TOPIC : SYSTEM AUDIT

Seminar on Audit & Compliance applicable to Stock Broker & Depository Participants

Venue : WIRC, MUMBAI

Date: Saturday, 15th March 2014

Presented by : CA Shardul Shah

Objective / Need

- Identification of Risk
- Maintaining Data Integrity
- To Improve System Effectiveness & Efficiency
- Evaluation of the adequacy of the Security Controls
- Ongoing process of evaluating controls
- Suggest security measures for the purpose of safeguarding assets/resources

Mandate by Regulators

- **Banking Sector – RBI**
- *Capital Market – SEBI & Stock Exchanges*
- *Commodity Market – FMC & Commodity Exchanges*
- *Insurance Industry - IRDA*

Qualifications / Eligibility

- **Qualification**
  - CISA
  - CISM
  - DISA
  - CISSP
- **Eligibility**
  - Minimum 3 years of experience in IT Audit of Securities Market participants Stock Exchange, Clearing Corporation, Depositories, Stock Broker, DP etc.
  - Shall not have any conflict of interest in conducting Fair, Objective and Independent Audit.
  - Directors / Partners shall not related to Stock Brokers

References

Authority	Ref No	Issue Date	Remarks, If Any
SEBI	CIR/MRD/DMS/34/2013	November 06, 2013	System Audit for ALL Brokers
SEBI	CIR/MRD/16/2013	May 21, 2013	Algo System Audit & clarification
NSE	89/2013	November 08, 2013	Trail of SEBI Circular on annual System Audit
BSE	20131107-6	November 07, 2013	Trail of SEBI Circular on annual System Audit
MCX'SX	MCX-SX/CTCL/1570/2013	November 08, 2013	Trail of SEBI Circular on annual System Audit
USE	USE/CMPL/417/2013	November 13, 2013	Trail of SEBI Circular on annual System Audit

Categories

I. **Annual System Audit for Brokers**

- **Who use**
  - Computer-to-Computer Link (CTCL) or Intermediate Messaging Layer (IML), Internet Based Trading (IBT) / Direct Market Access (DMA) / Securities Trading using Wireless Technology (STWT) / Smart Order Routing (SOR) **AND**
  - Presence in >10 Locations or >50 terminals

OR

- Broker who is DP or are involved in offering any other Financial Services

I. **Half Yearly System Audit for Brokers who use**

  - Algorithmic Trading

II. **Once in Two Year – Residual Category**

Timeline

Type	Trading Platform	Frequency	Due Date
1	Exchange Trading Platform (NEAT / BOLT / TWS etc.)	Once in 2 Year	30th April
II	API based Trading Terminals (CTCL/IML/IBT /DMA/STWT/SOR)	Annual	30th April
III	Algorithmic Trading	Half Yearly	30th April & 31st Oct

- Exchanges are instructed to keep track of findings of system audits of all brokers on **Quarterly** basis.
- Update status of Compliance to SEBI.

Scope / Framework (Common)

1. **System controls and capabilities** **(All 3 Type)**
    a. Order Tracking
    b. Order Status/ Capture
    c. Rejection of orders
    d. Communication of Trade Confirmation / Order Status
    e. Client ID Verification
    f. Order type distinguishing capability (Only Type II & III)
2. **Risk Management System (RMS)** **(All 3 Type)**
    a. Online risk management capability
    b. Trading Limits
    c. Order Alerts and Reports
    d. Order Review
    e. Back testing for effectiveness of RMS
    f. Log Management

Scope / Framework (Common)

3. **Password Security** **(All 3 Type)**
    a. Organization Access Policy
    b. Authentication Capability
    c. Password Best Practices
4. **Session Management** **(All 3 Type)**
    a. Session Authentication
    b. Session Security
    c. Inactive Session
    d. Log Management
5. **Network Integrity** **(All 3 Type)**
    a. Seamless connectivity
    b. Network Architecture
    c. Firewall Configuration

Scope / Framework (Common)

6. **Access Controls** **(All 3 Type)**

    a. Access to server rooms

    b. Additional Access controls

7. **Backup and Recovery** **(All 3 Type)**

    a. Backup and Recovery Policy

    b. Log generation and data consistency

    c. System Redundancy

8. **BCP/DR** **(All 3 Type)**

    a. BCP / DR Policy

    b. Alternate channel of communication

    c. High Availability

    d. Connectivity with other FMIs

Scope / Framework (Common)

9. **Segregation of Data and Processing facilities (All 3 Type)**
10. **Back office data (All 3 Type)**
    - a. Data consistency
    - b. Trail Logs
11. **IT Infrastructure Management (All 3 Type)**
    - a. IT Governance and Policy
    - b. IT Infrastructure Planning
    - c. IT Infrastructure Availability (SLA Parameters)
    - d. IT Performance Monitoring (SLA Monitoring)
12. **Exchange specific exceptional reports (All 3 Type)**

Scope / Framework (Type II & III)

1. **Software Change Management** **(Type II & III)**
   a. Processing/approval methodology
   b. Fault reporting / tracking mechanism
   c. Testing of new releases
   d. Version control- History, Change Management process
2. **Smart Order Routing (SOR)** **(Type II & III)**
   a. Best Execution Policy
   b. Destination Neutral
   c. Class Neutral
   d. Confidentiality
   e. Opt–out
   f. Time stamped market information
   g. Audit Trail
   h. Server Location
   i. Alternate Mode

Scope / Framework (Type II & III)

3. **Database Security** **(Type II & III)**
    a. Access
    b. Controls
4. **User Management** **(Type II & III)**
    a. User Management Policy
    b. Access to Authorized users
    c. User Creation / Deletion
    d. User Disablement
5. **Software Testing Procedures** **(Type II & III)**
    a. Test Procedure Review
    b. Documentation
    c. Test Cases

Scope / Framework (Only Type III)

1. **Algorithmic Trading** **(Type III)**
   a. Change Management
   b. Online Risk Management capability
   c. Risk Parameters Controls
   d. Information / Data Feed
   e. Check for preventing loop or runaway situations
   f. Algo / Co-location facility Sub-letting
   g. Audit Trail
   h. Systems and Procedures
   i. Reporting to Stock Exchanges

Executive Summary Report Format

I. For Preliminary Audit

Audit Date	**Observation No**	**Observation**	**Department**	**Status**	**Risk rating**	**TOR Clause**
(1)	(2)	(3)	(4)	(5)	(6)	(7)
Audited By	Root Clause Analysis	Impact Analysis	Suggested Corrective Action	Deadline	Verified By	Closing Date
(8)	(9)	(10)	(11)	(12)	(13)	(14)

Executive Summary Report Format

II. For Follow on / Follow up System Audit

Preliminary Audit Date	Sr. No	Preliminary Observation No	Preliminary Status	Preliminary Corrective Action	Current Finding
(01)	(02)	(03)	(04)	(05)	(06)
Revised Corrective Action	Deadline for revised Corrective Action	Suggested Corrective Action	Verified By	Closing Date	
(07)	(08)	(09)	(10)	(11)	

Any Question?

Thank You

- **Presented : CA Shardul J. Shah**
  - ***B. Com, ACA, CISA (USA), DISA (ICAI), DCL***