IS Audit Scope

Phase I:

Audit preparedness for Cyber Security & Cyber Resilience Framework.

Phase II:

Policies and procedures -

- Review policy / procedures related to the technology function and environment

1. **IT General & Cyber Security Controls review -**
   - **Logical Access –**
     - Review of user management procedures at Application, Operating System and Database Levels
     - Review of privileged access rights granted to application and system administrators
     - Review of account and password policy controls

   - **Physical & environmental Access Controls –**
     - Review of the procedures implemented at the Data Center (DC) / server rooms for:
     - Assess the critical assets for Environmental Management system.

   - **Change management process & system documentation –**
     - Review the program change management with respect to policy & procedures.
     - Review the procedures for requesting, development, testing and implementing changes.
     - Review the process for monitoring program modifications.
     - Review segregation of duties.

   - **System Maintenance –**
     - Review of Annual Maintenance Contracts (AMCs) / Warranties, Service Level Agreements (SLA)

   - **Event & application Log maintenance –**
     - Review the policies and procedures adopted for reviewing and following-up activity logs

   - **Third party Management–**
     - Review the process for monitoring and reporting on the achievement of third party service level
performance criteria.
     - Review Service Level Agreements(SLA)/Non-Disclosure Agreements (NDA) for the maintenance and upkeep of the systems

   - **Backup & recovery process–**
     - Review Backup related Policies & Procedures and compliance thereof.

   - **Incident Management –**
     - Review Incident Management related Policies & Procedures and compliance thereof.

   - **Exchange of Information –**
     - Review the interparty communication controls relating to exchange of information.

   - **Business continuity management –**

  - ○ Review the Business continuity management related Policies & Procedures and compliance thereof.

- **Compliance –**
  - ○ Perform compliance review vis-à-vis IT regulatory requirements provided by the AMC.

- **Interfaces -**
  - ○ Review controls over interfaces of Canara Robeco with –
    - ▪ Internal Systems
    - ▪ Broker systems (STP/Nifty Files upload)
    - ▪ Custodian / fund accounting systems
    - ▪ R&T agent

- **Security Review –**
  - ○ Security and controls review of Operating systems, SQL Database.
  - ○ Policies & Security review of Firewall, Servers & desktops.
  - ○ Website VAPT assessment

2. **<u>In Scope Applications to be covered:</u>**
   - AMC: Adrenalin, Employee Trading system, O365, SUN Accounting system & Call Management
   - Mutual Fund: Bloomberg – POMS, BTS Interface, Excel Micros, NDS system & Scheme Accounting
   - Fund Accountant – HSBC: IFS – Fund Accounting system
   - R&T – CAMS/Karvy: CRM, Unit processing process
   - Custodian – HSBC/HDFC: Software for Receipt entry & reconciliation

3. **<u>IT Infrastructure to be covered:</u>**
   - Firewall,
   - Servers,
   - Network,
   - Desktops

4. **<u>System software to be covered:</u>**
   - Operating Systems (system software)
   - SQL Database (system software).

5. **Website**
   - Distributor Portal
   - Catalogue Portal
   - Investor Online Portal

6. **<u>Audit to be conducted as per SEBI Circular (SEBI/HO/IMD/DF2/CIR/P/2019/57) dated 11th April 2019:</u>**

Audit Period (F.Y.): 2019-20, 2020-21 & 2021-22

Yearly Audit Schedule:

Stages	Activity	Time Lines
1	Project kick-off Meeting	4th Week of May
2	Planning	1st week of June
3	IT Policy & Procedures Review	2nd week of June
5	Audit Execution	4th week June till 1st week of July
6	Draft report for discussion	3rd week of July
7	Final Report for Management Review	1st week of August