Annex A

Consultation Questions for Phase 2

We welcome your comments on the consultation questions for Phase 2 listed below. Please provide your comments in writing on or before January 29, 2027.

Harmonization of current requirements

Question 1:

Should we impose different requirements for different types of entities, or have a single set of requirements that applies to all entities? Please explain.

Question 2:

Should distinct requirements be imposed according to the entity's relative importance or function within the market? Please explain.

Scope of entities

Question 3:

Should Phase 2 include registered entities such as registrant firms and investment fund issuers? Please explain.

Question 4:

Should other types of entities be included in Phase 2 to better align with international standards and facilitate harmonized regulatory treatment across entities? For example:

a) Should Phase 2 include market structure entities other than MIEs, such as benchmark administrators? Please explain.

b) Should regulation services providers or self-regulatory authorities be brought into Phase 2? Please explain.

Question 5:

What factors should be considered in determining whether an entity should be included in Phase 2?

Outsourcing and third-party risks management

Question 6:

Should the outsourcing provisions be extended beyond specified MIEs and apply to all MIEs? Please explain.

Question 7:

Should the outsourcing provisions include more specific obligations for managing risks related to outsourced technologies, such as AI? This could include governance, due diligence, certification, or reporting on the robustness and reliability of an outsourced technology.

Question 8:

In your view, which aspects of outsourcing (increasingly referred to as “third-party risk management”) should be strengthened? Please explain.

In particular, we invite feedback on the following:

- How should risks associated with the use of third-party AI vendors be managed?
- Should there be requirements for independent certifications or attestations regarding the reliability and security of third-party technology solutions?
- How should supply chain risks, including those arising from fourth- and fifth-party service providers, be addressed within the regulatory framework?

Data governance

Question 9:

In your view, how should we address any issues regarding the use of cloud services (e.g. data storage location and concentration risk) by MIEs?

Cybersecurity

Question 10:

Should Phase 2 introduce specific requirements for risk-based cybersecurity controls, including the continuous monitoring and testing of these controls by MIEs (such as penetration testing and vulnerability assessments, and scenario-based cyber resilience exercises), in line with international standards (e.g., ISO/IEC 27001: 2022 standards, NIST Cybersecurity Framework)?

a) What types and frequency of cybersecurity testing should be mandated to ensure ongoing resilience against evolving and emerging threats, including those enabled by new technologies?

b) Should there be specific requirements for independent third-party testing or attestation in connection with cybersecurity, and for reporting material findings to regulators?

Emerging technologies

Question 11:

Should emerging technological developments – such as AI, quantum computing, blockchain and distributed ledger technology (DLT) (e.g. tokenization) be addressed more explicitly? What risks do you see or foresee that could and should be addressed by securities regulation?

Question 12:

Given the increasing use of AI systems in capital markets, should Phase 2 include specific requirements regarding AI risk management consistent with the guidance in CSA Staff Notice and Consultation 11-348 *Applicability of Canadian Securities Laws and the Use of Artificial Intelligence Systems in Capital Markets*?

a) Should there be minimum standards for AI system oversight and transparency regarding AI-driven decision-making?

b) Should there be requirements for documenting and reporting to regulators on AI system uses in connection with a critical system or critical service?

Other

Question 13:

What other issues should we consider in Phase 2? Please explain.