Planning, Documentation and Audit Programme for Information System Audit:

The IS auditor will require to plan the information systems audit work to address the audit objectives and to comply with the applicable professional auditing standards. The IS auditor should follow the guidelines, as under, for planning the information systems audit work. This guideline also set out how the IS auditor should comply with the internationally accepted standards. In the planning process, the IS auditor should normally establish levels of materiality such that the audit work will be sufficient to meet the audit objectives and will use audit resources efficiently.

A preliminary programme for an audit engagement should normally be established by the IS auditor before the start of work. This audit programme should be documented in a manner that will permit the IS auditor to record completion of portions of the audit and identify work that remains to be done. As the work progresses, the IS auditor should evaluate the adequacy of the audit programme, based on the evidence/information being gathered in the process of auditing and indicate the areas that might require extended examination.

The IS auditor's plan should be documented in audit work papers to the extent necessary for the IS auditor to determine that the steps of the plan have been carried out. The IS auditor's plan may be documented on paper or in other appropriate and retrievable form.

Preference will be given to those firms which have previous experience of conducting the said audit.

Standards for IS Audit:

1. The specialized 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 being 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.
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 judgment in the application of the Standards and should also be prepared to justify any departure/deviation there from in the IS auditing work.
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.
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.
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.

Guidelines for IS Audit

1. Major areas, which will require being 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
2. IS auditing of the above areas at the micro level are as under:

2.1 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) 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
2.1.1 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 throughout 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, it's 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.

1. 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 from, 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.
a) History of signatures scanned is available in the system.
b) The entire stock of cheque books is fed to the system.
c) The cheque books issued are entered and confirmed in the system on day-to-day basis.
d) The data fed in to various accounts including the customer accounts is accurate and correct.
e) Clear administrative guidelines exist regarding the access to live data.
f) Clear guidelines exist for on-line transactions including those put through the INTERNET by the Customers.
g) Data Administration is a part of System Administration. However, Database Administration is separate from System Administration.
h) 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:
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) Input to the system through floppy is monitored and controlled. j) 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. 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.

G. 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.

H. Virus Protection:

The IS auditors should verify whether:
a) Antivirus software is loaded in the system.
b) Antivirus 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.

1. 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.

1. 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.

1. e Organization and Administration :

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) The entire staff is involved/motivated for working in the online environment.
h) The department allots online jobs to staff members accessing performance parameters like willingness, aptitude, expertise, skill, experience and knowledge.
i) Record is maintained showing details of the work assigned, period of assignment, rotation, training imparted, login name and acknowledgement obtained.
j) Dual control aspect is implemented for the important online operations.
k) 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.
l) Rotation of duties is carried out at regular intervals.

m) System Administrator is supervised and controlled with respect to the creation of user ids at the OS level and Application Software level.
n) There are at least 2 persons for key functions of online operations to take care of absenteeism.
o) Department/Office ensures to bring up the servers into operation readiness sufficiently in advance before the commencement of the business hours.
p) Computers are covered to keep them free from dust, rain water etc.
q) Clear communication from the Management of the organization to the effect that each member of the staff is responsible for maintaining security in the organization, as per the Security Policy.