Bank Branch Audit in Computerised Environment

The computerised environment provides advantages over manual system in terms of arithmetic accuracy and uniform processing of transactions. But at the same time it poses certain challenges before the auditor in terms of audit risk due to peculiar nature and characteristics of Computerised Information System (CIS) environment, where potential for fraud is much more and can be more easily hidden in the digital data. The overall objective and scope of an audit does not change in a CIS environment, nevertheless, the use of a computer changes the processing, storage, retrieval and communication of financial information and may affect the accounting and internal control systems employed by the bank. The approach and methodology to be adopted for bank audit in computerised environment is bound to be different and has to be correctly understood by the auditors. The auditor should obtain an understanding of the CIS environment and assess the inherent and control risk accordingly.

There has been a phenomenal growth in the number of banks who have computerised most of the businesses of their branches. New entrants in the banking business have augmented the competition. The customer is now well aware of the choices and products available to them. All this has necessitated access to information and state of the art technologies to serve the customer efficiently and effectively. In this ever-changing banking environment, members who are involved in auditing of banks require to equip themselves with the IT knowledge to meet new challenges and adopt a different approach and methodology for bank audit under computerised environment. Auditors need to test the accuracy of output by some test cases, and once it is established, their focus should be shifted to the areas, which have become vulnerable because of the computerised environment. If computerised report of NPA is found correct, the auditors need to concentrate on the methods of implementation and generation of the report and the logic computer uses. In one bank it was found that the software was giving an option to treat an NPA asset as a Standard Asset, and treated it as a normal advance. There is an inherent risk coming along with technology. Therefore, first of all, we need to concentrate on the potential Risk Areas in the computerised environment.

– CA. Ashwin Nagar

(The author is a member of the Institute. He can be reached at ashwin.nagar@capgemini.com)

Potential Risk Areas in Computerised Environment

Following are the Potential Risk Areas in computerised environment:

- The people may use general instructions to gain access to programme for unauthorised purpose.
- The computer utility available in the system may be used without authority to modify, destroy, copy or use data stored in computer.
- There is ample scope for changing the data before inputting/generating input.
- The software or the computer programmes, which are non-standardised, many times give way to unauthorised access into the system.
- In the systems with weak control, it is easy to insert virus into the computer system by use of computer floppy or other means to access to system.
- When terminal is kept open and user leaves the terminal without logging out, unauthorised access by immediately following the person who has accessed to

the computer system, is a big area of fraud.

Massive computerisation is taking place in all the banks. The approach and methodology to be followed in audit of any computerised branch needs to be understood correctly in the light of the fast-paced technological changes taking place. Information Technology makes it imperative that internal controls and systems get integrated in IT and are not apparent as a manual system.

The computerised branches may be divided into two categories. In the first category come the branches where partial computerisation has taken place. These branches are called ALPMs or PCs or PBA. In some branches of the banks, only a single PC is used for the processing of various important functions such as interest and product calculations. In partial computerisation, certain accounts may be maintained on computers while others are maintained manually.

The second category of computerised branches includes those branches that are fully computerised. These are called TBA (Total Branch Automation) branches. These branches work under LAN (Local Area Network) environment connected with a server in the branch.

The totally computerised branch may further be classified into two types:

Stand alone Computerised Branch: These bank branches are not connected online with other banks or the head office. The transactions take place in the server at the branch level and at the end of the day it is consolidated and sent to Regional/Head office for further consolidation.

Total Computerisation with Central Database: These bank branches are connected online with other branches or the central database. In the Core Banking Solutions (CBS), banks maintain a central database and all transactions that take place in various branches are updated in the central server online. People also can transact business from any of the branches of the bank.

AAS 29

After the AAS 29 on Auditing in a Computerised Information Systems (CIS) environment became operative for all audits related to accounting periods beginning on or after 1st April 2003, the responsibility of the bank branch auditor has increased manifold. As per AAS 29, the overall objective and scope of an audit does not change in a CIS environment, however, the use of a computer changes the processing, storage, retrieval and communication of financial information and may affect the accounting and internal control systems employed by the entity. Therefore, an auditor needs to check the various controls implemented throughout the system and their existence. A CIS Environment may affect:

- The procedures followed by the auditor in obtaining a sufficient understanding of the accounting and internal control systems.
- The auditor's evaluation of inherent risk and control risk through which the auditor assesses the audit risk.
- The auditor's design and performance of tests of control and substantive procedures appropriate to meet audit objective.

Auditors need to be satisfied about existence of adequate security control in the Computer System as also about implementation of these controls by the bank.

Controls in Information System Environment

All the transactions put through need to be continuously monitored for their integrity and compliance with control requirements. Two key controls in any IT environment are:

1. **Application Controls:** These are the controls that exist within the application software, which puts through the transactions at the branch level. For example, permitting of overdrawing in any account, which should be permitted only by the authorised person and none else.

2. **Information System Controls:** These are the controls in developing IT packages, ensuring system security and monitoring IT processes. In the system security, effective controls should be exercised in physical access as well as in access to control software. Password controls and access levels have to be clearly defined and well documented.

Like internal audit in a bank supports and helps in statutory audit, Systems audit is a prerequisite for financial audit in banks. ATMs, Internet and mobile banking are some of the areas where security is a serious concern. If the bank has undergone the IS audit, it is important for the auditor to go through the report of IS audit and ensure that the security issues raised in the audit report have been addressed and resolved.

Important Security Control Aspects

These are certain key security control aspects that a branch auditor needs to address when undertaking audit of a computerised branch:

Evaluate Reliability of Accounting and Internal Control Systems

- Ensure that authorised, correct and complete data is made available for processing.
- Ensure that system provides for timely detection and correction of errors.
- Ensure in case of interruption due to power, mechanical or processing failures, the system restarts without distorting the completion of the entries and records.
- Ensure the accuracy and completeness of the entries and records.
- Ensure system provide adequate data security against fire and other calamities, wrong processing, frauds etc.
- Ensure that the system prevents unauthorised amendments to the programmes.
- Ensure that the branch provides for safe custody of source code of application software and data files.

Security and Control Issues Relating to Parameters

- Verify whether "User levels" assigned to the staff-working match with the responsibilities, as per manual. It is very important for the auditor to ensure that access and authorisation rights given to various employees are proper because unauthorised access rights given to any employee can jeopardise the whole security and control system. Verify that branch parameters are properly set.
- Verify that changes made in the Parameters or user levels are authenticated.
- Verify that charges calculated manually for accounts when function is not regulated through parameters are properly accounted for and authorised.
- Verify that all modules in the software are implemented.

Security and Control Issues Relating to Operations

- The maker can't be the checker of the transaction. Verify that transactions are not created and authorised by the same persons.
- Verify that Beginning of the Day and End of the Day register is properly maintained and Time is properly entered and time and date are normal and during office hours only.
- Exception reports are the major audit tool. Anything that is not allowed in the normal course of business is reflected in the exceptional reports. Verify that exceptional transactions report where details of dishonoured cheques, large withdrawals, overdrawn accounts etc. are recorded are being authorised and verified on a daily basis by the branch officials. The Exception Report generally contains the following details, though it varies from software to software:

- Debit /Credit balance change
- Maturity record deleted
- Inactive accounts reactivated
- Excess allowed over limit
- Debits to Income head accounts
- Overdue bills and bills returned
- Withdrawal against clearings
- Deposits accounts debit balance
- Temporary O/D beyond sanction limit
- Standing instruction failed in day

- Verify that inoperative or dormant accounts are operated only after authorisation by supervisor.
- Verify that balances are downloaded on PC daily from the server.
- Verify that the Account Master and balance cannot be modified/amended/altered except by the authorised personnel. If any other person can do it then it means a serious security threat exists.
- Verify that branch has posted a System Administrator and there is system of changing the system administrator at periodic intervals.
- Check that the record of errors arising during daily operations are reported and properly dealt with. It is important to verify how these errors are rectified.
- Verify that interest indicators are correctly given for all types of account. Ensure that interest rate applied is as per the sanction order.
- It is also very important for the auditor to test check interest by manual checking in case of a large account and compare it with computer generated amount. Sometimes it happens that the programme for all types of accounts does not give correct interest logic and there may also be inaccuracy in interest calculation due to faulty programming. There is no need of checking all the accounts. It is enough if at least one account of all the account types is checked for accuracy of interest application.
- Verify that all standing instructions/ stop payment instructions are properly updated in the system.
- Verify that lien is marked in the system against fixed deposits pledged for taking loans, so that no payment could be made against them without cancellation of lien.
- Verify that all accounts (Opening & Closing) are duly authorised.
- Verify that all creation and cancellation of lien in the computer are properly authorised.
- Verify that all the GL accounts codes authorised by HO are in existence in the system.
- Verify that balance in GL tallies with the balance in Subsidiary book. Computerised environment doesn't necessarily means that these are automatically tallied.
- Verify that periodical updating of drawing power is done in the computer. If it is not updated in the computer regularly, the actual drawing power and the drawing power entered in the computer may vary and the system may allow unauthorised overdrawing.
- Verify that charges like folio charges; minimum balance breach charges etc are collected/charged in the account by the system for all eligible accounts.

There is no need of checking all the accounts. It is enough if at least one account of all the account types is checked for accuracy of interest application.

Security Issues Relating to User IDs and Passwords

- Verify that passwords are changed at regular intervals and the staff of branch does not know Manager's password because whole of the computerised system works on the authorisations and passwords only.
- Verify that important passwords like DBA, branch managers are kept in sealed cover with branch manager, so that in case of emergency and the absence of any of them the passwords could be used to run the system properly.
- Verify that passwords of staff on long leave are deactivated, so that nobody else could make the unauthorised use.

The backup media should be duly labelled and indexed properly and should be maintained under joint custody. Ideally, daily backup should be taken in 6 sets, one for each weekday and 12 sets of month end.

- Verify that no two or more same user id's exist in the same branch.
- Verify that dummy accounts created using master creation should not exist in the Branch.
- Verify, whether staff that are transferred/ retired still have user id in the system?

Security and Control Issues Relating to Backups

- Verify that the branch takes daily and monthly backups. The backup media should be duly labelled and indexed properly and should be maintained under joint custody. Ideally, daily backup should be taken in 6 sets, one for each weekday and 12 sets of month end.
- Verify that one time backup of programme is taken and preserved. The backup should be updated for every change in the programme.
- Verify that backup register is maintained and updated.
- Verify that backup is tested for readability on a regular basis. Record of verification and testing should be properly maintained. It is desired that backup is restored in some other system for checking data readability.
- Verify that procedure to take Interim Backups is followed by the branch.
- Verify that the backup media is stored in fireproof cabinet secured with lock and key.
- Verify that offsite backups are preserved for the emergency.
- Verify that yearly data is downloaded in optical disk drive/CDROM.
- It is important to see that old records are preserved on floppy, or CDROM/ Hardcopies.
- Where an extra server is installed for copying the data, auditors should verify that disk mirroring is taking place properly.

Security and Control Issues Relating to Reports/Registers

- Verify that user id register, password register, floppy register, and Checksum register are maintained and updated.
- Verify that the reports generated by the system are checked and signed by the officer.
- Verify that asset register containing details of all the computers and peripherals are maintained at the branch.
- Verify that manuals, CPPD guidelines are readily available at the branch.

Insurance

- Verify that Insurance policy of computers is on record.
- Verify that Annual Maintenance Contract of UPS/Computers are renewed on due date.

Vendors

- Verify that user ids created by the Vendor doesn't exist in the system.
- Verify that list of standard directories/files is available at the branch.
- Verify that vendor's contact numbers are easily available with the branch.
- Verify that software vendors are allowed to port new versions with approval of ITD/ nodal offices only.

General

- Verify that the antivirus software of latest version is installed in servers/PCs of branches to prevent data corruption, and is being regularly updated for new virus definitions.
- Verify that access to the computer room is restricted to authorised persons only.
- Verify that the users log out every time they leave the terminal. It has been observed that the bank staff leave terminal without logging out and the terminal is exposed to serious security threats.
- Verify that unauthorised software/games doesn't exist in the system, these could be source of virus and data corruption.

Advantages

The computerised environment provides advantages over manual system in terms of arithmetic accuracy and uniform processing of transactions. That reduces the audit risk as there is no need to maintain and verify balancing ledgers and no need to verify postings if there is a fool proof computer system. Further, the system calculates interest automatically and chances of error are limited. The clerical errors ordinarily associated with manual processing are virtually eliminated. Many of the functions earlier carried out under manual system get automated and get eliminated under computer system. Many of the operations get redundant due to computerisation.

Challenges

The use of technology in banks also poses certain challenges before the auditor. A single person now performs many control procedures that were performed by different persons in manual system. Thus, it compromises some times, the basic principle of segregation of duties and allows performance of incompatible functions.

The clerical errors ordinarily associated with manual processing are virtually eliminated. Many of the functions earlier carried out under manual system get automated and get eliminated under computer system.

The lack of transaction trail and audit evidence is the biggest challenge for auditors. The electronic evidences are very fragile. In so many cases, where a complex application system performs a large number of automated operations and transactions, to find a complete transaction trail is very difficult. Proper documentation is also a challenge, which auditors need to cope up with in the computerised environment. Some of the audit evidence may be in the electronic form, some of them are not capable of being retrieved again as they are generated once only. As required by the AAS 29, "The auditor should satisfy himself that such evidence is adequately and safely stored and is retrievable in its entirety as and when required." ❐