Information System Audit Scope

Information Systems Audit should cover entire Information Systems Infrastructure which includes Servers & other hardware items, Operating Systems, Databases, Application Systems, Technologies, Networks, Facilities, and Process & People of the undernoted locations:

1. **Data Center**
2. **DR Center**
3. **CBS endpoint applications, Servers, Interfaces, Network & Other Devices,**
4. **ATM Switch**
5. **SMS Alert**
6. **3 rd party product & Interfaces**

DETAILED SCOPE OF AUDIT:-
IS Audit should cover entire gamut of computerized functioning as listed above including Internet Banking & functional areas with special reference to the following:

A	**Policy, Procedures, Standard Practices & other regulatory requirements :**	1. Bank's IT Security Policy & Procedures. 2. RBI guidelines on Information Security & other legal requirements. 3. Best practices of the industry including ISACA's Guidelines.
B	**Physical and Environmental Security**	1. Access control systems 2. Fire / flooding / water leakage / gas leakage etc. 3. Assets safeguarding, Handling of movement of Man /Material/ Media/ Backup / Software/ Hardware / Information. 4. Air-conditioning of DC/ DRC, humidity control systems 5. Electrical supply, Redundancy of power level, Generator, UPS capacity. 6. Surveillance systems of DC / DRC 7. Physical & environmental controls. 8. Pest prevention (rodent prevention) systems

C	**Operating Systems Audit of Servers, Systems and Networking Equipments**	1. Setup & maintenance of Operating Systems Parameters 2. Updating of OS Patches 3. OS Change Management Procedures 4. Use of root and other sensitive Passwords 5. Use of sensitive systems software utilities 6. Vulnerability assessment & hardening of Operating systems. 7. Users and Groups created, including all type of users" management ensuring password complexity, periodic changes etc. 8. File systems security of the OS 9. Review of Access rights and privileges. 10. Services and ports accessibility 11. Review of Log Monitoring, its" sufficiency, security, maintenance and backup.
D	**Application level Security Audit**	1. Only authorized users should be able to edit, input or update data in the applications or carry out activities as per their role and/or functional requirements 2. User maintenance, password policies are being followed are as per bank's IT security policy 3. Segregation of duties and accesses of production staff and development staff with access control over development, test and production regions. 4. Review of all types of Parameter maintenance and controls implemented. 5. Authorization controls such as Maker Checker, Exceptions, Overriding exception & Error condition. Authentication mechanism.

		6. Change management procedures including testing & documentation of change. 7. Application interfaces with other applications and security in their data communication. 8. Search for back door trap in the program. 9. Check for commonly known holes in the software. 10. Identify gaps in the application security parameter setup in line with the banks security policies and leading best practices 11. Audit of management controls including systems configuration/ parameterization & systems development. 12. Audit of controls over operations including communication network, data preparation and entry, production, file library, documentation and program library, Help Desk and technical support, capacity planning and performance, Monitoring of outsourced operations. 13. To review all types of Application Level Access Controls including proper controls for access logs and audit trails for ensuring Sufficiency & Security of Creation, Maintenance and Backup of the same.
E	**Audit of DBMS and Data Security**	1. Authorization, authentication and access control are in place. 2. Audit of data integrity controls including master table updates. 3. Confidentiality requirements are met. 4. Logical access controls which ensure the access to data is restricted to authorized users. 5. Database integrity is ensured to avoid concurrency problems.

		6. Separation of duties. 7. Database Backup Management. 8. Security of oracle systems files viz. control files, redo log files, archive log files, initialization file, configuration file, Table space security etc. 9. Password checkup of Systems and Sys Users (default password should not be there) 10. Checking of database privileges assigned to DBAs
F	**Network Security**	**Security architecture of the entire network including :** 1. Understanding the traffic flow in the network at LAN & WAN level. 2. Audit of Redundancy for Links and Devices in CBS Setup. 3. Analyze the Network Security controls, which include study of logical locations of security components like firewall, IDS/IPS, proxy server, antivirus server, email systems, etc. 4. Study of incoming and outgoing traffic flow among web servers, application servers and database servers, from security point of view. 5. Routing protocols and security controls therein. 6. Study and audit of network architecture from disaster recovery point of view. 7. Privileges available to Systems Integrator and outsourced vendors. 8. Review of all types of network level access controls, logs, for ensuring sufficiency & security of creation, maintenance and backup of the same. 9. Secure Network Connections for CBS, ATM and Internet Banking including client/ browser based security.

		10. Evaluate centralized controls over Routers installed in Branches & their Password Management. 11. Checking of VLAN Architecture 12. TCP ports 13. Checking of Firewall Access control List 14. Routers and Switches are using AAA model for all User authentication 15. Enable passwords on the Routers are encrypted form and password comply with minimum characters in length. 16. Local and remote access to network devices is limited and restricted.
H	**Audit of ATM Switch, ATM Card Management, ATM & Internet Banking PIN management**	1. Audit of ATM Switch covering Application, Network Security, Switch Functionality, Interface, Audit Trails, transmission security, authorization, Fallback / fail over procedures, Status Update, compliance to VISA & other standards. 2. PIN Management (Generation & Re-generation etc.) of ATMs and Internet Banking. 3. Adequacy of security defenses. 4. Scalability for expanding network in future & sharing arrangements. 5. Connectivity to other networks 6. Card management (Delivery of cards / PIN, hot listing of cards and reconciliation with settlement agency.) 7. ATM Switch operational controls, & Reconciliation/
I	**Backup & Recovery Testing**	1. Audit of Backup & recovery testing procedures. 2. Sufficiency checks of backup process. 3. Audit of access controls, movement and storage of backup media.

		4. Audit of media maintenance procedures. 5. Security of removable media. 6. Controls for Prevention of Data Leakage through removable media or other means. 7. Media disposal mechanisms and Database archival & purging procedures. 8. Synchronization between DC & DRC databases. 9. DR Services to be up for Branches, as per RTO & RPO of BCP.
K	**Others**	1) Inventory movement controls & maintenance, equipment maintenance and disposal measures, change & configuration management processes, 2) Audit of Logging and monitoring processes, 3) Audit of Delivery channels, 3rd Party Products and various other interfaces NGRTGS, NEFT, NACH, CTS and E-mail Systems which are integrated with the Core Systems.