Audit of Banks Operating in a Computerised Information Systems Environment

Today, operations of banks are extensively computerised. More and more banks are shifting its operations to core/centralised banking solutions (CBS). The core banking solution invariably has a layer of Internet based software, facilitating net banking by the customers of the bank. The host systems of the bank may also be interfaced with ATMs and other point of sale machines. It is quite likely that in addition to the core banking solution, bank might use specialised software to take care of specific operations like trade finance (in case core banking solution does not adequately meet the operations of any particular area). Banks may also have specialised software catering to its integrated rupee and forex treasury, inter branch reconciliation etc.

Understanding of the CIS Environment

Before the auditors commences the audit, it is imperative that he has a thorough understanding of the CIS environment prevalent, each application software used at all points of time during the year as well as interfaces established between several sub systems of the bank. Without a proper understanding of the functioning of each item of software, the auditor would not be in a position to gear up for an effective audit of banks operating in a computerised environment. Accordingly, the auditor needs to carry out the following tasks: -

- Shyam Ramadhyani

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

Auditing and Assurance Standard (AAS) – 29 establishes standards on procedures to be followed by an auditor when an audit is conducted in a computerised information system (CIS) environment. The overall objective and scope of statutory audit does not change in a CIS environment. However, the use of computers changes the processing, storage, retrieval and communication of financial information and may affect the accounting and internal control systems employed by a bank.

- Obtain sufficient understanding of the CIS environment prevalent in the bank, the interfaces established between various sub systems, flow of data, validations, functionality of each item of software etc.
- Obtain sufficient understanding of the effect of CIS environment on internal control systems.
- Flow of authorised, correct and complete data to the processing centre.
- Processing, analysis and reporting undertaken with the use of computer.
- The impact of computer based systems on the audit trail that could otherwise be expected to exist in an entirely manual system.
- Determine the effect of CIS environment on the assessment of overall audit risk and of risk at the account balance and class of transaction level.
- Design and perform appropriate tests of control and substantive procedures.

Nature of Risks and Internal Control Prevalent

The nature of risks and internal control characters in CIS environment include the following: -

Lack of Transaction Trails:

Some CIS are designed so that a comprehensive transaction trail that is normally useful for audit may exist only for a short period of time or only in computer readable form. Several accounting entries passed and its impact on general ledger are system generated, based upon logic in built in the computer programs. Accordingly, errors in the programming logic may not be detected by merely manual procedures.

Uniform Processing Transactions:

Computers handle uniformly transactions with the same pro-

cessing instructions. While clerical errors ordinarily associated with manual processing are virtually eliminated, programming errors would ordinarily result in all transactions being processed inaccurately. It may also happen that the programming instructions may not take care of all business intricacies and situation. For example, banks charge penal interest to customers for delayed receipt of stock statements beyond the stipulated time. In case computer programs do not take care of this contingency, calculation of interest would be incorrect.

Lack of Segregation:

Many control procedures that would ordinarily be performed by different individuals in manual systems may become concentrated in a CIS environment. Thus, an individual, who has access to computer programs, processing or data may be in a position to perform incompatible functions. There have been newspaper reports about certain call centre employees making irregular payments by having access to privileged information.

Potential for Errors and Irregularities:

The potential for human errors in the development, maintenance and execution of computer information systems may be greater than in manual systems, *inter alia* due to level of details inherent in these activities. Further, the potential for individuals to gain unauthorised access to data or alter data without visible evidence are greater in CIS than in manual systems.

Initiation or Execution of Transactions:

Computer information system may include the capability to initiate or cause the execution of certain types of transactions automatically. Maker and checker concepts though prevalent in a particular application software may be given a go either by using facilities for auto authorise or by the maker himself giving the go ahead for a transaction by logging on using the checker's password.

Dependence of Other Controls Over Computer Processing:

Computer processing may produce reports and outputs that are used as a base for audit. The effectiveness of audit shall depend to a considerable extent on the accuracy, correctness and completeness of the reports generated by the computer system. It is quite likely that some of the reports generated by the computer system are wrong either due to faulty logic, inaccurate functionality or even by manual intervention by the bank staff before handing over this report to the auditor. It is quite possible that reports on computer are downloaded to excel where certain values are altered before being handed over to the auditors.

Potential for the Use of Computer Assisted Audit Techniques:

While evaluating the reliability of accounting and internal control systems, the auditor would consider whether these systems are *inter alia*:

- Ensure that authorised, correct and complete data are made available for processing.
- Provide for timely detection and correction of errors.
- Ensure that in case of interruption in the working of the CIS environment 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 output.
- Provide adequate data security against fire and other calamities, wrong processing, frauds etc.
- Prevent unauthorised amendments to the programs.
- Provide for a safe custody of source code of application software and data files.

Auditor should make enquiries and satisfy himself whether:

a. Adequate procedures exist to ensure that data is transmitted correctly.

The potential for human errors in the development, maintenance and execution of computer information systems may be greater than in manual systems, *inter alia* due to level of details inherent in these activities.

b. Cross-verification of records, reconciliation statements and control systems between primary and subsidiary ledgers do exist and are operative. There should be no assumed accuracy of computerised records.

The auditor should also document the audit plan, the nature, timing and extent of audit procedures performed and the conclusions drawn from the evidence obtained. All audit evidence which is in electronic form should be properly and safely stored and are to be retrieved in its entirety as and when required.

To facilitate the audit of a bank operating in CIS environment, a general purpose activity check list is given ahead. This check list is to be modified to suit individual requirements depending upon the auditors' impression of the efficacy of the CIS environment and other relevant factors.

CHECK LIST FOR ENSURING COMPLIANCE WITH AAS 28-AUDITING IN A COMPUTERIZED INFORMATION SYSTEMS ENVIRONMENT

Name of the bank:

Particulars of branch:

Period during which audit/review was carried out:

Review carried out by:

Sl. No	Audit review carried out	Find-ings	Working paper reference
1.	**General understanding**		
1.1	Please furnish an overview of the CIS environment prevalent in the bank, indicating separately each software application used by the bank/branch at any time during the year under review (for example, if the bank used a core banking solution along with separate ATMs, Internet banking software application, set out the CIS environment for each of these, the period for which each software is being used etc).		
1.2	Were different versions of the software used by the bank/branch during the year? If so, furnish details for each item of such software.		
1.3	Did the bank migrate from an earlier legacy system to the current system during the year? If so, furnish details of the old software, and date of migration.		
1.4	Please furnish an overview of the hardware environment available with the bank/branch, the details of the relevant manufacturers, the date from which each item is being used.		
1.5	Has the bank carried out any IS audit during the year? If so, summarise the scope of the review, the period covered, their salient observations and the corrective action taken by the bank as a result thereof.		
1.6	Summarise observations of previous statutory auditors/internal inspectors/concurrent auditors/RBI relevant for the current exercise.		
1.7	List out areas/activities/transactions/instruments which are handled manually or outside system. How is each such item handled?		
1.8	Are there documented procedures available for all activities to be carried out by the data centre/IS department?		
1.9	Are there user manuals available for each item of application software at bank/branch? Are they current and up-to-date?		
1.10	What are the functions of each person in the IT department/data centre.		
1.11	Is system administration and business application administration kept as separate activities?		
1.12	Does the bank provide Internet banking facilities? Did the bank obtain the approval of the Reserve Bank of India before offering such facilities?		
1.13	Set out briefly interfaces available between different sets of software and data movement from one to another.		
2.	**Application Software (To be prepared separately for each application software)**		
2.1	**Authentication**		
a.	When a new user is created in the system, who generates the default password and is this forced to be changed on first login?		
b.	How is the password generated communicated to the end-user?		
c.	How are passwords transferred in the application to the database?		

d.	Is there a password policy; If so, are users aware of the same?		
e.	Can passwords be reused, if so at what frequency?		
f.	Are number of changes to password in a day restricted?		
g.	Are one-way hashes or any other encryption used to store and compare the passwords?		
h.	Are entered passwords decrypted to be compared with the one stored in the database?		
i	What is the min & max length of passwords? Are they case sensitive? Can user names and passwords be the same?		
j.	How is password loss handled?		
k.	Are the user details encrypted in the database?		
l.	Does the system lock out users on 'x' number of login attempts? If so, how is the same controlled by the Application administrator?		
m.	Is the session expiry time and other authentication related parameters configurable?		
n.	Are failed login attempts logged?		
o.	Is the previous login information flashed on login?		
p.	Does it show the duration of the session?		
q.	How are administrator's details managed? How are the details managed when a system or application administrator is on leave?		
r.	How user records of those who have quit or transferred are handled in the application?		
s.	Is remote access to applications provided? If so, how are security issues are handled? If remote access is provided, are there any secure communication channel established?		
2.2	**Access Control**		
a.	Are user groups maintained? If so, are access rights granted at the group level or at an individual user level? And how are read/write access given to a module?		
b.	Is there a maker-checker process in place? If so, set out details		
c.	How is maker-checker met when the assigned checker is not available?		
d.	Does the system allow auto authorise?		
e.	Obtain a matrix setting out the authorisation limits for accessing each module (data entry, verify, cancel, reverse, view)		
f.	Can software applications be accessed during holidays and non-working hours?		
g.	Are there any EOD and BOD operations?		
h.	Can a transaction be input after the EOD and before BOD?		
i.	Please furnish major activities carried out during EOD and BOD.		
J	Is application access logged? How often this log is reviewed for any intrusions?		
2.3	**Data Security**		
a.	What is the security provided to the database?		
b.	How does the application access the database?		
c	Can users access the database using any other utility or directly?		
d.	How are temporary users handled in the system?		
2.4	**Data Integrity**		
a.	What are the back-end changes that have been made in applications? Is there a record of changes made, date of change, person who authorised the same, person who made the change, table readings before and after the change?		
b.	Have you procured all available documents in this respect and reviewed them?		
c.	Are back end changes resorted to occasionally with adequate reasons or are there a number of them indicating a larger problem?		
d.	How is transmission of sensitive information handled in the systems?		
e.	Are any standard encryption algorithms used for the same?		

f.	Are all user activities logged?		
g.	How are adjustments/corrections, if any, handled in the applications?		
h	Does the testing area application is in sync with the production area (which includes the application software, any middleware, database objects, reports etc)?		
2.5	**Audit Logs**		
a.	Are all changes to master information captured and logged in the system?		
b.	Please set out briefly all audit logs available in the system.		
c.	Have you reviewed changes to master information carried out during the year and are you satisfied that they are in order?		
d.	Have you verified all changes to interest and tax masters with reference to circulars received from central office along with the date of their validity?		
2.6	**Testing**		
a	Did the bank carry out a formal testing of all new software/versions of the same before being incorporated into the production environment?		
b.	Have you reviewed the test cases, the expected results document and the results generated from the new system to ensure their accuracy and consistency?		
c.	Are the test and production environment clearly segregated and demarcated?		
d.	Were formal signoffs issued for each item of new software/version?		
e.	What are the known bugs in the software/functionality and how are these controlled?		
f.	What change requests are pending completions from the software vendor? Do any of these reveal any bugs or deficiencies in the application software?		
g.	Are there any documented procedures for change requests, change management, release to test area from development and release to production area from test environment?		
h.	How are failures in EOD/BOD handled?		
I	Are there multiple resources authorised to run the EOD/BOD?		
j.	Are there any unprocessed transactions outstanding as at 31st March 2006? If so give details and how are they proposed to be handled?		
2.7	**Accounting Entries**		
a.	Summarise all system generated entries.		
b.	Have you reviewed the scheme of accounting entries passed by the system to ensure their correctness?		
c.	Are there any value or back dated entries and what is the mechanism to control the same?		
d.	Is there a record of all value or back dated entries?		
e.	Can value or back dated entries be passed for a closed accounting period?		
f.	Is it possible to reconcile balances in accounts prior to and post passing of value dated entries?		
g.	Take a sample of entries passed by the system and verify its calculations and correctness (particularly calculations of interest/fees paid or charged. While selecting sample of accounts to be verified, please ensure that all types of loan and deposit accounts are covered- fixed deposits, FCNR, NRE, RFC, recurring deposits, cumulative deposits, term loans, term loans where repayments are made by EMI, cash credit, PC, PCFC, bills, foreign bills, LCs, bank guarantees etc. Sample must cover cases where payment of interest/installment, receipt of stock statements etc are delayed). Document the same. In case an audit of treasury is involved, all calculations of profit/loss on sale of securities, pay outs on derivatives etc are to be test verified.		
2.8	**Data migration**		
a.	If data has been migrated from any legacy system during the year, have you reviewed the migration process?		

b	Data migration - Is this done manually or through application utilities? If through application utilities, have these utilities been tested to ensure correctness of the data migration process and accuracy of data.		
c.	Have you reviewed the pre and post migration reports to ensure consistency and integrity of data migrated to new system?		
d.	If any data was not available in earlier legacy system, explain the process by which they were collected and input into the new system.		
e.	Was there a parallel run before which the new system went live?		
f.	What are the issues and problems still pending in the post live environment?		
3.	**IT Infrastructure at the bank**		
	Network & RDBMS Security		
a.	Who creates the user accounts and assigns folder access rights?		
b.	How are users groups maintained and ensured not part of sensitive groups like root, system etc.		
c.	What is the frequency of password change?		
d.	Is there a password policy if so what is it?		
e.	How is the creation or deletion of a network user account managed e.g. when an employee quits the organisation or transferred?		
f.	Is there a validity associated with each user account?		
g.	How are vendors/visitors from other branches (e.g. head office) provided access to the network?		
h.	Have Default passwords of RDBMS and applications been changed?		
i.	How are the RDBMS and Server Space monitored and administered to prevent crashes?		
j.	On what basis are roles organised in the RDBMS from a security perspective?		
k.	Are any system administration utilities used?		
l.	What are the precautions taken against viruses? How and what is the process of ensuring latest DAT files are updated on all servers, desktops, laptops? Are these being monitored?		
m.	Can you please share the guidelines on users from the computer policy and planning department (CPPD)?		
n.	Spy ware, adware, malware, trojans - What kind of protection is provided to ensure these are not present in the network?		
o.	Are all hardware equipments, network under maintenance contracts? Are they being serviced, maintained regularly?		
p.	Perimeter security - How is the bank's network infrastructure and server infrastructure protected? Has anyone tested the routers, firewall, gateway, bridge configuration parameters? Has anyone done a penetration and intrusion testing on these? What are the results?		
q.	How often are the application and the database backed up? What is the backup policy? Is it daily incremental or daily full? What about weekly backups? Where and how are the tape media stored? Is it stored in an off-site location? Are these tapes tested for backup effectiveness? Are back up logs maintained, monitored, and reviewed?		
r.	How are end users trained on using the application software? How is it done for new users? How are users trained on new modules / enhancements?		
s.	Is the tape media life monitored? What happens once a tape reaches its life? How is this tape destroyed? Are there any logs for these?		
4.	**Business Continuity and Disaster Recovery Plans**		
a.	What is the business continuity plan of the bank/branch?		

b.	What are the backup procedures that are in place?		
c.	Where is the DR site located? Is it in the same building or geographically different location? How is the live production environment replicated on a DR site? Is this tested regularly? Is this facility manned? What kind of security process is implemented in a DR site? What kind of communication links are provided at the DR site? How is the switch over from the live site to DR site is planned? Has this been tested? How often is this tested? Are these tests documented? Are there any teams responsible for BCP and DR activities?		
d.	Where are the backups stored, what is the frequency of recycling the tapes, are periodic readability tests performed on the tapes and are logs of the same maintained?		
e.	What are the service level agreements with vendors and the Information System Department of the bank for uptime of applications?		
f.	Are all software licensed? How is this monitored? Are there any document / database to monitor licenses? How is software license usage audited?		
g.	Are vital and statutory documents printed regularly or backed-up electronically?		
h.	Are databases mirrored?		
i.	Is there a periodic review of the BCP related activities?		
j.	In case of server crashes, what is the contingency plan in place?		
k.	Was there any crash in the computer system during the year? If so, how were the application software and data base restored?		
l.	Were any consistency checks made before restoring the application software and data base?		
5.	**Hacking**		
a.	Were there any reported cases of hacking of the computer systems during the year? If so, please furnish details.		
b.	Have there been complaints from customers regarding wrong balances/transactions in their accounts? If so, please furnish details of each of them.		
c.	Have any frauds or irregularities been detected due to malfunction of the computer systems?		
d.	Have there been instances where cash as per ATM did not match with books? If so, furnish full details.		
6.	**Identification of transaction for substantative checking**		
a.	Use the data available in the computer system to identify large transactions, select a sample, transactions which are outside the mean value by a significant percentage. For this purpose, the data base can be down loaded into excel , which could then be sorted, arranged in ascending/descending order to facilitate identification of transactions which are large or outside the mean value by a significant percentage.		
7.	**Use of reports generated by system**		
a.	Before relying on any report generated by the system, carry out validation checks to ensure that the same is complete and correct. This could be done by identifying a sample of transactions, validating them with the base records in the system and cross checking the results arrived at by the system. Do not take all reports which are generated by the system at its face value. There may be bugs or deficiencies in the report generated or there may be interventions by the bank while generating the report (by down loading data to excel and making corrections to certain fields before they are handed over for audit)		
b.	Are all control accounts and subsidiary ledgers compared and reconciled?		
c.	Are there any instances of the same data as per different sets of reports being different and inconsistent?		
8.	**Documentation**		
	Is all information in electronic form properly indexed, labelled and maintained in a readily retrievable form?		