OPERATIONAL CAPABILITY TECHNOLOGY QUESTIONNAIRE

Please provide all relevant documents responsive to the information requests listed within each area below. In addition to the specific documents requested, please provide any other policies, procedures, standards or guidelines, plans, independent assessments (including internal audits), test results, and representations that will assist the Commission in assessing the degree to which: the proper function and adequate security and capacity of automated trading systems and related systems such as those used for dissemination of market data and recording and safe storage of audit trail information is ensured; that appropriate principles for system oversight and risk analysis to identify and minimize sources of operational risk by means of appropriate controls and procedures are followed; and that periodic, objective testing and review of those systems is conducted.

A. Organizational Structure, Facility Locations and Geographic Distribution of Staff and Equipment

1. Please provide high-level organization charts and staffing level information for all groups that are directly involved in supporting the development, operation and maintenance of the system, including information technology, computer operations, network and telecommunications, information security, quality assurance, capacity planning, contingency planning (including disaster recovery), technical call center staff , and market operations.

2. Please describe or provide a diagram showing the locations of all facilities that house the staff described above and the equipment on which your system operates. Please indicate the nature of the facilities (e.g., headquarters, primary and backup data centers, primary and backup market operations centers, etc.), and a description of your rationale for the distribution of staff and system components across those facilities.

B. System Description and Development Activities

1. Please provide the following information for the system (including information regarding interfaces to the clearing system, surveillance systems, quote vendors and any other essential service providers):

   a. System description and overview.

   b. A logical diagram of the software components, including the following information for each component:
      1) Name.
      2) Functional description, including upstream and downstream feeds.
      3) Measure of redundancy of component hosts at both production and DR locations (e.g., N+1, where N represents the minimum number of hosts required).

4) Essential support software for the component (name and purpose).

c. A high-level application flow diagram.

d. A representative physical diagram of the hardware components (servers and communications equipment) that shows the placement of the hardware and software components at both the primary and backup data centers, and for each hardware component, provide the following information:

1) Device type (e.g., switch, server, SAN, etc.).
2) Device O/S and version.
3) Functional description.
4) Internal redundancies (e.g., power supplies, RAID).
5) External redundancies (e.g., mirroring, clustering).
6) Essential support software (names and versions) if different than software listed in B(1)(b)(4) above.

e. A physical diagram of the network topology within and between data centers and external entities, and for each external connection provide the following information:

1) Purpose(s) of connection.
2) Type and bandwidth of each connection.
3) Description of any redundancies.

f. A description of and schedule for the significant data processing jobs occurring each week (e.g., data and system backups, data transmissions to clearing and surveillance systems).

C. Functional Capabilities

1. Please provide information regarding the functional capabilities of your system for each of the following areas:

a. Edit and validation controls for participant transactions.
b. Placement and display of quotations and indications of interest.
c. Order placement (types, limits, modification, cancellation).
d. Order management.
e. Prioritization and execution of orders (i.e., the order-matching algorithm).
f. Account and member management.

2. What functions are restricted to a specific class of market participant and why?

D. Physical Security and Environmental Controls

1. Please provide information regarding the physical security controls used in the communications and central computer facilities to protect system components and critical infrastructure. In your response, please address:

    a. Perimeter and external building controls and monitoring, including:

        1) Lights.
        2) Cameras.
        3) Motion detectors.
        4) Guards.
        5) Fences, gates, and other barriers.
        6) Building entrances, including loading docks.

    b. Internal building controls and monitoring, including:

        1) Guards.
        2) Metal detectors.
        3) Door locks.
        4) Visitor controls, including scheduling, identification, logbooks, and escort requirements.
        5) Compartmentalization of computing, communications, and building infrastructure equipment.
        6) Cameras, video recording, and monitoring stations.
        7) Access authorization and review procedures.
        8) Mail and package handling procedures.

2. Please provide information regarding the environmental controls used in the communications and central computer facilities to protect system components and critical infrastructure. Please address redundancy, monitoring, maintenance, and testing of:

    a. Electrical supply, including:

        1) Sources and paths of commercial power.
        2) Generators (and associated on-site fuel supply and fuel delivery contracts).
        3) Power distribution units.
        4) Uninterruptible Power Supply units.
        5) Emergency shutoff controls.

    b. Cooling equipment, including:

        1) HVAC units.
        2) Air handlers.
        3) Chillers.
        4) Other associated items such as water supply and humidifiers.

c. Fire control equipment, including:

1) Smoke and heat detection.
2) Fire suppression.
3) Water damage protection.

E. Logical Security

1. Please provide a logical security architecture diagram and description.

2. Please provide information regarding the access controls and procedures that are used to ensure the identification, authorization, and authentication of system users.

3. Please provide information regarding the procedures that are used to ensure proper account management, including:

a. Establishing, changing, reviewing and removing accounts (including emergency and other temporary accounts).
b. Maintaining user awareness of the authorized uses of the system.

4. Please provide information regarding the administrative procedures (such as adherence to least privilege and separation of duties concepts) and automated system that will be employed to prevent and detect the unauthorized use of the system.

5. Please provide information regarding the use and management of safeguards and security tools used to protect the critical data and system components, including:

a. Encryption and data compression.
b. Denial of service protection.
c. Firewalls
d. Routers.
e. DMZs and network segmentation.
f. Intrusion detection.
g. Event logging and log analysis.
h. Virus protection.

6. Please provide information about your incident handling program, including:

a. Staffing.
b. Training.
c. Procedures (including detection, analysis, containment, and recovery).
d. Communication/notification and reporting.
e. Testing.

7. Please provide policies, guidelines, and procedures for authorization and use of remote operations facilities.

8. Please provide information about your procedures for sanitation of equipment and media.

F. Risk Assessments and Other Reviews

Principle 5 of the IOSCO Principles states that "Before implementation and on a periodic basis thereafter, the system and system interfaces should be subject to an objective risk assessment to identify vulnerabilities which may exist in the system design, development, or implementation." The scope of the risk assessment must include each of the areas noted in request 1 below.

In addition, parts 38 and 39 of the Commission's regulations include guidance for Core Principle 9 (for DCMs) and Core Principle I (for DCOs) that calls for review of automated systems to be "performed by a qualified independent professional" (i.e., those parties responsible for either development or operation of the system are not the same individuals who conduct the review).

Given the broad scope of the areas for which risk assessments are required, it is expected that those assessments may have been conducted by various parties at different times. It is further expected that, as implied in the paragraph above, some of those assessments may have been conducted by qualified independent internal staff. Please respond to the following requests keeping that guidance in mind.

1. Please provide the following risk assessment documents:

   a. Data center – including physical security, environmental controls, facilities management, and change management.

   b. System Development Life Cycle, including:

      1) Specification.
      2) Software change management.
      3) Software testing.
      4) Issue tracking.
      5) Release management.
      6) Documentation.

   c. System security measures, including:
      1) Access controls.
      2) Configuration management.
      3) Patch management.
      4) Vulnerability scanning.
      5) Intrusion detection.
      6) Log management.

d. Capacity testing.

e. Problem identification, reporting, and resolution.

f. Development and maintenance of essential documentation.

g. Disaster recovery.

2. Please provide copies of:

a. Your most recent independent risk assessments.
b. Management's responses to the findings of those assessments.

3. Please provide copies of your mitigation plans for addressing the vulnerabilities identified by those risk assessments.

4. Please provide documentation (policies, standards, guidelines) that attests to the development of and adherence to an ongoing information security program whose purpose is to minimize future information security risks.

5. Please provide other system assessments (e.g., vulnerability scanning, penetration test, capacity and performance test) or audits that were recently performed. Include reviews done by internal audit or quality control departments, independent accounting firms, and other third parties.

G. Internal Controls for Operations

Please describe your plans and schedule for ongoing independent reviews, including roles and responsibilities for selection of review areas, scheduling, conducting, reporting, and responding to the findings.

1. Personnel

a. Please provide information regarding the controls and procedures that will be used to ensure that:

1) Appropriate background investigations are conducted prior to assigning personnel to sensitive roles.
2) Periodic recurring background investigations are conducted for staff in sensitive roles.
3) Personnel are aware of, receive appropriate training for, and formally acknowledge their security responsibilities.
4) Access privileges (logical and physical) are reviewed when personnel are reassigned or terminated.

2. Configuration Management

    a. Please provide information regarding the controls and procedures that will be used to ensure:

        1) Consistent inventory maintenance.
        2) Adherence to standards for baseline configuration.
        3) Pre-installation testing and authorization.
        4) Pre-change testing and authorization.
        5) Post-installation and post-change monitoring.

3. Software change management

    a. Please provide information regarding the controls and procedures that will be used to ensure the integrity and reliability of system and application software, including:

        1) Justification for change.
        2) Unit and integration testing.
        3) Independent review for quality assurance.
        4) Approval for production installation.
        5) Post-change monitoring.
        6) Separation of duties.

4. Patch management

    a. Please provide information regarding the controls and procedures that will be used to ensure the timely application of essential patches, including:
        1) Staffing.
        2) Analysis.
        3) Testing.
        4) Implementation and fallback procedures.
        5) Communication and reporting.

5. Event and problem management

    a. Please provide information regarding the staffing, procedures, and controls that will be used to ensure the timely notification about operational events and resolution of operational problems, including:

        1) Identification.
        2) Tracking.
        3) Escalation.
        4) Resolution.
        5) Reporting.

H. Functional Testing

1. Please provide information regarding the testing methodology, including management controls, used to verify the system's ability to function as intended, including all interfaces to external systems such as those used for market information, audit trail, surveillance, and clearing. Please include copies of the two most recent test results (for verification of follow-up actions).

2. Please identify what group is responsible for recording, correcting, and retesting errors, and detail their procedures for those activities.

I. Security Testing

1. Please provide information regarding your use of vulnerability scanning to identify and eliminate vulnerabilities in your computing and communications equipment. Please address each of the following:

    a. Frequency of use.
    b. Methodology and tools.
    c. Distribution of reports.
    d. Remediation of findings.
    e. Tracking of mitigation activities.

2. Please provide the results of the most recent vulnerability scan and management's response and plan of action.

3. Please provide information regarding your use of penetration testing to identify and eliminate vulnerabilities in your computing and communications equipment. Please address each of the following:

    a. Frequency of use.
    b. Methodology and tools.
    c. Distribution of reports.
    d. Remediation of findings.
    e. Tracking of mitigation activities.

4. Please provide the results of the most recent penetration test and management's response and plan of action.

5. For items 1 through 4 above, if the scanning or testing was performed by someone other than an independent third party, please address the issue of objectivity.

6. Please provide information about any internal password scanning you perform, including:

    a. Frequency of use.

b. Tools used.
c. Scope.
d. Follow-up.

7. Please provide information about any verification testing performed to ensure that security controls are operating as expected.

J. Capacity Planning and Testing

1. Please provide the capacity levels and associated performance (i.e., response time) for each of the following aspects of your system, including at a minimum, target, average daily, historical high, and system stress-tested sustained and peak levels:

a. Simultaneous workstation sessions.
b. Market participant transactions.
c. Trade matches.
d. Quote vendor transactions.
e. Data mirroring transactions.

2. Please provide a list of all products used for monitoring and analyzing capacity and performance metrics for hardware, software, and communications.

3. Please provide copies of guidelines and procedures for the use of each of the products listed in response to item 2 above.

4. Please describe any formal process you employ for the ongoing review of capacity and performance levels.

5. Please describe at what levels the addition of new system resources would be triggered to ensure adequate capacity and performance.

6. Please describe how quickly additional capacity and performance resources could be activated in an emergency situation.

7. Please provide charts depicting your 10 most recent historical high system utilization days, and a description of actions taken to mitigate any resulting systems performance issues.

K. Business Continuity and Disaster Recovery ("BC-DR")

1. Please provide the following information:

a. A description of your DR sites, including the following information for each site:

1) State of readiness (hot, warm, cold).

2) Whether a commercial or self-managed site.
3) Location.
4) Distance from production site.

b. A description of the public infrastructure supporting each of your BC-DR sites.
c. A list of the mission-critical systems that each BC-DR site will support on a routine, non-disaster basis, and a description of your reasons for this overall data center strategy.
d. A list of the mission-critical systems that each of your BC-DR sites will support in the event of a disaster.
e. Copies of all agreements, including service level agreements, with third parties to provide services in support of your BC-DR plans.
f. A description of your strategy for ensuring the availability of essential market data, including security and testing of data backups.
g. A description or assessment of the maximum potential data loss in the event of a disaster.
h. A description of your strategy for staffing DR sites in the event of a disaster, including a pandemic.
i. A description of any plans or capabilities for remote management and operation of your primary or DR sites in the event that they become inaccessible but remain functional.
j. Any third party or internal audit assessments of your BC-DR arrangements or plans, including pandemic plans.
k. Briefing materials for senior management regarding BC-DR and pandemic plans.
l. BC-DR and pandemic training materials prepared for employees.
m. A list of essential documentation and a description of your procedures for ensuring its currency and availability to team members.
n. Your BC-DR plans (including lists of essential functions, staffing assignments, security requirements, recovery procedures, test plans, external dependencies and any pandemic plans.
o. Your Emergency Communications Plan, including emergency contact information.
p. Communications to DCM or DCO members about the BC-DR plans.
q. A description of how your BC-DR plan is coordinated with members' BC-DR plans.
r. A description of your strategy for testing your DR sites, including frequency, types of tests, and scope of staff and market participant involvement.
s. A copy of the most recent SAS 70 Type II report for your DR sites, including, if applicable, any actions taken to remediate findings in the report.
t. A description of the three most recent operational tests conducted with respect to your DR sites, including the results of each test and any "lessons learned."

u. A description of your participation in any industry wide tests relating to BC-DR matters.
v. A description of any instances of activation of your BC-DR plans, and any resulting "lessons learned."

2. What is your recovery time objective ("RTO") for each of the following:

a. Resumption of trading.
b. Completed clearing of transactions executed prior to disruption.
c. Resumption of clearing of new transactions.
d. Resumption of market surveillance.
e. Access to audit trail information and resumption of trade practice surveillance.

L. Outsourcing

1. Please provide a copy of each service agreement for IT support provided to your organization.

2. Describe your process for monitoring the performance of those service agreements, including roles and responsibilities, frequency of review, and remediation of identified deficiencies.

3. What are the expected service levels for responsiveness to the various anticipated problems?

M. Training

1. To what groups (e.g., technical staff, managers, senior executives) do you provide basic security awareness training before authorizing access to the system?

2. How often do you require refresher training?

3. Please identify the roles of personnel that have significant information system security responsibilities and describe the information system security training they are required to complete before being authorized to perform their assigned duties.

4. Please describe the type of training that is provided for the users of the system.