

Bank Audit in Computerised Environment

Existing Installation

Auditors need to verify the system software and version being operated at the Branch. It is advised to obtain the licensed copy of the software along with the documentation provided by the vendor and compares the same with the software running in the live environment. To carry out verification, auditor may look into the following:

- a) The software registers to check whether all the softwares in use is entered and maintained desktop-wise.
- b) Note the Name and Version of software currently in use.
- c) It is the latest version of the software authorised by the Central Office of the Bank to be used.
- d) Installation of the Software is in accordance with the directions issued by the Central Office.
- e) All the modules of the software are properly installed and are working. If any module is not in use presently, reason has to be ascertained and documented.
- f) Physical verification of the copies of the softwares, documentation and manuals was carried out by Internal / Concurrent / Statutory Auditors.
- g) The existence of Annual Maintenance Contract is in operation and was duly renewed on the expiry date.

Purchases

Computerisation is a constant process of development and improvement over the previous technology. In this process Banks also upgrade there hardware's and softwares installed to improve efficiency and provide better service to the customers. There has being a phase of such improvements, where branches operating on Automatic Ledger Posting Machines (ALPM) where upgraded to semi-computerised branches and then to fully computerised branches. The fully computerised branches are now in the process of being upgraded to fully networked branches. The phase is not over and there are still ALPM branches, which are in the process of upgradation. Auditors, in many branches might come across the purchases made for new softwares during the concerned Financial Year. To achieve the desired level of satisfaction that the purchase process was in accordance with the guidelines of the Central Office and installation was carried out under the supervision of the appropriate person auditor may verify the following:

- a) Software register is duly updated with new purchases.
- b) Purchase Order was duly filed and purchase was properly authorised and software was obtained from authorised vendor only.
- c) The license of the software, warranty obtained and registration with the manufacturer is completed.
- d) Installation was inspected and completed in the prescribed order.
- e) Purchase was at reasonable value.

Logical Access Controls

To ascertain that assets are safeguarded and data integrity is maintained by the computer system, auditors may verify the following:

- a) Does security policy address specific capabilities of operating systems and require that the available security features be implemented?
- b) Is there a security officer appointed in writing?
- c) Does the security officer ensure that available features have been implemented?
- d) Is there a process in place for granting access levels?
- e) Do users have only the minimum access level needed to do their job?
- f) Are Users' access restricted to specific applications, menus within applications, files, and servers?
- g) Is file maintenance a separate access privilege?
- h) Is maintenance restricted to a minimum number of persons and is it properly approved and reviewed?
- i) Is the password file encrypted?
- j) Are methods in place to detect security violations?
- k) Can security restrictions be overridden?
- l) Are access levels periodically reviewed by the internal auditor?
- m) Are procedures implemented to limit access to workstations after normal working hours?
- n) Is modem access protected by a secure system, such as call back?
- o) Are modem numbers-changed periodically?

Password Controls

There are few fundamental problems in maintaining the integrity of the Password, they are:

- i. Users for their convenience write down the password, as they are hard to remember. ii. Users to reduce the burden of remembering cumbersome passwords, opt for easy to use passwords, which are also easy to guess.
- iii. Users in routine do not change their passwords at regular intervals.
- iv. Users fail to appreciate the importance of having password and consequences of its being compromised.
- v. Passwords in Banks change hands very fast for the convenience of work.
- vi. Certain Access Control Mechanism requires users to enter multiple passwords.
- vii. Certain System Software does not store password in the encrypted form.
- viii. Passwords are not changed / deleted on the transfer / retirement of the operator / officer in the Master Record of the System Software.
- ix. Passwords are transmitted in clear text form, especially in Wide Area Network (WAN).

Auditors are required to take extra caution in verifying the integrity of passwords in the Branches. Following issues should be looked into to establish the integrity:

- a) Password Register for the updating with the changes.
- b) Passwords secrecy is maintained by the following officers of the Bank:

- i. Branch Manager
 - ii. System Administrator
 - iii. Users
 - iv. Authorised Persons
- c) The critical passwords, for accepting sensitive jobs are known only to Branch Manager or System Administrator. Sensitive jobs include:
- i. To enter operating systems.
 - ii. To take back-ups.
 - iii. To monitor disk space.
 - iv. To create/edit Master Records.
- d) The Operating System Password is kept under Dual Control of Branch Manager and System Administrator. The password should be protected in a sealed cover and opened in the presence of at least two persons. It should be changed at once on being opened. .

Day Start-up Activities

Following areas require the attention of the auditor:

- a. Verify that day start-up Activities of a computer system is carried out either by the Branch Manager or System Administrator. It should be properly documented and signed in the register maintained.
- b. Verify the time of commencement of day-start-up activities. It should not be carried o u t prior to the banking hours.
- c. Verify that all the security checks are performed as per the prescribed guidelines from the Central Office of the Bank.
- d. Verify that Banking date is verified daily and check sum facility is used regularly.

Transaction Controls

Following are the areas the auditor may verify along with going through the manuals in relation to data base management:

- a. Date is authorised either by Branch Manager or System Administrator.
- b. The control exists in the software to check that the entries pertaining to current date would be only accepted. There should not be any provision to feed back dated or future dated entries.
- c. In the case of non-usage of terminals, terminals are logged-off.
- d. Register for recording of problems in the software and the suitable action taken.
- e. For only physically present users of the computer system, the requisite terminal/user account is enabled, else the account remains disabled.
- f. Special batch reports are printed, checked, authenticated and duly filed.

Personnel Controls

To discourage misuse of funds and such practices, it is important to implement Personnel Controls. Auditor may verify the following to establish that efficient and effective personnel management practices are followed:

- a. The technical competence of the employees of the bank, operating the computer system.
- b. Whether adequate training was imparted to the employees in connection with the operations of the software, presently being used in the bank.
- c. The segregation of duties among the bank employees and the process of monitoring the performance of each employee.
- d. Authorization for amounts entered by the operators are clearly defined and documented.
- e. Job rotation is carried out at regular intervals.

Day End Activities

Keeping in view, the serious effects on the system software, auditor may scrutinize the entries on and around the various closing dates of the Bank. This verification can be conducted by going through the exceptional report or Supplementary generated by the system software. Besides this, auditor should also verify that following activities are carried out regularly and documented:

- a. Day end activities are carried out by either the Branch Manager or System Administrator and are properly documented.
- b. Supplementary are checked and special users are deleted.
- c. The following functions are completed at the day end:
 - i. Minimum balances calculated.
 - ii. Products calculated for Current Account (Debit balances)
 - iii. Mandatory reports generated. .
 - iv. Fall back procedures activated.
 - v. Day end back up taken.
 - vi. Recording of entries in back-up register.
 - vii. Recording in Log Books.
 - viii. Filing of reports.
 - ix. Shutting down of complete computer system.
- d. The data back-ups taken are in safe custody and properly documented.
- e. Server Room is properly locked and the keys are kept only with authorised person. f. The generation of following documents:
 - i. Access log
 - ii. Supplementary
 - iii. Audit Trail
 - iv. Transaction number is given for each transaction entered.
- g. After the business hours of the bank computer operators perform the following functions:
 - i. Supplementary Report is printed either by Branch Manager or System Administrators and filed.
 - ii. Cash Denomination Report is printed and filed.
 - iii. Vouchers are tallied and signed either by Branch Manager or System Administrator.

Parameter/ Master File

Parameters! Master is quantity constant but could vary for different cases. In banks, we come across various types of accounts with different guidelines to operate them. In a Parameter/ Master File, all the relevant information related to that particular account is feeded and stored. The information would related to Rate of Interest to be applied, Penal Interest to be charged, Commission Rates, Operation limits in case of loans, Nature of operation of account, single / jointly etc. This exercise is carried out at the first stage of implementation of computerisation of the Branch. Thereafter, the system software behaves according to the Parameters enforced currently are as per latest circulars. It important to check that Parameter/ Master File if accessible to the operators should only be in read-only format, else it would invite undesirable modifications, which would lead to revenue leakage and misuse of funds. Whenever any alterations are to be made in the Parameter/ Master File, printouts of the file prior to the changes and after the changes should be taken and documented in safe custody of Branch Manager. Auditor should verify the following:

- a. Authorised personnel mark all the Bank Holidays into the software in the beginning of the Financial Year.
- b. Operation limits and authorisation levels are defined clearly for the operators and supervisors.
- c. The parameters for Interest and Bank Charges are defined in accordance with the relevant rates and guidelines. The file is updated as and when changes are announced.
- d. Printouts of parameter file are taken out before and after changes are given effect and documented.
- e. The safe custody of the printouts with Branch Manager and alterations are entered into "Parameter Register".

e-Banking/Internet Banking Procedures

1. **Identify the bank's current and planned e-Banking activities and review the bank's public Internet Websites. Consider whether the bank provides the following types of services:**
 - a. Telephone banking
 - b. Retail Internet banking services
 - c. Corporate! wholesale Internet banking services
 - d. Internet services provider (ISP)
 - e. Brokerage services over the Internet
 - f. Insurance service over the Internet
 - g. Trust services over the Internet
 - h. Account aggregation
 - i. Electronic bill payment
 - j. Other activities (e.g. Web portals, financial calculators, cross-marketing arrangements and alliances, unique services, etc.)
2. Review prior audit reports related to e-Banking, including compliance, information technology, and other examination areas that may be relevant.
3. Determine if material changes have been made to e-Banking products, services, or operations since the last examination and if any significant changes are planned in the near future.

4. Determine if the bank operates the Web site(s), e-Banking system(s) or core data processing system(s) internally and whether any activities are outsourced to a vendor. Identify the location of the following operations:
 - a. Design and maintenance of the bank's public Web site or home page.
 - b. Computer/ server for the bank's public Web site.
 - c. Development and maintenance of the bank's electronic banking system(s).
 - d. Computer/ server for the bank's e-Banking system(s).
 - e. Customer service (e.g., call center) for electronic banking services.
 - f. Electronic bill payment processing or other ancillary services.
5. If the bank operates the e-Banking system or core data processing system in house, review the topology (schematic diagram) of the systems and networks, and determine whether there is a direct, on-line connection between the bank's core processing systems and the electronic banking system.
6. If the bank operates the e-Banking system or core data processing system in house, review the transaction processing flows between the e-Banking system and the bank's core processing systems and identify key control points. Determine whether information is exchanged in a real-time, batch (overnight), or hybrid processing mode. In case the bank uses the services of any professional agency for any part of the work, the auditor should apply the standards laid down in AAS 24, "Audit Considerations Relating to Entities Using Service Organisations".
7. Determine the adequacy of risk management for e-Banking activities given the level of risk to the institution, following procedures are to be valuated:
 - a. Adequacy of policies and procedures governing e-Banking activities.
 - b. Adequacy of internal controls and security for e-Banking activities.
 - c. Adequacy of audit coverage for e-Banking activities.
 - d. Adequacy of monitoring and compliance efforts.
 - e. Adequacy of vendor and outsourcing management.
 - f. Adequacy of Board and management oversight.
8. Determine the impact of any deficiencies on the financial condition of the organization.
9. Determine the extent of supervisory attention needed to ensure that any weaknesses are addressed and that associated risk is adequately managed.

Adequacy of Internal Controls:

1. Are updates and changes to the bank's public website(s) are made only by authorised staff and subject to dual verification?
2. Are website information and links to other websites regularly verified and reviewed by the bank for:
 - a. Accuracy and functionality?
 - b. Potential reputational, compliance, and legal risk?
 - c. Appropriate disclaimers?
3. Do operating policies and procedures include:
 - a. Procedures for, and controls, over opening new customer accounts submitted via electronic channels to verify potential customer identity and financial condition?

BANK BRANCH AUDIT (2007-2008)

- b. Procedures for administering access to the electronic banking system (e.g., customer passwords, PINs, account numbers)?
- c. Requirements for review of or controls over wire transfers or other large transfers initiated through the electronic banking system for potentially suspicious activity?
- d. Appropriate authorizations for electronic debits initiated against accounts at other institutions, if such transfers are allowed?
- e. Depending on the type of account, dollar limits on transactions over a given time period initiated through the electronic banking service?
- f. Reconciliation and accounting controls over transactions initiated through the electronic banking system, including electronic bill payment processing?
4. Do written information security policies and procedures address electronic banking products and services?
5. Are business recovery procedures adequate? Consider whether the procedures address:
 - a. Events that could affect the availability of the electronic banking system, such as system outages, natural disasters, or other disruptions?
 - b. Planned recovery times that are consistent with the degree of importance of the electronic banking activities to the institution?
 - c. Has management established an incident response plan to handle potential system security breaches, website disruptions, malicious tampering with the Web site, or other problem situations?
6. Has the bank or service provider implemented a firewall to protect the bank's Web site?
7. Are ongoing monitoring and maintenance arrangements for the firewall in place to ensure the firewall is properly maintained and configured?
8. If the bank uses a turnkey e-Banking software package or out sources to a service provider:
 - a. Are bank staff are familiar with key controls detailed by the vendor's security and operating manuals and training materials?
 - b. Are workstations that interface with the service provider's system for administrative procedures or transfer of files and data are kept in a secure location with appropriate password or other access control, dual verification procedures, and other controls?
9. Does the bank's administration of access to the e-Banking system by bank staff and customers include:
 - a. Procedures to ensure that only appropriate staff is authorised to access e-Banking systems and data, including access to any workstations connected to a remote system located at a service provider?
 - b. The length and composition of passwords and PINs?
 - c. Encryption of passwords and PINs in transit and storage?
 - d. The number of unsuccessful logon attempts before the password is suspended?
 - e. Procedures for resetting customer passwords and PINs?
 - f. Automatic logoff controls for user inactivity?
10. Have security vulnerability assessments and penetration tests of e-Banking systems been conducted and results reviewed by the bank?
11. Has the bank or its service provider established:
 - a. An intrusion detection system for e-Banking applications?

- b. Procedures to detect changes in e-Banking files and software?
 - c. Measures to protect the e-Banking system from computer viruses?
 - d. Procedures for ensuring on an ongoing basis that e-Banking applications, operating systems, and related security infrastructure incorporate “patches” and upgrades that are issued to address known security vulnerabilities in these systems?
12. If e-mail is used to communicate with customers, are communications encrypted or does the bank advise customers and not to send confidential information via e-mail?
13. Are adequate summary-level reports; are made available to management to allow monitoring of:
- a. Web-site usage?
 - b. Transaction volume?
 - c. System problem logs?
 - d. Exceptions?
 - e. Unreconciled transactions?
 - f. Other customer or operational issues?
14. Has management established adequate procedures- for monitoring and addressing customer problems regarding e-Banking products and services?
15. Does management accurately reports its primary public web-site address on the Report of Condition?
16. Have required Suspicious Activity Reports involving e-Banking, including any computer intrusions, been filed?
17. Is each significant vendor, service provide, consultant, or contractor relationship involved in development and maintenance of the e-Banking services covered by a written, signed contract? Depending on the nature and criticality of the services, do contracts specify:
- a. Minimum service levels and remedies or penalties for non-performance?
 - b. Liability for failed, delayed, or erroneous transactions processed by the service provider and other transactions where losses may be incurred (e.g. insufficient funds).
 - c. Contingency plans, recovery times in the event of a disruption, and responsibility for back-up of programs and data.
 - d. Data ownership, data usage, and compliance with the bank’s information security policies.
 - e. Access by the bank to the service provider’s financial information and results of audits and security reviews.
 - f. Insurance to be maintained by the service provider.
18. Has legal counsel has reviewed the contracts to ensure they are legally enforceable and that they reasonably protect the bank from risk?
19. Has the bank ensured that any service provider responsible for hosting or maintaining the bank’s web site has implemented:
- a. Controls to protect the bank’s Web site from unauthorized alteration and malicious attacks?
 - b. Procedures to notify the bank in the event of such incidents?
 - c. Regular back-up of the bank’s Web-site information?

20. Depending on the nature and criticality of the services, does the bank conduct initial and periodic due diligence reviews of service providers, including:
 - a. Reviewing the service provider's standards, policies and procedures relating to internal controls, security, and business contingency to ensure they meet the bank's minimum standards?
 - b. Monitoring performance relative to service level agreements and communicating any deficiencies to the service provider and to bank management?
 - c. Reviewing reports provided by the service provider relating to response times, availability/downtime, exception reports, and capacity reports and communicating any concerns to bank management and the vendor?
 - d. Periodically reviewing the financial condition of the service provider and determining whether back-up arrangements are warranted as a result?
 - e. Conducting on-site audits of the service provider if appropriate based on the level of risk?
 - f. Ensuring the bank staff receives adequate training and documentation from the vendor or service provider?
21. If the bank operates a turnkey e-banking software package:
 - a. Is software held under an escrow agreement?
 - b. Has the bank-established procedures to ensure that relevant program files and documentation held under the software escrow agreements are kept current and complete?
22. If a vendor maintains the bank's electronic banking system, does the bank monitor on-site or remote access of the bank's systems by the vendor, through activity logs or other measures?

Evaluation of Operation System

1. Obtain or prepare logical and physical diagrams of the operating system and attached local and wide area networks.
2. Document the operating system domain(s), identifying the Primary Domain Controller (PDC), Backup Domain Controller, and any other operating system servers or significant operating system workstations participating in the domain.
3. Using the information obtained in the prior steps, document the server and directory location of the significant application programs and data within the network; document the flow of transactions between systems and nodes in the network.
4. Using the Server Manager utility, review all trusted domains assigned to the audit domain and include these trusted domains within the audit scope.
5. Assess whether the trusted domains are under the same physical and administrative control and are logically located within the same sub-network.
6. Determine that router filtering is being used to prevent external network nodes from spoofing the IP address of a trusted domain.

User Security

Determine that the user log in identification and authentication process are properly configured and that users are assigned to operating system groups which are consistent with their job requirements for system access:

1. Obtaining the documented security policies and procedures for the operating system server environment. Use the User Manager utility to display the global log in accounts security parameters and review and assess the following settings:
 - a. Forcibly disconnect remote users (forces users to log off the system after a predetermined limit of time).
 - b. Minimum password age in days
 - c. Maximum password age in days
 - d. Minimum password length
 - e. Password uniqueness (number of past passwords disallowed for future use)
 - f. Account lockout after X number of bad log on attempts
 - g. Account lockout-reset the bad log on count after X number of minutes
 - h. Accounting lockout duration-require administrator to unlock or automatically unlock after X number of minutes.
 - i. User must log on to change password (may allow or restrict users with expired passwords from logging on and changing the password themselves or requiring an administrator to change the password for them)
2. Determine that the Administrator (super user) and Guest accounts have passwords assigned to them (by attempting to log on without providing a password). Also ascertain that the Administrator account password is well controlled and used! known by only the system administrator and one backup person.
3. Using the User Manager utility, review the following account properties settings active in each user's individual profile, which may override the global account policy:
 - a. Full name (should be used to facilitate ill management)
 - b. Description (job, department, etc.)
 - c. Change password at next log in (should be used for new users' initial log in)
 - d. User cannot change password (forces administrator to manage the password; may be used for vendor and other third-party accounts)
 - e. Password never expires (may be used to override the global restriction in the Accounts Policy)
 - f. Account disabled
 - g. Account locked out
 - h. Groups (cross-reference to group's audit procedures)
 - i. Profile (each user should have a home directory, path statement, and log in script)
 - j. Hours (log in time restrictions)
 - k. Log on to (restricts workstations from which the user may log in from)
 1. Account (specifies local or global and may specify an expiration date)
4. Using the User Manager utility, review and assess User Rights assigned to groups and individual users.
5. Use the user manager utility, review and access User Rights assigned to groups and individual users.

6. Use the User Manager utility to view and assess membership in the sensitive built-in groups: Administrators, Domain Administrators, and Account Operators. Assess the appropriateness of users assigned to these groups.
7. Using the User manager utility, document user membership in groups used to grant access to resources with audit significance (application program and data directories and files), cross-reference. to review file system security audit steps, and assess appropriateness of each user's membership in groups.

File System Security

To ensure that significant system and application program and data resources are protected from unauthorized access and modifications.

1. Review the file system directory trees to ensure that only operating system file systems are used on servers within the audit scope (since any other file system type, DOS or other, cannot be controlled by operating system security with the exception of operating system share security).
2. Using the File Manager directory tree directory tree utility, list out the Security Permissions for all system directories and significant application programs and directories; perform the following:
 - a. Determine that the owner of all operating system directories is the Administrator account
 - b. Determine that application program and data directories are owned by a restricted application owner account of the operating system Administrator account
 - c. Review and assess permissions assigned to groups and individual accounts, noting that Full Control (all permissions) and Change (Read, Write, Execute, and Delete) permissions are restricted to authorized users (cross-reference groups to earlier step, identifying users with the groups they belong to)
 - d. Determine that Change permissions and Take Ownership permissions are restricted to Administrative accounts and groups
 - e. Using the File Manager directory, identify all shared directories (directories made available to users the network). Review and assess Share permissions assigned to these directories on a group or user basis.

Operating System Audit and Logging

To determine whether adequate detective controls have been configured and that the information generated by these controls is being reviewed and followed upon:

1. Using the User Manager utility, review the Audit Policy options in effect for the domain (and server, if applicable). Normally, all failure conditions should be audited.
2. Using the Event Viewer utility, review the audit log for suspicious events and follow up on these events with the security administrator.

Operating System Services

To ensure that only necessary, secure services are active in the operating system environment:

1. From the control panel, click on the services option and review all active or dormant services. Identify the purpose and necessity of each. Unnecessary services should be disabled.
2. Ensure that each service, logs on as on account other than the system account unless the service requires the system account. Audit the permissions granted to each service account.

3. Determine that each service account has the advanced user right, called logon as a service.

Operating System Networking

To determine that the network and network services are protected against unauthorized access and use:

1. Identify all necessary netbios services offered on each server. Access the propriety of each and if it is running as a non-privileged service account, unless the service requires the system account.
2. Review router configurations for routers that connect the operating system network to external networks. Ensure that the TCPIUDP ports 137, 138 and 139 are blocked or altered to restrict Netbios traffic coming into and going out of the network.
3. Identify all active, native, and third party TCP/IP network services active on the operating system server. Audit the security of each service.

The Operating System Registry

To review the security over system and program control parameters in the operating system registry:

1. Review the operating system directory and file permissions over system and program control parameters in the operating system registry.
2. View the registry permission for the major system and program keys and sub keys to ensure the following:
 - a. The administrators' local group owns each key
 - b. The owner group and system global group have full access permissions.
 - c. The global group called everyone has restricted special access permissions.

Automatic Teller Machines

More than two decades have elapsed since the introduction of ATMs by Banks in India. Initially, these were installed by larger co-operative Banks and the new private sector Banks. Today, ATM service is offered by even small co-operative Banks making such a service sinqua. non of Banking in India. Seemingly technical in nature, it houses one of the primary asset of the Bank - cash which has to be recognized by the auditor in his scope of work. While verification of cash in the ATM is one aspect, the operational efficacy should be responsive to the policy of the Bank and the standard operating procedures including the directives of the Reserve Bank of India.

Few ATM frauds are reported till date but this has no implication on their occurrence. Banking business deals with money and ATM is one part of its service. The auditor needs to view this service with the same critical eye as any manual cash management. Following aspects of internal control in relation to ATMs may be ascertained and evaluated by the auditor:

Pre-installation Stage

1. Board's sanction of ATM installation service.
2. ATM installation complies with the strategic Information Technology plan of the Bank.
3. Purchase of ATMs need to be driven through the same formality of a purchase of asset of the Bank like flotation of tenders, etc.

4. Location of the ATMs both branch attached as well as independent locations should be finalized to achieve the aim of Bank's investment in this service.
5. All requisite permissions and licenses should be obtained by the Bank including communication to the Reserve Bank of India.
6. Environmental preparations should be made considering legal, security and operational issues. Environmental policy should be also set in writing to permit standard environment with sufficient provision to permit customization necessitated by location peculiarities.
7. The estate department of the Bank or an independent architect should certify to the Estate department about the quality and appropriateness of translation of set policy at each of the ATM location.
8. Cash replenishment policy needs to be finalized before operating any the ATMs. This can be a set policy or a contingent policy determined by the number of ATMs units set up by the Bank. Cash replenishment can either managed by the Bank itself or it can be outsourced. With the Bank itself it can either be done by a Central or Regional office or a nodal equivalent branch in which case, the ATM cash balance is reflected in the books of this Branch. The various alternatives should be evaluated and selected.
9. If the cash management of ATMs is to be outsourced, similar procedure should be adopted by invitation of either open tenders or inviting tenders.
10. Insurance of cash in ATMs should be negotiated with insurance companies and if the number of ATMs is numerous, select insurance companies may be invited to bid.
11. Application software should be able to communicate with the ATM software and this delicate requirement should be specifically mentioned in the agreement with the ATM vendor and application vendor since their co-operation is essential at this stage.
12. ATM software, its operation and reflection in the main application should be software tested either internally or through a professional firm before operations commence.
13. Cash replenishment policy should be set ensuring the maximum limit set per ATM is not exceeded.

Operational stage

1. Is the security manual in place describing the security measures to ensure at the time of replenishing cash in the ATMs?
2. Are all the staff involved in cash transfers screened thoroughly and their photos and prints taken? In case of a contract, does the service vendor follow similar formalities? This should be periodically checked by the Bank and this point needs to be have been specifically made in the agreement with him.
3. Is the process of allocation of ATM cards secure?
 - a. Are the Personal Identification numbers (PIN) generated randomly?
 - b. Are the PIN cards printed in a manner that no staff is able to read them without tearing open the seal?
 - c. Are the cards and PIN numbers sent separately? Popular delivery mode is delivery of card only through a courier agency. The PIN number is physically delivered through the branch. In case the PIN number is also to be delivered, it should be given on a later date and that too through another courier agency.

- d. Courier agency should be under separate contract to fulfill the extra formality of identification confirmation of the person accepting the card with the strict instruction to hand over the card only to the person to whom the card is allotted.
 - e. Bin filling exercise should be done in the presence of at least two persons who should not only supervise each other to ensure correct denominations are inserted in the correct bins.
 - f. User report if available on the 'special service ATM card' should be obtained and filed for future reference. This should ideally record the time and date of opening the ATM machine presumably to replenish it. Along with this, the cash balance after replenishment should also be printed.
 - g. Cash shortages should be thoroughly investigated with full reference to the server report compared with the ATM's log available on site of ATM.
 - h. All cards should be changed after a period say 2 years to allot cards to only regular users thus diminishing risk of the cards of non users.
- 4. Whether surprise checks are carried out by the vendor or the Bank's departmental officer to ensure the amount and time of currency replenished as reflected in the register is accurately recorded?
 - 5. Whether schedules of currency replenishment are not static and are changed on each occasion randomly to ensure that there is no definitive pattern?
 - 6. Whether ATMs providing additional service like refilling phone cards or e-transfers etc. are system audited periodically?
 - 7. Whether the bank has a system to thoroughly report and investigate complaints regarding non-performance of services?
 - 8. Whether Cash in ATM and Cash in transit insurance is kept alive at all times?