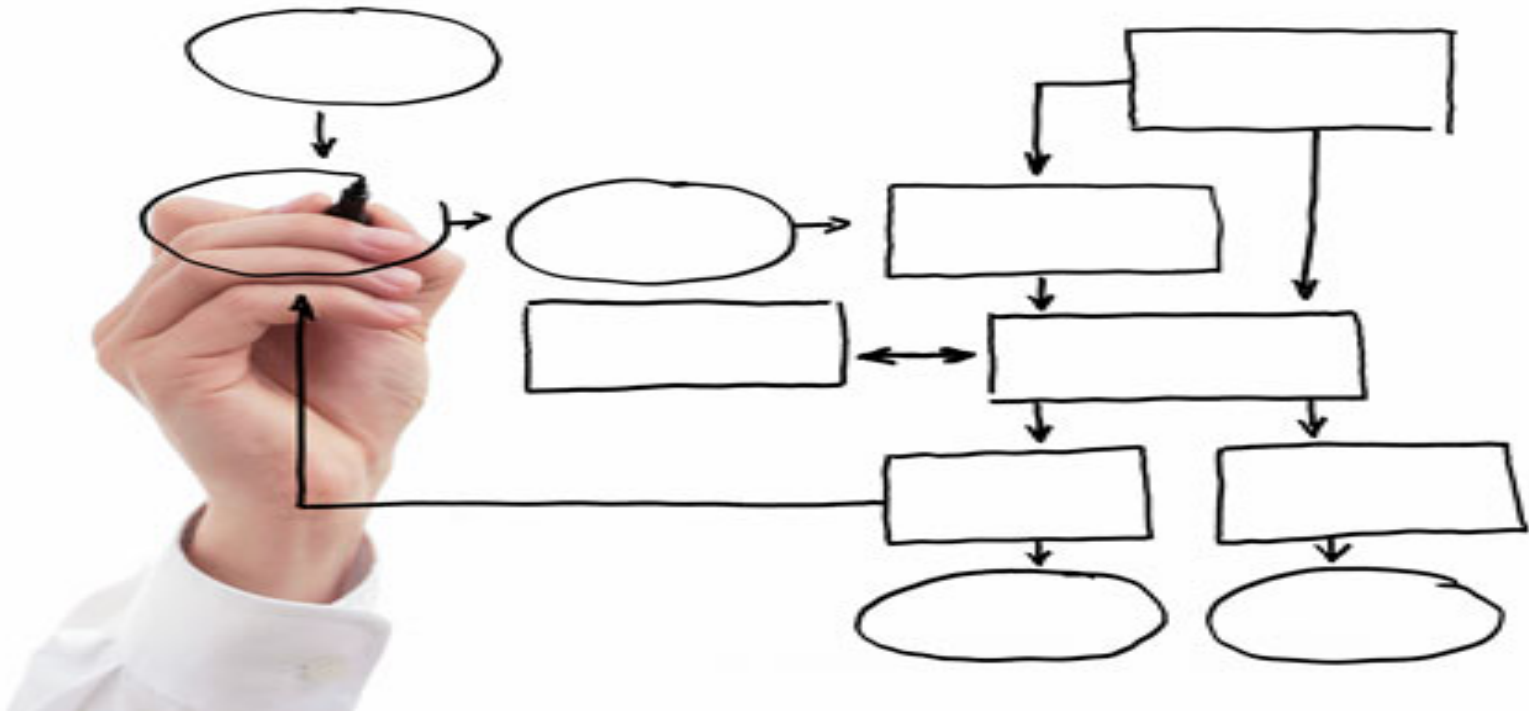


MIS 5121: Business Process, ERP Systems & Controls  
Week 9: *Security: User Management,  
Segregation of Duties (SOD)*



MIS 5121: Business Process, ERP Systems & Controls

Real World Control Failures:

By: Yizhou An

# Control Failure: HP's Acquisition of Autonomy

- Background:

- ❖ Hewlett-Packard Company (HP): American multinational information technology company
- ❖ Autonomy Corp: UK enterprise software company
- ❖ HP acquired Autonomy in October 2011 for \$11.1 billion in cash
- ❖ Expectation: Autonomy's data analytics and search technology would boost HP's big data prowess

- Control Failures:

- ❖ "Serious accounting improprieties, misrepresentation and disclosure failures" prior to the acquisition
- ❖ Some former members of Autonomy's management team inflated Autonomy's financial metrics by:
  - ❖ Selling some hardware at a loss – booked those hardware sales as high-margin software sales
  - ❖ Selling software to value-added resellers – inflated revenue
  - ❖ Booking all future revenue for software subscription at once – inflated revenue again
- ❖ In turn, Autonomy accused HP of a "textbook example of defensive stalling" to conceal evidence of its own prior knowledge and gross mismanagement and undermining of the company



# Control Failure: HP's Acquisition of Autonomy

- Results:

- ❖ Mike Lynch, the former CEO of Autonomy was fired by HP in 2012
- ❖ HP wrote down \$8.8 billion of its \$11.1 billion acquisition
- ❖ HP lost \$26 billion of its market value, 37% decline in its stock price in three months
- ❖ HP had reached a \$100 million settlement in a shareholder lawsuit

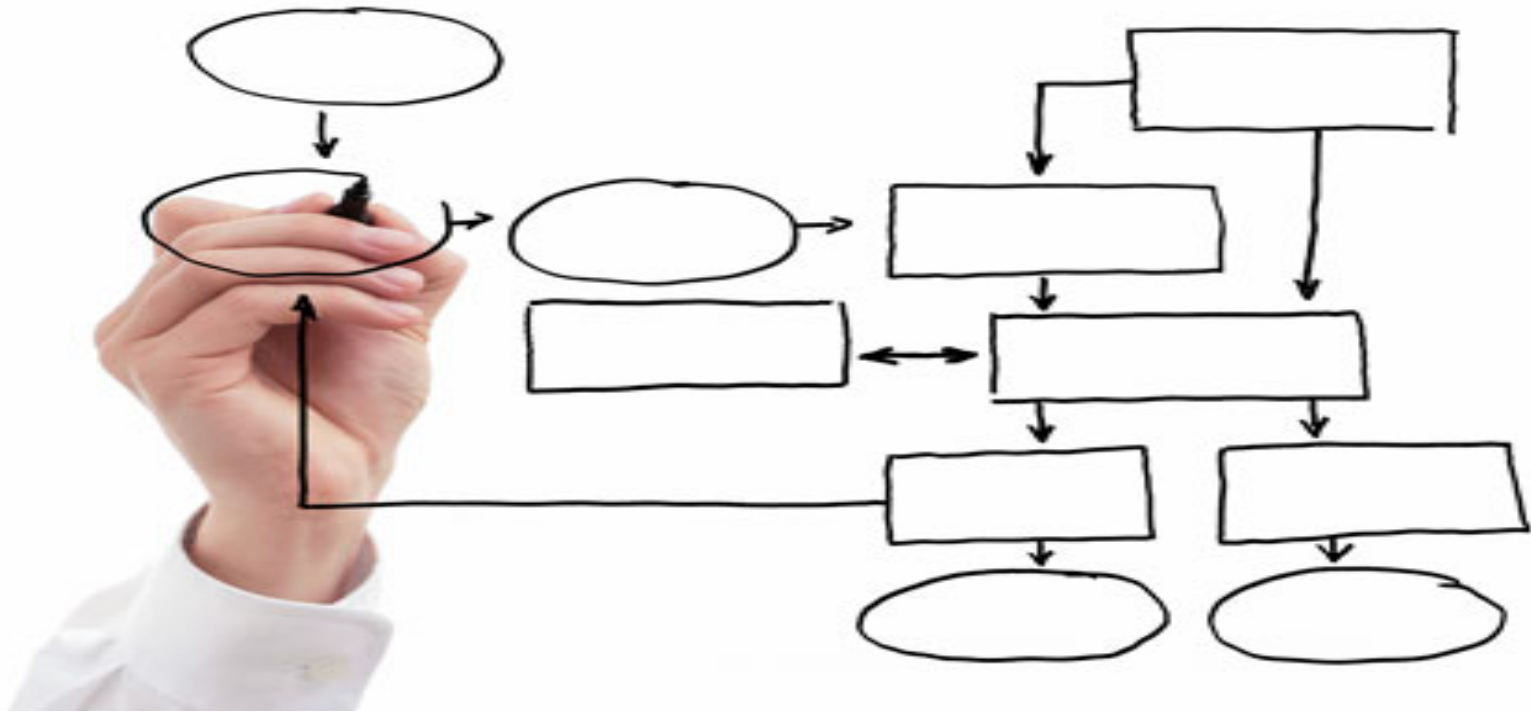
- What Could / Should those in Authority Have Done Different?:

- ❖ Adequate due diligence and analysis before and during acquisition
- ❖ Enhance external auditing to disclose Autonomy's accounting fraud

- Reference:

- ❖ [http://www.mercurynews.com/business/ci\\_28280542/hp-pay-100m-settle-case-tied-autonomy-deal](http://www.mercurynews.com/business/ci_28280542/hp-pay-100m-settle-case-tied-autonomy-deal)
- ❖ <http://www.forbes.com/sites/francinemckenna/2012/11/20/hewlett-packards-autonomy-allegations-a-material-writedown-puts-all-four-audit-firms-on-the-spot/#6f87e5226da4>
- ❖ <http://money.cnn.com/2012/11/20/technology/enterprise/hp-earnings/>
- ❖ <https://bus.wisc.edu/mba/corporate-finance-investment-banking/blog/2012/12/12/hewlett-packard-auditing-implications-of-the-autonomy-acquisition>





MIS 5121: Business Process, ERP Systems & Controls  
Real World Control Failures: Parmalat  
By: Shuvam DasGupta

# Control Failure: Parmalat, Italy

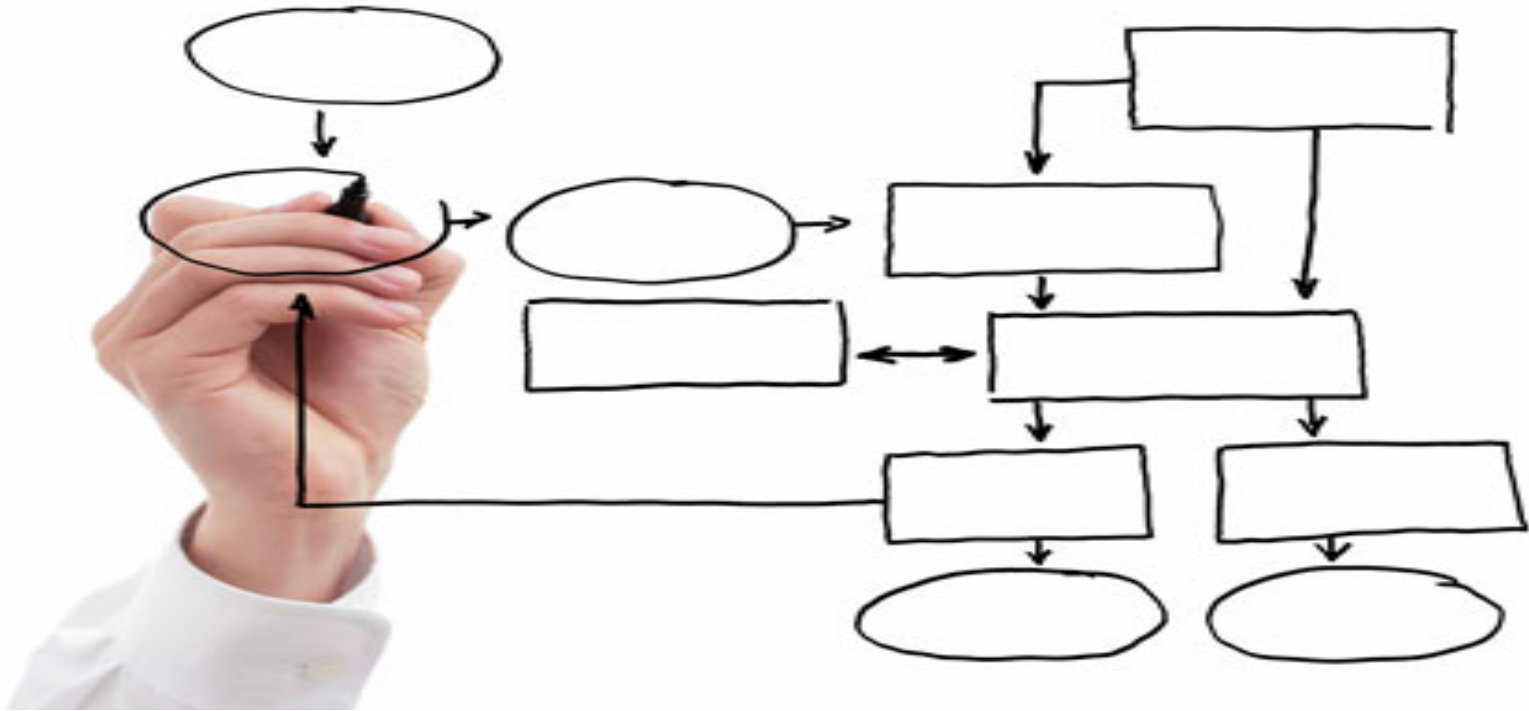


- Background:
  - ❖ Parmalat is multinational Italian dairy and food corporation
  - ❖ \$8.5 billion to \$12 billion in vanished assets – Europe’s biggest bankruptcy
- Control Failures: 2002 - 2005
  - ❖ Falsified accounts over a 15-year period
  - ❖ 38% of Parmalat’s assets was shown to be help in a \$4.9 billion BAC account – which never existed
  - ❖ Managers created assets to offset almost \$16.2 billion in liabilities
  - ❖ Used derivatives and other complex financial transactions to shore up the balance sheet
  - ❖ Accountants hide losses of almost \$10 billion
  - ❖ CEO Calisto Tanzi misplaced almost \$990 in company funds for his own use
  - ❖ Tanzi’s Family controls 51% of the company
- Results:
  - ❖ Calisto Tanzi, his son Stefano, brother Giovanni, former CFO Fausto Tonna, Former board members, company’s lawyers went under investigation
  - ❖ Tanzi was arrested on suspicion of fraud, false accounting, embezzlement and misleading the investors
  - ❖ Implementation of the a new financial market monitoring system modeled on Britain’s FSA by Italy government
- What Could / Should those in Authority Have Done Different?:
  - ❖ Proper implementation of Corporate governance
  - ❖ Supervision of the international or that country’s regulatory aspects
  - ❖ A proper monitoring mechanism for the company’s control structure

## • Reference:

- ❖ <http://www.bloomberg.com/news/articles/2004-01-11/how-parmalat-went-sour>
- ❖ <https://en.wikipedia.org/wiki/Parmalat>
- ❖ <http://wildonwallstreet.com/biggest-financial-scandals/>





MIS 5121: Business Process, ERP Systems & Controls

## Real World Control Failures

By Gladys Guardia

# Control Failure: Governance

- **Background**

- ❖ Sony Pictures Entertainment was hacked by group called Guardians of Peace on November 24, 2014 and the duration of the hack was unknown (some estimate a year prior to discovery of attack)
- ❖ GOP obtained access to servers and installed malware
- ❖ 10 TB of data taken including Personal Identifiable Information, Intellectual Property, emails, etc.
- ❖ Play Station Network breach in 2011- Sony Pictures Entertainment did not learn from the mistakes of this breach

- **Control Failures**

- ❖ Data retention policies were non-existent
- ❖ Data was not categorized, secured, or encrypted
- ❖ Executive Director talked auditors out of reporting failures relating to Access Controls
- ❖ Lack of corporate wide protective measures and information security training for employees
- ❖ No standardized processes such as inventory control, vulnerability assessments, employee training



# Control Failure: Governance

- **Results**

- ❖ In previous hacks, most criminals wanted credit card numbers or PII to sell- with Sony, hackers aimed for reputation damage which is tougher to quantify & continues causing harm months after
- ❖ Immediate financial damage: 10% drop of company's stock in wake of breach
- ❖ \$15 million to rebuild computer network & conduct forensic investigation attack
- ❖ Failure of properly securing employee PII brought joint lawsuits from employees for PII stolen – threat of harm due to data being posted online for anyone to grab
- ❖ Healthcare records stolen will bring more lawsuits due to the medical records protection laws California & other countries have in place

- **What Could / Should those in Authority Have Done Different?**

- ❖ Identify & segregate PII/IP
- ❖ Add layers of encryption to protect internal traffic from prying eyes
- ❖ Isolate confidential materials from central data-storage systems connected to the Internet
- ❖ Assure data loss prevention and intrusion detection systems are part of architecture
- ❖ Educate employees on information security practices company-wide

- **Reference**

- ❖ <http://www.risk3sixty.com/2014/12/19/the-sony-hack-security-failures-and-solutions/>
- ❖ <https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/>



# Remaining Exercises



- Exercise 3: Journal Entries Due: *March 21*
- Exercise 4: Segregation of Duties Due: March 31
- Final Case: Risk / Control Matrix Due: April 28
- Class Visitors: auditors Date: TBD
  - Ernst & Young – auditing manager and SAP subject matter expert
  - Discussion / Q&A format (~30 minutes)
  - Gather discussion topics and your ?'s next week

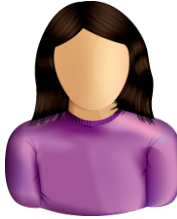
(2016)

# Security (Continued): User Management



# SAP Security: Review

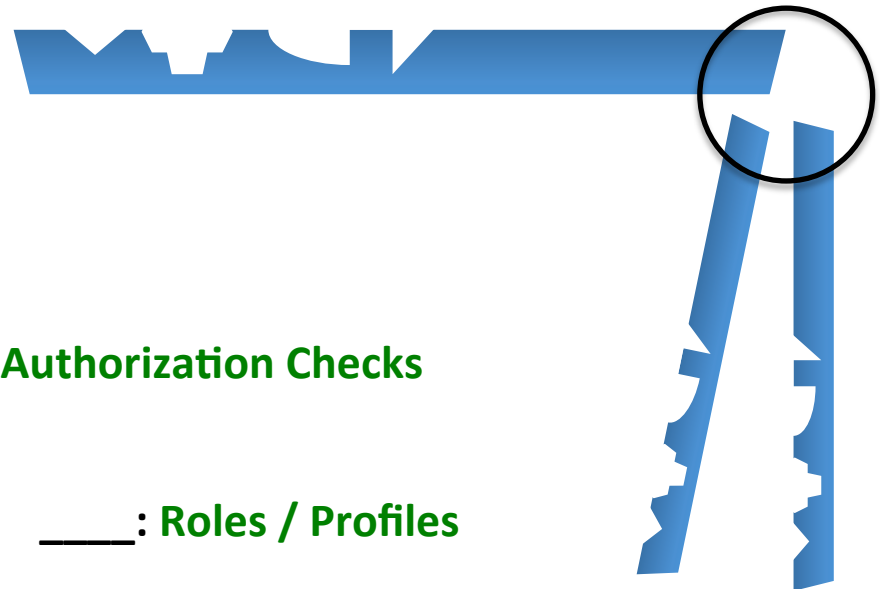
Program



User ID

\_\_\_\_\_: Authorization Object

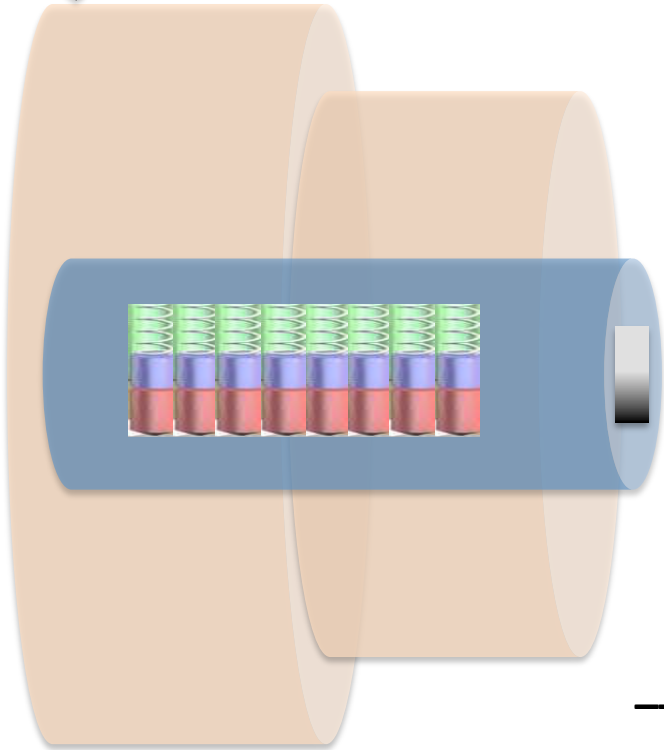
Authorization Values



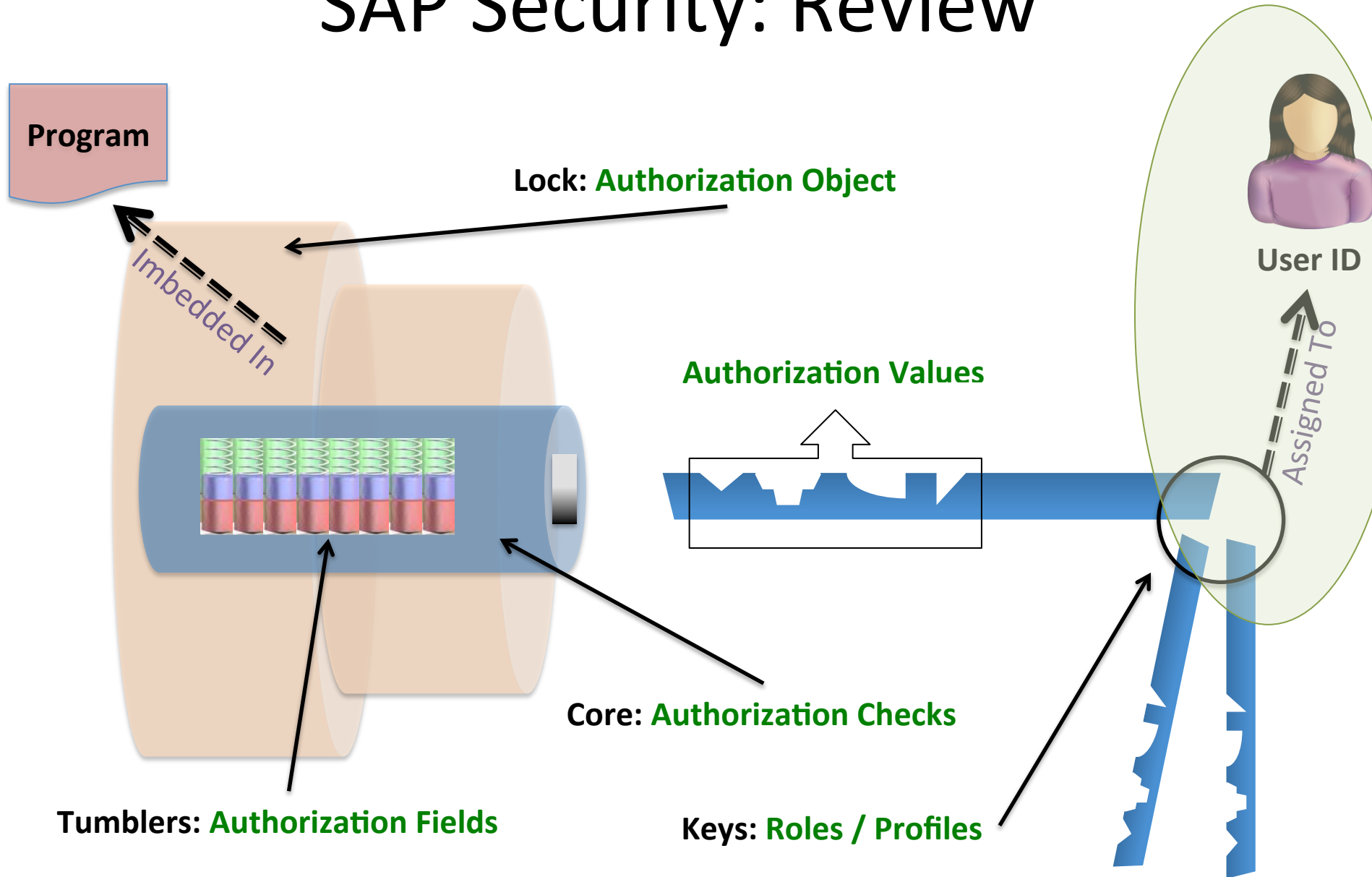
\_\_\_\_\_: Authorization Checks

\_\_\_\_\_: Authorization Fields

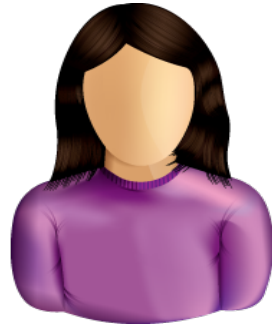
\_\_\_\_\_: Roles / Profiles



# 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

## User Maintenance: Initial Screen

Menu  ◀ Back Exit Cancel System **Create**

User

Alias

Address Logon Data SNC Defaults Parameters Roles Profiles Groups

### Person

Title

Last name

First name

Academic Title

Complete name

Language

### Work Center

Function

Department

Room Number  Floor  Building code

### Communication

Telephone  Extension

Mobile Phone

Fax  Extension

E-Mail Address

- 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

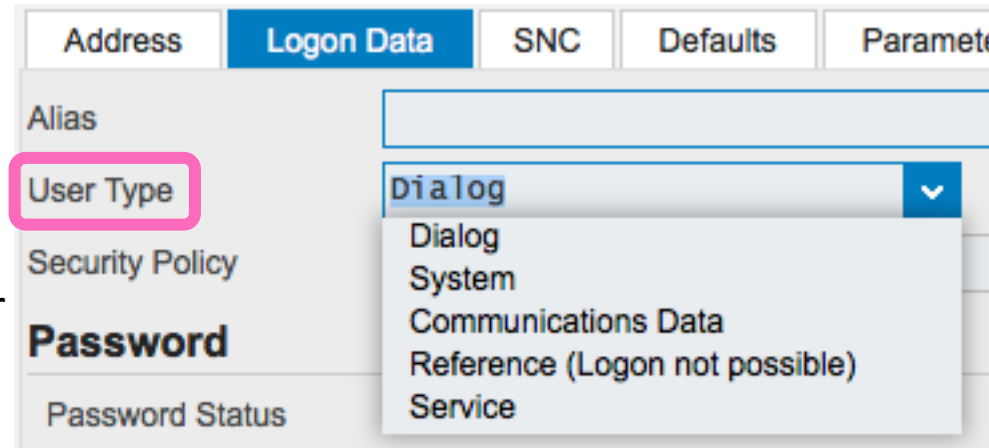
The screenshot shows the 'Logon Data' tab of a user configuration interface. The 'User Type' field is highlighted with a pink box, and its dropdown menu is open, showing options: Dialog, System, Communications Data, Reference (Logon not possible), and Service. Other visible fields include Alias, Security Policy, Password, and Password Status. The top navigation bar includes Address, Logon Data, SNC, Defaults, and Parameters.



# 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)

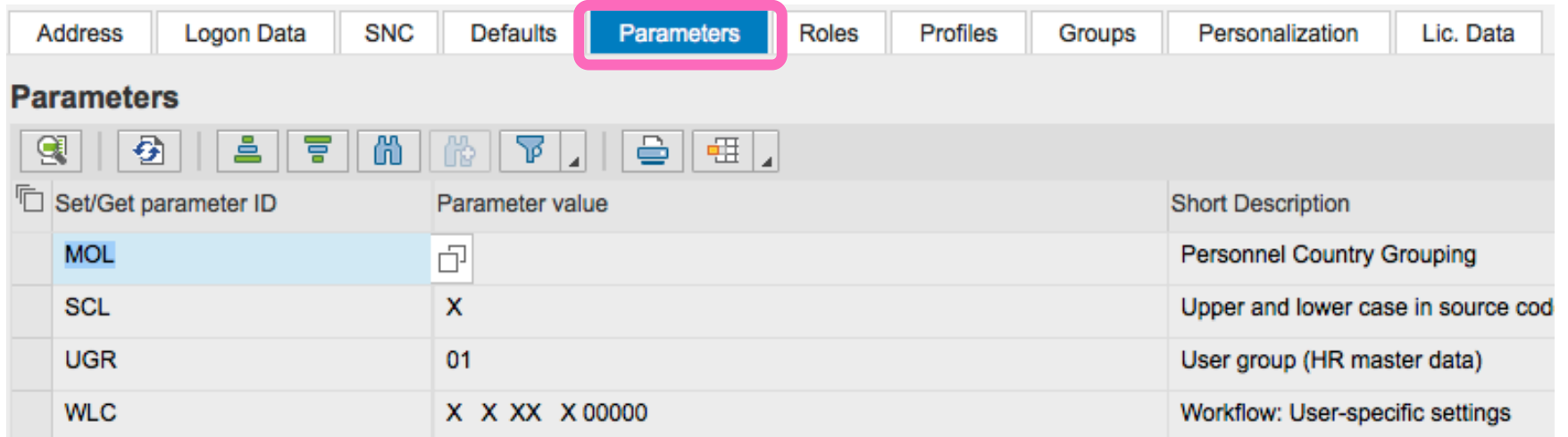
Address	Logon Data	SNC	Defaults	Parameters	Roles
Alias	<input type="text"/>				
User Type	Dialog <input type="text"/>				
Security Policy	<input type="text"/>				
<b>Password</b>					
Password Status	Productive Password				
<b>User Group for Authorization Check</b>					
User group	<input type="text" value="GBI230"/>	GBI 2.30 Group 2014			
<b>Validity Period</b>					
Valid from	<input type="text"/>				
Valid through	<input type="text"/>				

# 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

Address	Logon Data	SNC	Defaults	Parameters	Roles
Start menu		<input type="text"/>			
Logon Language		<input type="text" value="EN"/>			
Decimal Notation		<input type="text" value="1,234,567.89"/>			
Date Format		<input type="text" value="MM/DD/YYYY"/>			
Time Format (12/24h)		<input type="text" value="24 Hour Format (Example: 12:05:10)"/>			
<b>Spool Control</b>					
OutputDevice		<input type="text" value="LOCL"/>			
<input checked="" type="checkbox"/> Print immed.					
<input checked="" type="checkbox"/> Delete After Output					
<b>Personal Time Zone</b>					
Time Zone		<input type="text" value="CST"/>			
Sys. Time Zone		CST			

# Create user ID – SU01: Parameters



The screenshot shows the SAP SU01 Parameters screen. At the top, there is a navigation bar with tabs: Address, Logon Data, SNC, Defaults, Parameters (highlighted with a pink box), Roles, Profiles, Groups, Personalization, and Lic. Data. Below the navigation bar is the title 'Parameters' and a toolbar with various icons. The main area contains a table with three columns: 'Set/Get parameter ID', 'Parameter value', and 'Short Description'. The table lists several parameters, with 'MOL' selected and highlighted in blue.

Set/Get parameter ID	Parameter value	Short Description
MOL	X	Personnel Country Grouping
SCL	X	Upper and lower case in source cod
UGR	01	User group (HR master data)
WLC	X X XX X 00000	Workflow: User-specific settings

- 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

**Database selections**

Material

Plant

Storage location

Batch

**Stock Type Selection**

Also Select Special Stocks

Also Select Stock Commitments

**List Display**

Special Stock Indicator

Display version

Display Unit of Measure

No Zero Stock Lines

Decimal Place as per Unit

**Selection of Display Levels**

Company Code

Plant

**Performance Assist**

← → 📄 🛠️

**Plant**

Key uniquely identifying

**Technical Information**

**Screen Data**

Report

Program Name

Screen Number

**GUI Data**

Program Name

Status

**Field Data**

Table Name

Table category

Field Name

Data Element

**Parameter ID**

**Field Description for Batch Input**

Screen Field

*F1 - Help*

# Create user ID – SU01: Roles / Profiles

The screenshot shows the SAP SU01 user master record for user SU01. The 'Roles' tab is selected and highlighted with a pink box. Below the tabs, there is a 'Reference User' field. The main section is titled 'Role Assignments' and contains a table with the following data:

Status	Role	Start Date	End Date	Role name
<input checked="" type="checkbox"/>	Z_BPI	07/23/2014	12/31/9999	ZBPI Role for UCC Faculty Access to More Functio
<input checked="" type="checkbox"/>	Z_GBI_SCC_US	06/26/2013	12/31/9999	All SAP_ALL authorizations (except BC, CA, HR)

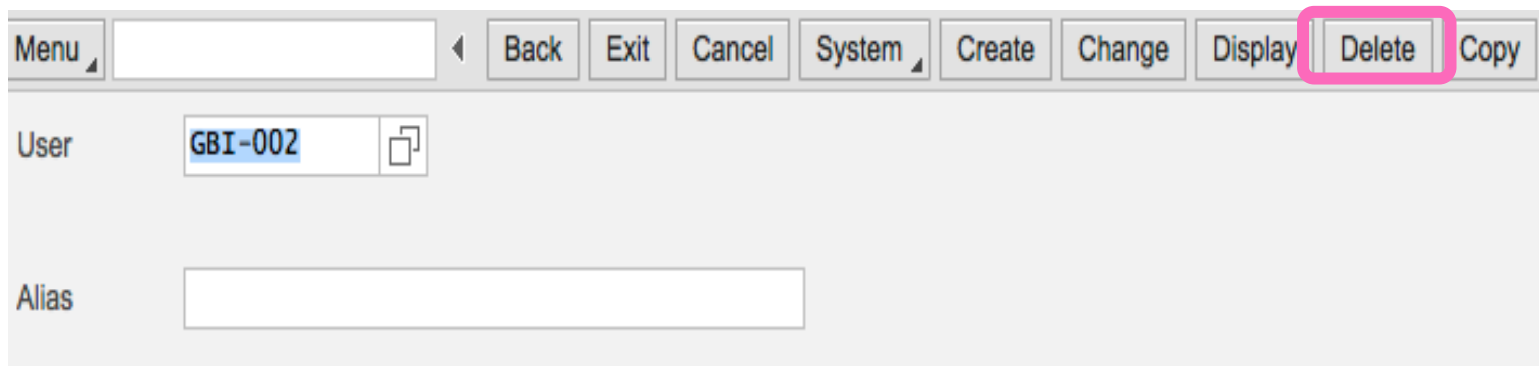
- Security Repository for User
- Note: Effective dates for Roles
- Profiles tab auto-populated based on Roles Assigned
- Details from these tabs pulled into User Buffer during Logon

The screenshot shows the SAP SU01 user master record for user SU01, with the 'Profiles' tab selected and highlighted with a pink box. Below the tabs, there is a table titled 'Assigned Authorization Profiles' with the following data:

Profile	Type	Text
IDES_DEVELOP	<input type="checkbox"/>	All authorizations without user authorizations
IDES_USER	<input type="checkbox"/>	Profile for IDES user (w/o development and customizing)
T-A4010009	<input checked="" type="checkbox"/>	Profile for role Z_GBI_SCC_US
T-A40100091	<input checked="" type="checkbox"/>	Profile for role Z_GBI_SCC_US
T-A40100092	<input checked="" type="checkbox"/>	Profile for role Z_GBI_SCC_US
T-A40100093	<input checked="" type="checkbox"/>	Profile for role Z_GBI_SCC_US
T-A40100094	<input checked="" type="checkbox"/>	Profile for role Z_GBI_SCC_US
T-A40100095	<input checked="" type="checkbox"/>	Profile for role Z_GBI_SCC_US

# 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




The screenshot shows a user management interface. At the top, there is a menu bar with buttons for 'Menu', 'Back', 'Exit', 'Cancel', 'System', 'Create', 'Change', 'Display', 'Delete', and 'Copy'. The 'Delete' button is highlighted with a pink rectangular border. Below the menu bar, there is a 'User' field containing the text 'GBI-002' and a copy icon. Below the 'User' field, there is an 'Alias' field which is currently empty.

# SU10: Mass User Maintenance

**User Selection**

Address Data	Authorization Data	Logon Data
--------------	--------------------	------------

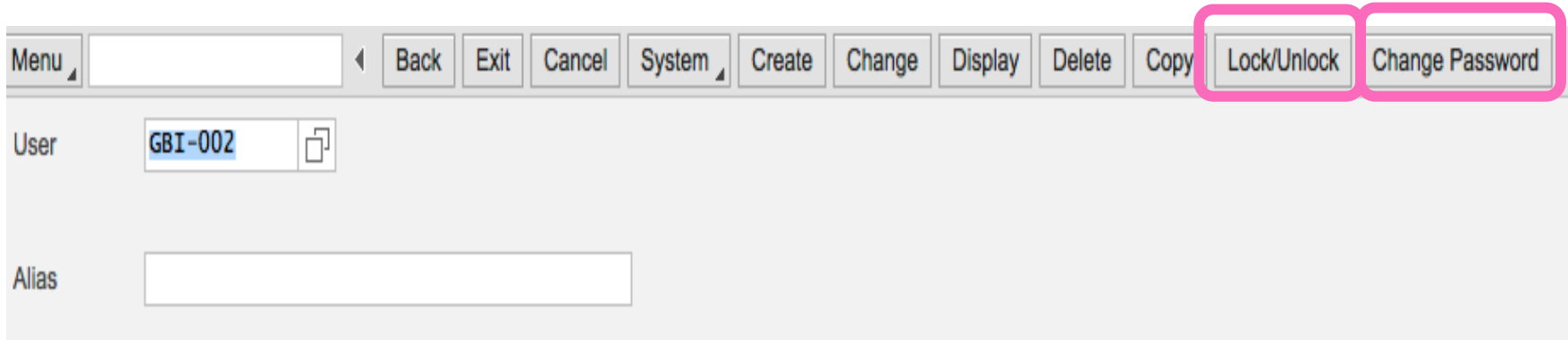
**User**

User	Full Name
	

- Same action – multiple IDs
- Limited data tabs (e.g. Address, Authorizations, ...)
- When would you use?



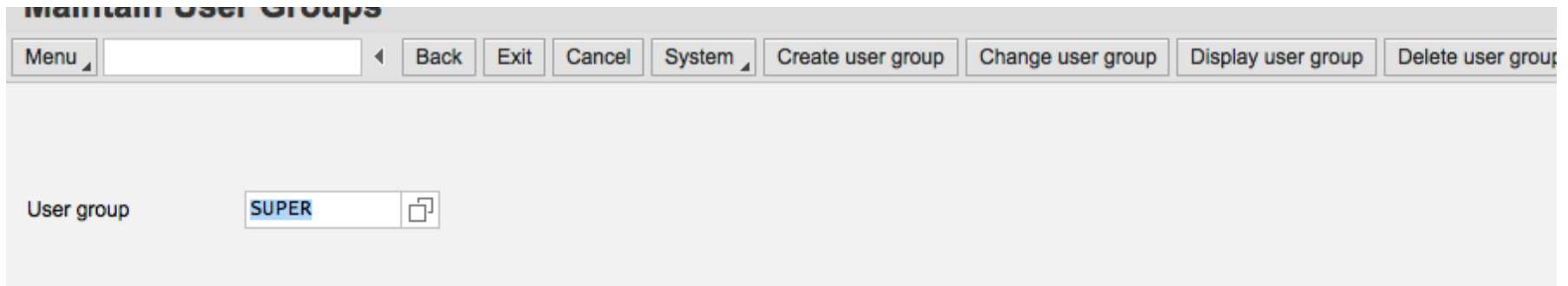
# SU01 / SU10: Lock / Unlock



The screenshot shows a user management interface. At the top, there is a menu bar with buttons for 'Back', 'Exit', 'Cancel', 'System', 'Create', 'Change', 'Display', 'Delete', 'Copy', 'Lock/Unlock', and 'Change Password'. The 'Lock/Unlock' and 'Change Password' buttons are highlighted with a pink border. Below the menu bar, there is a 'User' field containing the text 'GBI-002' and a copy icon. Below the 'User' field, there is an 'Alias' field which is currently empty.

- 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

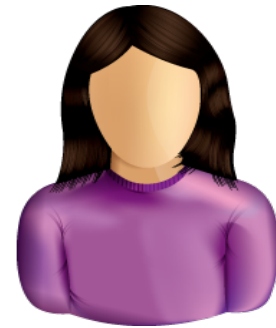
Alignment of client policies and auditor judgment is important

# 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 (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 many 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 **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

Job Based

User Role Mapping Complexity

Smaller, more Roles

Simpler role maintenance

Risk of SOD via multiple roles assigned

Global, standard Roles

User mapping Flexibility

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



# 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

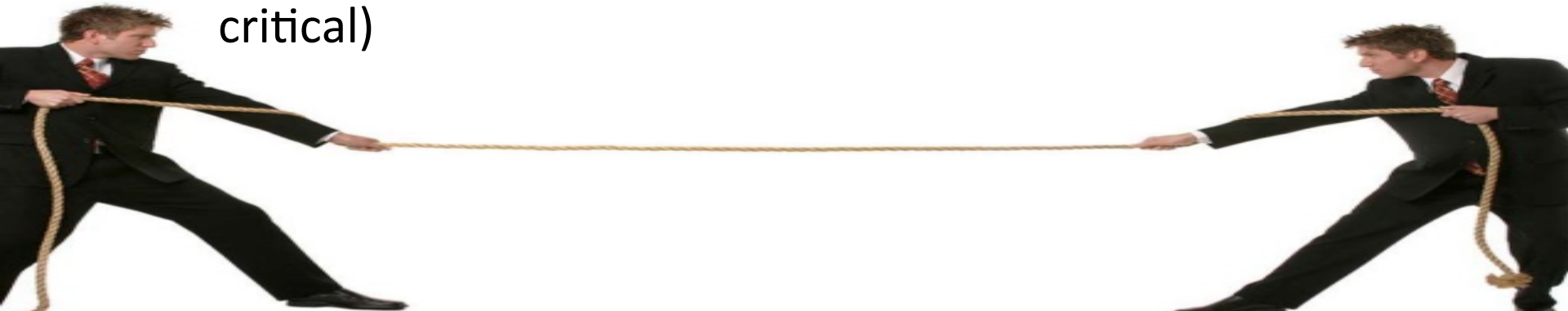


## Other names

- 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 21*): Steps 1 – 2 (Risks / Control & Organizational design with SOD)
  - Next Class (*March 28*): Step 3 - 4 (Paper process to system process with SOD and authorizations to design)
  - *Due March 31 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