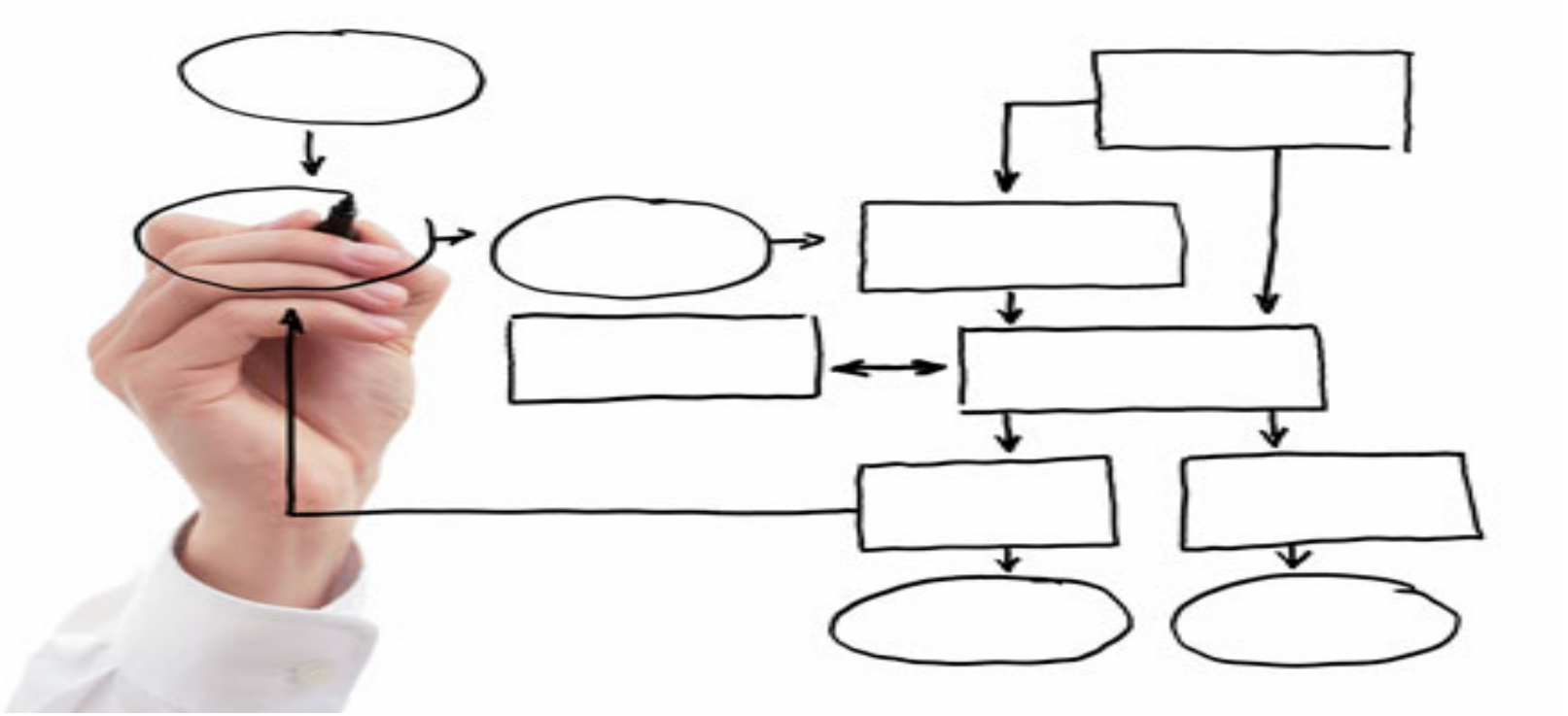
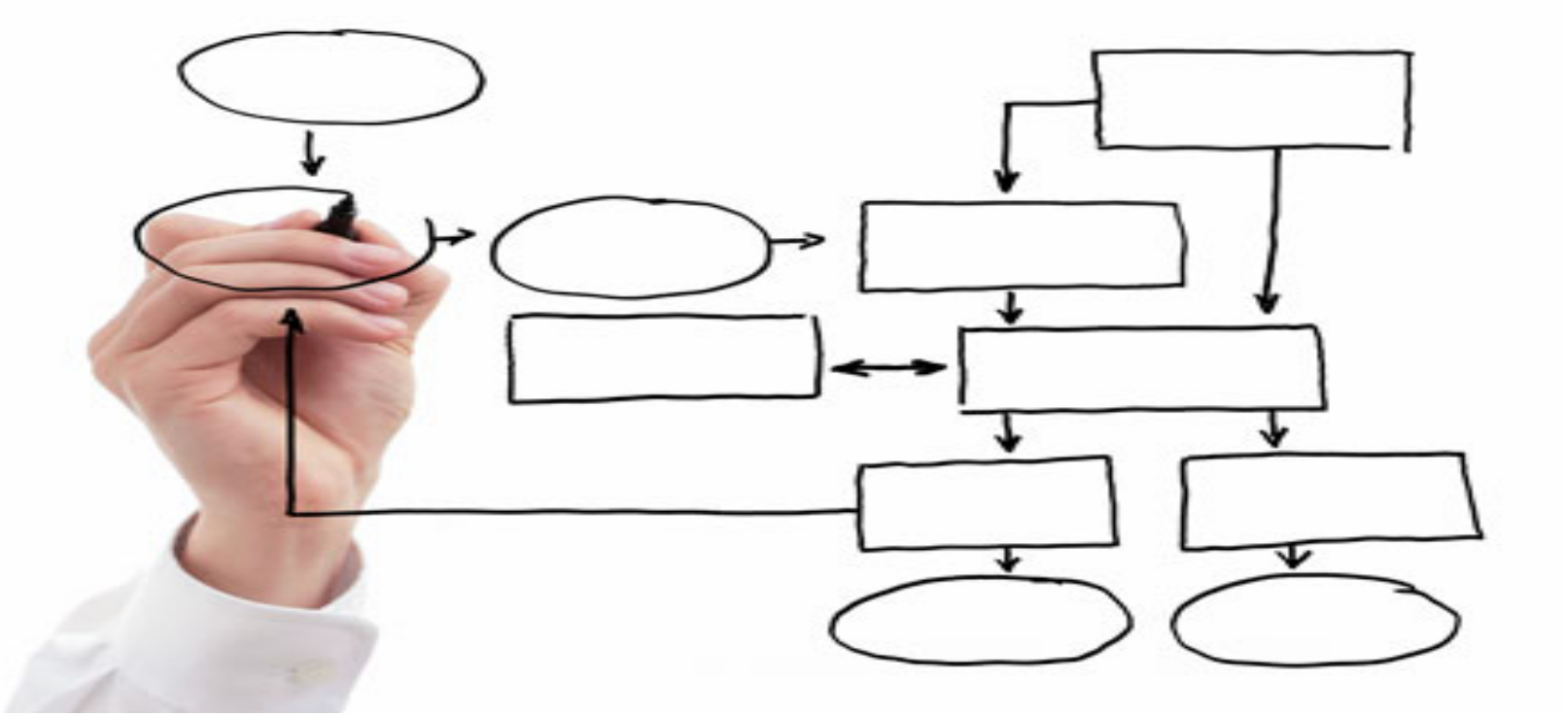


MIS 5121: Business Processes, ERP Systems & Controls

Week 10: *Data Migration, Segregation of Duties (SOD) 2*

FOX | MIS
Management Information Systems

Edward Beaver
Edward.Beaver@temple.edu
ff



MIS 5121: Business Process, ERP Systems & Controls

Real World Control Failures:

By: RAVI SHARMA

FOX | MIS
Management Information Systems

Control Failure: 2G Scam

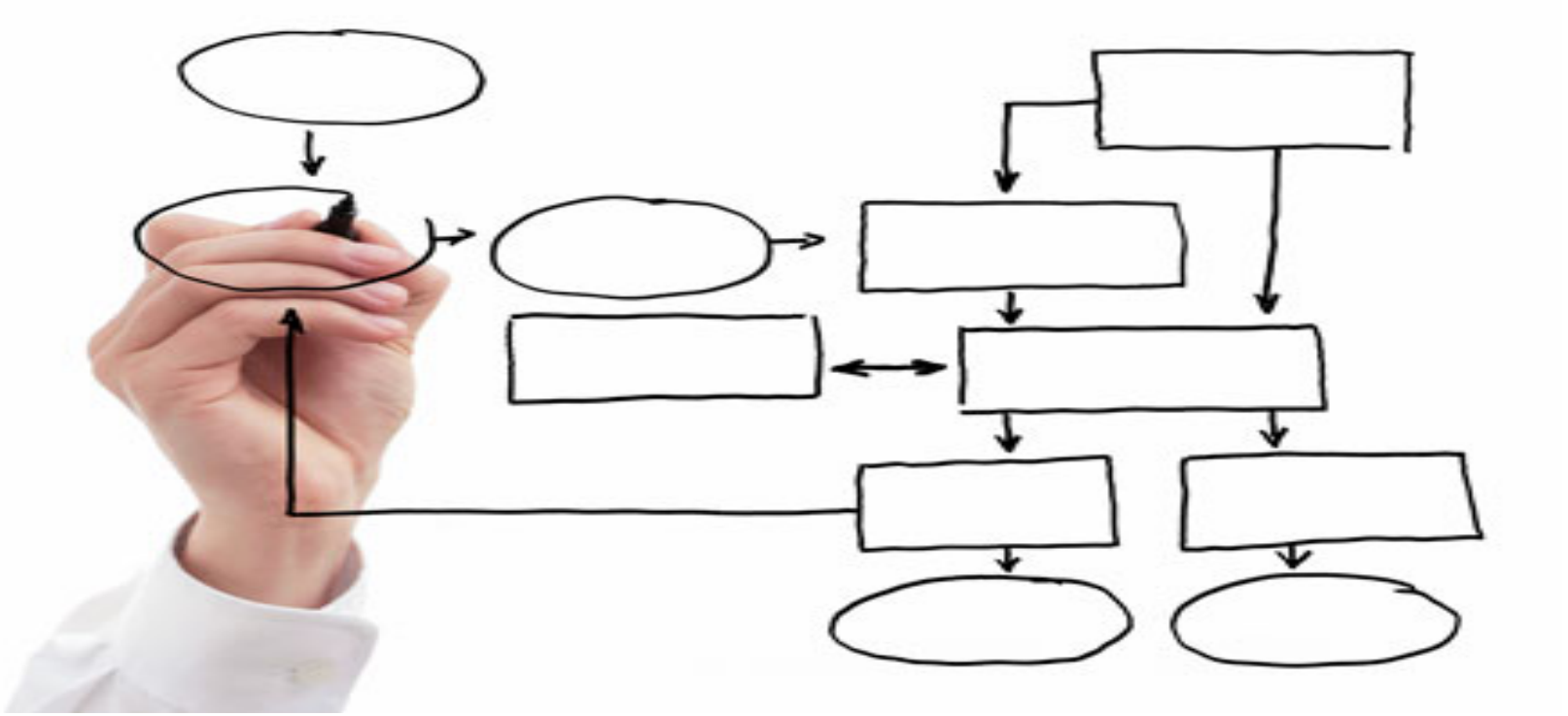
- Background:
  - In 2008, Indian Government started granting licenses for 2G spectrum on FCFS basis at 2001 price
  - Several laws were violated and bribes paid to favor certain firms
  - As per CAG, licenses were granted to ineligible corporations and with no experience in telecom sector
- Control Failures:
  - Rules were changed midway to favor some companies. It was changed only by one minister.
  - Serious financial implications and recommendations were overlooked
  - Officers were coerced into approving recommendations
  - The concerned minister did not consult finance ministry which was a norm
  - The concerned minister even circumvented the Prime Minister's letter suggesting transparency
  - Policies were modified without consultation or approval to enable applicants to meet the application deadline.
- Results:
  - A total loss of $30 billion
  - Supreme Court cancelled the allotment of all 122 2G licenses to all ineligible companies
  - Imposition of fine on many reportable companies.
  - Some cabinet ministers, many bureaucrats and company executives were arrested and sent to jail.
  - PM was accused of dereliction of duty
  - Congress after 10 years of rule lost the election badly and was reduced to 50 members in 350 seat parliament

Control Failure: 2G Scam

- What Could / Should those in Authority Have Done Different?:
  - Prime Minister should have shown the sense of duty and despite aware of the irregularities did not sack is minister. This should not have had happened.
  - Policies should have been followed. And any change to policies should have been approved.
  - Recommendations from telecom regulatory should have been flowed and Prime Minister should have intervened
  - The officers and bureaucrats should not have let them be coerced and complained to the higher ups.
  - When Prime Minister saw his suggestion not followed, he should have intervened and taken the minister to task.

- Reference:
- https://theconsiglieres.wordpress.com/2013/03/11/the-2g-scam-a-short-summary/
- http://indiatoday.intoday.in/story/what-is-the-2g-scam-all-about/1/188832.html

- Fun Fact:
- The then law minister accused the CAG saying there was no loss and gave a bizarre “zero loss theory” to save government's face. Superme Court discredited the theory.
- In 2011 Time ranked the scam second on their "Top 10 Abuses of Power" list, behind the Watergate scandal.



MIS 5121: Business Process, ERP Systems & Controls

Real World Control Failures:

By: Yue Zhang

FOX | MIS
Management Information Systems

Control Failure: HSBC-Money Launder

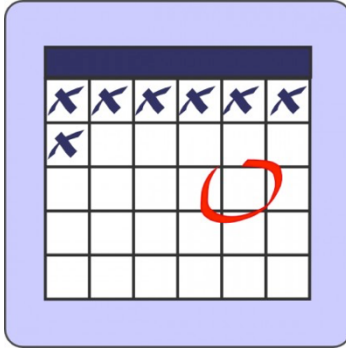
- Background:
  - HSBC, the largest financial institution in Europe
  - The money laundering linked to terrorism and drug deals, could result in HSBC paying fines of up to $1 billion
- Control Failures:
  - Treated some high-risk affiliates like low-risk clients.
  - Had inadequate and unqualified staff who received poor training
  - Cleared obviously suspicious bulk traveler's cheque transactions.
  - Failing to exit relationships with potential links to terrorist financing.
- Results:
  - HSBC pays record $1.9bn fine to settle US money-laundering accusations
  - A five-year agreement with the US department of justice
  - Avoid being criminally prosecuted
- What Could / Should those in Authority Have Done Different?:
  - Effective training and education of all staff involved in AML is essential
  - Leadership starts at the top
  - Audit to the controls

Control Failure: HSBC

- Reference:

- http://www.int-comp.com/ict-views/posts/2012/7/18/hsbc-money-laundering-failures-5-points-we-must-all-learn-for-a-start-aml-is-not-just-a-process/
- https://www.washingtonpost.com/business/economy/senate-report-criticizes-hsbc-for-money-laundering-inadequate-monitoring/2012/07/16/gJQABhqXpW_story.html
- http://www.bankdirector.com/committees/governance/jpmorgan-and-hsbc-time-to-refocus-on-internal-controls/

MIS 5121: Upcoming Events



- Exercise 4 (Segregation of Duties)-*Due: March 31*
- Reading Assignment 6 – *Due: April 3*
- **Exam 2** – In class*: April 3*

  Content of Exam

  – Review Items included in Week 7 Lecture notes
  – Topics listed on any 'Overview' / 'Review' slides in Weeks 7 – 10 (today's) lecture notes
  – You can bring 5 pages (single sided) of notes to the Exam

- Guest Lecture: Auditor's Perspective - *April 18*

MIS 5121: Auditor's Visit Topics

- _____
- _____
- _____
- _____
- _____
- _____

Key Information Technology Risks

- System Security
- Information Security Administration
- Background Processing (Batch vs. foreground: real-time)
- Powerful User ID's and Profiles
- Instance Profile Security
- Change Management (including Logs and Traces)
- Table Security
- Data Dictionary, Program and Development Security
- Transport Security
- Change Control
- **Data Migration**
- **Data Interface**
- Firefighter access

Data Migration / Interfaces: Control Concerns

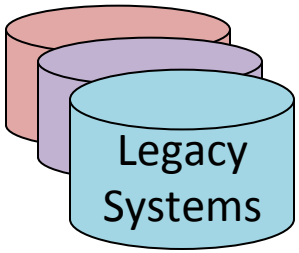
Data Migration (Conversion)

Migration Magic

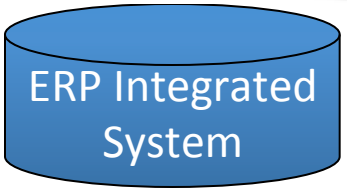
Legacy Systems

'New' ERP System

Data Migration: Flow

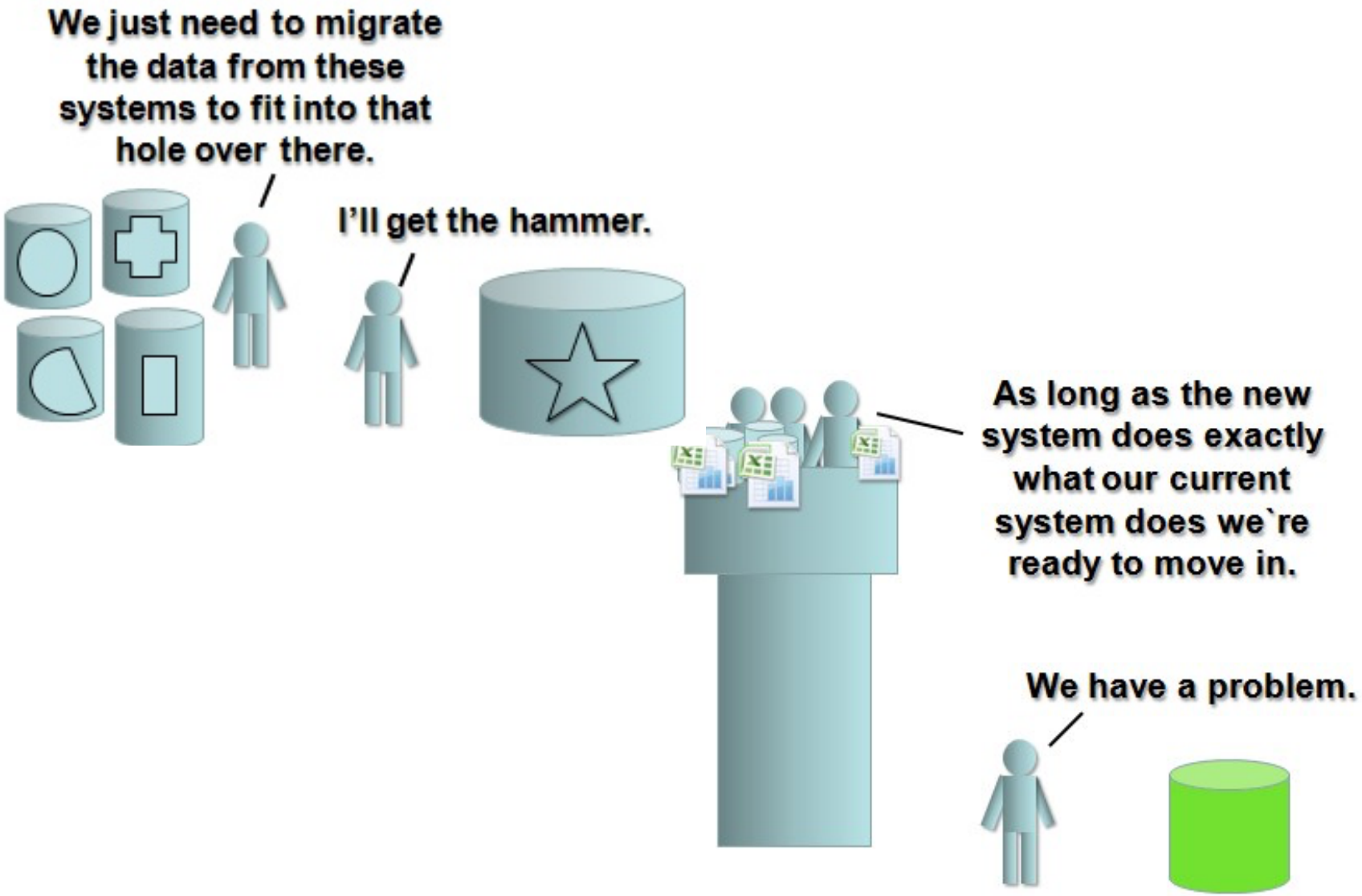


Data Migration



- Extract
- Clean
- Augment
- Transform
- Validate
- Load
- Reconcile

Data Migration – How??



Data Migration: Process

Analysis

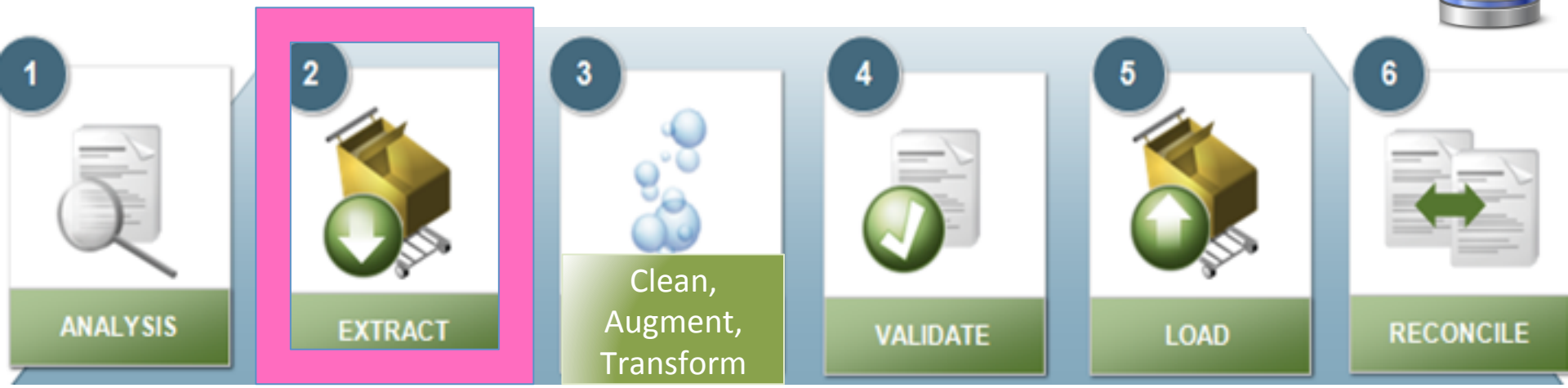
- Solid understanding of both source and destination systems (data structure, how used)
- Differences in data layout, use between systems
- Differences in data definitions

Data Migration: Process

Analysis

- Solid understanding of both source and destination systems (data structure, how used)
- Differences in data layout, use between systems
- Differences in data definitions

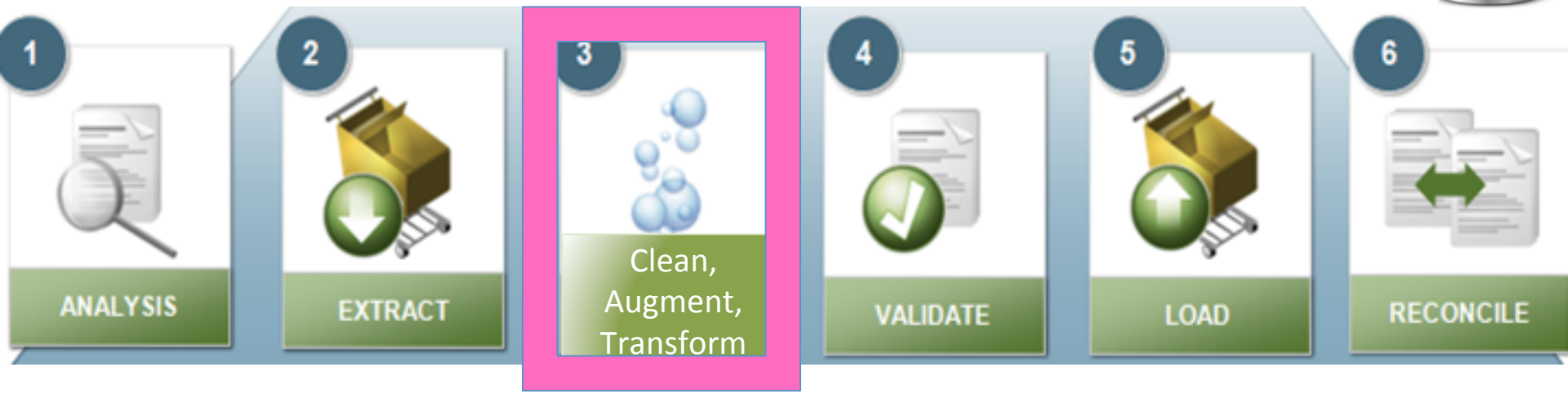
Data Migration: Process



Data Mapping

- Source data fields to fields, format required by new system
- Often involves logic (mapping rules)
  - From / to transformations
  - Transformation 'rules'
- Scope: what data will be migrated vs. not (history, activity level, relevance, etc.)
  - Master and 'open' transactions
  - History?

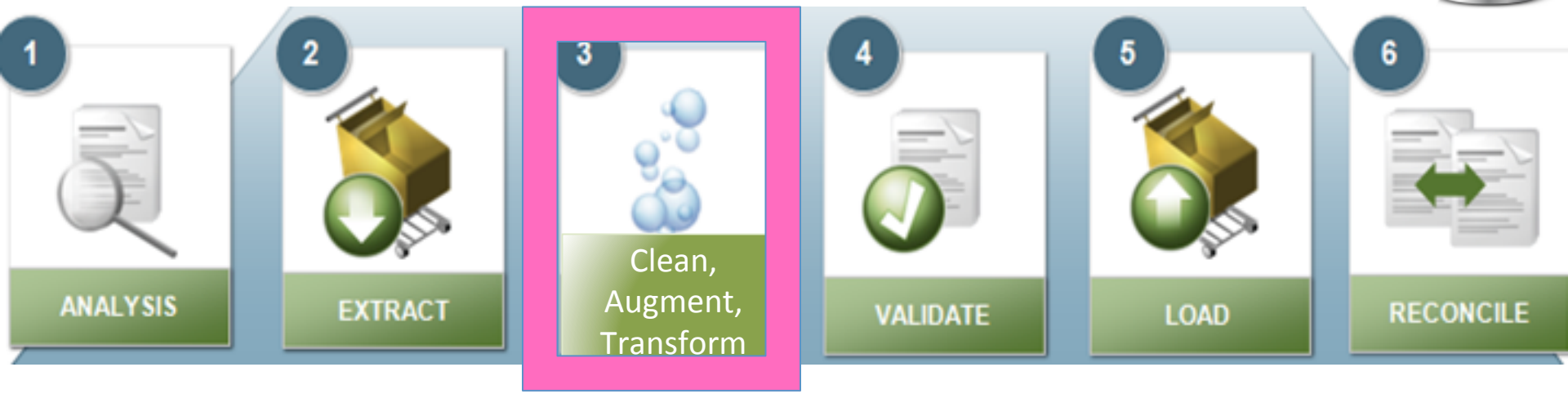
Data Migration: Process



Data Conversion (Complex)

- Extract programs
- Transform programs
- Augment (as needed)
- Load Programs
- Leverage a tool (e.g. BackOffice)

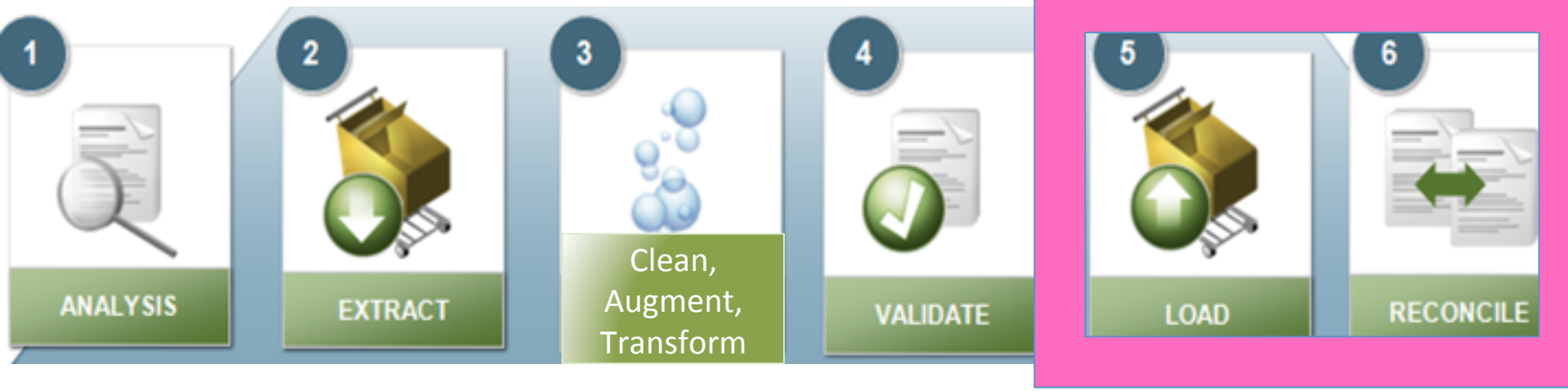
Data Migration: Process



Data Clean-up

- Critical for successful migration (can move any data -> moving quality data that is business ready)
- Cleanse outdated, incorrect information from legacy systems
- Requires solid understanding of source data and destination requirements
- Define ‘rules’, requirements of high quality, business ready data

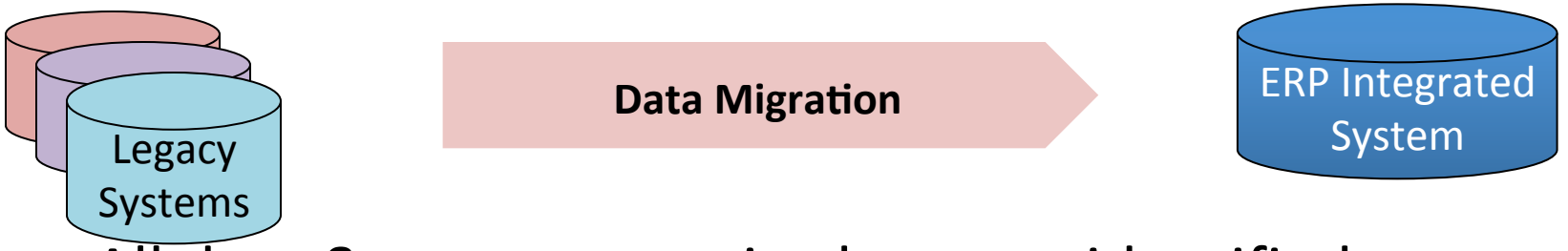
Data Migration: Process



Data Load and Reconciliation

- Meticulous planning and focused project management
- Dependencies (sequencing) (load and reconcile before proceed)
- Must be reconciled to legacy system (assure accurate, complete)
  - Records, field values
  - Quantities and $$ value
- Standard / custom reports – not difficult but critical

Data Migration: Risks



- All data & sources required are not identified
- Data dependencies not understood (load sequence)
- Data gaps exist
- Translation rules not fully understood to migrate data
- Legacy data is not complete or inaccurate
- Data relationships in legacy data compromised during migration
- Data transfer data errors not discovered timely and resolved

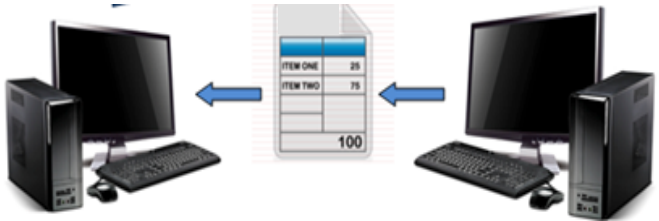
Data Migration: Control Objectives

- Data migrated from legacy systems is Accurate
- All data migrated to target system is Complete
- Synchronize data between legacy and target systems
  - Scope / Data 'Freeze'
  - Dual Maintenance
- Data migrated to target system is recoverable and auditable

Data Interfaces

Data Interfaces: exchange data from one system to another

Goal: accuracy, completeness and timeliness of data - esp. those that impact financial results

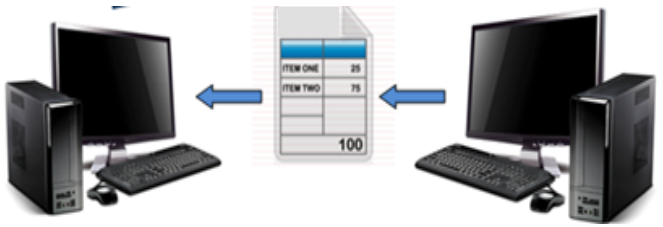


Data Interfaces: Process

Timing / Scope

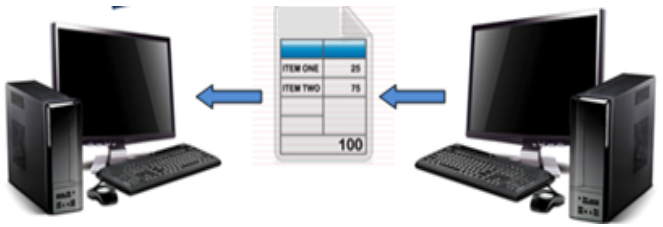
- Event Driven (e.g. transaction)
- Scheduled / periodic
- Initiation (Start of process sequence)

Systems could be internal or External

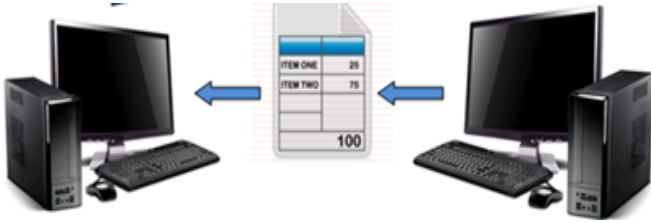


Data Interfaces: Process

- Extract from source system
- Transmit data to destination / target system
- Receipt of interfaced data by target system
- Verify received data is correct (e.g. right format), valid and complete
- Staging data prior to upload to target system
- Import into target system
- Validate data once imported



Data Interfaces: Risks



- Inaccurate or incomplete data extracted or pass over interface
- Duplicate data is extracted
- Data not extracted or passed timely
- Exceptions and errors are not detected or acted on to resolve
- Data not extracted in appropriate sequence
- Inbound interfaces with errors cannot be backed out
- Sensitive data not protected during transmission
- Data modified before, during, after transmission

Data Interfaces: Control Focus

- Adequate detection and prevention of duplicate data Processed
  - Some data (e.g. master data) just updated with latest value extracted (e.g. by Key match)
  - Transaction & Event data requires more duplicate controls
- Data sequencing and timing are monitored. Failures are reviewed, root cause identified and corrective actions put in place
- 'System of Record' clearly defined and process / application respects this
- Exceptions and errors are detected and procedure / method to review and resolve exists
- Sensitive data is sent via encrypted or secure channels only
- Adequate security and controls exists in source and target systems to prevent unauthorized modifications to data.

Data Migration / Interfaces Overview

Data Migration (typically Project oriented)

- Risks (Few)
- Controls (Few)

Data Interfaces (usually on-going)

- Risks (Few)
- Controls (Few)

Security and Segregation of Duties (SOD) Real World Examples

SOD / SAT Risk Analysis Review

- Following tables are selected real entries from Real Annual Security Review (mature system – 10 years)
- I was responsible person (Order to Cash Process Steward)
  - My team took raw results and analyzed
  - I was responsible to sign off on the results
  - Point person for audit challenges
- SOD: Segregation of Duties (Risk: User with ability to ___ and to ____)
- SAT: Sensitive Transaction Access

SOD Risk Analysis Review

Risk Description	Level	Process	Role	Comments
ZS10 : Create/change a sales doc and generate a billing doc for it	High	OTC	R/3 173 CSR OR&H - Chem APR	New CSR position. Same mitigating controls exist per control 1100-417 for this position
ZS03 : Users with the ability to process outbound deliveries and process customer invoices (SD)	High	OTC	R/3 185 CSR with Pricing/Billing/ Shipping	Mitigated Position - GRC Report Showing Incorrectly
ZS10 : Create/change a sales doc and generate a billing doc for it	High	OTC	R/3 175 Pricing Admin w/Rebates & Contracts	Access limited to ProForma (non-accounting) invoices only

SOD: Example of Mitigating Controls

Key Control	Risk	Testing Results	Pass/ Fail	Mitigating Controls
1100-417 Identify users who have access to Process Sales Orders and Process Customer Invoices (SD)	Enter / change order fraudulently (VA01) and enter incorrect customer invoice to hide (VF01)	Add POS173 to mitigated position list (e.g. CSR positions). POS175 issues mitigated by restricting to Proforma billing documents only	Pass	**Manual controls**: - BU Fin Mgr reviews monthly actual income statement vs. forecast and historical information - Monthly S&OP meetings held to discuss analytical review of monthly results vs. targets - BU Fin Mgr performs a monthly review of financial results for unusual activity - Review Manufacturing Variance Analysis and capitalization of the variances as appropriate. - Budget vs. actual analysis

SOD / SAT Risk Analysis Review

- Risks reported via SAP GRC Tool
- 'Risks' were company versions of SAP supplied risk reporting SOD and SAT rules (adjusted per internal and external auditor agreement – e.g. company configuration, other controls, etc.)
- Comments were results of analysis. e.g.
  - If solution is agreed (e.g. mitigating controls exist …) it is documented to exclude from future reports or Risk rule updated to exclude
  - Risk rule too broad – agreed low risk or mitigated risk scenarios
  - Fix a found SOD Situation

SOD Risk Analysis Review

Risk Description	Level	Process	Position	Comments
ZS21 : Cover up shipment by creating a fictitious sales doc	High	OTC	R/3 116 Toll Man Production Planner - Helena Chemicals	VL02, VL02N not in position - Investigate where access derives from (back door)?
ZM08 : Users with the ability to perform goods receipts **and** goods withdrawal transactions.	High	OTC	R/3 112 Product/ Process MD Owner	Mitigated Position - GRC Report not excluding it
ZM10 : Users with the ability to perform goods receipts **and** process inventory documents(IM)	High	OTC	R/3 173 CSR OR&H - Chem APR	OK - access is to complete inventory checks (no inv. postings allowed). Needed for consignment processing

SAT Risk Analysis Review

Position	Role	Critical Action	Risk Description	Comments
R/3 154 Customer and Material Master Maintenance (REST)-AGBL	ZR:MD00:CUST_MTL_MNT_EXP-AGBL	Create Customer (XD01)	ZS12 : SAT - Users with the ability to maintain customer master data.	Ok
R/3 868 Intercompany Specialist w/Bank Stmt Upload-AGBL	ZR:FI00:INTER_SPL_WBANKST-AGBL	Create Condition (VK11)	ZS13 : SAT - User with the ability to maintain pricing condition records	Action: Change Access to be limited to Inter-company conditions only
R/3 872 Accountant I - Espana, S.A.	ZR:FI00:ACCT_MGR_AM-ESP	Create Condition (VK11)	ZS13 : SAT - User with the ability to maintain pricing condition records	OK - access limited to Inter-company conditions only

SAT Risk Analysis Review

Position	Role	Critical Action	Risk Description	Comments
R/3 031 System Billing Job Authority - Global	ZR:IT00:SYS_BILLJOB_AUTH-GBL	Change Sales Order (VA02)	ZS14 : SAT - Users with the ability to process sales orders/contracts.	Investigate Why - should not occur
R/3 162 Site Purchasing Expert-AAPR	ZR:PPUR:SITE_PURC_EXPERT-AAPR	Create Sales Order (VA01)	ZS14 : SAT - Users with the ability to process sales orders/contracts.	Action: Access OK - wrong derivation (limit to non-standard order types)
R/3 175 Pricing Admin w/Rebates & Contracts-OMX	ZR:OCPR:PRCADM_REB_CONT-OMX	Create Billing Document (VF01)	ZS16 : SAT - Users with the ability to process customer billing documents	OK - access limited to ProForma invoices

SAT Risk Analysis Review

Position	Role	Critical Action	Risk Description	Comments
R/3 037 Production Support position for FIN	ZR:SUPPORT_FIN	Post with Clearing (FB05)	ZS17 : SAT - Users with the ability to post incoming payments.	Investigate: Ask Finance
R/3 175 Pricing Admin w/Rebates & Contracts - APC APR	ZR:OCPR:PRCADM_REB_CONT-APCA	Change Customer (Sales) (VD02)	ZS19 : Users with access to perform customer master data changes	OK - Configuration limited change access allowed

Segregation of Duties (SOD) Overview

- SOD Definitions
- SOD Implementation Concepts
- SOD Examples
  - 1 or 2 in each area
  - How phrased

- SAT (Sensitive Access Transaction) Concept
  - Definition
  - 1 or 2 examples

Break Time

Segregation of Duties Exercise 4

- Agenda
  - Last Class *(March 21)*: Steps 1 – 2 (Risks / Control & Organizational design with SOD)
  - This Class *(March 28)*: Step 3 - 4 (Paper process to system process with SOD and authorizations to design)
  - *Due March 31 11:59 PM:* Assignment Submission

Segregation of Duties Exercise 4

Step 3:

a) Examine the list of ERP System documents required to execute the process (from Step 2)

b) Develop an authorization matrix for each document and each organization position who uses document (e.g. specifies the extent of computer access for each of the employees)

Segregation of Duties Exercise 4

Step 4: Examine the SAP authorizations where you will see how to establish rules that enforce segregated duties.

a) *Tools -> Administration -> User Maintenance -> Role Administration -> Roles* (**PFCG**) View predefined roles and related authorizations (Page 18 of guide)

b) Answer questions related to your review / analysis

Extra Slides

Segregation of Duties Exercise 4

- Primary learning objectives are:
  - Experience how to specify controls to address known business risks
  - Review and assign positions appropriate to handle process tasks
  - Make choices to manage the tension of SOD controls vs. excess personnel costs
  - Translating process tasks assignments to computer task assignments
  - Creating authorization design details necessary to implement security that enforce SOD

Segregation of Duties Exercise 4

Steps

1. Determine appropriate controls to mitigate defined business process risks. You will also be asked to assess additional risks associated with this business process.
2. Using the risk analysis as a base, examine assigned positions within the organization to be sure that there is adequate segregation of duties without incurring excess personnel costs.
3. Develop an authorization matrix that specifies the extent of computer access for each of the employees designated in the previous step (transitioning from paper-based to integrated ERP System environment)
4. Examine the SAP authorizations where you will see how to establish rules that enforce segregated duties.

Segregation of Duties Exercise 4

Step 1: Determine appropriate controls to mitigate defined business process risks. You will also be asked to assess additional risks associated with this business process.

a) For first 5 listed risks – Identify from suggested list the top 3 Controls to use

b) Identify for GBI 3 additional risks for the process defined (an Order to Cash example). Then from suggested list choose top 3 Controls you recommend using

Segregation of Duties Exercise 4

Step 2: Using the risk analysis as a base

a) Examine matrix of assigned positions within the organization vs. each process task

b) Adjust (including adding positions) to be sure that there is adequate segregation of duties for the process without incurring excess personnel costs.