Audit in CBS platform (Banking Sector)

(Module - 6 : DISSA Course) **Part 2**

Arijit Chakraborty

April 03, 2022

CBS system controls in bank branches

- Access to the system is available only between stipulated hours and specified days only.
- Individual users can access only specified directories and files
- Exception situations such as limit excess, reactivating dormant accounts, etc. can be handled only with a valid supervisory level password.
- A user timeout is prescribed
- Once the end-of-the-day process is over, the ledgers cannot be opened without a supervisory level password.
- The system maintains a record of all log-ins and log-outs
- If the transaction is sought to be posted to a dormant (or inoperative) account, processing is halted and can be proceeded with only with a supervisory password
- The system checks whether the amount to be withdrawn is within the drawing power.

System Audit of CBS

- ***RBI = IS Audit is the process of evaluating the adequacy of controls and also ensuring relevant application modules deal comprehensively with business process***.
    1) *Review of Security Policy*
    2) *Review of Business Continuity Planning & BCP policy*
    3) *Review of Systems Development and Change Management Procedures & process*
    4) *Network vulnerability Assessment of Effectiveness of Intrusion Detection Systems.*
    5) *Evaluation of controls in operating systems.*
    6) *Control in databases*
    7) *Testing of application modules of the Core Banking Solution.*
    8) *Review of Systems logs.*
    9) *Audit of Internet Banking, ATM and RTGS/ NEFT*

OWASP Top 10

- OWASP (Open Web Application Security Project) is an open source project.
- Community includes = large companies, variety of different organizations & interested persons
- This group of enthusiasts collaborate to develop free articles, tutorials, papers, technologies, & instruments.
- **OWASP Top Ten** = powerful awareness document for web application security. & most critical web application security flaws

❑ Injection

❑ Broken Authentication

❑ Sensitive Data Exposure

❑ Security Misconfigurations

- Insufficient Logging & Monitoring= when security-critical event is not logged off properly, & system is not monitored

System Effectiveness

- **The IS auditors should verify whether:**
- a) Computerized operations provide better customer service in terms of time and quality.
- b) Staff serves a larger number of customers during the day than prior to the introduction of online operations.
- c) Customer information is provided timely and accurately.
- d) The system reflects any improvement in the overall quality of products and services offered.
- e) System has improved the tasks accomplishment capacity of its users by enabling them to be more productive.
- f) Users are satisfied with the performance of the system.
- g) System is user friendly and takes less effort.
- h) The users are putting the software to frequent use, which requires less effort and is easier to use and the users are satisfied with performance of the software.

System Efficiency

- **: The IS auditors should verify whether:**
- a) Department/Office ensures the use of every computer asset.
- b) Department/Office utilizes every computer asset to its optimum capacity.
- c) Periodical maintenance of hardware asset ensures its uninterrupted service.
- d) The online operations help complete day’s workload on the same day consuming less time than time taken for the respective manual operations.
- e) The online operations provide accurate, complete and consistent data at each stage of processing.
- f) Department/Office takes consistency check of balances daily to aid in the detection of errors or fraud.
- g. Department/Office uses the hardware peripherals such as printers, nodes etc. efficiently.

IS Audit Checklists for Banks- COBIT Control Objective A - Information Security:

- *Controls provide reasonable assurance that:*
- *IT Infrastructure, applications and databases are protected from unauthorized network intrusions or access.*

Control Objective B – Recruitment & Training

- Controls provide reasonable assurance that personnel policies promote the appropriate hiring and continued security awareness and training of resources

Control Objective C - Logical Security

- ***Controls provide reasonable assurance that logical access to IT applications is restricted to authorized individuals only***
- ***PAM:***
- Privileged Access Management (PAM) refers **to systems that securely manage the accounts of users who have elevated permissions to critical, corporate resources**.
- These may be human administrators, devices, applications, & other types of users.
- **Privileged user accounts** = high value targets for cyber criminals.

Control Objective D

- ***Controls provide reasonable assurance that <u>data communication through the network is secured and monitored</u>***

Control Objective E – Change Management

- *Controls provide reasonable assurance = changes to IT applications are recorded, analyzed, tracked, approved and tested before implementation on production environment.*
- *Controls = provide reasonable assurance that emergency changes are implemented and approved as per documented process*

Control Objective F - Backup & Restoration Management

- *Controls provide reasonable assurance = data is backed up at pre-defined intervals & as per established backup procedures.*
- *Controls = provide reasonable assurance that adequate DR plans & procedures are documented & tested for critical systems*

Control Objective G – Physical Security

- *Controls provide reasonable assurance =* ***physical access to DC & DR site is restricted to authorized personnel***

Control Objective H - Environmental Controls

- *Controls provide reasonable assurance* = ***environmental safeguards have been implemented within DC & DR site***

Control Objective I – Security Operations Centre

- **Independent security program review = assess security risk & overall maturity** of security function for Finacle Core, Finacle Treasury

SWIFT System

- SWIFT codes = combination of various kinds of letters & used to identify branch codes of banks.
- These codes used as **Bank Identifier Codes (BIC).**
- SWIFT Message = Maker, Checker, Verifier
- A **SWIFT code** is used to identify a particular branch of a bank.
- Key components of package –

❑ Business Identifier Code (BIC),

❑ International Bank Account Number (IBAN),

❑ Legal Entity Identifier (LEI).

- **SWIFT system** - used by banks, brokerage institutions, trading houses, securities dealers, AMC , clearing houses, depositories, exchanges, corporate business houses, FX brokers.

PNB case - Key issue

- LoUs were opened for pearl import for which total time period allowed by RBI is 90 days.
- Some of the overseas branches of Indian banks overlooked the rule.
- PNB alleged - “clear criminal connivance” of group companies of Modi and Gitanjali with some officials of PNB and other banks.
- PNB complained - some of the branches of other Indian banks have not shared key documents related to the credit with PNB.

AP Mahesh Cooperative Urban Bank case -2022

- Servers of Hyderabad-based AP Mahesh Co-operative Urban Bank hacked by some people and funds to the tune of nearly Rs 12 crore were allegedly fraudulently transferred to several bank accounts across the country.
- Mahesh Bank has 45 branches across four states.
- AP Mahesh Co-operative Urban Bank said funds of the bank was found to be transferred by the hackers and no amount was diverted from customers' accounts.
- Officials said = Rs 12.48 crore were transferred to several individual accounts of many banks, most of them located in other states and also in Telangana.
- "The destination banks were informed and necessary steps were immediately initiated to secure our funds. The bank's funds are insured against cyber-attack," - Bank Official
- Case was registered and Police team visited bank's main branch
- Hackers siphoned off Rs 94 crore from Pune-based Cosmos Bank, India's 2nd largest cooperative bank, by cloning thousands of credit cards in 2018.
-

- **Process of Fraud**
- Nigerian handlers operating from India were tasked to open bank accounts through locals in banks.
- Phishing mails were sent by an unidentified hacker to 200 staff of Mahesh bank (November 4, 10 and 16, 2021) , 2 of them clicked on links in mails,
- This allowed = remote access trojan malware to be installed.
- Then = key logger software was installed in 2 computers obtaining login credentials of two staff.
- Sniffing through bank’s single network, hacker obtained access to master administrator’s login details, gaining access to bank’s database
- *‘’ since all the systems in the bank are interconnected, the hackers were remotely able to access the Core banking server of the bank.‘’* - CV Anand, CP Hyderabad