



THE ANDHRA PRADESH STATE CO-OPERATIVE BANK Ltd.,

(A State Govt. Partnered Scheduled Bank)

HO: NTR Sahakara Bhavan, # 29-27-28, Governorpet, Vijayawada-520 002.

Url: <http://www.apcob.org>, Email: dos@apcob.org

Notification

Request for Quotations from Qualified Information System Auditors to do IS Audit for the AP State Cooperative Bank, 13 District Cooperative Central Banks and its Data Centre & Data Recovery

1. Andhra Pradesh State Cooperative Bank Ltd, invites quotations from qualified IS Auditors who fulfills the eligibility criteria mentioned here under and are willing to conduct Information System Audit of the Andhra Pradesh State Cooperative Bank, 13 DCCBs in Andhra Pradesh in AP and its Data Centre (DC) at Ctrl, Madhapur, Hyderabad & Data Recovery (DR) at Sify, Noida..
2. The Quotation should be submitted in the prescribed format (Annexure - 3) to the Deputy General Manager(DoS), Andhra Pradesh State Cooperative Bank Limited, Head Office, #27-29-28, NTR Sahakara Bhavan, Governorpet, Vijayawada- 520002 only by e-mail (dos@apcob.org).
3. Applying professionals should submit self-attested signed & scanned in prescribed format, valid CISA certificate/s along with application.
4. Incomplete application or application without requisite enclosures will be rejected.
5. Mere submission of application does not, in any way, constitute guarantee for Allotment of the audit job of any nature from the bank. The allocation of the Banks to the auditors will be purely the prerogative of the Bank.
6. **The Auditors/Agencies associated with the bank prior to this notification are also required to submit their quotation afresh as our entire previous notification, stand cancelled. The eligibility criteria for job allocation with the Bank are as under:**
 - a. Shall have experience of Information Systems Audit of minimum three other Banks.
 - b. Should be having CISA (ISACA) qualified and/or having completed certified course on IS Audit from ISACA will be preferred. (documentary evidence to be produced)
7. The IS Audit Scope document enclosed herewith also need to be signed by the applicant.

The auditors fulfilling above criteria are requested to submit quotation and send the soft copy (signed & Scanned) to dos@apcob.org along with copies of relevant certificates/ documents to Dy. General Manager (DoS)/Chief Information Security officer (CISO), latest by 27.01.2020

Note: The applicant can find the quotation form as Annexure-3 to this notification and can be downloaded from website under 'Notifications' tab.

Annexure -1 : Application/Firm Details

Annexure -2 : Scope

Annexure -3 : Quotation Format

Applicant/Firm Details

Sl. No	Particulars	
1	Name of the firm	
2	Name of the coordinating person from your firm & Designation	
3	Address	
4	Contact Nos. and e-mail address	Mobile No. _____ E-mail id: _____
5	Total amount quoted to conduct IS Audit of The Andhra Pradesh State Cooperative Bank, 13 dccbs in Andhra Pradesh in AP and its Data Centre (DC) at Ctrl's, Madapur, Hyderabad & Data Recovery (DR) at Sify, Noida.. As per enclosed quotation	

I/We hereby declare that all the information submitted by me/us is true and the certificates/documents attached are genuine. In case any information/documents is found as untrue/misleading, the Bank may take necessary action, including Blacklisting of the firms/members, as it may deem fit.

Signature & Stamp Date:

Place:

NOTE: Bank reserves the right to ask for original copy of enclosed certificates for verification.



THE ANDHRA PRADESH STATE CO-OPERATIVE BANK Ltd.,

(State Govt. Partnered Scheduled Bank)

HO: NTR Sahakara Bhavan, # 27-29-28, Governorpet, Vijayawada – 520 002
DoS Dept., email: dos@apcob.org, url: www.apcob.org, Ph:0866-2429052

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

DETAILED SCOPE OF AUDIT

IS Audit should cover entire extent 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 Equipment

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.
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 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
 1. 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.

G. Audit of ATM Switch, ATM Card Management, ATM and Internet Banking PIN management

1. Audit of ATM Switch covering Application,
 1. Network Security, Switch Functionality, Interface,
 2. Audit Trails, transmission security, authorization,
 3. 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

H. 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.

I. 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.

//On the letter head of the Agency/Firm//

Annexure-3

Quotation

To
The Dy. General Manager (DoS),
The AP State Coop Bank Ltd.,
Head Office,
Vijayawada.

Sir,

We are here by submitting the Quotation to conduct Information System (IS) Audit for AP State Cooperative Bank, 13 District Cooperative Central Banks and its Data Centre & Data Recovery.

Quotation for AP State Cooperative Bank, 13 District Cooperative Central Banks and its Data Centre & Data Recovery	
(In. Rupess)	
Particulars of area to be Audited	Quoted Amount
APCOB Data Centre, Ctrl, Madapur, Hyderabad	
DCCB Data Centre, Ctrl, Madapur, Hyderabad	
APCOB Data Recovery, Sify, Noida, Delhi	
DCCB Data Recovery, Sify, Noida, Delhi	
APCOB HO & 2 Branches	
Srikakulam DCCB HO & 2 Branches	
Vizianagarm DCCB HO & 2 Branches	
Visakhapatnam DCCB HO & 3 Branches	
Kakinada DCCB HO & 5 Branches	
Eluru DCCB HO & 3 Branches	
Krishna DCCB HO & 6 Branches	
Guntur DCCB HO & 4 Branches	
Prakasam DCCB HO & 3 Branches	
Nellore DCCB HO & 2 Branches	
Kadapa DCCB HO & 2 Branches	
Kurnool DCCB HO & 2 Branches	
Anathapur DCCB HO & 3 Branches	
Chittoor DCCB HO & 4 Branches	
Total Amount	

I/We hereby declare that the quoted amount submitted by me/us is the final amount (inclusive of all taxes). In case any deviation is found, the Bank may take necessary action, including Blacklisting of the firms/members, as it may deem fit.

Signature & Stamp

Place & Date: