MIS 5121: Business Process, ERP Systems & Controls
Week 8: Security 2 – Roles

Financial Processes and Controls 2
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?
ISC framework in the ERP environment

- Entity level controls
- Automated application controls
- Manual and semi-automated business process controls
- Authorizations and access protection (confidentiality, integrity)
- IT General controls (change management, operation, security)
- Automated testing and monitoring of business processes, KPIs, etc.
Security: SAP Authorization Concept
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
SAP Environment Security Components
SAP Security: Key Concepts

- **Lock**: Authorization Object
- **Core**: Authorization Checks
- **Tumblers**: Authorization Fields
- **Key Slot**
- **Transactions & Programs**
- **User ID**
- **Key**
- **Authorization Values**
- **SAP Terminology**

Imbedded In
SAP Security Terminology

• **Authorization Object**: Logical template (‘lock’)
  – Implements access restrictions in SAP
  – Contains 1+ fields
  – Referenced by authority-check statements coded in programs
  – Often many objects referenced by same program
  – Objects are **ANDed** together
  – More than 900 SAP Supplied authorization objects
  – Examples:
    • V_VBAK_AAT: Sales Document: Auth for Sales Document Types
    • V_VBAK_VKO: Sales Document: Auth for Sales Area
    • F_BKPF_BES: Account Authorization for G/L Accounts
SAP Security Terminology

• **Authority Check:** (the lock ‘core’)
  – Program statement(s)
  – Checks the user’s authorizations buffer for fields and values (based on the referenced authorization object)

• **Authorization Field:** (the lock ‘tumblers’)
  – 1-10 fields used in each object / check.
  – Examples:
    • Activity: function to be performed (create, change, display, etc.)
    • Document type (e.g. sales, purchasing, production, …)
    • Enterprise Hierarchy node (e.g. company, sales org / area, plant, etc.)
    • Account type (e.g. customer, vendor)
SAP Example

Transaction: **SUIM**
Select Role: ‘**Z_BPI**’
  – **Authorizations** tab
SAP Example

Transaction: SUIM - Select Role: ‘Z_BPI’ – Authorizations tab

Field values
- Object: F_FAGL_LDR
- Field Name: BUKRS
  Company Code

Value Intrvl
- 'From':
- 'To':
SAP Security: Key Concepts

Lock: Authorization Object

Key Slot

Core: Authorization Checks

Tumblers: Authorization Fields

Transactions & Programs

Transactions & Programs

SAP Terminology

User ID

Program
**SAP Security Terminology**

- **Authorization Values:**
  - Collection of fields & values (‘keys’) referencing authorization objects
  - Contained in user’s assigned authorization roles / profiles
  - May or may not match values checked by an authorization check statement
  - Values for same fields are ORed together
SAP User IDs

Transaction: **SU01 / SU01D**
Select Role: ‘user ID’
SAP User Roles / Profiles

Transaction: SU01 / SU01D - ‘Roles’ and ‘Profiles’ tabs
SAP Security Terminology

• **Role**: grouping of privileges
  – Assigned to SAP users, user groups or other roles
  – In general: roles contain logic used to generate profiles
  – Logic in roles includes transactions and user assignments making it the starting point for setting up and maintaining authorizations
  – Can resemble a job description i.e. sales representative, accountant, treasurer

• **Profile**: used to access SAP Functions or running programs.
  – Assigned to users in the user master record
  – Could represent a simple job position
  – Contain authorization and authorization objects

• The basic difference is that the roles contain the "profile" and "user master data"
Application Security: Example

User

Business Job / Role (e.g. Buyer)

Business Intelligence System (BI)

- **Role: Procurement Reports**
  - T-code: ME51 Create Purchase Req
  - T-code: ME51 Create Purchase Req

Enterprise Central Component (ECC)

- **Role: Maintain Purchase Requisitions**
  - T-code: ME51 Create Purchase Req
  - T-code: ME52 Change Purchase Req
  - T-code: ME5K Reqs by account Assign

Role: Display Purchase Requisitions

**Role:**
- Maintain Purchase Requisitions
- Display Purchase Requisitions
- Procurement Reports
SAP Security: Business vs. Technical View

**Business View**
- Employee
- Job
- Task
- Privileges
  - Activities
  - Business Structure

**SAP Technical View**
- User Master Record
- Roles / Profiles
- Transaction Code in roles / profiles
- Authorizations
  - Object
    - Fields
    - Values
SAP Security: Logic to Access

Check Transaction Code

Pass → Check Object

Pass → Within Program

Pass

Transaction Code Executed

"No Authorization for
• Transaction Code ____

"No Authorization for
• Transaction Code ____
• Activity ...
• System Element ...

"No Authorization for
• Activity ....
• System Element ...
SAP Security: Diagnosis

- **SU53**: Display authorization data for failed checks
  - Identifies transaction checked (note sometimes SAP transitions to other transactions e.g. during drill downs)
  - Authorization objects and fields checked and values used / available
  - Helps identify ‘missing’ authorizations

Example:

- **Date**: 03/05/2015, **Time**: 09:47:20
- **Transaction**: SMEN
- **Authorization Obj.**: S_USER_PRO
- **Authorization Field**: ACTVT
- **Authorization Field**: PROFILE

User Master Maintenance: Authorization Profile

Auth. profile in user master maintenance
SAP Authorization Concept Overview

• SAP Authorizations allow you to protect transactions and programs from unauthorized use
  – ‘New’ custom transactions must include authorization objects to be controlled (if missing – open to every user)

• Access must be explicitly granted through use of authorizations

• Authorizations are assigned to roles (profiles) which in turn are assigned to User Master Records (User IDs)

• Only users with active user master records can log onto system. User IDs needed for:
  – Dialog: people via screens
  – System: batch processes
  – Communication / interfaces
Security (Continued): Role Design
SAP Security Role Design

Defining Roles

Define roles within each business process and mapped to jobs, positions and users

Access requirements for each roles identified by:

- Transaction Code
- Organizational Hierarchy access
- Other functional system access

Role relationships and access requirements should be fully documented and continually refined throughout the project.
SAP Security Role Design

Restricting Access

– Transaction Codes (T-Codes) Develop roles
  • Ex: ME21N, ME22N, ME23N (Create, Change, Display PO)

– Organizational Scope Criteria (Business areas configured in SAP)
  • Plant
  • Company Code
  • Sales Organization

– Activity Level (e.g. Display PO’s only allow viewing)
  • Create
  • Change
  • Display / View
SAP Security Role Design

Role Concept Overview

SAP application security uses roles to group transactions necessary for users to perform their job

- Develop roles
- Example: Maintain Purchase Orders role allows users to create and change PO’s
- Positive security approach: develop roles so least amount of privilege or authorizations are assigned for any one user to perform their job
SAP Security Role Design

Role Definition: Job Level  Option A

- Must assign common transactions to many roles
  - Increases risk of configuration error (role creation and maintenance)
  - More complex model (e.g. single T-code assigned to many users – why??)
- Roles become very large
  - Small changes may require considerable ‘clean-up’
  - Large roles with may responsibilities difficult to manage
  - Higher risk of Segregation of Duties (SOD) compromise
- Creating almost identical access for multiple users / positions
  - Decreased control of consistency over security configuration

*Job level security not standard methodology*
Role Definition: Task Level  

Option A

- Common transactions in fewer roles
  - One role adjustment automatically activated for all assigned users
- Less effort to configure & Maintain
  - T-code changes require less ‘clean-up’ because roles smaller
  - T-code adjustments occur less often (most changes involve only re-mapping of roles to users)
  - Simpler model -> less effort to configure & maintain
- User maintenance (role assignment) more complex but more flexible
SAP Security Role Design

Managing the Tension

Role Complexity
Larger Roles
Maintenance ‘clean-up’
Risk of SOD in roles

User Role Mapping Complexity
Smaller, more Roles
Simpler role maintenance
Risk of SOD via multiple roles assigned

Job Based
Task Based
Security Design: Best Practices

• Design security considering cost vs. benefit
• Use Risk based approach to design security measures and build a controlled environment
• Global design: standardized
• Flexible model (anticipate future additions, changes)
• Use ‘Least privilege access’
• Create application specific roles consistent with organization roles
• Leverage pre-designed security roles if possible
Security Design: Best Practices

• Application security consistent with company policies, requirements, procedures (e.g. password expiration)

• Minimize custom code (use ‘out of box’ functions if available)

• Integrate security design / policies with all implementation threads / teams
SAP Security Role Design

Managing the Tension

Role Complexity
Larger Roles
Maintenance ‘clean-up’
Risk of SOD in roles
Unique Role Design – more roles
Role Flexibility

User Role Mapping Complexity
Smaller, more Roles
Simpler role maintenance
Risk of SOD via multiple roles assigned
Global, standard Roles
User mapping Flexibility

Job Based
Task Based
Security Role Design Overview

• Job vs. Task level Definition
  – What are the trade-offs
  – Who / How to define?

• Best Practices
  – Design from beginning
  – Standardization vs. flexibility
  – Least Privilege Access Concept
  – Addition Couple best practices
Question:
Is ‘Ignorance’ a valid Security Technique?

Answer: In Two (2) Weeks
Journal Entries Exercise

• Primary learning objectives are:
  – Experience concepts of beginning financial accounting
  – Review the accounting cycle
  – Work with a manual accounting information system
  – Experience how an ERP system handles the steps of the accounting cycle
Exercise 3: Journal Entries

• Agenda
  – Last Class *(October 17)*: Tasks 1 - 3 (Manual steps)
  – This Class *(October 24)*: Tasks 4 - 6 (SAP steps)
  – *Due October 27 11:59 PM*: Assignment Submission sheet
Task 4: Use SAP ERP system to make all above entries using the general ledger system in SAP.

(Instructions for using the SAP ERP system start on page 15 of this document)

a) Accounting ➔ Financial Accounting ➔ General Ledger ➔ Posting ➔ Enter G/L Account Document (FB50)

Record beginning account balances in the SAP general ledger. Enter as one composite journal entry (first journal entry). Use journal entry date of January 1.

Be sure to compare to Excel spreadsheet to make sure the entries are correct.
Exercise 3: Journal Entries

Step 4: Using SAP general ledger system

b) Accounting ➔ Financial Accounting ➔ General Ledger ➔ Posting ➔ Enter G/L Account Document (FB50)

Record the daily and month-end transactions for January in the SAP general ledger

- Do each journal entry as a separate entry, not as one giant composite entry
- Use appropriate dates – this allows for a good audit trail.
Exercise 3: Journal Entries

Task 5: Using SAP General / Ledger system

a) Display the trial balance.

b) Compare this balance to your manual entries.

c) If the trial balance does not match your manual entries, research the errors and make necessary corrections.
Exercise 3: Journal Entries

Task 5: SAP General / Ledger system:

Options for viewing the journal entries:


– **Source Document Drill Down**: Accounting → Financial Accounting → General Ledger → Account → Display/Change Line Items (FBL3N)

Exercise 3: Journal Entries

Task 6: Using SAP general ledger system

Review the Balance Sheet and Profit and Loss Statement:

Accounting → Financial Accounting → General Ledger → Information System → General Ledger Reports → Balance Sheet/Profit and Loss Statement/Cash Flow → General → Actual/Actual Comparisons → Balance Sheet/Profit and Loss Statement (S_ALR_87012284)

How do these statements match your manual trial balances?

Print or save in Excel or Word format
Extra Slides
Exercise 3: Journal Entries

**Task 1:** In SAP ERP system, review the chart of accounts for GBI.

Accounting ➔ Financial Accounting ➔ General Ledger ➔ Information System ➔ General Ledger reports ➔ Master Data ➔ Chart of Accounts ➔ Chart of Accounts *(S_ALR_87012326)*

Examine the **GLXX** chart of accounts (**XX** is your assigned SAP student login ID#.)
Exercise 3: Journal Entries

- **Task 2:** Record the daily transactions
  - Record if appropriate, (some events may not involve journal entries)
  - Record into Excel
  
  - Review the post of these journal entries into t-accounts (Excel automation) and the calculated account balances using cell formulas in Excel.
  
  - Review t-account balance flow into your Excel worksheet as a trial balance. Assure validity of links within spreadsheet that expedites the process and minimize risk of an error in data entry
Exercise 3: Journal Entries

• **Task 3:** Record the adjusting entry transactions
  
  – Based on the Month-end Adjustment Checklist, Record the needed journal entries into Excel

  – Review the post of these journal entries into t-accounts (Excel automation) and the calculated account balances using cell formulas in Excel.

  – Review t-account balance flow into your Excel worksheet as a trial balance. Assure validity of links within spreadsheet that expedites the process and minimize risk of an error in data entry