Annex B

Proposed National Instrument 26-101 *Information Technology System Integrity*

PART 1
DEFINITIONS AND INTERPRETATION

Definitions and interpretation

1. **(1)** In this Instrument:

"auxiliary system" means a system, other than a critical system, operated by or on behalf of an MIE that, if breached, poses a security threat to the critical system;

"clearing agency" means a recognized clearing agency;

"critical service" means a service that supports any of the following:

(a) a marketplace's order entry, order routing, execution, trade reporting, trade comparison, data feeds, market surveillance or trade clearing;

(b) a clearing agency's clearing, settlement or depository functions;

(c) a trade repository's collection and maintenance of data, its dissemination of data to a participant or the public or the provision of a trade repository's data to the regulator or the securities regulatory authority under securities legislation;

"critical system" means a system that supports any of the following:

(a) a marketplace's order entry, order routing, execution, trade reporting, trade comparison, data feeds, market surveillance or trade clearing;

(b) a clearing agency's clearing, settlement or depository functions;

(c) a trade repository's collection and maintenance of data, its dissemination of data to a participant or the public or the provision of a trade repository's data to the regulator or the securities regulatory authority under securities legislation;

(d) an information processor's receipt or dissemination of data under National Instrument 21-101 *Marketplace Operation*;

(e) a matching service utility's trade matching function;

“information processor” has the meaning ascribed to it in National Instrument 21-101 *Marketplace Operation;*

“marketplace” has the meaning ascribed to it in National Instrument 21-101 *Marketplace Operation;*

“market surveillance system” means a system, operated by or on behalf of a recognized exchange, a recognized quotation and trade reporting system, or a regulation services provider, that is a critical system and supports real-time market surveillance;

“matching service utility” has the meaning ascribed to it in National Instrument 24-101 *Institutional Trade Matching and Settlement*;

“MIE” means a market infrastructure entity that is a marketplace, a clearing agency, a trade repository, an information processor or a matching service utility;

"participant dealer" has the meaning ascribed to it in National Instrument 23-103 *Electronic Trading and Direct Electronic Access to Marketplaces*;

“regulation services provider” has the meaning ascribed to it in National Instrument 21-101 *Marketplace Operation*;

“specified MIE” means an MIE that is a marketplace, a clearing agency or a trade repository;

“system integrity event” means a failure, malfunction, delay or security incident, each of which is material and related to a critical system;

“trade repository” means

(a) in Alberta, British Columbia, New Brunswick, Québec and Saskatchewan, a recognized trade repository,

(b) in Manitoba and Ontario, a designated trade repository,

(c) in Newfoundland and Labrador, Northwest Territories, Nunavut, Prince Edward Island and Yukon, a recognized quotation and trade reporting system for derivatives, and

(d) in Nova Scotia, a recognized derivatives trade repository.

(2) For the purposes of this Instrument, in Québec, a clearing agency includes a clearing house, a central securities depository and a settlement system recognized under the Quebec *Securities Act* and a clearing house and a settlement system recognized under the Quebec *Derivatives Act*.

PART 2
SYSTEM INTEGRITY REQUIREMENTS

Operational risk management framework

2. **(1)** An MIE must develop, maintain and apply appropriate systems, controls and procedures reasonably designed to identify and minimize the impact of the plausible sources of internal and external operational risk, including, for greater certainty, risks to data integrity, data security, business continuity and capacity and performance management.

(2) An MIE must develop, maintain and apply written policies and procedures that require its board of directors to ensure that the operational risk management framework for each critical system operated by or on behalf of an MIE is reasonably designed to function effectively.

Requirements for critical systems

3. For each critical system operated by or on behalf of an MIE, the MIE must do the following:

(a) develop, maintain, and apply

(i) adequate internal controls,

(ii) adequate information technology general controls, including controls relating to information system operations, information security, change management, problem management, network support and system software support, and

(iii) adequate cyber resilience controls;

(b) on a reasonably frequent basis and, in any event, at least annually

(i) make reasonable current and future capacity estimates, and

(ii) conduct capacity stress tests to determine the processing capability of the critical system to perform in an accurate, timely and efficient manner.

System integrity event

4. **(1)** For each system integrity event, an MIE must promptly notify and provide timely updates to the following:

(a) the regulator or the securities regulatory authority;

(b) if applicable, the MIE's regulation services provider;

(c) if the MIE is an information processor, each recognized exchange or recognized quotation and trade reporting system monitoring trading of the securities about which information is provided to the information processor.

(2) The updates referred to in subsection (1) must address the following:

(a) the status of the system integrity event;

(b) the resumption of service, if applicable;

(c) the status of the review referred to in subsection (3).

(3) The MIE referred to in subsection (1) must conduct an internal review of a system integrity event and provide the regulator or the securities regulatory authority with a written post-incident report setting out the results of the review.

Recordkeeping for system incidents

5. An MIE must keep a record of each failure, malfunction, delay or security incident involving a critical system and identify, in the record, whether or not it is material.

Requirements for auxiliary systems

6. **(1)** For each auxiliary system, an MIE that is a marketplace or a clearing agency must develop, maintain and apply adequate information security controls that address security threats posed by the auxiliary system to any critical system.

(2) The MIE referred to in subsection (1) must keep a record of each security incident involving an auxiliary system and identify, in the record, whether or not the incident is material.

(3) For each security incident referred to in subsection (2) that is material, the MIE must promptly notify and provide timely updates to the following:

(a) the regulator or the securities regulatory authority;

(b) if applicable, the MIE's regulation services provider.

(4) The updates referred to in subsection (3) must address the following:

(a) the status of the security incident;

(b) the resumption of service, if applicable;

(c) the results of any internal review relating to the security incident.

PART 3
PRE-OPERATIONAL REQUIREMENTS - SPECIFIED MIE

Availability of technology requirements and testing facilities

7. **(1)** Before a specified MIE begins operations, it must make the following available:

(a) all technology requirements, in their final form, regarding interfacing with or accessing it;

(b) testing facilities for interfacing with or accessing it.

(2) If the specified MIE is a marketplace or a trade repository, the technology requirements must be made available to the public.

(3) If the specified MIE is a clearing agency, the technology requirements must be made available to the clearing agency's participants.

Time period for availability - marketplace

8. If the specified MIE is a marketplace

(a) the technology requirements referred to in paragraph 7(1)(a) must be made available for at least 3 months immediately before it begins operations, and

(b) the testing facilities referred to in paragraph 7(1)(b) must be made available for at least 2 months immediately before it begins operations.

Time period for availability – clearing agency and trade repository

9. If the specified MIE is a clearing agency or a trade repository, the technology requirements and testing facilities referred to in subsection 7(1) must be made available sufficiently in advance of the specified MIE beginning operations to allow for a reasonable period for testing and system modification by its participants.

Confirmation and certification

10. If the specified MIE is a marketplace, it must not begin operations unless, if applicable, its regulation services provider has confirmed to the marketplace that trading may commence on the marketplace.

11. If the specified MIE is a marketplace or clearing agency, it must not begin operations unless its chief information officer, or an individual performing a similar function, has certified in writing to the regulator or the securities regulatory authority that all information technology systems used by the specified MIE have been tested according to prudent business practices and are operating as designed.

PART 4
MATERIAL CHANGES TO A CRITICAL SYSTEM - SPECIFIED MIE

Availability of technology requirements and testing facilities

12. (1) A specified MIE that has begun operations must not implement a material change to a critical system before it makes each of the following available:

(a) all technology requirements, in their final form, regarding interfacing with or accessing it;

(b) testing facilities for interfacing with or accessing it.

(2) If the specified MIE is a marketplace or a trade repository, the technology requirements must be made available to the public.

(3) If the specified MIE is a clearing agency, the technology requirements must be made available to the clearing agency's participants.

Time period for availability – marketplace

13. If the specified MIE is a marketplace

(a) the technology requirements referred to in paragraph 12(1)(a) must be made available at least 3 months before the date that it implements a material change to a critical system, and

(b) the testing facilities referred to in paragraph 12(1)(b) must be made available at least 2 months before the date that it implements a material change to a critical system.

Time period for availability – clearing agency and trade repository

14. If the specified MIE is a clearing agency or a trade repository, the technology requirements and testing facilities referred to in subsection 12(1) must be made available sufficiently in advance of implementing a material change to a critical system to allow for a reasonable period for testing and system modification by the specified MIE's participants.

Compliance and certification

15. **(1)** A specified MIE must not implement a material change to a critical system unless its chief information officer, or an individual performing a similar function, has certified in writing to the regulator or the securities regulatory authority that the change has been tested according to prudent business practices and is operating as designed.

(2) Subsection (1) does not apply to a trade repository.

Emergency exception

16. **(1)** Sections 13, 14 and 15 do not apply if

(a) the change must be made immediately to address a failure, malfunction or material delay of the specified MIE's critical systems or equipment,

(b) the specified MIE immediately notifies the following of its intention to make the change

(i) the regulator or the securities regulatory authority,

(ii) if applicable, its regulation services provider, and

(c) the specified MIE makes the revised technology requirements available as soon as practicable.

(2) If the specified MIE is a marketplace or a trade repository, the revised technology requirements referred to in paragraph (1)(c) must be made available to the public.

(3) If the specified MIE is a clearing agency, the revised technology requirements referred to in paragraph (1)(c) must be made available to its participants.

Uniform test symbols

17. A specified MIE that is a marketplace must use uniform test symbols, as set by the regulator or the securities regulatory authority, for the purpose of performing testing in the marketplace's production environment.

PART 5
BUSINESS CONTINUITY

Business continuity planning

18. (1) An MIE must develop, maintain and apply reasonable business continuity plans, including disaster recovery plans designed to

(a) achieve prompt recovery of its operations following a disruption, and

(b) allow for the timely recovery of information following the disruption.

(2) An MIE must test its business continuity plans, including its disaster recovery plans, on a reasonably frequent basis and, in any event, at least annually.

Resumption of operations

19. (1) An MIE listed below must develop, maintain and apply written policies and procedures reasonably designed to ensure that its critical systems can resume operations within the following specified timeframes:

(a) if the MIE is an information processor, within one hour of its declaration of a disaster;

(b) if the MIE is a marketplace with a total dollar value of the trading volume in any type of security equal to or greater than 10% of the total dollar value of the trading volume in that type of security on all marketplaces in Canada during at least 2 of the preceding 3 months of operation, within 2 hours of its declaration of a disaster;

(c) if the MIE is a trade repository or a clearing agency, within 2 hours of a disruptive event.

(2) Each of the following must develop, maintain and apply written policies and procedures reasonably designed to ensure that its market surveillance systems can resume operations within the following specified timeframes:

(a) a recognized exchange or quotation and trade reporting system that directly monitors the conduct of its members or users and enforces the requirements set out under subsection 7.1(1) or 7.3(1) of National Instrument 23-101 *Trading Rules*, within 2 hours of its declaration of a disaster;

(b) a regulation services provider that has entered into a written agreement with a marketplace to conduct market surveillance for the marketplace, within 2 hours of its declaration of a disaster.

Industry-wide business continuity tests

20. Each of the following must participate in all industry-wide business continuity tests, as determined or conducted by a regulation services provider, the regulator or the securities regulatory authority:

(a) a participant dealer,

(b) an MIE that is any of the following:

(i) a marketplace;

(ii) a clearing agency;

(iii) an information processor.

PART 6
OUTSOURCING

Outsourcing

21. If a specified MIE outsources a critical service or critical system to a service provider, including, for greater certainty, a service provider that is an affiliate or an associate of the specified MIE, the specified MIE must

(a) develop, maintain and apply written policies and procedures to conduct suitable due diligence in the selection of service providers and for the evaluation and approval of those outsourcing arrangements,

(b) identify any conflicts of interest between the specified MIE and the service provider and develop, maintain and apply written policies and procedures to mitigate and manage those conflicts of interest,

(c) enter into a written contract with the service provider that

(i) is appropriate for the materiality and nature of the outsourced activities,

(ii) includes service level provisions, and

(iii) provides for adequate termination procedures,

(d) maintain access to the books and records of the service provider relating to the outsourced activities,

(e) ensure that the regulator or the securities regulatory authority has the same access to all data, information and systems maintained by the service provider on behalf of the specified MIE that the regulator or securities regulatory authority would have access to absent the outsourcing arrangements,

(f) take appropriate measures to ensure that the service provider develops, maintains, and periodically tests an appropriate business continuity plan, including a disaster recovery plan,

(g) ensure that each person or company conducting an audit or an independent review of the specified MIE under this Instrument has appropriate access to all data, information and systems maintained by the service provider on behalf of the MIE that the person or company would have access to absent the outsourcing arrangements,

(h) take appropriate measures to ensure that the service provider protects the proprietary and confidential information of the specified MIE, and, if applicable, its participants, including taking measures to protect information from loss, thefts, vulnerabilities, threats, unauthorized access, copying, use and modification,

(i) take appropriate measures to ensure that the service provider does not disclose the proprietary and confidential information referred to in paragraph (h) unless legislation or an order of a court or tribunal of competent jurisdiction requires the disclosure, and

(j) develop, maintain and apply written policies and procedures to regularly review and monitor the performance of the service provider's obligations under the outsourcing arrangement.

PART 7
VULNERABILITY ASSESSMENTS AND SYSTEM REVIEWS

Vulnerability assessments

22. On a reasonably frequent basis and, in any event, at least annually, an MIE other than a trade repository must engage a qualified person or company to perform appropriate assessments and testing to identify security vulnerabilities and measure the effectiveness of information security controls that assess the MIE's compliance with paragraph 3(a) and, if applicable, subsection 6(1).

System reviews

23. (1) On a reasonably frequent basis and, in any event, at least annually, an MIE must engage a qualified auditor to conduct an independent system review and prepare a report in accordance with established audit standards and best industry practices that assesses the MIE's compliance with the following:

(a) paragraph 3(a) and section 18;

(b) if the MIE is a trade repository, paragraph 3(b);

(c) if the MIE is a marketplace or a clearing agency, subsection 6(1).

(2) If the MIE referred to in subsection (1) is a marketplace, a clearing agency or an information processor, the qualified auditor referred to in subsection (1) must be an external auditor.

(3) An MIE must provide the report referred to in subsection (1)

(a) to the board of directors or audit committee of the MIE, promptly after the report's completion, and

(b) to the regulator or the securities regulatory authority, not later than 60 days after the report's completion.

PART 8
BOOKS AND RECORDS

Books and records

24. **(1)** An MIE must keep books, records and other documents as are reasonably necessary to record its activities, business transactions and financial affairs related to the following:

(a) its critical systems;

(b) if the MIE is a specified MIE, its critical services;

(c) if the MIE is a marketplace or a clearing agency, its auxiliary systems.

(2) An MIE must retain the books, records and other documents referred to in subsection (1)

(a) in a safe location and a durable form,

(b) in a manner that permits them to be provided promptly to the regulator or the securities regulatory authority, and

(c) if the MIE is a marketplace or a clearing agency, for a period of at least 7 years from the date the books, records and other documents were created or received, whichever is later.

PART 9
EXEMPTION AND EFFECTIVE DATE

Exemption

25. **(1)** The regulator or the securities regulatory authority may grant an exemption from this Instrument, in whole or in part, subject to such conditions or restrictions as may be imposed in the exemption.

(2) Despite subsection (1), in Ontario, only the regulator may grant such an exemption.

(3) Except in Alberta and Ontario, an exemption referred to in subsection (1) is granted under the statute referred to in Appendix B of National Instrument 14-101 *Definitions* opposite the name of the local jurisdiction.

Effective date

26. (1) This Instrument comes into force on [•], 2027.

(2) In Saskatchewan, despite subsection (1), if these regulations are filed with the registrar of regulations after [insert date], these regulations come into force on the day on which they are filed with the registrar of regulations.