THE CHANDIGARH STATE CO-OPERATIVE BANK LTD. • CHANDIGARH •

Request For Proposal (RFP)

for

Information System (IS) Audit

The Chandigarh State Cooperative Bank Ltd.

Head Office: S.C.O. 1088-89 Sector 22 B Chandigarh

Website: www.cscbapex.com Email Id: cscbapex@gmail.com, cscbapex@yahoo.co.in, it.secion@cscbapex.com Contact No *0172-5025328, 0172-5024969*

The Chandigarh State Co-op. Bank Ltd. • Chandigarh • Sector 22-B

TENDER NOTIFICATION

The Chandigarh State Cooperative Bank Ltd.
SCO 1088-89, Sector 22 B
Chandigarh. 160 022

The Chandigarh State Cooperative Bank Ltd, hereby invites sealed Proposals from qualified Firms (CISA/ISA/DISA/CISSP) to conduct Information System (IS) Audit in the bank. The Proposals should be submitted according to two cover System consisting of Technical Bid and Financial Bid. The Tender Document can be downloaded from Bank's website https://cscbapex.com from 4th April 2023 at 10:00 am. The last date of submission of Bids is scheduled on 19th April 2023 up to 04:00 pm by physical mode only in two separate sealed envelope to be put in the box kept in the bank's head office at the given address.

The Chandigarh State Co-op. Bank
Sector 22-B

Important Dates;

Schedule of dates:

SN	Particulars	Details
1	Project Name	Selection of IS Auditor
2	RFP Reference No.	CSCB/IT/IS Audit/2023/01
3	Availability of RFP Documents	To be downloaded from The Chandigarh state Coop bank Ltd's Website **'www.cscbapex.com'**
4	Price of RFP Document	NIL
5	Date and Time of commencement of available of Bid Document (RFP)	04.04.2023, 10:00 am
6	Last Date and Time for Receipt of Bids at The Administrator The Chandigarh State Cooperative Bank Ltd, SCO 1088-89, Sector 22 B, Chandigarh U.T. 160022.	19.04.2023 up to 04:00 pm (By Physical Mode Only)
7	Date and Time of opening of Technical Bids	20.04.2023 at 11:00 am
8	Date and time of opening of Financial Bids	21.04.2023 at 4:00 pm
9	Address for Communication and submission of bid.	The Administrator The Chandigarh State Cooperative Bank Ltd, SCO 1088-89, Sector 22 B, Chandigarh U.T. 160022.

he Chandigarh State Co-op. Ba
Sector 22-B

Brief Profile of the Bank

The Chandigarh State Coop. Bank Ltd., Chandigarh, Registered Office: SCO 1088-89, Sector 22 B, Chandigarh UT was registered on 2.11.1966 under the Punjab Coop. Societies Act, 1961. The area of operation of the Bank with 18 branches in Union Territory of Chandigarh comprising of 371 Coop. Societies, and 3990 Individuals shareholders of the bank. The main emphasis of the bank is to improve the living conditions of service providers functioning as individuals in the city by organizing them into urban cooperative groups. Their empowerment through these cooperative self-help groups will help them to achieve economic independence and self-respect.

Current Banking Software:

Bank's software is Finacle version 7.0.29 provided by M/s WIPRO Ltd. as ASP (Application Service Provider) under NABARD project. All the 18 Branches are fully functional under CBS (Core Banking Solution)

Services being provided by the Bank:

- Core Banking Solution
- Aadhaar Based Payment System (ABPS) services
- Adhaar based Government subsidies to the customers
- RTGS/NEFT
- Exclusive Website of the Bank and domain E-mail
- Cheque Truncation System (CTS)
- ATM Facility (Acquirer Mode)
- ATM Facility (Issuer Mode)
- SMS Alert Facility
- EMV Rupay-cum-Debit Card
- IMPS (Immediate Payment Service)
- Insurances PMJBY/PMSBY
- 7 ATM Machines installed in the branches of the Bank.
- 18 Micro ATM Machines installed in all branches.

1 General Information

1.1 Disclaimer:

The information contained in this Request for Proposal (RFP) document or subsequently provided to interested parties, whether verbally or in documentary form by or on behalf of Bank by any of their authorized employees or advisors or consultants, is provided to the Bidders based on the terms and conditions set out in this RFP document only and any other terms and conditions subject to which such Information is provided.

This RFP document is not an agreement and is not an offer by the BANK to any other party. The purpose of this RFP document is to provide the Bidders with information to assist the formulation of their bid for short listing and final selection for appointment of IS Auditors for three years i.e. FY 2022-23, 2023-24, 2024-25 which would be renewed annually subject to satisfaction of the allotted work. If the allotted work is not satisfactory to the bank, conducting an IS Audit for further/next period would not be allotted to the firm.

The BANK may in their absolute discretion, but without being under any obligation to do so, update, amend or supplement the Information including the qualification process in this RFP document at any time including prior to submission of the bids.

The BANK reserves the right to accept or reject any or all Applications and qualify or disqualify any or all applicants without giving any reasons. The BANK will not entertain any claim for expenses in relation to the preparation of RFP submissions.

1.2 Objective:

The Chandigarh State Co-operative Bank Ltd. wants to selection of IS Auditors for Information System audit in the bank and all 18 branches for consecutively three years i.e. FY 2022-23, 2023-24, 2024-25 on the basis of NABARD circular ref No NB. Dos. HO. Pol./3634/J-1/2014-15 Dated 25.02.2015 and Circular Ref No NB. DoS. Pol. HO/794/J-1/2019-20 Dated 21.05.2019. Selected bidder is expected to make all efforts and commit all resources to make this project meet its objective.

2. Contents of the Tender Document

The Tender Document is divided into following sections:

1. Section I - Invitation for Bids
2. Section II - Instructions for Bid submission
3. Section III Broad Guidelines for Information System Audit (Annexure A(1))
4. Section IV - Scope of Work (Annexure B)
5. Section V – Technical Eligibility Criteria
6. Section VI – Financial Bid Submission Format

2.1. Section I - Invitation for Bids: Th e Chandigarh State Cooperative Bank Ltd, hereby invites sealed Proposals from qualified Firms (CISA/ISA/DISA/CISSP) to conduct Information System (IS) Audit in the bank for consecutively three years i.e. for FY 2022-23, 2023-24, 2024-25 which would be renewed annually subject to satisfaction of the allotted work. If the allotted work is not satisfactory to the bank, conducting an IS Audit for further/next period would not be allotted to the firm.

The Proposals should be submitted according to two cover System consisting of Technical Bid and Financial Bid. The Tender Document can be downloaded from Bank's website https://cscbapex.com from 24th March at 10:00 am. The last date of submission of Bids is scheduled on 07th April 2023 up to 04:00 pm by physical mode only in two separate sealed envelope to be put in the box kept in the bank's head office at the given address.

2. Section II - Instructions for Bid submission

2.1 Preparation of Bids: Bidders are requested to go through the tender advertisement and the Tender Document carefully to understand the documents required to be submitted as part of the bid. Please note the number of covers in which the bid documents have to be submitted, the number of documents - including the names and content of each of the document that need to be submitted. Any deviations from these may lead to rejection of the bid.

2.2 Bidder should consider all corrigendum/s, (if any), published on the Bank's website related to the Tender Document before submitting their bids.

2.3 Schedule of Request for Proposal (RFP)

- Request for Proposal Documents can be downloaded from the Bank's website http://www.cscbapex.com starting from 4th April, 2023. The Request for Proposal Document cost is NIL
- The sealed bids will be accepted on 19th April, 2023 up to 4:00 pm The Bank may at its sole discretion extend the bid submission date. The modified target date & time will be notified on the website of the Bank.
- The Technical Bids will be opened on 20th April, 2023 at 11:00 am. The Bidder(s) or their authorized representatives may be present if they so desire.
- The Financial Bids of only technically qualified Bidder(s) will be opened on 21st April 2023 at 04:00 pm. The Bidder(s) who have been declared eligible after evaluation of the technical bids or their authorized representatives may be present if they so desire at the time of opening of Financial Bid.
- For any clarification bidder may contact on mail Id cscbapex@gmail.com, it.section@cscbapex.com, atm.section@cscbapex.com

The Chandigarh State Co-op. Ba
Sector 22-B

2.4 Cost to Bid: There is no cost/No EMD

2.5 Evaluation of Bids:

- In this part, the bid will be reviewed for determining the compliance of the general conditions of the contract and Eligibility Criteria as mentioned in the Tender. Any deviation from general conditions of the contract and eligibility criteria will lead to rejection of the bid.
- Before opening and evaluation of the technical proposals, bidders are expected to meet all the general conditions of the contract and the eligibility criteria as mentioned below. Bidders failing to meet these criteria or not submitting requisite supporting documents / documentary evidence for supporting pre-qualification criteria are liable to be rejected summarily.
- The bidder must possess the requisite experience, strength and capabilities in providing the services necessary to meet the requirements, as described in the Tender Document.
- The bidder must also possess the technical knowhow and the financial wherewithal that would be required to successfully implement the project and provide the support services sought by THE CHANDIGARH STAE COOPEARTIVE BANK LTD. for the entire period of the Audit.
- The bids must be completed in all respects and should cover the entire scope of work as stipulated in the Tender Document.
- **Bids that are technically qualified would only be taken up for financial evaluation.**
- Bidders are required to submit all the supporting documents as per the criteria mentioned in the Tender. Bidders are required to comply with all the Technical Specifications as mentioned in Tender, no deviation will be accepted. Any deviation would be summarily rejected without assigning any reason.

2.6 Evaluation of Financial Bids: Financial bids submitted by only those bidders, who have qualified both pre- qualification and technical evaluation, will be eligible for further evaluation.

The Chandigarh State Co-op.
Sector 22

3. Section III

Annexure-A(I)

Suggested check list for the guidance of Auditor carrying out IS audit

I. Segregation of Duties

I.A. Are duties segregated between the data processing function and users?

a. Does the organizational structure provide for separation of functions between:
  i. Transaction initiation & authorization?
  ii. Console operations and data-entry?
  iii. Programme team and Custody of System Documentation (including programmes), confidential data, etc.?

b. Does the Data Bank Administrator (DBA) / IS manager reports to higher authorities about day-to-day as well as non-routine activities?

c. Are data processing personnel restricted from having asset custodianship functions, and access to assets, particularly liquid assets?

I.B. Are the duties segregated within the IS functions?

(a) Does a current organization chart exists which defines the organizational structure within IS department/Computer Cell?

(b) Do current job descriptions exist for all personnel associated with IS department/Computer Cell?

(c) Are new employees provided with orientation upon recruitment?

(d) Have IS department/Computer Cell employees been provided with formal and on-the-job training to maintain knowledge, skills and ability in Information Technology and control-requirements?

(e) Is there a separation between Data Base Administration and other data processing functions?

I.C. Precautions regarding personnel involved in IS functions :

(a) Are employees who constitute a potential threat transferred or suspended immediately?

(b) Are references verified before an employee is recruited?

(c) Is the IS personnel (including DBA) required to take regular vacations, and are their duties reassigned during the vacation period?

II. Access Controls

II.A. ***Access controls: is access to the main processor (i.e. system-console or server) adequately controlled?***

a. Does the computer room have adequate physical barriers to prevent unauthorized access to the system console / server?

b. Are combination locks, security badges or other means used to restrict access to the computer server room, back-up storage library and documentation library?

c. Are combination locks, security badges or other devices changed periodically?
d. Has detective equipment been installed to monitor access to the computer server room, (or e.g. cameras with time and date stamp in case of ATM-Unit)?
e. Does the location of off-line storage of data, transaction journals and critical reports are safeguarded against unauthorized access?

II.B. *Access controls: if access to programmes and data including Data Centre / Disaster Recovery Centre is primarily controlled through passwords? are procedures adequate?*

a. Are password administration facilities in Operating System (OS) and in Application packages are in vogue?
b. Is a security package in use, or any other security facilities in O.S. and App. Packages is being explored?
c. Is suitable security software installed and updated regularly in all systems for protecting software systems against virus, spyware, spamware and other malicious programs?
d. Are various levels of passwords established for different transaction types, files and programmes?
e. Are various levels of passwords required based on the usability, confidentiality and significance of information?
f. Are passwords periodically changed? How often passwords are changed?
g. Are all modifications to authorization tables and access privileges recorded and reviewed?
h. Are all Systems / Database logs validated by the Solution/Service provider at periodical intervals?
i. Are log-in IDs of terminated employees immediately disabled on the system?
j. Are users prohibited from selecting passwords that contain their names, or the passwords, which are very easy to guess?
k. If the DBA/password administrator assigns passwords first time, are delivery procedures appropriate to assure that an employee's password is not intercepted?
l. Does that employee change the password immediately after he receives from the DBA?

IIC. *Access controls: if access to programmes and data files is primarily controlled through physical restrictions in terminals, are procedures adequate?*

a. Does the layout of the area where terminals are located prevent unauthorized access to equipment?
b. Do the location of terminals used for either data entry or inquiry, restrict access to authorized personnel when the system is in operation?

II D. *Access controls:* **Are the programming activities properly controlled?**

a. Do the procedures and system - mechanisms prevent programmers from accessing production data, object programmes and other automated procedures during the testing and debugging process?
b. Are programmers required to work on a separate computer system (i.e. other than production system)?
c. Is all live data removed from the computer system and secured in a separate library at the time software or hardware maintenance activities take place?
d. Does production software (i.e. programmes in use) protected from unauthorized access (i.e. use of a restricted facilities)?
e. Is all testing activity restricted to non-production programmes and data?
f. Do the procedures used FOR INCORPORATING NEW OR ALTERED PROGRAMMES IN PRODUCTION SYSTEMS, prevent unauthorized access to other programmes?

II.E. Access controls: is system-activity appropriately monitored?

a. Does the computer system maintain a log of access activity?
b. Are invalid access attempts reported to, and investigated by management, DBA, and Computer Auditors?
c. Is the system capable of distinguishing activity source by terminal identification?
d. Is the system capable of identifying authorized individuals by multi-level passwords?
e. Are all entries by personnel restricted or secured areas recorded?

II.F. *Access controls: is hardware and software maintenance properly monitored/ controlled?*

1. Do supervisory activities ensure that all hardware and software-maintenance is:
i. Identified?
ii. Authorized?
iii. Recorded?
iv. Reviewed?
v Monitored?

II.G. *Access controls: is the operating system properly controlled?*

a. Are the operating system options / configuration settings properly documented?
b. Is the operating system free of extensive modifications?
c. Are the modifications in operating system configuration-settings subject to the same controls as application programmes?
d. Does the data processing department have a system-software programmer on staff?
e. Are the patches/ upgrades / updates applied regularly on operating systems and other system applications?

II.H. Access controls: Distribution of Reports

a. Do the procedures for receipt and distribution of computer-outputs ensure that access to information is authorized?

b. Is a report distribution list used, for this purpose?

c. Do the waste disposal procedures include the destruction of obsolete reports, which contain sensitive data?

II.I. ***Access controls: is access to blank cheques, demand drafts and other critical documents controlled?***

a. Are these documents issued (internally to the concerned employee/s) on the basis of run schedules only?

b. Are these documents kept locked in a secure location when unattended?

c. Are records of supply of these forms maintained?

d. Are records of ACCESS TO supplies of these forms maintained?

e. Are these documents periodically inventoried?

f. Are the documents pre-printed?

g. Are the documents pre-numbered or sequentially numbered and accounted for?

II.J.*Access controls: is there other access controls in place in the following areas?*

a. Are all computer language-compilers removed from the production system, (and at the location of software development site, protected from unauthorized access)?

b. If the computer system uses an interpreter of the language, have adequate measures been taken to prevent the illegal interrupt of programme execution or alteration of programme logic by computer operators?

c. Are report-generation packages secured from the update capabilities (especially from modifying the contents of the reports generated)?

d. Do the reports generated clearly identify their source?

e. Is the availability of utilities, which can be used to alter or copy data and programmes restricted and controlled?

III. <u>Authorization</u>

III.A. ***Authorization:*** *does the senior management or a committee authorize the following IS-related functions?*

a. IS Personnel Policy?

b. Hardware Policy?

c. Software Policy

d. Software Development Policy?

e. Programming Methodology?

f. IS Security Policy?

g. Documentation Policy?

h. Information Policy?

i. Priorities of IS-related activities?

j. Major system / design /equipment changes?

k. Manpower allocations by project?
l. Procedures for security and control measures?
m. Research and Development studies?
n. IS budgets?
o. IS long-range plans?

III.B. *Authorization: are only authorized transactions processed, and unauthorized transactions (if any) identified?*

a. Are clerks / computer-operators provided an approval-form to assure authorization (in addition to on-line authorization), in order to process the transactions?
b. Does the computer system verify authorization for transactions entered on-line, through terminal identification? (i.e. a data-entry terminal cannot be used simultaneously as authorization terminal).
c. Are individuals held accountable for all transaction-activities through the use of transaction - logs?
d. Do the transaction logs contain the log in-id, the source (i.e. terminal #), Voucher #, Date & time of transactional for ALL the transactions during on-line data-entry?
e. Are permanent records of ALL the live programmes and data on the computer system (in the following areas), maintained by System Administrator as well as Branch Manager?

i. Production (i.e. live) files and directories?
ii. Production programme libraries?
iii. Production environment parameter settings (e.g. O.S. and DBMS configuration settings)?

III.C. *Authorization: are written standards developed / prepared to provide management's general and specific authorization for various IS-related activities?*

a. Is a written manual of systems and procedures available for all computer operations, and does it provide a definition and explanation of management's general and specific authorization to process transactions?
b. Are there written standards for:
i. Hardware selection?
ii. System Software selection?
iii. Application package selection?
iv. Network component selection?
v. System design and development?
vi. Programming standards?
vii. Testing?
viii. Programme approval standards?
ix. Implementation (including procedures for putting a programme/system into production)?
x. Hardware and especially Software Change Management Procedures?

•The Chandigarh State Co-op. Bank Ltd.• Chandigarh
Sector 22-B

III.D. *Authorization: is system development properly controlled?*

a. Is a formal System Development approach used? (Please specify):
b. Does management make a clear distinction between production (i.e. live) and development programmes?
c. Is "prototyping" done?
d. Do the procedures for system design, including the acquisition of software packages require active participation by representatives of users, accounting, internal audit, and computer auditors (I.S. auditors), as appropriate?
e. Does each system have a written (in detail) specification, which are reviewed and approved by management, and applicable users before preparation of the detailed systems design specifications to assure implementation of an acceptable quality standards?

III.E. *Authorization: are new systems adequately tested?*

a. Do software-testing a joint effort of programmers, system developers, computer (I.S.) - auditors, and users?
b. Does system testing include testing of both, the manual and computerized phases of the system?
c. Is test data developed to specifically test the functioning of programmed control procedures?
d. During parallel testing, is consideration given to whether errors exist in the populated data, to test programmed controls?
e. Is documentation of system tests (data and results) retained for future use, which will be required in case of later system modifications?
f. Are test results reviewed and approved by user / management personnel before authorizing the transfer of programmes into the live environment?
g. Do final testing procedures provide user, management, IS-staff and IS-audit personnel with a clear identification of the programme version used to perform the test?
h. Are programmers prohibited from using live data files to test programmes?

III.F. *Authorization: Is system conversion adequately planned and controlled?*

a. Are formal, written conversion procedures prepared?
b. Is formal approval by system development steering - committee / management and IS auditor obtained, of IS related activities including a review of changes from original design specifications, review of system test results, review of input and output controls, and review of documentation prior to putting a new system into production?
c. Are these written conversion procedures approved by management, internal audit, IS auditing, user departments and accounting personnel as appropriate?
d. Are all master file / table and transaction file / table conversions controlled to prevent unauthorized changes, to provide accurate and complete results, and to ensure data integrity?
e. Do programme transfer - procedures ensure that only those programmes, which were used for the final test, are transferred to the live environment?

f. Are control totals such as record counts and hash total established to allow reconciliation of converted files to the original manual or computer files?
g. Are critical matter files / tables printed before and after conversion (e.g. deposits file, payroll master file / table, central information table / file, etc.)?
h. Does someone without incompatible duties compare the before and after details of these critical matter files / tables?

III.G. *Authorization: are programme changes authorized?*

a. Do policies and procedures for initiating changes to programmes and other forms of processing logic ensure that management authorizes all changes?
b. Do policies, procedures and mechanisms ensure that personnel responsible for application programme perform no changes to the operating system configuration?
c. Is a log maintained of all changes requested that identify the person initiating the change, the date initiated and the date implemented?
d. Does this log also identify the specific programme (s) and / or operating procedures affected by the change?

III.H. *Authorization: are programme changes monitored and controlled?*

a. Do procedures ensure that all changes to the system are documented?
b. Are programme modifications made ONLY TO COPIES OF current production programmes rather than the programmes themselves?
c. Does a responsible official INDEPENDENT OF PROGRAMME authorize operations personnel to put a modified programme into production?
d. Are source programmes supplied when programme changes are authorized for putting into live operation?
e. Is the following documentation obtained / prepared before and after each change, and retained as a permanent record?
i. Files / directories in the system?
ii. Production library directories?
iii. Programme source listings?
iv. Operation procedures' listings?
v. Systems flowcharts?
vi. Data flow diagrams?
vii. Entity Relationship (ER) diagrams?
f Are operations' procedures updated to reflect system changes?
g Do system administrators of all transfers to production libraries (i.e. live environment) maintain logs?
h If patching techniques are used:
i. Are they allowed only in emergencies?
ii. Are they allowed only after supervisory approval?
iii. Are records of patches maintained, including appropriate approvals, records of the instructions / routines altered, the name of the person making the changes and the reason for the changes?

The Chandigarh State Co-op. Bank Ltd
Sector 22-B

IV. *Supervision and Review*

IV.A. ***Supervision and review:*** *are IS related activities subject to review by management?*

a. Is management knowledgeable about the activities performed by the computer system and the methods used for operation and maintenance of the system?

b. Are logs of computer processing and balancing activities available, and reviewed by Management at least on half-yearly basis.

c. Are logs the basis for preparation of performance statistics to be reviewed by management?

d. Are logs the basis for charging computer expenses to user departments, (if applicable)?

e. Is the system log file / table properly controlled to prevent unauthorized changes?

f. Are all reports of reprocessing activity retained, reviewed by supervisory personnel and is computer time accounted for?

g. Is computer processing scheduled, either manually or through automated techniques, and regularly compared to machine utilization reports and / or console logs?

h. Does the processing schedule include periodic (i.e. daily, fortnightly, month-end, quarterly, six-monthly, yearly, exceptional etc.) processing-requirements?

i. Are significant variations from scheduled processing investigated?

IV.B. ***Supervision and review:*** *does the management periodically review access - authorization?*

a. Are authorization levels for terminal users and points of transaction / operation organization periodically reviewed?

b. Do supervisory or managerial personnel routinely review the logs and reports of invalid access attempts?

IV.C. ***Supervision and review:*** *are computer operations well documented and organized in an orderly fashion?*

a. Is computer operations staff (including DBAs / System Administrators, and computer auditors) adequately trained to the extent necessary to perform all their tasks in a systematic manner (without relying upon external personnel)?

b. Do computer processes detect or prevent the initiation of processing steps, which are OUT OF SEQUENCE?

c. Are hardware maintenance boundaries contractually defined with each vendor when the bank (or even a branch / office within a bank) uses hardware from more than one manufacture?

d. Is a record of all Hardware problems (including UPS) properly maintained in a register?

The Chandigarh State Co-op Bank
Sector 22-B

e. Is a record of all Software problems properly maintained in a register?
f. Is preventive maintenance routinely performed?
How frequently?
g. Is a record of such maintenance prepared and reviewed?
h. Is the use of off-line data files for processing, controlled through verification by the system, before the processing is initiated?

IV.D. ***Supervision and review:*** *has management established documentation standards to allow for maintenance and supervision of IS-related activities in the following areas:*

a. Information Systems setup documentation (at each location)?
b. Systems documentation?
c. Programmes documentation?
d. Operations documentation?
e. User documentation (e.g. user profile and the kind of operations he is allowed to perform)?
f. Do supervisors review "Users" and "Technical" manuals to make sure that prescribed documentation standards are adhered to?
g. Are "documentation standards" and "change procedures" adequate to ensure that documentation is maintained in a correct and consistent manner?

IV.E. ***Supervision and review: does adequate and up-to-date system-documentation exist (for every system) including the following:***

a. Systems narrative?
b. Systems flowcharts?
c. Broad input-design?
d. Broad Database design?
e. Broad (context-level) DFDs i.e. Data Flow Diagrams?
f. Data element definitions?
g. Codes Design?
h. Dialogue Design?
i. Broad Procedure-Design?
j. Held Design?
k. Broad Output Design (Report and Screen Design)?
l. Data capture procedures?
m. Backup and recovery procedures?
n. System changes?

IV.F. ***Supervision and review: does adequate and up-to-date documentation exist including the following:***

a. Detailed System Flowcharts?
b. Narrative description of each major programme module, subsystem?
c. In-detail programme-flowcharts?
d. In-detail DFDs (Data Flow Diagrams)?

The Chandigarh State Co-op. Bank Ltd.
Sector 22-B
Chandigarh

e. Decision tables?
f. In-detail database design?
g. In-detail ER diagrams?
h. List of constants, codes and tables used?

Source programme listing?

- Operating System (OS) Commands listings?
- Specimen vouchers?
- Specimen data-entry (and other interface) screens?
- Specimen reports?
- Programme changes?
- Changes in ANY COMPONENT of the system?

IV.G. *Supervision and review: are computer jobs streams supported by computer set-up and run instructions including:*

- Set-up instructions and device assignments?
- Identity of input and output data tables/files?
- Parameters of Job Control Language /OS Commands?
- Normal console/server-messages for each run?
- List of error and halt messages, probable causes, programmed and machines halts, and required action?
- Restart and recovery procedures?
- Estimated run times and maximum run time (for every major job /major task)?
- Form (and distribution) of printed and other outputs?
- End of job instructions?
- Output destination and retention instructions?

IV.H. *Supervision and review: are procedures for input and output documented?*

- Are input procedures documented to describe all tasks necessary for the control of transactions processed by the system including:

i. Input receipt?
ii. Data entry?
iii. Error correction?
iv. Source document control?
v. Permanent record retention?

- Are procedures documented for the generation, verification and distribution of computer output including:

i. Output reports generation?
ii. Report balancing and reconciliation?
iii. Report distribution?
iv. System inquiries?

- Are control totals produced by the system to allow balancing with input control totals including:

i. Batch number?
ii. Amount totals of significant fields?

iii. Hash totals of significant fields?
iv. Transaction or record counts?
v. Ending number of master file records?
vi. Total number of master file / table records?

V. *Security and recovery*

V.A. ***Security and recovery: has the potential risk of events, which could cause short-term or sustained loss of computer-processing capability, been identified?***

❖ Has the maximum time period, for which loss of computer processing could be tolerated without serious disruption to the business, been identified (separately for every business-operation based on nature and criticality of that business operation)?

❖ Has the effect of loss at differing times i.e. start of day, peak business-hours time, end of week, end of month, end of year etc.), been addressed?

❖ Have the effects of daily operating practices, customer reaction, and exposure to loss been considered?

❖ Has the effect of loss of individual components of the system (Hardware components, network components, system and application Software components, data, documentation, people etc.) been isolated?

V.B. ***Security and recovery: has Information Systems activities related insurance coverage been considered for the following risks:***

❖ Equipment destruction?
❖ Programme or software destruction?
❖ Loss of data?
❖ Business interruption?
❖ Errors of omissions?
❖ Fidelity insurance on IS personnel?
❖ Payment for use of alternative equipment?
❖ Annual management review and approval of IS activities related insurance coverage?

V.C. ***Security and recovery: do the plans and procedures exist to prevent a short-term or partial failure in a controlled manner?***

❖ Does the environment for the computer systems conform to manufacturer's specifications for electrical, humidity, temperature and air particle tolerance?

❖ Does the physical location of computer equipment discourage access or interruption by unauthorized personnel and reduce vulnerability to environmental effects and natural disasters?

❖ Does the on-premises backup-storage area provide reasonable protection against accidental damage or destruction of data, programmes and documentation?

❖ Does the bank have written policies and procedures for backup and recovery of all data and programmes stored on magnetic media, to assure sufficient backup exists to restore them if they are destroyed?

V.D. *Do the plans and procedures exist to recover from a short-term or partial system failure in a controlled manner?*

❖ Do procedures exist for recovery in an orderly manner in the event of processing interruptions resulting from such occurrences as equipment malfunction, power fluctuations, software error or loss of on-line data?

❖ Is there procedure for continuation of processing in the absence of key individuals (IS persons) within the branch/office?

❖ Are programmes, which have backup data, included in the routinely run application software, so that the backup procedure will not be a DBA's or operator's choice?

❖ Is at least one current copy of the supervisory and application programme library maintained in the nearby magnetic-storage-library, as immediate backup?

❖ Are error-recovery procedures for short-term failure tested periodically to ensure control of the process?

❖ How frequently?

❖ Are computer operators' duties rotated periodically, to have internal controls, and also to ensure the availability of trained backup staff?

❖ Is the "Maker-Checker" principle used in Software development activities also?

V.E. *Security and recovery: are backup procedures adequate?*

❖ Are current copies of the following maintained off-site? :

i. Operating systems?
ii. Source programmes?
iii. Runtime (executable) codes?
iv. Master data?
v. Transaction data necessary for recovery?
vi. Programme documentation?
vii. Operating instructions?
viii. Critical forms and supplies?
ix. Disaster recovery plan?
x. System documentation?

❖ When "backup copies" of programmes are used, are they duplicated before being put into production?

❖ When backup copies of master or transaction data are used, are they duplicated before being put into production?

❖ Are restoration / recovery procedures tested periodically, after having secured backup copies of all data, software, documentation and transaction sources?

❖ How frequently?

The Chandigarh State Co-op. Bank Ltd. Chandigarh
Sector 22-B

V.F. *Security and recovery: are the arrangements with vendors adequate?*

- ❖ Are vendors responsible for reliable hardware and software support to avoid the possibility of processing interruption due to lack of support?
- ❖ Do remedial equipment - maintenance arrangements provide for response to problems in sufficient time to prevent business disruption?
- ❖ What is the average response time after registering the complaint?
- ❖ Does the equipment maintenance vendor maintain an inventory of replacement components (which are frequently required for local service)?

V.G. *Security and recovery: is the disaster recovery planning adequate?*

- ❖ Is there a detailed disaster recovery planning explaining procedures and steps necessary for recovery after the disaster?
- ❖ Is a copy of the plan stored off premises or in a location where it would not be destroyed in the event of a disaster?
- ❖ Have backup alternatives been considered (i.e. hot site, cold site, warm site, reciprocal arrangements, etc.)?
- ❖ Are alternative computer equipment arrangements tested periodically to ensure that the plan functions?
- ❖ Has the disaster recovery plan been tested?
- ❖ How frequently?

V.H. *Security and recovery: is other recovery - considerations adequate?*

- ❖ Do documented operating procedures permit continuation of computer processing in the event of permanent loss of key operations personnel?
- ❖ Does the documentation of the system permit maintenance by alternate support personnel in the event of loss of key programmers?
- ❖ Does the Disaster Recovery Plan (DRP) include the provision for continuation of business operations in the event of any (minor or major) disaster?
- ❖ Is the bank (i.e. every computerized branch and office) in compliance with the regulatory / statutory requirements, with respect to retention of data, generate reports which is in the machine-readable form?

****

•The Chandigarh State Co-op. Bank Ltd. • Chandigarh •
Sector 22-B

Annex - B

IS Audit Scope

The indicative scope of IS Audit is given below :

- Alignment of IT strategy with Business strategy
- IT Governance related processes
- Long term IT strategy and Short term IT plans
- Information security governance, effectiveness of implementation of security policies and processes
- IT Architecture
  - Acquisition and Implementation of Packaged software
    - Requirement Identification and Analysis
    - Product and Vendor selection criteria
    - Vendor selection process
    - Contracts
    - Implementation
    - Post Implementation Issues
  - Development of software - In-house and Out-sourced
    - Audit framework for software developed in house, if any
    - Software Audit process
      - Audit at Program level
      - Audit at Application level
      - Audit at Organizational level
    - Audit framework for software outsourcing
  - Operating Systems Controls
    - Adherence to licensing requirements
    - Version maintenance and application of patches
    - Network Security
    - User Account Management
    - Logical Access Controls

The Chandigarh State Co-op. Bank Ltd. Sector 22-B Chandigarh

  - System Administration
  - Maintenance of sensitive user accounts
- Application Systems and Controls
  - Logical Access Controls
  - Input Controls
  - Processing Controls
  - Output Controls
  - Interface Controls
  - Authorization Controls
  - Data Integrity / File Continuity controls
  - Review of logs and audit trails
- Database Controls
  - Physical access and protection
  - Referential Integrity and accuracy
  - Administration and Housekeeping
- Network Management audit
  - Process
  - Risk acceptance (deviation)
  - Authentication
  - Passwords
  - Personal Identification Numbers ('PINS')
  - Dynamic password
  - Public key Infrastructure ('PKI')
  - Biometrics authentication
  - Access Control
  - Cryptography
  - Network Information Security
  - E-mail and Voicemail rules and requirements
  - Information security administration
  - Microcomputer / PC security

The Chandigarh State Co-op. Bank Ltd.
Sector 22-B
Chandigarh

    - Audit trails
    - Violation logging management
    - Information storage and retrieval
    - Penetration testing
- Physical and environmental security
- Maintenance
    - Change Request Management
        - Software developed in-house
    - Version Control
    - Software procured from outside vendors
    - Software trouble-shooting
        - Helpdesk
    - File / Data reorganization
    - Backup and recovery
        - Software
        - Data
        - Purging of data
    - Hardware maintenance
    - Training
- Internet Banking
    - Information systems security framework
    - Web server
    - Logs of activity
    - De-militarized zone and firewall
    - Security reviews of all servers used for Internet Banking
    - Database and Systems Administration
    - Operational activities
    - Application Control reviews for internet banking application
    - Application security
- Privacy and Data Protection

The Chandigarh State Co-op. Bank Ltd.
Sector 22-B
Chan

    - Controls established for data conversion process
    - Information classification based on criticality and sensitivity to business operations
    - Fraud prevention and Security standards
    - Isolation and confidentiality in maintaining of Bank's customer information, documents, records by banks
    - Procedures for identification of owners
    - Procedures of erasing, shredding of documents and media containing sensitive information after the period of usage.
    - Media control within the premises

- Business Continuity Management
    - Top Management guidance and support on BCP
    - 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')
        - Minimising 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.
    - Independent Audit and review of the BCP and test result
    - Participation in drills conducted by RBI for Banks using RTGS / NDS / CFMS services
    - Maintaining of robust framework for documenting, maintaining and testing business continuity and recovery plans by Banks and service providers

- Asset Management

The Chandigarh State C
Sector 22-B
Bank Ltd.
Chandigarh

  - Records of assets mapped to owners
  - For PCI covered data, the following should be implemented :
    - 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, authentication 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.

- Human Resources
  - Recruitment policy and procedures for staff
  - Formal organization chart and defined job description prepared and reviewed regularly
  - Proper segregation of duties maintained and reviewed regularly
  - Prevention of unauthorized access of former employees
  - Close supervision of staff in sensitive position
  - People on notice period moved in non-sensitive role
  - Dismissed staff to be removed from premises on immediate effect
- IT Financial Control
  - Comprehensive outsourcing policy
  - Coverage of confidentiality clause and clear assignment of liability for loss resulting from information security lapse in the vendor contract
  - Periodic review of financial and operational condition of service provider with emphasis to performance standards, confidentiality and security, business continuity preparedness
  - Contract clauses for vendor to allow RBI or personnel authorized by RBI access relevant information / records within reasonable frame of time.
- IT Operations
  - Application Security covering access control
  - Business Relationship Management
    - Customer Education and awareness for adaptation of security

The Chandigarh State Co-op. Bank
Sector 22-B

measures

- Mechanism for informing banks for deceptive domains, suspicious emails
- Trade marking and monitoring of domain names to help prevent entity for registering in deceptively similar names
- Use of SSL and updated certification in website
- Informing client of various attacks like phishing

- Capacity Management
- Service Continuity and availability management
    - Consistency in handling and storing of information in accordance to its classification
    - Securing of confidential data with proper storage
    - Media disposal
    - Infrastructure for backup and recovery
    - Regular backups for essential business information and software
    - Continuation of voice mail and telephone services as part of business contingency and disaster recovery plans
    - Adequate insurance maintained to cover the cost of replacement of IT resources in event of disaster
    - Avoidance of single point failure through contingency planning
- Service Level Management

- Project Management
    - Information System Acquisition, Development and Maintenance
        - Sponsorship of senior management for development projects
        - New system or changes to current systems should be adequately specified, programmed, tested, documented prior to transfer in the live environment
        - Scrambling of sensitive data prior to use for testing purpose
    - Release Management
        - Access to computer environment and data based on job roles and responsibilities
        - Proper segregation of duties to be maintained while granting access in the following environment -
            - Live

The Chandigarh State Co-op. Bank Ltd.
Sector 22-B

        - Test
        - Development
    - Segregation of development, test and operating environments for software
- Record Management
    - Record processes and controls
        - 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
    - Periodic review of software licenses
    - Legal and regulatory requirement of Importing or exporting of software
- IT outsourcing related controls
- Detailed audit delivery channels and related processes like ATM, internet banking, mobile banking, phone banking, card based processes
- Data centre operations and processes
  Review relating to requirements of card networks (for example, PIN security review)

5. **Technical Eligibility Criteria:** Bidder must comply all the four points to qualify in technical

SN	Eligibility Criteria	Documents to be submitted as proof	Complied (Yes/No)
1	Bidder should be Government Organization / PSU / PSE / partnership firm under Partnership Act / LLP /private or public limited company in India at least for last 5 years as on date of bid.	Documentary Proof to be attached (Certificate of Incorporation). Submit copy of PAN Card, GST Registration, Any other registration document etc	
2	Bidder must not be blacklisted / debarred by any Statutory, Regulatory or Government Authorities or Public Sector Undertakings / Banks (PSUs / PSBs) or Private Banks or Financial Institutions since last 3 FY years and till date.	Letter of confirmation (self-certified letter signed by authorized official of the bidder)	
3	The Bidder should have a certification who possess qualifications such as: CISA /ISA/DISA/ CISSP	Documentary Proof to be Attached	
4	The Bidder should have performed IS Audit/ Risk Assessment in at least 2 Banks	Purchase order from the Banks to be attached.	

The Chandigarh State Co-op. Bank
Sector 22-B
Chand

6. Financial Bid Performa:

SN	Particulars	GST	Total Amount in Rs (Including GST)
1	**IS Audit Fees per Year**		

Sd/

Administrator
The Chandigarh State Coop Bank Ltd
SCO 1088-89, Sector 22 B,
Chandigarh, 160022

Chandigarh State Co-op. Bank Ltd.
Sector 22-B
Chandigarh