Business Application – Acquisition, Development & Implementation

(Chapter - 5 : DISSA Course) **Part 2**

Arijit Chakraborty

July 3 , 2021

Guidance on executing IS Audit

1. Defining understanding of business process & IT environment
2. - Refining IS Audit scope & identifying internal controls
3. - Testing Control Design
4. - Testing outcome of control objectives
5. - Collecting audit evidence
6. - Documenting test results
7. - Concluding tests performed
8. - Considering use of audit accelerators- CAAT s, GAS, EWP
9. Considering work of other IS Auditors, Experts
10. Considering review of service providers (SOC)

IS Audit engagement- Project details

1. Each year's audit to be counted if IS audit cycle is for 3
2. No of transactions or records along with apps for Operations, DBMS & data security
3. Submission of PBG / security deposit
4. Whether access available from HO for IS audit of Data Centre
5. Nos of Network / Security Devices
6. No of Server, No of Desktop/Laptop
7. No of public facing & internal applications- no of Mobile Apps exposed to outside world
8. Network Architecture Review
9. No of in-scope process, policies & procedures
10. No of IS controls across applications
11. No of 3rd party/ service provided under scope . factors = biz volume, M&A, dynamic industry
12. For IS Infrastructure audit - frequency & number of devices

Types of Evidence

- Business evidence - business record of transaction, receipts, invoices, logs
- Data extraction which mines details from data files by CAAT
- Auditee claim in oral or written documents
- Analysis of plans, polices, procedures & workflow.
- Result of compliance & substantive tests
- Auditor’s observation

Evidence Grading

	Poor	**Good**	**Excellent**
Material Relevance	Unrelated	Indirect	**Direct**
Objectivity	Subjective	Requires few supporting facts to explain the meaning	**Needs no explanation**
Evidence Source	Unrelated third party with no evidence	Indirect involvement by second party	**Direct involvement by first party**
Competency of Provider	Biased	Nonbiased	**Nonbiased and independent**
Evidence Analysis Method	Novice	Experienced	**Experts**
Resulting Trustworthiness	Low	Medium	**High**

Snapshot of IS Audit Report

Content	Description
Introduction	•Audit objectives •Limitation of audit & scope •Period of Audit coverage •General statement on nature & extent of audit process
Overall conclusion and opinion	•Adequacy of controls and or procedures examined •The actual potential risk identified
Detailed and important audit finding and recommendation	•Controls & procedures examined are adequate or in adequate. •Specific finding based on viewpoint of both audit committee & organization •Recommendation for adding and/or modifying controls, procedures & organization.
A variety of finding	•All finding & recommendations.

Detailed Structure of Final IS Audit Report

- **1. Executive Summary**
- a) Executive summary of IS Audit findings
- **2. Detailed findings**
- a) **Detailed findings of IS Audit would be brought out** viz.
- *identification of flaws/ gaps /vulnerabilities in systems (specific to equipments/resources –*
- *name & IP address of equipment with Office & Department name),*
- *identification of threat sources, details of Servers/Resources affected*
- *identification of Risk,*
- *Identification of inherent weaknesses, etc.*
- b) Report **= classify Audit Units into Critical / Non Critical category** & assess category of **Risk Implication of Audit Observations** as CRITICAL/HIGH/MEDIUM/LOW risk based on impact.

- c) Various **checklist formats, templates designed & used for IS Audit as per scope, maybe included in report separately**
- **Servers ,** OS, RDBMS, network equipments, security equipments etc to provide **minimum domain wise baseline security standard /practices to achieve reasonably secure IT environment** for technologies deployed in auditee entity
- d)Reports **: substantiated with snap shots/evidences /documents etc.** from where observations were made

3. Critical Analysis & Recommendation

- a) Findings of entire IS Audit Process **= be critically analyzed & controls suggested as corrective / preventive measures for strengthening / safeguarding IT assets** against existing / future threats in short / long term.
- b) All observations/recommendation - have **specific references to SOPs, guidelines & industry best practices** with analysis & justification.
- c) Report contain= **recommendations for improvement in systems wherever required + alternate solutions(mentioning steps for implementing recommendations for closure**), if recommendations could not be implemented due to technical feasibility/business constraint.
- d) IS Audit reports (Hard & Soft copies) - be submitted in English

- a) HARD COPY: Neatly & robustly bound on good-quality paper
- b) SOFT COPY: CD/DVD containing IS Audit reports in MS-Word/MS-Excel/PDF formats **should be necessarily password protected/encrypted**
- **B. Presentation to CISO/Audit Committee, BOD, Targeted Group:**

✓ Presentation must be made to targeted group of officials of entity, explaining methods of assessment followed,

✓ weaknesses/vulnerabilities observed,

✓ recommended course of action

- IS Auditor may **provide customized material (PPT/PDF etc.) for circulation in entity** , to create awareness about information security & audit among employees of entity
- **Single Point of Contact**
- IS Auditor appoint SPOC, with whom entity will deal, for any activity

Risk Assessment Document

No	Category	Risk	Description	Process owner.	Control

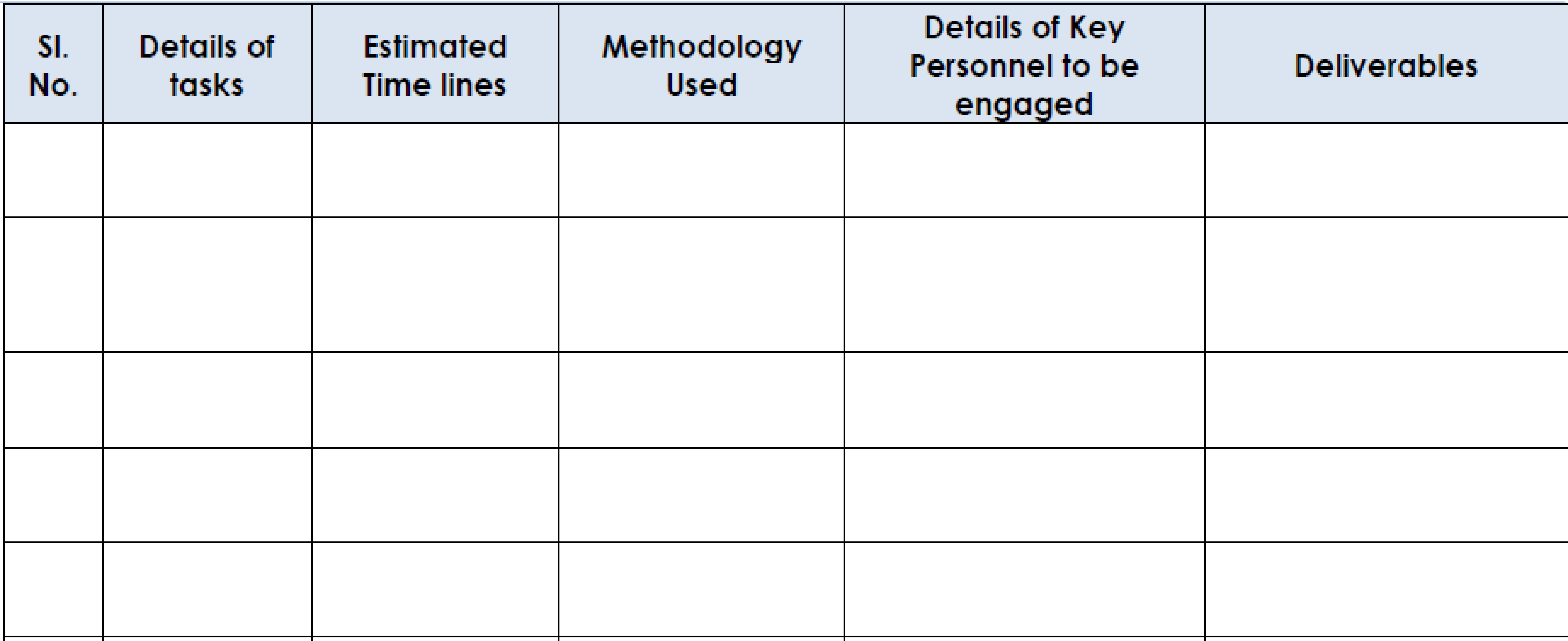
Means of controls

Example of Control	
Avoid	Disconnect from network, stopping services
Reduce	Backup site, Duplex system, Monitoring
Transfer	Insurance,
Accept	Enhancement of website

RCM (Risk & Control Matrix)

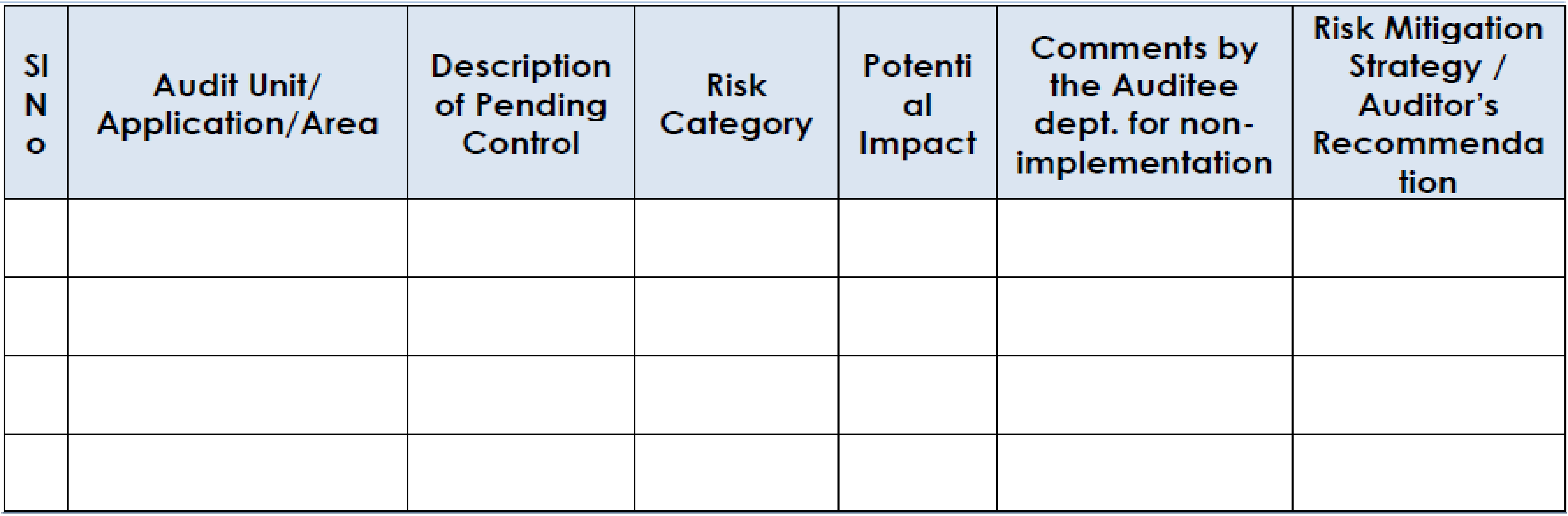
No	Type	Risk	Control and Procedure	Audit Procedure	Result & comment

Engagement worksheet



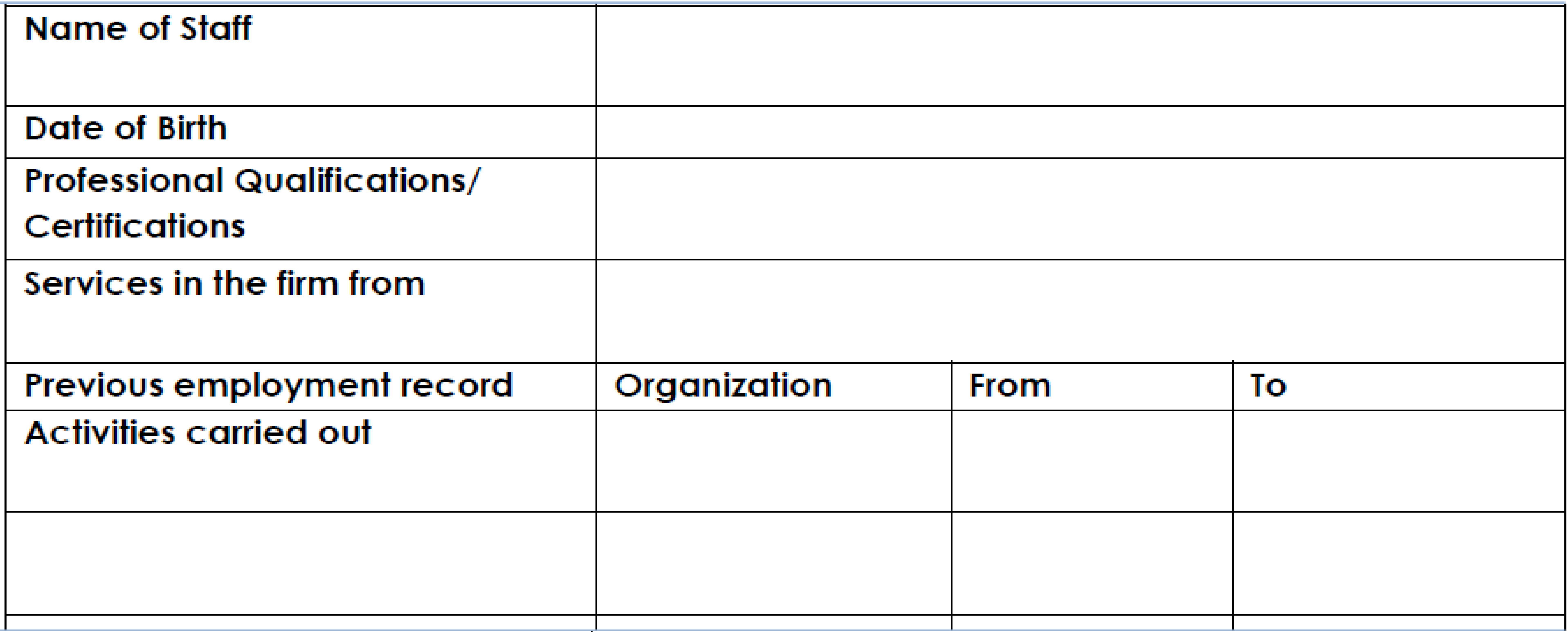
Sl. No.	Details of tasks	Estimated Time lines	Methodology Used	Details of Key Personnel to be engaged	Deliverables

Risk Assessment of IS Controls still pending (if any) from Previous Audit

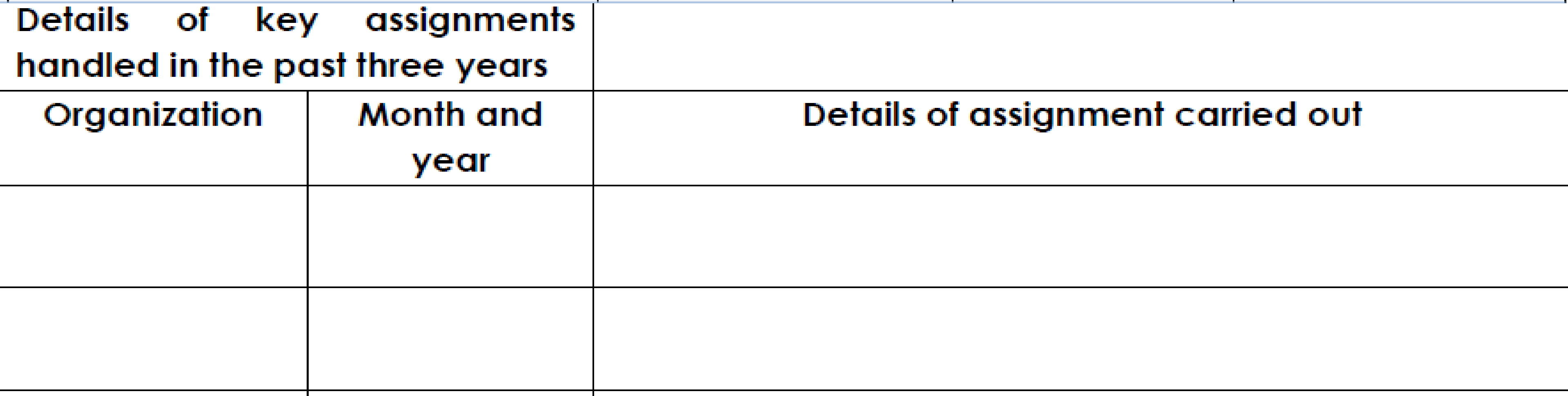


Sl No	Audit Unit/ Application/Area	Description of Pending Control	Risk Category	Potential Impact	Comments by the Auditee dept. for non-implementation	Risk Mitigation Strategy / Auditor's Recommendation

Resume of IS Audit Core Team Member / TL



Name of Staff			
Date of Birth			
Professional Qualifications/ Certifications			
Services in the firm from			
Previous employment record	Organization	From	To
Activities carried out			



Details of key assignments handled in the past three years		
Organization	Month and year	Details of assignment carried out

IS Audit Report – Templates
Part 1

Auditee
Organization :
Location / Address :
Area/Process/Function :
Process Owner / Coordinator :
Background : -Business : -IS Environment

Part 2

IS Audit	
Scope :	
Methodology :	
Executive Summary :	
Conclusions & Road Map :	

IS Audit Record
List of personnel interviewed :
List of evidences verified / obtained :

Part 3 - Audit findings & observations

No.	Observations / Findings	Requirements	Recommendations
1.			
2.			
3.			
4.			

IS Audit Report Observations
Petroleum sector = (ERP- SAP)

- Client not communicated IT roadmap to all levels of organisation.
- Client not been able to provide adequate training to all users
- Client = failed to appreciate possible risks of not keeping off-site data back up at site(s) other than PDC before ‘go-live’
- Cases of breakdown of leased links interrupting business transactions occurred at sites
- Primary Disaster Recovery Centre within same premises as of PDC , exposed to same immediate risks of physical disaster.
- Data loaded on SAP = authorised only by Middle Management & not by HOD of each site

. IS Audit Observations
Metals & Mining sector : ERP : Oracle

- IS Audit : implementation of Oracle e-Business Suite (EBS)
- 1. IT policies
- Client not formulated any IS Policy stating user classification
- for profile creation, password policy, number of failed login attempts, etc.
- Risk : system exposure to threats of unauthorized usage & loss of data
- 2. Logical access control
- Many application user accounts kept with default password against SOP of Secure Configuration Guide for Oracle E Business Suite, of Oracle Corporation
- *Unauthorised login activity- IS Audit observaions*
- User ids of few users were logged in when original user was absent or on leave indicating possibility of user id being shared.
- 3. Secure Configuration Guide for Oracle E-Business Suite, max no of failed login attempts per day = configured as 5.
- IS Audit observation : unsuccessful logins not being monitored as significant no of failed login attempts noticed under various user ids

– Real Estate

- **IS Audit of HR module in SAP R/3 System**
- Deficiencies in customisation, lack of input controls – Impact = in erroneous & incomplete data affecting data integrity, dependency on manual controls
- ***Reimbursement of conveyance for official use***
- • Vehicle numbers against reimbursements not entered as it was not made mandatory to enter vehicle numbers = Risk : incomplete data.
- • System accepted invalid registration numbers & reimbursements continued to be made against them.
- • Inbuilt controls to restrict reimbursement to single vehicle at a time were bypassed & 2 vehicles allowed to be mapped against an employee at a time.
- ***Dependency status***
- Marital/employment status of daughters deciding dependency not monitored through system due to non updation of such status in system.
- SAP R/3 not customised completely & business rules mapped inadequately

Tehelka Ltd : Petrochem
ERP : RAMCO e Applications System

- **IS Audit observations :**
- 1. Procurement processes <u>not linked & led to absence of audit trail</u> in system.
- 2. <u>Non integration of RAMCO e Applications system</u> among various units = in manual intervention
- **Risk =** data entry errors
- 3. <u>Lack of input controls</u> & validation checks
- **Risk =** data incorrect, incomplete & unreliable
- 4. User identities (IDs) <u>not linked</u> with Employee ID
- **Risk =** absence of any control ensuring accountability