Scope of work for Information Systems Audit

We refer to RBI Circular No. UBD.BPD.Cir.No. 71/12.09.000/2013-14 dated June 11, 2014 on Introduction of Information System(IS) Audit for Urban Cooperative Banks.

Having regard to risks emanating from adoption of technology, there is a need to introduce IS Audit in UCBs. It is therefore, advised that UCBs may adopt an IS Audit Policy, if not already done, appropriate to its level of operations, complexity of business and level of computerization and review the same at regular intervals in tune with guidelines issued by RBI from time to time.

i. UCBs may also adopt appropriate systems and practices for conducting IS Audit on annual basis covering all the critically important branches (in terms of nature and volume of business).
ii. Such audits should be undertaken preferably prior to the statutory audit so that the IS Audit reports are available to the statutory auditors well in time for examination and for incorporating comments, if any, in the audit reports.
iii. IS Audit Reports should be placed before before the board and compliance should be ensured within the time frame as outlined in the Audit Policy.
iv. The above instructions may be implemented during the current accounting year i.e April 1, 2014 to March 31, 2015.

Information Systems Audit Policy for the Banking and Financial Sector (Part 2 of 2) dated 11.03.2002. As per the above report of RBI the following guidelines have been mentioned with regards to IS audit:

Standards & Guidelines for IS Audit (Chapter 8 of the Circular)
8.1 The specialised nature of the Information Systems (IS) auditing and the skills necessary to perform such audits require standards that apply specifically to IS auditing. Such standards will require to be internationally accepted standards only. This will ensure that the IS auditor performs auditing, conforming to the minimum level of acceptable performance and meeting the required professional responsibilities.

8.2 The IS auditing Standards define the mandatory requirements for IS auditing and reporting. The IS auditing Guidelines provide the guidance for the application of the IS auditing standards. The IS auditor should take care of how to achieve the implementation of the Standards, the use of professional judgement in the application of the Standards and should also be prepared to justify any departure/deviation therefrom in the IS auditing work.

8.3 The IS auditor shall prepare the procedure including the information on how to meet the Standards while performing the IS auditing work. However, the procedure shall not set the requirements for IS auditing.

8.4 IS auditing should be performed by personnel with the required expertise and skills such as Certified Information Systems Auditor, Certified Information Systems, Security Professionals etc.

8.5 The profitability and the future viability of the organizations in the banking and financial sector increasingly depend on the continued, secured and uninterrupted operations of the Information Systems. Therefore, it is essential for the IS auditors to be conversant with various aspects of Information Technology and the developments taking place in this area. The role of the IS auditors is to see that the organization's assets are protected and suitable internal controls are in place to protect its information and information resources.

IS audit is responsible for providing an organization with independent and objective views on the level of security that should be applied to the Information Systems. Computer Security on the other hand is responsible for implementing security in the computerized environment. The IS auditor will learn to co-exist with the Computer Security function and work together for the benefit of the whole organization ensuring that professional standards are maintained at all times.

8.6 Major areas, which will require to be IS audited, are broadly as under:
a) Safeguarding of Assets
b) Data Integrity
c) System Effectiveness
d) System Efficiency
e) Organization and Administration
f) Business Continuity Operations

8.7 IS auditing of the above areas at the micro level are as under :

8.7.1 Safeguarding of Assets :
The IS auditors will require to concentrate on the following areas to ensure that the Information Systems Assets of the organisation are safeguarded:
a) Environmental Security
b) Data
c) Uninterrupted Power Supply
d) Electrical Lines
e) Data Cables & Networking Products
f) Fire Protection
g) Insurance of Assets
h) Annual Maintenance Contract
i) Logical Security & Access Control - Operating System Level
j) Logical Security & Access Control – Application System Level

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

A. Environmental Security :
Checking: Central Server Level
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 away from the basement, water/drainage systems.
d. Server room can be locked and the key being under the custody of the authorized persons (System Administrator) only. Any failed attempts or system tampering as also unscheduled movement in restricted areas, glass breakage or the opening of doors will require to be logged and immediately reported to the Control Staff at the site.
e. Server is not in close proximity to the UPS room.
f. Access to server room is restricted to authorized persons and activities in the server room are monitored.
g. Air-conditioning system provides adequate cooling.
h. Storage devices to keep stationary and other such items are not kept inside the server room.
i. Smoking, eating and drinking are prohibited in the server room to prevent spillage of food or liquid into sensitive computer equipment.
j. 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.
k. Server room is neat and clean to ensure dust free environment.
l. Scanners are kept in safe custody and access is restricted.

B. Uninterrupted Power Supply :

Checking: Central Server Level and Branch/Department Level

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 :

Checking: Central Server Level and Branch/Department Level

The IS auditors should verify whether:

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

D. Data Cables :

Checking: Central Server Level and Branch/Department Level

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 :

Checking: Central Server Level and Branch/Department Level

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 :

Checking: Central Server Level

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 organisation.

G. Annual Maintenance Contract :

Checking: Central Server Level and Branch/Department Level

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

Checking: Central Server Level, Dept. of Information Technology Level and Branch/Department 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

Checking: Dept. of Information Technology Level and Branch/Department 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) Super User access in application level is not given to staff who is under notice period, retiring shortly, under disciplinary action etc.
g) The application system user list is periodically reviewed.
h) The access privileges granted in the system are in accordance with the designation/duties performed.
i) None of the staff members has multiple level or duplicate access ID in the system.
j) Allocation of the suspended, disabled user ID to new users is avoided.
k) Active user IDs of the transferred, retired, suspended or dismissed employees are not present in the system.
l) There is no dummy user ID created in the system.
m) The user ID of staff on long leave, training etc. is suspended.
n) System logs out automatically if the user is inactive for a specified time (or user consciously logs out when he/she leaves a terminal).

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

8.7.2 Data Integrity :

Checking: Central Server Level and Dept. of Information Technology Level

The IS auditor will require to address, 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 therefrom, the data inputs required therefor including the data input controls to be in place in the organisation 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.

a) The entire stock of cheque books is fed to the system.
b) The cheque books issued are entered and confirmed in the system on day-to-day basis.
c) The data fed in to various accounts including the customer accounts is accurate and correct.
d) Clear administrative guidelines exist regarding the access to live data.
e) Data Owner(DA) and Database Administrator (DBA) are independent of both the systems development and operational activities.
f) 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:

a) The designated/authorized officials do start-of-day process.
b) The operating staff pay attention to the error messages displayed on the screen and initiates corrective action.
c) Entries are cancelled only by the appropriate authority.
d) Cash entries are not deleted from the system.
e) Prescribed reports are generated at the end-of-day process.
f) Printouts are scrutinized and preserved.
g) Proper record is maintained in respect of the corrections made in database under authentication.
h) Master data printouts are preserved carefully
i) 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 labelled 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. 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) List of the cancelled entries is scrutinized and reasons for cancellation are recorded.

H. 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.

8.7.3 System Effectiveness:

Checking: Branch/Department Level

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.

8.7.4 System Efficiency:

Checking: Dept. of Information Technology Level , Central Server Level, Branch/Department Level & Central Office Level

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.

8.7.5 Organization and Administration:

Checking: Dept. of Information Technology Level and Branch/Department Level & Central Office Level

The IS auditors should verify whether:

a) There is an Information Systems Security Programme for the entire organization, approved by the Board of Directors.
b) There is a Corporate Information Systems Security Policy, well defined and documented and implemented including Information Systems Awareness Programme.
c) There is an established hierarchy in the organization with a Senior Executive in charge of the implementation of the Corporate Security Policy with Information Systems Security Officials at various levels in an Office.
d) Identified System Administrator for each computerized Office / Department, as required.
e) Job description for each level is prepared and implemented (including System Administrator).
f) Training is imparted to all staff members in turn for better results and output.
g) Dual control aspect is implemented for the important operations.
h) The functions of initiating, authorizing, inputting, processing and checking of the data are separated to ensure that no person has complete control over a particular function.
   Therefore, abuse of that function is not possible without collusion between two or more individuals.
i) Rotation of duties is carried out at regular intervals.
j) System Administrator is supervised and controlled with respect to the creation of user ids at the OS level and Application Software level.
k) There are at least 2 persons for key functions of operations to take care of absenteeism.
l) Department/Office ensures to bring up the servers into operation readiness sufficiently in advance before the commencement of the business hours.
m) Computers are covered to keep them free from dust, rain water etc.
n) Clear communication from the Management of the organisation to the effect that each member of the staff is responsible for maintaining security in the organisation, as per the Security Policy.

8.7.6 Burglar Alarm system and security system whether functioning and are adequate.

CPD – Structural Financial Messaging System (SFMS Audit)

The scope of SFMS Audit is as follows:

a) Verification of internal controls on SFMS process at branch level as well as centralized level.
b) Verification of Software and Hardware, if they are according to the norms decided by IDRBT.
c) Verification of Security aspects of Hardware, Software, passwords and digital signatures.
d) Verification of the user rights at the different levels of SFMS system.
e) Verification of messaging system followed for different type of Fund Transfers i.e. RTGS, NEFT, ECS etc.
f) Verification of records and logs maintained for the past transactions i.e. verification of transactions of at least last 3 months.
g) Verification of Compatibility of CBS Software (Fincraft) with SFMS interface.
h) Verification of DRP/BCP arrangements, to confirm the uninterrupted and continuous services.
i) IS Security in terms of Physical Infrastructure, accessibility, OS Application, Connectivity, VAPT, Personnel, Communication System, Database Backup, Monitoring, Archiving, Monitoring, Controls, Logs, Vendor Monitoring, Password Controls.

   All other features which are necessary for maintenance of security, availability, accessibility and serviceability.

ATM & Electronic Channel Department

The scope of ATM Department Audit is as follows:

a) Verification if the requisite regulatory requirements are adhered to by the bank in case of new ATMs installed and operations of ATM.

b) Verify whether periodic visits are made by the ATM channel manager.

c) Verify whether monitoring of uptime is done on a real time basis by the department.

d) Verify whether online system for enabling immediate notification to vendor about breakdown is available.

e) Verify whether system of periodic preventive maintenance is done by the Bank.

f) Verify whether corrective actions are taken on the basis of root cause analysis.

g) Verify whether network penetration testing for ATMs is conducted to check that they are on network or not.

h) Verify discrepancies in cash dispensation:

   i) Whether complaints related to cash dispensation are resolved within 7 days.

   ii) Whether online monitoring of ATMs having higher dispenser problem is done.

i) Check whether regular monitoring and forecasting of cash requirements is made.

j) Verify whether cash levels are set and monitored at intervals? Whether the branch is informed to replenish cash immediately when cash in the machine falls below a pre-determined level?

k) Verify whether the message regarding non-availability of cash in ATMs is displayed before transaction is initiated by the customer.

l) Verify access to grievance redressal mechanism:

   i) Whether systems are in place to provide smooth access to grievance redressal mechanism for ATM related complaints.

   ii) Whether the requisite circulars and grievance redressal procedure is displayed in the ATM premises.

   iii) Procedure of customer complaints redressal and whether time limits for redressals is adhered to by the department.

m) Verify Security measures:

i) Is the security measures adequate at the ATM centres and ATM machines? What are the internal checks and controls in place?

ii) Analysis of complaints to identify complaint prone ATMs and monitoring transactions at the said ATMs.

iii) Customer awareness and education measure.

n) Are there backup power arrangements for the ATMs? If yes, for how long can ATM operations be supported by it.

o) Is the communication link being used for connecting the ATM and branch host server with the ATM controller adequate?

p) Verify whether new ATM cards and PINs are mailed to customers at different time intervals? Verify the procedures in place for customer due diligence and its implementation.

q) Are the records of ATM cardholders, fee status, renewal of cards, hot/warm cards being properly documented?

r) Sanction from appropriate authority and requisite documentation is in place for issue of duplicate, renewed cards and re issue of PIN mailers.

s) Is there a procedure in place for destruction of ATM cards and PIN mailers lying in the branch uncollected beyond a certain period.

t) If an independent sales organization is used as an agent for the bank's privately owned ATMs, does management conduct appropriate identification and due diligence procedures as outlined in the bank's Bank Secrecy Act policy and ATM policy?

u) Verification of immediate blocking of ATM cards in case of loss of ATM card or closure of account by the ATM card holder.

v) Verification of documentation and recording maintained by the department for the following:

i) Stock Records for ATM applications sent to the vendor form embossment of cards, receipt of the embossed cards from the vendor, dispatch of the embossed cards to the branches.

ii) Stock Valuation and reconciliation of ATM/Debit Card Stock lying with the vendor

w) Verify if the ATMs of the Bank are adequately insured.

x) Verify the MPOS and IMPS set up of the Bank with respect to adherence to regulatory requirements and bank's policy.

y) Verify if the reconciliation of the following is done by the branch on a regular basis:

   i) ATM payable and receivable

   ii) MPOS commission

   iii) IMPS commission

z) All regulatory circulars and guidelines are adhered by the department.

Kindly note the above scope is indicative and not exhaustive.