BANKING APPLICATION AUDIT

CA Kiran Kunte
B.Com, FCA, Cert. In IFRS [ICAI], DISA, LL.B

PUNE

Audit objectives:

"To ensure that the Information technology infrastructure is logically and physically protected and that generates the reliable output which ensures data integrity and maintains confidentiality "

Practical Difficulties

Use of CAAT Tools is not permissible

Auditors Computer System has no Banking Software Installation

Way out

Auditing AROUND the Computer and Not

Auditing WITH Computer

Conducting both Compliance testing and substantive testing

Why a challenge ?

- Reporting is Not in Structured/ Predefined Format
- Goes much beyond TRUE AND FAIR..
- It's a PROPRIETY AUDIT and Not Vouch & Post Audit..

Logical access

NEED TO KNOW
&
NEED TO DO BASIS

Name of the user
Designation/ Grade
Role of the user

What is MOST IMPORTANT ???

What are the rights available to a User

- ✓READ/ VIEW
- ✓WRITE
- ✓AMEND
- ✓AUTHORISE

Ideal matrix of user rights-
Name- XYZ/ Convention
Designation/Grade: Chief Manager
Role- Auditor

Banking Prgramme	Read	Write	Amend	Authorize
Cash Management	YES	NO	NO	NO
Drawing Power	YES	NO	NO	NO
NPA Identification	YES	NO	NO	NO

Auditor is required to KNOW All and DO Nothing in Banking Software

For how many days Pass word is valid?
Does the System enforces Password change after XX days ?
Can DBA Change Pass word in the case of extreme necessity?
Are the users DISABLED when they proceed on leave?
Whether MAKER CHECKER Principle is embedded in User Management ?
Does the System allow creation of more than one user id ?
Whether Pass word has a syntax requirement?

Few more compliance tests..

Whether Unattended terminal gets logged off after XX Minutes ?

Who Updates BASIC PARAMETRES In the System?

Whether there exists a mechanism to Detect Intrusion?

INPUT Control..

Garbage in… Garbage Out..

Whether each transaction has a Transaction ID ?
Whether System rejects IMPURE Data ?
Range Check/ Validity Check/ Control Total/Hash Total?
Whether Exceptional report mechanism is in place?
Whether Data Mapping mechanism exists in Input Control?
Whether there is COMPLETENESS in Input Structure?
Are Vital fields Mandatory ?
Whether manual data entry is Minimum?.....Senior Citizen….

Whether the time and date stamp is available for each transaction?

PROCESS CONTROLS

Correct Input but a Wrong Process leads to Wrong Output

Each New Input UPDTE some file.
Are those Updations duly authorized?
Who validates KEY DATA + PROGRAMMED PROCEDURE applied on Key data? Ref.Interest Run on Batch processing
What are the MANDATORY Controls for DAY BEGIN and DAY END Process?

Whether Process throughput can take care of peak period Volume ?

Whether Centralised Codification process to master data exists? If not its fragmentation of data base..

Whether Standing Instructions not executed are rolled over to next day?

Whether System monitors unexecuted standing Instructions and decide the Priority of handling the same?

Whether System Prompts Console Messages?

Whether there is a system to By pass the message?

If so whether this is with Proper Authorisation?

INTERFACE CONTROL

Internal Communication between 2 Processes/Application Modules

Financial and Non financial data..

An example of Interface

Cheque Book issue: Clerical event
Issuing a Bank Guarantee- Non Fund event
Stock statement Receipt entry: Clerical event
Receipt of PAN Details: Clerical event

AUTHORISATION CONTROL.

- Whether Maker Checker Principle is followed?
- Whether Authorisation process and Logical access are complementing each other?
- Are the Transactions needing Approval Stacked in queue and released in time?

OUTPUT CONTROL

DATA+ INPUT+AUTHORISATION+PROCESS

=

OUTPUT

Whether Output generated is tested?
Is it reliable?
Does it reach the User on NEED TO KNOW basis

Identify Reports on PULL Method

Identify reports on PUSH Method

DATA INTEGRITY

ACCURACY and CONSISTENCY

Of Stored data

indicated by an absence of Alteration between two updates of a data record.

No data can be deleted

Checks like HASH Totals etc are applied so as to ensure that No data is tampered/altered/deleted

If at all done, System must report this..

REVIEW OF LOG AND AUDIT TRAIL

Does the audit trail associate with the product/service support the ability to log and review all actions performed by systems operators, systems managers, system engineers, system administrators, highly privileged accounts and emergency IDs?

Does the financial transactions as well as additions, changes and deletions to customer's demographic data/important statistics, get recorded in the product/service audit trail?

Does the audit trail for product/service record all identification and authentication processes? Also Is there a retention period for the Audit trails

Does the audit trail associate with the product/service log all actions by the ISA?

Is there a process to log and review all actions performed by systems operators, systems managers, system engineers, system administrators, security administrators, and highly privileged IDs.

Is there a process in place to log and review actions performed by emergency IDs associated with the product/service?

BEST RESOURCE

PERFORMANCE AUDIT OF IT SYSTEMS IN J & K BANK LTD-

Audit carried out by C& AG…..

Full text available on Public domain

REFER

Clause No:

6.3, 6.5.

7.1, 7.2, 7.3, 7.5, 7.6,

7.7,7.8, 7.10,7.11, 7.12

Thank You all

For Sparing your Week end..