the CSA to address the challenges posed by third-party AI vendors whose technology cannot easily be replaced post implementation. By fostering transparency and accountability, the CSA can ensure that AI systems enhance rather than undermine the capital markets.

Training of CSA Staff Members in the Use of AI

The PCMA believes that effective regulation of AI in the capital markets requires the CSA to develop substantial internal capabilities and expertise. While the current consultation appropriately focuses on market participants' use of AI, the PCMA believes that successful regulatory outcomes will depend equally on the CSA's own AI literacy and technical competencies.

The rapidly evolving nature of AI technologies creates a potential knowledge asymmetry between regulated entities and regulators. As market participants deploy increasingly sophisticated AI systems, the CSA must develop commensurate expertise to evaluate compliance with regulatory requirements, assess potential systemic risks, and provide meaningful guidance to the industry.

The complexity of modern AI systems, particularly those utilizing advanced machine learning technologies, demands specialized knowledge. Without appropriate technical understanding, even well-designed regulatory frameworks may prove ineffective in practice, as regulators may lack the capacity to evaluate whether compliance is being meaningfully achieved.

The PCMA notes several international regulators have recognized this challenge and implemented specific initiatives to enhance their internal AI capabilities. For example, the March 2025 IOSCO report *"Artificial Intelligence in Capital Markets: Use Cases, Risks, and Challenges"*, indicates multiple member jurisdictions are actively building staff capability through specialized training programs and the formation of dedicated AI oversight teams.[2]
These regulators recognize that effective supervision of AI in financial markets requires more than familiarity with traditional regulatory principles. It demands practical understanding of technical

[2] Section VI, "Responses by IOSCO Members," specifically under the subsection "*Resources and Expertise*" states that 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.

concepts such as model validation, algorithmic bias, explainability techniques, and governance frameworks specific to machine learning systems.

Accordingly, the PCMA recommends that CSA members implement a comprehensive strategy to develop internal AI expertise, including:

- *Specialized Training Programs* - Development of tailored training programs for CSA staff responsible for AI oversight, covering both technical concepts and practical applications in the capital markets;
- *Interdisciplinary Expertise* - Recruitment of staff with diverse backgrounds spanning technology, data science, financial markets, and regulatory compliance to provide the multidisciplinary perspective necessary for effective AI oversight;
- *Regulatory Technology Implementation* - Strategic investment in regulatory technology capabilities to enhance the CSA's ability to evaluate and monitor AI systems employed by market participants; and
- *Industry Engagement Programs* - Creation of structured engagement programs with industry practitioners to facilitate mutual understanding of evolving AI applications and associated risks.

The PCMA recognizes developing internal AI capabilities presents resource challenges for regulatory authorities. However, the PCMA believes this investment is essential to ensure regulatory frameworks remain effective as AI technologies transform the operations of the Canadian capital markets. The development of internal AI competencies should be viewed as a foundational element of the CSA's regulatory strategy, complementing the substantive requirements that will ultimately be imposed on market participants.

Regulatory Leadership Through Transparency: CSA Member AI Governance Frameworks

The PCMA recommends that each CSA member should model best practices by establishing and disclosing their own internal AI governance frameworks. Regulatory transparency regarding AI usage would set meaningful precedents for market participants developing their own compliance protocols.

The PCMA respectfully recommends that each CSA member should publicly disclose their use of AI technologies and related compliance frameworks. As an example, the United States Securities and Exchange Commission's ("**SEC"**) publication of its AI Compliance Plan in September 2024 provides a constructive precedent for regulatory transparency on the usage of AI.[3] The SEC's approach outlines specific risk management protocols, oversight mechanisms, and ethical guidelines governing its internal AI usage.

The PCMA believes analogous disclosure from CSA members would serve multiple public interest objectives, including: (a) establishing clear regulatory expectations regarding AI governance protocols that may become central to potential enforcement actions; (b) providing market participants with visibility into how AI technologies influence core regulatory functions, including compliance reviews, enforcement investigations, continuous disclosure reviews, and prospectus receipting; and (c) creating a foundation for constructive dialogue between CSA members and market participants regarding evolving AI governance standards.

The PCMA also believes each CSA member should appoint a "Chief Artificial Intelligence Officer" or equivalent oversight position with responsibility for: (a) developing and implementing the regulator's

[3] See "AI at the SEC" at: https://www.sec.gov/ai

internal AI governance framework; (b) coordinating AI-related policy development across operational divisions; (c) leading engagement with market participants on AI governance issues; and (d) ensuring consistent application of AI principles across regulatory functions. Such appointments would signal organizational commitment to thoughtful AI governance and provide clear points of contact for market participants seeking guidance on emerging AI issues.

Market participants require clarity on how CSA members themselves implement AI governance frameworks as part of developing their own compliance programs. This regulatory transparency would enhance market efficiency by reducing compliance uncertainty and establishing consistent expectations across the industry. The PCMA believes that CSA member leadership in AI governance will foster trust and shared understanding, thereby enabling more effective regulation of AI within Canada's evolving capital markets.

Investor Education: A Critical Component of AI Regulation in the Capital Markets

The PCMA believes that effective investor education must also be a pillar of the CSA's approach to AI regulation. As AI technologies transform the capital markets, investors require enhanced knowledge to navigate this evolving landscape and make informed decisions.

The PCMA believes there is a significant knowledge gap among retail investors regarding AI usage in capital markets. The PCMA understands many investors demonstrate strong interest in AI-related investment opportunities without sufficient understanding of the underlying technologies. This knowledge deficit creates several concerning vulnerabilities:

- *Susceptibility to "AI Washing*" - Investors are increasingly targeted by marketing materials that may make exaggerated or misleading claims about AI capabilities to attract investment. Without appropriate knowledge, investors struggle to distinguish between substantive AI applications and superficial marketing claims;
- *Limited Understanding of AI Opacity* - Most retail investors lack awareness of the inherent limitations in explainability of advanced AI systems, particularly those utilizing deep learning or LLMs. This creates unrealistic expectations regarding transparency and predictability of AI-driven investment products; and
- *Vulnerability to AI-Enhanced Fraud* - Sophisticated AI-powered investment scams using deepfakes, voice cloning, and personalized messaging have demonstrated significantly higher effectiveness compared to traditional fraud approaches. Investors require specific education on recognizing these emerging threats.

Based on the foregoing, the PCMA recommends that the CSA implement a comprehensive investor education strategy focused on AI in the capital markets, including:

- *Plain-Language AI Disclosure Guidelines* - Developing standardized, plain-language frameworks for disclosing AI usage in investment products and services, with specific guidance on describing model limitations, data dependencies, and potential biases;
- *Interactive Educational Resources* - Creating interactive tools demonstrating how different AI technologies function in financial contexts, helping investors develop practical understanding of capabilities and limitations;
- *AI Fraud Awareness Campaigns* - Implementing targeted campaigns highlighting emerging AI-enhanced fraud techniques, with practical guidance on identifying red flags in AI-generated

communications. One such example is the British Columbia Securities Commission's innovative campaign targeting investment scams use of AI;[4] and

- *Collaborative Industry Initiatives* - Partnership with industry associations to develop and distribute educational materials through existing distribution channels, leveraging the reach of market participants to enhance investor knowledge.

The PCMA believes a robust investor education initiative would deliver several benefits to the Canadian capital markets including:

- *Reduced Information Asymmetry* - Narrowing the knowledge gap between sophisticated institutional investors and retail participants regarding AI technologies;
- *Enhanced Market Efficiency* - Improving capital allocation by enabling more informed investment decisions regarding AI-related opportunities;
- *Fraud Prevention* - Reducing successful AI-enhanced investment frauds through improved investor awareness and skepticism; and
- *Realistic Expectations* - Fostering appropriate investor expectations regarding AI capabilities, limitations, and risks in financial contexts.

The PCMA believes investor education represents a cost-effective regulatory approach that complements traditional disclosure and governance requirements. By enhancing investor knowledge regarding AI in the capital markets, the CSA can strengthen market integrity while supporting continued technological innovation.

The PCMA encourages the CSA to prioritize the development of investor education initiatives alongside other regulatory measures, recognizing that informed investors represent the first line of defense against potential harms associated with AI in capital markets.

PCMA RESPONSES TO SPECIFIC QUESTIONS

1. Are there use cases for AI systems that you believe cannot be accommodated without new or amended rules, or targeted exemptions from current rules? Please be specific as to the changes you consider necessary.

(a) AI-Enhanced Client Onboarding and KYC Processes

Current Regulatory Challenges: Current KYC requirements under National Instrument 31-103 – *Registration Requirements, Exemptions and Ongoing Registrant Obligations* ("**NI 31-103**") presume direct human involvement in gathering and assessing client information. While the use of technology to support these processes is not prohibited, requirements for "*meaningful interaction*" with clients can limit the adoption of fully automated AI systems that could significantly improve efficiency and accuracy in client onboarding.

Proposed Changes: The PCMA recommends targeted amendments to NI 31-103 and its Companion Policy to explicitly permit AI-enhanced client onboarding processes with appropriate safeguards. Specifically:

[4] See https://www.bcsc.bc.ca/about/media-room/news-releases/2025/06-bcscs-new-campaign-targets-investment-scams-use-of-artificial-intelligence

- clarify that "*meaningful interaction*" requirements can be satisfied through AI-enabled interfaces when supported by appropriate human oversight mechanisms;
- establish a principles-based framework for validating the accuracy and reliability of AI-based KYC processes; and
- create a regulatory sandbox pathway specifically for testing innovative AI-based KYC solutions.

(b) Limited Automated Investment Decision Tools

Current Regulatory Challenges: As stated in the Consultation Paper, the CSA discourages AI systems that engage in "black box" processes and require high levels of explainability. While the PCMA supports transparency, these requirements may inadvertently limit the development of sophisticated AI investment tools that could benefit investors. In the PCMA's view, current regulations are unclear as to when an AI system's output constitutes a "recommendation," thus triggering suitability obligations.

Proposed Changes: The PCMA recommends the following:

- creating a principles based regulatory framework that scales explainability requirements proportionally to the level of autonomy and risk in the AI system;
- establishing clear thresholds for when AI-generated information constitutes a "recommendation"; and
- providing exemptive relief for limited-scope AI investment tools that operate within clearly defined parameters.

By adopting these reforms, the PCMA believes that CSA members can foster responsible AI adoption while maintaining investor trust in automated tools.

(c) AI-Enhanced Compliance and Risk Management Systems

Current Regulatory Challenges: Current compliance and supervisory obligations under NI 31-103 are designed for human-operated compliance systems. While firms are increasingly implementing AI for compliance monitoring, suspicious activity detection, and risk management, regulatory requirements for "effective supervision" and "system of controls" present ambiguity regarding acceptable levels of automation and required human oversight.

Proposed Changes: The PCMA recommends the following:

- amending NI 31-103 to explicitly recognize and provide guidelines for AI-augmented compliance systems;
- developing principles-based standards for validating AI compliance tools;
- establishing a compliance technology sandbox for EMDs to test advanced AI compliance tools; and
- creating a safe harbour provision that protects registrants implementing validated AI compliance systems from regulatory action if those systems fail in ways that could not reasonably have been anticipated.

(d) Advanced Document Analysis and Generation

Current Regulatory Challenges: Private market documentation (*e.g.,* offering memoranda, subscription agreements, etc.) require significant resources to prepare and review. AI tools could dramatically improve efficiency while ensuring regulatory compliance, but current regulations regarding disclosure,

and dealer obligations create uncertainty about the permissible use of AI in document preparation and review.

Proposed Changes: The PCMA recommends the following:

- clarifying that AI-assisted document preparation is permissible when subject to appropriate human review;
- establishing guidelines for the use of AI in reviewing investor documents for compliance with regulatory requirements;
- creating a framework for validating AI document analysis tools; and
- developing a regulatory sandbox specifically for testing AI tools.

(e) Cross-Cutting Regulatory Considerations

In addition to the foregoing, the PCMA also recommends several broader regulatory approaches:

- *Principles-Based Framework.* The PCMA strongly supports a principles based approach to AI regulation that focuses on outcomes rather than prescriptive technical requirements. This would allow for continued innovation while ensuring appropriate investor protections.
- *Harmonized Regulatory Approach.* The PCMA encourages coordination between the CSA, CIRO, and other relevant regulators to ensure consistent approaches to AI regulation across jurisdictions and regulatory bodies.
- *Implementation Timeline*. Any new regulatory requirements should include adequate implementation periods that recognize the complexity of AI systems and the resources required to develop appropriate governance frameworks.
- *Exemptive Relief Process.* The PCMA recommends establishing a streamlined process for obtaining exemptive relief for innovative AI applications, building on the successful models of the CSA Regulatory Sandbox and OSC LaunchPad.

The PCMA believes that with appropriate regulatory amendments and exemptions, AI technologies can enhance the efficiency, compliance, and client service capabilities of EMDs and other private market participants while maintaining robust investor protections. The PCMA encourages the CSA to adopt a balanced approach that promotes innovation while addressing potential regulatory concerns.

2. [a] Should there be new or amended rules and/or guidance to address risks associated with the use of AI systems in capital markets, including related to risk management approaches to the AI system lifecycle? [b] Should firms develop new governance frameworks or can existing ones be adapted? [c] Should we consider adopting specific governance measures or standards (e.g. OSFI's E-23 Guideline on Model Risk Management, ISO, NIST)?

a) Should there be new or amended rules and/or guidance to address risks associated with the use of AI systems in capital markets, including related to risk management approaches to the AI system lifecycle?

The PCMA believes new or amended rules and guidance are necessary to address the unique challenges posed by AI technologies throughout their lifecycle.

The Consultation Paper recognizes that as AI technology evolves, regulatory approaches must adapt accordingly. The PCMA concurs with this assessment and recommend that the CSA consider expanding

NI 31-103 to explicitly address AI system development and deployment phases. The current regulatory framework, while robust for traditional technologies, may not adequately address the distinct characteristics and risks associated with AI systems, including issues related to explainability, bias, data quality, cybersecurity vulnerabilities, and potential systemic risks.

The PCMA believes that a robust, AI-specific governance framework represents an important tool for responsible AI use in the capital markets. The distinct nature of AI risks compared to those associated with traditional technologies necessitates governance measures that may extend beyond conventional approaches.

As discussed below, the National Institute of Standards and Technology's ("**NIST"**) AI Risk Management Framework ("**AI RMF"**) 1.0, released in January 2023,[5] provides valuable insights into managing risks throughout the AI system lifecycle, from design and development through deployment and ongoing monitoring. A lifecycle approach is particularly important given that AI risks can manifest at any stage and may evolve over time as systems are updated or as they interact with changing market conditions.

For private market participants specifically, the PCMA recommends that the CSA provide industry-tailored guidance that acknowledges the diverse nature of entities operating in this space. Such guidance should emphasize proportionate principles that scale regulatory expectations based on the size and complexity of the entity. Smaller entities with limited resources should not face the same implementation requirements as larger institutions with more substantial capabilities. This proportionate approach would support innovation while maintaining appropriate safeguards. The PCMA encourages the CSA to adopt a flexible regulatory framework that can evolve alongside technological developments while providing sufficient clarity for market participants to operate with confidence.

b) Should firms develop new governance frameworks or can existing ones be adapted?

The PCMA supports the development of new governance frameworks specifically designed to address the unique risks associated with the use of AI systems in the capital markets. While existing governance frameworks provide a foundation for risk management, they are typically not tailored to the complexities and specific challenges posed by AI technologies, particularly in the financial sector.

The PCMA believes AI systems in the capital markets present unique risks that differ significantly from traditional financial risks. These include risks related to cyber safety, security, resilience, and ethical considerations. Traditional risk management frameworks are not designed to account for the intricacies of AI, including algorithmic bias, data integrity, autonomous decision-making, and the dynamic nature of AI models.

As discussed above, the NIST AI RMF is an example of a model that establishes a comprehensive AI governance framework. It addresses the need for specialized risk management approaches that encompass the entire AI system lifecycle, offering a structured approach through four core functions:

- *Govern* - Establishing and maintaining robust AI governance systems;
- *Map* - Identifying and contextualizing risks associated with AI systems;
- *Measure* - Developing methodologies to assess AI risks; and
- *Manage* - Implementing strategies to mitigate and manage identified risks.

[5] https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf

By focusing on these functions, the PCMA believes the NIST AI RMF provides an example of a holistic and iterative approach to managing AI risks, which is particularly relevant for capital markets where AI applications can evolve rapidly and unpredictably.

The Consultation Paper raises the possibility of adopting governance measures inspired by frameworks like the NIST AI RMF. This acknowledgment underscores the CSA's recognition of the evolving risks posed by AI and the need for frameworks that can dynamically adapt to technological advancements. The CSA's focus on model risk management, highlights the importance of addressing AI-specific risks rather than merely adapting existing, more generalized frameworks.

Additionally, the International Organization of Securities Commissions ("**IOSCO"**) has recognized the NIST AI RMF 1.0 as a voluntary standard that could be instrumental for regulators and market participants to address AI-related risks.[6] This international perspective aligns with the UC Berkeley white paper's guidance on evaluating AI systems for trustworthiness under the NIST framework.[7]

While existing governance and risk management frameworks, such as those developed for financial risk or traditional IT systems, offer foundational elements, they are not inherently designed to address the dynamic, data-driven, and evolving nature of AI. Attempting to retrofit these frameworks to encompass AI risks may result in inadequate coverage and potential oversight gaps.

Based on the foregoing, the PCMA recommends that Canadian capital market participants consider adopting governance frameworks specifically designed for AI, such as the NIST AI RMF. This approach would not only align with best practices recognized internationally but also address the specific needs of AI governance in the financial sector. Establishing clear, consistent, and comprehensive governance structures can better protect market integrity and reduce systemic risk.

c) Should we consider adopting specific governance measures or standards (e.g. OSFI's E-23 Guideline on Model Risk Management, ISO, NIST)?

The PCMA supports adopting a hybrid approach that integrates elements of OSFI's E-23 Guideline, ISO/IEC 42001, and the NIST AI RMF. Each framework offers valuable contributions to effective AI governance:

- OSFI's E-23 provides expanded scope for model risk management that aligns with capital market vulnerabilities;
- NIST AI RMF offers actionable steps for identifying and mitigating AI-specific risks; and
- ISO/IEC 42001 certification would signal adherence to international ethical norms and strengthen investor confidence.

The PCMA recognizes significant challenges in implementation, particularly for smaller market participants. Overlapping requirements between frameworks could create unnecessary redundancies, and the compliance costs associated with comprehensive framework adoption may disproportionately burden fintech startups and smaller firms. Additionally, without clear enforcement mechanisms, there is risk of inconsistent adoption and potential "AI washing".

[6] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD788.pdf
[7] https://cltc.berkeley.edu/wp-content/uploads/2023/01/Taxonomy_of_AI_Trustworthiness.pdf

To address these concerns, the PCMA recommends the CSA adopt core elements of OSFI's E-23 and NIST AI RMF while encouraging ISO/IEC 42001 certification primarily for high-risk use cases. Specifically, AI governance frameworks should include OSFI E-23-style model risk ratings, third-party oversight, and board accountability, integrated with the NIST AI RMF measurement functions for addressing explainability concerns. However, full ISO certification should be prioritized only for AI systems used in critical functions such as trading, client profiling, or fraud detection, where systemic risks are highest. There needs be a balance between investor protection and fair and efficient capital markets.

For private market participants, the PCMA recommends that the CSA implement a phased, principles based approach that recognizes the diverse nature of entities operating in this space. Pilot standards should begin with large institutions first, allowing smaller firms to adopt simplified controls such as automated AI compliance tools. Such a proportionate approach should support innovation while maintaining appropriate safeguards at what should be a manageable cost.

Additionally, the PCMA recommends the CSA establish AI documentation standards that strike a careful balance between necessary transparency and legitimate commercial confidentiality concerns. Firms investing substantial resources in developing proprietary AI systems require assurance that regulatory required disclosure will not compromise their competitive position, while sufficient documentation remains essential for effective supervision.

The evolving nature of AI technologies will likely require ongoing regulatory adaptation. The PCMA encourages the CSA to adopt a flexible regulatory framework that can evolve alongside technological developments while providing sufficient clarity for market participants to operate with confidence. By focusing regulatory requirements on higher-risk AI applications and harmonizing with existing guidelines, the CSA can achieve an effective balance between innovation, investor protection, and reducing regulatory burden.

While existing regulatory frameworks provide a foundation, the unique characteristics and risks associated with AI systems in the capital markets necessitate new or amended rules and guidance. By expanding NI 31-103, providing proportionate industry-tailored guidance, and establishing a balanced hybrid approach to AI governance, the CSA can foster responsible innovation while protecting investors and maintaining market integrity and financial stability. The PCMA believes this approach aligns with the CSA's mandate and would benefit all capital market participants.

3. Data plays a critical role in the functioning of AI systems and is the basis on which their outputs are created. [a] What considerations should market participants keep in mind when determining what data sources to use for the AI systems they deploy (e.g. privacy, accuracy, completeness)? [b] What measures should market participants take when using AI systems to account for the unique risks tied to data sources used by AI systems (e.g. measures that would enhance privacy, accuracy, security, quality, and completeness of data)?

(a) What considerations should market participants keep in mind when determining what data sources to use for the AI systems they deploy (e.g. privacy, accuracy, completeness)?

When determining what data sources to use for AI systems, the PCMA believes that capital market participants should keep several important considerations in mind for ensuring responsible innovation and compliance with applicable securities laws, including the following:

- *Privacy* - Market participants must account for privacy considerations when using data in AI systems. If outsourcing any service based on AI systems, they should bear in mind the privacy law implications associated with inputting client information and take appropriate steps to keep this information confidential. AI systems collecting vast amounts of data have the potential to directly or indirectly identify individuals, raising privacy concerns. The use of synthetic data generated by AI may alleviate some privacy challenges by mimicking real data without the same privacy restrictions.
- *Accuracy and Completeness* - It is vital that the data used by AI systems be accurate and complete. Poor data quality can lead to inaccurate assumptions, inadequate and erroneous modeling, and poor performance. Market participants should take measures to enhance the accuracy, security, quality, and completeness of data used by AI systems. They should also verify the quality and accuracy of information sources used by AI systems. Data quality improvement is a key area where AI is being used, involving identifying anomalies and ensuring data reliability for model training and insight generation.
- *Data Bias* - Market participants should be aware that data used to train AI systems can be biased if datasets are not sufficiently diverse or representative. Biased data sets used by an AI system may result in conflicted decisions that favour the interests of the market participant over those of their client. Model bias, stemming from algorithmic bias, cognitive bias, or training data bias, can cause AI systems to unfairly treat certain groups of investors or have a bias for certain investment types.
- *Data Provenance* - The source and providers of the data that the AI system uses should be considered and, where material, disclosed. However, the PCMA notes that open-source or vendor-built models, the provenance and type of training data may not be available, making it difficult to evaluate its quality and potential biases.
- *Data Drift* - Market participants need to be mindful of data drift, where the training data becomes unrepresentative over time, potentially impacting the AI system's performance.
- *Data Security* - Adequate measures should be in place to ensure the security of data used by AI systems. Exposing internal data, including client personally identifiable information, to an insecure AI system could lead to cybercrime, exposure, and misuse.
- *Relevance* - The data used should be relevant to the intended purpose of the AI system. Greater access to a broader range of relevant, high-quality data can contextualize a model's performance, potentially leading to more diverse and contextually relevant decision-making.
- *Data Management* - Market participants need to have robust policies and procedures for managing data used by AI systems, considering its volume, variety, sources, and quality.

In summary, the PCMA believes market participants must take a holistic approach to data source selection for AI systems, carefully evaluating privacy implications, ensuring the accuracy, completeness, quality, and relevance of the data, understanding its provenance, mitigating potential biases and security risks, and establishing robust data management practices.

(b) What measures should market participants take when using AI systems to account for the unique risks tied to data sources used by AI systems (e.g. measures that would enhance privacy, accuracy, security, quality, and completeness of data)?

The PCMA believes that market participants should take the measures below when using AI systems to account for the unique risks tied to data sources used by AI systems.

- The PCMA recommends that market participants implement *data governance frameworks* when using AI systems. Frameworks are important and should include establishing governance teams, implementing role-based access controls, and maintaining audit trails. These structures provide the necessary foundation for responsible AI deployment and ensure accountability throughout the data management lifecycle. Clear retention policies should be standardized to prevent the unnecessary storage of obsolete information, which could otherwise compromise data integrity and system performance.

- Market participants should implement *validation and verification protocols*, which may include pre-processing checks, bias audits, and *cross-validation techniques*[8] to ensure *model generalization*.[9] These procedures are important for identifying and addressing potential inaccuracies, biases, or inconsistencies in the data that could adversely affect AI system outputs. *Preprocessing data*[10] to handle missing values, outliers, and inconsistencies through techniques such as imputation or normalization enhances the reliability of AI systems. Regular dataset validation using statistical checks further reinforces data integrity, while optimization through *hyperparameter tuning*.[11] significantly improves prediction reliability.

- *Privacy protection* should be prioritized through the deployment of privacy-enhancing technologies such as data anonymization, encryption, and *federated learning*.[12] to protect sensitive information. Anonymizing sensitive data using encryption or tokenization helps to prevent re-identification of individuals, while federated learning approaches enable model training without transferring raw data to centralized servers, thereby minimizing exposure risks. Embedding privacy by design principles into AI development pipelines, including user consent mechanisms and transparency reports, aids compliance with applicable privacy laws. Additionally, enforcing access controls based on role-based permissions and maintaining audit trails for data usage further strengthens privacy safeguards.

- *Vendor and third-party management* is equally important when utilizing external data sources. Market participants should establish contractual safeguards that clearly define data quality requirements and usage limitations. Continuous monitoring of vendor performance and data quality from third-party sources is necessary to maintain integrity throughout the supply chain. Due diligence on vendor data practices before engagement and mechanisms for data integrity should be standard practice for all market participants leveraging external data sources for their AI systems.

[8] *Cross-validation* is a technique to assess how well a model performs on different subsets of data. It ensures that the model generalizes well to new, unseen data.
[9] *Generalization* means the model can perform well on new data, not just the data it was trained on. Techniques like cross-validation help confirm that the model is not overfitting (performing well only on training data) or underfitting (performing poorly on both training and new data).
[10] Before feeding data into an AI model, it's important to clean and prepare the data. *Pre-processing* can involve handling missing values (e.g., filling them in or removing them), identifying and dealing with outliers, and normalizing the data so that it fits within a consistent range or distribution.
[11] *Hyperparameters* are settings that define the model's structure or how it learns. *Tuning these parameters* can enhance model performance and prediction reliability.
[12] *Federated learning* is a machine learning technique designed to enhance privacy while training models

- *Security safeguards* constitute another important element in addressing data source risks. The implementation of *zero-trust architectures*[13] helps prevent unauthorized access to sensitive information, while anomaly detection systems monitor data pipelines to flag unauthorized transfers or breaches. Defending against adversarial attacks through simulated malicious inputs during training and applying *gradient masking*[14] enhances system resilience. *Encryption of data at rest*[15] and in transit, combined with regular security audits, provides protection against potential security vulnerabilities.

- *Data quality and completeness assurance measures* are important for reliable AI systems. Market participants should conduct completeness audits to identify missing critical variables across required dimensions, especially in high-stakes domains. Implementing *gap-filling strategies, including synthetic data generation*[16] for incomplete datasets, safeguards data comprehensiveness. Filtering data for relevance to remove redundant or unrelated information prevents output distortion, while maintaining timeliness through periodic dataset updates reflects current market conditions.

- *Continuous monitoring and improvement mechanisms* should be established, including model drift detection, regular security audits, and feedback loops for iterative refinements. These mechanisms enable the identification of performance deterioration due to changing data patterns and facilitate necessary adjustments. Regular security audits assess vulnerabilities in data handling processes, while feedback loops based on performance metrics drive system optimization. Documentation of model limitations ensures appropriate use and interpretation of AI outputs.

The PCMA recognizes the resource constraints faced by smaller EMDs and supports principles based approaches to regulation. A phased implementation of comprehensive measures would lessen the burden of compliance. Regulatory sandboxes for testing innovative solutions while managing risks should foster responsible innovation. Scalable governance models that can grow with organizational capacity and industry collaboration to share best practices would support effective implementation across entities of varying sizes.

The PCMA believes that effective AI deployment in the private capital markets depends on proactive data governance. By prioritizing data quality, privacy, security, and completeness, and implementing validation, vendor oversight, and monitoring measures, market participants can mitigate risks while harnessing AI's transformative potential. The PCMA supports a principles based regulatory approach

[13] A *zero-trust architecture* is a security model operates on the principle of "never trust, always verify". It ensures that every access request is authenticated and authorized, even if it comes from within the network. It reduces the risk of insider threats and unauthorized access to sensitive data.

[14] *Gradient masking* is a technique used to obscure the model's sensitivity to small input changes, making it harder for attackers to exploit the model.

[15] *Encryption of data at rest* protects stored data by converting it into an unreadable format unless decrypted by an authorized party.

[16] When data is incomplete, *gap-filling techniques* are used to enhance the dataset. One approach is *synthetic data generation*, where artificial data is created based on existing patterns to fill in the gaps. This helps maintain data comprehensiveness without compromising accuracy.

that allows for flexibility in implementation while ensuring adequate protection for investors and market integrity, recognizing the diversity of market participants and their varying resources and capabilities.

4. [a] What role should humans play in the oversight of AI systems (e.g. "human-in-the-loop") and how should this role be built into a firm's AI governance framework? [b] Are there certain uses of AI systems in capital markets where direct human involvement in the oversight of AI systems is more important than others (e.g. use cases relying on machine learning techniques that may have lesser degrees of explainability)? [c] Depending on the AI system, what necessary skills, knowledge, training, and expertise should be required? Please provide details and examples.

(a) What role should humans play in the oversight of AI systems (e.g. "human-in-the-loop") and how should this role be built into a firm's AI governance framework?

The PCMA recognizes that effective human oversight is crucial for the responsible deployment of AI in the capital markets. The PCMA believes that human involvement should fulfill three primary roles:

- *Real-Time Monitoring*: Continuous validation of AI inputs/outputs to detect anomalies, model drift, or biases, particularly in high-stakes applications like suitability assessments or fraud detection;
- *Strategic Intervention*: Exercising judgment to resolve conflicts, assess fairness or what is in the best interest of a client, and align AI outputs with CSA requirements; and
- *Override Authority*: Ability to halt or modify AI-driven decisions when risks exceed predefined thresholds.

These functions are essential for detecting anomalies, resolving conflicts, and halting AI-driven decisions when necessary.

To integrate human oversight into governance frameworks, the PCMA recommends implementing principles based oversight models. These should range from Human-in-the-Loop ("**HITL"**) for high-stakes applications like investment advice, to Human-on-the-Loop ("**HOTL"**) for transaction surveillance, and Human-out-of-the-Loop ("**HOOTL"**) for low-risk, repetitive tasks. Additionally, accountability mechanisms such as audit trails, escalation protocols, and cross-functional oversight committees should be established.

AI Use Case	Oversight Model	Rationale
Investment Advice	HITL	Mandatory for suitability determinations
Transaction Surveillance	HOTL	Requires post-hoc review of flagged activities
Back-Office Automation	HOOTL	Limited to low-risk, repetitive tasks

(b) Are there certain uses of AI systems in capital markets where direct human involvement in the oversight of AI systems is more important than others (e.g. use cases relying on machine learning techniques that may have lesser degrees of explainability)?

The PCMA has identified several high-priority use cases where it believes direct human involvement is essential:

- *KYC and Client Onboarding* - Despite AI's efficiency in gathering and processing KYC information, human oversight is critical to ensure "*meaningful interactions*" with clients. Human compliance officers must be available to monitor for errors, provide explanations, and engage directly with DRs and/or clients when necessary, particularly when information gathered will inform investment recommendations.

- *Investment Recommendations and Suitability Determinations* - While AI can efficiently analyze potential investments against client profiles, the ultimate responsibility for ensuring suitability remains with DRs and compliance officers. Human judgment is essential to interpret AI-generated insights within the broader context of client needs and to guard against automation bias, where DRs and compliance officers might over-rely on potentially flawed AI recommendations.

- *Limited Automated Decisions* - For any AI systems making limited automated decisions, particularly in trading environments, firms must maintain effective real-time monitoring and post-trade review systems. Human intervention capabilities should be commensurate with the level of AI autonomy and the potential impact of decisions.

- *Client Support Involving Advice or Complaints* - Human oversight is crucial when AI systems handle complex client inquiries, provide advice, or manage complaints. Human representatives should be ready to intervene when AI systems reach their capability limits, ensuring accurate information delivery and appropriate resolution of client concerns.

- *Risk Management and Compliance* - AI-enhanced fraud detection and market surveillance systems require human expertise to interpret alerts and determine appropriate actions. Human judgment is necessary to address both false positives and negatives, and to identify and mitigate potential biases in these systems.

- *Novel or High-Risk AI Applications* - When deploying AI in new or high-risk areas, significant human oversight from both market participants and the CSA is required. This includes proactive consultation with regulators and thorough assessment of whether regulatory obligations can be met.

The PCMA believes that while AI offers tremendous potential to enhance financial services, the level of human involvement should be proportionate to the role and potential impact of the AI system, with particular emphasis on explainability, regular testing, and the ability for humans to monitor and intervene when necessary.

(c) Depending on the AI system, what necessary skills, knowledge, training, and expertise should be required? Please provide details and examples.

The PCMA believes market participants utilizing AI outputs require adequate AI literacy as a baseline requirement. This foundational understanding must encompass not only the capabilities of these systems but also their inherent limitations, including potential biases and hallucinations. The PCMA emphasizes that personnel must be equipped to critically interpret AI outputs and determine their appropriateness within specific capital market contexts. This critical thinking ability becomes particularly important when AI systems generate recommendations for investment decisions or compliance monitoring.

For those responsible with the oversight and management of AI systems, a *more comprehensive skill set* is necessary. These individuals must possess the knowledge to assess whether an AI system is fit for purpose and understand the robustness of testing methodologies employed prior to deployment. This includes the ability to evaluate both the technical architecture and the business logic underpinning these systems. For example, an AI system designed to identify potential insider trading within a

registrant firm must be validated not just for technical performance but for its alignment with regulatory definitions and evidentiary standards of market abuse.

Risk management capabilities form another important component of the required expertise. Personnel must be able to monitor and mitigate technological and operational risks related to cybersecurity vulnerabilities, system bias, model drift, and output hallucinations. The PCMA believes these risks are more acute in private markets where data is more limited and less standardized than in the public markets. Consequently, risk management frameworks should be adapted to account for these unique characteristics of private capital data environments.

Data management skills represent an important capability for effective AI oversight. This includes ensuring data accuracy, completeness, and addressing privacy considerations throughout the AI lifecycle. Personnel should be able to assess the quality and provenance of data used to train AI models, recognizing that the integrity of outputs is directly dependent on input quality. In private markets, where information asymmetries are more pronounced, rigorous data governance becomes even more crucial to prevent reinforcement of existing market inefficiencies.

The *ability to balance advanced AI capabilities with appropriate levels of explainability* is becoming increasingly important. Oversight personnel need to understand the trade-offs between model complexity and transparency, determining the necessary level of explainability based on the specific use case and potential impact. For high-stakes applications such as investor suitability assessments, the PCMA advocates for prioritizing explainability even at the potential cost of marginal performance improvements.

For firms leveraging outsourced AI services, *specialized knowledge* becomes important. Personnel must understand registrant conduct requirements and develop specific capabilities to address the unique risks posed by third-party AI systems. This includes implementing robust due diligence frameworks and ongoing monitoring protocols.

Testing and ongoing monitoring expertise are an important function of effective AI governance. Regular evaluation of AI systems both before and after adoption is valuable, with testing scope proportionate to the system's role and potential impact.

The PCMA strongly advocates for a blended knowledge approach that combines technical AI expertise with deep domain knowledge of capital markets and applicable securities law. This integrated perspective enables more informed decisions about risk management and compliance, helping firms understand the complex trade-offs between bias mitigation and model performance in financial contexts. The PCMA believes that effective oversight teams include individuals with complementary skill sets spanning quantitative methods, regulatory expertise, and business domain knowledge.

To address the knowledge gaps in AI and data science, the PCMA recommends *implementing comprehensive training and development programs*. Continuous education on AI complexities should be tailored to capital market applications, with particular emphasis on cross-training between technical teams and compliance personnel. This approach would help bridge knowledge gaps and creates a shared understanding of both technical capabilities and regulatory requirements.

For EMDs transitioning to AI-augmented workflows, the PCMA encourages the CSA to provide specific regulatory guidance emphasizing skills development pathways. Many EMDs face resource constraints that could limit their ability to build comprehensive AI expertise in-house. Regulatory clarity regarding minimum competency requirements would help these firms prioritize their training investments and ensure adequate oversight despite resource limitations.

The PCMA advocates for a principles based approach to human oversight in AI systems. While AI can significantly enhance efficiency in the capital markets, human judgment remains crucial in high-impact, low-explainability applications. The PCMA recommends implementing targeted training programs, such as certification courses on AI explainability tools for compliance officers and simulation exercises for stress-testing human override protocols. Additionally, collaborative frameworks that facilitate knowledge sharing between quantitative developers and compliance teams can help bridge technical and regulatory knowledge gaps.

The PCMA believes that the appropriate investment in skills development and clear regulatory guidance, private capital market participants can harness the benefits of AI while maintaining robust oversight frameworks and investor protection. The PCMA stands ready to collaborate with the CSA on developing more detailed competency frameworks tailored to the unique challenges of AI deployment in the private capital markets.

5. [a] Is it possible to effectively monitor AI systems on a continuous basis to identify variations in model output using test-driven development, including stress tests, post-trade reviews, spot checks, and corrective action in the same ways as rules-based trading algorithms in order to mitigate against risks such as model drifts and hallucinations? [b] If so, please provide examples. Do you have suggestions for how such processes derived from the oversight of algorithmic trading systems could be adapted to AI systems for trading recommendations and decisions?

Not applicable in the private capital markets.

6. Certain aspects of securities law require detailed documentation and tracing of decision-making. This type of recording may be difficult in the context of using models relying on certain types of AI techniques. [a] What level of transparency/explainability should be built into an AI system during the design, planning, and building in order for an AI system's outputs to be understood and explainable by humans? [b] Should there be new or amended rules and/or guidance regarding the use of an AI system that offer less explainability (e.g. safeguards to independently verify the reliability of outputs)?

(a) What level of transparency/explainability should be built into an AI system during the design, planning, and building in order for an AI system's outputs to be understood and explainable by humans?

The PCMA supports the principle that AI systems deployed in the capital markets should incorporate the highest degree of explainability feasible given the specific AI technology being used. The PCMA believes this position aligns with CSA expectations while acknowledging practical implementation realities faced by market participants. The PCMA recognizes that transparency is fundamental to maintaining trust in the financial markets and AI systems should not be a means to circumvent existing regulatory obligations for accountability and disclosure.

The PCMA believes a principles based approach to explainability requirements would be more effective than prescriptive technical specifications. The field of AI continues to evolve rapidly, and overly specific requirements may quickly become outdated or could inadvertently restrict beneficial innovation. Prioritizing outcomes and ensuring market participants comprehend and assume accountability for deployed systems fosters technological adaptability while upholding investor protection standards.

A critical consideration in AI system design is the inherent tension between advanced capabilities and explainability. Some cutting-edge AI technologies offer significant performance benefits may have lower inherent explainability. In these cases, market participants should not be categorically prohibited from using such technologies, but should be required to implement additional safeguards commensurate with the reduced explainability. These safeguards might include more rigorous pre-deployment testing, enhanced documentation of development processes, more frequent post-implementation monitoring, and additional verification mechanisms.

Human oversight remains essential, particularly for AI systems operating in high-risk domains. The PCMA believes that regardless of the AI technologies employed, systems must provide sufficient context and explanation to enable meaningful human-in-the-loop monitoring. This is especially crucial in areas such as KYC processes, compliance monitoring, and trade execution where regulatory obligations and potential for client harm are heightened. The level of explainability should be sufficient to allow human overseers to understand why particular outputs or recommendations were generated and to intervene appropriately when necessary.

The PCMA recommends a principles based approach to explainability requirements that scales with the potential impact of AI system decisions. Systems directly making or supporting material investment decisions would reasonably be subject to higher explainability standards than those performing administrative or back-office functions with minimal direct impact on clients. This proportional approach would focus regulatory and industry resources where they can most effectively protect market integrity and investor interests.

To achieve appropriate explainability during AI system development, the PCMA recommends several practical implementation approaches:

- Establishing comprehensive documentation requirements to capture key design decisions, data selection criteria, and training methodologies;
- Including input-output analysis capabilities in all AI system, allowing users to trace relationships between specific inputs and resulting outputs;
- Incorporating feature importance detection to identify the key factors influencing system decisions; and
- Having standardized explainability metrics appropriate to different AI technologies which the PCMA believes would benefit both market participants and CSA members by providing consistent evaluation frameworks.

The challenge of addressing conflicts of interest is particularly relevant when considering AI explainability. Systems with limited transparency may complicate efforts to ensure decisions do not inappropriately favour the market participant over clients. In these situations, additional testing protocols and monitoring mechanisms become essential. The PCMA supports requirements for independent verification of AI systems where material explainability limitations could potentially mask conflicts of interest or other compliance concerns.

The PCMA believes explainability must be integrated from the earliest design phases of AI system development rather than attempted retroactively. By embedding these considerations throughout the development lifecycle, market participants can better meet their obligations under securities law while still benefiting from advances in AI. This approach aligns with the CSA's stated view that systems with the highest feasible degree of explainability will better assist market participants in meeting their regulatory obligations.

The PCMA recognizes that determining the "appropriate" level of explainability involves balancing multiple factors, including system purpose, risk level, technical constraints, and practical utility of explanations to different stakeholders. While complete technical transparency may not always be feasible or necessary, the focus should be on providing meaningful explanations that enable market participants, clients, and CSA members to understand the basis for system outputs and decisions in contexts relevant to their needs.

The PCMA supports a balanced regulatory approach that promotes the highest feasible level of AI explainability while allowing for continued innovation in capital markets. The PCMA believes thoughtfully designed explainability requirements, implemented through a principles-based framework with tiered application based on risk, would best serve the interests of all market participants while maintaining Canada's position as a leader in responsible financial innovation.

(b) Should there be New or Amended Rules and/or Guidance Regarding the Use of an AI System that Offers Less Explainability

The PCMA believes new tailored guidance rather than extensive new rules would be most effective in addressing the challenges posed by less explainable AI systems. The existing securities regulatory framework already establishes core principles of accountability, transparency and investor protection which remain applicable regardless of the technology employed. Specific guidance on how these principles apply to "black box" AI systems would provide valuable clarity to market participants.

The rapid evolution of AI technology suggests overly prescriptive rules could quickly become outdated or might inadvertently stifle beneficial innovation. Instead, the PCMA recommends developing flexible guidance focused on ensuring appropriate safeguards are in place when less explainable systems are deployed. This approach would allow the regulatory framework to adapt as AI capabilities and explainability techniques continue to advance.

For AI systems with limited explainability, the PCMA believes additional safeguards are necessary to maintain market integrity and investor protection. Any CSA guidance should emphasize a *risk-based approach* where the level of required independent verification scales with the potential impact of system decisions and the degree of explainability limitation. Higher-risk applications with lower explainability would warrant more robust verification protocols.

The PCMA recommends guidance for less explainable AI systems include requirements for *validation processes* both pre-deployment and during ongoing operation. These processes should include testing with diverse datasets, adversarial testing to identify potential failure modes, and regular benchmark comparisons against more traditional methodologies. Documentation of these validation processes should be sufficiently detailed to demonstrate due diligence to regulators if required.

Independent verification is particularly important for less explainable systems involving core regulatory functions. The PCMA supports guidance that would encourage or require third-party audits or reviews for high-risk applications of black box AI. These independent assessments could evaluate system performance, test for unintended biases, and verify appropriate governance controls are in place, without necessarily requiring access to proprietary algorithms or training data.

For systems where complete explainability remains technically unfeasible, the PCMA believes CSA guidance should require *alternative transparency mechanisms*. These might include providing statistical confidence metrics alongside outputs, maintaining libraries of representative case studies demonstrating system behaviour, implementing robust anomaly detection, and establishing clear escalation protocols when system outputs appear questionable.

Human-in-the-loop oversight is crucial for less explainable systems. CSA guidance should specify that even with limited system explainability, sufficient information must be provided to human overseers to enable meaningful review of system outputs and appropriate intervention when necessary. This might include providing confidence scores, highlighting unusual patterns in the input data, or flagging outputs that deviate significantly from historical patterns.

Record-keeping requirements should be enhanced for less explainable systems to ensure accountability and facilitate post-hoc analysis. The PCMA recommends CSA guidance specifying that a record of material inputs, outputs, and human interventions be maintained , along with relevant system state information, to create an audit trail that could help explain outcomes even when the internal decision process of the AI system is opaque.

Regarding actual or *potential conflicts of interest*, the PCMA emphasizes the need for enhanced safeguards, especially when employing less transparent systems in situations where firm incentives might outweigh a client's best interest. CSA guidance should require enhanced monitoring specifically designed to detect potential conflicted outcomes, even when the reasoning behind individual decisions by the AI system remains difficult to interpret.

The PCMA also recommends any guidance include *disclosure requirements* tailored to the use of less explainable AI systems. Market participants should be expected to communicate appropriately with clients about the use of such systems, the general nature of the technology employed, its limitations, and the safeguards in place to ensure reliable outputs. This transparency would help maintain trust while acknowledging technological constraints.

Finally, the PCMA suggest guidance include expectations for *ongoing monitoring* of less explainable systems throughout their lifecycle. This should include regular performance reviews, drift detection to identify when systems begin performing differently than expected, and periodic reassessments of whether advances in explainable AI might enable migration to more transparent alternatives.

The PCMA supports the development of targeted guidance rather than extensive new rulemaking to address the unique challenges of less explainable AI systems. By focusing on appropriate safeguards, independent verification, enhanced monitoring, and meaningful human oversight, such CSA guidance would help ensure even advanced "black box" systems operate in a manner consistent with regulatory objectives and market participants' obligations under applicable securities law.

7. FinTech solutions that rely on AI systems proposing to provide KYC and onboarding, advice, and carry out discretionary investment management challenge existing reliance on proficient individuals to carry out registerable activity. [a] Should regulatory accommodations be made to allow for such solutions and, if so, which ones? [b] What restrictions should be imposed to provide the same regulatory outcomes and safeguards as those provided through current proficiency requirements imposed on registered individuals?

(a) Should regulatory accommodations be made to allow for such solutions and, if so, which ones?

The PCMA believes that regulatory accommodations for AI-based FinTech solutions should be calibrated based on the nature of the registerable activity, the associated investor risks, and the current technological limitations of AI systems. The existing registration regime's reliance on proficient individuals serves the critical function of ensuring accountability, applying professional judgment, and maintaining investor protection. While technological innovation offers significant potential benefits, any regulatory accommodations must preserve these fundamental protections.

With respect to *KYC and onboarding processes*, the PCMA believes this area presents the most appropriate opportunity for regulatory accommodations. AI systems could reasonably be permitted to gather information, conduct preliminary risk profiling (i.e., risk tolerance and risk capacity), and flag inconsistencies or missing information, provided adequate safeguards are maintained. These safeguards should include human verification for complex cases, regular testing and validation of AI accuracy, comprehensive audit trails, and transparent client disclosure regarding the use and limitations of AI in the onboarding process. Such accommodations would likely enhance efficiency without materially compromising investor protection.

As for investment advice, the PCMA recommends more circumscribed accommodations. AI systems could appropriately support registered individuals by analyzing information and generating preliminary recommendations within narrowly defined parameters. However, a "human-in-the-loop" model where registered individuals review and assume responsibility for final recommendations is essential, in most cases. This model preserves the critical role of human judgment while leveraging AI's analytical capabilities. Additional safeguards should include enhanced explainability requirements for AI-generated advice, ongoing monitoring for systematic biases, and clear client disclosure about the role and limitations of AI in the advisory relationship.

The PCMA further believes that regardless of the specific accommodations granted, certain cross-cutting requirements should apply. These include:

- Clear accountability and governance frameworks with designated responsible individuals possessing appropriate securities and AI expertise;
- Enhanced transparency and explainability of AI systems sufficient to enable understanding and justification of decisions;
- Appropriate proficiency standards for individuals overseeing AI systems; and
- Meaningful client disclosure regarding the role, limitations, and risks of AI-driven services.

The PCMA recommends the CSA consider implementing these accommodations through a regulatory sandbox approach, which would permit controlled testing of AI solutions with appropriate safeguards, enable data collection on performance and risks, and allow for iterative refinement of regulatory requirements based on actual market experience. This approach would foster responsible innovation while ensuring that investor protection remains paramount.

The PCMA believes carefully constructed regulatory accommodations can enable the industry to harness the benefits of AI while maintaining robust investor protection. A principles based approach that applies stricter requirements as the potential impact on investors increases represents the most prudent path forward. While AI can enhance and support registerable activities, it should complement rather than fully replace human judgment, responsibility, and accountability, particularly for high-impact activities like suitability assessments.

(b) What restrictions should be imposed to provide the same regulatory outcomes and safeguards as those provided through current proficiency requirements imposed on registered individuals?

While acknowledging AI's potential benefits, the PCMA believes that any regulatory accommodation must provide equivalent investor protection as current proficiency requirements. To achieve this outcome, the PCMA proposes the following framework of necessary restrictions:

- *Registered individual oversight is paramount*. AI systems must operate under the supervision of a qualified registered individual who satisfies NI 31-103 proficiency requirements. This individual must maintain the authority to review and override AI-generated recommendations, with ultimate responsibility for any registerable activities performed by the system.
- *Explainability and transparency* must be required for AI systems to enable registered individuals to understand recommendations, compliance staff to verify adherence to securities legislation, and regulators to audit system operations. For complex systems with limited explainability, supplementary testing protocols should be implemented, along with comprehensive documentation of methodologies.
- *Governance frameworks* must include board-level oversight, designated senior officers responsible for AI governance, written policies addressing development and risk management, and regular independent audits. Prior to deployment, AI systems should undergo rigorous testing, including performance benchmarking, stress testing, and compliance verification, followed by continuous monitoring and validation during operation.
- *Enhanced proficiency requirements* should be established for individuals supervising AI systems, including demonstrated knowledge of AI technologies and their application in securities markets. Comprehensive record-keeping should document all system operations, human intervention, and testing results, maintained for regulatory examination.
- *Clients must receive clear disclosure* regarding AI involvement in services, human oversight mechanisms, associated risks, and their right to request human intervention. Certain activities should be prohibited from full automation, including complex suitability determinations for vulnerable investors.
- *Registrants utilizing third-party AI solutions must conduct due diligence on providers* while maintaining ultimate responsibility for regulatory compliance. Additionally, enhanced regulatory reporting should include initial certification requirements, regular performance reporting, specialized examinations, and mandatory reporting of material malfunctions.

The PCMA recommends a phased implementation approach with a regulatory sandbox for qualifying registrants, development of detailed guidance through industry collaboration, proportionate application of restrictions based on risk profile, and periodic effectiveness reviews.

The PCMA believes these restrictions represent a balanced approach that would provide regulatory outcomes equivalent to current proficiency requirements while allowing for responsible innovation. AI systems should augment rather than replace the professional judgment of qualified individuals.

8. [a] Given the capacity of AI systems to analyze a vast array of potential investments, should we alter our expectations relating to product shelf offerings and the universe of reasonable alternatives that representatives need to take into account in making recommendations that are suitable for clients and put clients' interests first? [b] How onerous would such an expanded responsibility be in terms of supervision and explainability of the AI systems used?

(a) Given the capacity of AI systems to analyze a vast array of potential investments, should we alter our expectations relating to product shelf offerings and the universe of reasonable alternatives that representatives need to take into account in making recommendations that are suitable for clients and put clients' interests first?

The PCMA believes that the CSA should retain its existing expectations concerning product shelf offerings for EMDs and the spectrum of suitable alternatives DRs should account for when providing client-focused counsel.

Analysis of private market securities (*e.g.,* private equity, private debt, real estate, and infrastructure) using standardized AI methods is problematic due to their inherent, non-uniform characteristics. Unlike public securities with transparent pricing, trading history, and disclosure requirements, private market investments are characterized by limited information availability, restricted access, complex legal structures, and heterogeneous terms. The opacity inherent in the private markets creates significant challenges for AI systems attempting to analyze the "vast array" of potential investments in this space.

While AI can process structured data efficiently, much of the critical information in the private markets is unstructured, relationship-dependent, and requires contextual understanding that the PCMA believes current AI systems cannot reliably replicate. Furthermore, private market investments may have limited liquidity windows, investment thresholds, and specific investor qualification requirements that cannot be easily aggregated or compared through automated systems.

There are also supervision and explainability challenges associated with AI-driven private market investment recommendations. DRs recommending private market securities must understand not only the investment's characteristics but also its unique risks, structural elements, and alignment with specific investor needs. The expectation that AI could meaningfully expand the universe of reasonable alternatives in the private capital markets overlooks the relationship-based, negotiated nature of many private transactions. Additionally, the PCMA believes private market investments often require ongoing relationship management that cannot be adequately assessed through algorithmic analysis.

At the current stage of AI development, the PCMA believes AI systems may serve as supplementary tools for data organization in the private markets, but cannot meaningfully expand the universe of suitable private market investments a DR should reasonably consider.

The PCMA recommends maintaining the current regulatory framework for private market securities, with a focus on qualitative assessment and DR expertise rather than quantitative expansion of investment alternatives.

DRs operating in the private capital markets should continue to leverage their specialized knowledge, networks, and judgment when making suitable recommendations, using AI tools as supplements rather than primary drivers of investment decisions. Given private market challenges of limited data and non-standard structures, expanding the alternatives universe would create unreasonable obligations that could reduce access to private investments rather than improve client outcomes.

(b) How Onerous Would such an Expanded Responsibility be in Terms of Supervision and Explainability of the AI Systems Used?

Not applicable based on response in 8(a).

9. [a] Should market participants be subject to any additional rules relating to the use of third-party products or services that rely on AI systems? [b] Once such a third-party product or service is in use by a market participant, should the third-party provider be subject to requirements, and if so, based on what factors?

(a) Should market participants be subject to any additional rules relating to the use of third-party products or services that rely on AI systems?

As stated in the Consultation Paper, registrants remain accountable for outsourced functions involving AI systems, requiring proper due diligence, ongoing supervision, and specialized skills. However, after analyzing the unique challenges presented by AI technologies, the PCMA believes targeted enhancements to the existing regulatory framework would be more beneficial than creating an entirely new regulatory regime. These enhancements should include a principles based oversight framework that scales requirements according to the AI system's potential impact, due diligence standards specifically addressing AI risks such as explainability and bias detection, and minimum transparency requirements for third-party providers to facilitate proper risk assessment by market participants.

Furthermore, the PCMA recommends the development of CSA guidance on essential contractual provisions for agreements with AI service providers. While supporting these targeted enhancements, the PCMA cautions against duplicative regulation that overlaps with existing frameworks, overly prescriptive rules could impede innovation and disadvantage Canadian market participants globally, and requirements might disproportionately burden smaller firms with limited resources.

While maintaining the principle that registrants ultimately remain accountable for outsourced functions, the PCMA believes there is merit in exploring circumstances where third-party providers may also bear direct regulatory responsibility, particularly when their AI systems are systemically important to capital markets. This approach would acknowledge the reality that risks can originate outside the regulated financial sector yet significantly impact market integrity and investor protection. Please see earlier comments regarding "***Concerns with Uncooperative Third-Party AI Vendors*".**

(b) Once such a third-party product or service is in use by a market participant, should the third-party provider be subject to requirements, and if so, based on what factors?

The PCMA recognizes that as AI adoption increases across capital markets, the regulatory framework must evolve to address emerging risks while enabling innovation. The PCMA believes that third-party AI providers should be subject to certain requirements, but these should be calibrated based on several key factors to ensure proportionality and effectiveness. These include the following:

- *Materiality and Impact Assessment* - The PCMA strongly supports using a materiality framework as the primary determinant for regulation. Third-party AI providers whose services directly impact critical functions such as investment decisions or client suitability determinations should face more stringent requirements than those providing auxiliary services with limited impact on investor outcomes or market integrity. This tiered approach would focus regulatory resources where they can provide the greatest protection while preventing unnecessary barriers to innovation in less critical applications.

- *Systemic Risk Considerations* - When a single AI provider or technology platform serves numerous market participants, risks emerge that could amplify market-wide vulnerabilities. The PCMA recommends that providers whose services are widely adopted across the industry should face enhanced oversight proportional to their potential systemic impact. This is particularly important where AI systems might create correlated behaviors or vulnerabilities across multiple market participants simultaneously.

- *Transparency and Explainability Standards* - The PCMA believes that requirements for third-party providers should include minimum standards for transparency and explainability tailored to the complexity and purpose of the AI system. While market participants retain ultimate responsibility for their regulatory obligations, they cannot effectively discharge these responsibilities without sufficient understanding of the AI systems they employ. The PCMA recommends a principles-based approach that requires providers to enable appropriate explainability without mandating specific technical approaches that might quickly become obsolete as technology evolves.

- *Data Governance Framework* - Given that AI systems fundamentally depend on data quality, the PCMA support requirements for third-party providers to maintain robust data governance practices, particularly when handling sensitive client information. This should include standards for data security, quality control, and appropriate limitations on data usage. These requirements should align with existing privacy regulations while addressing the unique challenges AI systems present for data governance.

- *Conflict Management Protocols* - Where AI systems might create or obscure conflicts of interest, providers should be required to implement conflict management protocols and provide sufficient transparency for market participants to identify and address potential conflicts. This is especially relevant for providers who serve multiple functions in the market or whose business models might create incentives that conflict with client interests.

- *Operational Resilience Requirements* - For providers of critical AI services, operational resilience requirements should address business continuity, disaster recovery, and cybersecurity. The level of requirements should reflect the potential market impact that could result from service interruptions. These standards should complement but not duplicate existing operational resilience frameworks applicable to market participants.

- *Contractual and Access Standards* – Market participants, including EMDs, often face challenges in negotiating appropriate contractual terms with technology providers. The PCMA recommends that the CSA establishing minimum standards for information access, audit rights, and termination provisions that would enable market participants to fulfill their oversight

responsibilities. These standards should ensure that market participants can obtain the information necessary to validate AI systems and demonstrate compliance to regulators without compromising the providers' legitimate intellectual property interests.

- *Balance of Responsibilities* - While the PCMA supports appropriate oversight of third-party AI providers, the PCMA acknowledges that market participants must retain ultimate responsibility for their regulatory obligations. Any requirements imposed on providers should complement rather than replace the obligations of regulated entities. Clear delineation of responsibilities between market participants and their technology providers would enhance accountability without creating regulatory gaps or overlaps.

The PCMA supports a measured approach to the regulation of third-party AI providers based on materiality, potential systemic impact, and the critical nature of the services provided. This approach would foster innovation while ensuring appropriate safeguards for investors and markets.

10. Does the increased use of AI systems in capital markets exacerbate existing vulnerabilities/systemic risks or create new ones? If so, please outline them. Are market participants adopting specific measures to mitigate against systemic risks? Should there be new or amended rules to account for these systemic risks? If so, please provide details.

Examples of systemic risks could include the following:

- **AI systems working in a coordinated fashion to bring about a desired outcome, such as creating periods of market volatility in order to maximize profits;**
- **Widespread use of AI systems relying on the same, or limited numbers of, vendors to function (e.g., cloud or data providers), which could lead to financial stability risks resulting from a significant error or a failure with one large vendor;**
- **A herding effect where there is broad adoption of a single AI system or where several AI systems make similar investment or trading decisions, intentionally or unintentionally, due, for example, to similar design and data sources. This could lead to magnified market moves, including detrimental ones if a flawed AI system is widely used or is used by a sizable market participant;**
- **Widespread systemic biases in outputs of AI systems that affect efficient functioning and fairness of capital markets.**

(a) Does the increased use of AI systems in capital markets exacerbate existing vulnerabilities/systemic risks or create new ones? If so, please outline them.

The PCMA recognizes that the expanding use of AI in capital markets heightens existing vulnerabilities and creates novel systemic risks requiring thorough evaluation. Below are several key risk categories that should be considered by the CSA.

- *Concentration and Single Points of Failure* - The capital markets ecosystem increasingly relies on a limited number of critical AI infrastructure providers, creating unprecedented risk. Unlike traditional financial concerns, these risks extend beyond individual institutions to include: (i) reliance on common cloud service providers to host multiple market participants' AI infrastructure; (ii) dependence on a small number of specialized data providers whose inputs become critical to multiple AI models; and (iii) common usage of foundation models and similar training methodologies may produce correlated behaviors across seemingly independent

systems. This technological concentration creates vulnerabilities where a single technical failure, security breach, or design flaw could simultaneously impact multiple market participants, potentially triggering cascading disruptions across interconnected markets.

- *Model Risk and Convergence* - AI systems in finance demonstrate a tendency toward model convergence despite apparent differences in design. This occurs through several mechanisms: (i) common training data sources leading to similar pattern recognition; (ii) industry adoption of similar methodologies and benchmarks; (iii) increasing use of transfer learning from foundation models; and (iv) competitive pressures that drive systems toward similar optimization goals. This convergence can create systemic blind spots where multiple systems fail to identify the same emerging risks or simultaneously make similar errors in judgment, particularly when faced with novel market conditions outside their training distributions.

- *Governance and Accountability Gaps* - The introduction of increasingly autonomous AI systems creates unique governance challenges. Traditional accountability frameworks assume human oversight at key decision points, but advanced AI systems may operate with degrees of autonomy that challenge these assumptions. This creates potential governance gaps where: (i) responsibility for decisions becomes diffused between system developers, operators, and the AI output (ii) traditional audit trails may not capture the complex, probabilistic reasoning behind AI decisions; (iii) the "black box" nature of some models complicates meaningful human oversight; and (iv) existing compliance frameworks struggle to encompass machine learning systems that constantly evolve their behavior. These governance challenges are particularly acute when systems operate across jurisdictional boundaries or when third-party providers fall outside traditional regulatory perimeters.

- *Cyber-AI Interaction Risks* - The intersection of AI systems and cybersecurity creates novel vulnerabilities. As markets become more dependent on AI for critical functions, they present increasingly attractive targets for sophisticated cyber threats. Particularly concerning are: (i) AI systems themselves becoming targets of adversarial attacks designed to manipulate their behavior; (ii) potential for compromised AI systems to conceal their manipulation by generating plausible-seeming justifications; (iii) the speed and scale at which AI-enabled cyber-attacks could propagate across interconnected systems; and (iv) potential for seemingly isolated incidents to cascade into system-wide disruptions.

Private Capital Market Examples

The private capital market in Canada faces some of the risks described above including the following:

- *Limited Number of Trust Company and Registrar & Transfer Agent Providers* - Many EMDs in Canada rely on a few trust companies that have developed proprietary software. The PCMA has not conducted an investigation into their specific use of AI technologies, however, the PCMA believes automation and AI services have been, or will be, adopted for efficiencies and competitive advantage. If these AI systems were to contain algorithmic biases or experienced a significant failure, multiple EMDs and other users of the systems (*i.e.,* issuers and investors) would simultaneously face regulatory exposure and operational disruptions; and

- *Limited Number of Compliance Service Providers* - The private capital market also faces substantial concentration risk in compliance technology providers. There are few regtech

providers in Canada serving the private capital market. This limited competition stems primarily from two factors: (i) the relatively small market size; and (ii) extreme price sensitivity among market participants. As stated above, compliance provider concentration risk creates and amplifies a single point of failure if compliance AI systems malfunction or are compromised.

Simply, the concentrated nature of service providers in the private capital market means that if an AI system fails, EMDs and issuers using such services have few alternatives to quickly transition. It also means that the impact could be widespread across numerous EMDs simultaneously.

The PCMA finds emerging systemic risks necessitate the development of innovative regulatory approaches to support AI technological advancement, maintain market stability and protect investors. Traditional regulatory frameworks focused on individual institutions must evolve to address risks that emerge from the collective interaction of AI systems across markets. Addressing these challenges requires enhanced collaboration between market participants, technology providers, and the CSA to develop shared standards and monitoring capabilities to keep pace with rapid technological evolution.

(b) Are market participants adopting specific measures to mitigate against systemic risks?

The PCMA understands that AI adoption in the private markets remains at a nascent stage, with EMDs primarily deploying such technologies for internal operational efficiencies rather than client-facing or investment decision-making functions. Notwithstanding this limited implementation, the PCMA has identified potential structural challenges that warrant regulatory attention.

EMDs operating in the private capital market may face substantial constraints in effectively managing AI-related risks. These include: (i) limited technical expertise necessary to evaluate increasingly sophisticated AI-based services; (ii) resource constraints that impede implementation of appropriate risk monitoring systems; and (iii) insufficient testing capabilities to independently validate AI system outputs against regulatory standards. These limitations create a notable asymmetry of knowledge between EMDs and their AI technology providers, resulting in a vulnerability that may impair EMDs' ability to fulfill their regulatory obligations. Most EMDs lack the specialized expertise required to conduct robust due diligence on AI systems, particularly with respect to algorithmic bias, model drift, and explainability factors.

In light of these constraints, the PCMA believes that EMDs would benefit substantially from specific regulatory guidance regarding AI vendor due diligence and contractual governance. Such guidance should address: (i) recommended provisions for service level agreements, including specific performance metrics tailored to AI-based functions; (ii) required vendor obligations regarding notification of material algorithm modifications; (iii) standardized provisions addressing data governance, privacy protections, and limitations on secondary use of client information; and (iv) appropriate allocation of liability for AI-related failures or malfunctions.

The PCMA notes that even with such guidance, EMDs face substantial challenges in negotiating adequate contractual protections with dominant service providers who may leverage their market position to limit their obligations regarding AI systems, particularly in areas of liability, transparency, and explainability.

Where EMDs have implemented AI technologies, the PCMA understands EMDs have generally maintained appropriate human oversight protocols. In many cases, AI serves as a decision-support tool

rather than an autonomous decision-maker, with qualified individuals retaining final determination on matters involving regulatory obligations or material client impacts.

The PCMA welcomes this Consultation Paper as a necessary step toward establishing a coherent regulatory AI framework in the Canadian capital markets. The PCMA notes that the current regulatory uncertainty creates material challenges for EMDs in developing comprehensive risk mitigation strategies. Specifically, EMDs face: (i) ambiguity regarding the scope and nature of their oversight responsibilities for third-party AI systems; (ii) an absence of standardized frameworks for AI risk management appropriate to the private capital market context; and (iii) significant concerns regarding potential liability for AI-related failures despite having limited technical control or visibility into such systems.

Based on the foregoing, the PCMA recommends development of a coordinated regulatory approach that acknowledges the unique constraints of the private capital market while providing appropriate investor protections. This should include: (i) industry-wide standards for AI governance tailored to the scale and resources of EMDs; (ii) enhanced regulatory guidance addressing the specific operational context of EMDs; and (iii) the development of standardized vendor assessment frameworks that EMDs can rely upon when conducting due diligence.

The private capital market's distinctive characteristics, including limited participant resources, high concentration of service providers, and technical capability gaps, necessitate a regulatory approach that balances prudential oversight with practical implementation considerations. The PCMA looks forward to continuing engagement with the CSA on this important initiative.

(c) Should there be new or amended rules to account for these systemic risks? If so, please provide details.

The PCMA believes that thoughtfully calibrated regulatory enhancements are warranted to address the systemic risks associated with AI in the Canadian capital markets, with particular attention to the unique circumstances of the private capital market. The PCMA recommends a principles based framework that balances innovation with prudential oversight, focusing on certain specific regulatory enhancements as discussed below.

The PCMA recommends the CSA develop due diligence guidance for AI vendors serving registrants, including transparency regarding model training, validation methodologies, and ongoing monitoring protocols. In addition, the CSA should establish minimum essential contractual provisions necessary in agreements with critical AI service providers, addressing service levels, access rights, audit capabilities, and incident reporting obligations.

The PCMA supports enhanced governance requirements tailored to the private capital market context including: (i) requirements defining necessary human oversight for AI systems, particularly for critical functions such as KYC verification, suitability determinations, and compliance monitoring; and (ii) the development of guidance for ongoing testing and validation of AI systems used in regulated functions, with documentation requirements proportionate to potential investor impact.

The PCMA recommends regulatory endorsement and support for industry-led initiatives including: (i) establishment of protected information-sharing protocols for AI-related vulnerabilities and incidents, with regulatory safe harbors to encourage participation; (ii) support for development of industry

standards for critical AI applications in the private capital market, potentially through regulatory sandboxes or innovation hubs; and (iii) cooperative initiatives to enhance AI literacy among market participants, particularly EMDs with limited technical resources.

In conclusion, the PCMA submits these targeted regulatory enhancements would substantially mitigate systemic risks associated with AI in the private capital market while maintaining necessary flexibility for innovation. Rather than imposing rigid technical requirements, the PCMA advocate for a principles-based approach that establishes clear expectations while allowing for diverse implementation approaches appropriate to each registrant's scale, complexity, and risk profile.

The PCMA emphasizes that any new requirements should be developed with sensitivity to the resource constraints facing many private market participants, with implementation timelines reflecting the practical challenges of building necessary capabilities. The PCMA welcomes the opportunity to collaborate with the CSA on developing these regulatory enhancements to address systemic risks while supporting the continued evolution of the private capital market.

* * *

The PCMA thanks the CSA for the opportunity to provide you with our comments and would be pleased to discuss them with you further at your convenience.

Yours truly,

PCMA Advocacy Committee Members*

"*Brian Koscak*"
PCMA Chair of Advocacy Committee &
Executive Committee Member

"*David Gilkes*"
PCMA Chair & Executive Committee Member

"*Nadine Milne*"
PCMA Executive Committee Member and
Co-Chair of the Compliance Committee

**The views expressed herein are those of the above individuals in their role as members of the PCMA and not necessarily those of the organizations of which they are employed or affiliated.*

cc: PCMA Board of Directors