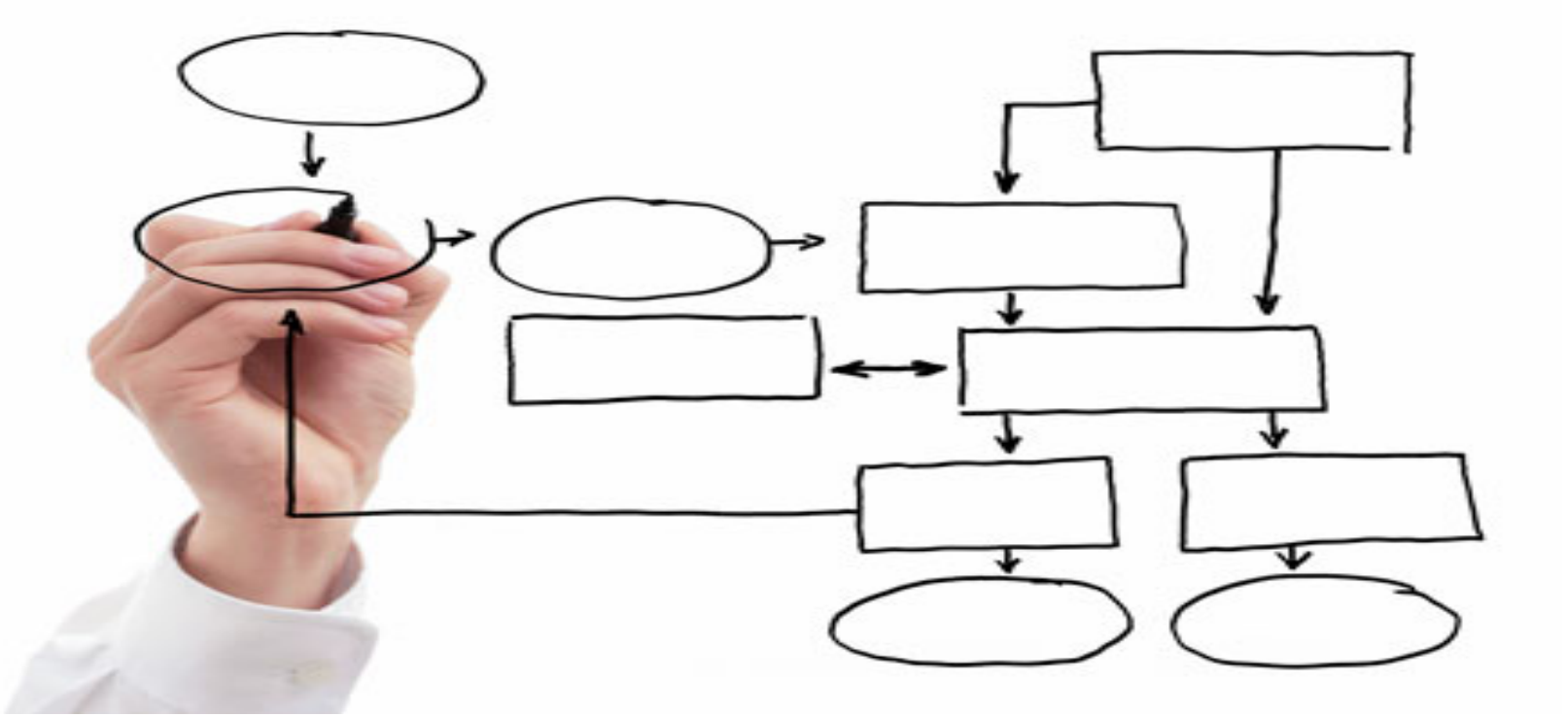


MIS 5121: Business Processes, ERP Systems & Controls

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

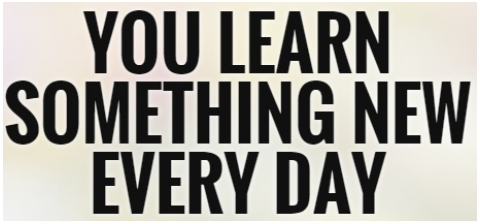
FOX | MIS
Management Information Systems

Edward Beaver
Edward.Beaver@temple.edu
ff

Video: Record the Class

Discussion

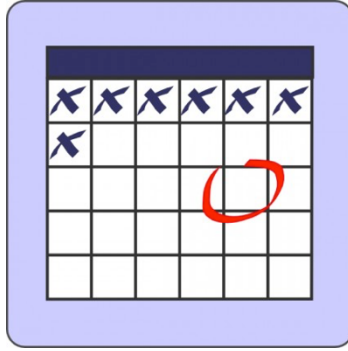
- Something really new, different you learned in this course in last week



- Questions you have about this week's content (readings, videos, links, …)?

- Question still in your mind, something not adequately answered in prior readings or classes?

MIS 5121: Upcoming Events



- Exercise 4 (Segregation of Duties)-*Due: November 10*
- **Exam 2** – Via Blackboard*: November 11 - 13*

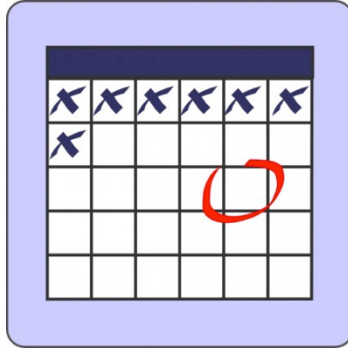
  Content of Exam

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

- Guest Moderator: Auditor's Perspective - *Week 12*

- Guest Moderator: SAP Futures - Week 13

MIS 5121: Extra Credit



- Blog Question Comments not required this coming week (due to Exam)

  However, any comments made will be considered extra credit

- **Extra Credit Assignment** *Due December 13*

  – See Course Blog for assignment details

Data Migration / Interfaces Overview

Master Data

- Examples of
- Master data vs. Transaction data
- Controls (Few)

Data Migration (typically Project oriented)

- Risks (Few)
- Controls (Few)

Data Migration / Interfaces Overview

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

Segregation of Duties Exercise 4

- Agenda
  - Last Class *(October 31)*: Steps 1 – 2 (Risks / Control & Organizational design with SOD)
  - ***This Class (November 7): Step 3 - 4 (Paper process to system process with SOD and authorizations to design)***
  - *Due November 10 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.