Scope of Work for IT System Audit

With a view to addressing the concerns of the Regulator and other stakeholders, the audit for Information systems security process includes within its scope the following areas:

1. Information security policy

- Review of IS policy
- Review of various procedure documents access management, change management, backup management, incident management etc.

2. Organization of information security

- Review of Roles and Responsibilities of CISO, IT Department
- Review of process in place for notifying and reporting of unauthorized
- disclosure or confidential information breaches
- Review of User activities being captured and monitored
- Review of Access to user granted and provided based on the roles that he
- performs and after adequate authorization

3. Human resource security

- Review of process for background verification for employees
- Review of periodic trainings being conducted for the employees
- Review of access rights disabled and removed for all users on termination of employment
- Review if the terms and conditions after termination of employment or
- contract is defined and communicated

4. Asset Management and Access Control

- Review of maintenance of asset inventory
- Review of Software licenses repository
- Review of Access control matrix defined and approved
- Review of User registration and de-registration procedure
- Review of Remote access to organization's network
- Review of privilege user access
- Review of User access rights
- Review of password management controls

5. Physical Access and Environmental controls

- Data Centre walkthrough and review of adequate physical security and environmental controls
- Review of maintenance of equipment

6. Operations & Cyber Security

- Review of Operating procedures documented and made available to all employees
- Review of Change & Incident management process
- Review of Capacity monitoring of the systems
- Review of antivirus agent is configured to scan
- Review of backup policy and procedure
- Review of encryption of data
- Review of Data Restoration from backup tapes
- Review of VAPT
- Review of User awareness training

7. Network and Communication Security

- Review of Network controls
- Review of process followed to ensure confidentiality and non-disclosure
- Review of Firewall rule review

8. Information security incident management

- Review of Security incident procedure and plan
- Review of incident response plan
- Review of incident monitoring

9. Business Continuity Management

- Review of IT Disaster Recovery Management process
- Review if Processes and controls are defined to ensure required level of business continuity
- Review if Business continuity plans are tested regularly and the BCP drill is conducted