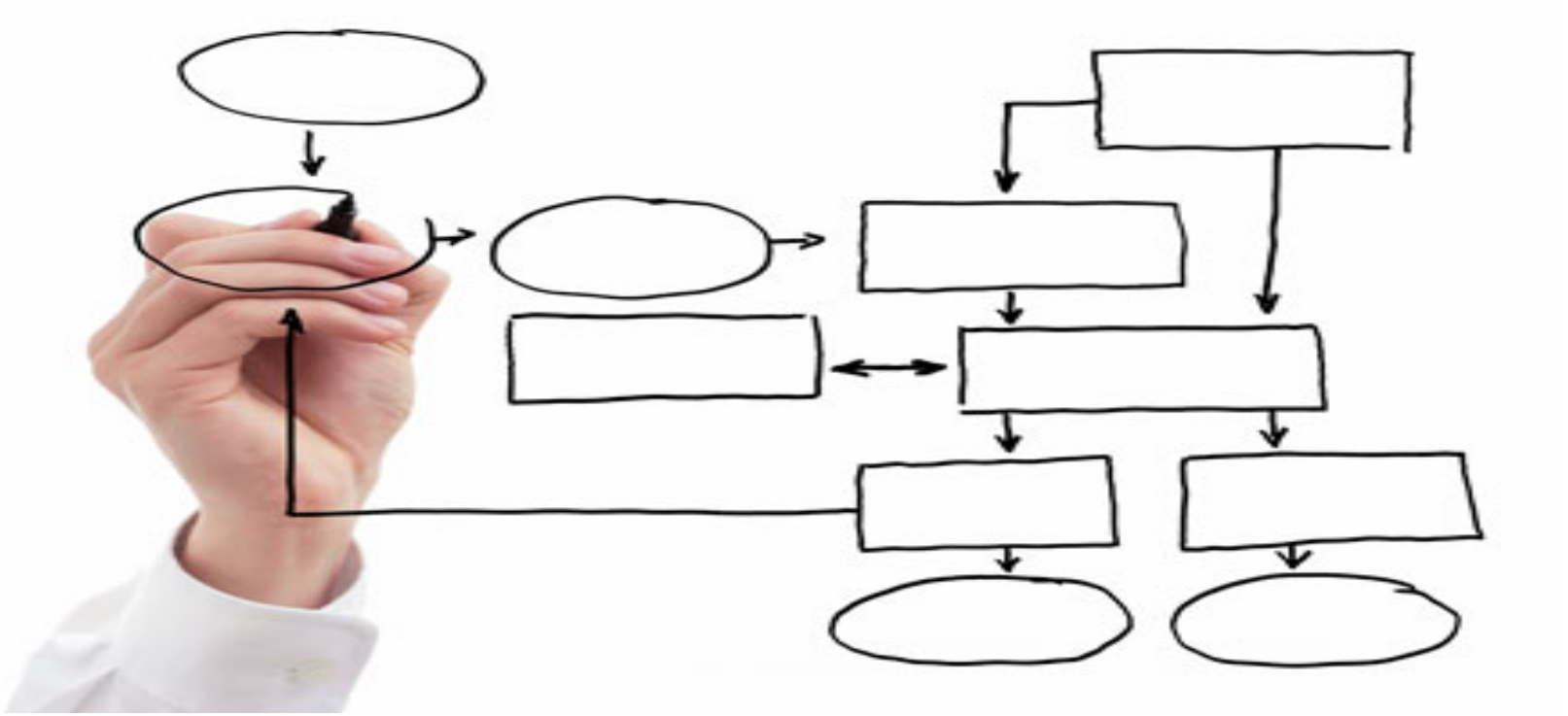


MIS 5121: Enterprise Resource Planning Systems

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

FOX | MIS
Management Information Systems

Edward Beaver
Edward.Beaver@temple.edu
ff

Special Guests

Kapish Vanvaria

- Ernst & Young
- Manager | Advisory Services
- Temple MIS Advisory Council

Shola Oguntunde

- Ernst & Young
- Senior Manager | Advisory Services
- SAP Subject Matter Expert
- Temple Alum

MIS 5121: Auditor's Visit Topics

- What are the general methodologies used for auditing?
- How do you classify risks?
- How do you review Segregation of Duties (modules vs. employees)?
- Have you personally detected a fraud scenario in your audit? If so, please explain
- How do you maintain your independence? Is that easy?
- What is your opinion on cyber-security laws being considered by the US government (CIA, CISA legislation)?
- How easy it it for an auditor to commit fraud?
- Does SAP provide good control environment vs. other systems (ERP, other)?
- Since SAP can be customized in so many ways, how does an auditor know what to audit when everything is different with each client?

Control Failure: Leandro Cinti's Presentation

- Background:
  - ❖
  - ❖
- Control Failures: 2006 – 2009
  - ❖
  - ❖
- Results:
  - ❖
  - ❖
- Reference:
  - ❖

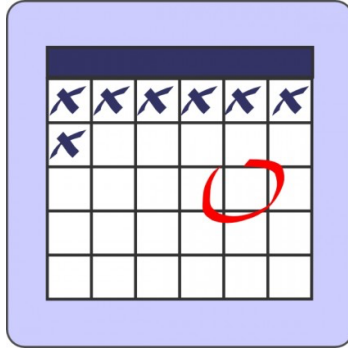
Control Failure: Anh Nguyen's Presentation

- Background:
  - ❖
  - ❖
- Control Failures: 2006 – 2009
  - ❖
  - ❖
- Results:
  - ❖
  - ❖
- Reference:
  - ❖

Control Failure: David Eve's Presentation

- Background:
  - ❖
  - ❖
- Control Failures: 2006 – 2009
  - ❖
  - ❖
- Results:
  - ❖
  - ❖
- Reference:
  - ❖

MIS 5121: Upcoming Events



- Reading Assignment 6 – *Past Due: March 29*
- Exercise 4 (Segregation of Duties) - *Due: April 2*
- Reading Assignment 7 - *Due: April 5*
- **Exam 2** – In class*: April 6*

  Content of Exam

  – Review Items included in Week 8 Lecture notes

  – Topics listed on any 'Overview' / 'Review' slides in Weeks 7 – 10 (today's) lecture notes

Data Migration / Interfaces: Control Concerns

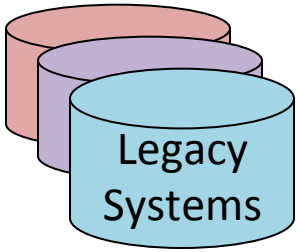
Data Migration (Conversion)

Migration Magic

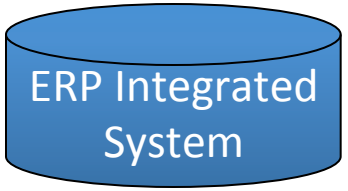
Legacy Systems

'New' ERP System

Data Migration: Flow

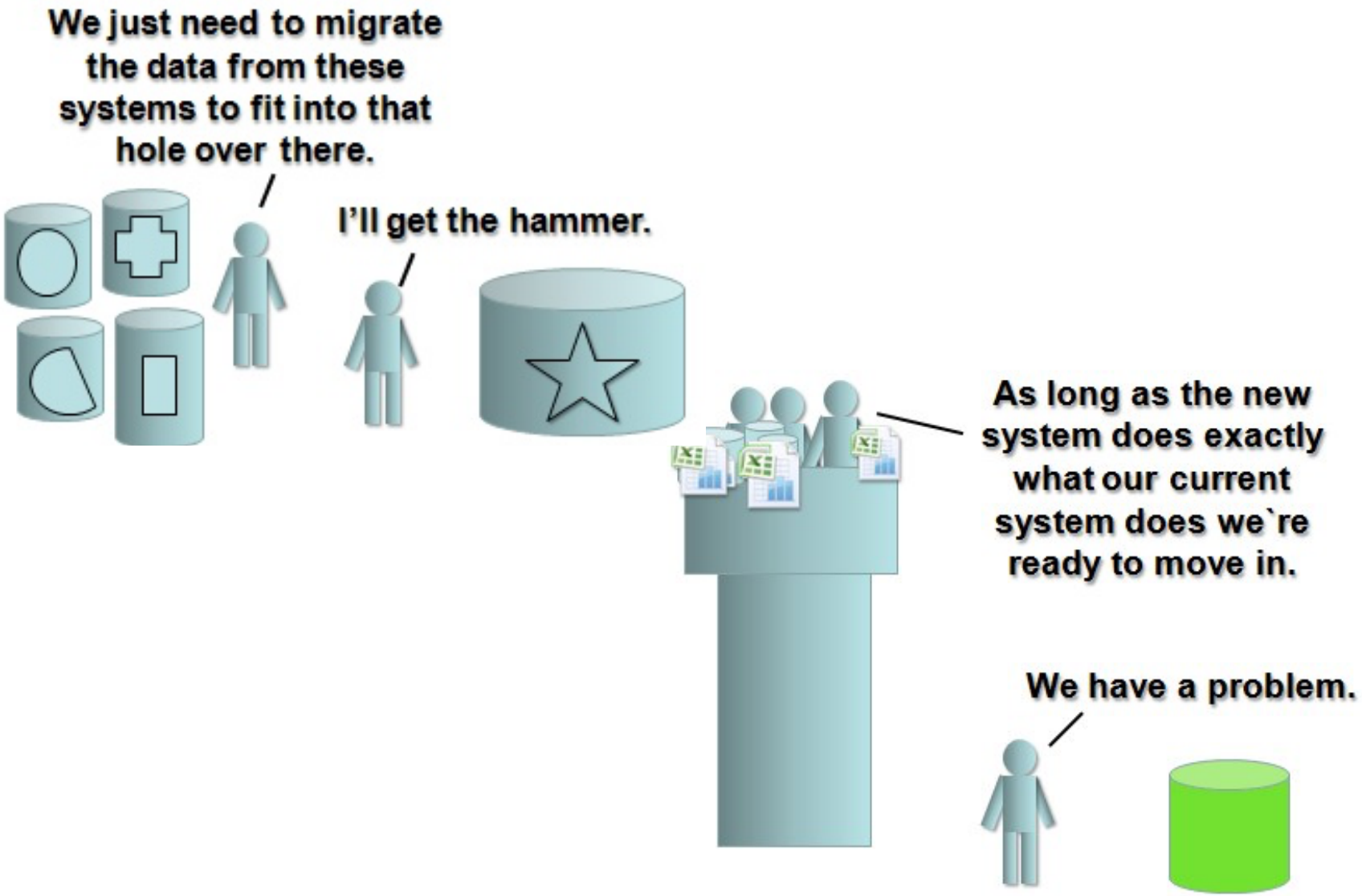


Data Migration



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

Data Migration – How??



Data Migration: Process

Analysis

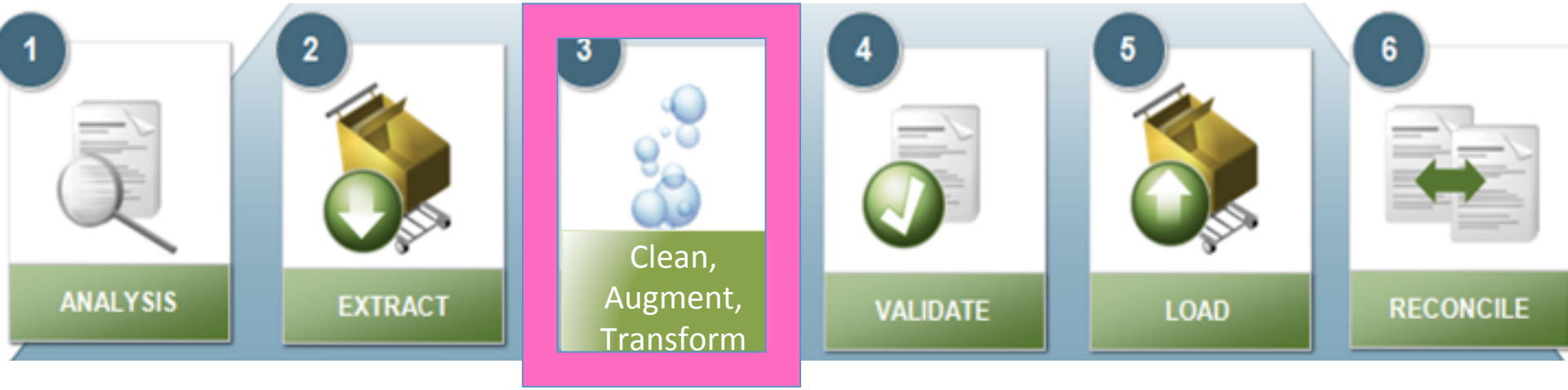
- Solid understanding of both source and destination systems (data structure, how used)
- Differences in data layout, use between systems
- Differences in data definitions

Data Migration: Process

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?

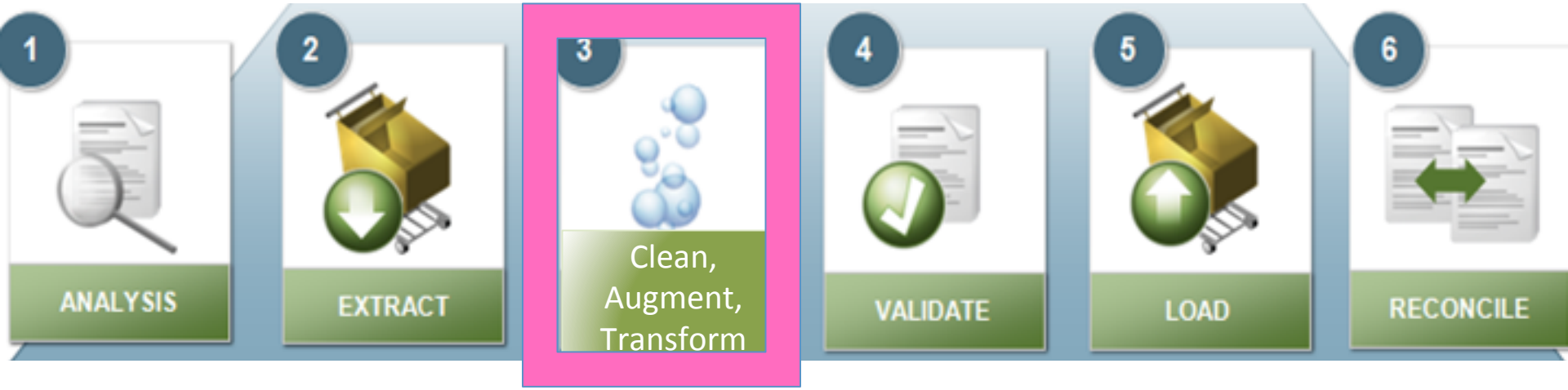
Data Migration: Process



Data Conversion (Complex)

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

Data Migration: Process



Data Clean-up

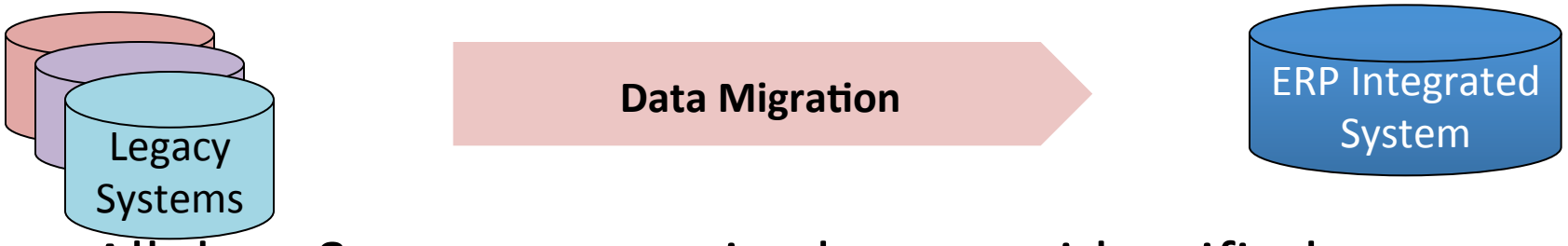
- Critical for successful migration (can move any data -> moving quality data that is business ready)
- Cleanse outdated, incorrect information from legacy systems
- Requires solid understanding of source data and destination requirements
- Define ‘rules’, requirements of high quality, business ready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

- 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
- Extract not duplicated
- 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 update with latest value extracted
  - Transaction 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 supports
- 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
- Controls

Data Interfaces (usually on-going)

- Risks
- Controls

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 (10 years mature)
- I was responsible person
  - My team took raw results and analyzed
  - I had to sign off on the results
  - Point person for 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 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 or mitigated risk scenarios
  - Fix a found SOD Situation

SOD Risk Analysis Review

Risk Description	Level	Process	Role	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 - Virsa 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

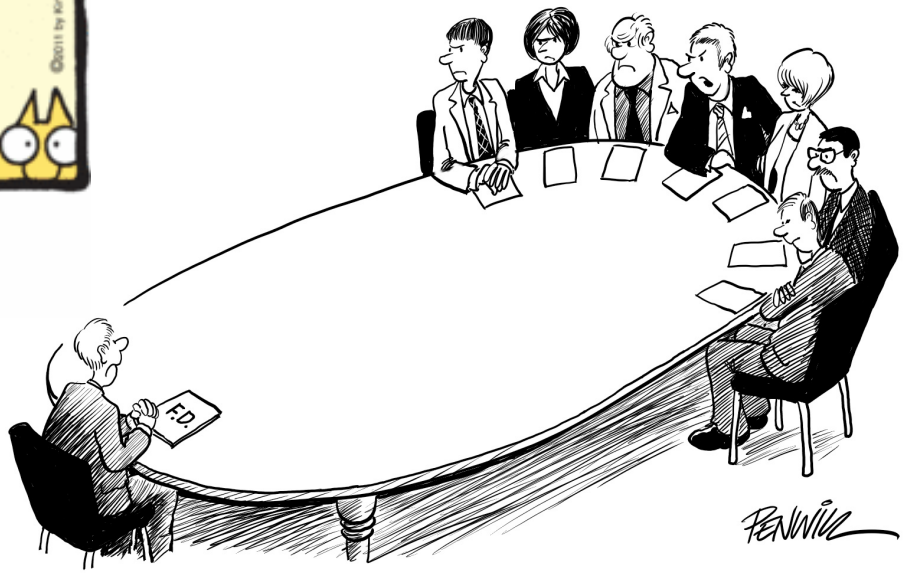
Position	Role	Critical Action	Risk Description	Comments
R/3 037 Production Support position for FIN	ZR:SUPPORT_FIN	Post with Clearing (FB05)	ZS17 : SAT - Users with the ability to post incoming payments.	Investigate: Ask Finance
R/3 175 Pricing Admin w/Rebates & Contracts - APC APR	ZR:OCPR:PRCADM_REB_CONT-APCA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

Success with Internal and External Auditing
My Personal Experience

"It went pretty well. The auditor took one look at my files and retired!"



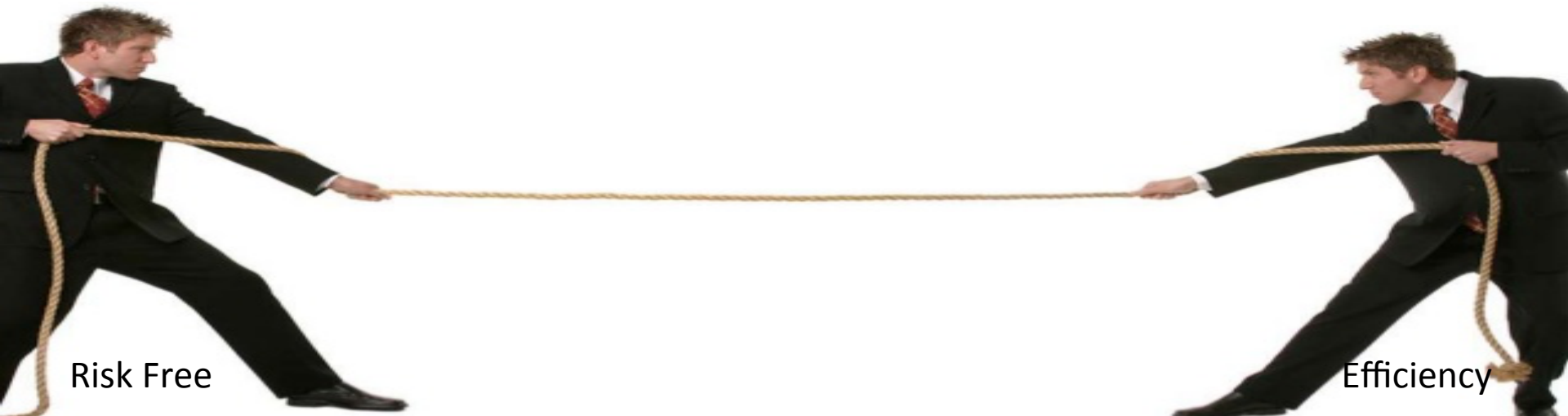
"WE DON'T WANT YOU TO VIEW THIS AUDIT COMMITTEE AS BEING IN ANY WAY CONFRONTATIONAL"

Success with Auditors

- Strong / Deep Knowledge
  - Process
  - Business / real world scenarios
- Able to Master the Details
- Understand Auditor perspectives
  - Job / Role to accomplish
  - Risks
  - Vocabulary

Success with Auditors

- Work Cooperatively
  - Balance the Tension: Know which side you're on and be an effective counter-weight
  - Focus on what's "best" for the organization



Assignment Questions

- **Can anyone who works in companies right now give examples of monitoring in their jobs? Is it continuous? Who administers the monitoring (if that's the right term)?**
- Why does monitoring controls counteract the breakdown of internal controls?
- Sometimes controls can have a negative impact on productivity so how do you determine if the control is worth the business loss?
- How is SAP outsourced – by function or process? What are the controls in place for this – and how are they monitored?
- What would be some of the potential negative consequences of not monitoring controls?

Assignment Questions

- What sources should be used to determine the threat/vulnerabilities that could affect company's operations?
- How does Benford's law come into play in SAP while configuring controls matrix or settings?
- What is the control baseline? Explain the concept of benchmarking for monitoring.
- If more controls and monitoring do not equal better control, how often should an organization review controls to assure they are efficient and compliant? How to assure that risk does not creep into pre-existing controls as they are updated, or when compensating controls are introduced?
- For the four-step monitoring process, should company put same amount of effort (time, resources, etc.) to each step or put more effort on the implement monitoring step?

Assignment Questions

- What do you think is a proper size staff of internal control monitors for a small company, medium size company, and a large company?
- *Currently the company may not be able to solely rely on automatic monitoring process. How to balance the manual monitoring and automatic monitoring?*
- *How does monitoring benefit the governance process?*
- What are some of the draw backs of using technology for monitoring internal controls?
- What is separate evaluation? How to evaluate?

Break Time

Segregation of Duties Exercise 4

- Agenda
  - Last Class *(March 23)*: Steps 1 – 2 (Risks / Control & Organizational design with SOD)
  - This Class *(March 30)*: Step 3 - 4 (Paper process to system process with SOD and authorizations to design)
  - *Due April 2 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

MIS 5121: Auditor's Visit Topics

- What does the auditor do to identify risks associated with SAP ERP?
- *Do you think the SAP P2P auditing process is too labor intensive to set-up and maintain for small to mid-size companies? Maybe a small scale ERP system would be better fit?*
- The security mechanisms in SAP look complex and safer than other systems (e.g. with rules, profiles, authorizations, etc.) However, has ahe implementation of SAP really reduced the chance or number of frauds (e.g. are there any statistics to support this hypothesis?)
- Within the financial accounting system of SAP, what area or field presents the most risk or greatest opportunity for fraud?

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.