SWAP EXECUTION FACILITY
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 compliance of your trading platform and related supporting systems with Core Principle 14, SYSTEM SAFEGUARDS. Core Principle 14 requires SEFs to: "(1) establish and maintain a program of risk analysis and oversight to identify and minimize sources of operational risk through the development of appropriate controls and procedures and the development of automated systems that are reliable, secure, and have adequate scalable capacity;[1](2) establish and maintain emergency procedures, backup facilities, and a plan for disaster recovery that allow for the timely recovery and resumption of operations and the fulfillment of the responsibilities and obligations of the SEF; and (3) periodically conduct tests to verify that backup resources are sufficient to ensure continued order processing and trade matching, price reporting, market surveillance, and maintenance of a comprehensive and accurate audit trail."

1. Organizational Structure, System Description, Facility Locations, and Geographic Distribution of Staff and Equipment

    a. 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 systems, including systems development, quality assurance, system operations, event management, market operations, network and telecommunications, information security, capacity planning, contingency planning (including disaster recovery), market surveillance, and trade practice investigation.

    b. Please describe or provide a diagram showing the locations of all facilities that house the staff described above and the equipment on which your systems operate. 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.

    c. Please provide a high-level application flow diagram and the specific information requested below for all systems that perform and support trading, price reporting, regulatory reporting, market surveillance, and trade practice investigation:

        1) System description and overview.
        2) A logical diagram of the software components, including the following information for each component:

[1] A SEF's program of risk analysis and oversight with respect to its operations and automated systems should address each of the following categories: (1) Information security; (2) Capacity and performance planning; (3) System operations (including configuration management, event management, and incident response); (4) Systems development methodology (including security controls requirements, software change management, and quality assurance) and outsourcing; (5) Business continuity and disaster recovery, including pandemic planning; (6) Enterprise risk management and internal audit; and (7) Physical security and environmental controls.

a) Name;
b) Functional description; and
c) Upstream and downstream feeds.

3) A representative physical diagram of the hardware components (servers and communications equipment) that exist at both the primary and backup data centers, and for each **representative** hardware component, provide the following information:
a) Device type (e.g., switch, server, SAN, etc.);
b) Device O/S;
c) Functional description;
d) Internal redundancies (e.g., power supplies, RAID); and
e) External redundancies (e.g., mirroring, clustering).

4) A physical diagram of the network topology within and between data centers and external entities, and for each connection provide the following information:
a) Purpose(s) of connection;
b) Type and bandwidth of each connection; and
c) Identification of carrier.

2. Risk Analysis and Oversight

a. Please describe your IT department's approach for assessing and managing the risks associated with the operation of and changes to your technology infrastructure.

b. Please describe your Enterprise Risk Management program as it relates to IT.

c. Please describe your internal audit program, including:
a. Organizational structure of internal audit;
b. Audit staff qualifications and use of external staff;
c. Controls that ensure independence;
d. Process for development of IT audit plan, including prioritization and allocation of audit resources; and
e. Follow up and resolution of IT audit findings and recommendations.

d. Please provide your most recent audit or other risk assessment documents for each of the following areas, including complete reports (not only executive summaries), management's responses, and mitigation plans and results for addressing findings:
1) Risk management;
2) Systems Development Methodology (including quality assurance and outsourcing);
3) Information security;
4) System Operations, including hardware and software change management, patch management, and event and problem management;
5) Capacity and Performance Planning;
6) Data centers – including physical security, environmental controls, and facilities management; and
7) Business Continuity and Disaster Recovery.

e. Please provide the results of the two most recent internal or 3rd party vulnerability scans (for our assessment of progress made), including complete reports (not only summaries), management's responses, and mitigation plans and results for addressing findings.

f. Please provide the results of the two most recent internal or 3rd party penetration tests (for our assessment of progress made), including complete reports (not only summaries), management's responses, and mitigation plans and results for addressing findings.

g. Please describe your plans and schedule for ongoing independent audits, other risk assessments, and tests.

3. System Operations

a. Configuration Management
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, including hardening;
3) Pre-installation testing and authorization; and
4) Post-installation monitoring.

b. System software change management
Please provide information regarding the controls and procedures that will be used to ensure the reliability of system software, including:
1) Testing;
2) Independent review for quality assurance;
3) Approval for production installation;
4) Post-change monitoring;
5) Separation of duties; and
6) Controlled access to code libraries.

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

d. Event and problem management
Please provide information regarding the controls and procedures that will be used to ensure the timely notification about operational events and resolution of operational problems, including:
1) Staffing;
2) Use of monitoring systems;
3) Tracking and escalation;
4) Resolution; and
5) Reporting.

e. Please provide information about your security incident handling program, including:
   1) Staffing;
   2) Training;
   3) Procedures (including detection, analysis, containment, and recovery);
   4) Communication/notification and reporting; and
   5) Testing.

4. Systems Development Methodology

   a. Please describe your process, including roles and responsibilities, for identifying and approving functional, security, and capacity/performance requirements.

   b. Please describe your software change management process, including quality assurance and issue tracking and resolution.
      1) Please provide information regarding the testing methodology, including management controls, used to verify the system's ability to perform as intended (regarding functionality, security, and capacity and performance requirements).
      2) Please provide copies of current representative samples of your test results documentation.
      3) Please identify what group is responsible for recording, correcting, and retesting errors, and detail their procedures for those activities.

   c. Please describe the documentation required during the development of new software and as part of the software release package for installation, operation, and maintenance.

   d. Please describe the controls in place for promotion of application software into the production environment, including approval, access controls, and post-implementation monitoring.

   e. Please provide a copy of each service agreement for IT development or support currently in place.

   f. Describe your process for monitoring the performance of those development or support agreements, including roles and responsibilities, frequency of review, and remediation of identified deficiencies.

5. Information Security

   a. Please provide documentation (policies, standards, guidelines) that attests to the development of and adherence to an ongoing information security program.

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

   c. Please provide information regarding the controls and procedures that will be used to ensure that:
      1) Appropriate background investigations, including credit checking, are conducted prior to assigning personnel to sensitive roles;

2) Periodic recurring background investigations, including credit checking, are conducted for staff in sensitive roles; and
3) Personnel are aware of, receive appropriate training for, and formally acknowledge their security responsibilities.
    a) To what groups (e.g., technical staff, senior executives) do you provide basic security awareness training before authorizing access to the system?
    b) How often do you require refresher training?
    c) Please identify the roles of personnel that have significant information system security responsibilities and describe the information security training they are required to complete before being authorized to perform their assigned duties.
    d) Please describe the type of training that is provided for the users of the system.

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

e. Please provide information regarding the procedures that are used to ensure proper account management, including:
1) Establishing, changing, reviewing and removing accounts (including emergency and other temporary accounts).
2) Maintaining user awareness of the authorized uses of the system.

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

g. Please provide information (including specific products used, guidelines for use, and roles and responsibilities) regarding the use and management of safeguards and security tools used to protect the critical data and system components, including:
1) Encryption and data compression;
2) Denial of service protection;
3) Firewalls;
4) Routers;
5) DMZs and network segmentation;
6) Intrusion detection;
7) Event logging and log analysis, including:
    a) Scope of log coverage (e.g., production/development; servers/firewalls);
    b) Focus of event details captured (e.g., unauthorized activities, system issues);
    c) Monitoring of system logging alerts (e.g., log failure alert); and
    d) Frequency and level of log review, analysis, and reporting.
8) Virus protection;
9) Encryption and control of portable mobile devices;
10) Encryption and control of portable external media (e.g., USB drives, optical media, external hard drives, etc.); and
11) Data Loss Prevention (DLP) tools.

h. Please provide policies, guidelines, and procedures for authorization and use of remote access capabilities to manage the system, including hardware and software tools that protect the information and system while using those capabilities.

i. Please provide information about your procedures for sanitization of equipment and media.

j. Please provide information regarding your use of vulnerability scanning to identify and eliminate vulnerabilities in the configuration of your computing and communications equipment. Please address each of the following:
   1) Frequency of use;
   2) Methodology and tools;
   3) Distribution of reports;
   4) Remediation of findings; and
   5) Tracking of mitigation activities.

k. Please provide information regarding your use of penetration testing to identify and eliminate vulnerabilities in the architecture and configuration of your computing and communications equipment. Please address each of the following:
   1) Frequency of use;
   2) Methodology and tools;
   3) Distribution of reports;
   4) Remediation of findings; and
   5) Tracking of mitigation activities.

l. Please provide information about any internal password scanning you perform, including:
   1) Frequency of use;
   2) Tools used;
   3) Scope; and
   4) Follow-up.

m. Please provide information regarding the manual and automated processes that will ensure:
   1) fair and equitable trading;
   2) your ability to detect and investigate persons suspected of violating trading rules; and
   3) that information that could be necessary to detect, investigate, and prevent customer and market abuses (i.e., audit trail information) is captured and securely stored for five years.
      a. Identify the specific audit trail information captured, including, but not limited to, telephone, instant messaging, email, written records, and electronic communications within a trading system or platform. Additionally, please describe specifically how audit trail information is linked to a particular transaction or quote.
      b. Describe the controls that provide for reliable collection of audit information, including those that ensure sufficient capacity and alerting of audit failures.
      c. For each copy of the audit trail information, describe the processes that protect the information from unauthorized alteration, accidental erasure or other loss prior to its planned disposal. Include information about:

i. Access controls (physical and logical);
ii. Environmental controls (e.g., fire protection) provided at storage locations;
iii. Schedule and procedures for secure movement of information;
iv. Retention period; and
v. Distance between storage locations.

6. Physical Security and Environmental Controls

a. 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:
   1) Perimeter and external building controls and monitoring, including:
      a) Lights;
      b) Cameras;
      c) Motion detectors;
      d) Guards;
      e) Fences, gates, and other barriers; and
      f) Building entrances, including loading docks.
   2) Internal building controls and monitoring, including:
      a) Engineering and physical security staffing, including shift coverage, minimum qualifications and training;
      b) Metal detectors;
      c) Door locks;
      d) Visitor controls, including scheduling, identification, logbooks, and escort requirements;
      e) Compartmentalization of computing, communications, and building infrastructure equipment;
      f) Cameras, video recording, and monitoring stations;
      g) Access authorization and review procedures; and
      h) Mail and package handling procedures.

b. Please provide information regarding the environmental controls used in the communications and central computer facilities to ensure reliable availability of system components and critical infrastructure. Please address redundancy, monitoring, maintenance, and testing of:
   1) Electrical supply, including:
      a) Sources and paths of commercial power;
      b) Generators (and associated on-site fuel supply and fuel delivery contracts);
      c) Power distribution units;
      d) Uninterruptible Power Supply units; and
      e) Emergency shutoff controls.
   2) Cooling equipment, including:
      a) HVAC units;
      b) Air handlers;
      c) Chillers; and
      d) Other associated items such as water supply and humidifiers.

   3) Fire control equipment, including:
      a) Smoke and heat detection;
      b) Fire suppression; and
      c) Water damage protection.

7. Capacity Planning and Testing

   a. Please provide the capacity levels and associated performance (i.e., response time) for each of the following system activities, including target, average daily, historical high, and system stress-tested sustained and peak levels:
      1) Simultaneous workstation sessions;
      2) Market participant transactions;
      3) Trade matches;
      4) Quote vendor transactions; and
      5) Data mirroring transactions.

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

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

   d. Please describe the methods by which additional capacity and performance resources could be activated in an emergency situation and state how long those processes would take.

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

   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; and
      3) Distance from production site.

   b. A description of the public infrastructure (e.g., water, electric) supporting each of your BC-DR sites, including redundancy, resilience, and physical security.

   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 software and data, including security and testing of 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. Briefing materials for senior management regarding BC-DR and pandemic plans.

k. BC-DR and pandemic training materials prepared for employees.

l. A description of your procedures for ensuring the currency and availability to team members of essential documentation.

m. Your technology-related BC-DR plans, including roles and responsibilities, staffing assignments, recovery procedures, test plans, external dependencies and any pandemic plans.

n. Your Emergency Communications Plan, including emergency contact information.

o. Communications to DCM members about the BC-DR plans.

p. A description of how your BC-DR plan is coordinated with members' BC-DR plans.

q. A description of your strategy for testing your DR sites, including frequency, types of tests, and scope of staff and market participant involvement.

r. A copy of the most recent SSAE16 Type II reports for each of your data centers, including, if applicable, any actions taken to remediate findings in the report.

s. Documentation from the three most recent operational tests conducted with respect to your DR sites, including the test plan, the results report, and the mitigation plan and results.

t. Documentation from your participation in the most recent industry wide test relating to BC-DR matters, including the test plan, the results report, and the mitigation plan and results.

u. A description of any instances of activation of your BC-DR plans, including the results report and the mitigation plan and results.

w. What is your recovery time objective ("RTO") for each of the following:
   1) Resumption of trading.
   2) Completed clearing of transactions executed prior to disruption.
   3) Resumption of clearing of new transactions.
   4) Resumption of market surveillance.
   5) Access to audit trail information and resumption of trade practice surveillance.