Audit in Banking Sector
(Chapter - 6 : DISSA Course) **Part 2**

Arijit Chakraborty

August 08, 2021

LFAR: RBI Guideline Extracts

- *'' The revised LFAR formats are required to be put into operation for the period covering FY 2020-21 and onwards.*
- *The mandate and scope of the audit will be as per this format and if the SCA feels the need of any material additions, etc., this may be done by giving specific justification by the SCA and with the prior intimation of the bank's Audit Committee of Board (ACB).*
- ***VI. INFORMATION SYSTEMS***
- *1.* ***Robustness of IT Systems:***
- *Auditors should comment on the robustness of IT systems covering all the software used by the bank along with functions thereof, inter-linkage/interface between different IT Systems, ATM network and its security, payment system products & services among others.*
- *Further, it should be examined whether the software used by the bank were subjected to Information System & Security Audit, Application function testing and any other audit mandated by RBI. ''*

RBI Guidelines

- Adequacy of IS Audit, migration audit (as and where applicable) and any other audit relating to IT and cyber security system and bank's compliance to the findings of those audits should be commented upon.
- 2. **IT Security and IS Policy:** Auditors should comment whether the bank has duly updated and approved IT Security and IS Policy and whether the bank has complied with the RBI advisory/directives relating to IS environment/cyber security, issued from time-to-time.
- 3. **Critical Systems / Processes:** It should be examined whether there is an effective system of inter-linkage including seamless flow of data amongst various software / packages deployed, via *Straight Through Process (STP).*
- Special emphasis should be placed on outsourced activities and bank's control over them, including bank's own internal policy for outsourced activities.

IS Audit – Detailed Scope

(As per RBI Guidelines 2020, PCI DSS ,OWASP & ISO 27001)

- *Scope of Information Systems Audit is to determine: -*

1. *The effectiveness of planning and oversight of IT activities.*
2. *Evaluating adequacy of operating processes and internal controls.*
3. *The adequacy of enterprise-wide compliance efforts, related to IS, IT & Cyber Security policies & internal control procedures.*
4. *Identifying areas with deficient internal controls, recommend corrective action to address deficiencies and follow-up, to ensure that management effectively implements the required actions.*
5. *Whether = IS risks are appropriately identified , managed and whether the controls and risk management processes are adequate & implemented as per the instructions issued by the Bank from time to time.*

Independent Assurance

- **Independent Assurance of Bank's IS Audit function**
- **Scope of Audit :**
- to provide assurance to Bank's management & regulators:
- on the bank's internal IS function, to validate approach and practices adopted by them in the discharge of its responsibilities as laid out in IS Audit Policy.
- **Scope includes** = review & revision of IS Audit Procedure & IS Audit Manual (separate ToR)

CBS Environment= IS Audit scope

- *1. The objectives of Confidentiality, Integrity and Availability of data are maintained & legal and regulatory requirements complied with.*
- *2. The IS resources are acquired economically, justifiably, used efficiently and protected adequately to effectively achieve Bank's business objectives.*
- *3. Review and evaluation (wholly or partly) of automated information processing systems, related non-automated processes & interfaces among them = RPA, AI Tools , Cloud interface*
- *4. Evaluate appropriateness of Risk Management exercise done by the Asset Owners & Control Self-Assessment.*
- *5. IS Audit should cover areas specified by RBI.*
- *6. IS Auditors = verify adequacy of Business Continuity Planning (BCP) arrangements, periodical Vulnerability Assessment and Penetration Tests (VAPT) & corrective measures taken by concerned departments.*
- *7. Bank will conduct Vulnerability Assessment & report will be shared with IS auditor.*

RBI : Additional requirements

1. ***Mobile Banking Transactions*** *in India- compliance with Operative Guidelines for Banks vide RBI Master Circular–DPSS.CO.PD.Mobile Banking.No./2/02.23.001/2016-2017 dated 01.07.2016 or the current Master Circular as on date of Audit.*
2. ***BCP, VAPT & Information Security*** *vide RBI Circular DIT.CO(Policy) No. 2636/ 09.63.025/2012-13 dated 21.01.2013.*
3. ***Security and Risk Mitigation Measures*** *for* ***Electronic Payment Transactions*** *vide RBI Circular DPSS (CO) PD No.1462 / 02.14.003 / 2012-13 dated 28.02.2013 / instructions/guidance issued by RBI.*
4. ***Master Circular on Credit Card, Debit Card and Rupee Denominated Co-branded Prepaid Card operations of Banks*** *vide RBI Circular No. RBI/2015-16/31 DBOD.No.FSD.BC.18/24.01.009/2015-16 dated 1st July, 2015 or the latest instructions / guidance issued by RBI*

- ***NPA Classification***

1. *Extant logic for classification of NPA as 'Doubtful Assets' is in place where = erosion in realizable value of security is more than 50% of the value assessed by the bank or accepted by RBI at the time of last inspection, as the case may be.*
2. *Extant logic for classification of NPA having security less than 10% of the outstanding as 'LOSS Assets' is in place.*
3. *Oldest NPA date is stamped in all accounts of Borrower within a branch as per Borrower-wise NPA rule.*

- *(one a/c NPA = all a/cs NPA)*

IS Audit with evidence

- Needs to be tested with appropriate evidences:
- **a. General Security settings** with respect to Application, Operating System and Database
- **b. Procedures for New User setup**, Terminated Users, Transfers
- **c. User Access Reviews**
- **d. Segregation of Duties**

Backup Policy

- **Check =**
- 1. Whether approved backup policy is in place & back up of data and software essential for the continued operations of the bank is taken as specified in the backup policy
- such backups are tested periodically for recovery.
- Security controls over backup data & media are stringent.
- IT Media handling is in compliance with Bank's IT Policy

IS Audit areas

- Review of previous audit / test reports & actions taken on the recommendations
- Review of **privileged access rights granted to application**, **system administrators, service providers & vendors**
- Assess process for review of user logs for administrator
- **Understand** = how unsuccessful access attempts to applications in scope are logged & monitored.
- **Understand** = manpower deployment for application maintenance
- Based on control design weaknesses identified =
- Highlight areas for conducting forensic audit / Review

Check =Use of Proximity Cards

- **Proximity cards** = leading smart cards provided

✓ contactless cards with an antenna embedded inside.

✓ read-only cards & information on these cards cannot be manipulated.

✓ work on RFID technology & used for access control, identification & security.

- **CCTV**

1. CCTV surveillance equipment = monitor critically identified points within DC & DR sites.
2. CCTV digital feeds are stored & retained for a minimum of 15 days.
3. Recordings are reviewed by Admin Manager on a daily basis
4. Exceptions are recorded in CCTV review register &
5. reported to Facility Manager.
6. CCTV performance is checked online, &
7. findings are logged into CCTV breakdown register on a daily basis.

Audit of Networking & Security Devices

- *Access Control*
- *System Authentication*
- *Auditing and Logging*
- *Insecure TCP/IP Parameters*
- *System Insecurities*
- Payment System Department: SWIFT Alliance Access applications

Database Configuration Audit

- *Database Account Authentication*
- *Password Policy*
- *Access control & authentication*
- ***Security configuration of desktops & laptops*** = *used by business users can be performed on sampling basis (say 10% of total Assets in the concerned Dept.) as per Bank's requirements*

UAT & Review

- Check sufficiency & coverage of UAT test cases,
- review of defects & tracking mechanism deployed by Bidder&
- resolution including re-testing & acceptance.
- Backup/ Fallback/ Restoration/ Recovery & Restart procedures

OWASP Top 10

- Open Web Application Security Project
- **What Is OWASP?**
- 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

Disaster Recovery:

1. Whether DR strategy adopted is adequate for continuity of operations of IS which are critical to the Bank's business in the event of disasters.
2. Whether it has necessary safeguards to minimize risks, costs & duration of disruption to the business processes caused by disasters.
3. Whether DR Drills conducted were adequate enough to ensure continuity of operations in the event of actual disaster.
4. Where DR strategy is dependent upon vendors, whether adequate arrangements are available with vendors to enable the DR exercise function successfully & they have necessary infrastructure

Risk Management

- Whether Risk Assessment done by departments concerned has taken into account :
- a. Maintaining IT inventory
- b. Classification of Assets
- c. Classification of Information
- d. Risk Assessment (including process risks)
- e. Risk Treatment
- f. Risk Mitigation
- Risk Assessment is done periodically or whenever changes are made to IT infrastructure.

Foreign Operations & Overseas branches

- SSAE 18 SOC 1 Type 2 Report & ISAE 3402 Report to provide information on controls applicable to Information Technology (“IT”) General Computer Controls (“GCC”)

RBI New Guidelines on IT & CBS – 2020
IS Audit : new Scope

- In order to ensure the completeness and integrity of the automated Asset Classification (classification of advances/investments as NPA/NPI and their upgradation), Provisioning calculation and Income Recognition processe
- RBI issued notification Automation of Income Recognition, Asset Classification and Provisioning processes in banks And banks are advised to put in place / upgrade their systems to conform to the following guidelines latest by June 30, 2021.
- Banks shall also ensure that the updated account status, including asset classification of the customer accounts, flow to the CBS automatically, if NPA classification process is performed outside CBS.

User Access Management

A. 20. Ensure that all "user-ids" in the solution have unique identification. If there are any generic user-ids used, **it should only be used under exceptional circumstances** and such ids should be mandatorily mapped to the employee ID of the user to fix accountability of the activities carried-out under the generic ID.

B. 21. Provide *for two-factor or higher level of authentication* for the users of the application.

C. 22. Restrict the access to the solution on "need to have/least privilege" basis for all users.

D. 23.. Provide for maker checker authorisation /control for transactions

E. Cases:

F. updating/modifying the internal accounts,

G. customer accounts,

H. parameters – both financial and non-financial that affect the status of the credit portfolio/loan/asset.) entered in the solution.

Administrator accounts

- This shall also include transactions/activities carried out by administrator accounts in the application.
- **Case :**
- create/update/modify user-ids,
- roles,
- privileges including access rights to various modules; system related activities including updates to master data, etc. should have at least two individuals to complete the activity.

Back-end Data Access Restriction

- Any changes to the data, parameters **from backend shall be avoided**.
- The solution should provide for changes to the data items only through front end (from the application (Ex: CBS) itself and not through the backend database update) after requisite authorisation.
- Audit trails/logs of access, changes to any data, parameters, if any, **should be captured** with specific user details in the system.
- In case of exceptions in rare circumstances, such changes should be duly approved at an appropriate level and documented.
- Provision for **MIS report** should be available to auditors to generate complete list of back-end access and changes made.

RBI New Rules 2020
System Requirements and System Audit:

- *In case a separate application outside the CBS is used as the System for NPA/NPI identification and/or classification, the System must have access to the required data from the CBS and/or other relevant applications of the bank and the borrower/investment accounts shall be updated back into the CBS automatically, wherever applicable, through STP.*

- *Banks shall keep the business logic and other parameters/configurations of the System updated to ensure that the System based identification, classification, provisioning and income recognition* ***are strictly in compliance*** *with the regulatory guidelines on an ongoing basis.*

- *There should* ***be periodic system audit, at least once in a year, by Internal / External Auditors*** *who are well versed with the system audit both on system parameters as also from the perspective of compliance to Income Recognition, Asset Classification and Provisioning guidelines.*

Aspire for a successful professional career.

Thank You