THE ANDHRA PRADESH STATE CO-OPERATIVE BANK Ltd.

(State Govt. Partnered Scheduled Bank)

REQUEST FOR PROPOSAL

Invitation of Bids for Conducting IS Audit (F.Y 2022-2023)
for APCOB and 13 DCCBs

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

Url: https://www.apcob.or HYPERLINK "https://www.apcob.org/" HYPERLINK "http://www.apcob.org/" HYPERLINK "https://www.apcob.org/"g HYPERLINK "https://www.apcob.org/" HYPERLINK "http://www.apcob.org/" HYPERLINK "https://www.apcob.org/" HYPERLINK "https://www.apcob.org/" HYPERLINK "mailto:email-dos@apcob.org" HYPERLINK "https://www.apcob.org/"email-dos@apcob.org

Bids are invited for "**Conducting IS Audit (F.Y 2022-2023) for APCOB and 13 DCCBs"**. The details of the tender are as under.

1. Invitation for Tender Offers

- APCOB invites tender, in two bid system (Technical and Financial bid), from firm/company/organization having sufficient experience in **Conducting IS Audit.**

- APCOB reserves the right to alter the scope of work at any stage with suitable adjustment in charges payable.

INDICATIVE CRITICAL DATA SHEET

Bid Security/Earnest Money Deposit (Refundable)	Rs. 5,000/- (Rupees Five thousands only)
Bid Submission Start Date	20-01-2023
Bid Submission End Date	31.01.2023 before 2.00 P.M
Technical Bid opening	31.01.2023 TIME:3.00 P.M
Commercial Bid Opening	02-02-2023 TIME: 10.30 A.M
ISSUING OF PURCHASE ORDER TO SUCCESSFUL BIDDER	06-02-2023
Audit Action Plan Submission by Successful bidder	10-02-2023
COMMENCEMENT OF I S AUDIT	13-02-2023
INTERIM IS AUDIT REPORT Submission	13-03-2023
FINAL REPORT SUBMISSION	20-03-2023
Point of Contact for Bid Submission	Sri Bh. Satya Prasad Dy. Gen. Manager (DOS) **The A.P.State Co.op Bank Ltd.,** NTR Sahakara Bhavan, Governorpet, Vijayawada 520002 Mobile: 7729969646 e-mail: dos@apcob.org
Address for Tender Submission	Sri Bh. Satya Prasad Dy. Gen. Manager (DOS) **The A.P.State Co.op Bank Ltd.,** NTR Sahakara Bhavan, Governorpet, Vijayawada 520002 Mobile: 7729969646 e-mail: dos@apcob.org
Technical Clarifications	**Mr. S.V.Subrahmanyam** **Chief Information Security Officer (CISO)** Mobile: 7989316150 e-mail ID: ciso@apcob.org

- Bidder(s) shall submit their bid (comprising of "Technical" and "Financial" bid in separate covers clearly superscribing the name of bid, in physical form to "Address for Tender Submission"

Technical Bid:

- The technical information should be prepared very carefully and as indicated in the tender document since it will form the basis for pre-qualification of bidder(s). Only relevant and to the point information/document should be submitted (Preferable format .pdf). Failure to provide any required information, may lead to the rejection of the offer without entertaining further communication. Bidder(s) must read the tender document very carefully.

- All Annexures must be signed by the authorized representative along with date as token of acceptance of the terms & conditions of tender (Annexures are attached for this purpose)

Financial Bid:

Bidder(s) must read the terms and condition as mentioned in this tender document and submit the form accordingly. Bidder(s) are required to check the prices / amount carefully before uploading financial bid.

- Submission of more than one bid is not allowed and shall result in disqualification of the bidder.

- Validity of bids: Bid submitted by the Bidder(s) shall remain valid for acceptance for a minimum period of Ninety (90) days from the last date of submission of bid (Technical and Financial), including extensions, if any.

- APCOB reserves the right to reject any or all the bids without assigning any reasons thereof at any stage of bid.

- Authorization and Attestation: Bidder(s) must submit an Authorization Letter or valid Power of Attorney on behalf of firm for signing the document.

- The Standard Terms and Conditions of this RFP also form part of the Open-Tender specifications. The information furnished shall be complete by itself. Bidder(s) are requiredto furnish all the details and other documents as required.

- Bidder(s) are advised to study all the tender documents carefully.

- Any conditional bid received shall not be considered and will be summarily rejected in veryfirst instance without any recourse to the bidder.

- Any submission of bid shall be deemed to have been done after careful study and examination of this RFP document and with the full understanding of the implications thereof.

- In case of any doubt about the meaning of any portion of this RFP or any discrepancies or omission(s) in the scope of work or any other portion of this RFP or any incomplete portionor requires clarification on any aspect, scope of work etc. Bidder(s) shall contact the authority inviting the tender as per date and time mentioned in the Indicative Critical Data Sheet.

- Bidder(s) request for clarification shall be with reference to clauses in this RFP document.

- The specifications and terms and conditions shall be deemed to have been accepted by the Bidder(s) in their offer.

- Non-compliance with any of the requirements and instructions of this RFP document may result in the rejection of the tender.
- This document has not been filed, registered, or approved in any Court of Competent jurisdiction. Recipient of this document should inform themselves of and observe any applicable legal requirements.
- This document constitutes no form of commitment on the part of the APCOB. Furthermore, this document confers neither the right nor an expectation on any party to participate in the tendering process.
- Merely participation in this Tender Document by any party does not confer or constitute anyright of association with APCOB.
- APCOB reserves the right to reject any or all the bids without assigning any reasons thereof at any stage of bid or at any point of time

2. Bid Security / Earnest Money Deposit (EMD)

Bids received without EMD is liable to be rejected. Bidder should pay specified amount towards Earnest Money deposit as follows:

- Rs. 5,000/- (Rupees Five Thousand Only) in the form of Demand Draft drawn on any Nationalized /Schedule bank in favour of "APCOB" at Vijayawada;
- EMD will not carry any interest.
- EMD will be refunded to the unsuccessful bidders after finalization of the bid and EMD of successful bidder shall be returned after acceptance of entire terms and conditions mentioned inthe tender document.

3. The Earnest Money Deposit submitted by the bidder may be forfeited if,

- Successful bidder fails to accept the terms and conditions mentioned in the Agreement within specified time as per intimation/request of APCOB;
- Successful Bidder withdraws its tender or backs out after acceptance;
- Bidder withdraws his tender before the expiry of validity period stipulated in the bidding document;
- Bidder violates any of the terms and conditions of the tender;
- Bidder revises any of the items quoted during the validity period;
- Bidder is found to have indulged in fraudulent practices in the bid submission process.

4. INTERPRETATION

In this Tender Document, unless the context otherwise requires,

- For the purpose of this Tender Document, where the context so admits:
- The singular shall be deemed to include the plural and vice versa and versa.
- Masculine gender shall be deemed to include the feminine gender and References to a "person" if any shall, where the context so admits, include references to natural persons, partnership firms, companies, bodies, corporate and associations, whether incorporated or not

or any other organization or entity including any governmental or political subdivision, ministry, department or agency thereof;

- References to Clauses, Recitals or Schedules are references to clauses and recitals of and schedules to the Contract and the Tender Document. The Schedules, annexure and addendums shall form an integral part of this Contract.
- Any reference herein to a statutory provision shall include such provision, as is in force for the time being and as from time to time, amended or re-enacted in so far as such amendment or re-enactment is capable of applying to any transactions covered by this Contract. Any references to an enactment include references to any subordinate legislation made under that enactment and any amendment to, or replacement of, that enactment or subordinate legislation. Any references to a rule or procedure include references to any amendment or replacement of that rule or procedure.
- The headings and sub-headings are inserted for convenience only and shall Document. References to the word "include" and "including" shall be construed without limitation. Any reference today shall mean a reference to a calendar day including Saturday and Sunday.

5. DUE DILIGENCE

The Bidder is expected to and shall be deemed to have examined all instructions, forms, terms and specifications in this Tender Document. The Bid should be precise, complete and in the prescribed format as per the requirement of the Tender Document. Failure to furnish all information required by the Tender Document or submission of a bid not responsive to the Tender Document in every respect will be at the bidder's risk and may result in rejection of the bid. APCOB shall at its sole discretion be entitled to determine the adequacy /sufficiency of the information provided by the bidder.

6. COST OF BIDDING

The Bidder shall bear all costs associated with the preparation and submission of its bid and APCOB shall in no event or circumstance be held responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

7. SCOPE OF IS AUDIT

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 at CtrlS Hyd and at Netmagic Mumbai
2. Data Recovery (DR) at Netmagic Bangalore
3. CBS endpoint applications, Servers, Interfaces, Network & Other Devices,
4. ATM Switch and random 10 % of the ATM in operation in each bank (Total ATMs 440)
5. Mobile Banking (Android & IOS)
6. 3rd party products & Interfaces
7. VAPT (Vulnerability Assessment & Penetration Testing): Conducting VA specifically for Bank's Public facing Applications like Internet Banking, Mobile Banking, Corporate Website etc.,)
8. Active Directory (AD)
9. Secure Email and Messaging systems
10. Secure Configuration

11. IT Asset Management

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/ISO 27001:2013/CIS (Center for Internet Security)/CSA (Cloud Security Alliance) etc.,

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. Electrical supply, Redundancy of power level, Generator, UPS capacity.
5. Surveillance systems of DC / DRC
6. Physical & environmental controls.

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. Vulnerability assessment & hardening of Operating systems.
6. Users and Groups created, including all type of users_ management ensuring password complexity, periodic changes etc.
7. File systems security of the OS
8. Review of Access rights and privileges.
9. 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
11. Database Files and Directories Permission

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. Analyse 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 Users 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/ 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/BIA.

I. Vulnerability Assessment Scope:

General Controls for the Systems: i) Access Control and Authentication ii) Password and account policies iii) Patches and periodical updates

Configuration Audit for Network & Critical Security Devices: i) Access Control; System authentication process and procedures ii) Auditing and logging iii) System Insecurities; Unnecessary Services iv) Remote login settings; Latest Software version and patches if any

J. **Penetration Testing – Scope:**

1.Checking for strong authentication mechanism controls
2.Testing of SQIL, XSS and other web application related vulnerabilities
3.Testing of information disclosure such as internal IP disclosure
4.Identifying potential backdoors if any, checking of older vulnerable version

5.Missing Patches and versions
6.Checking of vulnerabilities based on version of device/servers
7.Testing of default passwords, DOS and DDOS vulnerabilities
8. Testing should cover OWASP TOP 10 attacks but shall not be restricted to. Best industry assessment standard PT to be ensured.

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.
4. VAPT of entire Network, Mobile Banking, Internet, website.
5. Capacity Monitoring
6.Environmental Controls
7.Antivirus Patch Management
8.Vendor Risk Assessment covering the aspects like: i) Assess Information Security Risk in Outsourced Vendor Operations ii) Conducting Risk Assessment for the outsourced vendor services carrying out key operational process of the Bank iii) To assess whether the Outsources Vendors comply with IT/IS policy of the Bank wherever applicable in comparing with SLA/MSA, ISO 27001:2013 Standard, SOC2 report as the case may be. iv) To assess whether outsourced Vendor/s of the Bank meet/incorporate adequate level of security controls commensurate with the business information they receive/store/process from or on behalf of the Bank.

8. CLARIFICATION ON BID DOCUMENTS

All prospective bidders requiring any clarification on the bid documents may request/forward their clarifications/queries to the Point of contact of APCOB, before the last date of seeking clarifications. Copies of consolidated queries of bidders and response of APCOB will be issued by APCOB as addendum in the website, only if the clarifications requested for, are considered appropriate by APCOB.

9. ELIGIBILITY CRITERIA

- Should be having CISA/CISM (ISACA), CISSP certified and Certification in force (documentary evidence to be produced). IS Auditors (who are conducting the IS Audit) should have minimum of three years' experience in the field (Experience certificate should be submitted before commencement of AUDIT). Amongst the team of the Auditors for conducting VAPT, one of the professional should have valid CEH/OSCP certification.

- Incomplete application or application without requisite enclosures will be rejected.

- Mere submission of an application does not, in any way, constitute a guarantee for Allotment of the audit job of any nature from the bank. The allocation of the Bank/s to the auditors will be purely the prerogative of the Bank.

- Bidder should have registered as Company under the companies act/LLP/MSME

- Shall have experience of Information Systems Audit of minimum three Nationalized Banks /Private sector Banks-scheduled /StCB/DCCB Banks in the preceding three years.

Other Conditions:

- The IS Audit Scope document enclosed herewith also need to be signed by the applicant.
- The final reports should be submitted by **20th March, 2023.**

10.SPECIAL TERMS AND CONDITIONS

- APCOB shall reserve the right to verify the operation and performance of project by the bidder and the bidder shall permit APCOB to do so. The APCOB will evaluate the information submitted by the bidder with regard to bidder's capacity. The bidder cannot subcontract the work at any stage without prior written approval from the APCOB.
- The job would be awarded to the L1 bidder, whosoever declared as L1 bidder, as per the criteria defined in the tender document.
- Rates quoted should be valid for the complete contract period as no changes in the price bid would be considered at a later stage.
- The bidder cannot make any amendment in the Technical Bid /Commercial Bid; neither can he impose any condition. All such bids will be rejected at the discretion of APCOB.
- The rates quoted in the price bid will be inclusive of all taxes, (except GST), fees, levies etc.
- The Bank reserves the right to alter/modify/cancel the bid process without assigning any reason at any stage. selected Bidder has to provide undertaking letter on letter head for not blacklisted format as applicable and industry acceptable format.
- The selected Bidder has to submit NDA (on non-judicial stamp paper- stamp duty applicable to AP) as per the Industry standard/Bank's requirement on the date of commencement of I S Audit programme.

11. PAYMENT TERMS AND CONDITIONS:

- The agency will submit the invoice supported by complete description of work and rate payable as per job order. Further the invoice should also be supported with detail of documents serial/date wise, with hard/soft copies without duplication containing exact number of pages.
- The invoice should contain PAN No., GST No., Job Order no. and address of the bidder when the payment has to be made.
- 10 % of bid value will be release on commencement of IS Audit and remaining will be released on submission of final report to the satisfaction of Bank.

12. UNDERTAKING

An undertaking from the Bidder stating the compliance with all the conditions of the Contract and Technical Specifications of the Bidding Document will be required, since

13. Other Terms and Conditions:

- No extra boarding, lodging, TA, DA or any other expenses shall be paid by APCOB for providing services.
- Auditors shall arrange to and fro logistics to APCOB & logistics to visit DCs & DR on their own and on reaching the APCOB location, logistics will be arranged by bank for local branch visits.
- Bank will arrange logistics to visit DCCBs and DCCBs' branches.
- Boarding & lodging has to be taken care by selected bidder.

14. TAXES AND DUTIES

The prices (including all taxes, duties, etc. but excluding Service tax and/or GST) quoted in the bid shall hold good and shall be binding on the bidder, notwithstanding any increase in the prices of materials and labour or in the freights or levy of other charges whatsoever and the bidder shall not be entitled to claim any increase over the rates quoted by him during the period of currency of the contract except taxes and duties as introduced / modified by Govt. from time to time if any within the period from last date of bid submission to the original completion date of the Contract. Reimbursement of any new tax or variation of existing tax, introduced during last date of bid submission to the original completion date of the Contract shall be paid in actual on submission of documentary evidence.

The extended period of service for the purpose shall only be in exceptional case.

15. NOTIFICATION OF AWARD & SIGNING OF CONTRACT WITH PURCHASER

The Bidder whose Bid has been accepted shall be notified of the award by APCOB, by registered letter, fax or by official mail. The Bidder shall acknowledge in writing, the receipt of the Letter of Indenter Notification of award of work and shall send his acceptance to enter into the Contract within three (3) days from the receipt of the Letter of Intent notification of work award.

16. EXPENSES FOR THE CONTRACT

All incidental expenses of the execution of the contract/ agreement shall be borne solely by the successful bidder and such amount shall not be refunded to the successful bidder by the APCOB.

17. FAILURE TO ABIDE BY THE IS AUDIT ASSIGNMENT"

The conditions stipulated in the assignment shall be strictly adhered to and violation of any of these conditions shall entail immediate termination of the assignment without prejudice to the rights of APCOB.

18. TERMINATION FOR DEFAULT

The bank may, without prejudice to any other remedy for breach of assignment terms, by written notice of default, sent to the bidder, terminate this assignment in whole.

- If the bidder fails to deliver and perform services within the time period(s) specified in the assignment, or any extension thereof granted by the company.

Note: Bidders should submit the Annexures (Attached)

- **Annexure-1**
- **Annexure-2**
- **Annexure-3**

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

Annexure -1

Applicant/Firm Details/Technical bid

<table>
<tr><th>Sl. No</th><th>Particulars</th><th></th></tr>
<tr><td>1</td><td>Name of the firm</td><td></td></tr>
<tr><td>2</td><td>Name of the coordinating person from your Firm/company/LLP/MSME & Designation</td><td></td></tr>
<tr><td>3</td><td>Address</td><td></td></tr>
<tr><td>4</td><td>Contact Nos. and e-mail address</td><td>Mobile No._____

E-mail id:_____</td></tr>
<tr><td>5</td><td>Experience in the field of Information Systems Audit (minimum of three other banks shall be considered)</td><td></td></tr>
<tr><td>6</td><td>Details of IS Auditors (who are conducting the IS Audit) should have minimum of three years' experience in the field and should be having CISA/CISM (ISACA), CISSP certified and Certification in force (documentary evidence to be produced).</td><td>
<table>
<tr><th>Name of the Auditor</th><th>Qualification</th><th>Experience</th></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
</table>
</td></tr>
</table>

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 - 520002

CISO Dept., email: ciso@apcob.org,

Annexure -2

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 at CtrlS Hyd and at Netmagic Mumbai
2. Data Recovery (DR) at Netmagic Bangalore
3. CBS endpoint applications, Servers, Interfaces, Network & Other Devices,
4. ATM Switch and random 10 % of the ATM in operation in each bank (Total ATMs 440)
5. Mobile Banking (Android & IOS)
6. 3rd party product & Interfaces.
7. VAPT (Vulnerability Assessment & Penetration Testing): Conducting VA specifically for Bank's Public facing Applications like Internet Banking, Mobile Banking, Corporate Website etc.,)
8. Active Directory (AD)
9. Secure Email and Messaging systems
10. Secure Configuration
11. IT Asset Management

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/ISO 27001:2013/CIS (Centre for Internet Security)/CSA (Cloud Security Alliance) etc.,

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. Electrical supply, Redundancy of power level, Generator, UPS capacity.
5. Surveillance systems of DC / DRC
6. Physical & environmental controls.

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. Vulnerability assessment & hardening of Operating systems.
6. Users and Groups created, including all type of users_ management ensuring password complexity, periodic changes etc.
7. File systems security of the OS
8. Review of Access rights and privileges.
9. 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 check-up of Systems and Sys Users (default password should not be there)
10. Checking of database privileges assigned to DBAs
11. Database Files and Directories Permission

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. Analyse 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/BIA.

I. Vulnerability Assessment Scope:

General Controls for the Systems: i) Access Control and Authentication ii) Password and account policies iii) Patches and periodical updates

Configuration Audit for Network & Critical Security Devices: i) Access Control; System authentication process and procedures ii) Auditing and logging iii) System Insecurities; Unnecessary Services iv) Remote login settings; Latest Software version and patches if any

J. **Penetration Testing – Scope:**

1.Checking for strong authentication mechanism controls
2.Testing of SQIL, XSS and other web application related vulnerabilities
3.Testing of information disclosure such as internal IP disclosure
4.Identifying potential backdoors if any, checking of older vulnerable version
5.Missing Patches and versions
6.Checking of vulnerabilities based on version of device/servers
7.Testing of default passwords, DOS and DDOS vulnerabilities
8. Testing should cover OWASP TOP 10 attacks but shall not be restricted to. Best industry assessment standard PT to be ensured.

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.
4. VAPT of entire Network, Mobile Banking, Internet, website.
5. Capacity Monitoring

6.Environmental Controls

7.Antivirus Patch Management

8.Vendor Risk Assessment covering the aspects like:

I. Assess Information Security Risk in Outsourced Vendor Operations.

II. Conducting Risk Assessment for the outsourced vendor services carrying out key operational process of the Bank.

III. To assess whether the Outsources Vendors comply with IT/IS policy of the Bank wherever applicable in comparing with SLA/MSA, ISO 27001:2013 Standard, SOC2 report as the case may be.

IV. To assess whether outsourced Vendor/s of the Bank meet/incorporate adequate level of security controls commensurate with the business information they receive/store/process from or on behalf of the Bank.

Signature of Authorized representative

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

Annexure-3

Quotation/Commercial Bid

To

The Chief Information Security Officer,

The A.P. State Coop Bank Ltd.,

Head Office,

Vijayawada.

Sir,

We herewith submit the Quotation to conduct Information System (IS) Audit for The A.P. 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, Srikakulam, Vizianagaram, Visakhapatnam, Eluru, Prakasam, Kurnool, Kakinada, Krishna, Guntur, Nellore, Kadapa, Anantapur, Chittoor DCCBs Data Centre (DC) at Netmagic Mumbai	
APCOB Data Centre, Ctrls, Madapur, Hyderabad.	
APCOB, Srikakulam, Vizianagaram, Visakhapatnam, Eluru, Prakasam, Kurnool, Kakinada, Krishna, Guntur, Nellore, Kadapa, Anantapur, Chittoor DCCBs Data Recovery Centre (DR) at Netmagic Bangalore	
APCOB HO & 2 Branches	
Srikakulam DCCB HO & 2 Branches	
Vizianagaram 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: