MIS 5121: Business Processes, ERP Systems & Controls

Week 12: Systems Development 2: Data Dictionary, Program Security

Edward Beaver
Edward.Beaver@temple.edu
Controls: Integration Points

Risk/Control Matrix can serve as the primary vehicle for integrating control design into project activities and deliverables.

Program Development
- Functional Spec
- Technical Specification
- Automated (Custom) & Manual Controls

Business Process Teams
- Training & Procedures
- Bus Process Reqmts
- Manual Controls

Security Analysis Tool
- SOD Controls & Sensitive Access
- GRC

IT / Security
- Security Configuration
- Risk Control Matrix
- Integration
- Segregation of Duties

SOX Section 404 Integration
- Automated: Standard & Configuration
- Risk / Control Matrix Subset
Key Information Technology Risks

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

- Types of Development Objects (FRICE)
  - **Forms** – outputs (invoices, Purchase orders, ...)
  - **Reports** – custom reports
  - **Interfaces** – SAP to other systems
  - **Conversions** – Data migration
  - **Enhancements** – Change system logic, use additional fields, etc.
    - User-Exits: defined SAP branches to custom code (lower risk)
    - Change SAP code (high risk, long term extra maintenance)
  - **Workflow** – non-config components, logic

- Development: custom programs
  - Typically ABAP (SAP SQL extension programming language)
Programs in SAP

➢ Transaction SE38 (Program Editor)
  ✦ This program used when executing Create Sales Order transaction VA01
INCLUDE MV45ATOP.

ENHANCEMENT-POINT SAPMV45A_03 SPOTS ES_SAPMV45A STATIC.

ENHANCEMENT 2  ECO_HBS_SAPMV45A.  "active version

include for RE-SCM sales functions. also known as Home Building Solution

ENDENHANCEMENT.

ENHANCEMENT-POINT SAPMV45A_01 SPOTS ES_SAPMV45A STATIC.

INCLUDE MV45ATZZ.  " Data definitions in MV45ATOP
INCLUDE MV45A0ZZ.  " User-modules PBO
INCLUDE MV45AIIZZ.  " User-modules PAI
INCLUDE MV45AFZA.  " User-forms < 3.0
INCLUDE MV45AFZB.  " User-forms
INCLUDE MV45AFZC.  " User-forms < 3.0D
INCLUDE MV45AFZD.  " User-forms 3.0E
INCLUDE MV45AFZF.  " User-forms 3.0F

include mv45afzg.  " User-forms 3.1G
include mv45afzh.  " User-forms 4.6B
INCLUDE MV45AFZZ.  " User-forms
INCLUDE MV45AFZ4.  " User-forms 4.0

MILL 0008 01 TSCH Kundenauftragsversion

INCLUDE MILL_vs_MV45A.  "item versioning
INCLUDE MILL_CAD_MV45A.  "CAD interface
**INCLUDE** MV45AFZH.

**************************************************
* * This include is reserved for user modifications *
* Forms for sales document processing *
* *
**************************************************

*----------------------------------------------------------*
* FORM  AUTHORIZATION_VALUE_SPLIT  *
*----------------------------------------------------------*

* This userexit can be used to split up the total authorization *
* value of sales order items with regard to invoices that will be *
* created from these items in the future. *
*
* Order items/schedule lines are stored in the table *
* OPEN_VALUES. A grouping term, which can be set freely, must *
* be entered in the field OPEN_VALUE-ZUKRI. The authorization is *
* carried out separately for each grouping term! *
*
* The program includes 2 examples. Please apply your own coding *
* if necessary: *
*
* 1) an invoice simulation is used to find out in which order *
* items/schedule lines will be invoiced in ONE billing *
* document. The field OPEN_VALUES-ZUKRI contains the document *
* number of the virtual invoice document (DA_XVBRP-VBELN). *
* Please see application help: Sales and Distribution -> *
* Billing -> The General Billing Interface, especially order *
* type, order item category and invoice type. Please be aware *
* that this simulation may temporarily affect system *
* performance. This example employs order type TA, item *
* category DN and Invoice type EX. Please make sure that
Programs in SAP – User Exit

* controlling parameter
* DA_EXAMPLE must be set with the number of the example
  = 1, if you want to have invoice simulation
  = 2, if you want to have special fields

FORM AUTHORIZATION_VALUE_SPLIT TABLES OPEN_VALUES STRUCTURE BEZS132.

DATA: DA_EXAMPLE(2) TYPE N VALUE 0.
DATA: DA_AUART LIKE VBAK-AUART VALUE 'TA'.
DATA: DA_FKART LIKE VBRK-FKART VALUE 'FX'.
DATA: DA_PSTYV LIKE VBAP-PSTYV VALUE 'DLN'.
DATA: DA_SUBRC LIKE SY-SUBRC.

IF DA_EXAMPLE EQ 1.
* first example: invoice simulation
  PERFORM AUTHORIZATION_VALUE_SPLIT1 TABLES OPEN_VALUES
    USING DA_AUART
    DA_FKART
    DA_PSTYV
    CHANGING DA_SUBRC.

  IF DA_SUBRC NE 0.
  * message Innm "error in invoice simulation, no split of
  * authorization value possible"
  ENDIF.

ELSEIF DA_EXAMPLE EQ 2.
* second example, for example shipping point
  PERFORM AUTHORIZATION_VALUE_SPLIT2 TABLES OPEN_VALUES.

  ENDIF.
ENDFORM.
Program & Development Security

- **Is program code ‘good’**
  - Does what it’s supposed to do
  - Limited to requirements only (not branch off to perform other nefarious actions)
  - Well-behaved: doesn’t mess up other programs, logic, operation of ERP system

- **Good Development Practices**
  - Clear, documented, approved requirements defined before coding
  - Define Requirements, Design Logic before major coding (e.g. use of function modules for common logic)
  - Peer Code Reviews
  - Experienced development leadership
  - Test, Test, retest **BEFORE** moving to PRD (strong change management governance)
Risk and Recommendation
Program Security

Risks:
- Unintended, nefarious uses of program code
- Users capable of executing programs directly can compromise standard controls (access security, audit trails)
- Display access to ABAP code gives backdoor access to program execution
- Debug authority provides unsecured table viewing and table change

Recommendations:
- Active review, manage program code details
- Access to run programs restricted via SAP Security / Authorizations
- Further secure programs via assignment to authorization groups
- Basis Admin no Display access to ABAP code (prevent backdoor access)
- Debug authority restricted to effectively monitored ‘emergency users’
Data Dictionary Security

- Central Catalogue of:
  - Data definitions and descriptions
  - Relationships between data elements / structures
  - Relationships between data and use in programs and screens

- Control Concerns:
  - Data Dictionary changes could affect the data integrity in system
  - Access to make changes needs to be restricted to appropriate individuals
  - S_DEVELOP Authorization object controls access to create / maintain / delete APAP dictionary & repository objects

- Also called ABAP/4 Dictionary in SAP
Risk and Recommendation
Data Dictionary

Risks:

- PRD Access to S_DEVELOP Allows direct changes to Data Dictionary which could compromise integrity of the data
- Any Data Dictionary change could compromise integrity of the data

Recommendations:

- No one (including Basis Administrators) should have update access to Data Dictionary in Production (PRD)
- Changes to data dictionary performed in DEV, tested in QA and migrated to PRD per change management process
- Developer access restricted appropriately using SAP Security / authorization concept
Key IT Controls Overview

- Program, Development, Data Dictionary
  - 2-3 risks that exist
  - Common control recommendations for each
Extra Slides
Information Security Administration

- Security Administration can be:
  - Centralized
  - Decentralized
  - Hybrid of both

- Control Concerns:
  - Segregate:
    - Role Development
    - User Administration (Assign Roles, change).

  - Do not Develop / Change Roles directly in PRD
    - Develop and unit tested in DEV, integration tested in QA and migrated to PRD per change management process
Risk and Recommendation

Information Security Administration

Risks:

- If User Administration access is not limited, higher risk of unauthorized and excessive access in SAP
- No Segregation of User Administration tasks, higher risk of inaccurate or unauthorized access assigned to users and profiles in SAP

Recommendations:

- Define Owners of all SAP systems, clients and data or Processes
- System and Client Owners responsible for:
  - Approving all changes to their systems / clients
  - Authorizing overall access to the system
- Data / Process Owners responsible for:
  - Control of overall data / process components in the systems / clients
  - Authorizing specific access to data / processes within the PRD system
- Same people do not have access to create, maintain and assign roles
- Role Creation or maintenance not performed in PRD environment