Ontario Securities Commission

Automation Review Program

For Market Infrastructure Entities in the Canadian Capital Markets

Capital Markets Branch

Version: October 18, 2002

Table of Contents

PART I. INTRODUCTION

This document has been prepared by Market Regulation (Capital Markets Branch) of the Ontario Securities Commission ("Commission" or "OSC") to address issues raised by the growing automation and integration of trading and clearing and settlement systems in the securities industry. It proposes the establishment of an Automation Review Program ("ARP" or "Program") for any specified market infrastructure entity ("Entity") that operates key technology systems and processes in the Canadian securities markets.

A. Management Summary

The Program has been developed because of the growing importance of automated systems in Canada's securities markets and global financial systems. A serious disruption could have an adverse impact on financial systems, the efficiency of the securities market and the public's confidence in the market.[1]

With the implementation of real-time systems and the move to straight-through-processing ("STP"), the securities industry becomes much more dependent upon the proper operation of automated systems. As manual processes are no longer able to address systemic deficiencies, reliability and capacity assessments of technology systems become more vital.

In December of 1999, just prior to the transition to Year 2000, certain regulated entities entered into arrangements with the Commission under which they would provide periodic reporting of technology plans and progress and immediate reporting of significant systems disruption or outages. This arrangement, called the Systems Reporting Protocol, was the first step in the process of developing a more comprehensive ARP.[2]

To supplement the reporting defined in the Systems Reporting Protocol, Commission staff ("Staff") believe that periodic independent reviews are required. Further, Staff should address follow-up issues and review major initiatives in a collaborative manner.

The Program is intended to provide Staff with essential background and current

---

[1] See Financial Crisis Management: Four Financial Crises in the 1980s (May 01, 1997, GAO/GGD-97-96). It provides a very clear impact analysis of the 1987 Market Break on the financial markets. The potential for financial disaster from the 1987 Market Break is clearly described. This GAO Staff study can be found on the GAO web site: www.gao.gov.

[2] This ARP (Program) document considered the work of the U.S. Securities and Exchange Commission ("SEC") in its ARP (Policy) statements, published in response to severe operational difficulties experienced during the 1987 Market Break. The first being Securities Exchange Act Release No. 27445, Policy Statement: Automated Systems of Self-regulatory Organizations, (November 16, 1989), 54 FR 48704 ("ARP Statement I") and the second being Securities Exchange Act Release No. 29185, Policy Statement: Automated Systems of Self-regulatory Organizations (II), (May 9, 1991), 56 FR 22489 ("ARP Statement II"). These are found on the SEC web site: www.sec.gov.

information relevant to regulatory oversight. In establishing the scope of the Program, Staff are mindful of maintaining a balance between minimizing the costs and disruption to the Entity in complying with the Program and ensuring that the OSC can effectively pursue its mandate.[3]

This paper discusses the Program. The ARP will be tailored to particular institutions and, over time, to changes in the industry.

There are three components to the ARP.

1. Systems Reporting Procedure ("SRP")

Building on the Systems Reporting Protocol, the SRP provides the Commission with information on material production system outages and other problems, planned major production system changes and recent production system changes. The SRP calls for reporting significant incidents on a timely basis and for reporting other information on a periodic basis.[4]

2. Independent System Review ("ISR")

The ISR will be completed by an independent auditor or consultant with appropriate qualifications or, with agreement from the Commission, by the Entity's internal audit group. The initial review will cover a set of general information system control areas. The scope of subsequent reviews will be established jointly in order to maximize the benefits to both the Entity and the Commission. The format of the report is subject to discussion and may take the form of an internal management report or a formal opinion report.[5]

3. System Examination Module

The System Examination Module extends the general examination process performed by the Commission from time to time on Entities. It will involve an examination of the Entity's systems and procedures, with a focus on one or more particular systems-related issues for any given exam. Typically, a System Examination Module will include: i) the exploration of some specific operation of the Entity; ii) the review of any specific regulatory concerns or marketplace complaints; iii) the monitoring of ARP compliance; and iv) follow-up items (with questions and issues that have not been fully addressed) arising from the SRP or ISR components.[6]

---

3 See discussion under *Constraints* at page 5.

4 See PART II. SYSTEMS REPORTING PROCEDURE at page 8 for an elaboration of this component.

5 See *PART III. INDEPENDENT SYSTEM REVIEW* at page 11 for an elaboration of this component.

6 See *PART IV. SYSTEM EXAMINATION MODULE* at page 15 for an elaboration of this component.

Specific reporting, review and examination details are tailored to the nature of the Entity's business and reflect any known risks to trading, clearing and settlement and to the level of regulatory oversight provided by the Commission.

B. Purpose of the Automation Review Program

The Program provides Staff with essential information on an Entity's systems in terms of allowing Market Regulation to more effectively monitor serious incidents.[7] It provides a mechanism to encourage Entities to follow a formal methodology in identifying and managing IT risk. The goal is to encourage the use of industry "Best Practices".

Further, the Program provides the Commission with a mechanism to follow up on outstanding issues and to better understand the operation of the Entities while minimizing disruption to them.

The Program has been designed to address two additional objectives: i) to provide a framework for the regulatory oversight of systems capacity and reliability; and ii) to help strengthen the Entity's own internal processes through the benefits gained in responding to the ARP.[8]

C. Constraints

While the Commission has a regulatory oversight mandate, there are practical limits in the application of this mandate with respect to an Entity's operations. Some factors include:

1. The practical implementation of ARP must strike a balance between: i) minimizing the costs and disruption to the Entity in complying with the Program; and ii) ensuring that the OSC can effectively pursue its mandate.
2. The Entity is on the "front line", directly involved with providing a high quality service to market participants. While drafting the ARP, consideration has been given to ensuring that daily operations have priority over addressing routine reporting matters, with no material impediment to regulatory oversight.
3. Requiring information or processes without a clear and valid purpose serves to reduce the effectiveness of the ARP process.

---

[7] See *Role of Market Regulation* at page 6.

[8] For example, the Entity can obtain significant benefit from the ISR by reducing its own risk and addressing opportunities for improvement. The real benefit of such reviews comes from the internalization by the Entity of review recommendations.

To lessen the disruption to an Entity, the System Examination Module has been structured to enable Staff to assemble outstanding issues, so that such issues can be addressed together. The intent is to minimize disruption by consolidating various issues of regulatory interest into a single examination.

D. Discussion

1. Regulated Entities

For purposes of the ARP, Entities will include recognized stock exchanges, recognized commodity futures exchanges, recognized quotation and trade reporting systems, and recognized clearing and settlement systems.[9] In addition, certain Alternative Trading Systems ("ATSs") which meet the threshold tests discussed in National Instrument 21-101 Marketplace Operation and Companion Policy 21-101CP.[10] "Information Processors", "Market Integrators"[11] and other organizations may be considered Entities.

2. Role of Market Regulation

Market Regulation's role in the Ontario capital markets includes:

- supervising and monitoring the activities of the Entities (oversight);
- identifying the potential for systemic risk and emerging issues; and
- identifying necessary regulatory responses to such risks and issues.

3. Addressing Risk

A hierarchy of risks, ranging from the impact of the failure of an individual dealer or trading or clearing and settlement system, to the failure of a whole market, whether domestic or global, must be addressed.[12] Because of the impact that significant systems failures may have on the investing public and financial markets, Staff believe that it is appropriate for the Entities to take certain steps to ensure that their automated systems have the capacity to accommodate current and reasonably anticipated future trading volumes and to respond to localized emergency conditions.

While on the whole, technology has been successfully used to mitigate a variety of

---

9 Through arrangements entered into with securities regulatory authorities in other jurisdictions, the ARP may be applicable to exchanges, quotation and trade reporting systems and clearing and settlement systems that are not necessarily recognized or formally regulated by the Commission.

10 (2001) 24 OSCB 6591

11 The terms "Information Processor" and "Market Integrator" are defined in National Instrument 21-101.

12 The strong linkage between the securities industry and the financial systems was demonstrated by the market break of 1987.

risks arising from traditional market practices, a new type of risk arises due to the high level of integration of financial systems. This operational risk, a dependency on technology that may fail under stress, may increase with greater integration to come from initiatives such as STP. The risk is a concern because computer systems are less adaptive to unusual conditions than humans: an isolated problem not anticipated during one system component's design can result in the disruption of the entire automated process. It is Staff's view that good systems design and thorough testing are important risk-mitigating factors. These considerations are included in the ISR, and in the System Examination Module if appropriate.

To address risk as part of a plan, it is Staff's view that Entities should: i) establish reasonable current and future capacity estimates for each major system; ii) conduct periodic capacity stress tests with market participants; and iii) address potential market disruptions through appropriate contingency planning.[13]

E. Confidentiality of Entity Material

All materials provided under the ARP that the Entity considers as non-public and confidential should be clearly marked "Confidential". It is the intention of the Commission to treat such information as non-public and confidential.

F. ARP Process Implementation Methodology

A separate, tailored, document ("*ARP Implementation at [Entity-name]*") provides specific information on implementation of the ARP for the Entity, including, for example, exact times frames of reports (reporting periods), report details and designated Staff contacts.

The implementation of the various reports, reviews and examinations will be phased in over time for each Entity new to the process. If appropriate, the Program will be customized for each Entity, through this separate document, to reflect the circumstances of the Entity.

---

[13] These topics are addressed in more detail in Part III *ISR Scope* at page 12.

PART II. SYSTEMS REPORTING PROCEDURE

A. Introduction

The SRP calls for two types of reports: *"Periodic Reports"* and *"Exception Reports"*.

i. **Periodic Report.** These are regular reports that provide a summary of plans, changes and incidents.
ii. **Exception Report.** These are incident reports that provide notification at the time of a material event or a serious outage or issue.

For certain incidents, an additional written, detailed follow-up report may be requested by Staff.

B. Purpose of the System Reporting Procedure

The SRP is intended to support the OSC in its regulatory role. If a regulatory response to an emergency situation is required, Staff must have relevant information in order to fully assess the situation. In addition, Staff must be in a position to promptly respond to any public enquiry concerning the situation or provide any regulatory response required of the Commission.

C. Scope

Under the SRP, the Entity will report on significant events and provide periodic summary reports. The scope of the reported information should be consistent with that normally available to the organization's senior management.

The reporting requirements should not cause any adverse impact on the Entity's business, as the SRP process can be readily incorporated into the Entity's internal management escalation procedures. Staff are prepared to accept the Entity’s internal management reports.

D. SRP Periodic Report Description

A Periodic Report is a written report for a given period that will include the following three components:

i) a summary of planned major systems changes for the coming period;
ii) a summary of major systems changes during the reporting period; and
iii) a summary report of all systems incidents during the reporting period.

1. Production Plan Summary

This outlines management-level plans for major systems changes in the following period. This would include information on new or significantly changed production processes. This information can be part of the planning management information summary normally completed by the organization before production systems or processes are changed.

The scope would include planned material changes to production hardware/ software/connectivity systems or processes. Also to be included is a discussion of any important risk factors, such as introduction of new technology or planned changes that would require formal industry testing for a new major initiative.

Staff may request additional information. For example, a summary of industry testing, implementation and fallback plans.

2. Production Change Summary

This outlines major systems changes in the reporting period. The scope would also include previously reported, planned material changes to production hardware/software/connectivity systems or processes.

3. Production Outage Summary

This part of the Periodic Report contains a list of all outages, material delays and slowdowns and other important systems events which occurred during the reporting period.

4. Reporting Period

The reporting period for the Periodic Report will vary with each Entity. Staff, in consultation with the Entity, will determine an appropriate reporting period. In determining an appropriate reporting period, Staff will have regard to a variety of factors, including (i) the extent to which the Entity's business or activity is critical to the efficiency and integrity of the Ontario capital markets and (ii) the complexity of the Entity's systems, networks and processes.

E. SRP Exception Report Description

A set of Exception Reports are expected for any significant event related to an Entity's production systems or networks. Exception Reports consist of:

i) Notification Report – to advise the Commission of a material event;

ii) Status Change Report – to advise of a significant change of status;

iii) Resumption of Service Report – to advise of a return to normal service;

iv) Final Summary Report – summary of the incident as of one day after resolution of the incident; and

v) Final Detailed Report - optionally requested by Staff for final resolution of problems or additional detailed information.

1. Exception Report Submission

If the event is a significant systems outage or other event described below, it should be reported promptly. (All events that occurred during a particular reporting period should be noted in the Periodic Report for that period.) As material changes in status occur, including return to normal service, these too should be promptly reported. A final written report will provide a summary of the incident.

All of the above reports, with the exception of the Final Summary Report and the Final Detailed Report, may be communicated orally to a designated Staff person or transmitted via email to the list of designated Staff persons.

2. Exception Report Criteria

An incident should be of a certain degree of severity for it to be reported through the exception reporting procedure. The determination of the severity of an event is made by the Entity and should relate to the impact that the loss of service will have on the Entity's members or users or on market participants generally. For example, users of online systems are more sensitive to outages and delays. However, it should be noted that some entities have batch processes which are time-critical. To be clear, an Entity should report to Staff any incident that has been reported, or is reasonably expected to be reported, to the press or to the Entity's members, users or participating organizations.

Conditions for which an incident should be reported include: delays and outages over a certain duration, serious security incidents or threats, or incidents causing the Entity to operate from a backup system or site.

PART III. INDEPENDENT SYSTEM REVIEW

A. Introduction

An Independent System Review should be performed by the Entity on a periodic basis. This review will typically be performed by an independent auditor or consultant with appropriate industry and technology expertise. The review may, with the Director's[14] prior approval, be performed by the Entity's Internal Audit group. If the review is performed by Internal Audit, the Entity will need to engage an independent auditor to attest to the independence and skills of the audit team performing the work and to the quality and completeness of the review.

B. Purpose of the Independent System Review

The purpose of the Independent System Review is to provide the Commission with assurance that the Entity has:

- A system of internal controls in place that is consistent with best practices of the industry, and
- Procedures in place to appropriately identify and address risk issues as they relate to the Entity's technology environment.

C. Type of Report

The type of report to be issued will be discussed and jointly agreed to by Staff and the Entity. If the Entity already engages an auditor to perform an independent system review (such as a CICA Handbook Section 5900 review[15]), such review, as currently provided or with certain modifications, may meet the needs of the Commission.

When the Entity does not currently arrange for an independent system review, a 'management report' will typically be expected, at least for the initial review. A management report does not include an audit opinion. Rather, within the defined scope (discussed below), the report will identify the major internal controls in place, identify any control weaknesses or deficiencies, assess the risks and implications of each weakness, and provide a practical recommendation for correcting the weakness.

---

[14] "Director", as defined in the Ontario Securities Act.

[15] A Section 5900 Review is an examination performed by external auditors, usually once a year of an Entity's controls under Section 5900 of the *Canadian Institute of Chartered Accountants' Handbook*, *Opinions on Control Procedures at a Service Organization.*

This report will provide the 'baseline' for future reviews. The Entity and Staff will jointly determine whether subsequent reviews will continue to use a management report format or take the form of an opinion report such as a Section 5900 or SysTrust[16] report.

D. Scope

The following matters relate to the scope and delivery of the review.

1. ISR Methodology

Independent auditors and consultants will likely have their own audit methodology to perform this type of review and Staff will not attempt to establish standards in this regard. When the review will be communicated as a management report, auditors are encouraged to structure the defined scope around a set of relevant control objectives such as those found in the Canadian Institute of Chartered Accountants publication, *Information Technology Control Guidelines.*

2. ISR Scope

The initial review and resulting management report will typically address each of the following areas:

- Operations and performance evaluation including the existence and adequacy of processes to establish, measure and assess acceptable computer and network operations performance;
- Capacity planning and measurement including a review of the processes in place to address the adequacy of current capacity, performance testing and future capacity requirements in light of changing market conditions;
- Change management including the adequacy of the controls in place to ensure sufficient design, planning and testing is carried out to minimize any unexpected impact of changes on operations and on other market participants;
- Problem management including processes in place to determine the nature and extent of problems, assess their impact on system and market performance, escalate issues to senior management, provide prompt and effective notification to market participants, implement necessary repairs quickly and determine necessary steps to prevent a future reoccurrence; and

---

16 *"The SysTrust℠ service is an assurance service developed … to increase the comfort of management, customers, and business partners with the systems that support a business or a particular activity. …* [by testing and evaluating] *whether a service is reliable when measured against four essential principles: availability, security, integrity, and maintainability."* AICPA/CICA SysTrust Principles and Criteria for Systems Reliability, Version 2.0, at page 3, published jointly by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants.

- Contingency planning including plans and procedures in place for incident recovery, disaster recovery and business continuity planning, the adequacy of testing undertaken to ensure the feasibility of these plans and the process for assessing contingency risks.

The review should also include the timeliness and effectiveness of procedures to notify market participants.

The scope of subsequent reviews will be determined in such a way as to maximize the benefits to both the Entity and the Commission. These reviews may focus on specific general control areas and may include an assessment of one or more systems. If a SysTrust report is planned, the scope will need to be consistent with that standard.

3. Consultation with Market Participants

As part of its independent review, the auditor may wish to consult with certain market participants such as users of the Entity's services, information vendors, service providers and clearing and settlement facilities. This may be appropriate in order to complete the assessment of the scope issues noted above that involve other market participants.

Two areas of communication with market participants for specific consideration are: i) communication of planned system changes; and ii) notification of availability of services.

The Entity should have plans and procedures for system changes that include: i) an analysis of the business and technological implications of the proposed changes on the market participants prior to approval and implementation; ii) coordinating the impact of the changes on the participants; and iii) obtaining, where possible, agreement from market participants on schedules for testing and implementation.

Since interruptions of service are risks with all technologically based systems, market participants need an effective mechanism for notification of a serious event and the corrective action being taken.[17] This notification should include a description of the impact on market participants. Since the Entity is more likely to be effective in communications with the larger participants, the Commission is particularly interested in the quality of communications provided to smaller participants.

4. Scope Limitations

It may be necessary for the auditor to consider any limitations in scope resulting

---

[17] For example, "all orders/trades from <time> must be re-entered".

from the decentralized environment within which the markets operate today. That is, some networks and systems accessed or used by the Entity may not be proprietary. The auditor should not be limited in scope to those systems and processes that are within the exclusive "control" of the Entity. At the same time, any scope limitations due to lack of access or other reasons need to be clearly identified.

5. Independent Attestation of Internal Review

If an Entity has an Internal Audit group with the appropriate skills and experience, this group may undertake the review, with the Director's prior approval. In such case, the report must be accompanied by an "attestation" from an independent auditor. The attestation is an opinion of the independent auditor attesting to: i) the adequacy of the qualifications and objectivity of the internal reviewer to conduct the review; ii) the completeness of the review in addressing the agreed scope; and iii) the appropriateness of the review methodology for the subject matter.

6. Entity Response Content

When the results of the review are communicated as a "management report", the management of the Entity should consider the report and prepare a "response" that is either attached to the report or is incorporated into the body of the final report. For each deficiency identified and related recommendation, the response should include:

- The Entity's position on the deficiency and related recommendation (i.e., whether or not there is acceptance of the issue raised and the degree of acceptance of the respective recommendation);

- The Entity's response to the recommendation. If in agreement, the Entity should set out the action plan and the implementation timetable. If not in agreement, the Entity should include a short discussion of the impact (risk) of not implementing the recommendation, and how the impact of not implementing will be addressed (i.e., how the Entity will mitigate the potential impact).

PART IV. SYSTEM EXAMINATION MODULE

A. Introduction

The System Examination Module forms part of a compliance review or other examination of the Entity performed by Staff. It will involve an examination by Staff, or a consultant obtained by the Commission, of the Entity's systems and/or procedures with a focus on one or more particular systems-related issues for any given system examination.

During the ongoing operation of the Entity's operation, a variety of issues may arise. The important issues will be addressed immediately, but inevitably some issues will need follow-up.

Occasionally, an Entity will modify its systems and operations but will fail to provide necessary details to the Commission, the necessity of which will only become apparent later. Staff may also become aware of a potential regulatory concern.

A system examination may include any combination of the components outlined below.

B. Purpose of the System Examination Module

The System Examination Module provides the Commission with:

- The opportunity to ensure outstanding issues are systematically addressed while minimizing any disruption to the Entity’s operations;
- The ability to obtain additional in-depth information regarding the Entity's operations and procedures; and
- The opportunity to follow up on outstanding issues.

C. Scope

A system examination in a given year may range from an in-depth review of one or more topics to a follow-up memorandum or meeting.

1. Examination Strategy

A system examination may include:

- A formal examination at the request of the Commission or Director;
- A presentation by the Entity to Staff on a particular topic;
- An informal meeting to discuss previously identified issues;
- An in-depth review of one or more specified issues; and
- A follow-up memorandum.

A system examination schedule will be determined by Staff in consultation with the Entity, to define the frequency of such examination. Serious outages, data integrity, security or regulatory issues may also trigger a system examination.

2. Topics/Components

The range of topics governing a system examination may include the following items:

a) Follow-up items

- Outstanding questions or issues on any serious incidents (reported under the SRP)
- Outstanding questions and issues based on Commission inquiries

b) Exploration of some specific operation

- Request for information on a new or changed function or feature
- Request for information on a function or feature where Staff require additional understanding of the operation
- Request for clarifying information where the Entity has requested a Commission response

c) Review of any specific regulatory concerns

- Questions or issues based on complaints from market participants
- Questions or issues where Staff or the Commission have identified possible regulatory concerns
- Conversely, the Entity may wish to use this process as an opportunity to informally discuss its own market integrity concerns with Staff

d) Compliance with ARP

- Outstanding questions or issues on the results of an Independent System Review
- Review of the Entity's performance of capacity planning, contingency planning or other ARP concern
- Review of incidents and system changes[18]

[18] The intention is to confirm the level and appropriateness of SRP reporting.

3. System Examination Report Description

There is no formal report unless one is specifically requested by the Director.

D. Process Outline

1. Planning

The System Examination Module is intended to be coordinated with other OSC examinations being performed during a given year. Staff will determine specific examination objectives to apply to a particular system examination.

2. Examination Process

If some aspect of the examination is not fully understood or further issues arise, a follow-up examination may be scheduled. If a system examination detects serious discrepancies, Staff will meet with management of the Entity to review the issues and possible solutions. This may be followed by a re-examination once corrective action has been completed or additional material is available.