Compliance & Security Framework

(Chapter -2 : DISSA Course)

Arijit Chakraborty

May 23, 2021

Hacking- nature

- **Black Hat hackers** = Hackers , criminals who break into computer networks with malicious intent.
- release malware that *destroys files, holds computers hostage, or steals passwords, credit card numbers, other personal information.*
- **Black Hat malware kits** sold on Dark Web (part of internet deliberately hidden from search engines) sometimes even include warranties & customer service.
- phishing or managing remote access tools
- HACKING = ORGANISED BUSINESS , nexus with criminal organisations
- **Black Hat *call-center* scam :**
- 1. *hacker calls as Microsoft call center technician*
- *2. convinces victims to allow remote access or download software for faster computing experience*
- *3. once access given, hacker harvests banking & Personal info,*
- *4. take over control, uses computer to launch attack on other victims*

Ethical Hacking- nature & tools

- Ethical hacking tools help companies identify possible shortcomings in internet security & prevent data breaches.
- VAPT - Voluntary periodic testing
- Detailed Scope , Structured agreement with entity management= CONFIDENTIAL
- CEH = prevent fraudulent crimes and identity thefts
- White hat hacker
- Only owners, CEOs and Board Members (stake holders) who asked for such a security review are aware
- Org staff usually not aware of Ethical hacking going on
- **Ethical hackers may arrange for :**

✓ cloned test systems,

✓ organize a hack late at night while systems are less critical

✓ Denial of service attack- disrupting service to host

✓ Disk & memory forensics

✓ Network security test

✓ Use of social engineering

✓ Use of Data Recovery Tools:

Process risk

- Process risk is after considering the control isn't it please?
- Is there a gradation of Process risk?
- **Response**
- Process risk : gross risk
- ***Less :*** internal control
- = net risk
- **Gradation :**

❑ Insignificant

❑ Low

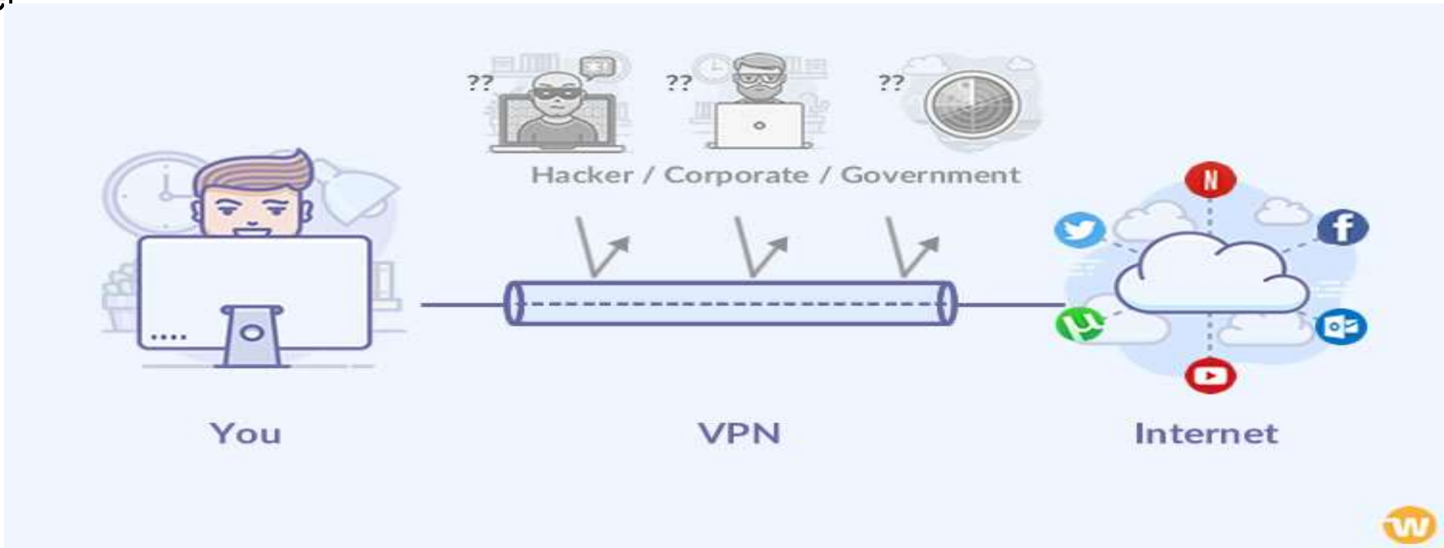
❑ Medium

❑ High

❑ Catastrophic

Virtual Private Network

- ✓ establish a protected network connection when using public networks.
- ✓ encrypt internet traffic & disguise user's online identity.
- ✓ makes it more difficult for 3rd parties to track user activities online and steal data.
- ✓ encryption takes place in **real time**.
- ✓ VPN hides user IP address by letting e network redirect it through a specially configured **remote server** run by a VPN host.
- **Implies :** if user surfs online with a VPN, VPN server becomes source of his data.
- Internet Service Provider (ISP) & third parties cannot see which websites user visits/ data sent & received online. A VPN works like a filter



VPN – possible risks

- **1. Logging Policies**
- Usage logs may remain unprotected
- **2. Data Leaks**
- Data may leak through VPN tunnel: IP leaks, DNS leaks, WebRTC leaks
- **3. Privacy Policies**
- VPN provider **may share data with advertisers / 3rd parties**
- **4. Weak-Configured Encryption**
- **5. Malware Infections**
- Malware injected into device when downloading VPN client
- **Impact :**

✓ *spying on user activities,*

✓ *spamming with malicious ads,*

✓ *stealing personal and financial details.*

✓ *ransomware which may encrypt user data & ask for big ransom in exchange*

Phishing attack (Vishing = attack by landline / mobile)

- Used to steal user data - login credentials and credit card numbers.
- Attacker, masquerading as a trusted entity, dupes a victim into opening :

❑ email,

❑ instant message,

❑ Text message.

- Recipient tricked into **clicking a malicious link**, which can lead to :

❖ *installation of malware,*

❖ *the freezing of the system as part of* ***ransomware attack***

❖ *or the revealing of* ***sensitive information.***

इंडियनऑयल

Indian Oil Corporation Limited

WEBSITE DATA PRIVACY POLICY

DEFINITIONS

- **Agent**: Any individual or entity which has a contractual relationship with IOCL, where IOCL is the principal and the other individual or entity is the agent, shall hereinafter be referred to as an "Agent". For instance, IOCL’s distributors, dealers, CFA, contractors, etc. shall be considered Agents.
- **Data Subject:** All individuals whose personal information is either collected, received, processed, stored, dealt or handled by IOCL shall be referred to as “Data Subject”.
- **Information:** Personal Information of a Data Subject collected by IOCL under this Policy shall hereinafter be referred to as “Information”.
- Such Information includes, interalia, Sensitive Personal Data or Information as defined under the Indian Information Technology Act, 2000 and the **Aadhaar number** and/or the **biometric information** associated with an Aadhaar number.
- **GOVERNING LAW**
- IOCL is an organisation based and existing in India and is thus bound by the laws of the Republic of India. This Privacy Policy has been prepared in accordance with applicable Indian laws, including the Indian Information Technology Act, 2000
- **APPLICABILITY**
- This Policy applies to all individuals whose Information is either collected, received, processed, stored, dealt or handled by **IOCL.**

- **OBJECTIVE**
- This Privacy Policy is intended to inform the **Data Subject** on how **IOCL** collects, processes, stores, and uses personal information that a **Data Subject** provides to **IOCL** either directly or indirectly**.** This Privacy Policy also covers **IOCL's** treatment of any personal information that Third Parties share with **IOCL**.

- **HOW IOCL COLLECTS DATA SUBJECT'S INFORMATION**
- **IOCL** collects **Data Subject's** Information during their visit to the IOCL Websites. This also includes instances where a third-party may provide such Information on the IOCL Websites on behalf of the Data Subject.
- Data where the identity has been removed [anonymous data] such as cookies, web beacons and other browsing information do not come under the ambit of **Data Subject's Information**.
- Such browsing information is collected through cookies and web beacons to track what features or web-pages the **Data Subject** has viewed on the IOCL Websites, and other information about **Data Subject's** browser and browsing behavior. IOCL uses browsing information to improve the design and content of the IOCL Websites, to suggest content and products that **IOCL** thinks may be relevant to the **Data Subject**, and other related purposes. Most browsers accept cookies automatically

- **WHY IOCL COLLECTS DATA SUBJECT’S INFORMATION [PURPOSE]**
- **IOCL** uses the **Information** to conduct its business and to provide **Data Subject** with the best possible services/products. **IOCL** will only use the **Information** based on this Privacy Policy, its understanding with the **Data Subject**, or as required by law.
- **IOCL** will collect adequate, relevant and necessary **Information** and will process such Information fairly and lawfully for the purpose it is collected . Most commonly, **IOCL** will use the **Information** in the following circumstances:
- (a) Where **IOCL** needs to perform the obligations it has promised the **Data Subject,** such as to provide a service or product to the **Data Subject** and to enable the **Data Subject’s** use of **IOCL’s** products/services, including but not limited to dealing with enquiries and complaints made by or about the **Data Subject** relating to services/products provided by **IOCL** and to improve and customise **IOCL’s** services/products in accordance with the **Data Subject’s** preferences;
- (b) Where **IOCL** needs to comply with a legal, accounting, business or reporting obligation, including compliance with requests from the Government of India or any Governmental Agency;

- (c) To send marketing as well as non-marketing commercial communications to the **Data Subject**;
- (d) To send the **Data Subject** notifications that the **Data Subject** has specifically requested for as well as to send statements, invoices and payment reminders to the **Data Subject**, and to collect payments from the **Data Subject**;
- (e) To provide Third Parties with statistical information about its customers but those Third Parties will not be able to identify any individual from that information;
- (f) To keep **IOCL's** website, mobile applications and other systems secure and to prevent fraud;
- (g) To promote the mission and objectives of Skill Development in India and/or to provide and disseminate information about relevant programmes under the Skill Development Mission.
- (h) To manage the employment of the data subject with IOCL.

- **INFORMATION SHARING AND DISCLOSURE**
- **IOCL** may disclose the **Information** to any of its Agents or Third Parties insofar as reasonably necessary for the purposes set out in this Policy and for the purpose of providing services/products to the **Data Subject**.
- Such Agents and Third Parties are expected to provide a similar level of protection to the **Information** as is adhered to by **IOCL**.
- In addition to this, **IOCL** may disclose the **Information** where it is required to do so by law or to Governmental Agencies.
- **TRANSFER OF INFORMATION OUTSIDE INDIA**
- Unless stated otherwise, **IOCL** stores and processes the **Information** in India. There may, however, be occasions when **IOCL** needs to transfer the **Information** outside India for its business requirements. In such instances, **IOCL** will exercise the same level of care in handling the Information as it does in India.
- **DATA SECURITY**
- The **Information** is processed by **IOCL** in strict accordance with the Indian Information Technology Act, 2000, and the rules notified thereunder. **IOCL** implements and maintain 'Reasonable Security Practices and Procedures' as stated in the Indian Information Technology Act, 2000 and the Information Technology [Reasonable Security Practices and Procedures and Sensitive Personal Data or Information] Rules, 2011, while processing, collecting, storing or handling any **Information.**

- **DATA RETENTION**
- **IOCL** will only retain the **Information** for as long as necessary to fulfil the purposes **IOCL** collected it for, including for the purposes of satisfying any legal, business, accounting, or reporting requirements.
- In some circumstances, **IOCL** may anonymise the **Information** so that it can no longer be associated with the **Data Subject**, in which case **IOCL** may use such information without a further reference to **Data Subject**.
- **REVIEW OF INFORMATION**
- **CHANGES TO THIS PRIVACY POLICY**
- **GRIEVANCE OFFICER**

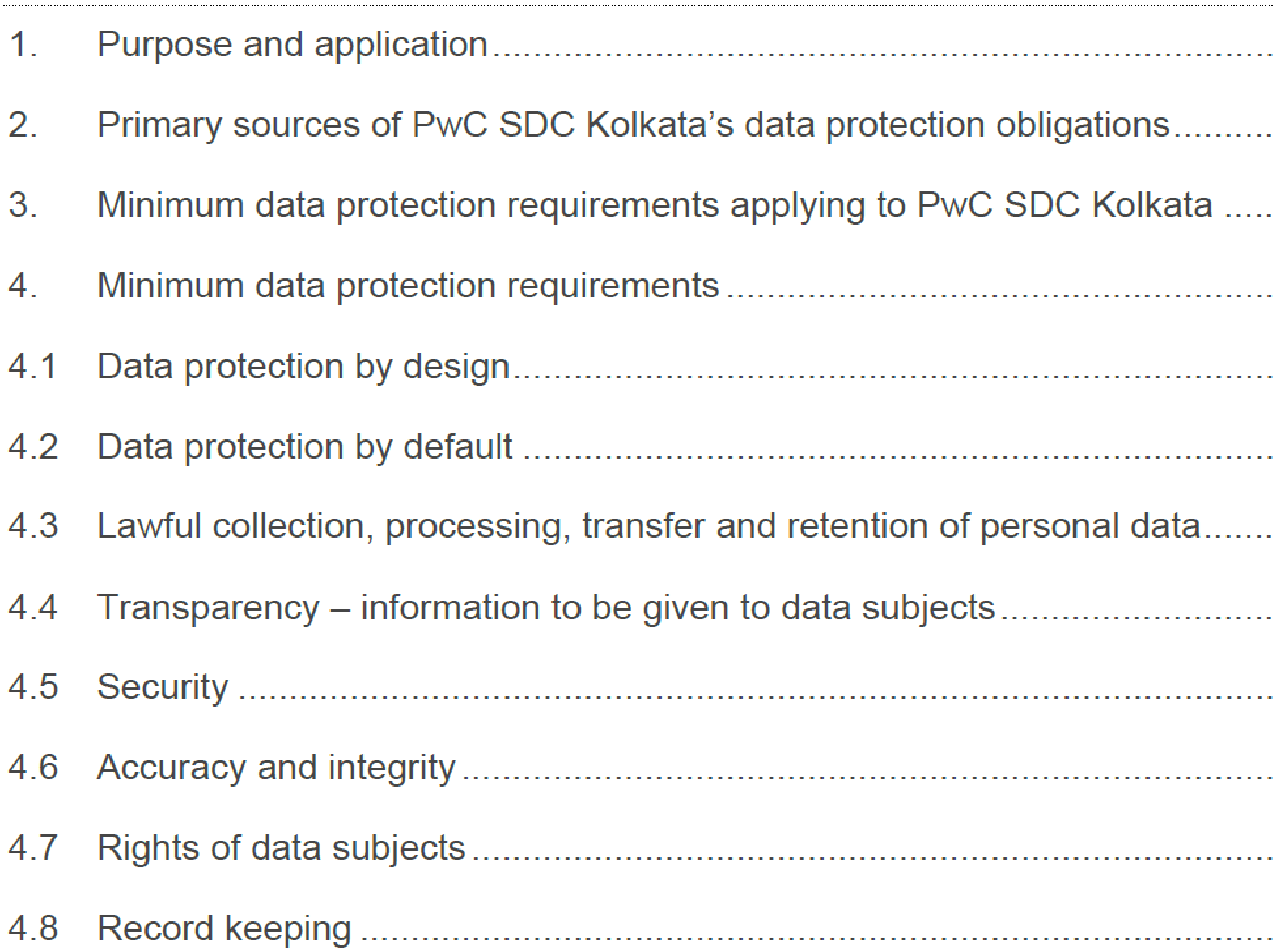
PwC SDC Kolkata Data Protection and Privacy Policy

Document Owner: Risk and Ethics
Classification: Public

Version: 1.3

Released: 24 August 2020

Contents



CASE STUDY : Bank audit in CBS
Finacle - Overview

- Some of the Banks using Finacle are
  - Bank of Baroda
  - Bank of India
  - Union Bank of India
  - Canara Bank
  - Federal Bank
  - IDBI Bank
  - ICICI Bank
  - Axis Bank
  - ABN Amro
  - Vijaya Bank
  - UCO Bank

Finacle universal banking products designed to address core banking, e-banking, treasury, wealth management & CRM requirements of retail, corporate and universal banks. developed by Infosys

Finacle – outreach

100
Countries

1.05 billion
Consumers

81,560
Branches

1.3 billion
Accounts

Cloud Ready

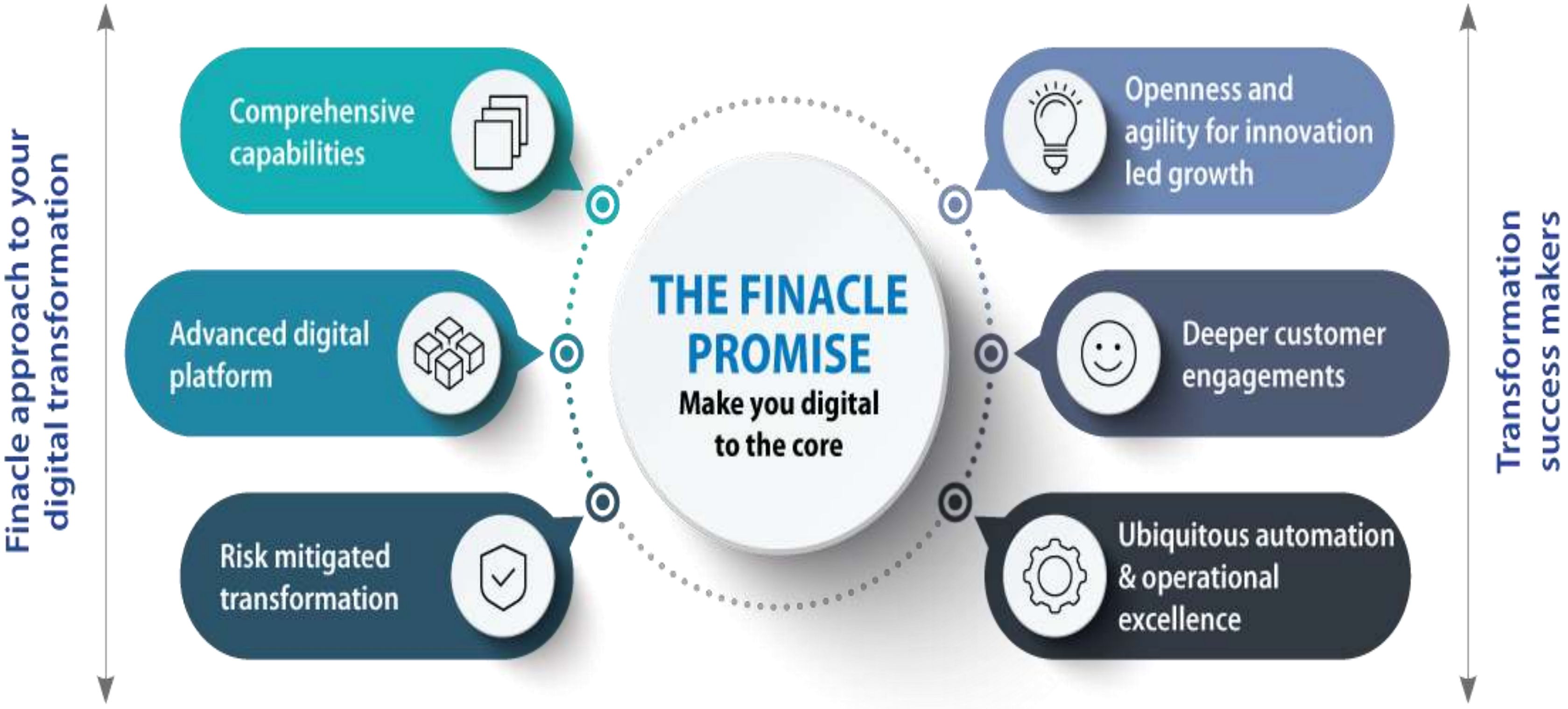
Technology Platform Choice

Truly 24x7 Real-time Processing

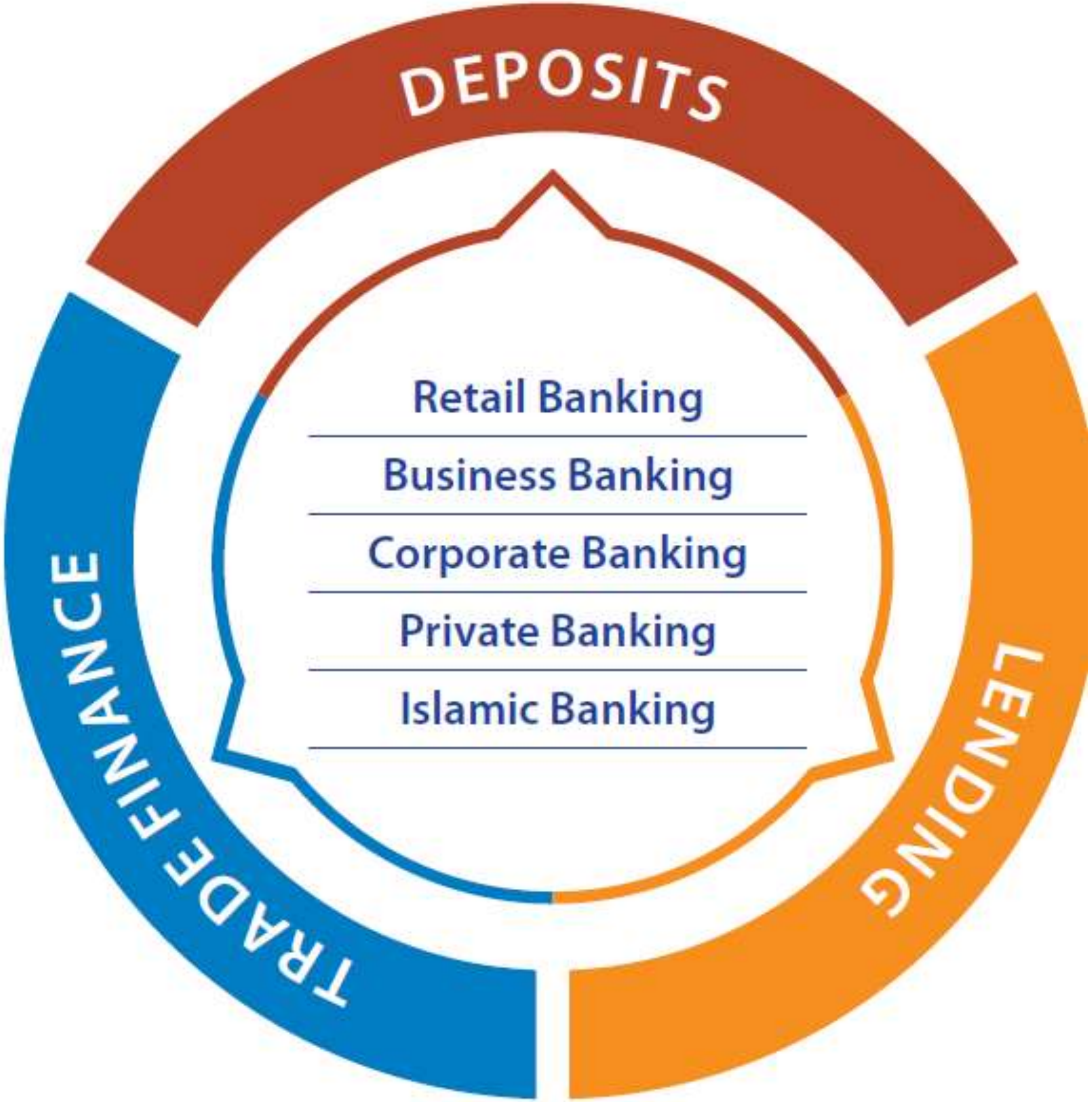
Multi Capabilities

Highly Secure

USP


Finacle approach to your digital transformation
Comprehensive capabilities
Advanced digital platform
Risk mitigated transformation
THE FINACLE PROMISE
Make you digital to the core
Openness and agility for innovation led growth
Deeper customer engagements
Ubiquitous automation & operational excellence
Transformation success makers

Finacle - CBS



Retail Banking

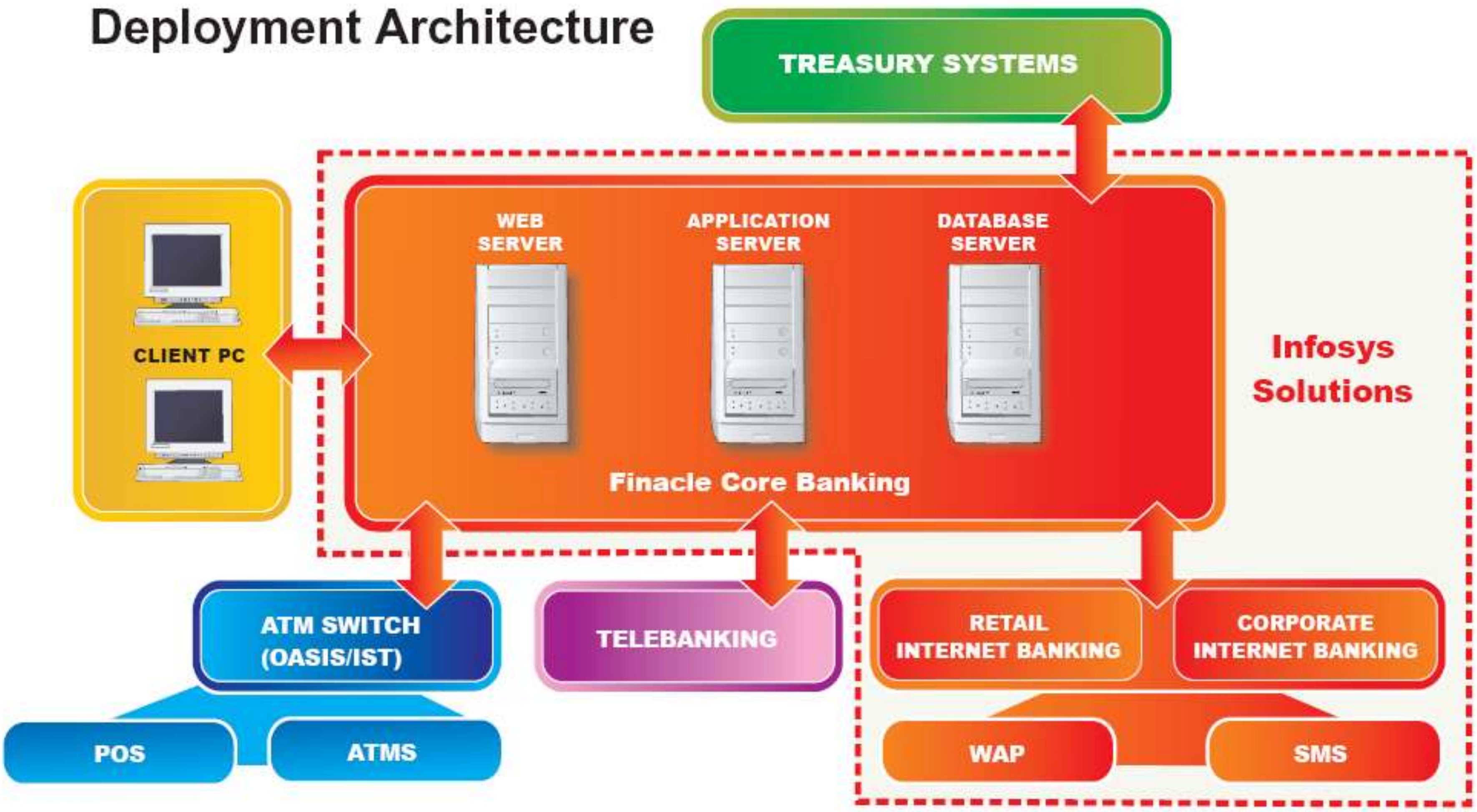
Business Banking

Corporate Banking

Private Banking

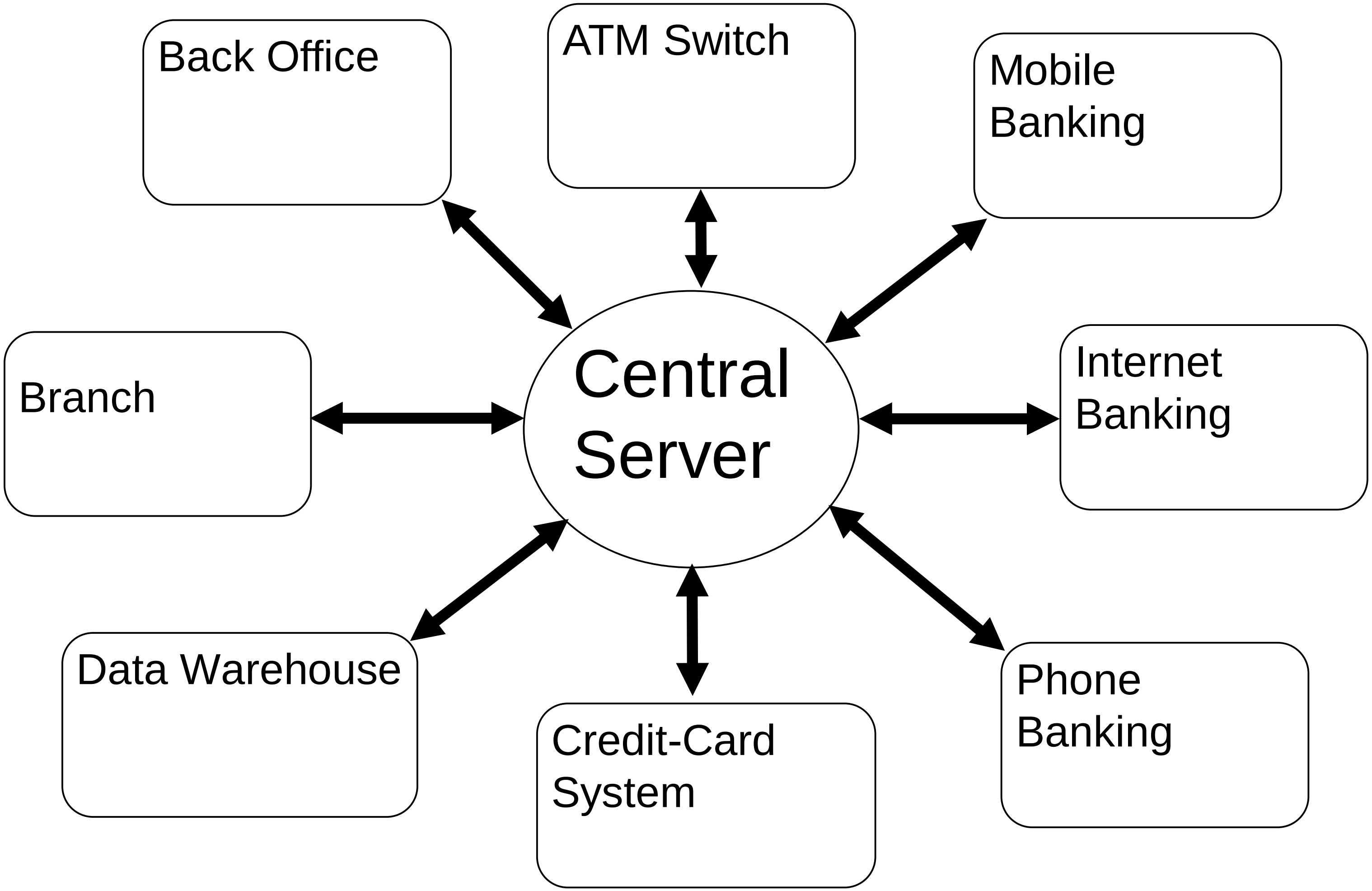
Islamic Banking

Finacle in IDBI Bank

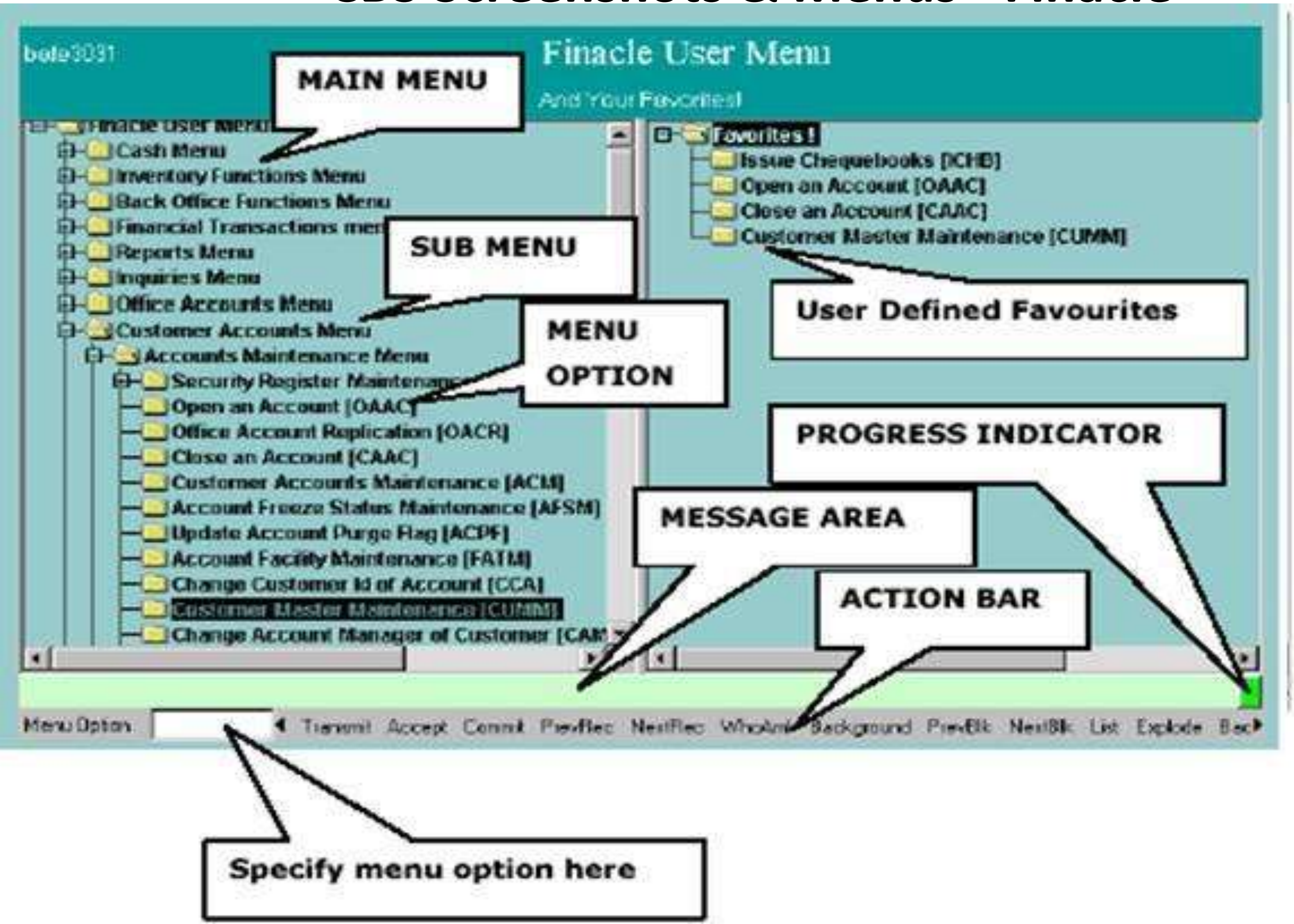


Source: *www.infosys.com*

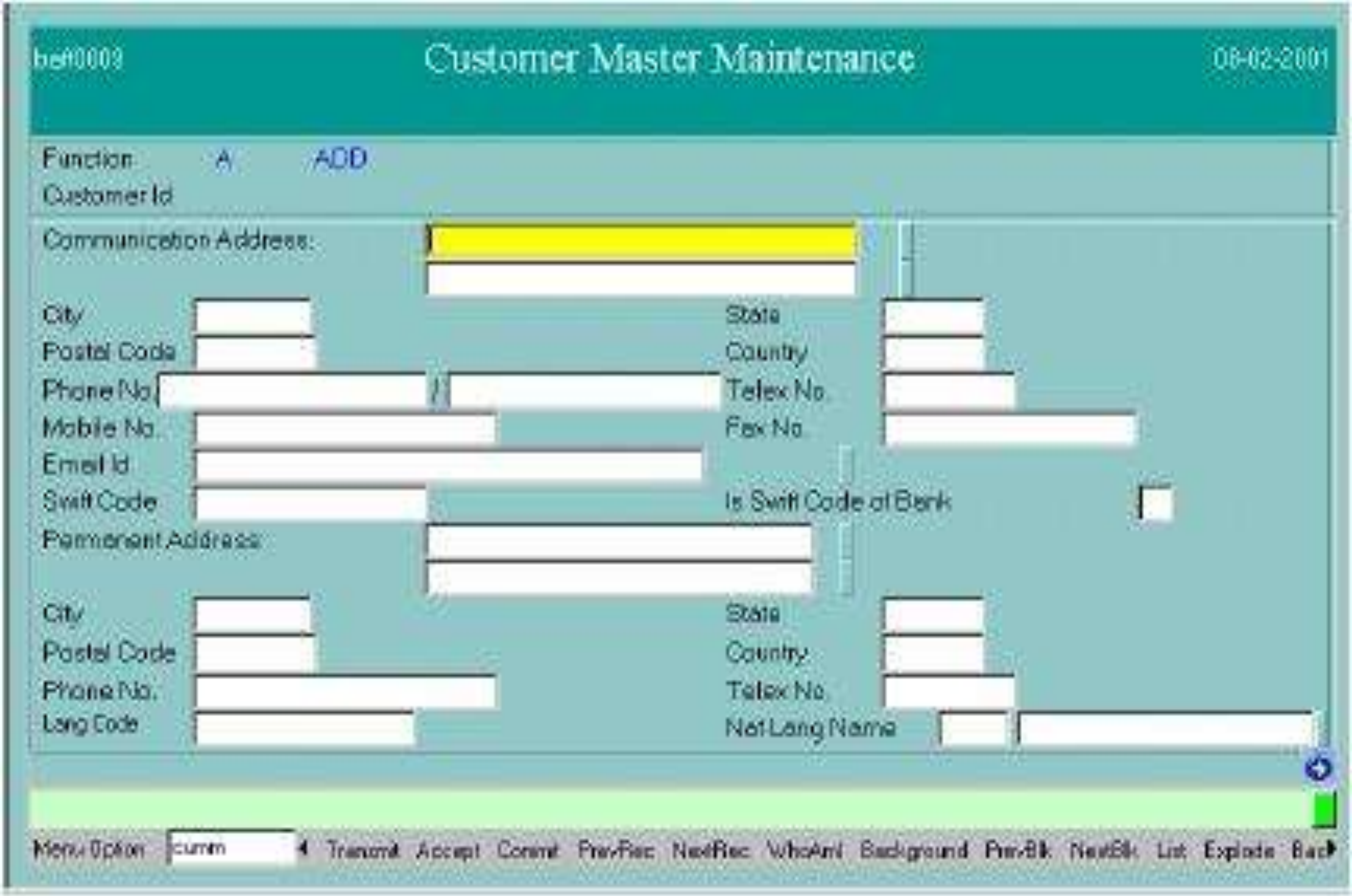
CBS architecture – Overview



CBS Screenshots & Menus - Finacle



Customer Master Maintenance - CUMM



baf0003 Customer Master Maintenance 08-02-2001

Function A ADD

Customer Id

Communication Address:

City

State

Postal Code

Country

Phone No /

Telex No.

Mobile No.

Fax No.

Email Id

Swift Code

Is Swift Code of Bank

Permanent Address:

City

State

Postal Code

Country

Phone No.

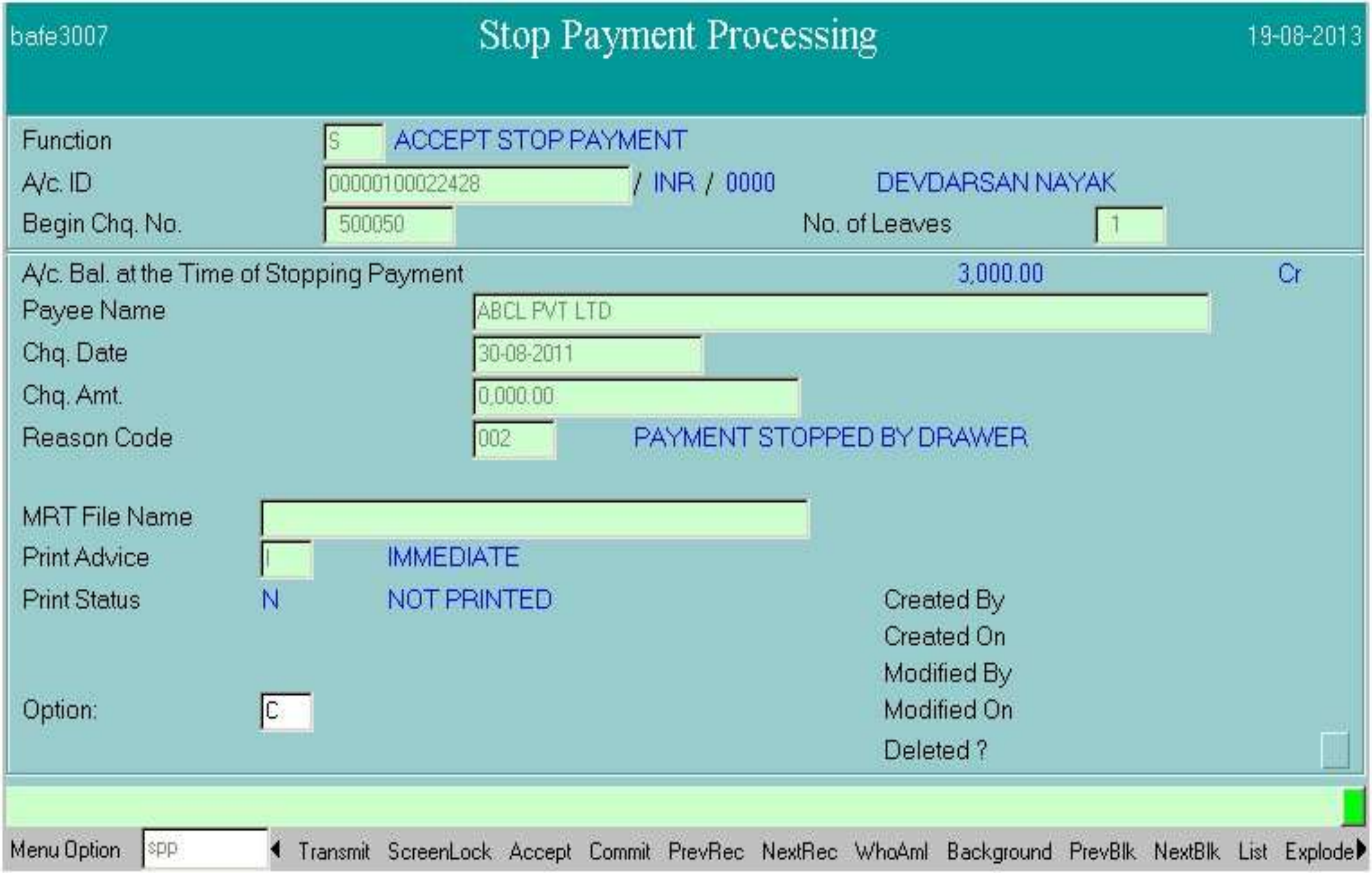
Telex No.

Lang Code

Nat Lang Name

Menu Option cumm

Stop payment processing – code : SPP



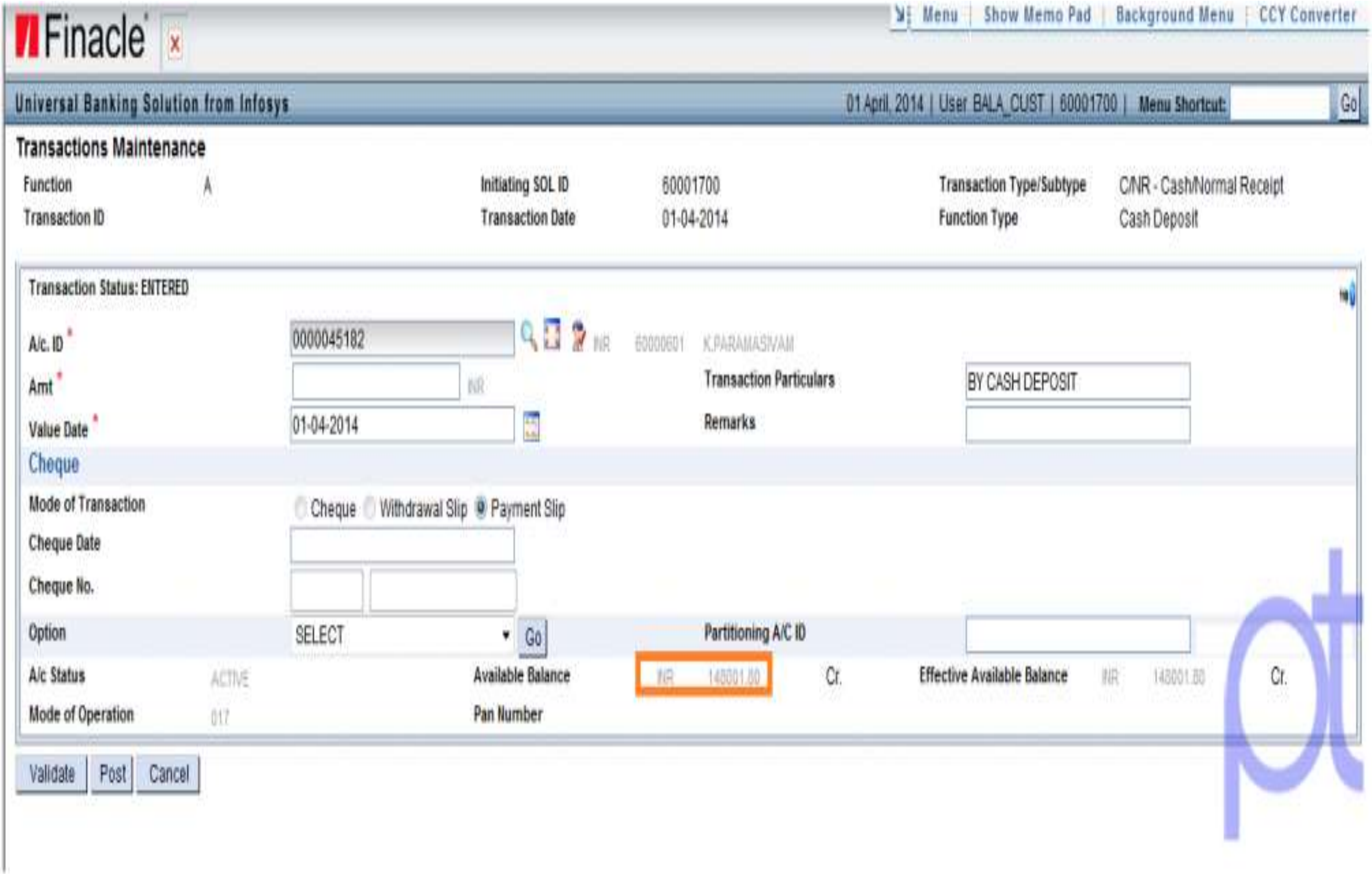
bafe3007 Stop Payment Processing 19-08-2013

Function	S	ACCEPT STOP PAYMENT	
A/c. ID	00000100022428 / INR / 0000	DEVDARSAN NAYAK	
Begin Chq. No.	500050	No. of Leaves	1
A/c. Bal. at the Time of Stopping Payment	3,000.00	Cr	
Payee Name	ABCL PVT LTD		
Chq. Date	30-08-2011		
Chq. Amt.	0,000.00		
Reason Code	002	PAYMENT STOPPED BY DRAWER	
MRT File Name			
Print Advice	I	IMMEDIATE	
Print Status	N	NOT PRINTED	
Option:	C		

Created By
Created On
Modified By
Modified On
Deleted ? □

Menu Option spp

Transaction maintenance


Finacle
Menu | Show Memo Pad | Background Menu | CCY Converter
Universal Banking Solution from Infosys
Menu Shortcut:
Go

01 April, 2014 | User BALA_CUST | 60001700 |

Transactions Maintenance

Function	A	Initiating SOL ID	60001700	Transaction Type/Subtype	C/NR - Cash/Normal Receipt
Transaction ID		Transaction Date	01-04-2014	Function Type	Cash Deposit

Transaction Status: ENTERED

A/c. ID * 0000045182 INR 60000601 K.PARAMASIVAM

Amt * INR

Transaction Particulars BY CASH DEPOSIT

Value Date * 01-04-2014

Remarks

Cheque

Mode of Transaction ○ Cheque ○ Withdrawal Slip ● Payment Slip

Cheque Date

Cheque No.

Option SELECT ▾ Go

Partitioning A/C ID

A/c Status ACTIVE

Available Balance INR 148001.80 Cr.

Effective Available Balance INR 148001.80 Cr.

Mode of Operation 017

Pan Number

Audit Activity through CBS

- Logical Access Controls:
  - Creation / Deletion / Amendment in User Profile, Powers done centrally. If not, verify the compliances as follows.
    - **Records for User** – ID Creation properly maintained?
    - **Records for Deletion of user-ID** with proper authorisation available?
    - **Security of password, compulsory change of password**, Transaction Limit for employees etc.
    - Unsuccessful login attempts

- Output Controls:
    - Whether Hard copies of Accounts available?
    - Whether such reports are signed?
- Security of Data:
    - Whether the encryption software is available in Server / Backup Server (If data is stored)
    - Whether the computers are having Antivirus Software?
    - Whether the AV Software is updated on regular basis?
- Backups
    - Important Activity for Non CBS Branches
    - Backup should be stored on Off-site Location
    - Backup should have been tested at periodical intervals
    - Backup Register should be maintained

Important CBS Finacle Codes

1. ACI – Account Inquiry (Prin, intrst, repayment sch)
2. ACLI – Account Ledger Inquiry
3. LAOPI – Loans & Advances OD Position Inquiry
4. AFI – Audit File Inquiry
5. AVGBAL , CUMI – Cust Master Inquiry
6. SRM: Security Register Maintenance
7. STKSTMT- Stock Statement not submitted
8. CULI – Customer Unutilized Limit Inquiry
9. TODRP – Temporary OD Report
10. TDSIP – TDS Inquiry / Print
11. NPARPT – NPA Report
12. EXCPRPT – Exception Report – A/c due for review, Adv bal > Sanctioned limit, a/c opened without introduction

Thank You