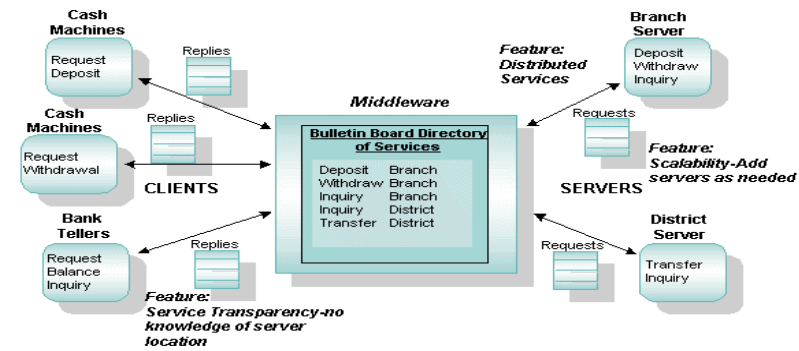# Risk Based Audit in CBS Environment

WIRC Seminar on Statutory Audit of Bank Branches

Ashutosh Pednekar

M P Chitale & Co.

Mumbai, India
March 18, 2017

Banks and CBS

■ Computerisation in banks has come a long way from manual processes:

- Ledger posting machines

- Dispersed desk top computing

  ■ Supported by end user applications

- Softwares for banking operations at branches

  ■ Client – server technologies

  ■ Exception reporting

- Centralised banking solutions or Core Banking Solutions

Centralized **O**nline **R**eal-time **E**nvironment"

CBS characteristics

- Server at a central location

- Connectivity to all banking locations
  - Branches
  - ATMs
  - Internet
  - Mobile

- Transaction recorded onto the central server

- Report generations controlled centrally

- Lot of peripheral systems integrated with CBS

Controls in CBS

- Understand how the CBS is implemented

- Understand what controls are in place to ensure that the CIA principle works unfettered in the bank

  - *Confidentiality*

  - *Integrity*

  - *Availability*

To use these controls for audit objectives, we have to rely on our "Audit Smartness" and not be bogged down that we may not be "IT Smart"

Our basic material for evaluating computerized environment

- **SA 315 → Identifying and assessing Risks of Material Misstatement through understanding the Entity and its environment**

  - Controls over IT Systems are effective if they maintain the integrity of information and security of data

- **Guidance Note on Audit of Banks**

  - General guidance on controls in a computerised environment

  - CBS specific guidance

Our basic material for evaluating computerized environment...

- Also peruse the Guidance Note on Audit of Internal Financial Controls over Financial Reporting

  - Though not applicable to audits of nationalised banks that are not companies, the guidance note has good reference to IT controls in an automated processing environment

Our basic material for evaluating computerized environment...

- **Risk Assessment & Responses to Assessed Risks Standards on Auditing**

  - SA 300 – Planning

  - SA 315 – Identification & Assessment of Risks of Material Misstatements Through Understanding an Entity & its Environment

  - SA 320 – Materiality in Planning and Performing an Audit

  - SA 330 – The Auditors Responses to Assessed Risks

  - SA 402 – Audit Consideration Relating to an Entity Using a Service Organisation

  - SA 450 – Evaluation of Misstatements Identified During an Audit

First steps at the branch

- Take two interviews:-
  - Systems in charge / System Executive (SE)
  - Branch Manager
- Obtain an overview of the systems
  - Software
  - Hardware
  - Network configurations
- Ask the SE of his perception of CIA principle in the branch
- Take the SE's views on the LFAR questions

First steps at the branch...

■ Take written and oral representations that:-

- System is implemented as designed

- No modifications are made to the system at / from the level of the branch

- All problems faced during implementation / upgradation / migration & thereafter are resolved

- Problems faced have not affected the confidentiality, integrity & availability of data

First steps at the branch...

- Now meet the branch manager & take his view on information gathered from the SE

- Specifically inquire of his methodologies about

  - EOD / SOD process

  - Sign off on MIS & exception reports

  - Any additional responsibility due to implementation of CBS & whether it affects the branch banking business

Some key audit processes

- **Access Control Matrix**

  - Peruse and inquire whether it matches with users at the branch

    - Satisfy yourself that users in the Branch are aware of the importance of access controls

  - User management processes

    - Creation / Modification / Deletion / Restoration

  - Inquire whether logs of unauthorised access are available at branch / data centre

    - If so, review management action

Some key audit processes...

- **Transaction logs**

  - Serial control over all transactions without manual intervention

  - Peruse logs of "heavy days"

- **Reports from CBS**

  - For business / monitoring / audit & inspection / regulatory reporting

  - For exceptional transactions

  - Distribution → electronic / manual

  - Sign-offs on the reports

Some key audit processes...

■ Access to CBS

- Normally a read-alone access is given.

- In case it is not given, request for access with aid of a valid user of the branch.

- Please mention the type of access granted in the LFAR

- Even with a read-alone access help of a valid and experienced user may be necessary for due audit completion

- Query the database

Some key audit processes...

- **Queries on the database**
  - Use the help and expertise of the SE to run queries & generate information needed for the audit
    - Various courses conducted by WIRC on Concurrent Audits have explained the product specific reports that are available
  - The SE will seek help of the Data Centre in case required
  - Analyse data collected as per specific query (i.e. purpose for which the details / data have been extracted)
  - Data collected along with Auditors' remarks should be stored as Audit Working Paper

Controls in CBS

■ Various types of Controls are embedded at various levels in CBS; two main categories of controls:-

- Application Controls
- IT Administrative Controls & Security

Controls in CBS – Application Controls

- **Access Controls in Software Areas as per delegated powers to Employees / Users**

- **Data Input (Validation) Controls**

- **Product Level Controls**

  - Prefixed Financial Parameters (Like Interest Rate, Penal Interest Rates)

  - Fixed Tenure (Pre-defined terms Fixed Deposits / Service Types (Principal and Interest Repayment Type and Periodicity)

  - Tax and Regulatory compliances

- **Authorization of a transaction as per delegated authority**

- **Controlled Error Handling through Warning, Exception and Error Reporting**

Controls in CBS – IT Admin. Control & Security

- Controls are associated with processing activity

- It allows user to use the Software as per Access Rights Table

- Confirmation / Prior Authorisation for any outside Software Installations.

- To ensure encryption of Data

- To ensure no changes are effected in IT Hardware

- Logical Access Controls

  - Access to System / Menu as per the Category and Type of Branch / SOL

  - Single Sign-on for all the applications

  - Maker & Checker Control

- Security policies for all IT Assets (incl. Hardware, Softwares, Databases etc.)

Audit Processes & Use of Technologies

- <u>Be aware of vulnerabilities that reside in usage of CBS:</u>

  - Processing is completely automated. Hence, a manual error in Master Data updation has a huge effect on all the transactions of the same kind.

  - Processing is not visible

  - Lack of discipline in Access Control

  - Lack of Training for New software environment

  - Audit Trail may not be visible for all the type of transactions

Audit Processes & Use of Technologies…

- **Which Techniques / Technologies to be used?**

  - CAAT – Computer Assisted Audit Techniques

    - Not every auditor has such a tool

    - Not every bank permits usage of such a tool on its systems

  - General Audit Softwares / Spreadsheets

  - Query Languages like SQL

Querying the database

- Query Languages like SQL can be used to carve out data as per criteria from Database Servers.

  - However, it requires expertise and in-depth knowledge of System and Software.

  - Requires permission to Access the Database to apply the procedures.

  - Analyse data collected as per specific query (i.e. purpose for which the details / data have been extracted)

  - Data collected along with Auditors' remarks should be stored as Audit Working Paper

- If the Auditors are not having direct access to Database Server, a request to Data center officials can be placed for requirement of Data and Parameters.

- Based on the parameters and Field requirements, Data Center can generate the reports to be shared with Auditors for their further processing.

Income – interest

- Interest rate parameters are controlled centrally

- Obtain list of transactions where interest rate has been entered by branch management

- Ensure that such entry and authorization is as per Access Control Rules

- Review process of interest rate modifications in similar manner

- Test check a few interest calculations

Income – charges

- As in case of interest rate, parameters for other charges are controlled centrally

- Ensure that the software relates the transaction with the income to be applied

  - Bank Guarantee / LC and its Commission / Charges

  - ATM / Credit Card charges

  - Charges for miscellaneous transactions

    - Number of debits

    - Note counting

- Review transactions where branch has an authority to deviate from the set parameters

- Test check a few transactions

Advances

- Verify data entry of new sanctions into the CBS

  - Rate of Interest

  - Date of sanction

  - Date of commencement of interest

  - EMI – static over period of loan or dynamic (EMI changes after a block of years)

- Inquire whether loan documentation is controlled through the system

  - If so, whether system prompts for the same

- Whether system prompts for renewals

NPAs

- Inquire whether system identifies NPAs and reverses income

- Check paramterisation of system to identify NPAs:-

  - Defaults in excess of 90 days principal repayment or continuously overdrawn

  - Interest not fully serviced

  - Sanction limit expired and account not renewed

  - Packing credits defaults – running account

- Certain accounts not NPAs

  - Account with credit balance or not outstanding amounts

  - Staff schemes

  - Accounts under Central Government Guarantee

NPAs…

- Potential NPA → Audit list of defaults nearing but not exceeding 90 days (SMA 2)

- Peruse list of customers / accounts with high credits within last week / fortnight of March

- Identify whether there are heavy withdrawals in first week / fortnight of April of customers / accounts in this list

- One customer – one classification

- Upgradation of account

  - Balance within limits

  - No overdues

  - Credits available for servicing interest

Deferment due to Demonitisation

- **Circular dated November 21, 2016**

  - Eligibility:

    - i) Running working capital finance (CC/OD), Crop loans with sanctioned limits upto Rs. 1 crore

    - ii) Term Loans with original sanctioned limit upto Rs. 1 crore

    - iii) Loans to NBFC / Housing Finance Companies, PACs

    - iv) Loans by State Co-op. Bank to DCCBs

  - Conditions:

    - i) Dues are payable between 01.Nov.16 to 31.Dec.16

    - ii) Deferment restricted to the above period for further 60 days

    - iii) Applies only to PAs and not to existing NPAs

Deferment due to Demonitisation

- **Circular dated December 28, 2016**

  - Eligibility:

    - i) Running working capital finance (CC/OD), Crop loans with sanctioned limits upto Rs. 1 crore

    - ii) **Business (including Agriculture)** Term Loans with

      - original sanctioned limit upto Rs. 1 crore

        (both limits are mutually exclusive)

  - Conditions:

    - i) Dues are payable between 01.Nov.16 to 31.Dec.16

    - ii) Deferment restricted to the above period for further 30 days (i.e., in all 60 + 30 = 90 days)

    - iii) Applies only to PAs and not to existing NPA

Deferment due to Demonitisation

- **Auditors' primary checks:**

    - Installments getting due during Nov. 2016 and Dec. 2016 will have immunity under this circulars.

    - Check how the system configuration is handled for such cases? Is it manual?

    - Whether Repayment Date is extended by 2 months in CBS? If so there is a possibility of extending entire loan tenure by 2 months (Not in line with Circular)

Deposits & interest thereon

- Ensure proper parameterization of deposit schemes and interest thereon

- Trace a sample of transactions

- Verify calculations of interest expenditure in few cases

- Review process of pre-mandated transactions and whether they have happened as per the mandate

  - Auto sweep account

  - Cumulative deposits

  - Recurring deposits

Office accounts

- **Review various office accounts**
  - Suspense
  - Sundry Deposits
  - Inter branch (Inter Sol)
  - ATM Suspense
  - Credit Cards
  - Cash Management
  - Pointing Type / Non-Pointing Type Accounts
- **Audit list of outstanding items**
- **Inquire whether frauds have occurred using these office accounts**

Office accounts...

- **Potential misuse patterns**

  - Cash Payment from Office Accounts

  - TOD through Office Accounts

  - Parking of Cash Difference in Office Accounts

  - Clearing / Remittance differences through Office Accounts

  - Rotation of entries in Office Accounts

  - Correctness in mapping of reversal transaction to originating transaction

  - Value Dated Transactions

  - Round Tripping

  - Advance paid for Fixed Assets not capitalized

  - Income realized not credited to Revenue Account

Retail banking & payment systems

- Review process of mobile banking

- Payment gateways

- Aadhaar based payments

- Internet banking

- Special reports generated for clients who have large retail customers

  - Insurance companies / e-commerce / payment wallets

Audit Processes & Use of Technologies...

- **General Data Collection:**

  - Physical Copy of Papers or related details / data should be verified and crosschecked from the details so extracted

  - The data serve the purpose of Audit Evidence and nature of Audit Process carried out

  - The data so collected should be part of working papers

Financials review

- **Process of generating financial statements**

  - Any manual intervention areas to be focused upon

  - MOCs for year under audit

- **Transfer of opening balances**

  - Proper accounting of MOCs of previous year

- **Reconciling EOD reports with Trial Balance**

Audit conclusion

- Document findings & conclusions

- Discuss them

- Take written and oral representations

- Formulate Audit Opinion

LFAR 2003

■ For each of the six questions one needs to:-

- Inquire about Bank's policy

- Level of understanding of the policy and implication if it is not adhered to

- Evidence of compliance with that policy at branch

- Peruse action taken on Concurrent & System audit findings & management action thereon

Area is too wide to be covered as part of Branch Statutory Audit if it is to be done diligently

Thank you

Views expressed today are mine and not of ICAI / RBI / M P Chitale & Co

ashu01@mpchitale.com