# CBS – Security, Controls and IS Audit

**V. Rajendran**

**Advocate and Cyber Law Consultant**

**URL: venkrajen.in**

**venkrajen@yahoo.com, rajcyberlaw@gmail.com**

**+91-44-22473849;  +91-9444073849**

# Security in CBS

- Criticality of security in CBS
- Information Security and controls
- Meaning and need for controls
- Controls – centralised and decentralised
- Evaluation of controls in TBA
- Enhanced controls especially for CBS
- Review of controls in CBS

# Controls in CBS

- Information Security Policy
  - What an ISS Policy should contain
  - Roles and responsibility of CISO
  - Factors affecting an ISS Policy
  - Effectiveness and efficiency of the Policy
  - Implementation aspects
- Review of Information Security Policy

# Access Control

- Access Control – Access Privileges
- Physical Access Control and Logical
- Procedures related to Access Control
- Password Management – Guidelines
- User Management – Best Practices
- Network Access Management
  - Logical Access, Network Access, Internet etc
  - Setting the various policies forming part of it

# Password Management

- Meaning of password policy
- Always included in the ISS Policy
- Conformance to the corporate security policy
- Depends upon factors like
  - the criticality of the application
  - User level awareness
  - Knowledge of the user
  - Nature of data handled
  - User requirements  etc

# Other Security features

- Management Controls
- Organisation Controls
- Operational Controls
- Application Controls
  - Validations: Front-end, Back-end, Network layer
  - Hardware and infrastructure controls’
  - Output controls
  - Process controls

# Audit of CBS

- Why audit of CBS is distinct from TBA ?
- Knowledge of the software and the CBS package
- Knowledge of the database – applications etc
- System related process
  - Banking domain
  - Audit function
  - The particular corporate policy

# I.S. Security Policy

- Formation of ISS Committee
- Asset Management – Information Asset
- HR Management
- Physical and Environmental Security
- Communications and Network Access
- Access Control
- Change Management Procedures
- Review of ISS Policy: Adequacy and Compliance

# I.S. Security Policy – BCP - DR

- Meaning and need for a BCP
- BCP for the Data Centre and for branches
- Administrative functions
- Internet Banking
- ATM and other electronic services
- Disaster scenarios and analysis in the BCP
- Review of the BCP – Adequacy and compliance
- Preparedness to face the threat
- Review of ISS Policy: Adequacy and Compliance

# Change Management and related issues

- Version Control and its significance
- Version control in software
  - Procured software, developed applications
- Change Management – Documentation
- Effectiveness of change management – Evaluate
- Testing and application
  - Testing environment
  - Testing cases, scenarios, samples etc

# Audit: Meaning and Significance

- Audit and Accounts
- Meaning of audit
- Verification of accounts
    - What, why, when, how and by whom
- Independence of audit –Segregation of audit functions
- Audit and Inspection
- Audit and Vigilance
- Audit and Evidence

# Information Systems Audit

- A review of the controls within an organisation's IT infra-structure;
- Process of collecting and evaluating evidence of an organisation's I.S. practices and operations;
- Evaluating

  -IS Security, data integrity

  - operational effectively and efficiently

  - right path to achieve the organisation's goals
- Top Management's commitment and understanding
- Earlier called 'EDP Audit'

# Systems Audit

- Data and Information
- Information Assets
- Ownership of Information Assets
    - Owner, Custodian and User
- Features of Information Security

    -Confidentiality, Integrity and Availability, Non – repudiation
- Access Control

    -Physical Access Control and Logical Access Control

    - Access privileges, Authentication, Authorisation

# Features of Systems Audit

- Understand and evaluate the computer systems
- Identify all the components – complete infra-structure
- Identify all the sub-systems based upon:

  Management Sub-systems: Top Management, Programming, Data Management, Security Administration and Systems Admin

  Application Sub-systems: Transaction processing, data processing, Input and Output, Communication, Processing of data etc.
- Various controls in the organisation:

  Hardware, Software, People and Processes

  Input Control, Access Control, Output control, Processing Controls
- Adequacy of controls and their effectiveness and efficiency

# Need for Systems Audit

- Computer penetration and wide acceptance, prevalence
- Technology products especially in banks
- High risk in handling computer data
- Undefined areas (owner of data, custodians and users)
- Reach and use of various software (programs and data)
- Computers as MIS and DSS in organisations
- Computer frauds
  - Innocent victims and lack of knowledge
  - Information theft and ID theft
  - Password Policy and Maintenance
  - User Awareness and Management Commitment
- Data handling at various levels

# Controls in the Information Systems

Control is a pattern of activities to ensure reliability of the components by preventing, detecting and correcting errors or irregularities.

- Components of controls:

  Authenticity – identify the objects (users, programs etc) correctly

  Accuracy – System should process correctly and give accurate data

  completeness – Protect against missing data or incomplete processing

  redundancy – in data, protect against wrong and second data entry

  Audit Trail - Keep logs of all activities

  Assets Safeguarding

  Efficiency and effectiveness in achievement of system's goals

  Understand and evaluate the computer system in the organisation

# Security and Controls

- Management Controls mainly involves the drafting, implementation and review of IS Security Policy
- Essentials of IS Security Policy
  - Contents of IS Security Policy
  - ISS Architecture – Committee etc
  - IT Asset Management
  - Access controls – Physical and Logical
  - Various policies forming part of it like
    - Email Policy, BC-DRP, Internet Access, Password , Network etc
- Controls like Input, process and Output

# CBS and IS Audit

- Process involved in the audit of CBS includes mainly the review of IS Security Policy and
  - BC DR Review
  - Network Assessment – VAPT
  - Controls of all kinds: input, database, O/s, Process
  - Review of all logs: Systems, DB, appn logs
  - Adequacy of the contents of the policy and compliance issues
  - Effectiveness and efficiency of controls

# Questions ???

Points for discussion:

CBS – It is advantageous to bank staff or customers or to the regulator?

Data Security: Is it compromised in CBS as compared to TBA?

How do you implement physical control measures in ATM?

How do you enforce logical access control in CBS database?

What are the HR issues while migrating from TBA to CBS in a major bank?

What are the security concerns in credit card transactions?