Audit in Banking Sector

(Chapter - 6 : DISSA Course)

Arijit Chakraborty

August 22, 2021

RBI – Early Waning System (EWS) for Banks

- **A. Operation of Accounts**

- ❑ Bouncing of high value cheques
- ❑ Delay observed in payment of outstanding dues
- ❑ Frequent invocation of BGs and devolvement of LCs
- ❑ Under insured inventory
- ❑ Funding of the interest by sanctioning additional facilities
- ❑ Frequent request for general purpose loans.
- ❑ Frequent ad hoc sanctions
- ❑ Significant increase in working capital borrowing as percentage of turnover

- B. **Concealment or Falsification of documents, Fund diversion**
- Concealment of certain vital documents like master agreement, insurance coverage
- Frequent change in accounting period and/or accounting policies
- Material discrepancies in the annual report
- Poor disclosure of materially adverse information and no qualification by the statutory auditors
- High value RTGS payment to unrelated parties
- Increase in borrowings, despite huge cash and cash equivalents in the borrower's balance sheet
- Not routing of sales proceeds through consortium / member bank/ lenders to the company

IS Audit : FY 20-21

- Name of the Core Banking Application
- (With Version) used by the Bank- Finacle – Version 7.0.25

IT Infrastructure of Bank

Key IT Application List 2020-21

1. Application = Description
2. Finacle 7.0.25 = Core Banking Solution
3. Symantec Client = Security Antivirus
4. Fraud Risk Monitoring Solution= FRM Application
5. Data De-Dup Application= Customer de-duplication
6. SOC Application = Security Operation Center
7. Corporate Mail (E-Interact) = Mail Application
8. CISCO = Router
9. Firewall (HW or SW based) & IDS /IPS= Software based for Desktops
10. Internet Banking = E-Banking server
11. Access Control System = DR and DC and other IT offices
12. ATM CMS= Card Management System
13. SMS Alerts= SMS Server

Purpose of IS Audit

PURPOSE

This RFP seeks to engage an Information Systems Audit Firm, which has the capability and experience to conduct a comprehensive Information Systems Audit of Bank's critical IT infrastructure and IT Governance.

Bank seeks to have an external examination of the IT security to ward off risks in the IT Domain and to appraise the findings there of to the Management.

- To determine the effectiveness of planning and oversight of IT Activities
- Evaluating adequacy of operating processes and internal controls
- Determine adequacy of enterprise-wide compliance efforts relating to IT Policies and Internal Control Procedures.
- Identifying areas with deficient Internal Controls and recommend corrective action to address deficiencies.

IS Audit objective

The Auditors shall give reasonable assurance to the Top Management explicitly in their audit report, with regard to

- Completeness, effectiveness of the various Policies/ Procedures/ guidelines defined by the Bank from time to time as per guidelines from the regulatory authorities.
- Compliance of all applicable guidelines / recommendations/ directions laid down by regulatory authorities like RBI, NPCI, UIDAI, CSITE etc. and ISMS control requirements of ISO/IEC 27001.

Saptagiri Grameena Bank (SGB) invites sealed quotations for and on behalf of all the three RRBs, from all eligible bidders to conduct Information system audit of their CBS, Internet and Mobile Banking applications, Data Center, Disaster Recovery Site, Network and its related infrastructure. Part-I of the bid document will consist of technical and other details and should be submitted manually and Part II will be a sealed bid for commercials

1 - Qualified professionals to be deployed for the job

The entire Security Audit work has to be got done by qualified CISA/CISSP/ISO 27001 Lead Auditor/Professionals having requisite expertise in Information Security Audit. The Information Security Audit should be completed within the mutually agreed time schedule. Franchise of Information System Auditors will not be permitted under any circumstances.

2 - Audit Coverage Period

The proposed Annual IS audit will be for a period of two years. Award of IS Audit assignment will be initially for a period of one year. On satisfactory performance and completion of first year assignment, the same may be extended for another one year on the same terms and conditions.

---

2. USE OF CONTRACT DOCUMENTS AND INFORMATION;

2.1 The IS Auditor shall not, without the bank's prior written consent, disclose the contract, or any provision thereof, or any specification, plan, drawing, pattern, sample or information furnished by or on behalf of the banks in connection therewith, to any person other than a person employed by the IS Auditing Firm in the performance of the contract. Disclosure to any such employed person shall be made in confidence and shall extend only as far as may be necessary for purposes of such performance.

2.2 The IS Auditor shall not, without the banks' prior written consent, make use of any document or information pertaining to this contract except for purposes of performing the contract.

IS Audit scope

Information System Audit, Vulnerability Assessment and Penetration Testing of Bank's entire CBS and allied infrastructure including Hardware, Operating System, Database, Application(s), Network, Security Devices, Process & People in following locations/Offices:

- Data Center
- Disaster Recovery Site
- Project Office at Chennai including helpdesk operations
- Information Technology Departments at each of RRBs Head Offices
- Other departments at Head Offices of RRBs or any other bank's office at any place, where critical application/IT infrastructure is installed or may be installed.
- Premises/activities of any third party/service providers (outsourced activities) to review compliance of services/T&C under service level agreements, both at their Primary Site and DR Site
- Minimum 5 CBS branches per RRB (including systems rendering various types of services like Passbook printing, Cheque acceptance etc.)
- OS and DB, Vulnerability assessment of atleast 5 branch servers in each RRB

Eligibility (selected points)

3. The bidder Organisation must have been empanelled by CERT-In for providing IT Security Auditing Service and the empanelment should currently be valid. Documentary evidence of the same to be enclosed with the technical Bid.

9. The Core Audit team assigned for I.S. Audit of the Auditee, should have at least Four qualified professionals with qualifications such as CGEIT (Certified in the Governance of Enterprise IT),CISA, CISSP, CCNA, CCNP, ISO 27001/BS7799 Lead Auditor, OCM & OCP, out of which at least 3 persons should be CISA qualified (including team leader). Bidder must warrant that these key project personnel to be deployed in this project have been sufficiently involved in similar projects in the past. Bidders should provide information about such key project personnel who are proposed to be part of the IS Audit team along with the Bid Document. Bidder should ensure that the members of Core Audit team are actively involved in the conduct of the Audit throughout the period of the contract

DC & DR – physical & environmental review

- DC perimeter & physical access security design & processes
- DC material inward / outward security
- Power and backup
- Safety systems – fire & smoke detection, suppression systems
- Rack, cabling and earthing
- DC access surveillance & monitoring
- Housekeeping & vendor management

Central Bank of India

- CYBER SECURITY AUDIT &
- COMPREHENSIVE AUDIT OF CBS PROJECT & OTHER APPLICATIONS

Scope of Audit

- **Application Audit :** Complete review of applications and security audit of all major applications including Core Banking Application (CBS-B@ncs24) and Delivery Channels i.e. Internet Banking, Mobile Banking (SMS/ WAP), RTGS/ NEFT etc. In-house developed applications. (Approximate 34 applications)
- **Top 10 OWASP Vulnerabilities : Compliance review of top 10 OWASP** (Open Web Application Security Project) vulnerabilities, especially for public facing applications viz. Internet Banking, Mobile Banking, Corporate Website etc.
- **- VAPT (Vulnerability Assessment & Penetration Testing) : VA** (Vulnerability Assessment) of all major applications including CBS & Delivery Channels, and Penetration Testing of public facing applications viz. Internet Banking, Mobile Banking, Corporate Website etc
- **IS Audit should comply the various guidelines issued by RBI time to time.**

- **2. DC/ DRC Audit :** Thorough Audit of bank‟s Data Centre (DC) at Navi Mumbai, Disaster Recovery Centre (DRC) at Hyderabad and Near Site at Navi Mumbai. Audit of Disaster Recovery and Business Continuity Plans for adequacy and conformance of BCP. Audit of effectiveness of Anti-virus system.
- **3. Network Audit :-**Network Infra & Security Audit
- **Configuration Audit :-** Configuration audit of various devices, especially for network & network security devices.
- **4. Audit of ATM Project :-** Security audit of ATM switch, ATM card related operations, ATM site audit (20 locations – Onsite/ Offsite), General review, Cash Management, ATM Branch related audit. (ATM locations – 4 Rural, 4 Semi-urban, 4 Urban, 8 Metro)
- **5. Branch IS Audit :**IS Audit of select branches at various Centers (10 branches – 2 Rural (1-VSAT), 2 Semi-Urban, 2-Urban, 4 Metro)

Aspire for a successful professional career.

Thank You