Canadian Securities Administrators | Autorités canadiennes en valeurs mobilières

# CSA Notice and Request for Comment

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

# Proposed Companion Policy 26-101 *Information Technology System Integrity*

**October 1, 2026**

## Introduction

The Canadian Securities Administrators (the **CSA** or **we**) are publishing the following for a 120-day comment period:

- Proposed National Instrument 26-101 *Information Technology System Integrity* (the **Proposed Instrument**),
- Proposed Companion Policy 26-101 *Information Technology System Integrity* (the **Proposed Companion Policy**),
- Proposed consequential amending instruments to the Source Rules (as defined hereinafter) (the **Proposed Amending Instruments**),
- Proposed consequential changes to companion policies to the Source Rules (the **Proposed Changes to Companion Policies**), and
- Proposed additional amendments to National Instrument 21-101 *Marketplace Operation* and proposed related changes to its companion policy (the **Proposed Additional Amendments and Changes**[1]).

Together, the Proposed Instrument, the Proposed Companion Policy, the Proposed Amending Instruments, the Proposed Changes to Companion Policies and the Proposed Additional Amendments and Changes are referred to as the **Proposed Materials** in this notice.

[1] These Proposed Additional Amendments and Changes are incorporated into the amending instrument and companion policy changes related to National Instrument 21-101 *Marketplace Operation*.

We are issuing this notice to solicit comments on the Proposed Materials. We welcome all comments on this publication. We have also included specific questions for your consideration in Annex A "Consultation Questions for Phase 2" below. The comment period will end on January 29, 2027.

The text of the Proposed Materials is published with this notice and is also available on the websites of the following CSA jurisdictions:

www.asc.ca
www.bcsc.bc.ca
www.fcaa.gov.sk.ca
www.fcnb.ca
www.lautorite.qc.ca
https://mbsecurities.ca
www.nssc.novascot
ia.ca
www.osc.ca

**Background**

Information technology (**IT**) plays a significant role in supporting Canadian financial markets. IT has enabled a substantial increase in the speed of transaction execution, provided greater market access to a broad range of market participants, and enhanced the efficiency and sophistication of trading and related functions.

Specifically, IT systems allow market infrastructure entities to facilitate, among other things, order entry and routing, trade execution, clearing and settlement of transactions, trade reporting, public dissemination of data, and market surveillance. At the same time, the rapid pace of change in IT and the consequent advent of new technologies may lead to increased risks for all of these operational functions essential to financial markets. These risks will evolve, and some will likely increase as new technologies play a larger role in our capital markets.

By providing a robust regulatory framework, we aim to preserve the stability, efficiency and integrity of Canadian financial markets. This will help avoid the financial losses, erosion of market confidence, and potential market instability that could arise from the disruption of market infrastructure entities' IT systems.

The Proposed Instrument consolidates the current IT-related requirements for various types of market infrastructure entities into a single rule, harmonizes similar wording and provisions, and introduces a few additional obligations for greater consistency across these entities. In our view, these additions do not constitute major changes.

Currently, the following market infrastructure entities are subject to a regulatory framework that includes IT system requirements:

- marketplaces;[2]
- information processors;
- recognized clearing agencies;
- matching service utilities;
- trade repositories.[3]

These entities are collectively referred to as **MIE**(**s**) in this notice.

This initiative is designed to establish the foundation for a comprehensive and harmonized framework for IT-related system requirements and oversight of such systems in Canada, through the creation of a single national instrument applicable to all MIEs (**Phase 1**).

Similar approaches have been adopted and implemented by international regulators, such as the U.S. Securities and Exchange Commission[4] and the European Securities and Markets Authority.[5] The Proposed Materials represent an initial step toward greater regulatory alignment between Canadian securities legislation and that of other jurisdictions.

**Substance and Purpose**

We are creating the Proposed Instrument for two reasons:

*(1) Consolidation and harmonization of existing IT-related system requirements*

MIEs are already subject to IT system requirements and oversight provisions, which are currently spread across the following instruments and rules:

- National Instrument 21-101 *Marketplace Operation* (**NI 21-101**)
- National Instrument 24-101 *Institutional Trade Matching and Settlement* (**NI 24-101**)
- National Instrument 24-102 *Clearing Agency Requirements* (**NI 24-102**)
- Manitoba Securities Commission Rule 91-507 Derivatives: Trade Reporting
- Ontario Securities Commission Rule 91-507 Derivatives: Trade Reporting
- *Regulation 91-507 respecting Trade Repositories and Derivatives Data Reporting* (Québec)

[2] Many foreign exchanges and alternative trading systems, including crypto trading platforms, are exempt from IT-related requirements through exemptive relief orders issued by CSA members.
[3] As defined in the Proposed Instrument, "trade repository" means: in Alberta, British Columbia, New Brunswick, Québec and Saskatchewan, a recognized trade repository; in Manitoba and Ontario, a designated trade repository; in Newfoundland and Labrador, Northwest Territories, Nunavut, Prince Edward Island and Yukon, a recognized quotation and trade reporting system for derivatives; and in Nova Scotia, a recognized derivatives trade repository.
[4] See *Regulation Systems Compliance and Integrity* at https://www.federalregister.gov/documents/2014/12/05/2014-27767/regulation-systems-compliance-and-integrity
[5] See Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 at https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

- Multilateral Instrument 96-101 *Derivatives: Trade Reporting*

These instruments are collectively referred to as the **Source Rules** in this notice.

Having IT system requirements spread across the Source Rules may present inefficiencies and challenges for MIEs. This fragmentation makes it more difficult to ensure consistent implementation of similar policy objectives and can result in outdated provisions that no longer reflect current international standards and industry practices. Consistently updating the various Source Rules can be also challenging, particularly when addressing emerging risks and concerns associated with the rapid pace of development of IT and the emergence of new technologies. Since amendments to system requirements have been introduced at different times across the Source Rules, some inconsistencies in language and interpretation have emerged. Streamlining these requirements is necessary to enhance regulatory coherence and to support more efficient compliance by MIEs.

This initiative aims to eliminate drafting and interpretation inconsistencies across the Source Rules. Having all IT system requirements consolidated into a single national instrument will provide MIEs with clearer and more consistent requirements. That said, we acknowledge that applying uniform IT-related requirements to all MIEs may not be appropriate in all circumstances, particularly when the differences across those requirements are substantive. We have also considered the distinct roles MIEs play within financial markets, in addition to international standards that may reflect these distinct roles. These include the 2012 *Principles for financial market infrastructures* published by the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions (**PFMIs**). As a result, harmonization would only occur where appropriate.

If adopted, the Proposed Instrument will establish a foundation from which the CSA can continue to effectively modernize IT system requirements, and that will allow us to better optimize regulatory approaches to the oversight of MIEs. The CSA will be able to respond more efficiently to future developments by eliminating the current difficulties associated with amending different Source Rules at different times. Furthermore, the Proposed Instrument will increase the clarity and efficiency of IT-related requirements applicable to MIEs by eliminating drafting discrepancies across the Source Rules. Given the role that MIEs' IT systems play in preserving the integrity and stability of Canadian financial markets, we are of the view that it is appropriate to consolidate the IT-related system requirements in the Source Rules into one new national instrument.

(2) *A foundation for future modernization*

Once the Proposed Instrument comes into effect, we plan to modernize it to better align current IT system requirements with international standards (**Phase 2**). Existing IT system requirements do not completely capture international standards and current best industry practices. We expect Phase 2 to allow the CSA to better address risks associated with, notably:

- third-party risk management;

- concentration risks;
- artificial intelligence;
- tokenization;
- quantum computers; and
- crypto assets.

Phase 2 will also enable the CSA to:

- further harmonize the existing IT system requirements across all MIEs, as appropriate;
- potentially expand the scope of the requirements to include additional market participants; and
- harmonize with international regulations and further align with relevant international standards and guidance.

We believe that implementing the Proposed Instrument will provide an effective foundation for the achievement of the Phase 2 objectives outlined above. While our immediate focus remains on Phase 1, we have included a series of consultation questions below relating to Phase 2. Your responses will guide our work to prepare for the next phase, ensuring that input from market participants is considered at the earliest stages of the initiative. These questions are intended to elicit thoughtful feedback and support a collaborative approach to advancing Phase 2, which will facilitate the implementation of an appropriate revised framework.

**Proposed Amending Instruments and Proposed Changes to Companion Policies**

To support the creation of a new national instrument, we would repeal the existing IT-related requirements from the Source Rules. We would also update the forms and companion policies associated with the Source Rules by adding cross-references to the Proposed Instrument. Additionally, to maintain the status quo regarding outsourcing provisions, we would incorporate cross-references to the Proposed Instrument within the applicable Source Rules as appropriate.

**Proposed Additional Amendments and Changes**

The Proposed Additional Amendments and Changes are comprised of the following amendments to NI 21-101 and its related Forms, and Companion Policy 21-101 *Marketplace Operation* (**21-101CP**). These amendments would not create any new regulatory requirements and, in some cases, would reduce regulatory burden:

- Section 6.7 of NI 21-101 requires an alternative trading system (**ATS**) to notify the regulator or the securities regulatory authority if at least one of three thresholds is met or exceeded, which may indicate that an ATS has significant market share in a type of security and that it would be more appropriate for the ATS to be regulated as an exchange. Currently, 21-101CP clarifies that “a type of security” is considered to refer to a distinctive category of security such as equity securities, debt securities or options. We propose to remove the requirement in section 6.7 because: (i) for equity securities, notification is not

needed since the regulator or the securities regulatory authority can use market share information readily available from the Canadian Investment Regulatory Organization (CIRO); and (ii) for debt securities, ATSs are not able to accurately calculate the notification thresholds since the debt market is not centralized and debt is mostly traded over-the-counter. The corresponding guidance in 21-101CP would be slightly modified and moved to another section which outlines the criteria used by the regulator or the securities regulatory authority to consider whether a marketplace is an exchange for purposes of Canadian securities legislation.

- We propose to add guidance to 21-101CP setting out conditions under which the regulator or the securities regulatory authority would consider granting exemptive relief to a marketplace from pre-trade transparency requirements for the display of dark orders.[6]

- In both Form 21-101F1 *Information Statement Exchange or Quotation and Trade Reporting System* and Form 21-101F2 *Information Statement Alternative Trading System* (**Form 21-101F2**), we propose to remove the requirement in item 1 of paragraph 2(ii) of Exhibit D. The item, requiring a marketplace to provide the address of all affiliates (i) to which it has outsourced key services or systems or (ii) with which it has a material business relationship, is duplicative as marketplaces are already required to provide the address of any affiliates in Exhibit D, section 1.

- In Form 21-101F4 *Cessation of Operations Report for Alternative Trading System*, we propose to remove Exhibit B, which requires an ATS ceasing operations to list each of the securities that it trades. The requirement is now viewed as being impracticable, as most ATSs would have to list hundreds of securities, and duplicative, as Exhibit I in Form 21-101F2 already requires disclosure of the types of securities traded on the ATS.

**Summary of the Proposed Instrument**

With the creation of the Proposed Instrument, we aim to consolidate and harmonize existing IT system requirements currently spread across the various Source Rules. We do not intend to introduce significant new requirements in Phase 1. However, we have proposed relatively minor changes to improve clarity, ensure greater consistency, and harmonize similar requirements and guidance in the Source Rules and associated companion policies. We do not expect these changes to have a significant impact on the MIEs. We have also revised the structure and location of certain provisions within the Proposed Instrument to improve readability and coherence. For example, the vulnerability assessments and system review provisions were moved closer to the end of the Proposed Instrument, compared to their location in the Source Rules. These adjustments would not change the nature or substance of the obligations. We have set out below a summary of the proposed modifications to existing IT system requirements.

[6] The proposed guidance reflects conditions in recent decisions granting exemptive relief from the pre-trade transparency requirements in subsection 7.1(1) of NI 21-101.

***Incorporation of New Definitions***

To promote harmonization and enhance clarity, we have incorporated new definitions into the Proposed Instrument. These definitions are taken from requirements in the Source Rules and consequently are not intended to introduce new concepts.

The new terms in the Definitions section include:

*(1) "critical system"*

We define this term as including the essential functions of each MIE (even if those functions are outsourced). For example, the functions include order entry, routing and execution for marketplaces; clearing, settlement and depository functions for recognized clearing agencies; and trade-matching functions for matching service utilities.

While the Source Rules use various terms to describe the systems relating to an MIE's essential functions, we consider the term "critical" to be more appropriate as it aligns with the terminology used in the PFMIs. In our view the change in language will not narrow the scope of the related requirements applicable to marketplaces, information processors, matching services utilities or trade repositories.

*(2) "critical service"*

Similar to "critical system", we define "critical service" in connection with an entity's essential functions. In this case, however, the term applies only to a subset of MIEs in the context of outsourcing: marketplaces, recognized clearing agencies and trade repositories (see "specified MIE" below).

*(3) " MIE"*

An MIE includes all market infrastructure entities that are subject to the Proposed Instrument – marketplaces, information processors, recognized clearing agencies, matching service utilities and trade repositories.

It is not our intention for the Proposed Instrument to apply to marketplaces (exchanges or ATSs, including crypto asset trading platforms) that have been exempted from the existing IT systems requirements in NI 21-101.

*(4) "market surveillance system"*

While this is a new definition, it was drawn from subsection 12.4(3) of NI 21-101, describing critical systems operated by or on behalf of regulation services providers or certain types of marketplaces that support real-time market surveillance.

*(5) "system integrity event"*

The definition of a system integrity event is based on language in the Source Rules and refers to material malfunctions, failures, delays and security incidents in critical systems. An MIE that experiences a system integrity event must report it to the regulator or the securities regulatory authority.

*(6) "specified MIE"*

A specified MIE means a market infrastructure entity that is a marketplace, a recognized clearing agency, or a trade repository. These entities are subject to more comprehensive IT system requirements[7] than other MIEs.

***System Integrity Requirements for MIEs***

The Proposed Instrument would establish a regulatory framework for critical and auxiliary systems that closely mirrors the existing provisions in the Source Rules. As is currently the case, the critical system requirements would apply to all MIEs, while the auxiliary system requirements would apply only to marketplaces and recognized clearing agencies.

To promote consistency in IT-related requirements across all MIEs, the Proposed Instrument introduces three minor changes:

- MIEs must develop, maintain and apply systems, controls and procedures that are reasonably designed to identify and mitigate plausible sources of operational risk, including risk to data integrity and data security. This requirement complements the existing provisions under the Source Rules and provides additional specificity to support effective risk management.

- MIEs must ensure that the operational risk management framework for critical systems is reasonably designed to function effectively. The board must be actively involved in and informed about the MIE's critical system controls and procedures.

- Trade repositories and matching service utilities would be required to provide timely updates to the regulator or the securities regulatory authority when a system integrity event occurs.

These three changes are not intended to impose any significant additional burden on MIEs, but rather to enhance clarity and align existing requirements. The first two provisions described above are based on requirements in local and multilateral trade reporting rules, as well as the PFMIs, and would apply to all MIEs going forward. The third change would extend to matching service utilities and trade repositories an important, but not unduly burdensome, requirement to update regulators if those entities experience a system integrity event. This requirement currently applies to marketplaces, information processors and recognized clearing agencies.

[7] Requirements relating to pre-operational and material changes to system and testing requirements as well as outsourcing provisions are located in Part 3, Part 4 and Part 6 of the Proposed Instrument.

***Requirements for Pre-operational and System Changes that are Material***

The Proposed Instrument would make structural changes to the testing provisions in the Source Rules. These changes are intended to provide greater clarity by separating the pre-operational and post-operational testing requirements applicable to specified MIEs and putting them in different Parts of the Instrument. Part 3 of the Proposed Instrument outlines the obligations specified MIEs must fulfill prior to starting operations. Part 4 then sets out the testing and access requirements applicable before a material system change can be made. Apart from these structural and related drafting changes, the requirements would remain unchanged.

***Business Continuity***

In Part 5, we consolidate the requirements related to business continuity and harmonize wording from the Source Rules. The provisions concerning resumption of operations and industry-wide business continuity testing requirements are unchanged, with some minor exceptions. First, a recognized clearing agency or a trade repository would have to develop, maintain, and apply policies and procedures reasonably designed to ensure that its critical system could resume operations within two hours following a disruptive event.

This two-hour recovery timeframe is included in the PFMIs, which are incorporated by reference into NI 24-102 and are therefore already a legal requirement for a recognized clearing agency under Canadian securities legislation. For a trade repository, the recovery timeframe is currently set out in the companion policy to the applicable Source Rule and would be incorporated directly into the Proposed Instrument in order to consolidate the location of this timeframe for all MIEs. It is important to note that this requirement pertains to the existence of policies and procedures that support recovery within the specified timeframe, rather than imposing a strict obligation to resume operations within two hours.

In addition, we would extend the requirement to test an MIE's business continuity plan (including its disaster recovery plan) to matching service utilities. This testing requirement currently applies to all the other MIEs. In our view, this change should not impose any new operational requirements on matching service utilities, as we would not consider a business continuity requirement to be effective if it was not tested on a regular basis.

Similarly, we would remove a requirement, currently applicable only to trade repositories, that a business continuity plan must provide for the appropriate exercise of authority. In our view it is not necessary to make this requirement explicit, as a business continuity plan that did not provide for the authority to implement the plan, or that did not clearly assign roles for carrying it out, would be ineffective and therefore not compliant with the requirements of Part 5 of the Proposed Instrument.

***Outsourcing***

The Proposed Instrument would incorporate and harmonize the outsourcing provisions taken from the Source Rules, which are close to but not entirely identical. While the Proposed Instrument defines the terms "critical service" and "critical system" for the entities that are subject to these requirements, it is not our intent to reduce the scope of the current outsourcing provisions to cover only IT-related services or systems. For this reason, we added cross-references to the Proposed Instrument's outsourcing requirements into the amended Source Rules, as appropriate. Given that the definitions of critical system and critical service would only apply in the Proposed Instrument, other key outsourcing services or systems[8] would continue to be covered in the Source Rules as is the case today. The replacement of the outsourcing provisions in the Source Rules with the cross-references to the Proposed Instrument is intended to facilitate harmonization and avoid the need to amend multiple instruments going forward.

As a consequential amendment arising from this approach, in order to avoid confusion between the cross-reference incorporated in NI 24-102 and the outsourcing provisions set out in the Proposed Instrument, we would replace the term "critical service or system" currently used for recognized clearing agencies with "key service or system".

***Vulnerability Assessments and System Reviews***

Part 7 of the Proposed Instrument reorganizes the IT system requirements related to vulnerability testing and system reviews. While the substance of these requirements remains consistent with the Source Rules, we are proposing two updates:

- Matching service utilities would be required to undergo a vulnerability assessment conducted by a qualified party at least annually. It is important to note that this requirement is already included in existing recognition orders[9] issued by members of the CSA and therefore in practice would not create a new obligation.

- MIEs would have to submit the report resulting from their annual independent system reviews (frequently referred to as "ISRs") no later than the 60th day following the report's completion. In the Source Rules the deadline for submitting this report is not consistent. In our view this is an appropriate provision to harmonize in Phase 1.

***Books and Records***

The Proposed Instrument sets out standard books and records provisions currently applicable to all MIEs. The scope of these requirements captures the critical systems of MIEs, the critical services of specified MIEs, and, in the case of marketplaces or recognized clearing agencies, their auxiliary systems. We note that in the Source Rules, some entities do not have a specified retention period for books and records. We considered whether or not a harmonized, specific

[8] Critical system and critical service are a subset of key systems and services, which also include services and systems that are necessary for a specified MIE to operate effectively and in compliance with regulatory requirements and appropriate standards.
[9] See Décision N° 2018-PDG-0079 issued by Autorité des marchés financiers, available at https://lautorite.qc.ca/fileadmin/lautorite/professionnels/structures-marche/services-appariement/decision_reconnaissance_dtcc_itp.pdf

retention period should apply to all MIEs but determined that this could amount to a significant change and impose additional costs. We plan to consider this question further in Phase 2.

**Alternatives Considered to the Proposed Instrument**

The alternative to the Proposed Materials would be not to proceed with the creation of the Proposed Instrument. However, in our view, not proceeding with the consolidation and harmonization of the existing IT system requirements applicable to MIEs would fail to address the risks inherent in the current regulatory framework, where the requirements are spread across multiple Source Rules, making it difficult to harmonize and effectively respond to emerging developments. This aggravates the risk of technological vulnerabilities in an environment where there is rapid adoption of new technologies which were not considered when the Source Rules were created and amended. Moreover, we are considering a larger-scale modernization of the systems and outsourcing regulatory framework applicable to MIEs in Phase 2. The creation of a new foundation with the Proposed Instrument is the precursor to this initiative.

**Unpublished Materials**

In developing the Proposed Materials we have not relied on any significant unpublished study, report or other written materials.

**Local Matters**

An Annex G is being published in any local jurisdiction that is making related changes to local securities laws, including local notices or other policy instruments in that jurisdiction. It also includes any additional information that is relevant to that jurisdiction only.

**List of Annexes**

This notice contains the following annexes:

**Annex A** – Consultation Questions for Phase 2
**Annex B** – Proposed Instrument
**Annex C** – Proposed Companion Policy
**Annex D** – Proposed Amending Instruments
**Annex E** – Proposed Changes to Companion Policies
**Annex F** – Table of Concordance
**Annex G** – Local Matters

**Authority of the Proposed Instrument and Proposed Companion Policy**

The securities legislation in each of the CSA jurisdictions provides the regulator or the securities regulatory authority with rule-making or regulatory authority in respect of the subject matter of the Proposed Instrument.

**How to Provide Comments**

We welcome your comments on the Proposed Materials, and also invite comments on the consultation questions for Phase 2 which can be found in Annex A of this Notice. Please submit your comments on or before January 29, 2027.

Submit your comments here: Consultations Archive - Canadian Securities Administrators. By using the link, your comments will be submitted to the following CSA members:

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

If Québec is a participating jurisdiction, and you are submitting your comments through the link above, you are also submitting your comments to:

M$^{e}$ 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: 514 864-6381
E-mail: consultation-en-cours@lautorite.qc.ca

We cannot keep submissions confidential because securities legislation in certain provinces requires publication of the written comments received during the comment period. Comments received will be posted on the websites of each of the Alberta Securities Commission at www.albertasecurities.com, the Autorité des marchés financiers at www.lautorite.qc.ca and the Ontario Securities Commission at www.osc.ca. You should not include personal information directly in comments as the comments will be published and publicly available. It is important that you state on whose behalf you are making the submission.

**Questions**

Please refer your questions to any of the following CSA staff:

*Alberta Securities Commission*

Julio Arboleda Ramirez
Senior Legal Counsel
Email: julio.arboledaramirez@asc.ca

*Autorité des marchés financiers*

Julie Boyer
Senior Policy Advisor
Email: julie.boyer@lautorite.qc.ca

*BC Securities Commission*

Catherine Tearoe
Senior Legal Counsel
Email: ctearoe@bcsc.bc.ca

*Financial and Consumer Affairs Authority of Saskatchewan*

Curtis Brezinski
Acting Director, Capital Markets, Securities Division
Email: curtis.brezinski@gov.sk.ca

*Financial and Consumer Services Commission of New Brunswick*

Nick Doyle
Legal Counsel
Email: nick.doyle@fcnb.ca

*The Manitoba Securities Commission*

Angela Duong
Deputy Director, Compliance and Oversight
Email: angela.duong@gov.mb.ca

*Nova Scotia Securities Commission*

Doug Harris
General Counsel, Director of Market Regulation and Policy and Secretary
Email: doug.harris@novascotia.ca

*Ontario Securities Commission*

Stacey Barker
Senior Accountant, Trading & Markets
Email: sbarker@osc.ca

Stephanie Wakefield
Senior Legal Counsel, Trading & Markets
Email: swakefield@osc.ca

# 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.

## 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.

# Annex C

## Proposed Companion Policy 26-101
## *Information Technology System Integrity*

### Purpose

National Instrument 26-101 *Information Technology System Integrity* (**NI 26-101**) amalgamates the technology-related requirements that apply to marketplaces, recognized clearing agencies, information processors, trade repositories,[1] and matching service utilities (**market infrastructure entities** or **MIEs**).[2] The relevant provisions were moved from National Instrument 21-101 *Marketplace Operation* (marketplaces and information processors), National Instrument 24-101 *Institutional Trade Matching and Settlement* (matching service utilities), National Instrument 24-102 *Clearing Agency Requirements* (**NI 24-102**), and local and multi-jurisdictional trade reporting rules (together, the **Source Rules**). We have harmonized comparable requirements where appropriate to do so. Some changes were made to existing requirements for the purposes of consistency and harmonization within NI 26-101. We also wished to avoid any interpretational issues that could arise by having separate but very similar requirements for different MIEs.

Marketplaces, recognized clearing agencies and trade repositories are subject to additional requirements relating to system testing and outsourcing. For this reason, these MIEs have been categorized as "**specified MIEs**", with a definition included in Part 1. Recognized clearing agencies should bear in mind that the system-related aspects of the *Principles for Financial Market Infrastructures* (**PFMIs**) that are incorporated by reference into NI 24-102 continue to apply, despite the excision of the specific information technology requirements from NI 24-102.

By grouping together the system-related requirements of the various MIEs subject to our regulatory oversight, going forward the CSA jurisdictions will be better able to modernize and make any necessary changes to these requirements in a consistent and timely way.

### Overview

Part 1 of NI 26-101 sets out its defined terms, many of which are drawn from and cross-reference defined terms in the Source Rules. Part 2 of NI 26-101 includes the system integrity requirements for MIEs' critical and auxiliary systems. Part 3 contains the technology and testing facility requirements that some MIEs must meet before they begin operations, while Part 4 sets out the steps those MIEs must take before making material systems changes. Part 4 also includes the uniform test symbol requirements for marketplaces. Part 5 of NI 26-101 contains business continuity provisions, while Part 6 addresses outsourcing requirements.[3] Part 7 sets out the requirements for vulnerability assessments and system reviews. Part 8 addresses books and records, and Part 9 includes a general exemption provision.

---

[1] As defined in NI 26-101, "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] We plan to update and further harmonize these requirements at a later date, with a view to incorporating global standards and best practices.

[3] Parts 3 and 4, as well as Part 6, apply only to specified MIEs.

**Part 1 – Definitions**

The new definitions in NI 26-101 are primarily based on scoping language that was previously included in the operative provisions of the Source Rules. The definition of "critical system", for example, is based on wording in the system requirements in NI 24-102. It is also consistent with the terminology used in the PFMIs.

**Part 2 – System integrity requirements**

***2. Internal controls and procedures***

An MIE should have comprehensive internal processes to help its board of directors oversee the adequacy and effectiveness of its operational risk management framework. These processes should be fully documented and readily available to the MIE's personnel who are responsible for their implementation. Evidence of board discussions of the MIE's risk management framework should also be fully documented, including in the minutes of the board meetings.

***3. Application to critical systems***

Sections 3 to 5 apply to MIEs' critical systems. While the Source Rules used various descriptors to refer to those systems, in our view the scope of the requirements applicable to MIEs is substantively unchanged from the previous regulatory framework. We note that the system integrity requirements apply to all the systems of an MIE whether operating in-house or outsourced.

***Information technology controls***

For guidance on what constitutes adequate information technology controls, refer to the principles and frameworks published by Chartered Professional Accountants of Canada (CPA Canada), the American Institute of Certified Public Accountants (AICPA), the Information Systems Audit and Control Association (ISACA), the International Organization for Standardization (ISO), the IT Governance Institute in *COBIT*, and the National Institute of Standards and Technology (U.S. Department of Commerce) (NIST). We are of the view that internal controls include controls which support the processing integrity of the models used to quantify, aggregate, and manage the MIE's risks. These controls also include reasonable procedures to review and keep current the testing methodology of the system. An MIE is expected to ensure that its information technology controls address the integrity of the data that it maintains. For a trade repository, this would include protecting all derivatives data submitted by its participants from corruption, loss, improper disclosure, unauthorized access and other processing risks.

***Capacity management***

Capacity management requires that an MIE monitor, review, and test (including stress test) the actual capacity and performance of its systems on an ongoing basis, and that it thoroughly assess and estimate future needs. Accordingly, section 3 of NI 26-101 requires an MIE to meet certain systems capacity, processing capability and disaster recovery standards. While the activities and tests required by paragraph 3(b) must be carried out at least annually, continuing changes in technology, trading volumes, risk management requirements and competitive pressures will often result in these activities being carried out or tested more frequently to ensure that the MIE can continue to appropriately serve its clients or participants. These standards and activities reflect and should be conducted in a manner consistent with prudent business practice.

***4. Prompt notification of system integrity event***

A relevant consideration in determining if a failure, malfunction, delay or security incident is considered "material" (and therefore constitutes a system integrity event) is whether the MIE would, in the normal course of operations, escalate the matter to or inform senior management

ultimately accountable for technology. Any event that requires non-routine measures or resources from the MIE would also be considered material and thus reportable to the regulator or the securities regulatory authority. For matching service utilities, system integrity events would generally include serious incidents that result in the interruption of the matching of trades for more than thirty minutes.

System integrity events would not generally include those that have or would have little or no impact on the MIE's operations or on its participants, although non-material events may become material if they recur or have a cumulative effect. The onus would be on the MIE to document the reasons for any security incident it did not consider material.

Prompt notification pursuant to subsection 4(1) is generally understood to mean notification within one hour from the time the incident was identified as being material. We expect the notification of a system integrity event to include the date, cause and duration of the interruption and its general impact on participants. An MIE may be asked to provide the regulator or securities regulatory authority with additional information such as reports, logs or other relevant systems or process-related documents or data.

***5. Recordkeeping for system incidents***

The MIE should have comprehensive and well-documented procedures in place to record, analyze, and resolve all system failures, malfunctions, delays and security incidents. In this regard, the MIE should undertake a "post-incident" review to identify the causes and any required improvement to its normal operations or business continuity arrangements. Such reviews should, where relevant, include the MIE's participants. Post-incident reports are expected to be communicated to the regulator or securities regulatory authority as soon as practicable.

***Security incidents***

A security incident is considered to be any event that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies.

MIEs should have documented criteria to guide the decision on when to disclose a security incident to their participants or to the public. The criteria for disclosure of a security incident would normally include, but not be limited to, any instance in which participant data – or, if applicable, client data – could be compromised. The disclosure should include information on the types and number of participants (and clients, if applicable) who are affected.[4]

***6. Requirements for auxiliary systems – security incidents***

Section 6 applies only to marketplaces and recognized clearing agencies. The discussion of security incidents in connection with section 4 above is also applicable for security incidents involving auxiliary systems. We note that a security incident involving an auxiliary system may also impact a system that shares network resources with a critical system.

**Part 3 – Pre-operational requirements**

The technology requirements that must be made available by a specified MIE under section 7 describe the hardware, software, communications networks, security controls, integration

[4] CSA Staff Notice 21-326 *Guidance for Reporting Material Systems Incidents* contains further guidance applicable to MIEs that are marketplaces.

standards, operational resilience capabilities, testing obligations, and system capacity necessary for a participant or stakeholder to securely connect to, exchange information with, and conduct activities through the MIE. These requirements, which do not include detailed proprietary information, are generally made accessible to the public or participants, as applicable, in a manner consistent with standard industry practices, e.g. via the MIE's website, portal, or an electronic communication. If a marketplace makes its technology requirements publicly available for longer than the three months required by paragraph 8(a), it may make the testing available during that period or thereafter as long as it is at least two months prior to the marketplace beginning operations. For recognized clearing agencies and trade repositories determining what would be a reasonable period for testing and system modification by participants under section 9, we expect that the needs of all types of participants would be considered, including those of smaller and less sophisticated participants.

For marketplaces and recognized clearing agencies, the readiness certification that must be provided pursuant to section 11 may be based on information provided to the chief information officer from staff knowledgeable about the MIE's information technology systems and the testing that was conducted.

**Part 4 – Requirements for system changes that are material**

For a specified MIE's technology requirements, we consider a system change that is material to include a change that would require a person or company interfacing with or accessing the MIE to incur a significant amount of systems-related development work or costs in order to accommodate the change or to fully interact with the MIE as a result of the change. For a marketplace, material system changes could include changes to technology requirements that would significantly impact a marketplace participant's trading activities, such as the introduction of an order type, or significant changes to a regulatory feed that a regulation services provider takes in from the marketplace.

As is the case for pre-operational technology requirements, the technology requirements that must be disclosed under section 12 with respect to system changes do not include detailed proprietary information. A marketplace that makes its technology requirements publicly available for longer than the three months required by paragraph 13(a) may make the testing available during that period or thereafter as long as it is at least two months prior to implementing a material system change. For recognized clearing agencies and trade repositories determining what would be a reasonable period for testing and system modification by participants under section 14, we expect that the needs of all types of participants would be considered, including those of smaller and less sophisticated participants.

For marketplaces and recognized clearing agencies, as in Part 3 the readiness certification that must be provided pursuant to subsection 15(1) may be based on information provided to the chief information officer from staff knowledgeable about the MIE's information technology systems and the testing that was conducted.

***17. Uniform test symbols***

The use of uniform test symbols is intended to facilitate functionality testing in a marketplace's production environment; it is not intended to enable stress testing by marketplace participants. We are of the view that a marketplace may suspend access to a test symbol where its use in a particular circumstance reasonably represents undue risk to the operation or performance of the marketplace's production environment. We also note that misuse of test symbols by marketplace participants could amount to a breach of the fair and orderly markets provisions of National Instrument 23-103 *Electronic Trading and Direct Electronic Access to Marketplaces*.

**Part 5 – Business continuity**

***18. Planning and testing***

Business continuity management is an essential component of an MIE's operational risk management framework. Business continuity planning should encompass all policies and procedures to ensure uninterrupted provision of vital services regardless of the cause of potential disruption. These plans should allow an MIE to provide continuous and undisrupted service, as back-up systems ideally should commence processing immediately.

An MIE's business continuity plan and its associated arrangements should be subject to frequent review and testing. Tests should address various scenarios that simulate wide-scale disasters and inter-site switchovers. Employees should be thoroughly trained to execute the business continuity plan. Industry participants, critical service providers, and other relevant MIEs should be regularly involved in the testing and be provided with a general summary of the testing results, including testing of back-up facilities. In fulfilling the requirements to develop, maintain and test reasonable business continuity plans, we expect MIEs to remain current with best practices and to adopt them to the extent that they address their critical business needs.

***19. Resumption of operations***

Section 19 also establishes requirements for information processors, certain marketplaces,[5] recognized clearing agencies and trade repositories to develop, maintain and apply policies and procedures reasonably designed to ensure that critical systems can resume operations within certain time limits following the declaration of a disaster. A disaster could include any external sources of operational risk, such as the failure of critical service providers or utilities or events affecting a wide metropolitan area, such as natural disasters, terrorism, and pandemics. We appreciate that what constitutes a disaster for the purposes of the requirements may not be the same for all MIEs. We expect that MIEs will be guided by their own business continuity plans in this respect.

We note that for trade repositories, the recovery timeframe was previously an expectation in companion policies to local and multi-jurisdictional rules, but we have determined that, consistent with Source Rule requirements for other MIEs,[6] it is more appropriately a rule requirement. In our view, this harmonization does not represent a substantive change, given the previous expectation and the fact that the requirement is to have policies and procedures in place reasonably designed to ensure recovery within a specified timeframe as opposed to an absolute time-based recovery requirement.

***20. Industry-wide business continuity tests***

We expect marketplaces, recognized clearing agencies, information processors, and participant dealers to make their production environments available for all industry-wide business continuity tests. These MIEs should make appropriate adjustments to their business continuity plans and associated arrangements based on the results of the testing exercises.

**Part 6 – Outsourcing**

Section 21 of NI 26-101 sets out the requirements applicable to specified MIEs that outsource any of their critical services or systems to a third-party service provider (including affiliates or

[5] The provision applies to marketplaces that meet a minimum threshold of total dollar value of trading volume, recognized exchanges or quotation and trade reporting systems that directly monitor the conduct of their members, and regulation services providers that have entered into a written agreement with a marketplace to conduct market surveillance.

[6] The recovery timeframe for marketplaces is explicitly stated in NI 21-101. For recognized clearing agencies, the timeframe is included in the PFMIs, which are incorporated by reference into NI 24-102.

associates of the MIE). The MIE should ensure that the outsourced operations are subject to and compliant with the same standards as would apply internally. The requirements in section 21 apply regardless of whether the outsourcing arrangements are with external service providers or with the specified MIE's affiliates. A specified MIE that outsources its critical services or systems remains responsible for those services or systems and for compliance with Canadian securities legislation.

Generally, a specified MIE is required to develop, maintain and apply policies and procedures to evaluate and approve outsourcing agreements with critical service providers. Such policies and procedures should include assessing the suitability of potential service providers and the ability of the specified MIE to continue to comply with Canadian securities legislation in the event of the service provider's bankruptcy, insolvency or termination of business. The specified MIE is also required to monitor and evaluate the service provider's ongoing performance and compliance. Accordingly, the specified MIE should define key performance indicators (KPIs) that will measure the service levels delivered against those outlined in the outsourcing agreement. Further, the specified MIE should have robust arrangements for the substitution of critical service providers, timely access to all necessary information, and the proper controls and monitoring tools.

As set out in paragraph 21(c), the contract between the specified MIE and the critical service provider should allow the MIE and relevant authorities to have full access to necessary information. The contract should specify that before the critical service provider can itself outsource material elements of the service provided to the specified MIE, the MIE's prior approval is mandatory. The contract should also ensure that in the event of outsourcing to a fourth party, full access by the specified MIE and relevant authorities is preserved. Clear lines of communication should be established between the specified MIE and the service provider to facilitate the flow of functions and information between parties in both ordinary and exceptional circumstances.

If a marketplace or a recognized clearing agency outsources critical services, it should disclose the nature and scope of this dependency to its participants. It should also identify the risks arising from its outsourcing and take appropriate actions to manage these dependencies through appropriate contractual and organizational arrangements.

A specified MIE should inform the relevant authorities about any such dependencies and the performance of these critical service providers. To that end, the specified MIE can contractually provide for and ensure that the regulator or the securities regulatory authority has direct contact with and can obtain specific reports and full information from the critical service provider.

## Part 7 – Vulnerability assessments and system reviews

### *22. Vulnerability assessments*

Section 22 applies to all MIEs other than trade repositories. Following a vulnerability assessment, we would expect an MIE to implement appropriate improvements where necessary. For the purposes of section 22, we consider a qualified party to be a person or company or a group of persons or companies with relevant experience in both information technology and in the evaluation of related internal systems or controls in a complex information technology environment. Qualified parties may include external auditors or third-party information system consultants, as well as employees of the MIE or an affiliated entity. We would not consider persons responsible for the development or operation of the systems or capabilities being tested to be qualified parties in this context.

***23. Independent system reviews***

We consider that best industry practices for independent system reviews under section 23 include the "Trust Services Criteria" developed by AICPA and CPA Canada. For a marketplace, the focus of the assessment of any systems that share network resources with trading-related systems would be to address potential threats from a security incident that could negatively impact a trading-related system.

Trade repositories and matching service utilities are not required to retain an external auditor to conduct an independent system review. The system review may be conducted by a person or company or a group of persons or companies with relevant experience in both information technology and in the evaluation of related internal controls in a complex information technology environment, such as external auditors or third-party information system consultants. We are of the view that this obligation may also be satisfied by an independent assessment by an internal audit department that is compliant with the Global Internal Audit Standards published by the Institute of Internal Auditors. Before engaging such a qualified party, a trade repository should notify the regulator or securities regulatory authority.

Section 23 requires marketplaces, recognized clearing agencies and information processors to retain a qualified external auditor to conduct an independent system review. We consider a qualified external auditor to be a person or company or a group of persons or companies with relevant experience in both information technology and in the evaluation of related internal controls in a complex information technology environment. Before engaging an external auditor pursuant to section 23, an MIE is expected to discuss its choice of auditor and the scope of the systems review mandate with the regulator or the securities regulatory authority. We further expect the report prepared by the external auditor to include, to the extent applicable, an audit opinion that (i) the description included in the report fairly presents the systems and controls that were designed and implemented throughout the reporting period, (ii) the controls stated in the description were suitably designed, and (iii) the controls operated effectively throughout the reporting period.

**Part 8 – Books and records**

We expect the books, records and other documents referred to in section 24 to include all correspondence, memoranda, papers, books, notices, accounts, test scripts, test results, and other similar records. Section 24 is based on the general record-keeping requirements in the Source Rules as well as in Canadian securities legislation. Consistent with the Source Rules, only marketplaces and recognized clearing agencies have specified retention periods.

## ANNEX D

## PROPOSED AMENDMENTS TO NATIONAL INSTRUMENT 21-101 *MARKETPLACE OPERATION*

***1. National Instrument 21-101 Marketplace Operation is amended by this Instrument.***

***2. Section 1.1 is amended by adding the following definitions:***

"critical service" has the meaning ascribed to it in National Instrument 26-101 *Information Technology System Integrity*;

"critical system" has the meaning ascribed to it in National Instrument 26-101 *Information Technology System Integrity*;**.**

***3. Section 5.12 is replaced with the following:***

**5.12** If a marketplace outsources any of its key services or systems to a service provider, including, for greater certainty, an affiliated entity or associate of the marketplace, the marketplace must comply with section 21 of National Instrument 26-101 *Information Technology System Integrity*.**.**

***4. Section 6.7 is repealed.***

***5. Section 11.3 is amended.***

***(a) by replacing paragraph (c) of subsection (1) with the following:***

**(c)** at least one copy of all records made or received by the marketplace in the course of complying with Part 2 and Part 5 of National Instrument 26-101 *Information Technology System Integrity*, including, for greater certainty, all correspondence, memoranda, papers, books, notices, accounts, reports, test scripts, test results and other similar records;**,**

***(b) by replacing paragraph (i) of subsection (1) with the following:***

**(i)** a copy of any contract referred to in paragraph 21(c) of National Instrument 26-101 *Information Technology System Integrity;*

***(c) by adding*** *"*and*"* ***at the end of paragraph (a) of subsection (2),***

***(d) by replacing*** *"*Part 3; and*"* ***with*** *"*Part 3.*"* ***in paragraph (b) of subsection (2), and***

***(e) by repealing paragraph (c) of subsection (2).***

***6. Part 12 is repealed.***

***7. Sections 14.5 to 14.6 are repealed.***

***8. Form 21-101F1 Information Statement – Exchange or Quotation and Trade Reporting System is amended by replacing "***key services or systems***" and** *"key services and systems"* **wherever the expressions occur with "***key services or systems, including, for greater certainty, critical services or critical systems,***".***

***9. Exhibit D – Affiliates of Form 21-101F1 Information Statement – Exchange or Quotation and Trade Reporting System is amended by repealing*** item 1 of paragraph 2(ii)***.***

***10. Exhibit F – Outsourcing of Form 21-101F1 Information Statement – Exchange or Quotation and Trade Reporting System is amended***

***(a) in item 4 by replacing*** *"*paragraph 5.12(a) of National Instrument 21-101 *Marketplace Operation"* ***with*** *"*paragraph 21(a) of National Instrument 26-101 *Information Technology System Integrity* and section 5.12 of National Instrument 21-101 *Marketplace Operation"**,***

***(b) in item 5 by replacing*** *"*paragraph 5.12(b) of National Instrument 21-101 *Marketplace Operation"* ***with*** *"*paragraph 21(b) of National Instrument 26-101 *Information Technology System Integrity* and section 5.12 of National Instrument 21-101 *Marketplace Operation"**,***

***(c) in item 6 by replacing*** *"*paragraph 5.12(f) of National Instrument 21-101 *Marketplace Operation"* ***with*** *"*paragraph 21(f) of National Instrument 26-101 *Information Technology System Integrity* and section 5.12 of National Instrument 21-101 *Marketplace Operation"**,***

***(d) in item 7 by replacing*** *"*paragraph 5.12(g) of National Instrument 21-101 *Marketplace Operation"* ***with*** *"*paragraph 21(h) of National Instrument 26-101 *Information Technology System Integrity* and section 5.12 of National Instrument 21-101 *Marketplace Operation"**, and***

***(e) in item 8 by replacing*** *"*paragraph 5.12(h) of National Instrument *21-101 Marketplace Operation"* ***with*** *"*paragraph 21(j) of National Instrument 26-101 *Information Technology System Integrity* and section 5.12 of National Instrument 21-101 *Marketplace Operation"**.***

***11. Exhibit G – Systems and Contingency Planning of Form 21-101F1 Information Statement – Exchange or Quotation and Trade Reporting System is amended***

***(a) in item 2 after the heading*** *"*General*"* ***and before the heading*** *"*Business Continuity Planning*"* ***by replacing*** *"*subsection 12.2(1) of National Instrument 21-101 *Marketplace Operation"* ***with*** *"*section 23 of National Instrument 26-101 *Information Technology System Integrity*"***, and***

***(b) in item 3 after the heading*** *"*Systems*"* ***and before the heading*** *"*IT Risk Assessment*"* ***by replacing*** *"*section 12.1 of National Instrument 21-101

*Marketplace Operation"* ***with*** *"*sections 2 and 3 of National Instrument 26-101 *Information Technology System Integrity"****.***

***12. Form 21-101F2 Information Statement – Alternative Trading System is amended by replacing "***key services or systems***" and** *"key services and systems"* ***wherever the expressions occur with "***key services or systems, including, for greater certainty, critical services or critical systems,***".***

***13. Exhibit D – Affiliates of Form 21-101F2 Information Statement – Alternative Trading System is amended by repealing*** item 1 of paragraph 2(ii)***.***

***14. Exhibit F – Outsourcing of Form 21-101F2 Information Statement – Alternative Trading System is amended***

***(a) in item 4 by replacing*** *"*subsection 5.12(a) of National Instrument 21-101 *Marketplace Operation"* ***with*** *"*paragraph 21(a) of National Instrument 26-101 *Information Technology System Integrity* and section 5.12 of National Instrument 21-101 *Marketplace Operation"****,***

***(b) in item 5 by replacing*** *"*subsection 5.12(b) of National Instrument 21-101 *Marketplace Operation"* ***with*** *"*paragraph 21(b) of National Instrument 26-101 *Information Technology System Integrity* and section 5.12 of National Instrument 21-101 *Marketplace Operation"****,***

***(c) in item 6 by replacing*** *"*subsection 5.12(f) of National Instrument 21-101 *Marketplace Operation"* ***with*** *"*paragraph 21(f) of National Instrument 26-101 *Information Technology System Integrity* and section 5.12 of National Instrument 21-101 *Marketplace Operation"****,***

***(d) in item 7 by replacing*** *"*subsection 5.12(g) of National Instrument 21-101 *Marketplace Operation"* ***with*** *"*paragraph 21(h) of National Instrument 26-101 *Information Technology System Integrity* and section 5.12 of National Instrument 21-101 *Marketplace Operation"****, and***

***(e) in item 8 by replacing*** *"*subsection 5.12(h) of National Instrument 21-101 *Marketplace Operation"* ***with*** *"*paragraph 21(j) of National Instrument 26-101 *Information Technology System Integrity* and section 5.12 of National Instrument 21-101 *Marketplace Operation"****.***

***15. Exhibit G – Systems and Contingency Planning of Form 21-101F2 Information Statement – Alternative Trading System is amended***

***(a) in item 2 after the heading "***General***" and before the heading "****Business Continuity Planning****" by replacing*** *"*subsection 12.2(1) of National Instrument 21-101 *Marketplace Operation"* ***with*** *"*section 23 of National Instrument 26-101 *Information Technology System Integrity"****, and***

***(b) in item 3 after the heading*** *"*Systems*"* ***and before the heading*** *"*IT Risk Assessment*"* ***by replacing*** *"*section 12.1 of National Instrument 21-101 *Marketplace Operation"* ***with*** *"*sections 2 and 3 of National Instrument 26-101 *Information Technology System Integrity"****.***

***16. Form 21-101F4 Cessation of Operations Report for Alternative Trading System is amended by repealing "Exhibit B".***

17. (1) This Instrument comes into force on [●].

(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.

## ANNEX D

## PROPOSED AMENDMENTS TO NATIONAL INSTRUMENT 24-101 *INSTITUTIONAL TRADE MATCHING AND SETTLEMENT*

***1. National Instrument 24-101 Institutional Trade Matching and Settlement is amended by this Instrument.***

***2. Section 1.1 is amended by adding the following definition:***

"critical system" has the meaning ascribed to it in National Instrument 26-101 *Information Technology System Integrity*;**.**

***3. Section 6.5 is repealed.***

***4. Exhibit A – External systems audit of Form 24-101F5 Matching Service Utility Quarterly Operations Report of Institutional Trade Reporting and Matching is amended by replacing "***core systems***" with "***critical systems***".***

***5. Exhibit B – Material systems failures reporting of Form 24-101F5 Matching Service Utility Quarterly Operations Report of Institutional Trade Reporting and Matching is amended by replacing "***section 6.5(c) of the Instrument**" with "***section 4 of National Instrument 26-101 *Information Technology System Integrity***".**

6. (1) This Instrument comes into force on [●].

(2) IIn 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.

## ANNEX D

## PROPOSED AMENDMENTS TO NATIONAL INSTRUMENT 24-102 *CLEARING AGENCY REQUIREMENTS*

***1. National Instrument 24-102 Clearing Agency Requirements is amended by this Instrument.***

***2. Subparagraph 2.1(1)(b)(ii) is amended by adding "***and National Instrument 26-101 *Information Technology System Integrity****" after "***applicable requirements under this Instrument***".***

***3. Sections 4.6 to 4.9 are repealed.***

***4. Section 4.10 is replaced with the following:***

**4.10** If a recognized clearing agency outsources a key service or system to a service provider, including, for greater certainty, an affiliated entity of the clearing agency, the clearing agency must comply with section 21 of National Instrument 26-101 *Information Technology System Integrity*.**.**

5. (1) This Instrument comes into force on [●].

(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.

## ANNEX E

## PROPOSED CHANGES TO
## COMPANION POLICY 21-101 *MARKETPLACE OPERATION*

***1. Companion Policy 21-101 Marketplace Operation is changed by this Document.***

***2. Subsection 3.1(4) is changed by adding the following at the end of the paragraph:***

For example, if an ATS meets or exceeds 10% market share in trading volume, value or number of trades in a particular security on all marketplaces in Canada, the securities regulatory authority intends to review the ATS and its structure and operations in order to consider whether the person or company operating the ATS should be considered to be an exchange for purposes of securities legislation or if additional terms and conditions should be placed on the registration of the ATS. The securities regulatory authority intends to conduct this review because these thresholds may be indicative of an ATS having significant market presence in a type of security, such that it would be more appropriate that the ATS be regulated as an exchange. If more than one Canadian securities regulatory authority is conducting this review, the reviewing jurisdictions intend to coordinate their review.

***3. Section 3.4 is changed by deleting subsections (7) and (8).***

***4. Section 5.1 is changed by adding the following subsection:***

**(4.1)** The securities regulatory authority may also consider granting an exemption from the pre-trade transparency requirements in sections 7.1 or 7.3 of the Instrument to a marketplace for the display of dark orders, other than orders that result from a request for quotes or facility that allows negotiation between two parties provided that:

(a) each order entered on the marketplace meets the size threshold set by a regulation services provider as provided in subsection 7.1(2) or 7.3(2) of the Instrument,

(b) affirmative actions are taken by the party entering the dark order that confirms their agreement to the display of their order information,

(c) as provided in subsection 5.1(2), the display of order information will be limited to the symbol of the security and side (buy or sell); information about the order price and size should not be conveyed; however, price and size may be inferable without precision, and

(d) the display of order information should not enable the recipient of the information to determine if a displayed order is a firm indication of a willingness to buy or sell a security or a non-firm indication of interest.

***5. Section 7.9 is changed***

***a) by replacing the text with the following:***

Section 5.12 of the Instrument sets out the requirements for marketplaces that outsource any of their key services or systems. Key services and systems are services and systems that are necessary for a marketplace to operate effectively and in compliance with regulatory requirements and appropriate standards. These may include, for example, a marketplace's audit function.[1] To promote a harmonized approach to the regulation of outsourcing, section 5.12 incorporates by reference the outsourcing requirements set out in section 21 of National Instrument 26-101 *Information Technology System Integrity*.

Generally, marketplaces are required to establish policies and procedures to evaluate and approve these outsourcing agreements. Such policies and procedures would include assessing the suitability of potential service providers and the ability of the marketplace to continue to comply with securities legislation in the event of the service provider's bankruptcy, insolvency or termination of business. Marketplaces are also required to monitor the ongoing performance of the service provider to which they outsourced key services, systems or facilities. The requirements under section 5.12 of the Instrument apply regardless of whether the outsourcing arrangements are with third party service providers, or with affiliates or associates of the marketplaces.

***b) by adding a footnote after the words*** "audit function."***:***

Critical services and systems, a subset of key systems and services, are separately regulated by National Instrument 26-101 *Information Technology System Integrity*.

***6. Part 14 is deleted.***

***7. Paragraph (f) of subsection 16.2(1) is replaced with the following:***

the systems report referred to in section 23 of National Instrument 26-101 *Information Technology System Integrity.*

***8. Section 16.4 is deleted.***

**Effective Date**

9. These changes become effective on •.

## ANNEX E

## PROPOSED CHANGES TO COMPANION POLICY 24-101 INSTITUTIONAL TRADE MATCHING AND SETTLEMENT

1. ***Companion Policy 24-101 Institutional Trade Matching and Settlement is changed by this Document.***

2. ***Section 6.5 is deleted.***

**Effective Date**

3. These changes become effective on •.

## ANNEX E

## PROPOSED CHANGES TO
## COMPANION POLICY 24-102 *CLEARING AGENCY REQUIREMENTS*

1. ***Companion Policy 24-102 Clearing Agency Requirements is changed by this Document.***

2. ***Section 2.1 is changed by adding the following sentence at the end of the first paragraph:***

   Applicants will also need to demonstrate equivalent compliance with the requirements of National Instrument 26-101 *Information Technology System Integrity*.

3. ***The first paragraph after the heading*** *"Division 3 – Operational Risk"* ***is deleted.***

4. ***Sections 4.6 to 4.9 are deleted.***

5. ***Section 4.10 is changed***

   ***a) by replacing the text with the following:***

   A recognized clearing agency that chooses to outsource a key system or service should ensure that the system or service meets the same standards that would apply internally. This requirement applies regardless of whether the outsourcing arrangements are with third-party service providers or with affiliated entities of the clearing agency.

   Section 4.10 sets out requirements applicable to a recognized clearing agency that outsources any of its key services or systems to a service provider. Key services and systems are services and systems that are necessary for a clearing agency to operate effectively and in compliance with regulatory requirements and appropriate standards. These may include, for example, a clearing agency's audit function. To promote a harmonized approach to the regulation of outsourcing, section 4.10 incorporates by reference the outsourcing requirements set out in section 21 of National Instrument 26-101 *Information Technology System Integrity*.

   Generally, the clearing agency is required to establish, implement, maintain and enforce policies and procedures to evaluate and approve outsourcing agreements with service providers regarding the outsourcing of key systems or services. Such policies and procedures should include assessing the suitability of potential service providers and the ability of the clearing agency to continue to comply with securities legislation in the event of the service provider's bankruptcy, insolvency or termination of business. The clearing agency is also required to monitor and evaluate the on-going performance and compliance of the service provider to which they outsourced key services, systems or facilities. Accordingly, the clearing agency should define key performance indicators that will measure the service level. Further, the clearing agency should have robust arrangements for the substitution of such providers, timely access to all necessary information, and the proper controls and monitoring tools.

A contractual relationship should be in place between the clearing agency and the service provider allowing it and relevant authorities to have full access to necessary information. The contract should ensure that the clearing agency's approval is mandatory before the service provider can itself outsource material elements of the service provided to the clearing agency, and that in the event of such an arrangement, full access to the necessary information is preserved. Clear lines of communication should be established between the outsourcing clearing agency and the service provider to facilitate the flow of functions and information between parties in both ordinary and exceptional circumstances.

Where the clearing agency outsources a key system or service, it should disclose the nature and scope of this dependency to its participants. It should also identify the risks from its outsourcing and take appropriate actions to manage these dependencies through appropriate contractual and organisational arrangements. The clearing agency should inform the securities regulatory authority about any such dependencies and the performance of its service providers. To that end, the clearing agency can contractually provide for direct contacts between the service provider and the securities regulatory authority, contractually ensure that the securities regulatory authority can obtain specific reports from the service provider, or the clearing agency may provide full information to the securities regulatory authority.

***b) by adding a footnote after the words*** "audit function."***:***

Critical services and systems, a subset of key systems and services, are separately regulated by National Instrument 26-101 *Information Technology System Integrity*.

***6. Annex II is changed by adding a footnote after the heading*** **"JOINT SUPPLEMENTARY GUIDANCE DEVELOPED BY THE BANK OF CANADA AND CANADIAN SECURITIES ADMINISTRATORS ON RECOVERY PLANS"*:***

The CSA notes that the terms "critical system" and "critical service" in Annex II are used in the context of the PFMIs and do not necessarily reflect the way these terms are used in National Instrument 26-101 *Information Technology System Integrity*.

**Effective Date**

7. These changes become effective on •.

## Annex F

## Table of Concordance

| NI 26-101 Provisions | NI 21-101 | NI 24-102 | Trade Reporting Rules[1] | NI 21-101 - Information Processor | NI 24-101 - Matching Service Utility |
|---|---|---|---|---|---|
| **Part 2 – System Integrity Requirements** | | | | | |
| Operational risk management framework | | | | | |
| s. 2(1) | | | s. 21(1) | | |
| s. 2(2) | | | s. 21(2) | | |
| Requirements for critical systems | | | | | |
| s. 3(a) | s. 12.1(a) | s. 4.6(a) | s. 21(3)(a) | s. 14.5(a) | |
| s. 3(b) | s. 12.1(b) | s. 4.6(b) | s. 21(3)(b) | s. 14.5(b) | s. 6.5(a)(i)<br>s. 6.5(a)(ii) |
| System integrity event | | | | | |
| s. 4(1) | s. 12.1(c) | s. 4.6(c) | s. 21(3)(c) | s. 14.5(e) | s. 6.5(c) |
| s. 4(2) | s. 12.1(c) | s. 4.6(c) | | s. 14.5(e) | |
| s. 4(3) | s. 12.1(c) | s. 4.6(c) | s. 21(3)(c) | s. 14.5(e) | |
| Recordkeeping for system incidents | | | | | |
| s. 5 | s. 12.1(d) | s. 4.6(d) | | s. 14.5(f) | s. 6.4(1) |
| Requirements for auxiliary systems | | | | | |
| s. 6(1) | s. 12.1.1(a) | s. 4.6.1(2)(a) | | | |
| s. 6(2) | s. 12.1.1(c) | s. 4.6.1(2)(c) | | | |
| s. 6(3) | s. 12.1.1(b) | s. 4.6.1(2)(b) | | | |
| s. 6(4) | s. 12.1.1(b) | s. 4.6.1(2)(b) | | | |
| **Part 3 – Pre-operational Requirements – Specified MIE** | | | | | |
| Availability of technology requirements and testing facilities | | | | | |

[1] Local and multi-jurisdictional trade reporting rules: Manitoba Securities Commission Rule 91-507 Derivatives: Trade Reporting; Ontario Securities Commission Rule 91-507 Derivatives: Trade Reporting; *Regulation 91-507 respecting Trade Repositories and Derivatives Data Reporting* (Québec); and Multilateral Instrument 96-101 *Derivatives: Trade Reporting*.

| NI 26-101 Provisions | NI 21-101 | NI 24-102 | Trade Reporting Rules[1] | NI 21-101 - Information Processor | NI 24-101 - Matching Service Utility |
|---|---|---|---|---|---|
| s. 7(1)(a) | s. 12.3(1)(a) | s. 4.8(1)(a) | s. 21(8)(a) | | |
| s. 7(1)(b) | s. 12.3(2)(a) | s. 4.8(2)(a) | s. 21(9)(a) | | |
| s. 7(2) | s. 12.3(1) | | s. 21(8) | | |
| s. 7(3) | | s. 4.8(1) | | | |
| Time period for availability - marketplace | | | | | |
| s. 8(a) | s. 12.3(1)(a) | | | | |
| s. 8(b) | s. 12.3(2)(a) | | | | |
| Time period for availability – clearing agency and trade repository | | | | | |
| s. 9 | | s. 4.8(2)(a) | s. 21(9)(a) | | |
| Confirmation and certification | | | | | |
| s. 10 | s. 12.3(3)(b) | | | | |
| s. 11 | s. 12.3(3)(c) | s. 4.8(3)(b) | | | |
| **Part 4 – Requirements for Changes that are Material** | | | | | |
| Availability of technology requirements and testing facilities | | | | | |
| s. 12(1)(a) | s. 12.3(1)(b) | s. 4.8(1)(b) | s. 21(8)(b) | | |
| s. 12(1)(b) | s. 12.3(2)(b) | s. 4.8(2)(b) | s. 21(9)(b) | | |
| s. 12(2) | s. 12.3(1) | | s. 21(8) | | |
| s. 12(3) | | s. 4.8(1)(b) | | | |
| Time period for availability – marketplace | | | | | |
| 13(a) | 12.3(1)(b) | | | | |
| 13(b) | 12.3(2)(b) | | | | |
| Time period of availability - clearing agency and trade repository | | | | | |
| s. 14 | | s. 4.8(1)(b) | s. 21(8)(b) | | |

| NI 26-101 Provisions | NI 21-101 | NI 24-102 | Trade Reporting Rules[1] | NI 21-101 - Information Processor | NI 24-101 - Matching Service Utility |
|---|---|---|---|---|---|
| | | s. 4.8(2)(b) | s. 21(9)(b) | | |
| Compliance and certification | | | | | |
| s. 15(1) | s.12.3(3.1)(b) | s. 4.8(4)(b) | | | |
| s. 15(2) | | | | | |
| Emergency exception | | | | | |
| s. 16(1)(a) | s. 12.3(4) | s. 4.8(5) | s. 21(11)(a) | | |
| s. 16(1)(b) | s. 12.3(4)(a) | s. 4.8(5)(a) | s. 21(11)(b) | | |
| s. 16(1)(c) | s. 12.3(4)(b) | s. 4.8(5)(b) | s. 21(11)(c) | | |
| s. 16(2) | s. 12.3.(4)(b) | | s. 21(11)(c) | | |
| s. 16(3) | | s. 4.8(5)(b) | | | |
| Uniform test symbols | | | | | |
| s. 17 | s. 12.3.1 | | | | |
| **Part 5 – Business Continuity** | | | | | |
| Business continuity planning | | | | | |
| s. 18(1) | s.12.4(1)(a) | s. 4.9(a) | s. 21(4) | s. 14.6(a) | s. 6.5(a)(v) |
| s. 18(2) | s.12.4(1)(b) | s. 4.9(b) | s. 21(5) | s. 14.6(b) | |
| Resumption of operations | | | | | |
| s. 19(1) | | | | | |
| s. 19(1)(a) | | | | s. 14(6)(c) | |
| s. 19(1)(b) | s. 12.4(2) | | | | |
| s. 19(1)(c) | | s. 3.1: PFMI Principle 17 – Key Consideration 6 | | | |
| s. 19(2) | | | | | |
| s. 19(2)(a) | s. 12.4(3) | | | | |
| s. 19(2)(b) | s. 12.4(4) | | | | |
| Industry-wide business continuity tests | | | | | |

| NI 26-101 Provisions | NI 21-101 | NI 24-102 | Trade Reporting Rules[1] | NI 21-101 - Information Processor | NI 24-101 - Matching Service Utility |
|---|---|---|---|---|---|
| s. 20 | s. 12.4.1 | s. 12.4.1 of NI 21-101 | | s. 12.4.1 | |
| **Part 6 – Outsourcing** | | | | | |
| Outsourcing | | | | | |
| s. 21(a) | s. 5.12(a) | s. 4.10(a) | s. 24(a) | | |
| s. 21(b) | s. 5.12(b) | s. 4.10(b) | s. 24(b) | | |
| s. 21(c) | s. 5.12(c) | s. 4.10(c) | s. 24(c) | | |
| s. 21(d) | s. 5.12(d) | s. 4.10(d) | s. 24(d) | | |
| s. 21(e) | s. 5.12(e) | s. 4.10(e) | s. 24(e) | | |
| s. 21(f) | s. 5.12(f) | s. 4.10(g) | s. 24(g) | | |
| s. 21(g) | | s. 4.10(f) | s. 24(f) | | |
| s. 21(h) | s. 5.12(g) | s. 4.10(h) | s. 24(h) | | |
| s. 21(i) | | s. 4.10(h) | | | |
| s. 21(j) | s. 5.12(h) | s. 4.10(i) | s. 24(i) | | |
| **Part 7 - Vulnerability Testing and System Reviews** | | | | | |
| Vulnerability assessments | | | | | |
| s. 22 | s. 12.1.2 | s. 4.7(1)(b) | | s. 14.5.1 | s. 6.5(a)(iv) |
| System reviews | | | | | |
| s. 23(1) | s. 12.2(1) | s. 4.7(1)(a) | s. 21(6) | s. 14.5(c) | s. 6.5(b) |
| s. 23(2) | s. 12.2(1) | s. 4.7(1)(a) | | s. 14.5(c) | |
| s. 23(3) | s. 12.2(2) | s. 4.7(2) | s. 21(7) | s. 14.5(d) | |
| **Part 8 – Books and Records** | | | | | |
| s. 24(1) | s. 11.1 | s. 5.1(1) | s. 18 relates to derivatives data | s. 14.4(3) | s. 6.4(2) |
| s. 24(2) | S 11.3(1) | s. 5.1(2) | s. 18 relates to derivatives data | | |

## ANNEX G

## PROPOSED AMENDMENTS TO MULTILATERAL INSTRUMENT 96-101 *DERIVATIVES: TRADE REPORTING*

***1) Multilateral Instrument 96-101 Derivatives: Trade Reporting is amended by this Instrument.***

***2) Subsection 1(1) is amended by adding the following definitions:***

"critical service" has the meaning ascribed to it in National Instrument 26-101 *Information Technology System Integrity*;

"critical system" has the meaning ascribed to it in National Instrument 26-101 *Information Technology System Integrity*;**.**

***3) Section 21 is repealed.***

***4) Section 24 is replaced with the following:***

**24.** If a recognized trade repository outsources a material system or service to a service provider, including, for greater certainty, an affiliated entity or an associate of the recognized trade repository, the recognized trade repository must comply with section 21 of National Instrument 26-101 *Information Technology System Integrity***.**

***5) Form 96-101F1 Application for Recognition – Trade Repository Information Statement is amended* by replacing** "key services or systems" **wherever the expression occurs with** "key services or systems, including, for greater certainty, critical services or critical systems**,**".

***6) Exhibit G - Form 96-101F1 Application for Recognition – Trade Repository Information Statement is amended by replacing the portion of the Form after the heading "****Exhibit G – Systems and Contingency Planning****" and before the item 1 "****Current and future capacity estimates****" with the following:***

For each of the systems for collecting and maintaining reports of derivatives date, including each of the critical systems to which National Instrument 26-101 Information Technology System Integrity applies, describe:**.**

**7**. (1) This Instrument comes into force on [●].

(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.

## ANNEX G

## PROPOSED CHANGES TO COMPANION POLICY 96-101
## *DERIVATIVES: TRADE REPORTING*

1. ***Companion Policy 96-101 Derivatives: Trade Reporting is changed by this Document.***

2. ***The chart under Section 2 is replaced by the following:***

| **Principle in the PFMI Report applicable to a recognized trade repository** | **Relevant section(s) of the Rule** |
|---|---|
| Principle 1: Legal Basis | Section 7 – Legal framework<br>Section 17 – Rules, policies and procedures (in part) |
| Principle 2: Governance | Section 8 – Governance<br>Section 9 – Board of directors<br>Section 10 – Management |
| Principle 3: Framework for the comprehensive management of risks | Section 19 – Comprehensive risk-management framework<br>Section 20 – General business risk (in part) |
| Principle 15: General business risk | Section 20 – General business risk |
| Principle 17: Operational risk | National Instrument 26-101 *Information Technology System Integrity*<br>Section 22 – Data security and confidentiality<br>Section 24 – Outsourcing |
| Principle 18: Access and participation requirements | Section 13 – Access to recognized trade repository services<br>Section 16 – Due process (in part)<br>Section 17 – Rules, policies and procedures (in part) |
| Principle 19: Tiered participation arrangements | Section 7 – Legal framework<br>Section 19 – Comprehensive risk-management framework<br>National Instrument 26-101 *Information Technology System Integrity* |
| Principle 20: FMI links | Section 7 – Legal Framework<br>Section 19 – Comprehensive risk-management framework<br>National Instrument 26-101 *Information Technology System Integrity*<br>Section 24 – Outsourcing |
| Principle 21: Efficiency and effectiveness | Section 7 – Legal framework<br>Section 8 - Governance<br>Section 11 - Chief compliance officer<br>Section 12 – Fees |

| | |
|---|---|
| | National Instrument 26-101 *Information Technology System Integrity* |
| Principle 22: Communication procedures and standards | Section 15 – Communication policies, procedures and standards |
| Principle 23: Disclosure of rules, key procedures, and market data | Section 17 – Rules, policies and procedures (in part) |
| Principle 24: Disclosure of market data by trade repositories | Sections in Part 4 – Data Dissemination and Access to Data |

***3. Section 21 is deleted.***

***4. Section 24 is changed:***

***a) by replacing the text with the following:***

Section 24 sets out requirements applicable to a recognized trade repository that outsources any of its material services or systems to a service provider. Material services and systems are services and systems that are necessary for a recognized trade repository to operate effectively and in compliance with regulatory requirements and appropriate standards. These may include, for example, a recognized trade repository's audit function. To promote a harmonized approach to the regulation of outsourcing, section 24 incorporates by reference the outsourcing requirements set out in section 21 of National Instrument 26-101 *Information Technology System Integrity*.

Generally, a recognized trade repository must establish policies and procedures to evaluate and approve these outsourcing arrangements. Such policies and procedures include assessing the suitability of potential service providers and the ability of the recognized trade repository to continue to comply with securities legislation in the event of bankruptcy, insolvency or the termination of business of the service provider. A recognized trade repository is also required to monitor the ongoing performance of a service provider to which it outsources a material service, system or facility. The requirements under section 24 apply regardless of whether the outsourcing arrangements are with a third-party service provider or affiliated entity of the recognized trade repository. A recognized trade repository that outsources its services or systems remains responsible for those services or systems and for compliance with securities legislation.

***b) by adding a footnote after the words*** "audit function."***:***

Critical services and systems, a subset of material systems and services, are separately regulated by National Instrument 26-101 *Information Technology System Integrity*.

5. **These changes become effective on •**.