WELCOME

CA M.R. (Abhay) Mate

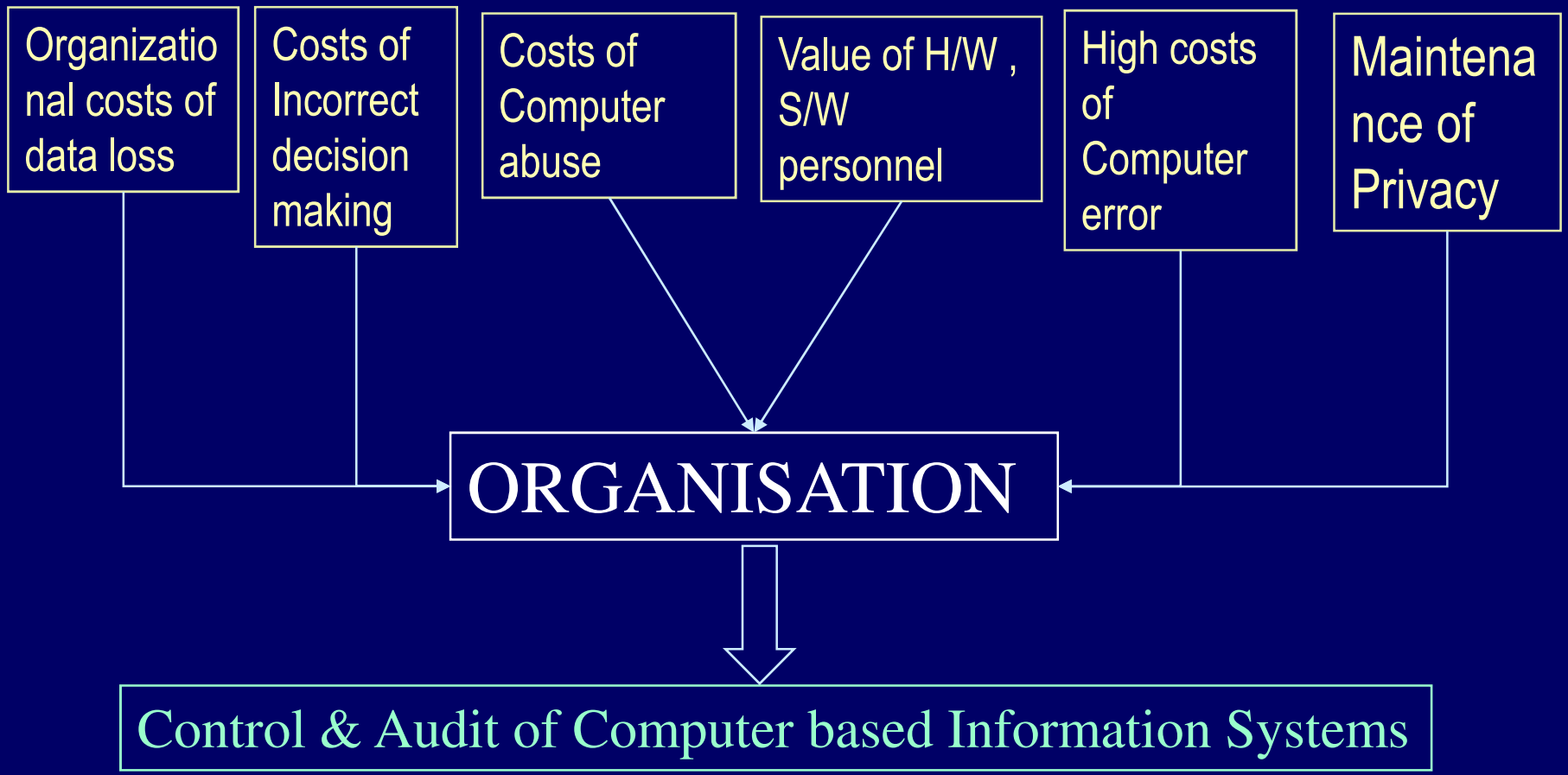
STEP BY STEP APPROACH TOWARDS INFORMATION SYSTEMS(IS)AUDIT

Presentation by
CA Madhav(Abhay) Mate (B.Com, F.C.A. DISA)

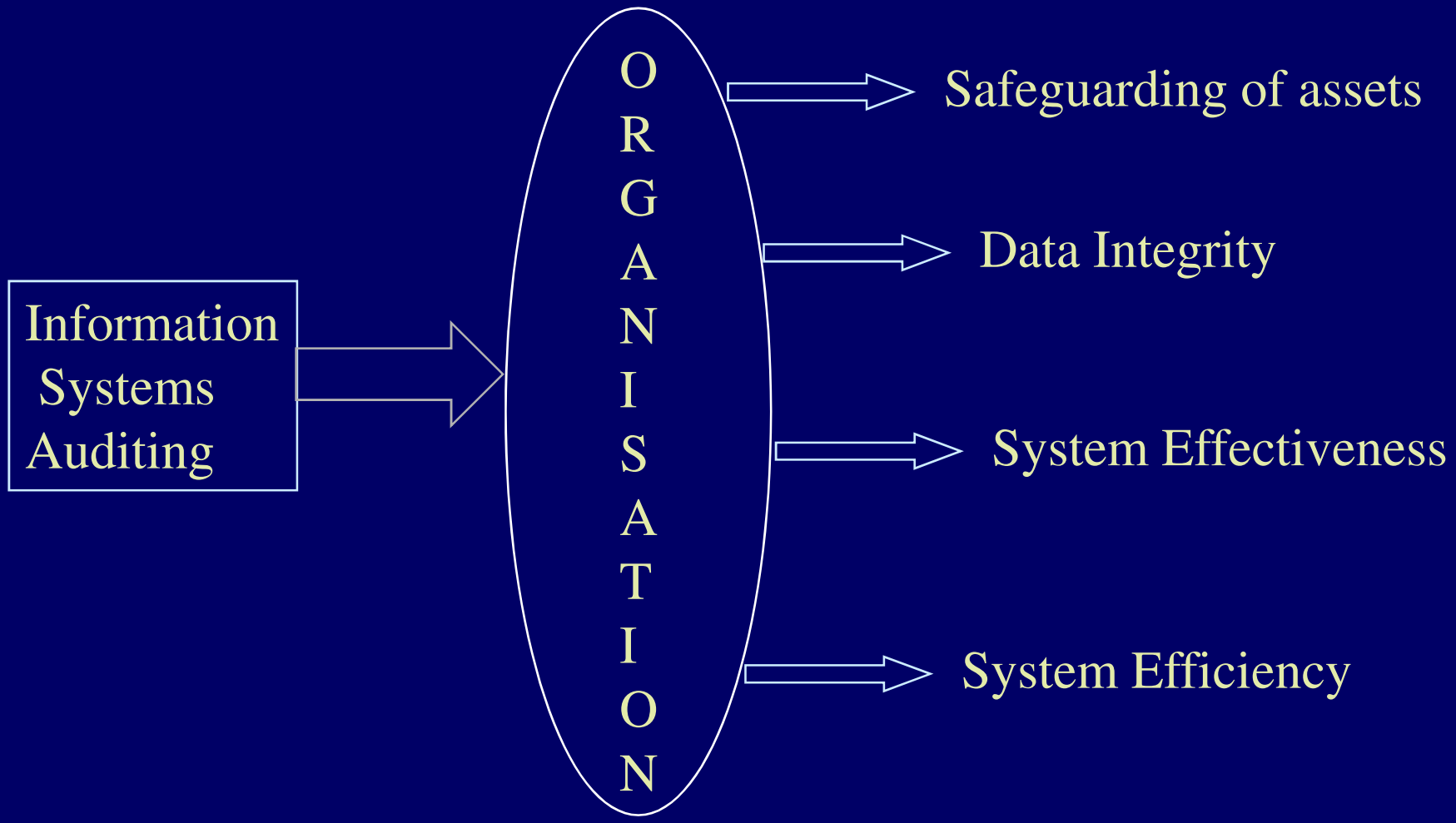
What is an Information Systems Audit ?

IS audit focuses on the computer-based aspects of an organization's information system.This includes assessing proper implementation,operation & control of computer resources.

Need for Information Systems Auditing



Objectives of Information Systems Audit



Scope of IS Audit

- All computerized departments
- Collection & evaluation of information /evidence to determine whether Information Systems fulfill objectives.
- Process for planning & organization of IS activity
- Process for monitoring of IS activity
- Management of IS staff
- Our main focus in this session –

-- ISA for Bank Branch

Benefits of IS Audit

- IS Audit acts like a preventive tool for identification of risks
- Regular conduct of IS audit would deter people/employees/users from indulging in manipulation of data,fraud etc
- Security features & controls in a computerized Information System could be assessed & improved
- IS audit can verify whether there exists appropriate security infrastructure in the organization for safeguarding the Information Systems
- IS audit assesses the health of Information Systems in an organization
- Adherence to various Government laws,statutes,circulars.

R.B.I.Directives

•R.B.I. has issued a circular no.POT/P.C.B.30/09/.96.00/2001-02 dt.12.2.2002 to all Primary(Urban)Co-operative banks .Its main points are:

•Circular is applicable to all urban co-operative banks which have fully/partially computerized their operations

• R.B.I.has decided to introduce EDP audit on perpetual basis

A) Branch Level Implementation Audit

- Environmental Aspects
- Organizational Facts
- Personnel And Training Matters
- Systems Security Characteristics
- Configuration Management
- Branch Parameter Verification & Controls
- Disaster Management / Continuity Of Operations

- Checking Methods Of Branch
- Data Consistency Checks
- Controls over Income Seepage
- Physical Access
- Logical Access
- Connectivity Issues
- ATM operations
- Availability & Adherence of IT Procedural Guidelines
- Aspects Pertaining To Central Office

B Banking / Functional Aspects

- Varity of Account Types
- Varity of Transaction
- Clearing
- Remittance
- Bills
- Non-Fund based Business
- Day-Begin & Day -End
- Interest Application
- Balance Books
- TDS
- NPA

C System Aspects

- User Access Privileges
- Software Package : Installation / Deinstallation
- Data : Backup,Restore,Other files like Print-Files, Floppy Files
- Hand-shake with Older Versions / Other Systems
- Networking Issues, Encryption , if used
- Error Handling
- One Time Data Entry Module

D Security Aspects

- Segregation of Maker & Checker Roles
- Control over Parameter
- Transaction Modification / Reversal
- Abrupt Stoppage : Recovery & Consistency
- Check-sum
- User Access Privileges
- File Access Privileges
- Day-Seal
- Audit Trails and related reports

ENVIRONMENTAL ASPECTS

- cleanliness of the Computer Installation / Room
- boards/signs suggesting Removal of Shoes, No smoking, Avoidance of Drinking and Eating etc. near or around computers
- air-conditioning provided
- electrification as per specifications, earthing
- server room located above the ground level
- premises free from any danger of water seepage near the computers
- UPS placed at proper location, UPS fully discharged at least once in a month
- Heat Detectors fitted in the installation

Organizational Facts

- Key personnel
- Hierarchy

Personnel And Training Matters

- proper training (on the system as well as application) given to the staff
- By the organisation / By hardware vendor / By software vendor
- - Operators
- - Officers
- formally designated officer to look after computer operations (system administrator/ DBA)

Systems Security Characteristics

- Logical access to computer restricted
- Physical access to console/server restricted
- locks available for Server room
- server / PCs / Terminals having virus protection mechanisms
- log available for unsuccessful login attempts
- passwords changed periodically, secrecy of passwords maintained
- record of user Management – Add / Change / delete / disable / enable
- users logging out every time they leave the terminal
- Auto log of all the users logged in on a particular day
- purged data stored on any standalone PC

Configuration Management

- Asset Register & S/W register containing details of all the computers and peripherals be maintained
- AMCs of hardware are active and continually renewed
- insurance cover
- vendor's user manuals, Bank's user manuals, IT Department guidelines and other documentation exist in the branch & referred to

Branch Parameter Verification & Controls

- Access to Parameters restricted, responsibility assigned to update the critical parameter values,
- Are parameters set properly? All parameter changes supported by proper documents / parameter change log
- Guidelines from HO about original parameter setting & parameter maintenance, Parameter record
- Record of interest rates maintained?
- Are the interest rates required to be given for each account?
- If yes, how the same are verified and controlled?

Disaster Management / Continuity Of Operations

- back up of data taken daily at the end of the day
- off-site back up preserved & away from original data
- back up of latest version of application software also to be maintained properly
- Are back-up media write protected? Is Backup taken before any maintenance activity (Hardware or Software) takes place? Is back-up media tested periodically?
- back-up media -keep securely away from electromagnetic devices
- How many generations of back-ups are maintained?
- hardware and software problems register-record of preventive and corrective maintenance
- location map available with equipment details
- contingency plan - tested at predefined frequency
- staff familiar with the procedure to be followed in case of disaster

CHECKING METHODS OF BRANCH EMPLOYEES AND REPORTS VERIFICATION

- Transaction list Supplementary, Cash Book & Journal
- Exception Statement / Officer override report
- Debit balances in savings / current accounts
- Report of cheque books issued CC / OD against clearing & overdrawn accounts statement
- S I (Standing Instructions) Register
- Does every operator put a) rubber stamp b) transaction number generated by the system & c) initials on all vouchers under his / her name on all vouchers?
- procedures to ensure that all the vouchers have been processed in the system
- Are compulsory reports defined by the Bank? Are the persons responsible for checking the reports independent of the persons responsible for data entry?
- modifications made in back office information checked
- all non-financial transactions checked
- care if any operator is working beyond working hours / on holidays

Data Consistency Checks

Consistency of daily transactions with G.L:

- Account Head Date 1:Bal. As per G.L. Debit transactions as on As per Day Book Credit transactions as on As per Day Book Date 2:Bal. As per G.L.

Consistency of Account balance with G.L:

- Balances of accounts from the account balance list should tally with GL figures so as to find an assurance of correctness of closing balances. Test on balances reveals that the data is consistent/not consistent.

Head of account Master balance as per balance report as on GL Balance as on Remark

Controls over Income Seepage

- Checks for accuracy of Interest calculation:
- Type of A/C A/C Numbers Int. Period Products Correct Y/N Int. Amount Correct Y/N
- Checks for bank charges

<u>Connectivity Issues</u>

- Internet connection available in the installation?
- Who uses the same? For What purpose? Is Internet PC stand-alone? What are the controls over its use?
- Are there any guidelines from HO for its use?

ATM operations

ATM On Site/ Offsite/ On Line / Off Line?

Guidelines received from Head Office about

- ATM Operations
- ATM Security Aspects
- ATM Card Maintenance
- ATM Card Pinning Process
- ATM registers to be maintained
- ATM Report Generation, Authentication

LFAR - as guidance for minimum reporting areas

In respect of computerized branches :

- Whether hard copies of accounts are printed regularly?
- Indicate the extent of computerization and the areas of operation covered.
- Are the access and data security measures and other internal controls adequate?
- Whether regular back-ups of accounts and off-side storage are maintained as per the guidelines of the controlling authorities of the Bank?
- Whether adequate contingency and disaster recovery plans are in place for loss / encryption of data ?
- Do you have any suggestions for the improvement in the system with regard to computerised operations of the branch?

Any Questions? ? ?

THANK YOU