Information System Audit Scope

Proposals are requested from CERT-In Empaneled Auditor Only

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

1. **Browser Based CBS Solution with Add Modules**
   – Implementation & smooth functioning.
2. **Data Center at Yotta Infrastructure Solutions LLP, Panvel, Mumbai**
3. **DR Center at Yotta Infrastructure Solutions LLP, Noida, Utter Pradesh**
4. **Branches of the Bank – Head Office + 6 Critical Branches + 9 Other Branches**
5. **CBS endpoint applications, Servers, Interfaces, Network & Other Devices,**
6. **ATM Switch & POS, ECOM Operations at ASP Vendor Finacus Solutions Pvt. Ltd.,**
7. **IMPS and Mobile Banking**
8. **SMS Banking**
9. **RTGS/NEFT Bank is primary Member with facility from IFTAS**
10. **UPI**
11. **Web site of the Bank**
12. **Internet Banking View Only**
13. **Postmaster E-mail Solutions from QLC**
14. **SOC Solution**
15. **Patch & Asset Management Solution**

DETAILED SCOPE OF AUDIT:-
IS Audit should cover entire gamut of computerized functioning as listed above & 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. 4. Audit inventory of licenses purchased and number of licenses required as per the licensing policy of the OEM. 5. Whether these licenses are under support from OEM (ATS Renewal has been done regularly), certificate from OEM to be submitted as supporting document. 6. Any short fall in the licenses to be informed to the Bank to regularize the same.
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. Authorization Control such as concept of maker checker, exceptions, overriding exceptions, and error conditions. 2. Authentication mechanism. 3. User Management & Password Management 4. Parameter Maintenance 5. Access rights; 6. Access logs/ Audit Trail generation; 7. Change management procedures including procedures for testing; 8. Documentation of change management; 9. Documentation of Data Centre Operations. 10. Review the implemented functionality of TrustBankCBS Core Banking solution & other applications in all the areas and to ensure correctness of functionality of each module and all modules in totality vis a vis availability of the functionality / features in the version currently implemented in the Bank.

		11. Review CBS & other applications for adequate input, processing and output controls and conduct various tests to verify existence and effectiveness of the controls. 12. Review Revenue Loss if any from the point of view of effectiveness and efficiency of the Applications. 13. Review of all controls including boundary controls, input controls, communication controls, database controls, output controls, and interfaces controls from security perspectives. 14. Review of all Interface of application with other system OR interface of other system with applications for Security, accuracy, consistency and safety. 15. Identifying critical risk areas, control weakness in application systems and recommended corrective actions from security prospective. 16. Identify gaps in the application security parameter setup in line with the bank's security policies and leading best practices 17. 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.
E	**Audit of RDBMS 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 11. DR Site synchronization
F	**Network Security**	1) Router Configuration and security 2) Network access control 3) Hardening of systems, switches and routers. 4) Patch update Management 5) Port based security controls 6) Process control for change management 7) Security incident and management 8) access control for DMZ applications 9) Content filtering for web access and data leakage 10) Password cracking 11) Intrusion detection system testing 12) Network design review from security, integrity and availability point of view. 13) Evaluation of Firewall policy and its implementation.. 14) Audit of Security Implementation of the Network based applications - ATM, Internet Access, Anti-Virus, E-mail, RTGS, etc.

H	**Audit of ATM Switch, ATM Card Management, ATM & PIN management**	IS Audit of ATM center card operational processes with respect to 1) PIN Management 2) Card Management 3) Delivery of ATM cards/ PINs to customers 4) Hot listing of cards 5) Customer dispute resolution 6) Reconciliation within the Bank and with settlement agency/Banks 7) ATM Network Security Architecture Analysis 8) ATM functionality audit, 9) ASP ATM Switch Audit, 10) ATM Switch Reconciliation, 11) Vulnerability analysis of ATM Network, 12) ASP Outsourcing arrangements, 13) ATM Key Management
I	**Mobile Banking**	1) VAPT of Mobile Banking Application 2) To Assess Flaws in Mobile Banking Application & Web hosting Software i.e. Security of web server and Design of the Applications. 3) Attempting penetration through perceivable network equipment/addressing and other vulnerabilities. 4) Checking the ASP Infrastructure for Mobile Banking from VAPT and Security perspective 5) Whether solution architecture provides 24 X 7 availability to customer.

		6) To check whether date and time stamp are appearing correctly on all transactions and reports. 7) Secrecy and confidentiality of Customer preserved. 8) Compliance to RBI Mobile Banking guidelines 9) Any other items relevant in the case of Mobile Banking security. 10) All the guidelines issued by RBI for Mobile Banking are compiled or not.
J	**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. Review of Disaster Recovery Plan and Procedure 9. Log Shipping management 10. Synchronization between DC & DRC databases. 11. DR Services to be up for Branches, as per RTO & RPO of BCP.
K	**RTGS\NEFT Primary Member**	1) RTGS and NEFT System with IFTAS 2) Interface for NEFT and RTGS Server 3) CBS Application RTGS\NEFT modules

L	**Others**	1) CTS System 2) Email System Audit 3) AML (Anti Money Laudering) 4) E-mail Domain .bank.in
M	**Web Site**	1) Web site Security Audit for Web Vulnerabilities 2) Site Quality and Accessibility 3) Data Security 3) Domain migration to .bank.in 5) Web site Changes authentication and trail
N	**Internet Banking View Only**	1) VAPT of Internet Banking View Only Application 2) To Assess Flaws in Internet Banking View Only & Web hosting Software i.e. Security of web server and Design of the Applications. 3) Attempting penetration through perceivable network equipment/addressing and other vulnerabilities. 4) Checking the ASP Infrastructure for Internet Banking View Only from VAPT and Security perspective 5) Whether solution architecture provides 24 X 7 availability to customer. 6) To check whether date and time stamp are appearing correctly on all transactions and reports. 7) Secrecy and confidentiality of Customer preserved. 8) Compliance to RBI Internet Banking View Only guidelines 9) Any other items relevant in the case of Internet Banking View Only security.

		10) All the guidelines issued by RBI for Internet Banking View Only are compiled or not. 11) Domain migration to .bank.in