Case Study

on

Information System Audit at

Uttar Bihar Gramin Bank, Muzaffarpur

(2014-15)

Dr. Shyam Kumar Garg

Bankers Institute of Rural Development, Lucknow

CONTENTS

CHAPTER 1

Introduction

1.1. About the Bank

Bihar is the 12th largest state of our country geographically and third largest demographically where the population was 10.38 Crore in year 2011. 99% of inhabited area is rural in Bihar. Bihar has the lowest per-capita state GDP and the highest density of population of 1100 persons per sq.km. In the year 2013 Bihar was the fastest growing state with 23.7% growth in GDP.

North Bihar is counted among the most backward regions of India. Muzaffarpur is the largest city of North Bihar. Uttar Bihar Gramin Bank (UBGB), headquartered at Muzaffarpur, is an amalgam of erstwhile eight RRBs sponsored by Central Bank of India. The Bank has its presence in 18 districts of North Bihar. The Bank represents about 40% of the entire Branch network of all Banks in these districts. UBGB has a network of 1020 Branches with 14 Regional Offices. UBGB has 3382 officials, working out to 2.99 staff members per Branch.

UBGB earned a Net Profit of Rs. 50.01 Crore during the year ended on 31st March 2013. Cumulative profits of the bank are Rs. 177.77 Crore. The Bank has Net worth of Rs. 632.31 Crore as on 31st March 2013. The authorized capital of the Bank is Rs. 40 Crore. Paid up share capital is Rs. 8 Crore which has been issued and subscribed by Government of India, Central Bank of India and Government of Bihar in the ratio of 50:35:15.

The aggregate deposit as on 31st March 2013 were 8,387.40 Crore. The share of low cost deposit (CASA) was 71.32% of the total deposit. The cost of deposit works out to 4.01%. The aggregate loans and advances outstanding as on 31 March 2013 were Rs. 4344.85 Crore. Out of total outstanding loans and advances, the loans under Priority Sector were Rs. 2,686.71 Crore. The CD Ratio of the Bank was 51.80%. The Gross and Net NPA of the Bank were 3.14% and 1.90% respectively.

The Management of the Bank intends to take the leadership position in the North Bihar region. The Management has taken many new initiatives to keep pace with the latest happenings in the Banking sector. A few initiatives are introduction of RuPay Debit Cards, Government to Public (G2P) payments, Group Insurance etc.

The Bank adopted a five year perspective plan called "Gram-Chetna" for holistic development and wealth creation in villages where each Banking outlet of UBGB will be a centre of rural vitality for not only channelizing the financial products for rural development but also imparting the financial literacy amongst rural population. Some of the Major Highlights of the Bank are as follows:

Self Help Groups	8,172 SHGs were formed and 5,845 SHGs were credit linked. Rs. 439.01 Crore disbursed in 53955 accounts as on 31 March 2014.
Kisan Credit Cards	3,97,977 KCCs were issues and Rs. 2,375.47 Crore was disbursed.
Swarojgar Credit Cards	25,618 Cards amounting to Rs. 74.52 Crore were issued.
General Purpose Credit Cards	The Bank issued 18,309 Cards and disbursed Rs. 55.18 Crore.
Farmer's Club	The Bank opened 1256 Farmer's Club by the end of FY 2012-13.
Financial Inclusion	UBGB has opened FLCs in all 18 districts. With the help of "Sunahara Sapna Ultra Small Branches" Bank is providing Banking services under Financial Inclusion programme in all the allotted villages.

1.2   Computerization in the Bank

Keeping in view the directives of RBI and the guidelines of sponsor Bank viz., CBI, all Branches of UBGB were put on Core Banking Solution (CBS). The Bank adopted FINACLE CBS s/w. CBS nodes were placed in Head Office and all Regional Offices. The Bank started the facilities like NEFT, INTERSOL CREDIT and issuance of ATM cards to its customers.

Computerization in the Bank at a Glance:

Main Software at Head Office, Regional Offices and Branches	Operating System: Windows 7 CBS Software: Finacle Link Access through Web
Main Hardware at Head Office, Regional Offices and Branches	Desktop Dual Core 2.6GHz or Higher, 3MB L2 Cache or Higher, 2GB RAM with 1066 MHz, 160GB HDD, 15" TFT Monitor, 101 Keyboard, Mouse Lipi 2250- Lipi passbook printer, Wipro DS 800 Printer and Scanner
Main Network Accessories at Head Office, Regional Offices and Branches	VSAT Hardware, Branch Router CISCO1841-SEC/K9, Ethernet Switch CISCO881G-S-K9, Wall Mount Racks, with structured Cabling on USB- CAT 5 cables
Connectivity	Two lines -MPLS (Lease Line and ISDN) at Head Office and all Regional Offices. VSAT in all the Branches. No backup line at present. The Bank is planning to provide Lease Line to 173 Branches as a secondary connectivity option.
Name of Vendors	WIPRO – System Integrator Hugh- VSAT Connectivity TCLS-MPLS Connectivity at HO & ROs

	BSNL-ISDN Backup Connectivity at HO & ROs
Data Centre and Disaster Recovery Sites (DC & DRC) sites	Shared with sponsored Bank i.e. Central Bank of India. Data Centre is situated at Central Business District (CBD), Belapur, Navi Mumbai and DRC is at Hyderabad.
Technology at Ultra Small Branches	HCL InfoTech

1.3. CBS and the Audit work in Bank - Some Observations

- **User Management:** Each user is associated with a "Work Class" in CBS. The "Work Class" determines the category for each user and assigns the rights of working called "Privileges" in CBS accordingly. For example Auditor's Work Class is 10, Branch Manager's Work Class is 400, Officer's is 300 etc.

- **Audit Queries:** There is a "Filter" feature in CBS, which may help the Auditors to perform various audit-queries in Finacle.

- **New Report Generation:** If Auditor needs a new report from Finacle, he has to send the request to DIT (Department of Information Technology) at Head Office of the Bank. The DIT in turn sends the requirement to the Administrator of Data Centre for generating the report.

- **Requirement of changes in Finacle:** If any change is required in the system, a "Requirement Document" is prepared by DIT and is sent to the Chief Internal Security Officer (CISO). CISO is the officer deputed by the sponsor Bank-CBI. If CISO is convinced he will recommend it to the Administrator of the Data Centre. The role of the Administrator would be to make the changes and percolate to all the Branches.

- **Data Security:** The regular backup is taken by DBA and daily data is shifted to the DRC site also. EOD operations take the backup of the data on the magnetic tapes at DRC automatically. At present there is no

concept of maintaining the "Shadow Database Server" at the Head Office of the Bank.

- **Management and Maintenance of CBS:** At present WIPRO, the system integrator of the Bank has deployed nine officials to work on the "Help Desk" at the Head Office for redressal of the problems being faced by the Branches in CBS.

- **Access Control Matrix and Parameter Setting:** It is routed through the DIT to the CISO posted by the sponsor Bank. After the approval of CISO, the DBA sitting at the Data Centre will set/ reset the parameters and amend the Access Control Matrix.

- **Proactive Management:** Management of UBGB is proactive and helping the Auditors in their capacity building so that they can work purposefully and professionally. Each Auditor has been equipped with a Laptop Computer. The Bank encourages the Auditors to use Laptop Computers effectively in "Risk Based Audit".

- **Audit Department at HO:** In Head Office there are only 5 officials in the Audit Department. The basic job of the Audit Department is to plan, coordinate and monitor the audit work of the Bank. There are 47 Auditors posted in different Regional Offices to audit the Branches of their respective area.

- **Compliance of Audit Report:** With reference to the Audit Work, the role of the Regional Manager is to monitor and ensure action on Audit Objections and send compliance report to Head Office. The Regional Manager may also inform the major problems to HO. As a Chairman of "Regional Closure Committee", he has to decide the closure of audit work after its completion.

1.4   Audit in Bank - Some Issues

- The computer literacy amongst the Auditors of the Bank needs to be enhanced as the knowledge on computer is very limited for most of the Auditors.

- The Bank has to prepare the inventory list of all authorized software (Application and System Software both) and Hardware so that the Auditors can verify them during their visits to the Branches.

- A list of users kept in "Disable" category may help the Auditors to check un-authorized users in the Branches. Users, who are retired, went on long leave, terminated from the services or the users against whom some disciplinary action is pending come under the "Disable" category.

- Bank may have a specific plan to reduce the dependency on external IT companies, which are maintaining DC, DRC, data and other computing resources. At any moment of time if the Bank decides to go for some new System Integrator, the Bank should have some "EXIT" policy.

- The Bank may think of auditing the Data Centre and Disaster Recovery Sites. Other delivery channels such as "Micro ATMs", "ATMs" etc. may also be audited.

- Auditors may be trained on understanding "Audit Trails", "Exception Reports'", "Inter Branch Reconciliation", "ATM payments" etc. in their audit work.

- The auditors may be sensitized on how to use "CAAT", "Audit Module of Finacle" and "MS-Excel" in their audit activities.

- Dependency of the Auditors on Branch functionaries in auditing a Branch should be as minimum as possible as audit work is an independent work and to be performed without much involvement of Branch functionaries.

CHAPTER 2
Information Requirements for IS Audit

During the audit of a CBS Branch, the Auditor has to collect various information from the authentic sources and has to physically verify them. The information collected by the Auditors is as follows:

- User-IDs details of staff
- Details of Hardware (Computers, Printers, Scanners etc.) inventory
- Details of Software (System and Application software) inventory
- Details of frauds in Branch/es
- Various Reports (Monthly, Quarterly, Half-yearly etc.) being generated by the Branch
- Details of UPS and Network items in the Branch
- Details of Fire Extinguishers, insurance of IT assets etc.

The Auditor has to give the above information along with the Branch profile in his audit report in the pre-defined format. The report finally prepared in the following format:

2.1   Report on Information System Audit of Branch office_____

BRANCH   PROFILE:

Branch Name	Branch Code	
Address:	Region:	
	Category:	Size:
Contact Nos.:	E-mail address:	
Fax No.:		
Total Deposits: Rupees (Crores): _____ As on :_____	Total Advances: Rupees (Crores):_____ As on :_____	

Average Number of Vouchers:-
AUDITING DETAILS

Checklist No.	Checklist	Maximum Score	Score Attained by the Branch
	For CBS Branches only	100	
Total		**100**	

Score (%) =TOTAL of Score Attained by Branch x 100/ TOTAL of Maximum Score	Score (%) =

Particulars	Previous Audit	Current Audit
Period of Audit		
Audited By		
Date of commencement		
Date of completion		
No. of Man days		
Score (%)		
Risk Rating*		

-Date of submission of minor irregularities, if any, to the Branch Manager--------
-Date of submission of interim report, if any---
-Date of submission of final report ---

2.2 STAFFING DETAILS

Designation	Name	Scale	Joining Date in Branch
Branch Manager			

OTHERS

	NUMBER
Officers	
Special Assistants	
Office Assistants	
Office Attendants	
Total Staff	

Staff Details and User-ID-wise details

Level	No. of Users	Active	Disabled/Deleted
1.			
2.			
3.			
4			
5			
TOTAL			

2.3 SYSTEM DETAILS (HARDWARE & SOFTWARE)
1. HARDWARE DEPLOYED AT BRANCH

Number	Vendor details	Date of Expiry
Computer Terminals 1. No. of PCs/ Terminals with :		
No. of Printers 1. Lipi 2250 2. Pass Book Printer 3. FDR Printer		
UPS Make: Capacity:		
Scanner:		

2.4 SOFTWARE MODULE INFORMATION

SOFTWARE NAME: _____VERSION NO.:_____

Modules	Functional	
	Yes	No
System Parameters (DC activity)		
Day End		
Account maintenance (SB/CC/CD/OD)		
Cheque Maintenance		
Inward and Outward Clearing (Voucher processing)		
Term Deposits		
DDs/PO		
TDS		
Loans & Advances		
Bills & Remittances		
Forex		
Safe Deposits		
Cash Transactions		
MIS , Control Return Reports		
Standing Instructions		

2.5   FRAUD DETAILS (Through System)

Nature of Fraud (Details)	
Modus Operandi	
Amount Involved	
Action Taken:	

2.6   OUTPUT REPORTS GENERATED BY THE BRANCH
A. DAILY REPORTS

Sr No	Reports Generated	Printed (Y/N)	Checked & signed(Y/N)	Preserved (Y/N)
1	Cash Book			
2	General Ledger Balance-Book			
3	Supplementary			
4	Transfer Scroll			
5	Outward Clearing Schedule			
6	Inward Clearing Schedule			
7	Cash Receipt			
8	Cash Payment			
9	Cash Balance Position			
10	Exceptional Transaction report			
11	List of cancelled entries			
12	List of Debit balances			
13	Consistency Check reports			
14	TOD Interest charge report			
15	Withdrawal against Effects (WAE) charges list			

B. MONTHLY REPORTS

Sr No	Reports Generated	Printed (Y/N)	Initialed(Y/N)	Preserved(Y/N)
1	**P&L Statement of Debits-**			
	Repairs			
	Travelling Expenses			
	Miscellaneous Expenses			

C. Quarterly Reports

Sr No	Reports Generated	Printed (Y/N)	Initialed (Y/N)	Preserved (Y/N)
1	**Interest Application in**			
a	Interest Rates Master			
b	Slab Rates Master			
c	Trial Interest Application			
d	Actual Interest Application			
e	Variation in Trial and Actual			
f	Interest for complete period			
2	**Ledger Printing**			
a	Saving Bank			
b	Current Deposit			
c	Overdraft			
d	Cash Credit			
e	Loans			
f	Term Deposits			
g	Sundries			
h	Profit & Loss			
i	Pay Slip Issued			

D. HALF YEARLY REPORTS

Sr	Reports Generated	Printed	Initialed	Preserved
1	**Saving Bank Interest**			
2	**Service Charges**			
	Folio Charges			
	MICR Cheque Charges			
	Stop Payment Charges			
	Cheque Return Charges			
	Commission & Exchange			

2.7   PRINTERS

HIGH SPEED PRINTER

Make /Model	Warranty / AMC Particulars				Amount
	Vendor Name	Period			
		From	To	Last serviced	

Inkjet PRINTER / DOT MATRIX PRINTER   NO. OF PRINTERS--------

Make /Model	Warranty / AMC Particulars				Amount
	Vendor Name	Period			
		From	To	Last serviced	

PASS BOOK PRINTER   NO. OF PRINTERS--------

Make /Model	Warranty / AMC Particulars				Amount (Rs)
	Vendor Name	Period			
		From	To	Last serviced	

2.8 UNINTERRUPTED POWER SUPPLY (UPS)   NO. OF UPS---------

Make /Model	Capacity	Warranty / AMC Particulars				Amount (Rs)
		Vendor Name	Period			
			From	To	Last serviced	

2.9 Router and MODEM

Make /Model	Capacity	Warranty / AMC Particulars				Amount (Rs)
		Vendor Name	Period			
			From	To	Last serviced	

2.10   Switch

Make /Model	Capacity	Warranty / AMC Particulars				Amount (Rs)
		Vendor Name	Period			
			From	To	Last serviced	

2.11   FIRE EXTINGUISHERS   NO. OF EXTINGUISHERS---

Make /Model	Capacity	Warranty / AMC Particulars				Amount (Rs)
		Vendor Name	Period			
			From	To	Last serviced	

2.12 INSURANCE   OF   HARDWARE :(Insurance covers to be obtained on w.d.v. by notionally charging 20% depreciation p.a.)

Description	Name of the insurance Co.	Amount insured	Premium Paid	Expiry date of insurance coverage

CHAPTER 3
Audit Controls for Information System Assets

The Bank has decided to develop audit controls for auditing and safeguarding the various Information System assets available in the Branch. According to the Bank, the Auditors have to concentrate on the following areas to ensure that the Information Systems Assets of the Branch are safeguarded:

a) Asset Management and Physical Security
b) Media Management
c) Software Integrity Management
d) Data Integrity Management
e) Data Process Controls
f) Audit Controls for System Effectiveness
g) Audit Controls for System Efficiency
h) Audit Controls for Others

The Auditor is required to verify/inspect the following points in respect of the areas mentioned above.

3.1   Asset Management and Physical Security

a) BRANCH LAYOUT

- Whether Branch layout permits free movement of customers and staff members after installation of computer nodes.
- Whether the PCs are installed away from passage to avoid unauthorized access.

b) UPS MAINTENANCE

- Whether separate area/cabin is provided for UPS system
- Whether the UPS is placed in proper place.
- Whether annual maintenance contract for UPS is in force to ensure periodic servicing of the UPS
- Whether UPS is in working condition during Branch visit
- Whether the computers are the only devices , which are connected to the UPS and have adequate plug-points for the same
- Whether the UPS alarm is installed.

- Whether testing and maintenance of Batteries for UPS is done regularly. Whether report is prepared. Please check the record for changes of batteries in audit period
- Whether Capacity of the UPS system is sufficient to take care of the electricity load required for computers installed.
  (CPU- 200 watts max ,TFT Monitor – 37 watts on online mode & 1 on sleep mode, CRT Monitor –75 watts, DMP Printer – 50 Watt approx, PB Printer – 59 watts app, Line Printer – 60 watts)

c) ELECTRICAL LINES AND SWITCHES

- Whether the input power supply to the UPS continues when the main power supply to other electrical equipments is switched off?
- Whether the wiring in the Branch is concealed / under casing capping?
- Whether proper earthing is done and earth leakage voltage is checked. (Please give the date of last test of earth leakage voltage)
- Whether electrical layout ensures adequate number of switches and plug points for users
- Whether the electrical cabling is done in two segments i.e. Critical (computers) & Non-Critical (Printers/other peripherals).

d) LAN CABLING

- If Hub / Switch for LAN is not kept in Server Room, whether it is protected
- Whether there is distance of at least 6 inches between Data Cables and Electrical Cables
- Whether the LAN cabling is 'structured' and any Electrical wires and computer cables are lying loose
- Whether LAN diagram is displayed in server room (as it is secret document)
- Whether there are adequate Network points (Cable Connections) to add workstations to the networking in future

e) FIRE PROTECTION MEASURES

- Whether fire extinguishers are installed at strategic locations
- Whether fire detection system is installed in the Branch and is in optimum working condition
- Whether proper record is maintained in the Branch for refilling /servicing of fire extinguishers

- Whether staff is conversant with the use of fire extinguishers
- Whether fire drills are conducted periodically and documented

f) INSURANCE

- Whether the computer equipment is insured under valid Electronic Equipment Policy, except new equipment which has been purchased within the last one month.
- Whether the value of insurance is adequate to cover all the equipments. The insurance is done on depreciated value as per W.D.V method (20% depreciation annually)

g) SOFTWARE LICENSES SAFEGUARDING

- Whether all original software packages, executables as well as system programs are preserved in fire proof safe/cupboard
- There is no unlicensed software installed on the PCs.

h) ASSET SAFEGUARDING

- Whether access to Gateway PC / Branch Server / Network equipments /scanner is restricted only to the authorized users
- Whether Floppy Disk Drives on nodes are restricted to authorized terminals
- Whether PC monitors / printers /keyboards are free from dust and covered if not in use
- Whether eatables (tea/ coffee/food items) are littered near computer equipments
- Are the PCs / Printers/ Scanners marked or numbered as Fixed Assets
- Whether all the computer equipment (Printers /Scanners /PCs /HUBS/Server) are covered under warranty / AMC and in force
- Stamped agreements for maintenance contract are executed in Bank's format and available.

3.2 Media Management

a) VENDOR MANAGEMENT
- Whether a Software Maintenance Register is maintained
- Whether the telephone numbers of software / Hardware vendors and UPS vendors are displayed in the BM room and a copy is maintained with the Branch Manager

b) MEDIA MANAGEMENT
- Whether the media register is maintained.
- Whether the Branch is holding adequate stock of consumables as under:- (Indicate Yes / No)

  Cartridges
  Floppy Disks
  Printer Paper
  Printer Ribbon

- Identify idle hardware in the Branch and determine the period for which they have been idle. If the hardware is usable the same must be brought to the notice of the B. M.,RO ,and Head Office
- Inquire if a process is in place to ensure that all files in a media containing critical information is purged in a manner that renders it unusable and unrecoverable prior to being sent for repairs.
- Whether a User Manuals Register is maintained containing acknowledgement of the availability of all the manuals in the Branch. Whether Users Manuals are available for the following:-

  Printers (Pass Book / Serial)
  UPS
  Signature Scanner
  Software installed in the Branch

- Whether the Application Software User Manual available in the Branch are in accordance with the current version of the Software
- Whether antivirus software is loaded on PCs with hard disk and is regularly updated with latest virus definitions?
- Whether outside floppies are scanned for virus before use

c) DISASTER RECOVERY PLANNING (DRP) / BUSINESS CONTINUITY PLANNING (BCP)

- Whether the Branch has a DRP / BCP document which is supplied by HO / DIT CO is available at the Branch
- Are all the people aware of the DRP / BCP plan and their role in it
- Whether the DRP /BCP has been tested on the Branch and frequent drills conducted in the Branch

- Ready or alternate source of hardware/software is there to resume business activity within the shortest possible time after disruption.
- A reliable backup of data and software is available all the times for restoration.

3.3   Software Integrity Management

a) Application Level Security

- Is there a unique login ID for each authorized personal including Auditors & Vendors? Is the unique login User ID assigned after Branch Manager's approval only?
- Are different Access levels defined in the software and allocated to the employees as per employee grades and responsibilities.
- Whether there is any active usage of transferred / suspended /disabled User IDs.
- Whether the User IDs of staff are suspended when they go on leave.
- Whether the users logout when leaving the work table/node each time.
- Whether modification in User Level and creation of new User ID is authenticated by Officers having higher level
- Whether restricted access to Menu's for users is supported by the software and access to specified Menu's allotted to User's at the time of creation of User ID
- Whether User Id allotment register is kept under lock & key and signature of individual are taken as acknowledgment of User Id allotted in the system.
- Passwords of alphanumeric characters and / or special characters are used.
- Whether secrecy of password is being maintained. Users do not write their passwords on wall, desk diary etc. and are aware of the need for the secrecy of their passwords.
- Whether record of cancellation of User Id register is maintained and authenticated by Manager.
- Whether dummy User Ids exist in the system.
- Whether review of allotment / cancellation and access level is being done by Branch Manager regularly
- Whether any staff is given multiple level / duplicate access User ID

- System does not allow concurrent login to a single user ID from different nodes.
- Users created for temporary purpose are cancelled immediately on completion of the job.
- Whether user's names are as per Bank's service records?
- Whether an undertaking for maintaining secrecy and confidentiality of password has been obtained from every user and preserved?
- Whether the facility of automatic intimation for Change of Password is activated. Is the frequency for such intimation set in the software?
- Whether the Max Inactive Time has been set for each user. (Max 2 Minutes)
- Whether the right menu option is specified for the appropriate user, for the following: (Indicate Yes / No)

    Access Level
    Passbook Printer
    Printer
    Scanner

- If the Password Retry Facility has been set appropriately. (Max 3 retries)

3.4   Data Integrity

a) DATA INPUT CONTROL

- Whether officer authorizes all voucher entries after posting of details by CTO / Office assistant
- Whether appropriate flags for application of interest rate are set for all debit and credit products (CC/OD/Term Deposits/SB. etc.
- Whether dormant accounts segregation and proper handling is done in the system. Whether dormant account is activated by authorized officer? Whether the operations in the dormant accounts are under dual control?
- Whether voucher/ journal number, scroll no. given on source document and duly signed by Officer.
- The entire stock of cheque books is fed to the system.
- Are the Menu categories in the software in accordance to the access levels defined for Users

- Scanners are kept in safe custody and access is restricted.
- Is the system recovering services charges relating to Service charges, DD / PO commission, Cheque-book charges (CC/OD), Stop Payment charges, penal charge for TOD / Excess over limit, additional 2% interest on withdrawals against clearing, Minimum balance charges, Account closure charges, Outward Return charges, Cheque Inward charges, etc.
- Has each User have Restricted rights for

  Access Types to Schemes
  Signature Image

- Confirm adequacy of reports generated at EOD (End of Day). (Indicate Yes / No)

  Final Cash Contra
  Day Book Supplementary
  Exceptional Transactions
  List of debit balances
  List of credit balances
  List of temporary overdrafts
  GL Balances

3.5   Data Processing Control

- Whether Day End activities are carried out by authorized persons. Whether a register /log maintained for the same, in case of a rotational system? Whether day-end process is being done as per laid down norms?
- Is the standing instruction programs run every day.
- The operating staff pay attention to the error messages displayed on the screen and initiates corrective action.
- Whether audit trail (modifications/ changes in master record and parameter files) report, exceptional transactions report, day book supplementary, list of TOD, Cash book, GLB, consistency check reports are generated/ checked & signed and preserved for record?
- Whether stock statement received date is updated and system supports the Bank's norms? Verify for few accounts if the date of stock statements recorded in the system is the same as that of physical receipt of the stock statement.

- Whether closing Cash tallied with cash book/ GLB
- No revenue leakage observed in the computer system either due to system or otherwise?
- Whether cash book, GL, GLB generated daily, checked, balanced and signed by BM/In-charge daily
- For a sample of frozen account entries, confirm whether entries are backed by appropriate legal documents authenticated by the Branch / Senior Manager.
- Whether birth date details are taken for all minor account holders.

a) Cheque Issuance
- Is there authorization for the Cheques assigned to a particular Savings, CC, CD, OD Account?
- Is there authorization for Cheque Book series numbers (issued by the Central Office) received by the Branch and entered into the System?
- Whether system generated stock of cheque book/ security stationery is tallying with physical stock.

b) Stop payment
- For a sample of entries, are these entries backed by physical documents (i.e. Letter Issued by the customer to the Bank), duly signed by the Senior Manager. Are these cheques restricted

c) TDS
- Are these vouchers prepared for TDS application (in the system) for an account

d) BOD/EOD Reports
- Check if exceptional reports are generated and print-outs checked & signed by official designated.
- Has the right amount of time being specified for making an A/c Dormant.

e) Cash Withdrawal and Cash Receipt
- Whether exceptions and error messages are generated for the following.   (Indicate Yes / No)
  Temporary Overdraft
  Withdrawal against effect
  Earmarking amount
  Sanction limit
  Drawing power
  Below Minimum Balance
  Borrowers limit exceeding
  Debit in credit account

Cheque related (Out of range, stop payments, already paid, encashed)

  f) Stop Payment

- Whether revocation of stop payment cheques can be done with higher level password only.

3. 6. System Effectiveness

- Purging of Data Files
- Purging activity is recorded and maintained in a register.
- Purged backup media is kept properly under safe custody. Access to purged data is restricted.
- Branch Server / Gateway PC are having sufficient work space in hard disk.
- The audit trail report generates the User ID of the operator and the official for any addition / modification / deletion of the transaction data effected in the database.

3.7. System efficiency

- Department/Office ensures the use of every computer asset to its optimum capacity.
- Department/Office takes consistency check of balances daily to aid in the detection of errors or fraud.

3.8. OTHERS

a)   Version Control

- The computer system has Authorized Version of an OS, Authorized Version of anti-virus software with its latest updates.
- Legally licensed copies of the software are used for computerized operations and the licenses are currently in force.

b)   Compliance of Previous Audit Report

- Determine if the Branch has complied with the last Information System Audit Report

c)   Registers Maintained

User ID/Password Allotment Register
Fixed Asset Register
Media register
Hardware maintenance Register
Charges/Interest application register
Day Begin/Day End Register

Stop Payment Register
Log Book for Software Vendor
Hardware Inventory Register
Computer Cabin Register

CHAPTER 4
CBS Audit Checklist ON FINACLE

To ensure that various processes in Core Banking Solution are running in proper and prudent manner in accordance with established policies and practices of the Bank, the following checklist covering mainly the functional aspects of FINACLE has been developed by the Bank. The Auditor has to identify and assess the risks to the Bank and ensure efficacy of CBS system.

CBS Audit Checklist

1. Whether the Branch is performing "End of Day" (EOD) checks before giving EOD signals and resolving all error messages displayed by the system.

2. Following System Suspense A/Cs are having NIL balances at EOD:-

    i. System Suspense A/C- DD to be issued (Dr/ CR)

    ii. System Suspense A/C- OLRR Suspense -Dr

    iii. System Suspense A/C- Trickle Feed Unposted-Dr

    iv. System Suspense A/C- Banker's Cheque to be issued-Cr

    v. System Suspense A/C Inward Clearing- Cr.

    Auditor should give details of outstanding entries in this account, if any.

3. Technical Contra A/c, Wash A/c and Migration Suspense A/c are having NIL Balance. If not, give details

4. Whether transactions of Technical Contra, Wash Account, Clearing Adjustment account and System Suspense Accounts are verified and monitored daily by BM/ Senior Officers of the Branch.

5. Branch is making payment of ISDN bills every month regularly and sends the photocopy thereof to CBS Department, Central Bank of India, so that in case of leased line failure, ISDN back up is available.

6. Branch is printing the supplementary and checking the same on Daily Basis, and tallying missing entries ,if any, with the amount in Technical Contra:

7. Physical cash at Branch is tallying with 'Cash in Hand' Balance of GLB.

8. Reconciliation of Technical Contra and Wash A/c is done on daily basis

9. Jottings (accounts) balances are tallying with respective GL Heads and report generated by system is checked and kept on record.

10. Cheque Book issued is authorized by Officer in the system.

11. Exceptional Transaction Report on EOD and Exceeds Drawing for a day is printed and checked by the Branch Manager.

12. Control Returns and MIS reports are printed and kept on record.

13. All modules in the Branch are migrated on CBS system. If not please give details of activities/ modules which are   manual.

14. Branches printing and checking the report of "Transactions By us" on Other Branches and "Transactions on Us" by other Branches".

15. Whether all staff members are given training in CBS.

16. Whether the CIFs of Joint Account holders, Nominees are properly linked to the accounts at the time of opening the Deposit accounts.

17. Whether all the accounts of one customer are linked to one/ unique CIF of the customer. No multiple CIFs exist for the same customer.

18. Whether the account type classification (SBFIN, GEN, STAFF, and Sr. Citizen Etc) is accurately done for Deposit accounts.

CHAPTER 5
Information System Audit Report and Risk Assessment Sheet

The Bank has started the "Risk Based Internal Audit (RBIA)" for all its Branches. For the IS Audit, the Bank has prepared an audit report in which the weightage has been given to each item in the report. The Auditor has to give the marks against each item. He has to place on record whether any item is at High, Medium or Low Risk in the report. The Auditor can also write comments against the item, in case he observes anything critical.

According to the Bank, classification of Branches according to the marks obtained is done as follows:

Risk Score < 40 %	=High Risk
Risk Score > 40 % < 70 %	=Medium Risk
Risk Score > 70%	=Low Risk

The IS audit report provided to the Auditors while conducting the audit of the CBS Branch is as follows: (This report is based on the audit controls defined in Chapter 2 of this document).

BRANCH:				RO:		
Sl.No	Risk Parameters	Yes/ No	Weightage	Auditors Score	Risk category H / M /L	Auditors comments
1	**Environmental Controls**					
1.1	**Server room protection & cleanness**					
	1. Whether all PCs/ printers are regularly cleaned and kept dust free.		2			
1.2	**UPS Maintenance**					
	1.Whether UPS is in working condition during Branch visit		4			
	2. Whether the computers are the only devices, which are connected to the ups		2			

	and have adequate plug points for the same.				
	3. Whether testing and maintenance of batteries for ups is done regularly. Whether report kept on record. Please mention the date of last testing? Please check the record for changes of batteries in audit period.	4			
1.3	**Electrical lines & LAN Cabling**				
	1. Whether the wiring in the Branch is concealed / under casing capping? Electrical wires and computers cables are not lying loose.	2			
	2. Whether proper earthing is done and earth to neutral voltage (ideally less than 2.5 v) is checked. (Please give the date of last test.)	2			
	3.Whether there is distance of at least one foot between Data Cable and Electrical cable.	2			
1.4	**Fire Protection**				
	1. Whether fire extinguishers are installed at strategic locations	2			
	2.Whether proper record is maintained in the Branch for refilling / servicing of the fire extinguishers	2			
	3.Whether staff is conversant with the use of fire extinguishers	2			

2	**Physical & Logical Controls**					
2.1	**Physical Controls**					
	1.Whether Floppy Disk Drivers / Pen drives / CD on nodes are restricted to authorized terminals.		4			
	2.Are the PCs /Printers Scanners marked or numbered as fixed assets		2			
2.2	**Logical controls**					
	1.Is there a unique login ID (User ID) for starting PCs		2			
	2. Whether Access levels are allocated to the employees as per employee grade and responsibilities.(user work class)		2			
	3.Whether there is active usage of transferred / suspended /disable/ extra user IDs		4			
	4.Whether the user IDs of staff are suspended when they go on leave.		4			
	5.Whether the users log out when leaving the work table / node each time.		2			
	6.Whether secrecy of password is being maintained. Users do not write their password on wall, desk, diary etc, and are aware of the need for the secrecy of their password.		6			
	7.Whether review of allotment / cancellation of user IDs and access level is being done by Branch Manager		4			

	regularly and recorded in the register.					
3	**Maintenance & Business Continuity**					
	1. No obsolete hardware is lying in Branch and the same is disposed off as per HO guidelines.	2			
	2. Whether old data of legacy system is preserved properly.	4			
4	**System & Networking Controls**					
	1. Netwotk equipment like Router / Switch / Modem are placed in the least accessible area in a mounted rack under lock & key.	4			
	2.Internet access is not given to PC/s connected to LAN	4			
5	**Operational Controls**					
	1. Scanners are kept in safe custody and access is restricted.	4			
	2.The signatures are being updated / verified in the system on daily basis	4			
	3. There are no unlicensed software installed on the PC.	2			
6	**Branch Operational Controls**					
	1.Whether the telephone numbers of Helpdesk / CBS department. / Software / Hardware /vendors and UPS vendors are displayed in the Branch premises and a copy is maintained with the BM.	4			

	2. Branch is performing "End of Day" (EOD) checks before giving EOD signals and resolving all error message displayed by the system.	4			
	3. Whether all modules in the Branch are migrated on CBS system. If not please give details of activities / Modules are manual.	2			
	4.Whether all staff members are given updated training in CBS.	2			
7	**Registers maintained at Branch level**				
	User ID maintenance register	2			
	Link downtime register	2			
	Media register	1			
	Hardware / Software maintenance register	2			
	Day begin /Day end register	2			
	Hardware Inventory register	1			
	Total Risk Score	**100**			

Class room Work

Discuss the following:

- Assess the audit issues in the Bank (Chapter 1).

- Assess the audit controls for IS Assets (Chapter 3) and suggest the amendments if any are required in IS Audit Report and Risk Assessment Sheet (Chapter 5) .

- Assess the Resource Requirements (Hardware, Software Tools etc) and capacity building requirements for auditing functional aspects of Finacle (chapter 4) and auditing data/reports of a Branch.

- Assess authentic sources for collecting information for IS Audit (Chapter 2) and issues therein.

- Sustainability and relevance of present form of the IS Audit from (Bank's point of view), when Bank decides to audit multiple Banking channels and audit DC/DRC sites in future.

Trainer's Note

The case is based on the initiatives taken by the Uttar Bihar Gamin Bank for auditing of CBS Branches in the Bank. The information was collected in from the Bank in the month of April 2014.

The discussion may be generated on the following topics:

- Assess the audit issues in the Bank (Chapter 1).

- Assess the audit controls for IS Assets (Chapter 3) and suggest the amendments if any are required in IS Audit Report and Risk Assessment Sheet (Chapter 5) .

- Assess the Resource Requirements (Hardware, Software Tools) and capacity building requirements for auditing the functional aspects of Finacle (chapter 4) and auditing the data/reports of a Branch.

- Assess the authentic sources for collecting the information for IS audit (Chapter 2) and issues therein.

- Sustainability and relevance of present form of the IS Audit from Bank's point of views, when Bank decides to audit multiple Banking channels and audit DC/DRC sites in future.

> The discussion may be done in groups or can be facilitated by the faculty in the class. Each group may be given 30 to 45 minutes to read the case. Flip charts or the meta-plan cards can be given to the participants for abridging their findings and to present their view/s.
>
> Time: 3 sessions (270 minutes)

Acknowledgements