Audit in Banking Sector
(Chapter - 6 : DISSA Course)

Arijit Chakraborty

August 07, 2021

Coverage

- CBS definition, implementation
- CBS Controls
- CBS Architecture
- DC Topology – types of servers,network
- IT Ops in CBS
- Security & Internal controls – CBS
- CBS IS Audit Process review
- CBS IS Audit scope – detailed discussion

Review

- Centralised Online Real time Electronic (CORE)
- Banking products
- RBI – Health code 1 to 8
- TBA = 1990
- CBS – 2000- full connectivity with DC

- CORE - Centralised Online Real-Time Electronic Banking
- All the bank's branches access applications from centralised DC
- Enhancing customer convenience = Anywhere & Anytime Banking
- Efficiency, Productivity and Convenience

CBS Definition

- Gartner defines = CBS *" as a back-end system which processes daily banking transactions, and posts updates to accounts and other financial records.*
- *CBS typically include deposit, loan and credit-processing capabilities, with interfaces to general ledger systems and reporting tools.*
- *Core banking applications are often one of the largest single expense for banks and legacy software are a major issue in terms of allocating resources.*
- *Spending on these systems is based on a combination of service-oriented architecture and supporting technologies."*
- Many banks implement custom applications for core banking

CBS implementation

- CBS = capable of being implemented in stages.
- **Initially** = basic modules : Savings Account, Current Account, Fixed Deposits, Bills & Remittances, Loans and advances models implemented.
- **Subsequently=** alternate delivery channels : ATM,
- Internet banking, RTGS/ NEFT, Mobile Banking, Treasury, Government Business etc., added.
- The customer is no longer a customer of the branch but **a customer of the bank**

CBS

- **CBS handles**
- • Recording of transactions,
- • Passbook maintenance,
- • Interest calculations on loans and deposits,
- • Customer records,
- • Balance of payments and
- • Withdrawal
- software = installed at different branches of bank &
- interconnected by means of communication lines

Softwares used by Banking Industry

- Base Software: Core Banking Software

- Add-on Softwares for,
  - Credit Risk Calculation as per Basel – II Norms
  - Risk Weighted Assets / Capital Adequacy Computation
  - Asset Classification and NPA Provisioning computation
  - Classification of Priority / Non-priority / Sensitive Sector Advances
- Sectorwise Asset Classification
- Credit Risk Calculation
- Risk Weighted Assets / Capital Adequacy Calculation

CBS Finacle

- • Bank of Baroda
- • Bank of India
- • Union Bank of India
- • Canara Bank
- • Federal Bank
- • IDBI Bank
- • ICICI Bank
- • Axis Bank
- • ABN Amro
- • Vijaya Bank
- • UCO Bank

CBS Requirement

- To meet dynamically changing market & customer needs.
- To improve & simplify banking processes = bank staff can focus on sales & marketing
- Convenience to customer as well as bank.
- To Speed up banking transactions.
- To expand presence in rural & remote areas.
- *Basic Elements of CBS that helps Customers :*

1. Internet Banking.
2. Mobile Banking.
3. ATM.
4. Fund Transfers – NEFT, RTGS.

RTGS, IMPS, NEFT

- ***Real Time Gross Settlement (RTGS)***
- continuous (real-time) settlement of funds transfers individually on an order-by-order basis (without netting).
- Funds settlement takes place in books of RBI , payments : final & irrevocable.
- RTGS = available for customer & inter-bank transactions round the clock,
- except for interval between 'endof-day' and 'start-of-day' processes.
- ***IMPS***
- IMPS = Immediate Payment Service
- Money transfer mechanism made available by RBI & National Payments Corporation of India (NPCI).
- Initiated in 2010 by NPCI
- Feature of IMPS = available at all times for usage.
- Transfers funds instantly & great banking platform in case of emergencies

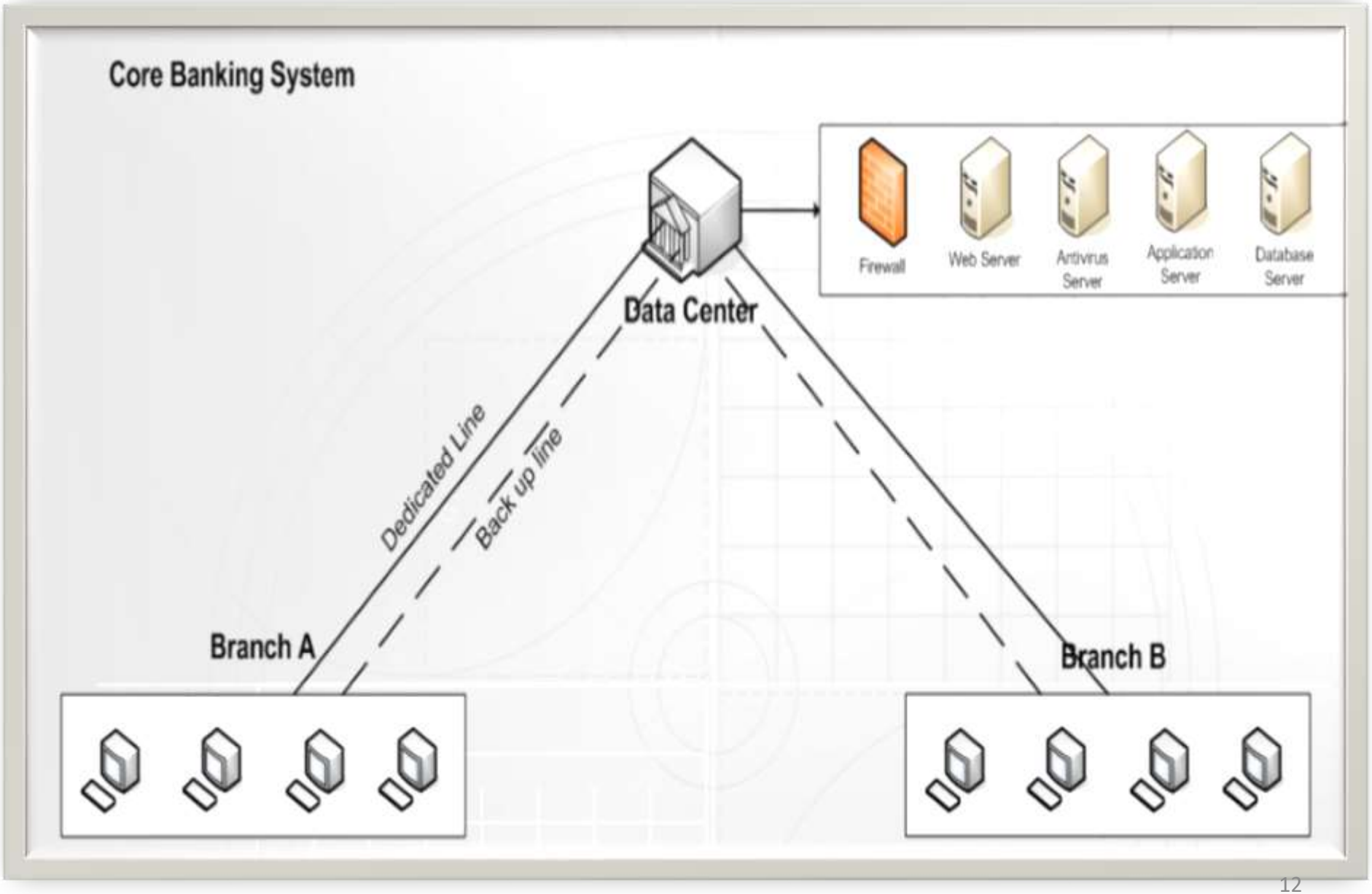
NEFT

- nation-wide payment system facilitating one-to-one funds transfer. individuals, firms & corporate can electronically transfer funds from any bank branch to any individual, firm or corporate having an account with any other bank branch in the country
- **IFSC or Indian Financial System Code** = alpha-numeric code that uniquely identifies a bank-branch participating in NEFT system.
- **11-digit code** = first 4 alpha characters representing bank,
- **last 6 characters** = representing branch. 5th character is 0 (zero).

Difference between NEFT & RTGS

	NEFT	RTGS
Suitable For	Small Transfers	Large Transfers
Settled In	Batches(Deferred Net Settlement Basis)	Continuous(Gross Settlement)
Minimum Transfer	No minimum limit	Rs. 2 lakh
Maximum Transfer	No Limit	No Limit
Transfer	After a cut-off time	At the time funds are received

CBS Architecture



Branch interface

- Application server hosts core banking application like Finacle, Flexcube, Quartz or Bankmate etc.
- Central server = powerful and robust system as it has to **perform all the core banking** operations.
- Branch does not have entire application.
- Branches have = only a version -called "client version" of application.
- Client version of application = capable of **only** entering data at the end point ,i.e branches.

Components of CBS

- ***Centralized Data Centre –***
- large data housing infrastructure = provides high bandwidth access to its clients & includes many services, Networking devices, Firewalls & related equipment.
- ***Network & Communication***
- ***Core Application Systems***
- ***Other Infrastructures***
- ***Networking Devices-*** Routers, Firewall, Switches
- ***Databases***
- ***Servers-*** Application servers, Data Base Servers, Web server, Mail server, Report Generating Servers etc.

Components of CBS – Data Centre

- Infrastructure
- Environment – Temperature, rodent & Fire control
- Structured Cabling
- Network operation centre
- Server Racks
- Logical Access Control
- Physical Access Control

Components of CBS- Network

- Local Area Network
- Firewall
- Networking Devices
  - Routers
  - Hubs
  - Switches
  - IDS
  - IPS

Components of CBS – types of Servers

1. ***Application Servers*** - hosts core banking application
2. ***Database Servers-*** Entire data of the bank - Master data
3. ***ATM Server-***ATM account holder details – ATM Switch
4. ***Internet Banking Database Server-*** stores username & password of all internet banking customers – located in DMZ
5. ***Internet Banking Application Database Server-*** Processes internet banking service requests
6. ***Web server***
7. ***Anti-virus/ Anti-malware server-*** All servers updated with latest anti-virus
8. ***Proxy Server***- Type of Firewall = provides Network Security & prevents malicious entry into network – located in DMZ
9. ***Mail/ Exchange Server***

Internet Banking = IBDS+ IBAS+ Central Db server+ Web server + Middleware

1. Security Administrators

1. Have to follow security policy approved at Board level.
2. Understand policies & procedures mentioned in security policy.
3. Assesses risks for non compliance.
4. Decides access rules for data & IT resources.
5. Should not have any access to transaction level data.
6. User creation, User deletion
7. Locating a branch code & providing connectivity to the branch
8. Defining interest rates for deposit loans & other products.
9. Responsible for processing of EOD & BOD operations.
10. Responsible for introducing latest application of CBS application program.

2.Data Base Administration

- Custodian of Bank's databases
- Responsible for management of data
- Database access control
- To ensure :
  - Data integrity
  - Availability
  - Security
  - Recoverability

3. Network Administrator

- Placement of devices – router, bridge, switch, hub etc.
- Securing devices – strong access control
- Configuration of firewall, other devices (IPS & IDS)
- Arrange to conduct VAPT
- **4. Librarian**
- Maintain detailed documentation of all receipts & issues of software.
- Keep a record of all licenses obtained for usage of software.
- Be in charge of user manual & system manual.

Functions of IT Department in CBS

- **Change Management**
  1. Requirement of changes on regular basis
  2. Change in business processes, hardware, software, communication systems
  3. Upgradation of technology
  4. Error/ bugs in the program
  5. Implementation of new functionality
  6. Well documented process, approval then scheduling
  7. Updated documentation

Operations of CBS Branch

1. All branches = directly connected to Data Centre
2. All transactions are happening at servers in Data Centre
3. No separate applications are available at branches
4. Branch users = created through centralized user creation process
5. No password/ID should be shared with anyone at any circumstances
6. All control parameters are created/ maintained centrally
7. Some limited application related controls = controlled at Branch Level.

Operations of CBS Branch

- **Access Control Procedures**
  1. System prompt for change of password for first log in.
  2. There should be a maximum number (usually 3) of failed log in attempts.
  3. Procedure for reviving deactivated accounts
  4. All USB ports, CD Rom drives should all be disabled.

- **Server related procedures**
  1. No DB/Web / App servers available at branch.
  2. Local server to address slow connectivity issues - temporary storage.
  3. Password of local server - under control of Branch Manager.

Operations of CBS Branch

- **Physical and environmental controls**
  1. Moisture & temperature control
  2. No inflammable material in server room.
  3. There should be a fire extinguisher in server room.

- **Network related procedures**
  1. Network devices should be secured
  2. Unused routers, switches & hubs should be protected to avoid misuse & unauthorized use.
  3. All network cables = protected properly.

Operations of CBS Branch

- **ATMs being attached to Branches**
  - ATM cards be secured with lock & key.
  - Regular reconciliation procedures for stock of ATM cards.
  - Updating of CBS with details of cards issued
  - ATM cards kept securely.
  - Procedures for loading cash, recording & reconciliation of cash.
  - Master key of ATM under dual control.
  - ATM journal rolls - reconciliation purposes & for detecting any unauthorized transaction
  - Procedures for dealing with swallowed card.
  - Procedures for dealing with cash which is in reject bin.
  - **Control = Surrendered & Captured Cards**
  - **Check** – SOP : replacement for cards

Operations of CBS Branch

- **Business Continuity Planning & Disaster Recovery Planning**
  - Properly Documented Disaster Recovery procedures + Business Continuity Planning.
  - Aware employees with course action for BCP & DRP .
  - **Periodic drills** - proactive control.
  - Well documented alternate connectivity with DC in case of break down in primary connectivity.

Security & Controls - Data Centre & Branches

- Various aspects of evaluation of security & controls of a branch in CBS environment are,
  - Information Security Policy
  - Access Control Procedures
  - Procedures connected with branch servers
  - Physical and environmental control for servers
  - Network & Communication control
  - Limited verification of applications
  - Operations connected with ATM/ Internet Banking
  - Business Continuity Plan
  - Change control procedures

Types of Security & Controls in CBS

1. Management Controls

- **Formulating a security policy** :
  - Formation of Security Committee/ Steering Committee
  - Asset Management
  - Human Resources Management
  - Physical and Environmental security
  - Communication & operative management
  - Access Control
  - Systems development and Change Management Procedure
- **Developing a business continuity planning**:
- RBI mandates BCP for every bank.
- **Laying down procedures for systems development** : Procedures include program development, program testing, movement to library, movement from library to production, roles & responsibilities of Computer Team members , highlighting incompatible functions.

Security & Controls in CBS

2. Organizational Controls

- Organization structure of IT Department
- IT Strategies roles and responsibilities
- Incompatible functions

3. Operational Controls

- Physical access
- Logical access
- Environmental controls
- Evaluation controls in operation systems
- Evaluation controls of network

Security & Controls in CBS

4. Application Controls – Input, Processing, Output

- ***Input*** **:** ensure data entered = complete & correct through built in checks,
  - Data validation
  - Reasonableness check
  - Format check (Mandatory files)
  - Range check

Application modules

- *Customer ID generation*
- *Accounts Management* -
- *Savings Bank & Current Accounts*
- *Fixed Deposits, Recurring Deposits and other Term Deposits.*
- *Cash Operations Module*
- *Clearing Module* - inward clearing and outward clearing
- *Bank Guarantee* , Performance guarantee
- *Letter of Credit*
- *Bills*
- *Remittances*

Application modules- functionality

- ***Master Maintenance - Parameter Setting***
  - *Operational Parameters:* Parameter setting for account type and structure settings
  - *Interest Related Parameters:* Parameter settings for interest rates applicable. vary for different parties e.g., staff, senior citizens & also for tenure of deposits.
  - *Charges Parameters:* SI charge, Stop Payment instruction charge, cheque book issues, account closing charges.
  - *User Related Password Change Parameters:* validity, password history, length, structure etc.
  - *Authorization Parameters :* Authorization of users varies for exceptional transactions.

IS Audit : Scope in CBS Branches

- *all Information Systems (IS) assets, viz.,*
- *hardware, systems software, applications software,*
- *communication systems, facilities, people (knowledge / skills), data, system documentations and supplies etc.,*
- *whether acquired / developed and / or maintained in-house or by outsourced vendors*
- *related interfaces and manual processes.*
- *Insider threats, cybersecurity threats*

Process review by IS Auditor

- Account opening
- KYC, Nominee
- Verification of interest
- Product selection
- Advance classification, NPA
- Security / Mortgage register
- ATM operation
- Internet Banking M-Banking Ops
- Credit SOP = Sanction letter /Renewal letter
- TDS enabled , 15G / 15 H
- Error reports
- Exception reports
- ATR
- Statutory compliance- SOP & Report

Branch Documentation

- Whether following manual/registers are properly maintained=

✓ Parameter Change Register

✓ User-ID register

✓ Complaint Book

✓ Day begin and Day End register

✓ Cheque Book issue Register

✓ Daily movement register for DD/FDR/BC etc.

- Is there any unauthorised User-Id in system generated User list?
- Whether backups are kept both on-site & off-site- Back-up register

Parameter check for Bank charges

- Whether the parameters for various service charges correctly set? (As per circularised instructions from time to time)

- ❑ DD
- ❑ Collection charges in outstation cheques
- ❑ Banker's Cheque / Pay Order
- ❑ EFT in applicable branches
- ❑ Penal Charges for fall in minimum balance
- ❑ Cheque Book Charges for SB/CC/OD a/cs
- ❑ Closure of SB a/cs
- ❑ Handling charges - Cheque return
- ❑ Stop Payment instructions
- ❑ Handling / I/C for inoperative/Dormant SB a/cs
- ❑ Issue of cheque books

CBS Generated daily reports

- Whether the following daily reports are generated from CBS

1. Active users list during the day
2. DD / Pay Order/ Bankers Cheque issued / paid (number wise)
3. Number wise Term Deposit Receipt issued
4. Bills lodged & realised, Bill type wise & Bills returned
5. Cheque return register
6. Cheque book issue/cancelled.
7. Stop Payment Instructions issued/cancelled
8. Standing Instructions executed/not executed/ entered/ deleted
9. Balance of Cash Credit / Overdraft a/c
10. Temporary Overdraft Report
11. If LOCKER module is implemented, list of a/cs operated in a day

CBS Generated Monthly reports

- Module wise balance sheet
- Charges statement
- Outstanding bills, cheques sent for Collection
- List of interest charged in CC/OD/TL
- Loan repayment notices to defaulting borrowers & guarantors
- If LOCKER module = List of a/cs with rental due
- If LOCKER module = Letter of reminder to customers with rent overdues

IS Audit Scope

- Scope of **IS Audit of Bank** based on:

✓ Bank's IT Policy & Standards,

✓ IT Procedure and Guidelines,

✓ IS Policy & Standards,

✓ IS Procedure and Guidelines,

✓ Cyber Security Policy & Standards,

✓ Cyber Crisis Management Plan.

Details of IT Departments, No. of Applications and No. of vendors

1. Core Banking – Technical Operations (CB-Tech Ops)
2. Data Centre and Cloud Services (DC & CS)
3. Enterprise Integration Services (EIS)
4. Internet Banking (INB)
5. IT ATM
6. IT Trade Finance
7. IT Networking & Communications
8. Mobile Banking
9. Payment Systems
10. Security Operations Centre
11. System & Application Audit of Bank's UPI as per NPCI guidelines

Indicative list of Domains:

- A. Information Security
- B. Recruitment & Training
- C. Logical Security
- D. Network Security
- E. Change Management
- F. Backup & Restoration Management
- G. Physical Security
- H. Environmental Controls
- I. Security Operations Centre

Thank You