AGREEMENT

AGREEMENT for System Audit of CBS implementation in District Cooperative Bank, _____

This Agreement is made on **13th day of March, 2013** between;

_____ [Insert the name of the Bank], a co-operative society registered under the Uttar Pradesh Cooperative Societies Act.1965 and carrying on Banking business under the Banking Regulation Act - 1949 and having its Registered Office at [Insert the full Address of the Registered Office of the Bank] _____, through its General Manager, (hereinafter referred as "Bank" and abbreviated as "DCB" which expression shall, unless repugnant to the context or meaning thereof, means and includes its successors and assigns) **OF THE FIRST PART (First Party)**:

AND

M/S **Singh Agarwal & Associates**, a registered partnership firm of chartered accountants (hereinafter referred as "System Auditor" which expression shall, unless repugnant to the context or meaning thereof, means and includes its successors and assigns) having its registered head office at 30, Ashok Marg, Ist Floor, Corporation Bank Building, Lucknow, **OF THE OTHER PART (Second Party).**

Collectively Bank and M/S Singh Agarwal & Associates may be referred as 'Parties'.

The "System Auditor" is engaged in providing services in the field of auditing including system audit of CBS implementation in various organizations including Banks etc and agreed to act as the Service Provider of the Bank.

Whereas Bank is desirous of availing the services of the System Auditor enumerated in this Agreement in respect of conducting System Audit of CBS implemented in the Bank including its branches, head office and data centre etc as detailed elsewhere in this agreement.

The terms and conditions of the assignment as System Auditor are given here under:

1. **Services**
   i) Scope of work for system audit shall be as enumerated in **Annexure – 1**;

   ii) General terms and conditions and conditions related to payments and other matters shall be as referred in **Annexure – 2**;

   iii) Major areas which will be required to be audited is as detailed in **Annexure – 3**;

2. **Terms of the Agreement**
   (Commencement and completion of the agreement)

   i) **Effectiveness of the Agreement**.
   The Agreement shall come into force **w.e.f. 13th March, 2013,** the date on which the said System Audit is undertaken by the System Auditors on the basis of scope of work.
   ii) **Expiration of the Agreement**.
   The Agreement shall terminate with the satisfactory completion of the System Audit of all the specified units and submission of signed off System Audit Reports.

3. **Performance standards**
   The System Auditor shall undertake the System Audit with the highest standard of professional and ethical competence and integrity. They shall promptly replace their official / Personnel conducting the System Audit in case of their performance is found unsatisfactory.

4. **Sub contract assignment.**
   In no case the System Auditor shall sub contract this Agreement.

5. Change Procedure

A change identified at any stage of this Agreement, which requires the deliverable under development to deviate from the then current base line will be conveyed by the Bank to the System Auditor in the form of change procedure document. The request for change will then be enforced by the System Auditor.

6. Confidentiality

No information relating to the System Audit conducted under this Agreement shall be divulged by the System Auditor to any other person, authority or agency without the written consent of the Bank. Strict secrecy will be maintained in respect of all information and transactions between the parties.

7. Ownership of System Audit Report.

Any System Audit Report or other material, software or otherwise prepared by the System Auditors for the Bank under the Agreement shall belong to and remain the property of the Bank. The System Auditors may retain a copy of such documents.

8. Delegation

Neither the Bank nor the System Auditors will have the right to delegate any right or obligations concerning this Agreement without the consent of the other party.

9. Law Governing the Agreement.

The laws prevalent in the state of Utter Pradesh shall govern this Agreement.

10. Jurisdiction

Only the courts established at Lucknow will have the jurisdiction to decide any dispute between the parties.

11. Language for communication

The official language for communication on this Agreement will the English / Hindi; Further all deliverables will be in English or in Hindi Languages only.

In WITNESS thereof the parties hereto have executed these presents at ……. through their respective authorized signatories and have affixed their respective seals to this agreement on the day and year first above mentioned.

SIGNED ON BEHALF OF	**SIGNED ON BEHALF OF**
…….[Insert the Bank name]	M/s Singh Agarwal & Associates
SIGNATURE WITH SEAL	SIGNATURE WITH COMPANY SEAL
NAME:	NAME:
TITLE:	TITLE:
PLACE: …….	PLACE:
DATE	DATE:

Witness	Witness
Signature	Signature
Name	Name

Scope of work:

Sl. No.	Point	Scope of Work and deliverables
1.		Pre & Post Delivery Inspection (PDI) / Acceptance Test of Computer Hardware and related peripherals, Equipments, Components etc. / ATMs/ UPS/VSAT/ Communication & network Equipments / any other hardware procured by the bank.
1A.		*Submit the methodology as to how the audit will be conducted by you and the deliverables based on following suggestive requirements*
		IS audit of CBS Banking application software i. Banking Application Software (Front Office as well as Back Office), Head Office application software's audit to verify that the designing tools and techniques used by the vendor is appropriate or not. ii. The auditor will also verify that the software does not have any security leakage and the software does not give such errors which affects throughout the application software in the long run which directly or in directly affects the bank's socio-economic health. iii. Whether the code optimization technique has been used or not. iv. Appropriate system logic has been developed by the vendor or not. v. Proper security features has been considered as per the standard norms. vi. The reports generated by the application software are accurate, following RBI and other statutory bodies' guidelines or not. **vii.** the environment (Operating System, Front End, Back End, Storage and backup software, Security software and other associated accessory software are licensed with latest versioned...)used to developed the application software is license an up to date or not. **viii.** Detailed and comprehensive control audit of each and every functionality in the software covering every banking domain (For example deposits, loans, bills, lockers, transactions. . etc) **ix.** User access control audit involving login/logout, password, user profile maintenance, access to application/database files, access controls required for data base administrator, system administrator **x.** Roles and privileges management **xi.** Monitoring system access and use **xii.** Income and Expenses module related detailed audit to ensure that there is no income leakage **xiii.** Ensuring that there is perfect control on possible irregularities and frauds **xiv.** All compliance as per IT Act 2000 and subsequent amendments **xv.** *Submit the comprehensive, easily understandable audit report* **xvi.** explain the audit outcome and suggest ways to overcome the deficiencies (if any) **xvii.** Your suggestions to overcome the deficiencies shall also include the method to be adopted by the Bank, in case it is not at all possible to correct the application software to comply with your audit report.

2.		**Data Center Audit and order checking**
	(a)	i. Physical and logical access controls ii. Infrastructure / Environmental controls iii. Operational controls iv. IT security organization controls v. Mobile/ATM computing vi. Power management controls vii. Personnel security viii. Data protection related issues ix. DBA and System administration controls x. Backup and recovery controls xi. Business continuity controls xii. Cryptography, Digital signature, licensing and related issues as per IT Act and other relevant laws and guidelines of controlling authorities *xiii. Submit detailed, informative and comprehensive audit report covering above* xiv. Check the various configurations of respective hardware installed at DC to ensure that the same is as per order or not. xv. Check other components installed in/for DC (other than hardware) xvi. *Submit order checking report for the DC*
3.		**Network Audit**
		i. Conduct comprehensive audit of the network ii. Audit related with Routers and related components iii. Key management iv. *Submit detailed, informative and comprehensive audit report covering above*
4.		**Audit and checking at + HO**
	(a)	i. Visit all the branches and conduct detailed IS / EDP Audit of branches as per RBI Guidelines ii. Check the hardware supplied by vendors to ensure its correctness Vs. Order with detailed information about the item like in case of software Product Name, Version, IPR, CISA certification, License detail etc... And In case of Hardware Model, Make, Specification, Product Sr. No., Warranty, etc... iii. Check the network equipments supplied by vendors to ensure its correctness
5.		Any other related audit job required by the bank.

Terms & Condition:-

General Terms and condition:

i. System Auditor will verify whether items supplied are as per the work order issued by the bank.
ii. The system auditor in association with bank's staff will prepare a format of report / Check-List to verify the items supplied by the vendor (For Example Sr.No, Name of the item, Configuration, Make, Model, Sr.No.,Warranty, etc...).
iii. The system auditor will verify that the items (Hardware/Software) supplied by the vendor are as per National / Inter National standard.
iv. System Auditor will conduct & perform Auditing work as per standard IS Auditing Norms & RBI Guidelines.

Payment Detail: Payment for entire scope of the work will be as follows:

S. No.	System Audit activities	Per unit Cost Rs.
1.	Systems Audit of Branch hardware & Software @ 5,700/= per branch for ___ branches	
2.	Systems Audit of CBS Banking application software	2,00,000.00
3.	Head Office Hardware and Software Audit	1,25,000.00
4.	Data Center Audit *(Hardware & Infrastructure)*	1,25,000.00
	Total	

Service tax @ 12.36% shall be paid over and above the said cost. Income tax at applicable rate shall be deducted by the Bank at the time of release of payment;

Payment related terms and conditions
Payments for the job of System Auditor will be milestone payments after completion of each assignment. The System Auditor's fees will be paid in the following manner:

25%	Of the System Auditors' fees after two weeks of commencement of the audit work and on submission of audit plan / procedures and methodology covering all the points as per Scope of Work for System
60%	Of the System Auditor's fees on submission of Interim Report covering all the points as per the Scope of Work.
15%	On final Sign-off

Note: Bank will be deducting the TDS at prevalent rates.

Report submission and payment methodology:
System Auditors will submit the System Audit Reports to the Bank in two sets for each auditing units. The Bank will examine the report in reference to Scope of work & T.O.R. and accordingly verify the bill of the System Auditor. Payment of System Audit fees at each stage will be made by the Apex Bank to the debit of The Bank after adopting the said System Audit Report in the committee formed for the purpose.

Broad terms and conditions of the Contract / agreement:

The Systems Auditors will have to audit the System Architecture and various audit as defined in the scope at the designated locations within the time period specified for this purpose by the bank.

Only Persons having **CISA / DISA & other technical** qualifications together with adequate experience will be utilized by the Systems Audit firm for auditing as team leaders. Franchise of Information Security Auditors will not be permitted under any circumstances.

Arbitration:

The Bank and the System Auditor shall make every effort to resolve amicably by direct informal negotiation any disagreement or dispute arising between them under or in connection with the Contract.

i. If any dispute, difference or question shall at any time arise between the parties as to the implementation / execution of this project or concerning anything herein contained or arising out of this Agreement or as to the rights, liabilities and duties of the parties hereunder, that the decisions of Bank is final and binding, the same shall be referred to arbitration and a final decision, after giving at least 30 days notice in writing to the other (hereinafter referred to as the Notice for Arbitration) clearly setting out the terms of disputes to a sole arbitrator who shall be appointed as hereinafter provided.

ii. For the purpose of appointing the sole arbitrator referred to above, Bank shall send to the System Auditor within 30 days of the notice of arbitration a panel of three names of persons who shall be presently unconnected with the organization of the Bank or the System Auditor.

iii. The System Auditor shall on receipt of the names as aforesaid select any one of the persons so named to be appointed as the sole arbitrator and communicate his name to the Bank within 15 days of receipt of the names. The Bank shall thereupon without any delay appoint the said person as the sole arbitrator. If the System Auditor fails to communicate such selections as provided above within the period specified, Bank shall make the selection and appoint the sole arbitrator from the panel notified to the System Auditor.

iv. If the arbitrator so appointed is unable or unwilling to act or refuse his appointment or vacate his office due to any reasons whatsoever, another sole arbitrator shall be appointed by selecting from remaining persons on the panel by Bank.

v. The sole arbitrator shall have power to open up, review and revise any certificate, opinion of decision, requisition or notice and to determine all other matters in dispute which shall be submitted for arbitration and of which notice shall have been given as aforesaid subject to aforesaid. The arbitrator shall be governed by the Indian Arbitration Act, 1957 or such other Act in force.

vi. The award of the arbitrator shall be binding and final on the parties. It is hereby agreed that in all disputes referred to the arbitration, the arbitrator shall give a separate award in respect of each dispute or difference in accordance with the terms of reference and award shall be a reasoned award.

vii. The fees, if any, of the arbitrator is required to be paid before the award is made and published, be paid in equal proportion by each of the parties. The cost of the reference and award including the fees, if any, of the arbitrator shall be directed to be borne and paid by such party or parties to the dispute, in such manner or proportion as may be directed by the arbitrator in the award.

viii. The Bank and the System Auditor also hereby agree that the arbitration under this clause shall be a condition precedent to any right of action under the contract with regard to the matters hereby expressly agreed to be so referred to arbitration.

ix. Securities contained to be rendered notwithstanding any reference or dispute to the arbitration. It is specifically agreed that the System Auditor shall continue to render their services provided herein with all the diligence, professional skill and tact notwithstanding that any matter, question or dispute has been referred to arbitration.

Schedule of System Audit:

Tentative schedule of systems audit will be finalized mutually by the Bank & System Auditor according to system auditing plan to be submitted by the system auditor.

Delays in the Information System Audit

The System Auditor must strictly adhere to the audit schedule, as specified in the Contract, executed between the bank and the System Auditor, pursuant hereto, for performance of the obligations arising out of the contract and any delay will enable the Bank to resort to any or all of the following:

(a) Claiming Liquidated Damages;

(b) Termination of the agreement fully or partly

Liquidated Damages for Delay:

Time is the essence of the contract. If the System Auditor fails to submit the report within the stipulated time and the delay is attributed to System Auditor, Uttar Pradesh Cooperative Bank Limited shall impose Liquidated Damages as under:

Sr No.	Condition	LD %
A	Delay up to one fourth period of the prescribed delivery period / Completion of work	2.50
B	Delay exceeding one fourth but not exceeding half of the prescribed period / completion of work	5.00
C	Delay exceeding one half but not exceeding three fourth of the prescribed period / completion of work	7.50
D	Delay exceeding three fourth of the prescribed period / completion of work	10.00

- Fraction of a day in reckoning period in Systems Audit shall be eliminated if it is less than half a day.
- The maximum amount of liquidated damages shall be 10.00 %.
- If the Systems Auditor requires an extension of time in completion of Systems Audit on account of occurrence of any hindrance, he shall apply in writing to the authority, which has executed the Contract, for the same immediately on occurrence of the hindrance but not after the stipulated date of completion of the Systems Audit.
- Period may be extended with or without liquidated damages if the delay in the supply of documents is on account of hindrances beyond the control of the bidder.
- Also liquidated damages would be deducted from the payment due for that milestone.

Governing Language

All correspondence and other documents pertaining to the contract shall be written in Hindi or English only.

Notices

Any notice given by one party to the other pursuant to this contract shall be sent to the other party in writing or by cable or facsimile and confirmed in writing to the sender's address (the address as mentioned in the contract).

A notice shall be effective when delivered or on the notice's effective date, whichever is later.

Use of Contract Documents and Information

The System Auditor shall not, without the Bank's written consent, disclose the Contract or any provision thereof, or any specification or information furnished by or on behalf of the Bank in connection therewith, to any person(s) other than a person(s) employed by the Security Audit or in the performance of the Contract. Disclosure to any such employed person(s) shall be made in confidence against Non- disclosure agreements completed prior to disclosure and disclosure shall extend only so far, as may be necessary for purpose of such performance.

Any document, other than the Contract itself, shall remain the property of the Bank and all copies thereof shall be returned to the Bank on termination of the Contract, if so required by the Bank.

The System Auditors shall not, without the Bank's prior written consent, make use of any document or information except for purposes of performing the Contract.

Indemnification

The Information System Auditor shall, at their own expense, defend and indemnify the Bank against any claims due to loss of data / damage to data arising as a consequence of any negligence during Information System Audit.

Professional Fees / Charges

The price charged by the Information System Auditor for the services performed shall not vary from the contracted schedule of fees. Taxes as applicable will be deducted from the fees, as per prevailing rules on the date of payments.

Force Majeure

The System Auditor or the Bank is not responsible for delays or non- performance of any contractual obligations, caused by war, blockage, revolutions, insurrection, civil commotion, riots, mobilizations, strikes, blockade, acts of God, plague or other epidemics, fire, flood, obstructions of navigation by ice of port of 11ispatch, acts of Govt. or public enemy or any other event beyond the control of either party which directly, materially and adversely affect the performance of any contractual obligation.

If a force majeure situation arises, the System Auditor shall promptly notify the Bank in writing of such conditions and the change thereof. Unless otherwise directed by the Bank, in writing, the System Auditor shall continue to perform his obligations under the contract as far as reasonably practiced and shall seek all reasonable alternative means for performance not prevented by the force majeure event.

Indemnity

The bidder shall indemnify, protect and save the Bank against all claims, losses, costs or damages, expenses, action suits and other proceedings resulting from infringement of any patent, trademarks, copyrights etc. or such other statutory infringements by the bidder.

Authorized Signatory

The selected bidder shall indicate the authorized signatories who can discuss and correspond with the Bank, with regard to the obligations under the contract. The bidder shall furnish proof of signature identification for above purposes as required by the Bank. The representative so authorized has to submit an authority letter duly signed by the selected bidder, authorizing him to represent on behalf of the bidder.

Publicity

Any publicity by the System Auditor in which the name of the Bank is to be used should be done only with the explicit written permission of the Bank.

Applicable Law and Jurisdiction of court

The Contract with the selected bidder shall be governed in accordance with the Laws of India for the time being enforced and will be subject to the exclusive jurisdiction of Courts at Lucknow (with the exclusion of all other Courts).

Cancellation of Contract and Compensation

The Bank reserves the right to cancel the contract of the selected bidder and recover expenditure incurred by the Bank on the following circumstances:

- The selected bidder commits a breach of any of the terms and conditions of the bid / contract.
- The bidder goes into liquidation voluntarily or otherwise.
- An attachment is levied or continues to be levied for a period of 7 days upon effects of the bid.
- The progress regarding execution of the contract, made by the selected bidder is found to be unsatisfactory.
- If deductions on account of liquidated Damages exceeds more than 10% of the total contract price.

After the award of the contract, if the selected bidder does not perform satisfactorily or delays execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice by giving one month's notice for the same. In this event, the selected bidder is bound to make good the additional expenditure, which the Bank may have to incur for the execution of the balance of the contract. This clause is applicable, if for any reason, the contract is cancelled. The Bank reserves the right to recover any dues payable by the selected bidder from any amount outstanding to the credit of the selected bidder, including the pending bills and/or invoking Bank Guarantee, if any, under this contract or any other contract/order.

Assignment

Neither the contract nor any rights granted under the contract may be sold, leased, assigned, or otherwise transferred, in whole or in part, by the Bidder, and any such attempted sale, lease, assignment or otherwise transfer shall be void and of no effect without the advance written consent of the Bank.

Subcontracting

The selected bidder shall not subcontract or permit anyone other than its personnel to perform any of the work, service or other performance required of the selected bidder under the contract without the prior written consent of the Bank.

Termination

The Bank may at any time terminate the contract by giving written notice to the Audit firm, if the Audit firm becomes bankrupt or otherwise insolvent. In this event, termination will not prejudice or affect any right of action or remedy, which has accrued or will accrue thereafter to the Bank.

The Bank reserves the right to cancel the contract in the event of happening one or more of the following Conditions:

- Failure of the successful Audit firm to accept the contract and furnish the Performance Guarantee within specific days of receipt of purchase contract as stated in the Purchase order;
- Delay in offering services;
- Delay in completing installation / implementation and acceptance tests / checks beyond the specified periods;

In addition to the cancellation of purchase contract, Bank reserves the right to appropriate the damages through encashment of Bid Security / Performance Guarantee given by the Audit firm.

SUPPLEMENTAL TERMS AND CONDITIONS

A. Proprietary and Related Rights

1. Bank Property: All data or information supplied by the Bank to System Auditor ("System Auditor") in connection with the services being provided by System Auditor ("the Services") shall remain the property of the Bank or its licensors. All deliverables to the extent prepared by System Auditor hereunder for delivery to the Bank ("the Deliverables") shall be the property of the Bank.

2. System Auditor Property: In connection with performing the Services, System Auditor may use certain data, modules, components, designs, utilities, subsets, objects, program listings, tools, models, methodologies, programs, systems, analysis frameworks, leading practices and specifications ("Technical Elements"). Certain Technical Elements owned or developed by System Auditor prior to, or independently from, its engagement hereunder and are the sole and exclusive property of System Auditor and System Auditor retains all rights thereto, as well as to all modifications, enhancements and derivative works of such Technical Elements created, developed or prepared by System Auditor during the performance of the Services. System Auditor also retains right to utilize certain tools and packages developed by third party over which System Auditor has acquired the rights to use. In addition System Auditor retains the right to use its knowledge, experience and know-how, including processes, ideas, concepts, and techniques developed in the course of performing the Services, in providing services to other clients. The Bank shall have no rights in the Technical Elements. All working papers prepared by System Auditor in connection with the Services shall remain the property of System Auditor.

B. Confidential Information

Except as otherwise expressly provided in the text of the engagement letter, System Audior receiving Confidential Information, as defined below, in connection with the provision of the Services shall not disclose such Confidential Information outside of its organization or use it for any purpose other than in connection with the Services. "Confidential Information" means all information in which a party has rights that is not generally known to the public and that under all the circumstances should reasonably to be treated as confidential or proprietary, whether or not the material is specifically marked as confidential.

C. Relationship of Parties

1. Independent Contractor: Nothing herein contained will be construed to imply a joint venture, partnership, Principal-agent relationship or co-employment or joint employment between the Bank and System Auditor. System Auditor, in furnishing services to the Bank hereunder, is acting only as an independent contractor. System Auditor does not undertake by this Agreement or otherwise to perform any obligation of the Bank, whether regulatory or contractual, or to assume any responsibility for the Bank's business or operations. The parties agree that, to the fullest extent permitted by applicable law; System Auditor has not, and is not, assuming any duty or obligation that the Bank may owe to its customers or any other person.

2. Concerning Employees: Personnel supplied by either party will be deemed employees of such party and will not for any purpose be considered employees or agents of the other party. Except as may otherwise be provided in this Agreement, each party shall be solely responsible for the supervision, daily direction, and control of its employees and payment of their salaries (including withholding of appropriate payroll taxes), workers, compensation, disability benefits, and the like.

D. Testing Services

1. If the Services include testing, penetration, intrusion or analysis of the Bank's information systems or enterprise whether by using intrusive or passive techniques and software tools ("Testing Services"), the Bank hereby consents to System Auditor performing the Testing Services.

2. If the testing services involve third party System Auditors, the Bank shall obtain all necessary consents of third party System Auditors.

E. Internet e-mail:

The Bank acknowledges that: (i) System Auditor, the Bank and others participating in this engagement may correspond or convey documentation via Internet e-mail.

Major Areas which will require to be audited are:

A) Safeguarding of Assets
B) Data Integrity
C) System Effectiveness
D) System Efficiency

A) Safeguarding of Assets :

The IS auditors will require concentrating on the following areas to ensure that the Information Systems Assets of the organization are safeguarded:

a. Environmental Security ,
b. Uninterrupted Power Supply
c. Electrical Lines
d. Data Cables & Networking Products
e. Fire Protection
f. Insurance of Assets
g. Annual Maintenance Contract
h. Logical Security & Access Control - Operating System Level
i. Logical Security & Access Control – Application System Level

The IS auditor shall be required to verify/inspect the following points in respect of the areas mentioned above.

a). Environmental Security: The IS auditors should verify whether:

a) There is separate room for the server.
b) Server room has adequate space for operational requirements.
c) Server room is visible from a distance, but is not easily accessible.
d) Server room is away from the basement, water / drainage systems.
e) Server room can be locked and the key being under the custody of the authorized persons (System Administrator) only. Entry doors are protected by biometric/PIN or proximity key card access verification. Any failed attempts or system tampering as also unscheduled movement in restricted areas, glass breakage or the opening of doors will require be logging and immediately reporting to the Control Staff at the site. The biometric system will require storing all attempts at access.
f) To access any equipment in the Data Centre, one has to pass through (preferably) a minimum of two separate security doors, utilizing biometric/PIN and/or proximity key card access verification facilities.
g) Server is not in close proximity to the UPS room.
h) Access to server room is restricted to authorized persons and activities in the server room are monitored.
i) Air-conditioning system provides adequate cooling.
j) Storage devices to keep stationary and other such items are not kept inside the server room.
k) All the walls with potential access will require to be heavily reinforced.

l) Humidity and heat measuring instruments like (Thermometer and Hygrometer) are installed in the server room.
m) Temperature readings are taken through out the raised floor and equipment areas, power rooms, basement, diesel fuel storage area, roof, generator, cooling towers, waiting and display areas.
n) Smoking, eating and drinking are prohibited in the server room to prevent spillage of food or liquid into sensitive computer equipment.
o) Briefcases, handbags and other packages are restricted from the server room, tape library and other sensitive computer area to prevent unauthorized removal of data held on removable media as also to prevent entry of unacceptable material into the area.
p) Server room is neat and clean to ensure dust free environment.
q) Scanners are kept in safe custody and access is restricted.
r) Floppy disk drives on the nodes can be disabled, if necessary for better security.
s) Steel bollards to be placed in the front of the building to prevent vehicular ingress.
t) Data Centre to be so chosen to have police protection and fire prevention services within a very short time, say, 5-10 minutes.

b). Uninterrupted Power Supply:

In addition to the availability of the Generator facility at the site, the IS auditor should verify whether:

a) There is a separate enclosure and locking arrangement for the UPS.
b) Maintenance agency provides battery service regularly.
c) There is a regular contract for maintenance of the UPS and the preventive maintenance is carried as per the contract.
d) The record of the tests undertaken is maintained to verify the satisfactory functioning of the UPS.
e) UPS cabin has adequate ventilation to take care of acid fumes emitted by the Lead Acid batteries.
f) Capacity of the UPS system is sufficient to take care of the electricity load required for computers installed.
g) UPS is free of the electricity load relating to the tube-lights, fans, water coolers etc.
h) UPS functions properly when electricity fails.

c) Electrical lines:

The IS auditors should verify whether:

a) There is a separate dedicated electrical line for the computer equipment.
b) Power supply to computer equipment is through UPS system only.
c) The electrical wiring looks concealed and is not hanging from ceiling or nodes.
d) The circuit breaker switches exist in locked condition only.

d). Data Cables:

The IS auditors should verify whether:

a) A map of the cable layout is kept in a secure place with proper authority. This is helpful in timely and fast repairs of LAN cable faults.
b) Cabling is properly identified and recorded as fiber optic, co-axial, unshielded twisted pair (UTP) or Shielded Twisted Pair (STP).

c) Electrical cable and data cable do not cross each other to avoid possible disturbance during data transfer within the network.

e). Fire Protection:

The IS auditors should verify whether:

a) Fire alarm system is installed.
b) Smoke detectors are provided in the server room and in the other areas of computer installations.
c) Smoke detectors are tested on a regular basis to ensure that they work.
d) Gas type (Carbon dioxide, Halon etc.) fire extinguishers are installed at strategic places like server room, UPS room and near the nodes and printers.
e) Dry powder or foam type extinguishers should not be used as they tend to leave deposits.
f) Staff knows how to use the fire extinguishers.
g) Fire extinguishers are regularly refilled / maintained.
h) An evacuation plan is documented and rehearsed at regular intervals for taking immediate action in the case of the outbreak of fire.

f). Insurance:

The IS auditors should verify whether:

a) All the computer equipments are covered under the appropriate electronic equipment insurance policy with a reputed insurance firm.
b) A record of the original policy is maintained with the detailed list of the equipments covered under the policy.
c) Information regarding shifting of computer equipment to or from or within the department/office is conveyed to the insurance firm.
d) Adequacy of the insurance cover should be verified as per the policy of the organization.

g). Annual Maintenance Contract:

The IS auditors should verify whether:

a) Stamped agreements for maintenance contract are executed and available.
b) Activities carried out during maintenance have been reported in the registers and duly authenticated.
c) Contract renewal rates are maintained in the register.
d) Access for maintenance purpose is granted only on verifying the identity of the service person.
e) The maintenance staff support is available in time.

h). Logical Security & Access Control – Operating System Level:

The IS auditors should verify whether:

a) Access to the systems is only through password protected user IDs.
b) Operating System (OS) allots unique user identity (ID) for all users.
c) OS provides for different levels of access rights to volumes, directories and files.
d) OS prompts for change of the user password after the lapse of specified periods.

e) OS ensures secrecy and security of the user passwords and the access rights granted to a user.
f) Unrestricted access to the systems is provided only to the System Administrator.
g) Administration level access is restricted to authorized and limited persons.
h) All the security features available in the OS are enabled/taken advantage of as far as possible for ensuring better security.
i) Administration access should not be available to the officials who are under notice period, retiring shortly, under disciplinary action etc.
j) OS provides for loading of virus prevention software and is implemented.
k) Record is maintained and authenticated regarding the installation of the Operating System, its up-gradation, re-installation and maintenance.
l) A register is maintained in respect of all the OS level users, giving the details such as the date of creation, suspension, cancellation, access rights granted, purpose of creation etc.
m) Users created for audit/maintenance purpose are disabled immediately after the work is over.
n) The department reviews the number of the OS level users periodically.

i). Logical Security & Access Control – Application System Level:

The IS auditors should verify whether:

a) System provides for unique user IDs and password for all users.
b) System provides for different levels of access.
c) System prompts for change of user password after lapse of specified period.
d) System ensures secrecy and security of the user passwords and the access rights granted to users.
e) Unrestricted access to the entire application system menus is provided only to a Super User.
f) Application makes use of all the security features available at the Application System level.
g) Super User access in application level is not given to staff who is under notice period, retiring shortly, under disciplinary action etc.
h) The application system user list is periodically reviewed.
i) The access privileges granted in the system are in accordance with the designation/duties performed.
j) None of the staff members has multiple level or duplicate access ID in the system.
k) Allocation of the suspended, disabled user ID to new users is avoided.
l) Active user IDs of the transferred, retired, suspended or dismissed employees are not present in the system.
m) There is no dummy user ID created in the system.
n) The user ID of staff on long leave, training etc. is suspended.
o) System logs out automatically if the user is inactive for a specified time (or user consciously logs out when he/she leaves a terminal).
p) System does not allow concurrent login to a single user ID from different nodes.

q) Users, created for maintenance purpose, are cancelled on completion of the job.
r) The system does not allow user to cancel his/her own user ID. s) Authority periodically reviews the user login status report.
t) Users do not share their passwords.
u) Passwords of alphanumeric characters are used.
v) Users do not write their passwords on wall, desk diary etc. and are aware of the need for the secrecy of their passwords.
w) System automatically locks the user ID after unsuccessful login attempts.
x) User log indicating date, time, node, user ID, transactions performed etc. are generated by the system and evaluated by the System Administrator.

B) Data Integrity: The IS auditor will require addressing, among others, the following areas under IS auditing:

a) Data Input Controls
b) Data Processing Controls
c) Patch Programs
d) Purging of Data Files
e) Backup of data
f) Restoration of Data
g) Business Continuity Planning
h) Output Reports
i) Version Control
j) Virus Protection

a). Data Input Controls:

The organizations in the banking and financial sector undertake diverse activities relating to the receipt of deposits, advancement of credit, investment of funds etc. Further, the areas of operation and the level of economic activities could also be different. All these activities, the transactions resulting there-of, the data inputs required therefore including the data input controls to be in place in the organization will require to be judiciously addressed. However, illustratively, such data input controls may relate to the following areas of activity and the IS auditors will require to verify the same.

1) History of signatures scanned is available in the system.
2) The entire stock of cheque books is fed to the system.
3) The cheque books issued are entered and confirmed in the system on day-to-day basis.
4) The data fed in to various accounts including the customer accounts is accurate and correct.
5) Clear administrative guidelines exist regarding the access to live data.
6) Clear guidelines exist for on-line transactions including those put through the INTERNET by the Customers.
7) Data Administration is a part of System Administration. However, Database Administration is separate from System Administration.
8) Data Owner (DA) and Database Administrator (DBA) are independent of both the systems development and operational activities.

i) The roles of DA and DBA are clearly defined in respect of, among others, (i) Definition, creation & retirement of data, (ii) Database availability to Users, (iii) Information and services to Users, (iv) Maintenance of database integrity and (v) Monitoring and performance.

b). Data Processing Controls:

The IS auditor should verify whether:

i. The designated/authorized officials do start-of-day process.
ii. The operating staff pay attention to the error messages displayed on the screen and initiates corrective action.
iii. Entries are cancelled only by the appropriate authority.
iv. Cash entries are not deleted from the system. e) Prescribed reports are generated at the end-of-day process.
v. Printouts are scrutinized and preserved.
vi. Proper record is maintained in respect of the corrections made in database under authentication.
vii. Master data printouts are preserved carefully.
viii. Input to the system through floppy is monitored and controlled.
ix. Use of the scanner is monitored and controlled.

c). Patch Programs:

The IS auditors should verify whether:

a) The application programs are exactly identical with the standard list of approved programs in respect of file name, file size, date and time of compilation.
b) Only approved programs have been loaded in the system.
c) There are programs other than the approved ones.
d) There is a record of the patch programs used and the reason thereof under authentication.

d**). Purging of Data Files:**

The IS auditors should verify whether:

a) Purging activity is recorded and maintained in a register.
b) Purged backup media is kept properly under safe custody.
c) Access to purged data is restricted.

e). Back up of Data:

The IS auditors should verify whether:

a) All the floppies/CDs/tapes, purchased, pertaining to the OS software, application software and utility programs, drivers etc. are recorded in a register and properly stored.
b) Hardware, software, operating system, printer manuals are properly labeled and maintained.
c) Latest user manuals of the application software and other end-user packages running on the system are available for guidance.
d) Daily/weekly/monthly and quarterly back-up of data is taken without fail and is available (as per requirement).
e) Backup tapes are properly labeled and numbered.
f) Proper storage procedures and facilities are in place for backup copies.
g) There is offsite storage of one set of the backup data.
h) Backup tapes are verified / tested periodically by restoring the data and record maintained.
i) Back up media is verified periodically for readability.
j) Record is available in respect of such verification.

k) Backup media are phased out of use after a specified period.
l) Backup register is maintained wherein all the events pertaining to the backup including the procedure of backup are recorded.
m) Physical and fire protection is provided to backup media.

f.) Restoration of Data:

The IS auditors should verify whether:

a) The instructions for restoration of the back-up data have been compiled.
b) The data integrity is verified after the restoration work is over.
c) Activities carried out during the restoration work are recorded indicating date, time, reason for restoration and size of the data restored.

g) Business Continuity Planning (BCP):

The IS auditors should verify whether:

a) Business continuity plan has been documented.
b) BCP covers all levels of disaster from partial to total destruction of facilities and contains guidelines to help determine the level of recovery necessary.
c) A copy of the plan is securely stored off site.
d) Detailed restart procedure has been documented in the plan.
e) BCP has been tested and is regularly tested to assess its effectiveness.
f) There is awareness among the staff members about the BCP and the modalities of its execution in case of an emergency.
g) Ready or alternate source of hardware/software is there to resume business activity within the shortest possible time after disruption.
h) A reliable backup of data and software is available all the times for restoration.

h). Output Reports:

The IS auditors should verify whether:

a) The audit trail report generates the user ID of the operator and the official for any addition / modification / deletion of the transaction data effected in the database.
b) Audit trail report is generated daily. Entries are scrutinized and verified.
c) Audit trail report indicates the evidence/information of unauthorized access outside application menu.
d) List of the cancelled entries is scrutinized and reasons for cancellation are recorded.

i.) Version Control:

The IS auditors should verify whether:

a) The computer system has Authorized Version of an OS, Authorized Version of anti-virus software with its latest updates.
b) There exist the documentary evidence/information about the authenticity and the right to use the copy of the OS software, OS system utility, third party software, the runtime system of specified language or database in use and the anti-virus software.
c) Legally licensed copies of the software are used for computerized operations and the licenses are currently in force.
d) Changes made to the application software with the approval from the controlling office/ department.

j) Virus Protection:

The IS auditors should verify whether:

a) Anti-virus software is loaded in the system.
b) Anti-virus software is regularly updated to cover software updates against the latest viruses.
c) All extraneous floppies are checked for virus including the floppies carried by the IS auditors.

C) System Effectiveness: The IS auditors should verify whether:

a) Computerized operations provide better customer service in terms of time and quality.
b) Staff serves a larger number of customers during the day than prior to the introduction of online operations.
c) Customer information is provided timely and accurately.
d) The system reflects any improvement in the overall quality of products and services offered.
e) System has improved the tasks accomplishment capacity of its users by enabling them to be more productive.
f) Users are satisfied with the performance of the system.
g) System is user friendly and takes less effort.
h) The users are putting the software to frequent use, which requires less effort and is easier to use and the users are satisfied with the performance of the software.

D) System Efficiency: The IS auditors should verify whether:

a) Department/Office ensures the use of every computer asset.
b) Department/Office utilizes every computer asset to its optimum capacity.
c) Periodical maintenance of the hardware asset ensures its uninterrupted service.
d) The online operations help complete day's workload on the same day consuming less time than the time taken for the respective manual operations.
e) The online operations provide accurate, complete and consistent data at each stage of processing.
f) Department/Office takes consistency check of balances daily to aid in the detection of errors or fraud.
g. Department/Office uses the hardware peripherals such as printers, nodes etc. efficiently.