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.

---

[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.

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 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.