AUDITING IN COMPUTERISED ENVIRONMENT

—Nitant. P. Trilokekar

Technology and its progress has often been linked to progress of civilization. From the time man learnt to control fire to the iron and Bronze Age, we have noted that the control over inventions like guns and cannons have given certain civilisations the upper hand over the ones they conquered. It is not necessary for the inventions and progress to be restricted to the field of military or defence. Progress in Banking is an equal parameter of the cultural development of a civilisation and like any other field, this sector is not spared from the technical revolution which has taken over other sectors. This article delves into the necessity of value added APPROACH to the traditional audit and not solely dependent on the system auditors. These approaches are general and can be applied to any environment whether LAN Branch or a core banking situation. By the time the reader goes through this article, even the unexposed and uninitiated auditor will be urged to recognise the need of the day and voluntarily embrace change in the angle of audit while keeping the audit objectives sacrosanct.

Progress in Banking is an equal parameter of the cultural development of a civilisation and like any other field, this sector too has not been spared by the technical revolution. While telex machine heralded faster fund transfer for decades beginning from the second half of the sixties, later inventions put a turbo charge in the speed of such transfers. While local clearing lagged behind, we have seen the introduction of Real Time Gross Settlement (RTGS) system by the RBI. One hopes the extension of the concern for a speedier settlement of all fund transfers. To the business, this spells an automatic potential for increase in turnover.

Audit approach change

By now it has dawned on all auditors that we cannot afford to ignore the computers and they form the integral part of the organization we are auditing. These systems affect the working of the organization to such a level that in extreme cases, an unsuitable solution can even kill the company and the auditor better forecast this. The question then comes to mind is that should the 'new generation' computer savvy generation auditors tackle it while the rest go to the hills and retire? There are various audits related to computers and if only these are employed, you will agree that the statutory or internal audit purpose is not fully covered and this therefore is not a solution. Admittedly, though these audits go a long way to make the system a success, the scope of internal and statutory audit is not covered here. Perhaps only the format validity in legal terms of the reports is covered under software audit but it stops there and the accuracy of Balance sheet is not the main purpose of that

The author is a member of the Institute. He can be reached at nitanttrilokekar@yahoo.com

audit. The question then still remains, how should the auditor deal with the matter? In simplified terms, in case the organisation is large and has live operations (all aspects are entered through the computer directly) then the auditor will be right in recommending the various system related audits to support himself.

Is the burden shifted to the system auditor?

There is unlikely any professional who will take this stand of shifting the burden to the other auditor. There are a few checks you can do without undergoing intensive training and examination! Please note that the computer system environment referred to here is a minimum of LAN (Local Area Network) or even a Core system where the data hub is at a Central Location and the branches/offices are connected to this data hub despite being many cities away. Apart from the large corporations and multinationals, many Banks, even large co-operative Banks have taken this option. Even the branch auditor, thus, has to take certain precautions to ensure he gives justice to his work.

Approaches

While the basic approach to any computerised environment should remain the same, the reality of different setups demands a light adjustment to either the depth or the scope of coverage. A LAN Banking solution being the simplest setup and core banking linked by VSAT being the other end of complexity may not radically change the auditor's approach- only slightly.

These approaches are the minimum essential and one hopes you are spurred to expand on this to make it an all comprehensive!

1.	**PHYSICAL ACCESS CONTROL**	In case the site is a LAN, the Server should be secure since the software and data is located in this device. Access to the Server room should be restricted and only senior management should permit 'outsiders' like software and hardware vendors to enter the server room. Many of the frauds that have already occurred in India would have been prevented only if this access was closely monitored.
2.	**ENVIRONMENTAL SECURITY**	Apart from protecting the server from bad intentioned persons, we have to ensure it is protected from accidents of fire and water by installation of smoke alarms in the server room and extinguishers outside the server room. In case of core banking, the devices used for communication should be accorded the status of protection of the server.
3.	**SAFEGUARDING OF ASSETS - UPS**	Computers require electrical power for working and when the environment is live, work comes to a standstill unless power is provided though a UPS (Uninterrupted Power Supply) This has battery bank and is activated immediately when the power fails providing a continuous power without any interruption. These machines heat when generating power and if proper ventilation is not provided, these UPS will provide service for shorter durations not only compromising the work but also wasting the investment of the company. Simple rules of maintenance should also be followed and monitored.
4.	**OPERATING SYSTEM CONTROLS**	While all pay attention to the application software access, many forget to police the access to the operating system. File copy, deletion even data manipulation (especially under database environments) etc. are some potential disasters that are possible unless controlled. You will have to ensure that the company holds the original license for using the operating system software. Ensure whether the original Operating System Media supplied by the vendor is available in the Company. This is necessary to ensure reloading in case of accidental corruption. Only if the company has the system can it be loaded without waiting for the vendor's representative.
5.	**APPLICATION SYSTEM CONTROL**	The application developed for the company should be encoded and not left in a manner that can be re-programmed by the user. This will enable any person knowing a bit of programming of that language to design trapdoors for fraud and these are later very difficult to identify. Over here, 'Prevention is easier than the cure'.
6.	**PASSWORD AND ACCESS CONTROL**	Password control is the 'logical' access to the computer. The system should have passwords and these should be demanded by the system to changed frequently ensuring that the last password is not accepted. (not accepting last 12 is the least) Along with this, the 'internal control' should be ensured by the system ensuring that the person creating the voucher should not be permitted to authorize the voucher and without authorization, no voucher (other than system generated vouchers) should be accepted by the system. The corollary of this requirement is to ensure (check) that each user has only one identity in the system otherwise one person will take the identity of the clerk and with a change in short name take another identity of an officer thus effectively compromising the system.

7.	**MASTER FILE AND PARAME-TER FILES**	There might be various nomenclature as per the application package terms but there are basically 3 main types of data files: 1. Transaction file, which contains the transaction of the company. 2. Master file, which contains the needed information of items needed at the transaction time thus, Sundry Creditor details are in the master file. 3. Parameter Files contains 'control' elements to avoid high frequency of changes. Thus the TDS rate and Service Tax rate which is known to change frequently will be in a set of files known as 'Parameter files' The senior management should check all the Master Files and Parameter files before the amended file is activated. The auditor can check it later. One important feature needed for the auditor is the history of the amendments in the parameter file to check transactions of the full period under audit. While the software of the 80's did not have this provision, many of the software developed or amended in the late 90's have these features to ensure we can work back the changes to ensure they were changed correctly on the correct day. *Master file and parameter files should be checked under any audit, as these are sensitive areas for fraud and leakages.*

To print or not to print

Many of the clients who have just heard of the Information Technology Act, 2000 will often confront the auditor and declare that it is not necessary to print any book as the law recognizes the electronic record. The law does recognize the electronic record but there are numerous riders important one of which is that **'the record should be secure in a manner that the record cannot be changed later**.' Very few of the locations survive the test of non-manipulation at a later date. Perhaps only the Indian Banking industry has such robust software not permitting backdated changes (careful! Some Banking software have features to change back date) But furthermore, is the digital signature applied (or any other legally recognized 'secure' measure)? Only then can you decide to agree not to get the books printed and do the audit 'online'.

Checklist for Audit of Computerised Operations

The following are the few minimum extra steps I would recommend in the computerised environment.

Environmental

No.	Check for	Discussion on checkpoint
1.	Securing computers	The computers need to be housed in separate cabins or kept at the counter with facility of locking.
2.	Maintenance register	The branch, if any, should keep record of maintenance. This maintenance includes regular cleaning as well as preventive maintenance by qualified engineers on contract. This records time, date & identity of persons touching the computer other than regular operators. Main purpose of such a register is to ensure the Bank is maintaining the machines to protect the data. Please ensure the Branch maintains this record and not just the engineers who have the maintenance contract. (this is often the reply given to auditors)
3.	Accounting consumables	Proper accounting of consumables is done and records should be maintained account wise. Floppies, cartridge tapes contain confidential data. A missing one may indicate pilferage of not only the item but of information exposing the Bank to a legal liability. A separate register needs to be shown to you recording all purchases and location / custody of used items & details of destroyed if any. This register is to be maintained on lines similar to that of sensitive stationery of the Bank.
4.	Inspection of consumables	There should be record of periodic inspection of consumables. Just like the sensitive stationery, which is inspected frequently, either by branch staff or by another branch staff, this should also be covered in such inspections.

5.	Securing the computers	The machines should be locked at the end of the day. Ensure that either the furniture, which is adjusted for locking, is locked or that the hardware lock of the computer is used. This is a simple point often ignored. Unlocked computer means any one can start it and the only hurdle after that is the password. Poor password maintenance further compounds risk of unlocked computers.
6.	Securing during operations	During computer operations especially during service hours, it is not uncommon for the operator to leave his/her seat. The operator and thus you as an auditor should ensure that the operator either exits form the system or leaves it at a point where it cannot proceed without a password.

Master files vs. Parameter files

In the corporate world, there is very little use of a parameter file. In the Bank however, it is important and we need to know the difference before we discuss either.

A parameter file contains control fields that affect ALL accounts of a particular category. For example, a savings parameter file affects all savings accounts and the fields here will be rate of interest, minimum balance, minimum balance charges etc.

No.	Check for	Discussion on checkpoint
1.	Parameter file print	Since the parameter files are affected only when there are changes, a print should be taken by the branch when change is done because most softwares do not give details of changes. Only changes in Master records are picked up in the audit trail. In absence of such a print approved by branch manager and department officer, you have the only alternative to sample study a few accounts to verify whether changes are done from the required days. The later application software have responded to this demand and leave a trail to the earlier records and thus the changes.
2.	Parameter file access	This is normally only under an officer's password. Test check if the operator can access it. If so, it warrants a serious objection.
3.	Master file print	Entire master file prints should be done every quarter. Doing it just before the application of interest aids the branch officer to ensure correct rates are applied. These should be made available to you with the attestation of the officer signifying his check. However, in the scenario of monthly interest on advances, the printing of master at monthly intervals seems too demanding. In such a case, one can concentrate on new masters and those masters, which have been amended. (these can be tracked from the audit trail)
4.	Account opening and closing	Relevant master file details must be printed at time of opening new accounts and filed with application. This permits us to verify whether the same instructions are entered as specified by the account holder. Status at time of closure of account should also be printed as audit trail just specified closure without a full master dump. In almost all Banks, master dump at time of closure is not taken.
5.	Account modification	At the outset please verify if the audit trail meets with your expectation. Audit trail should cover any modifications in master file. Addition of name and such events require changes in master file. Audit trail should cover such events and should be approved by the departmental officer. This report (audit trail) should be filed separately and not in the voucher bundle. This report should be available for all working days of the Bank.
6.	Computer change register	Account modification and Drawing power changes are instructed by means of 'computer change register'. Instructions are written and operator signs with date of execution of such a change. Verify maintenance of this register.

Password

Password is a key to something more valuable than cash - data

No.	Check for	Discussion on checkpoint
1.	Password allotment register	When a password is allotted, entry is made in this register. This is similar to the key register where entries are made at time of giving keys. Check here whether the password level is also specified. Authority to give password is to the branch manager and those who hold supervisor password.

2.	Password Change register	Where software does not control change in password (where not only warnings are given but user is disabled unless the password is changed after specified date) a register has to be shown to you with dates of change of password. In absence of this register, you do not have evidence that the passwords are changed frequently.
3.	Two to three supervisors only	Supervisor password level permits the holder of this password unlimited access. Ensure there are a minimum of two and a maximum of three such holders. Check the systems and procedure manual of the Bank in case they specify a different figure.

Cheque related transactions

No.	Check for	Discussion on checkpoint
1.	Audit trail listing cheques out of range	Check if chequebooks issued are updated to the customer's master on the same and a record of the same is maintained.
2.	Audit trail for date	Ensure that stop payment instructions are updated immediately on receipt of the instruction. Audit trail will give date of entry of such a stop payment. Verify with date of receipt written on the letter of the account holder. It should be the same day.
3.	Minimum balance charges	Accounts having chequebook facility (savings/current) require having a specified minimum balance. Ensure minimum balance charges are levied in case the balance falls below the minimum level. In good systems, this information is asked in the 'parameter' file and thus the charges are correctly levied either every month or every quarter.

Clearance module checklist

No.	Check for	Discussion on checkpoint
1.	Audit trail comparison	Audit trail for clearing transactions are available and these should tally with the clearing registers.
2.	Returned inward/ outward register comparison	Audit trails should be available for cheques returned in clearing and also for charges that are debited on account of such returned instruments.
3.	Missing days of clearance execution	Verify whether the clearing modules are executed daily. If not executed daily then the reason thereof (software/hardware problems etc.)

Transaction checklist

No.	Check for	Discussion on checkpoint
1.	Check each voucher to bear a transaction number	Every transaction posted in the system should be duly numbered and initialed by the operators. The audit trail available should be checked and they also reflect the operator's identity. The initials on the voucher and identity on the audit trail should match ensuring that the operators use only their password.
2.	Ensure exception list is printed and complete	Exceptional transaction lists in case of overdraft, cheques series mismatch, unauthorised operations such as joint operation, account operated by a single person etc. should be available and are checked and preserved. The passing authority's identity is also reflected in the trails.
3.	Errors are corrected	Check where there are posting errors, corrections to be made as per the transaction entry audit trail, these have been carried out the same day and further audit trail is produced.
4.	Examine trend	Make a scrutiny of exceptional transactions show that the same type of unauthorised transactions do not occur.

5.	Dormant a/c check	Ensure transactions in dormant accounts if any have been authorised by proper authority and audit trails for the same are verified. Dormant accounts are those where the account holder has not transacted for over 3 years. Many banks have a further filter under the status of 'inoperative' accounts where the depositor has not done any transaction for a year. Under the manual system, the inoperative as well as the dormant accounts were put in a separate ledger for the sole purpose of a stricter supervisory control as such accounts are more prone to fraud. The checking officer normally becomes the branch head in such cases. Since the computer does not have a physically distinct ledger, the logical triggers should be available to ensure that any transaction is passed only by the branch manager or the designate manager as per the manual of instructions of the bank.

Transaction checklist

No.	Check for	Discussion on checkpoint
1.	Trails must be available for each day	Audit trails as permitted by the system should be printed and preserved. They should be filed separately and old copies should be bound. In case of advanced systems where the system maintains a log, a variation can be done by annually (minimum) preserving a soft copy on a permanent external media like a C.D. This is to ensure that in case of any corruption, some external media is available for the audit trail.
2.	Response to audit trails	The concerned officers should initial audit trails. Absence of signature/initials will imply Report not read by the officers and should be viewed seriously. We have noted many valuable reports generated from the system but no action taken because the reports are not read as they may be generated by the designate system administrator who may not have sufficient experience or seniority to comprehend the results listed in the report to bring to attention of his seniors.

Balancing/jotting checklist

No.	Check for	Discussion on checkpoint
1.	Compare jotting printout with General ledger	While some of you may not believe this, there are some systems where the jotting did not balance with the General Ledger. In such cases, this classifies as a serious irregularity of 'books not in agreement with the final accounts.' Balances should tally with the general ledger. The department officers should check this by application of their signature in the balance book. For ALPM operations too this will apply but in some Banks, this signature is taken on the Cash Book in the form of a certificate. This should be taken at monthly frequency at least.
2.	Officer's checking	Balance printouts should be checked and initialed by the concerned officers.

Backup checklist

No.	Check for	Discussion on checkpoint
1.	Verify daily back-up	Back up of data should be taken on daily basis. Check the labels of the floppies (if floppies are used for back up) and normally you will see the popular frequency of 'day of the week' labels i.e. Monday, Tuesday etc.
2.	Monthly back-up importance	There is normally the other frequency of other back up to be taken on weekly or monthly basis. See if this is done.
3.	Reporting of restoration	Restoration of data if done, you should verify the reasons thereof and check out the frequency as this act may be taken to hide corrections of fraudulent entries without leaving a trail.
4.	Off site copy	Month end copies are usually in duplicate and stored at the other premises. These are usually
	or Fire copy storage	termed as 'Fire copies' where at least the precious month's position is available in case the entire records are destroyed by either fire or any such disaster. The importance of this is seen only in case of an eventuality[1]. Often the comments of the auditor are the only source for correction.

Conclusion

While the environment has turned from manual to computerised, the audit techniques for the traditional auditor need slight fine-tuning to exploit the technical advantage. After all, if the computer can calculate interest correctly in a sample of 50 accounts, it can do it accurately for 5 crore accounts. As auditors we can place reliance on this and thus adjust our coverage and direction accordingly. System auditors do provide a much-needed support to the traditional accountants and one hopes that all major systems should be audited at regular intervals to ensure minimum distraction to the traditional auditor. ■

2 Of all the offices destroyed in the World centre bombing at New York in the beginning of the '90's, only one third of the offices reported having fire copies and could carry on business the next day while the rest faced the painful & virtually an impossible task.