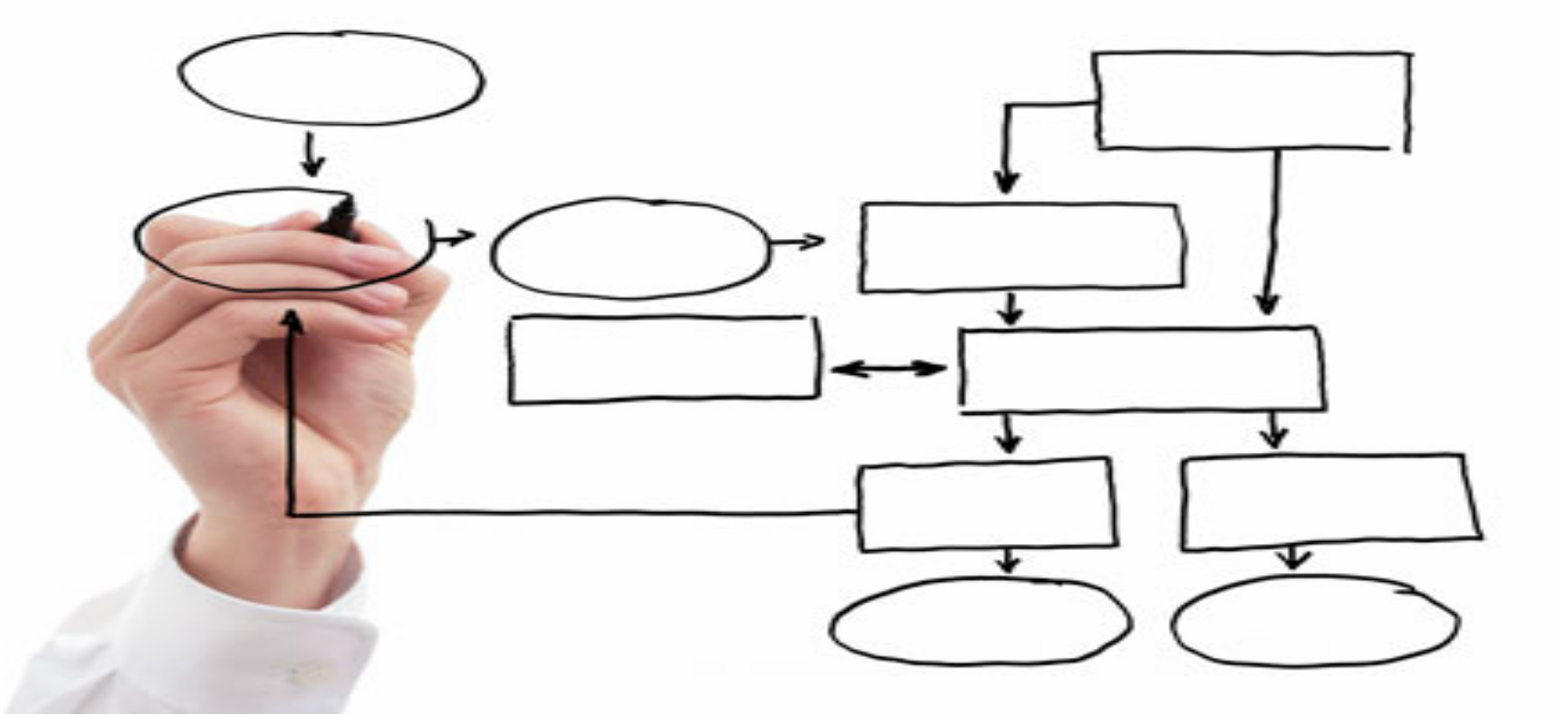


MIS 5121: Enterprise Resource Planning Systems

Week 9: *Security: User Management, Segregation of Duties (SOD)*

FOX | MIS
Management Information Systems

Edward Beaver
Edward.Beaver@temple.edu
ff

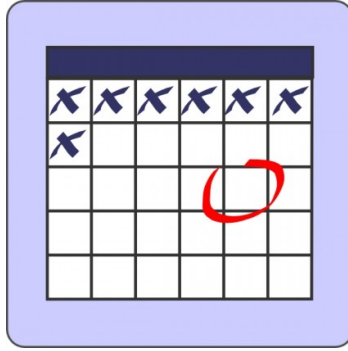
Control Failure: Paul Pagliaro's Presentation

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

Control Failure: Brandon's Presentation

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

MIS 5121: Upcoming Events



- Exercise 3 (Journal Entries) - *Due: March 19*
- Reading Assignment 6 - *Due: March 29*
- Class Visitors: auditors - *March 30*
  - Ernst & Young – auditing manager and SAP subject matter expert
  - Discussion / Q&A format (~30 minutes)
  - Gather discussion topics and your ?'s next week
- Exercise 4 (Segregation of Duties) - *Due: April 2*

MIS 5121: Extra Credit Opportunities

- *Due: latest - April 28 11:59 pm*
- Grade Points: 6 additional grade points in participation – (max 4 points boost to final grade)
- Choose **one (1)** of the 4 options on next slide

MIS 5121: Extra Credit Options

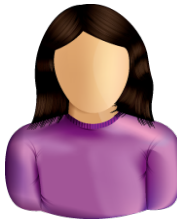
1. Using MindManager software tool (Mindjet) create map of Procure to Pay process risks and controls (core Idea: 'P2P Process Risks are Controlled') *(minimum of 10 risks)*
2. Same as 1 but: create map of Order to Cash key process risks and controls (core Idea: 'OTC Key Process Risks are Controlled') *(minimum of 10 risks)*
3. Same as 1 but: create map of Inventory control process risks and controls (core Idea: 'Inventory Control related Process Risks are Controlled') *(minimum of 10 risks)*
4. Paper (minimum 4 pages, 4 references) on topic: 'Lessons learned: Implementing ERP controls in ___ software'

Security (Continued): User Management

SAP Security: Review

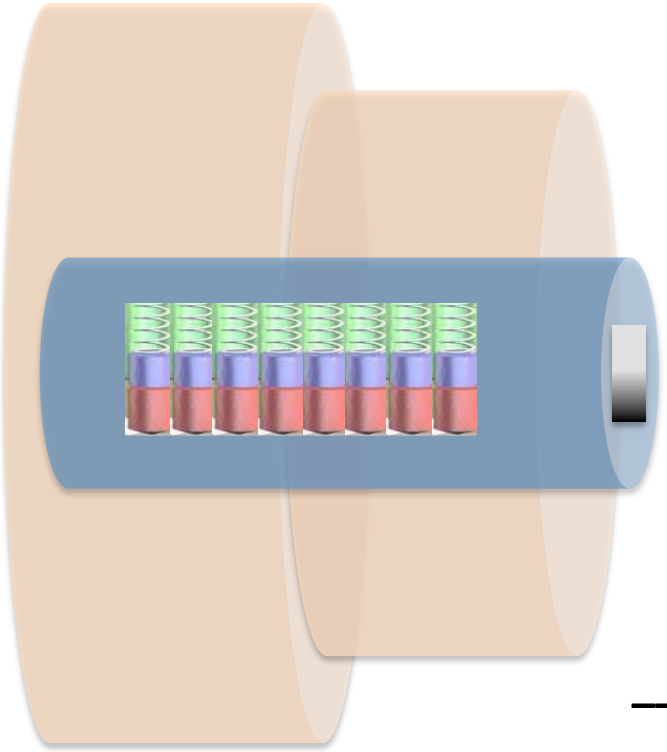
Program

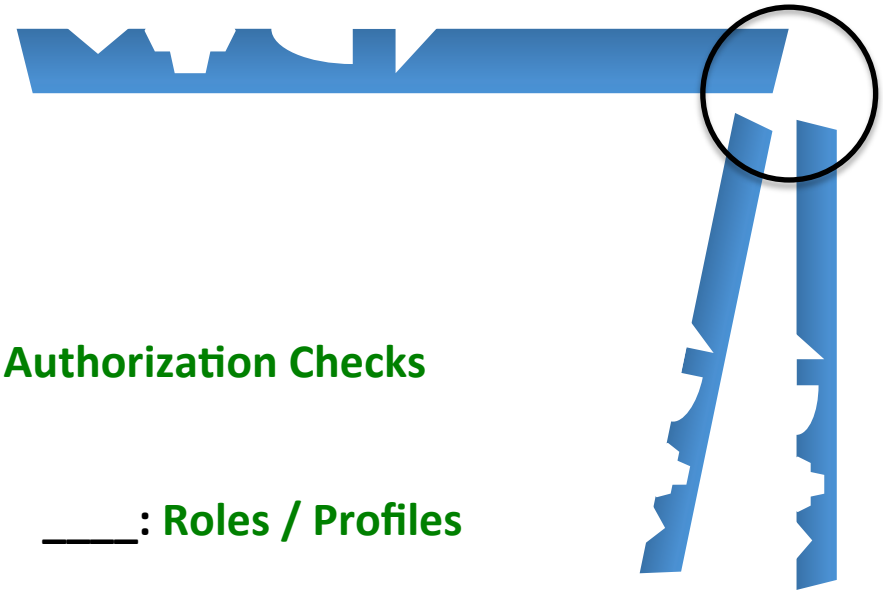
_____: Authorization Object



User ID

Authorization Values



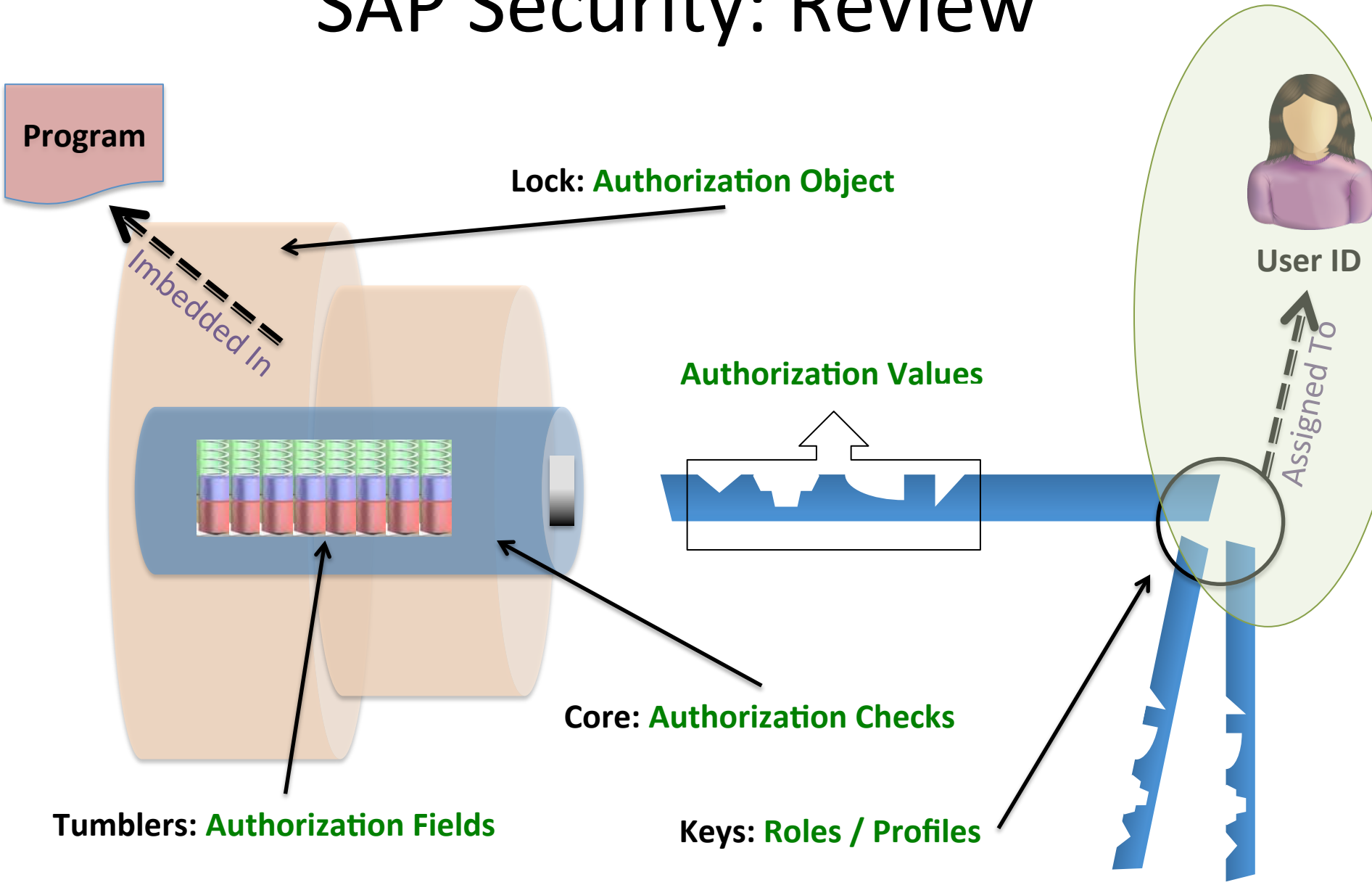


____: Authorization Checks

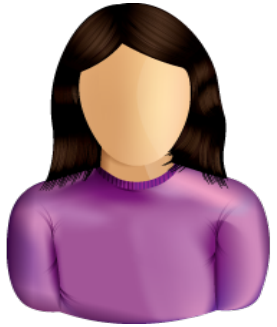
_____: Authorization Fields

____: Roles / Profiles

SAP Security: Review



User Administration – SU01

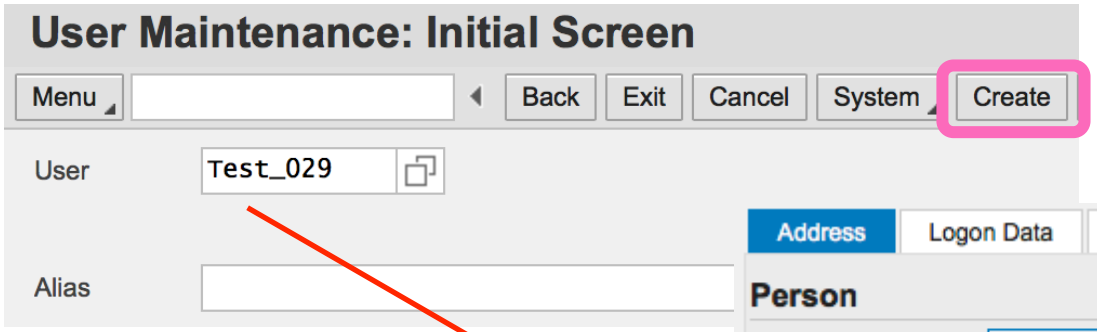


User ID

User Master Record

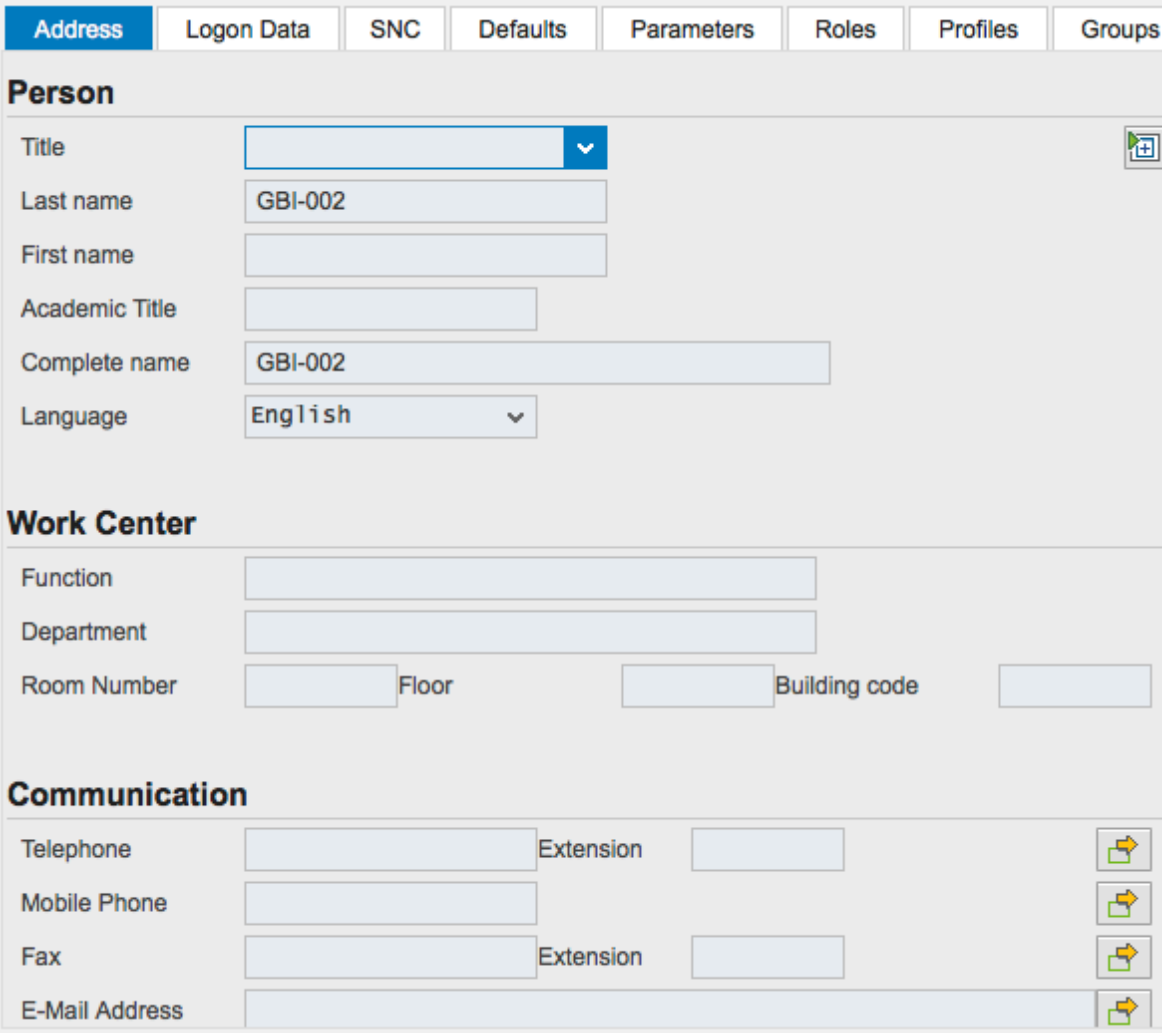
- Key: User ID *(Same as for other Systems?)*
- Contains privileges of the user
- Roles (and related profiles) assigned
- During SAP logon all assigned authorizations loaded from master record into User Buffer
- Other Data:
  - Address, Contact Info
  - Default Date format, decimal format
  - User Parameter data (can be used to prepopulate Data)
  - User Groups

Create user ID – SU01

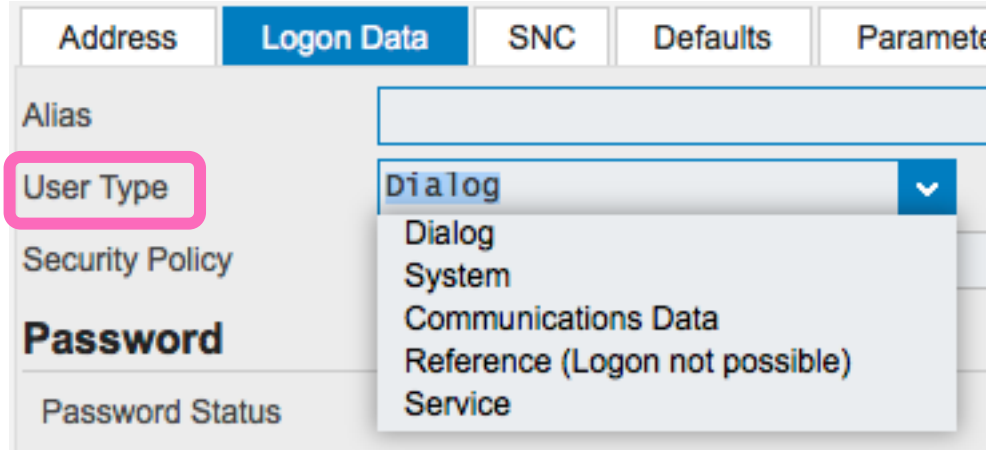


- Complete as many fields as possible (per user administration standards)
- Certain fields may be required

(F5)

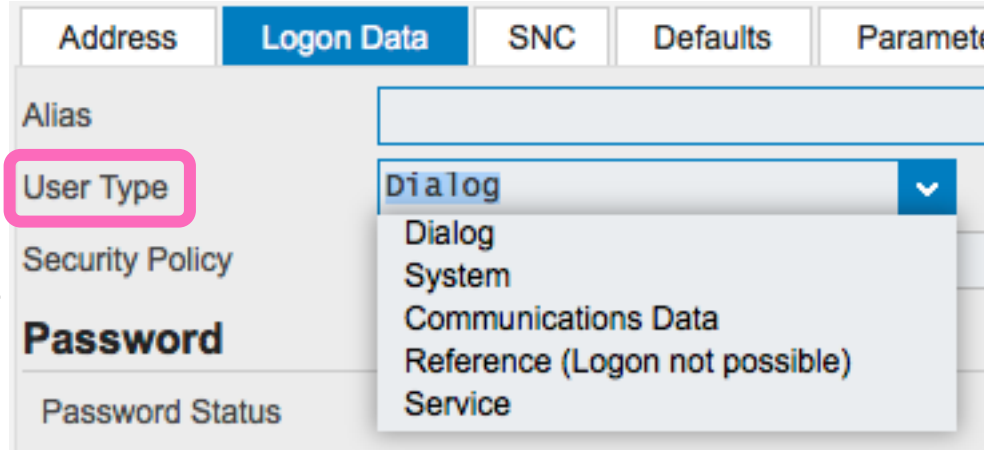


Create user ID – SU01: User Type



- 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

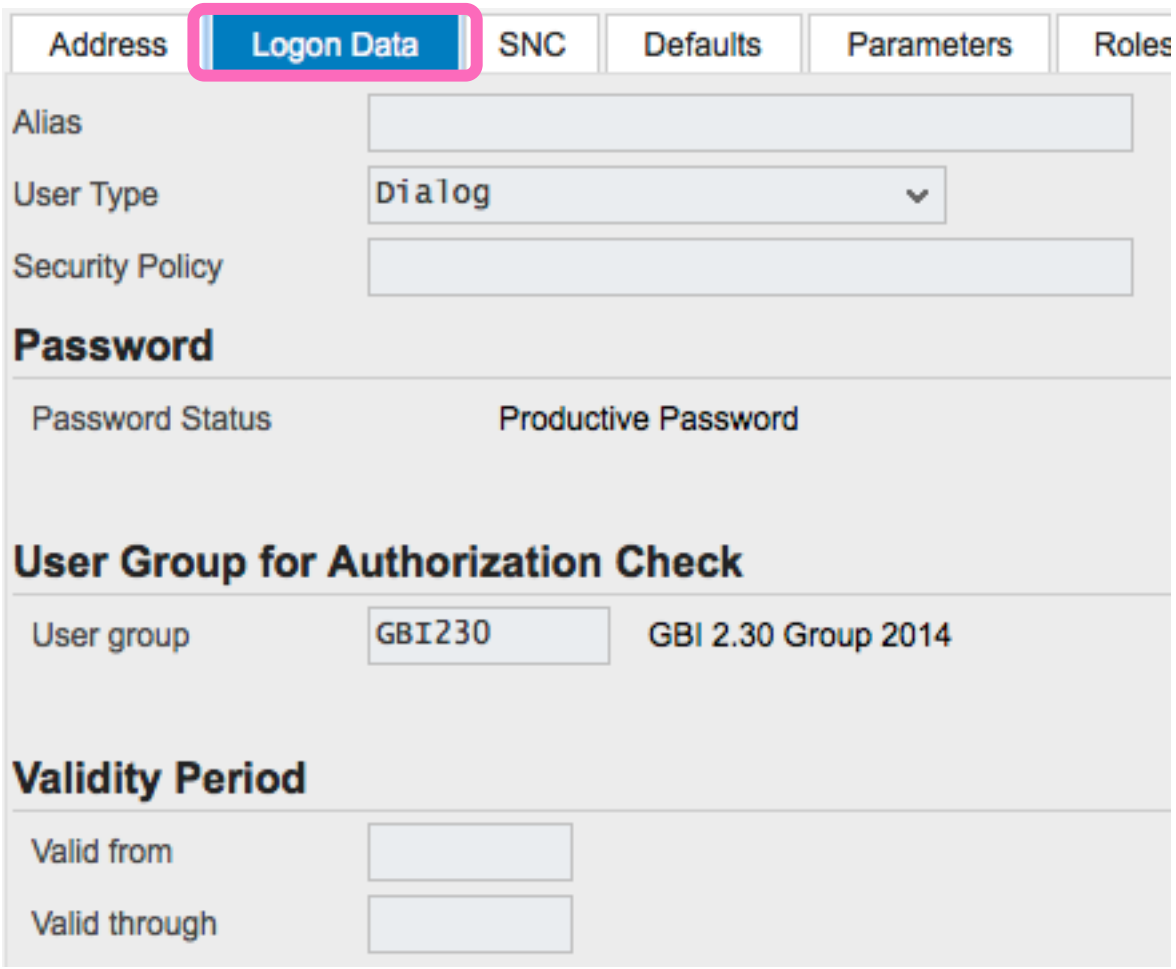
Create user ID – SU01: User Type



- 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

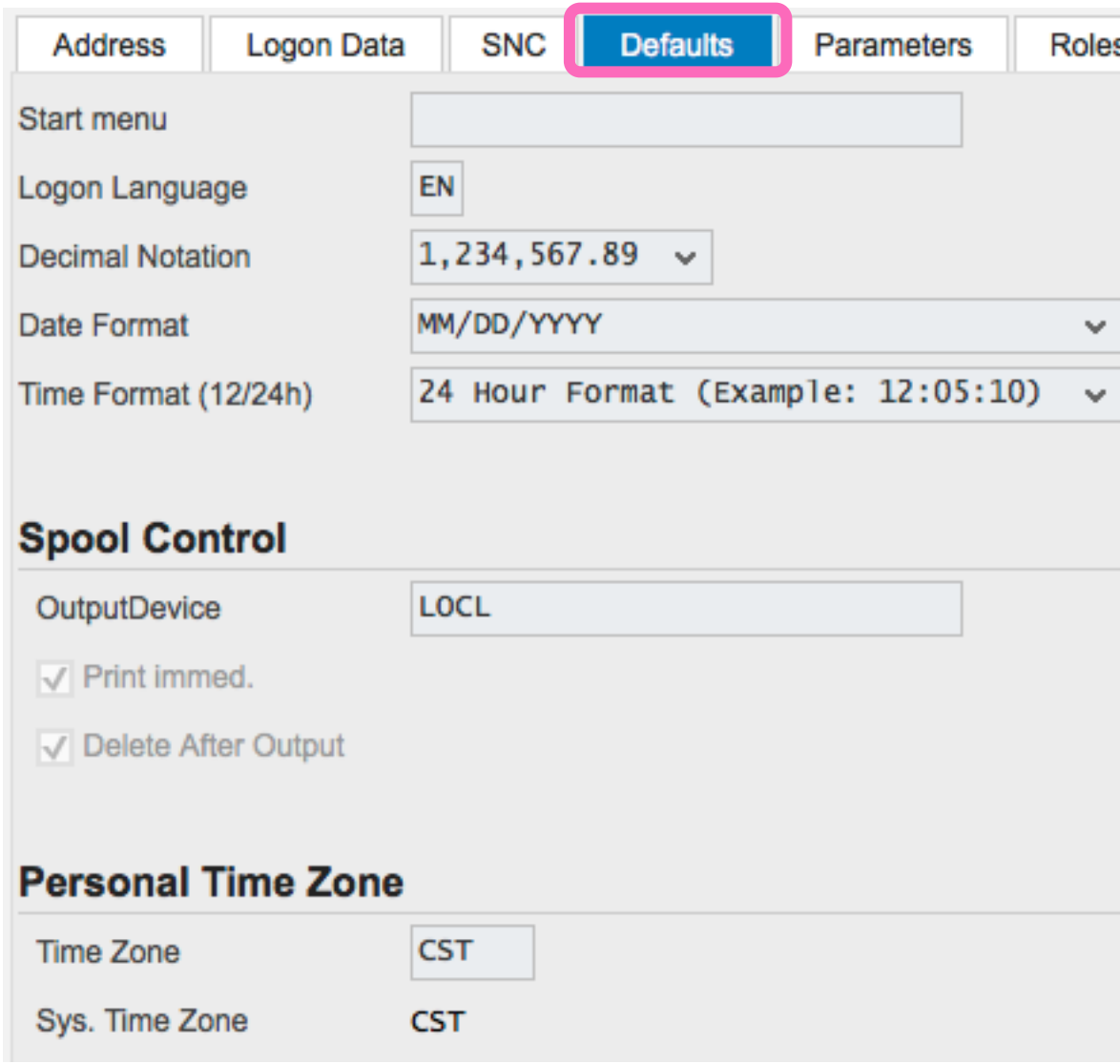
Create user ID – SU01: Logon Data

- 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)

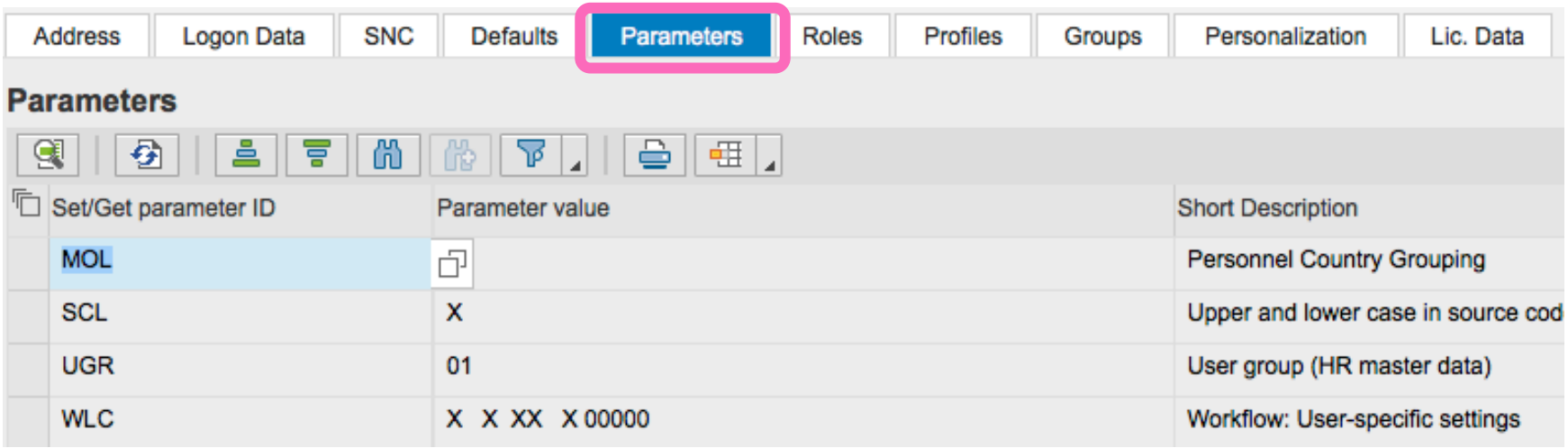


Create user ID – SU01: Defaults Tab

- 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

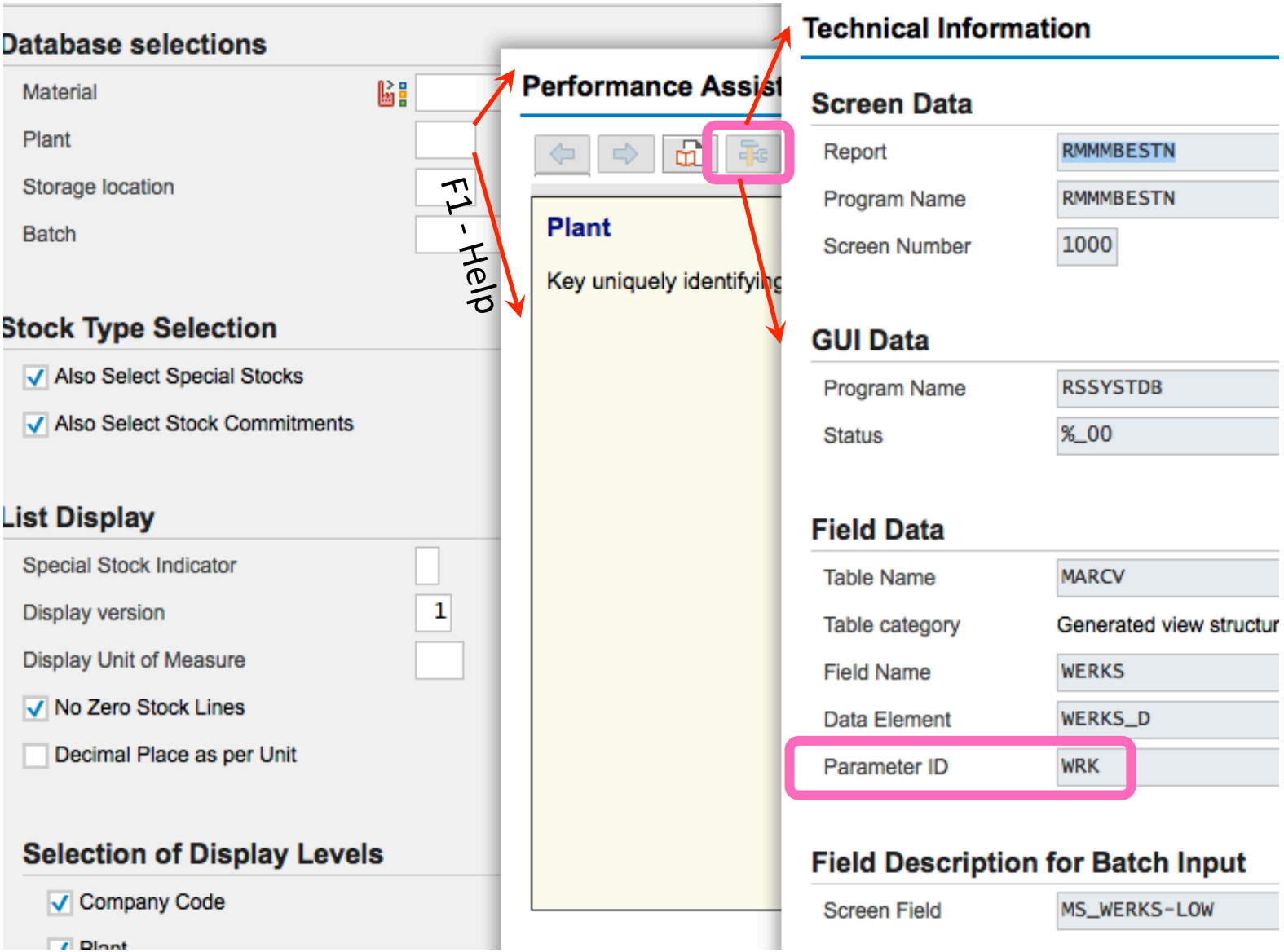


Create user ID – SU01: Parameters

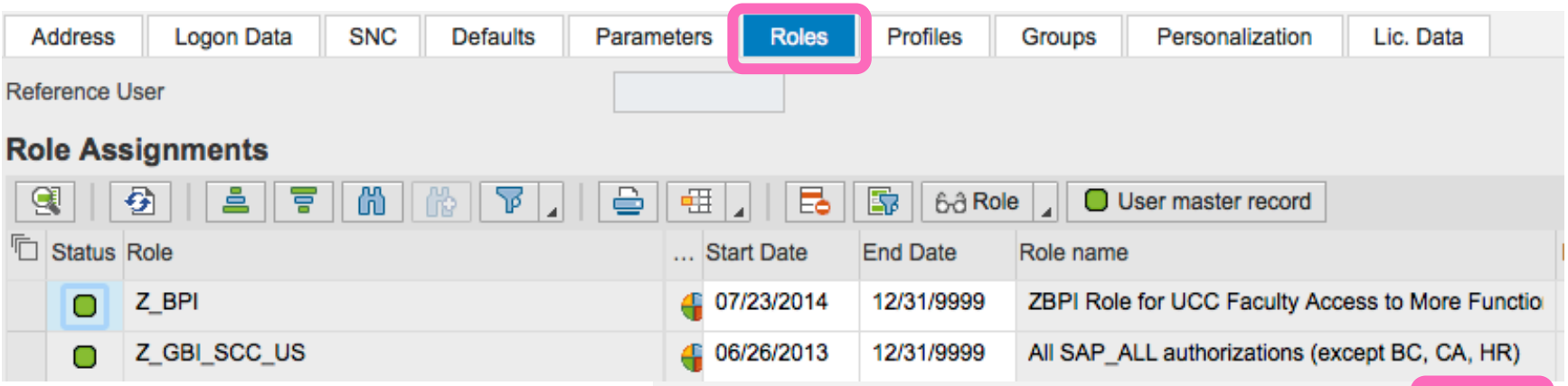


- Parameters: Screen independent data
- Usually linked to a field (e.g. plant, sales org, …)
- Useful to automatically provide a default value for a field
- Also used to manage via user settings how SAP works (e.g. ability to save OTC variants

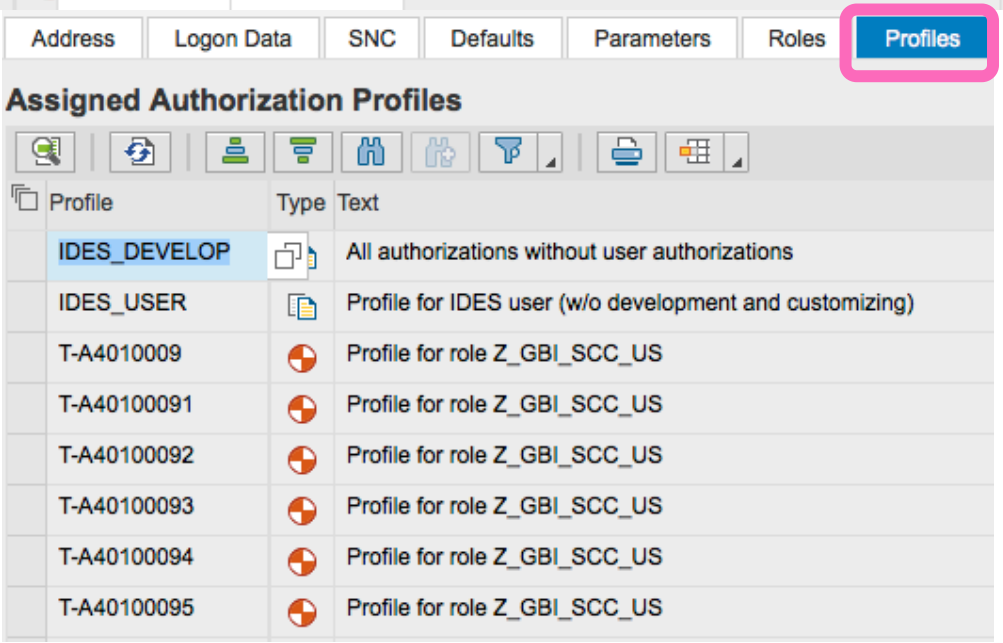
Parameters: Most fields Have one



Create user ID – SU01: Roles / Profiles



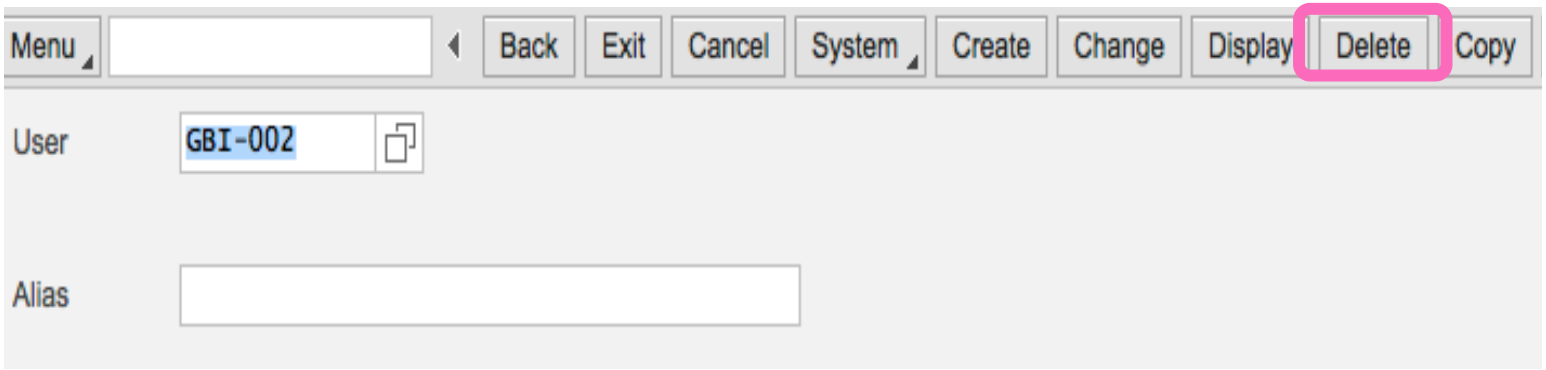
- Security Repository for User
- Note: Effective dates for Roles
- Profiles tab auto-populated based on Roles Assigned
- Details from these tabs pulled into User Buffer during Logon



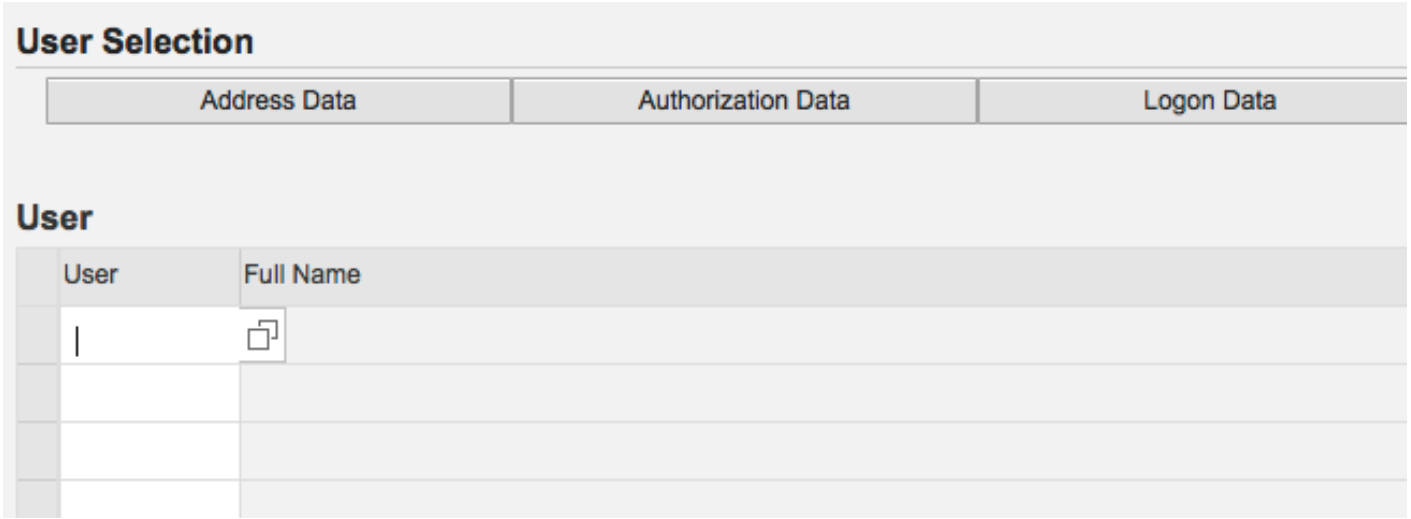
Delete user ID – SU01

- 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

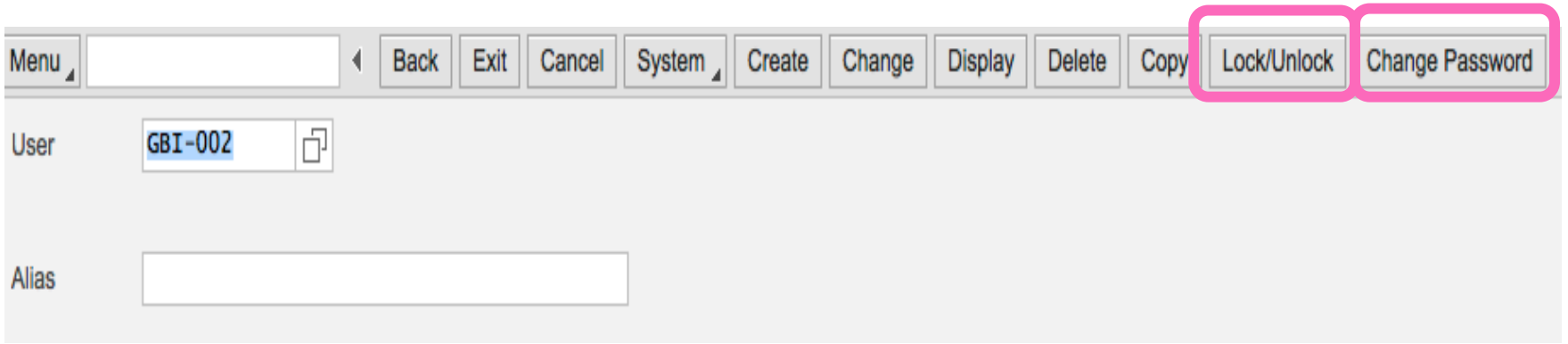


SU10: Mass User Maintenance



- 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 ??!?

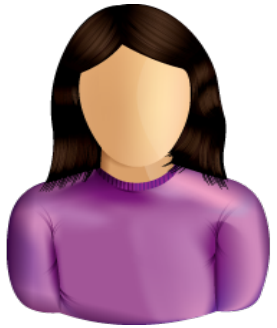
- Designed to protect system availability, integrity and privacy
- Authentication methods provided in SAP include:
  - Logon with password (Dialog user)
  - Secure Network Communications (SNC) (Single sign on?)
  - Client Certificates (interfaces?)
  - SAP Logon Tickets
  - Pluggable Authentication Services

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 (e) 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 issues
- 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
  - 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)
- Alternate User Authentication
  - Single sign-on concept
  - Client Certificates
  - How Controlled

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

- 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

SAP Security Role Design

Role Definition: Task Level

- 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

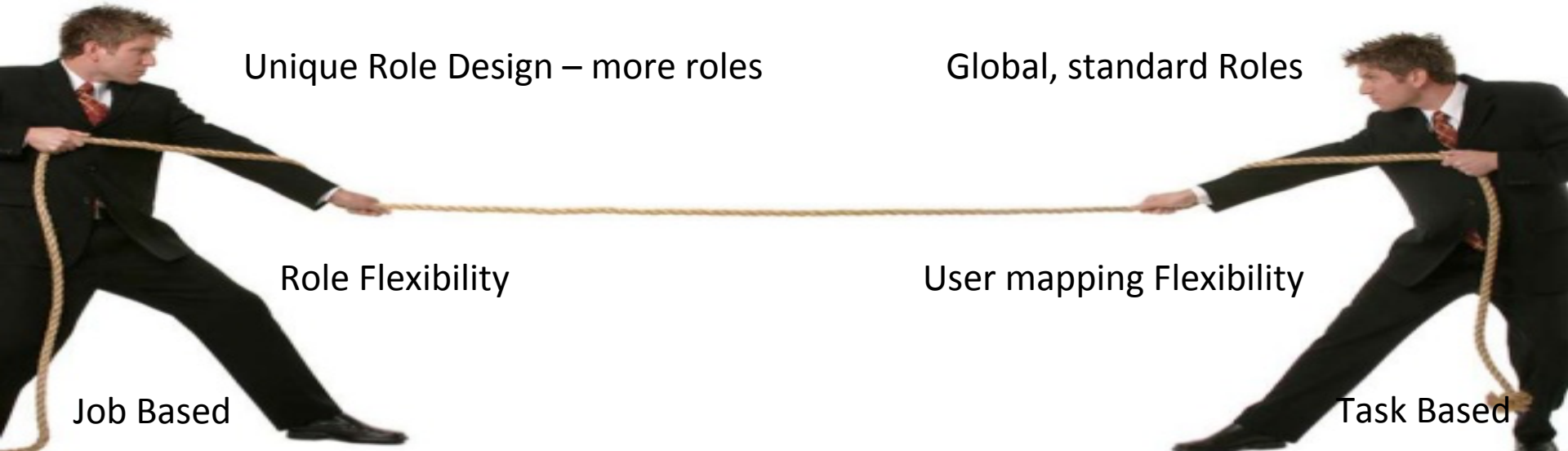
User Role Mapping Complexity

Smaller, more Roles

Simpler role maintenance

Risk of SOD via multiple roles assigned

Global, standard Roles



Role Flexibility

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
  - Other Couple

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

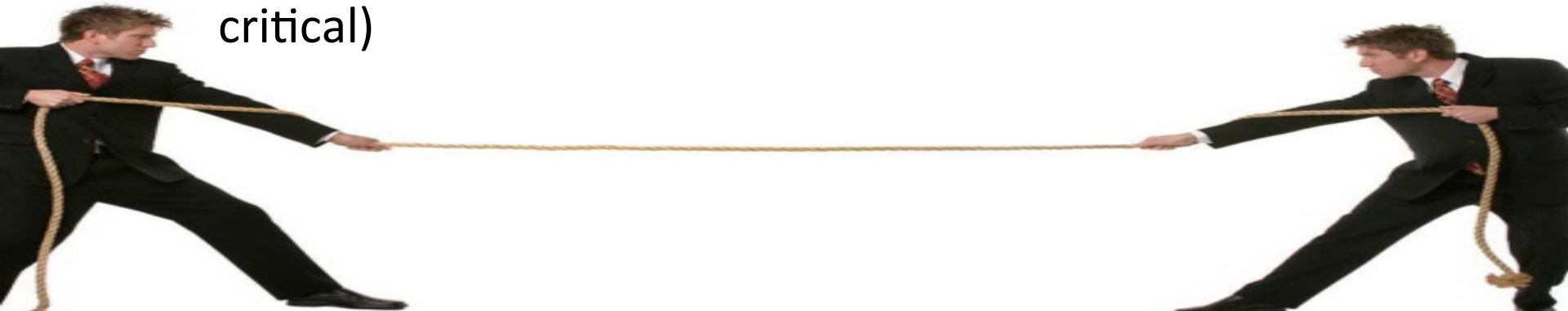
Segregation of Duties

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

Break Time

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

- Agenda
  - This Class *(March 23)*: Steps 1 – 2 (Risks / Control & Organizational design with SOD)
  - Next 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 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

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