Information Systems Audit

COASTAL BANK
Coastal Local Area Bank Ltd

Corporate Office,
Coastal Local Area Bank Ltd.,
Department of Information Technology
3rd Floor, D No.59-12-6, Grace Line,
Ghantasalavari Street,
Vijaywada-520 008, A.P.

1. Introduction

Coastal Bank was the first Local Area Bank licensed by RBI in 1999 to commence operations in 3 districts of Andhra Pradesh (later expanded to 5 Districts, viz., Krishna, Guntur, West Godavari, East Godavari & Visakhapatnam). The Bank with over 160 touch points (50 Branches; 44 ATMs; 20 BCs; 46 Collection Agents). The Banks's work force is 300+.

The Bank offers digital Banking services such as Mobile Banking, RTGS, NEFT, IMPS, UPI, POS, Rupay Cards & ATMs / Cash Deposit Machines.

The Bank's technical platforms and Core Banking Solution (Ban@s24) are wholly managed by C-Edge Technologies Ltd on shared basis under ASP agreement. The Data Center, Disaster Recovery Site, ATM Switch/Centre etc are managed by our IT Service Provider, viz., C-Edge Technologies.

2. Present proposal:

The Bank intends to subject its systems to Information Systems Audit including

- Robust IT security
- Mitigation of risks where there are significant control weaknesses
- Safeguarding the information assets viz. hardware, network etc.
- Maintaining security, confidentiality, integrity and availability of data
- Efficient utilization of IT resources
- Ensuring compliance of IT Security Policy/IS Audit Policy and procedures defined by the Bank

Interested Individuals / Organisations, fulfilling the following eligibility criteria can apply by sending their profiles to coastalho@coastalareabank.com

3. Eligibility Criteria:

1. Qualification	Must have CISA qualified member/s in the Audit Team.
2. Experience	Must have conducted Information Security Audit assignments during the last 3 years, preferably in Banks. Brief details of the past assignments to be enclosed.
	Should have thorough knowledge of RBI guidelines on IS Audit
3. Skills	The audit team should have good understanding of Information Systems in Banks, namely CBS, Network Security, Server Security, DC and DR set up, etc.

	Payment Systems of RBI and NPCI,
	Different banking service channels like ATM, BCs, Mobile Banking, etc.,
	Conducting VAPT (Vulnerability Assessment and Penetration Testing)
	Knowledge of KYC/AML, Risk management, IS Security standards and regulations, prescribed by RBI.
4. Stature	The audit team / organisation should have good standing in the industry. List of previous clients to be furnished.
5.Documents submission	KYC documents in the case of the individuals or group of individuals with requisite experience. Certificate of Incorporation, PAN, TAN, GSTIN Certificate and any other tax related document if applicable, to besubmitted. In case of LLP / partnership firms, a Deed of Partnership should be submitted. Copy of the audited balance sheet and Profit & Loss statements, Certificate from the Chartered Accountant (in case of Provisional Balance Sheet) of the company showing profit, net worth and turnover of the company for the last three financial years i.e. 2017-18,2018-19 & 2019-20 should be submitted. In case of individuals, the IT returns filed during the last 3 years be submitted. The profile of the Core Audit team must be submitted as per format given in Annexure – XXII format. Respective professional certificates to be submitted Documentary evidence with relevant copies of Purchase Order along with Satisfactory Working Certificates / Completion Certificates / Installation Reports / Project Sign-Offs in the **last three** years including names of clients with Phone and Fax numbers, E-Mail IDs etc.

Others:	Coastal Bank reserves the right to accept or reject in part or full any or all offers without assigning any reason thereof and without any cost or compensation therefor. Any decision of the Bank in this regard shall be final and no correspondence in this regard is entertained.

Scope of work

IS audit of the Bank should be guided by the guidelines issued by RBI from time to time on Computer Audit and Information Security Audit and should be as per the best practices in the industry. Bank has a Board approved IS Audit Policy which needs to be adhered to while conducting the audit. Information Systems Audit has to be undertaken covering the various key areas:

- Preparation of IS Audit Plan in Consultation with bank
- Defining Checklist for different applications/area of audit in Consultation with bank
- Planning execution of the Audit
- Conducting the IS audit
- Documenting the audit process
- Report submission to the bank
- Conducting the compliance audit

Broad Areas of Audit

- Vulnerability Assessment
- Penetration testing
- Application Audit
- Process Audit
- Network Architecture review
- Firewall rule base review
- Site Audit
- Database Audit
- Audit of all Outsourced activities/services.
- Audit for IT Act Compliance
- Audit of Disaster Recovery Plans & Business continuity plan
- Capacity Planning of IT Infrastructure of Critical Applications
- Audit of Service Level Management
- Cyber Security Framework

Process Audit should inter alia include

i. Anti-Money Laundering (AML) – Domestic

ii. Alternate Delivery Channels including
    - Mobile Banking Application
    - Debit Card
    - POS machine
    - Automatic Teller Machine (ATM) installed at different locations

iii. Email/Mail Messaging System
iv. Email Archival System
v. RTGS/NEFT Infrastructure / SFMS
vi. Core Banking System (CBS) including Interfaces
vii. MIS & Automated Data Flow Audit
viii. NACH & Mandate Management System
ix. Micro ATM
x. Review of interface with Payment Gateways used by the Bank viz. ATM, Mobile Banking etc.
xi. Anti-Virus

Vulnerability Assessment

- Placement/ Deployment of security equipment, network equipment for securing database, application, web servers of various applications.

Security Management Review

The Security Management Review shall cover following aspects:-

- Security Equipment Configurations & Policies

- **Infrastructure Review**

Audit of Disaster Recovery Plans
Audit of privileged users (Database, OS)
Capacity Planning of IT Infrastructure of Critical Applications
Audit of Service Level Management (Part of process Audit)
Cyber Security Framework Audit

CONTROLS TO BE COVERED

- Power Supply, UPS & DG
- Logical Access Control
- Physical Access Controls
- Infrastructure – network cabling, raceways, server / Communication racks, Rack Power Distribution Units (PDU), KVM
- Fire & Smoke, Water leak Detection and suppression Systems
- Air-conditioning:- Temperature & Humidity control systems
- Assets safeguarding, Handling of movement of Man / Material / Media / Backup / Software / Hardware / Information

- Surveillance systems
- Pest prevention (rodent prevention) systems
- Lightning Protection
- Training, Documentation, monitoring, duty list, storage management
- Asset Register, asset tracking, asset management
- High availability

Application Audit (Controls)

The Application audit shall cover following aspects:-

- Controls for performing/changing parameter setup of functionality across applications
- Segregation of duties
- Availability of necessary audit logs and its accuracy and effectiveness.
- Adherence of reporting to legal and statutory requirements
- Automated batch processing, scheduled tasks, critical calculations etc.
- End of Day, Start of Day, period closure operations including End of Month, End of Quarter and End of Year operations
- Integration with Delivery Channels including data and transaction integrity for the same
- Release of software governed by formal procedures – ensuring sign-off through testing, handover, etc.
- Formal procedure for change management being adopted.
- Maintenance personnel have specific assignments and that their work is properly monitored. Their system access rights are controlled to avoid risks of unauthorized access to automated systems
- Controls for opening/modifications of Office Accounts / GL heads

Network Audit

Network Audit is to be conducted for all network devices viz. Router, Switch, Firewall, IPS, IDS etc.

The Network audit shall cover following aspects: -

- Overall Network architecture
- Overall Network management
- Review of detailed Network architecture
- Rule base of the Core Network devices like Firewall, Router, Switch, IPS, IDS etc.
- Network traffic analysis and base lining
- Virtual LANS (VLANs) & Routing
- Network device life cycle
- Evaluate procedures adopted for:
    xii. Secured transmission of data through leased line / ISDN / VPN / VSATs / MPLS, Wireless etc.
    xiii. Bandwidth management

xiv. Uptime of network – its monitoring as per SLA iv. Fault management

Mail Messaging System Audit

The Mail Messaging audit shall cover following aspects: --

- Overall Mail Messaging System management
- Architecture & design review of Mail Messaging System
- Performance of Mail Messaging Servers under SLAs
- Archival & backup process including cloud
- Configuration Audit, if applicable, for all servers, network devices (Routers, Firewall, Switches) used in Mail Messaging System
- Impact Analysis of Mail Servers

IT Policies review

An assessment / review of all the important Policies / Procedure Documents of the Bank such as:-

- Information Technology (IT) Policy
- Any other IT related policies of the Bank which are not listed above

Payment Gateway Audit

- Verification of controls for RTGS, NEFT, SFMS, SWIFT, NFS etc. at Payment Gateway, as per the regulator"s policies and guidelines

Privacy and Data Protection

Privacy and Data Protection Audit shall cover following aspects: --

- Procedures of erasing, shredding of documents and
- Media containing sensitive information after the period of usage.

Business Continuity Management

Business Continuity Management Audit shall cover following aspects:--

- The BCP methodology covering the following:
  - Identification of critical business
  - Owned and shared resources with supporting function
  - Risk assessment on the basis of Business Impact Analysis („BIA")
  - Formulation of Recovery Time Objective („RTO") and Identification of Recovery Point Objective („RPO")
  - Minimizing immediate damage and losses
  - Restoring of critical business functions, including customer-facing systems and payment settlement systems
  - Establishing management succession and emergency powers
- Addressing of HR issues and training aspects
- Providing for the safety and wellbeing of people at branch or location at the time of disaster
- Assurance from Service providers of critical operations for having BCP in

place with testing performed on periodic basis.

- Maintaining of robust framework for documenting, maintaining and testing business continuity and recovery plans by Banks and Service Providers.

Asset Management

Asset Management shall cover following aspects: --

- Records of assets (Software, Hardware, Licences etc.) mapped to owners
- Proper usage policies for use of critical employee facing technologies
- Maintenance of Inventory logs for media
- Restriction of access to assets through acceptable usage policies, explicit management approval, authorized use of technology, access control list covering list of employees and devices, labelling of devices, list of approved company products, automatic session disconnection of remote devices after prolong inactivity
- Review of duties of employees having access to asset on regular basis.

Management

Record processes and controls shall cover the following aspects: -

- Policies for media handling, disposal and transit
- Periodic review of Authorization levels and distribution lists
- Procedures of handling, storage and disposal of information and media
- Storage of media backups
- Protection of records from loss, destruction and falsification in accordance to statutory, regulatory, contractual and business requirement

Technology Licensing

Technology Licensing shall cover the following aspects: -

- Periodic review of software licenses
- Legal and regulatory requirement of Importing or exporting of software

IT outsourcing related controls

The following correlates significant third party risks to the assessments utilized by organizations to evaluate the effectiveness of third party controls in place to mitigate risks.

- **Compliance**: Assess the third-party's ability / control framework in place to comply with laws/regulations.
- **Information Security & Privacy**: Assess third party controls over the Availability, confidentiality, and integrity of third party data.
- **Physical Security**: Assess facility access and security measures implemented by the third party.

AUDIT APPROACH

Information Systems Security Audit approach includes the following:

- Auditing around the computer
- Auditing through the computer
- Auditing with the computer
- Through preparation of IS audit checklists based on globally accepted standards and RBI guidelines/ Circulars / IT Acts.
- Based on the audit findings risk assessment to be classified as Low, Medium and High in each specific audit areas.

The selected auditors must understand the business and IT environment, risks and internal control framework. During audit, auditors shall obtain evidences, perform test procedures, appropriately document findings, and conclude a report.

Guidance on executing the IS Audit may entail the following steps:

- Refining the understanding of business process and IT environment
- Refining the scope and identifying internal controls
- Testing Control Design

AUDIT PHASES AND SCHEDULE

The empanelled bidders have to undertake the audit within 2 weeks from date of issue of Work Order, in the following phased manner:

1	**PHASE – I**	Planning and conduct of the audit	4 weeks
2	**PHASE – II** [REPORTING of Findings]	Submission Audit Report with Risk rated (Critical, High Medium, Low) observations	1 week from the date of completion of **Phase I**.
3	**PHASE – III** [COMPLIANCE & CLOSURE]	1. Compliance review 2. Submission of Review Report with Risk rated (Critical, High Medium, Low) observations vis-à-vis compliance by bank. 3. Issuance of Closure Certificate on completion of the compliance audit.	Within 4 **Weeks** from the end of relevant quarter. Exact date of commencement of Review Audit will be intimated by the Bank.