System Audit Framework

Audit Process

Following steps would be repeated annually to ensure that the process is comprehensive & effective:

1. The Audit shall be conducted according to the Norms, Terms of References (TOR) and Guidelines issued by SEBI.

2. Stock Exchange / Depository (Auditee) may negotiate and the board of the Stock Exchange / Depository shall appoint the Auditors based on the prescribed Auditor Selection Norms and TOR. The Auditors can perform a maximum of 3 successive audits. The proposal from Auditor must be submitted to SEBI for records.

3. Audit schedule shall be submitted to SEBI at-least 2 months in advance, along with scope of current audit & previous audit.

4. The scope of the Audit may be extended by SEBI, considering the changes which have taken place during last year or post previous audit report

5. Audit has to be conducted and the Audit report be submitted to the Auditee. The report should have specific compliance / non-compliance issues, observations for minor deviations as well as qualitative comments for scope for improvement. The report should also take previous audit reports in consideration and cover any open items therein.

6. The Auditee management provides their comment about the Non-Conformities (NCs) and observations. For each NC, specific time-bound (within 3 months) corrective action must be taken and reported to SEBI. The auditor should indicate if a follow-on audit is required to review the status of NCs. The report along with Management Comments shall be submitted to SEBI, within 1 month of completion of the audit.

7. Follow-on audit, if any, has to be scheduled within 3 months of the Audit to ensure that the corrective actions have been taken.

8. If follow-on audit is not required, the Auditee management has to submit a report of actions taken and evidence of corrections to the Auditors & SEBI within 3 months. This report should include updated Issue-Log to indicate the corrective actions taken, verified by the auditors.

Auditor Selection Norms

1. Auditor must have minimum 3 years of experience in IT audit of Securities Industry participants e.g. stock exchanges, clearing houses, depositories etc. The audit experience should have covered all the Major Areas mentioned under SEBI's Audit Terms of Reference (TOR).

2. The Auditor must have experience in / direct access to experienced resources in the areas covered under TOR. It is recommended that resources employed shall have relevant industry recognized certifications e.g. CISA (Certified Information Systems Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, GSNA (GIAC Systems and Network Auditor), CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium, commonly known as (ISC)².

3. The Auditor should have IT audit/governance frameworks and processes conforming to industry leading practices like CobiT.

4. The Auditor must not have any conflict of interest in conducting fair, objective and independent audit of the Exchange / Depository. It should not have been engaged over the last three years in any consulting engagement with any departments / units of the entity being audited.

5. The Auditor may not have any cases pending against its previous auditees, which fall under SEBI's jurisdiction, which point to its incompetence and/or unsuitability to perform the audit task.

Terms of Reference (ToR)

1. General Controls for Data Center Facilities – It must include
   - Application access – Segregation of duties, Database & Application access etc.
   - Maintenance access – Vendor engineers.
   - Physical access – Permissions, logging, exception reporting & alerts.
   - Environmental controls – Fire protection, AC monitoring etc.
   - Fault resolution mechanism.
   - Folder sharing and Back-up controls – Safeguard critical information on local desktops
   - Incidences of violations in last year & corrective actions taken

2. Software Change Control – It must include
   - User awareness
   - Processing of new feature request
   - Fault reporting / tracking mechanism & process for resolutions
   - Testing of New releases / Bug-fixes – Testing process (automation level)
   - Version Control – History, Change Management process etc.
   - Development / Test/ Production environment – Segregation
   - New release in Production – Promotion, Release note approvals
   - Production issues / disruptions reported during last year & corrective actions taken

3. Data communication / Network controls – It must include
   - Network Administration – Redundancy, Monitoring, breakdown resolution etc.
   - WAN Management – Connectivity provisions for business continuity.
   - Encryption - Router based as well as during transmission
   - Connection Permissions – Restriction on need to have basis
   - Fallback mechanism – Dial-up connections controls etc.
   - Hardware based Signing Process
   - Incidences of access violations in last year & corrective actions taken

4. Security Controls – General office infrastructure – It must include
    - Security Policy & quality of implementation of the same
    - LAN security control and monitoring
    - OS & Database Security controls & monitoring
    - Internet connection controls – Firewall protection, Intrusion Detection System, Access rights and privileges.
    - Virus protection – Controls to mitigate the Virus attacks / Outbreaks.
    - Secured (digitally signed) e-mail with other entities like SEBI, other partners
    - Email Archival Implementation
    - Incidences of security violations in last year & corrective actions taken

5. Access policy and controls

6. Electronic Document controls

7. General Access controls

8. Performance audit – It must include
    - Comparison of changes in transaction volumes since previous audit
    - Review of systems (hardware, software, network) performance over period
    - Review of the current volumes against the last Performance Test performed

9. Business Continuity / Disaster Recovery Facilities – It must include
    - BCP manual, including Business Impact Analysis, Risk Assessment and DR process
    - Implementation of policies
    - Back-up procedures and recovery mechanism using back-ups.
    - Storage of Back-up (Remote site, DRS etc.)
    - Redundancy – Equipment, Network, Site etc.
    - DRS installation and Drills - Management statement on targeted resumption capability (in terms of time required & extent of loss of data)

- Evidence of achieving the set targets during the DRS drills in event of various disaster scenarios.
- Debrief / review of any actual event when the DR/BCP was invoked during the year

10. IT Support & IT Asset Management – It must include
    - Utilization monitoring – including report of prior year utilization
    - Capacity planning – including projection of business volumes
    - IT (S/W, H/W & N/W) Assets, Licenses & maintenance contracts
    - Insurance
    - Disposal – Equipment, Media, etc.

11. Entity Specific Software

12. Any other Item
    - Electronic Waste Disposal
    - Based upon previous Audit report as well as any other specific information given by SEBI

Audit Report Guidelines

The Audit report should have explicit coverage of each Major Area mentioned in the TOR, indicating any Nonconformity (NCs) or Observations (or lack of it).

For each section – auditors should also provide qualitative input about ways to improve the process, based upon the best practices observed

The report should also include tabulated data to show NCs / Observations for each Major Area in TOR.

Fully detailed report should be submitted, along with an Executive Summary in tabulated form including following information:

Issue Log Column Heading	Description	Responsibility
Major Area	Major area/relevant clause in Terms of Reference against which compliance is being audited	Auditor
Description of Finding/ Observation	Describe the findings in sufficient detail, referencing any accompanying evidence (e.g. procedure manual, interview notes, reports *etc*.)	Auditor
Reference	Reference to the section in detailed report – where full background information about the findings are available	Auditor
Process/ Unit	Process or unit where the audit is conducted and the finding pertains to	Auditor
Category of Findings	Major/Minor Nonconformity, Observation, Suggestion *etc.*	Auditor
Audited By	Which Auditor covered the findings	Auditor
Root Cause Analysis	A detailed analysis on the cause of the nonconformity	Auditee
Remediation	The action (to be) taken to correct the nonconformity	Auditee
Target Completion Date for Remedial Action	The date by which remedial action must be/will be completed	Auditor/Auditee
Status	Status of finding on reporting date (open/close)	Auditor/Auditee
Verified By	Auditing personnel (upon verification that finding can be closed)	Auditor
Closing Date	Date when finding is verified and can be closed	Auditor

The Executive Summary should also include an overall comment from the Auditors to indicate if a follow-on audit is required and the time lines of respective corrective action for non conformities.

Further, along with the audit report, the Stock Exchange / Depository shall also submit a declaration from the MD / CEO certifying the integrity and security of IT Systems.