MIS 5121: Business Process, ERP Systems & Controls

Week 9: Security: User Management, Segregation of Duties (SOD)
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?
Security (Continued): User Management
SAP Security: Review

_____: Authorization Object

Authorization Values

_____: Authorization Checks

_____: Authorization Fields

_____: Roles / Profiles
SAP Security: Review

- Core: Authorization Checks
- Tumblers: Authorization Fields
- Keys: Roles / Profiles
- Lock: Authorization Object
- Program
- User ID

Imbedded in
User Master Record

- Key: User ID (*Same as for other Systems?*)
- Contains privileges of the user
- Roles (and related profiles) assigned
- During SAP logon all assigned authorizations loaded from master record into User Buffer

Other Data:
- Address, Contact Info
- Default Date format, decimal format
- User Parameter data (can be used to prepopulate Data)
- User Groups
Create user ID – SU01

- Complete as many fields as possible (per user administration standards)
- Certain fields may be required
Create user ID – SU01: User Type

- **Dialog (A):** Normal type user
  - Password enabled (check, change expired, ...)
  - Multiple logons checked and logged

- **System (B):** e.g. Batch User
  - Communication without dialog in one system or
  - Background processing in one system
  - Excluded from general password validity settings (change, expiration, etc.)

- **Communication (C):** Communication between systems (without dialog)
  - RFC or CPIC service users. E.g. ALE, Workflow, TMS, CUA
Create user ID – SU01: User Type

- **Reference (L):**
  - General user not assigned to person
  - Cannot log on using Reference User
  - Used to equip Internet users with identical authorizations

- **Service (S):**
  - Required for dialog-free communication between central components of SAP via PI
  - Used by Java components of PI
  - PI (Process Integration) is SAP Netweaver integration tool
  - Used between SAP modules (e.g. ECC, GTS, CRM, SRM, ...) and non-SAP applications
  - Generally this user is assigned very restricted authorizations
Create user ID – SU01: Logon Data

- **Alias**: Reference for internet applications / users. Max 40 characters

- **Password**: Initial password

- **User Group**: Department, country, ...Can be used for security and in SUIM

- **Validity Period**: For temporary users (e.g. contractors)
Create user ID – SU01: Defaults Tab

- Complete fields per User Administration Standards

- **Formatting**: Changes what appears on screen, not what’s stored in system (display format only)
  - Language
  - Decimal Notation
  - Date Format
  - Time Format

- **Output Device**: Default printer / output parameters LOCL – uses PC’s default printer (can be formatting issues)

- **Time Zone**: Display only? Note system time zone
Create user ID – SU01: Parameters

- Parameters: Screen independent data
- Usually linked to a field (e.g. plant, sales org, ...)
- Useful to automatically provide a default value for a field
- Also used to manage via user settings how SAP works (e.g. ability to save OTC variants)
Parameters: Most fields Have one
Create user ID – SU01: Roles / Profiles

- Security Repository for User
- Note: Effective dates for Roles
- Profiles tab auto-populated based on Roles Assigned
- Details from these tabs pulled into User Buffer during Logon
Delete user ID – SU01

- Deleting ID’s impacts items associated with ID
  - Parked documents
  - Workflow requests
  - Batch Jobs

- Recommend inactivating rather than deleting in production (e.g. for defined transition period of time)
  - Inactivate by ‘Locking’ the user

![Image of user interface with 'Delete' button highlighted]
SU10: Mass User Maintenance

- Same action – multiple IDs
- Limited data tabs (e.g. Address, Authorizations, ...)
- When would you use?
SU01 / SU10: Lock / Unlock

- User / Password Administration
- Recommend Users manage their own passwords / sign-on credentials when possible
- Change password – for dialog users requires resetting at next logon session
- SU01 – single User ID
- SU10 – Multiple ID’s
SUGR: User Groups

- Define user groups with SUGR
- Assign Users to groups in SU01, SU10, ???
- Can do following with User Groups
  - Segregate users by technical teams (e.g. Basis, development, training, etc.) or process teams
  - Pull ID’s into SU10 (Mass Maintenance) by user groups
  - Reporting: can help with auditing
User Authentication

And You are Who ??!??

- Designed to protect system availability, integrity and privacy
- Authentication methods provided in SAP include:
  - Logon with password (Dialog user)
  - Secure Network Communications (SNC) (Single sign on?)
  - Client Certificates (interfaces?)
  - SAP Logon Tickets
  - Pluggable Authentication Services

Alignment of client policies and auditor judgment is important
Logon with Password Security

- Initial password must be assigned to user
- Passwords must meet internal requirements set by system (SAP Password Rules)
  - Cannot be more than 8 characters
  - First character not ‘, ?, or space
  - First three (3) characters not same order as User ID
  - First three (3) characters not identical
  - Password cannot be ‘Pass’ or ‘SAP’
  - User can change password maximum of once per day
  - User defined password cannot be same as last five (5) passwords
Logon with Password Security

Password parameters that Can be set by Customer (Customer Password Rules)

- May not be in a list of impermissible passwords (table USR40)
- Must be at least 6 characters long
  - System profile parameter login/min_password_ing
- At least one (1) character in the new password must be different from old password (can’t shuffle same characters)
  - login/min_password_diff
- Must be changed periodically (e.g. every 60 days)
  - login/min_expiration_time
- Password Contents
  - login/min_password_uppercase
  - login/min_password_lowercase
  - login/min_password_letters
  - login/min_password_digits
  - login/min_password_specials
Access Other than User ID / Password

Secure Network Communication (SNC)
- Available when using SAP GUI for Windows or Remote Function Call
- Uses external security product to authenticate

Client Certificates
- Used for Web applications such as SAP Web AS ABAP
- Authenticate by user presenting X.509 client certificate
- Authenticate takes place on Web server using Secure Sockets Layer (SSL) protocol
- Transfer of passwords not needed
- ‘Single Sign-On’
Access Other than User ID / Password

**SAP Logon Tickets**
- Single Sign-on to multiple SAP Systems
- Authenticate once and SAP logon ticket is issued
- Log in to other systems (SAP / non-SAP) via ticket

**Pluggable Authentication**
- Delegates authentication to external system
  - E.g. Windows Domain Controller or a Directory Server
- External system obtains SAP User ID from mapping table USREXTID
- If successful: User issued a logon ticket (see above)
User Management Overview

- User Types (examples, why different)
- User Maintenance (Create / Change / Delete)
  - Examples of data maintained and why
- Password Options
  - Couple Examples of SAP password rules and why useful
  - Couple Examples of Customer Password Rules (configuration options and why useful)
Security and Segregation of Duties (SOD)
Segregation of Duties

Definition

‘ensuring that at least two individuals are responsible for the separate parts of a task’

Goal: prevent error and fraud
Segregation of Duties

Implementation

- Break down tasks that might reasonably be completed by a single individual into multiple tasks
- No one person is solely in control
- Prevent one person from having 2 of:
  - access to / custody of assets (operational responsibility)
  - Responsibility for asset’s accounting / reconciling
  - Approval
- Prevent opportunity to commit and hide errors, fraud, theft
Segregation of Duties

Other names

- Separation of duties
- Four eyes / two-man / two-person principle: two individuals approve some action before it can be taken

Implications

- Break down can make process less efficient, require more people
- Choose where to implement (high risk, mission critical)
SOD Examples

Examples of SOD related risks and controls in each area discussed

– Procure to Pay Process
– Order to Cash Process
– Master Data
– Financial Processes
– Inventory

*Person who __________________ should not be the person who __________________.*
SOD Examples

Procure to Pay

• Person who requisitions the purchase of goods or services should not be the person who approves the purchase.
• The person who approves the purchase of goods or services should not be the person who reconciles the monthly financial reports.
• The person who approves the purchase of goods or services should not be able to obtain custody of checks.

Order to Cash

• The person who negotiates Customer Prices should not be the person who approves the prices
• The person who negotiates or approves Customer Prices should not be the person who enters the prices used on orders
• The person who opens the mail and prepares a listing of checks received should not be the person who maintains the accounts receivable records.
SOD Examples

**Master Data**
- Person who creates / maintains customer master data should not be the person who processes customer orders or receives payment.
- Person who creates / maintains vendor master data should not be the person who processes purchase orders or processes vendor payments.

**Financial Processes**
- The person who approves journal entry values should not be the person who enters or reconciles the journal entries.
- The person who maintains and reconciles the accounting records should not be able to obtain custody of checks.
- The person who opens the mail and prepares a listing of checks received should not be the person who makes the deposit.
SOD Examples

Inventory Controls

• Person who physically handles inventory should not be the person who enters inventory related transactions
• The person who counts inventory stock should not be the person who reconciles vs. system inventory records not enters inventory adjustments.
Segregation of Duties (SOD) Overview

• SOD Definitions

• SOD Implementation Concepts

• SOD Examples
  – 1 or 2 in each area
  – How phrased
Breakout Activity – Rules

• Break into teams – max of 5 people / team
  – Diversity a must.

• Assignment – return via WebEx Notes or Word Document

• How: WebEx breakout?

• Time: assigned today 20 min (including break)
  – Start back on-time
Breakout Question

Security

What has been your Experience?
- __________
- __________
- __________

Why is Security so Complex?
- __________
- __________
- __________
- __________

What about SAP Security don’t you Understand?
- __________
- __________
- __________
- __________
Report Back
Segregation of Duties Exercise 4

• Primary learning objectives are:
  – Experience specifying 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

• Agenda
  – This Class (*October 31*): Steps 1 – 2 (Risks / Control & Organizational design with SOD)
  – Next 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 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.
Extra Slides
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