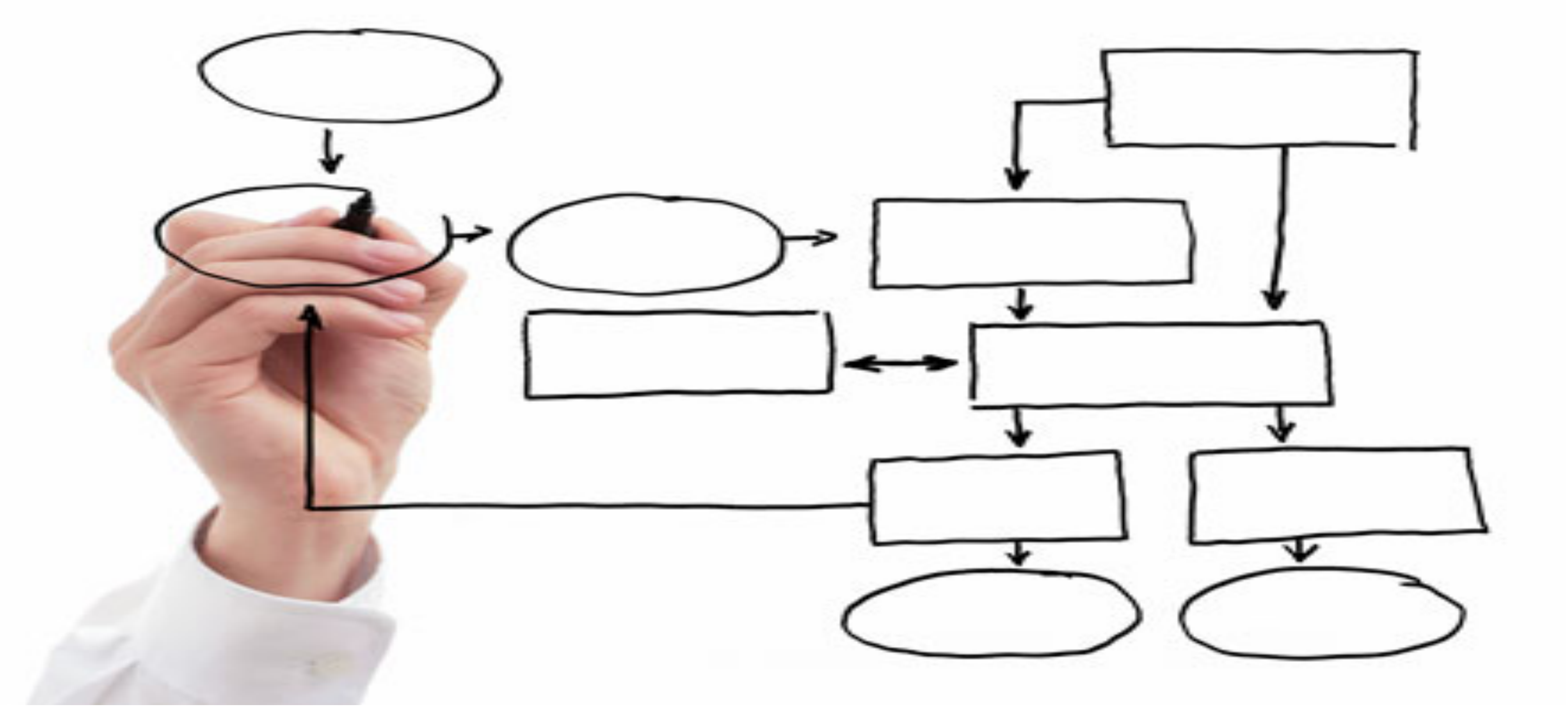


MIS 5121:Business Process, ERP Systems & Controls

Week 8: *Security 2 – Roles*

Financial Processes and Controls 2

FOX | MIS

Management Information Systems

Edward Beaver

Edward.Beaver@temple.edu

ff

Video: Record the Class

Class Logistics

- Exercise 3 due Thursday October 27 end-of-day
- 2 additional in-class sessions - Alter Hall 603
  - November 14
  - December 12

- Real World Control Failure Presentation
  - Schedule (you're deadline) in Roster / Schedule / Teams
  - Post your responses as new 'Post' on blog
    - I'll send e-mail with invitation
    - Post as 'new' post with link to contents (e.g. drop box, google file, …)
    - Be sure to assign category or 'Real World Control….' to your post

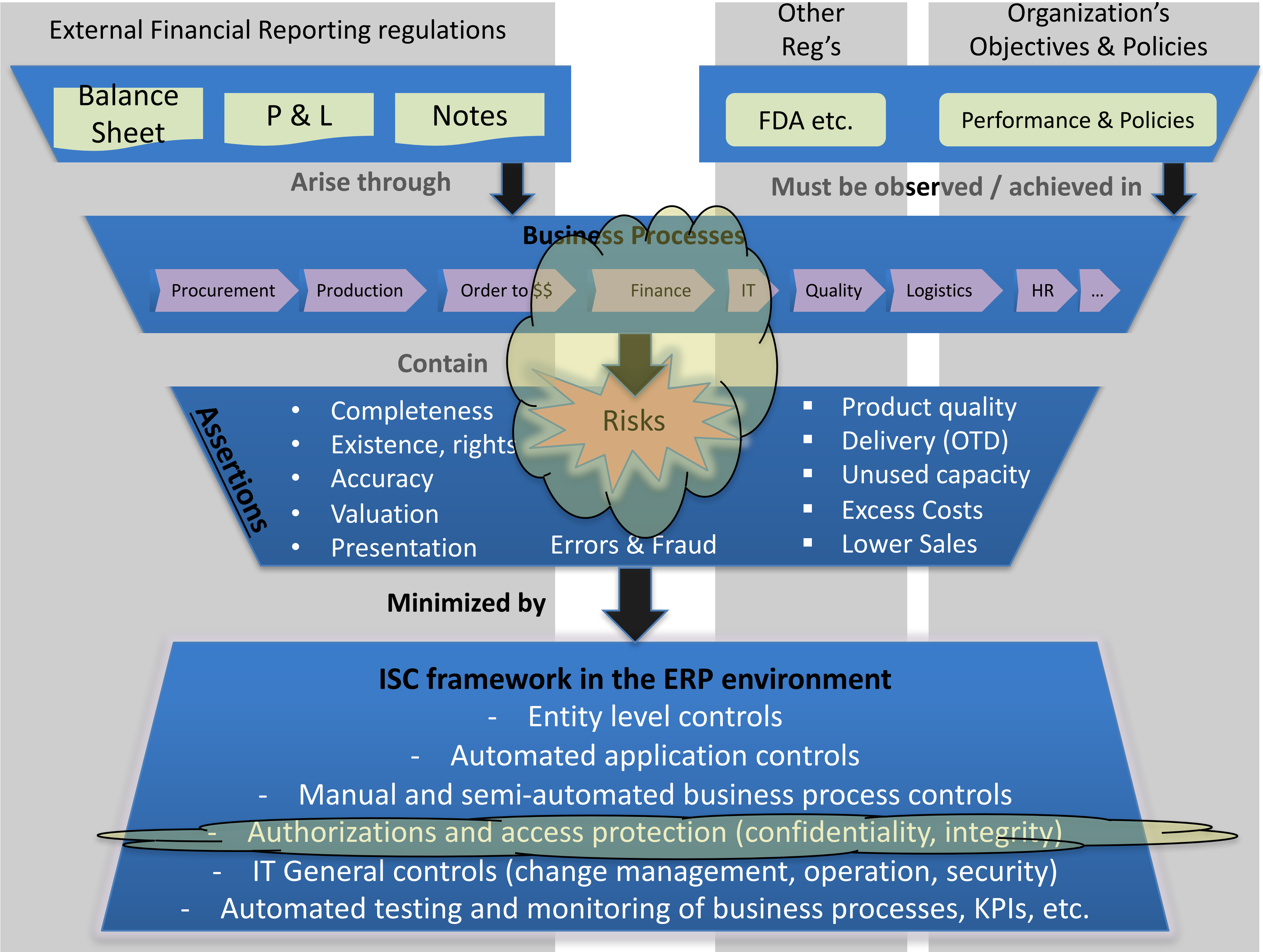
Discussion

- ❖ Something really new, different you learned in this course in last week

YOU LEARN SOMETHING NEW EVERY DAY

- ❖ 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?



External Financial Reporting regulations

Balance Sheet

P & L

Notes

Other Reg's

Organization's Objectives & Policies

FDA etc.

Performance & Policies

Arise through

Must be observed / achieved in

Business Processes

Procurement

Production

Order to $$

Finance

IT

Quality

Logistics

HR

...

Contain

Risks

Assertions

- Completeness
- Existence, rights
- Accuracy
- Valuation
- Presentation

Errors & Fraud

- Product quality
- Delivery (OTD)
- Unused capacity
- Excess Costs
- Lower Sales

Minimized by

ISC framework in the ERP environment

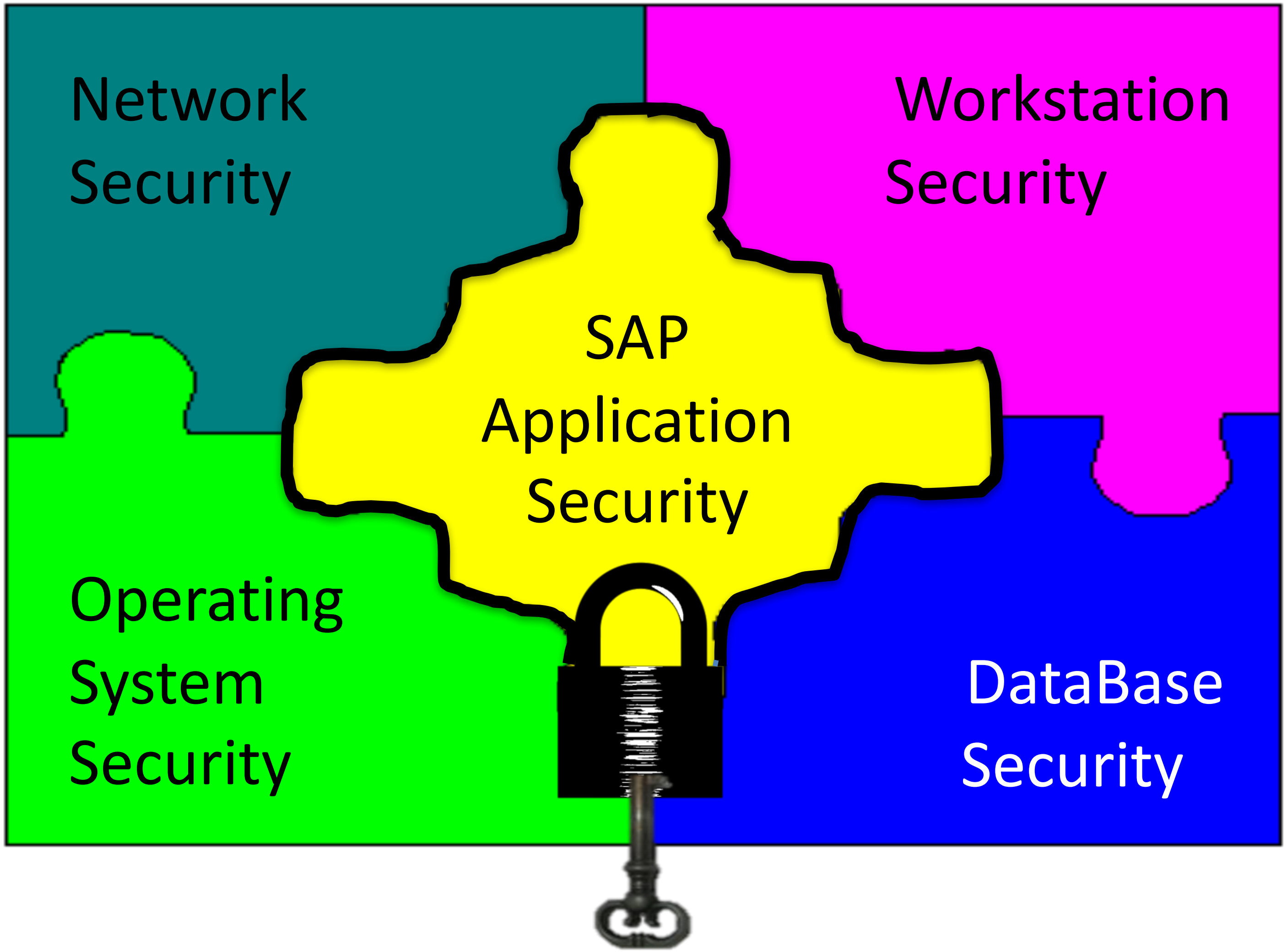
- Entity level controls
- Automated application controls
- Manual and semi-automated business process controls
- Authorizations and access protection (confidentiality, integrity)
- IT General controls (change management, operation, security)
- Automated testing and monitoring of business processes, KPIs, etc.

Security: SAP Authorization Concept

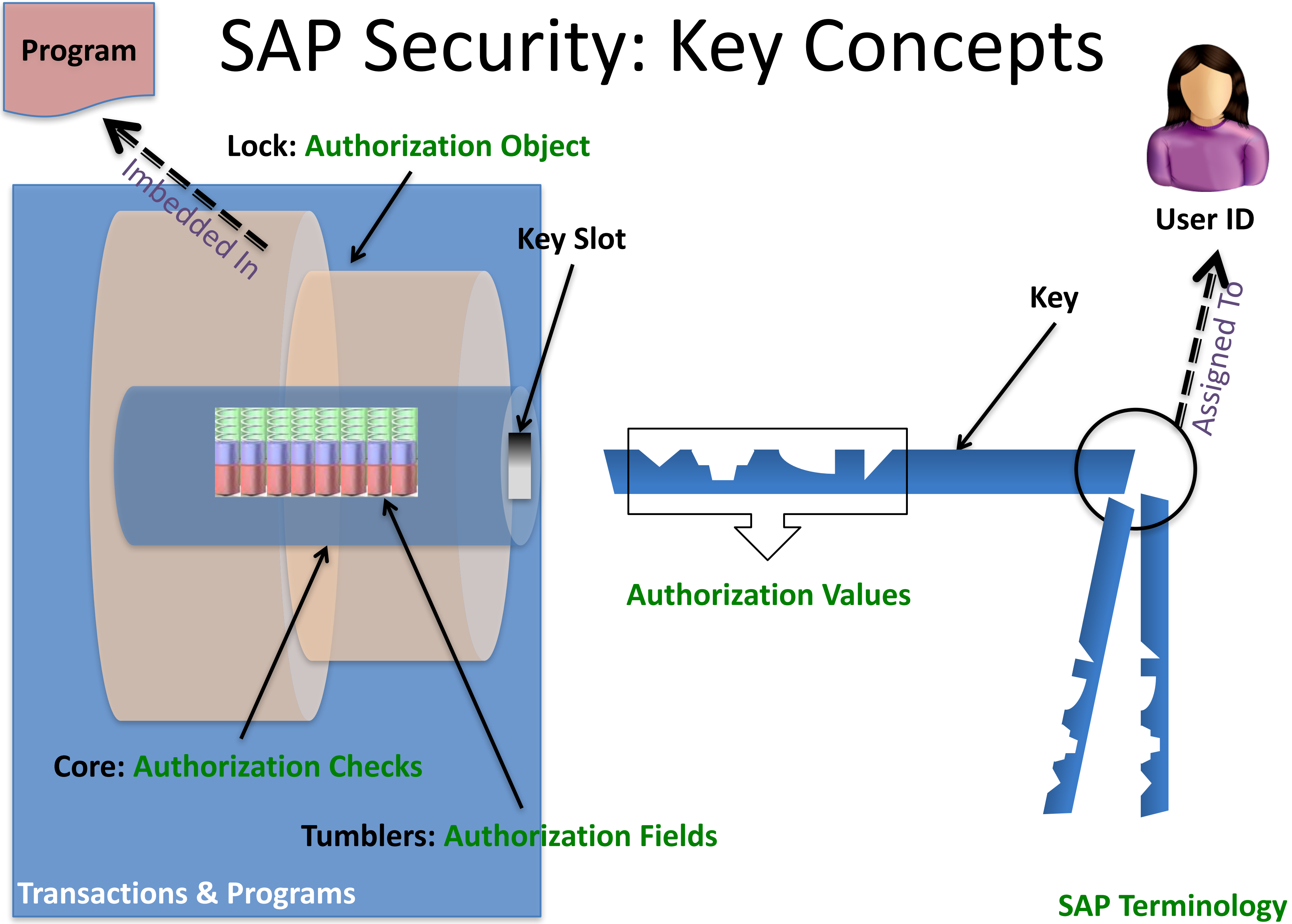
Key Information Technology Risks

- **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

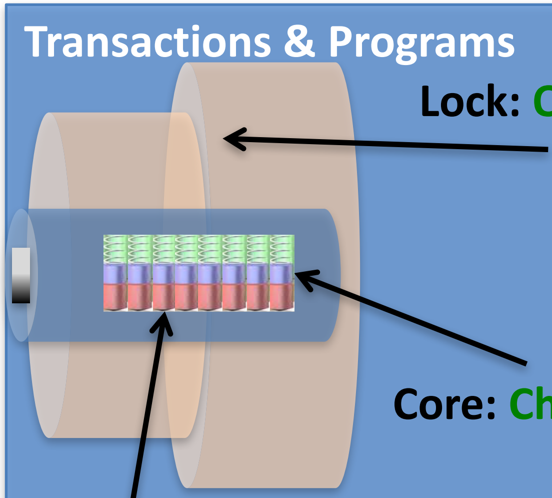


SAP Security: Key Concepts



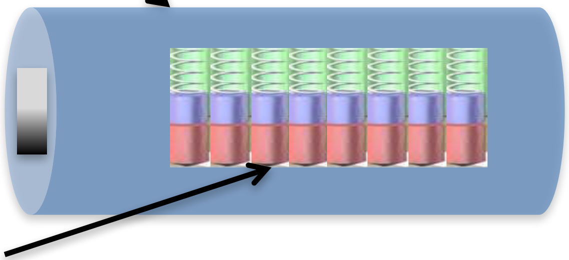
SAP Security Terminology

- **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 **AND**ed 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

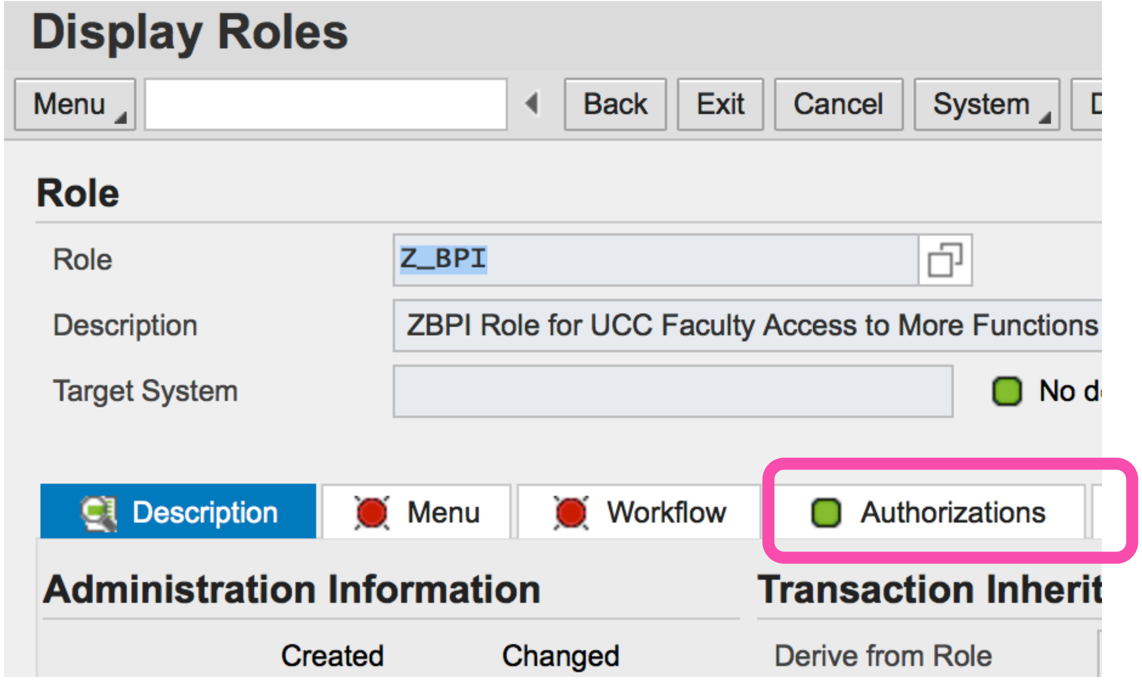
- **Authority Check:** (the lock 'core')
  - Program statement(s)
  - Checks the user's authorizations buffer for fields and values (based on the referenced authorization object)



- **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



Display Roles

Role

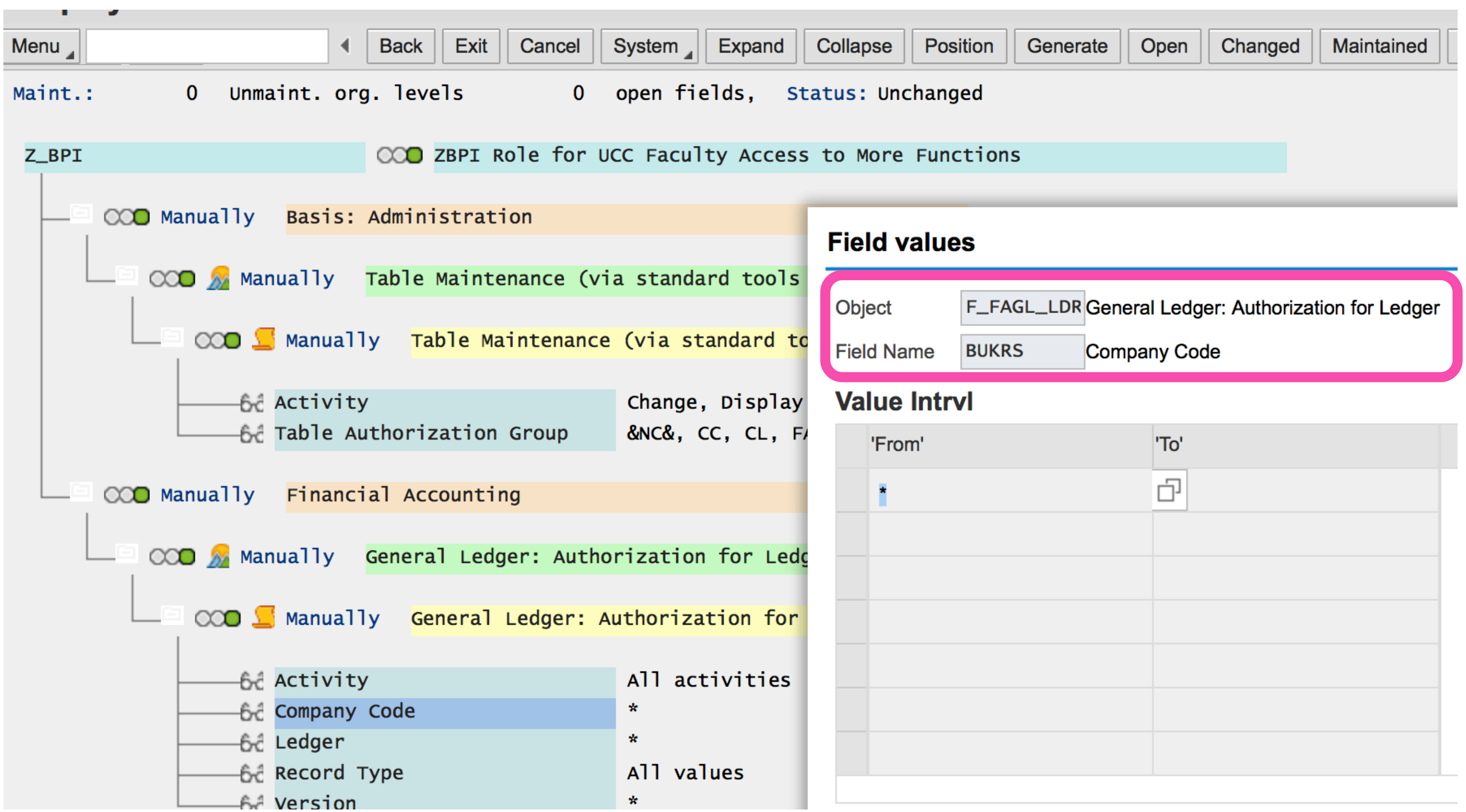
Role: Z_BPI

Description: ZBPI Role for UCC Faculty Access to More Functions

Target System:

SAP Example

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



Maint.: 0 Unmaint. org. levels 0 open fields, Status: Unchanged

Z_BPI ZBPI Role for UCC Faculty Access to More Functions

- Manually Basis: Administration
  - Manually Table Maintenance (via standard tools
    - Manually Table Maintenance (via standard to
      - Activity Change, Display
      - Table Authorization Group &NC&, CC, CL, F
- Manually Financial Accounting
  - Manually General Ledger: Authorization for Ledg
    - Manually General Ledger: Authorization for
      - Activity All activities
      - Company Code *
      - Ledger *
      - Record Type All values
      - Version *

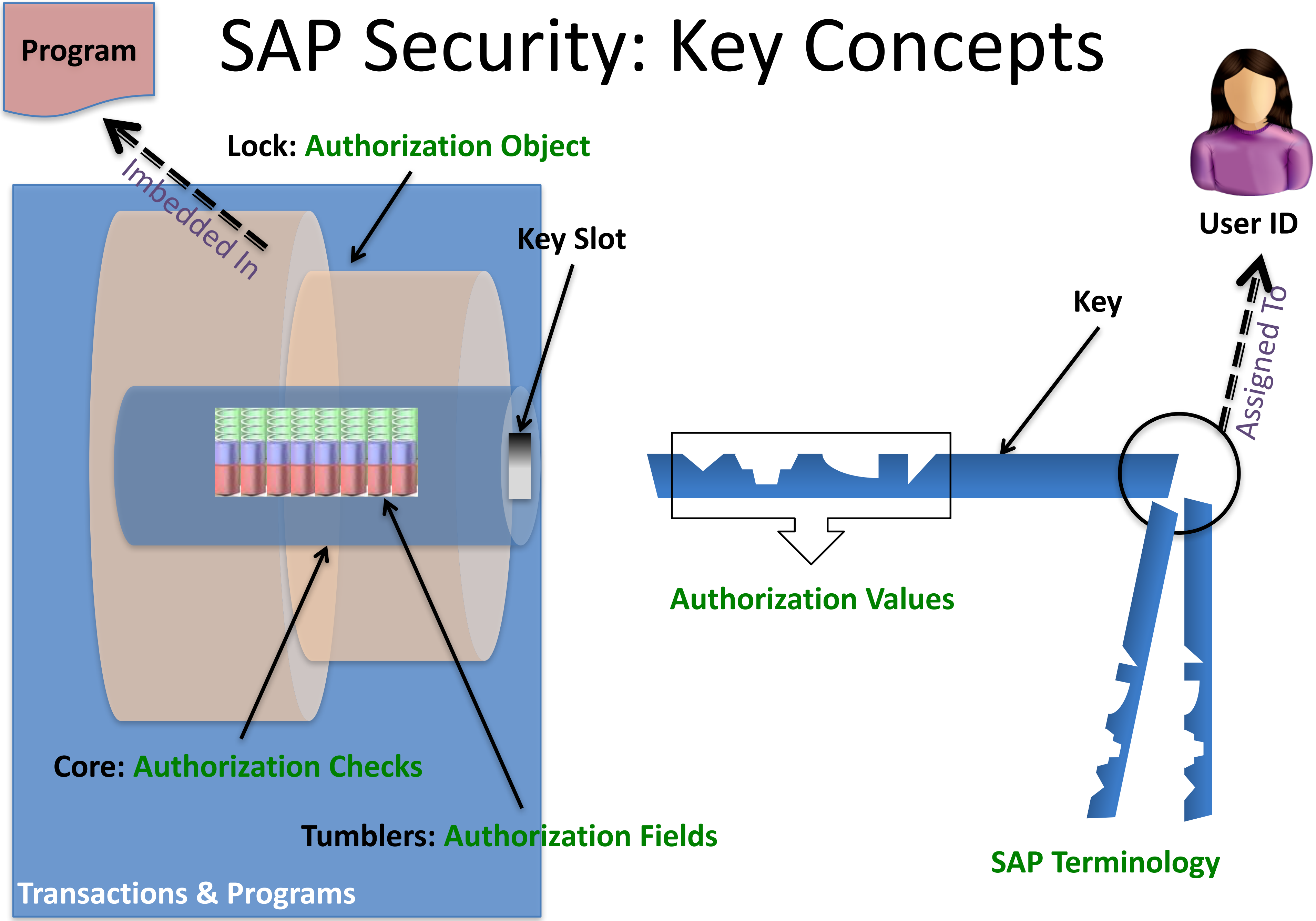
Field values

Object	F_FAGL_LDR	General Ledger: Authorization for Ledger
Field Name	BUKRS	Company Code

Value Intrvl

'From'	'To'
*	

SAP Security: Key Concepts



Program

Imbedded In

Lock: Authorization Object

Key Slot

Core: Authorization Checks

Tumblers: Authorization Fields

Transactions & Programs

User ID

Assigned To

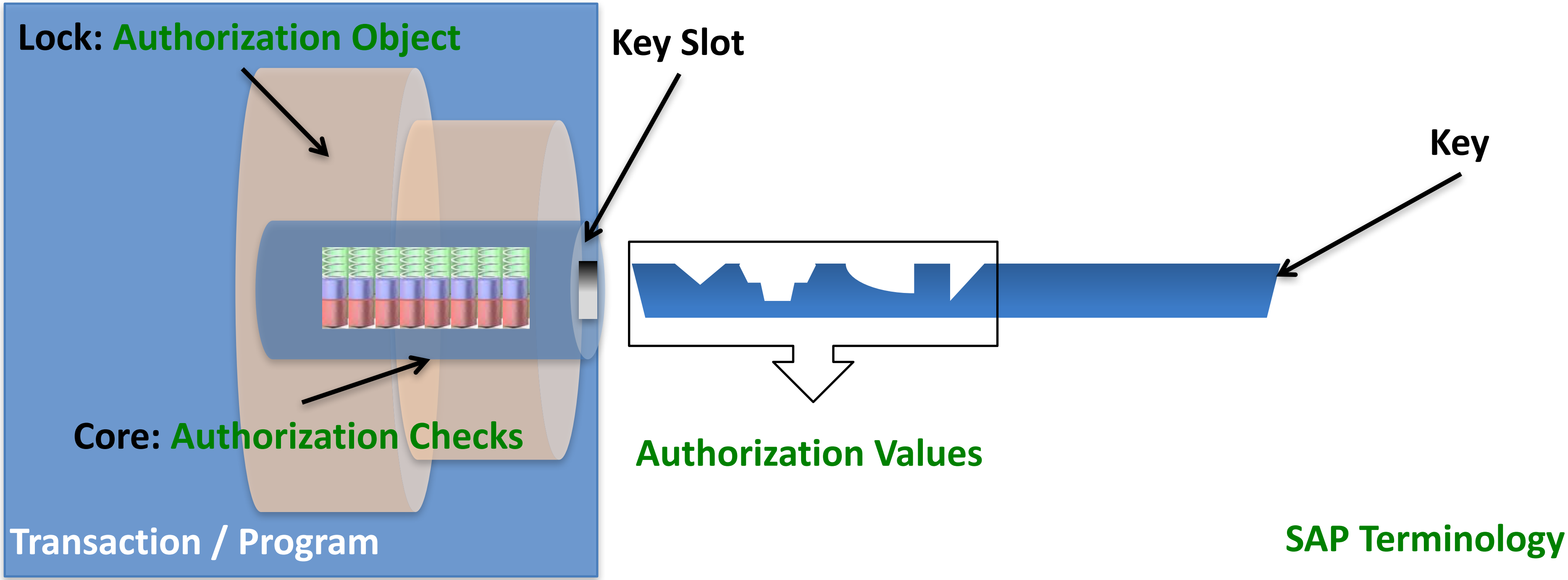
Key

Authorization Values

SAP Terminology

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 **OR**ed together



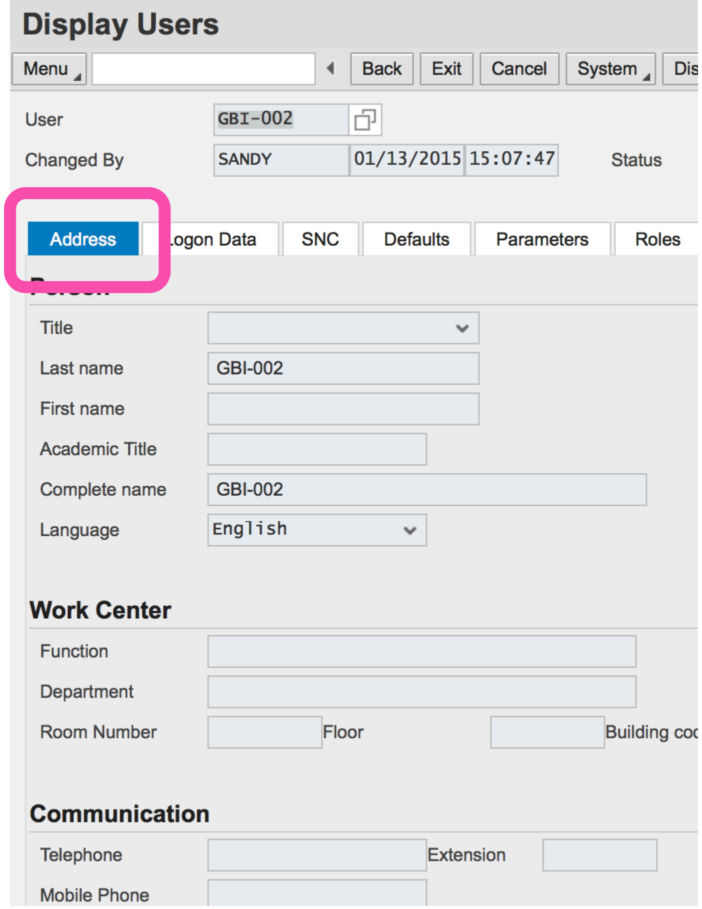
SAP Security Terminology

- **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"

SAP User IDs

Transaction: **SU01 / SU01D**
Select Role: ‘user ID’



Display Users

User	GBI-002			
Changed By	SANDY	01/13/2015	15:07:47	Status

Person

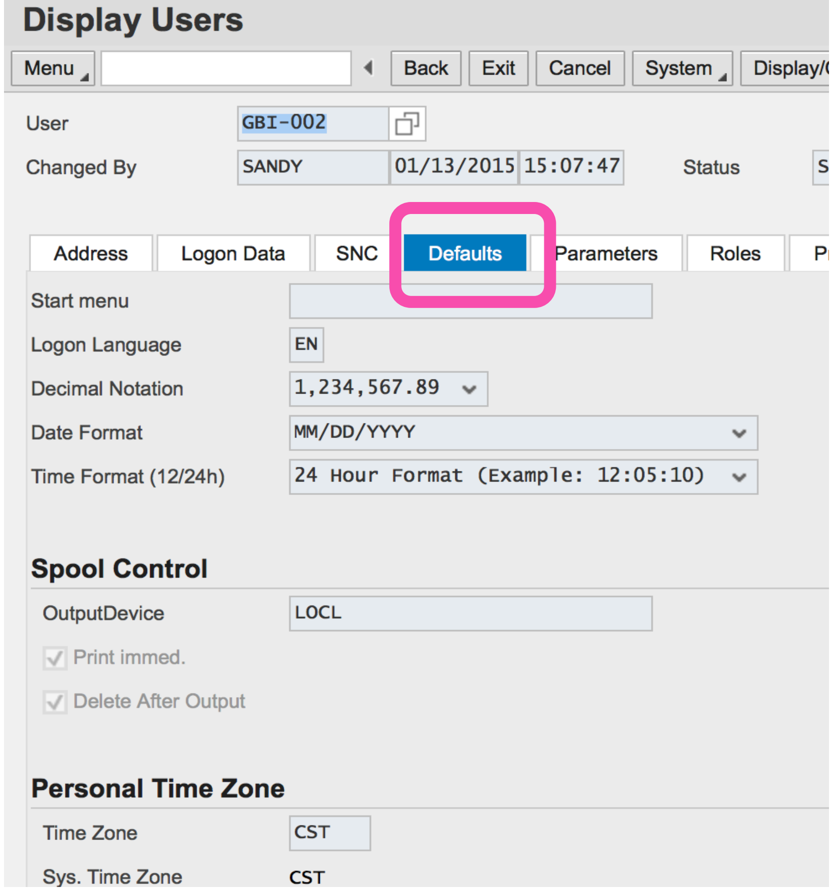
Title	
Last name	GBI-002
First name	
Academic Title	
Complete name	GBI-002
Language	English

Work Center

Function				
Department				
Room Number		Floor		Building coc

Communication

Telephone		Extension	
Mobile Phone			



Display Users

User	GBI-002			
Changed By	SANDY	01/13/2015	15:07:47	Status S

Start menu	
Logon Language	EN
Decimal Notation	1,234,567.89
Date Format	MM/DD/YYYY
Time Format (12/24h)	24 Hour Format (Example: 12:05:10)

Spool Control

OutputDevice	LOCL

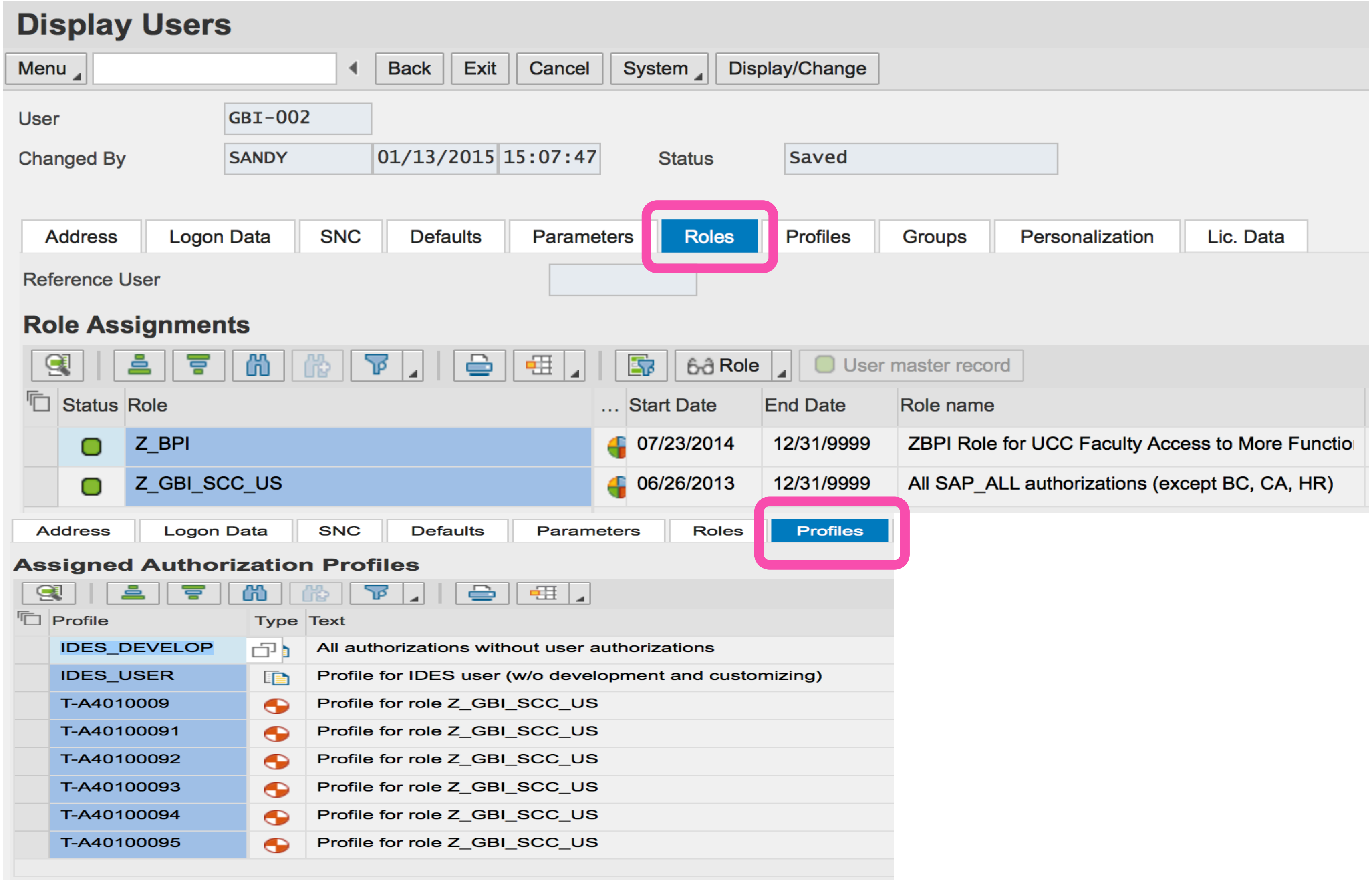
☑ Print immed.
☑ Delete After Output

Personal Time Zone

Time Zone	CST
Sys. Time Zone	CST

SAP User Roles / Profiles

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



Display Users

User	GBI-002			
Changed By	SANDY	01/13/2015	15:07:47	Status: Saved

Reference User

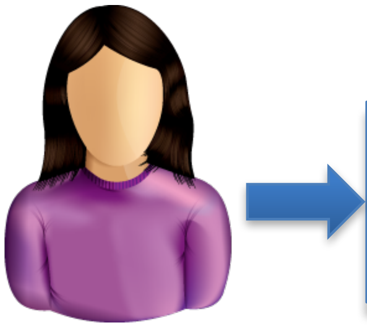
Role Assignments

Status	Role	…	Start Date	End Date	Role name
●	Z_BPI		07/23/2014	12/31/9999	ZBPI Role for UCC Faculty Access to More Functio
●	Z_GBI_SCC_US		06/26/2013	12/31/9999	All SAP_ALL authorizations (except BC, CA, HR)

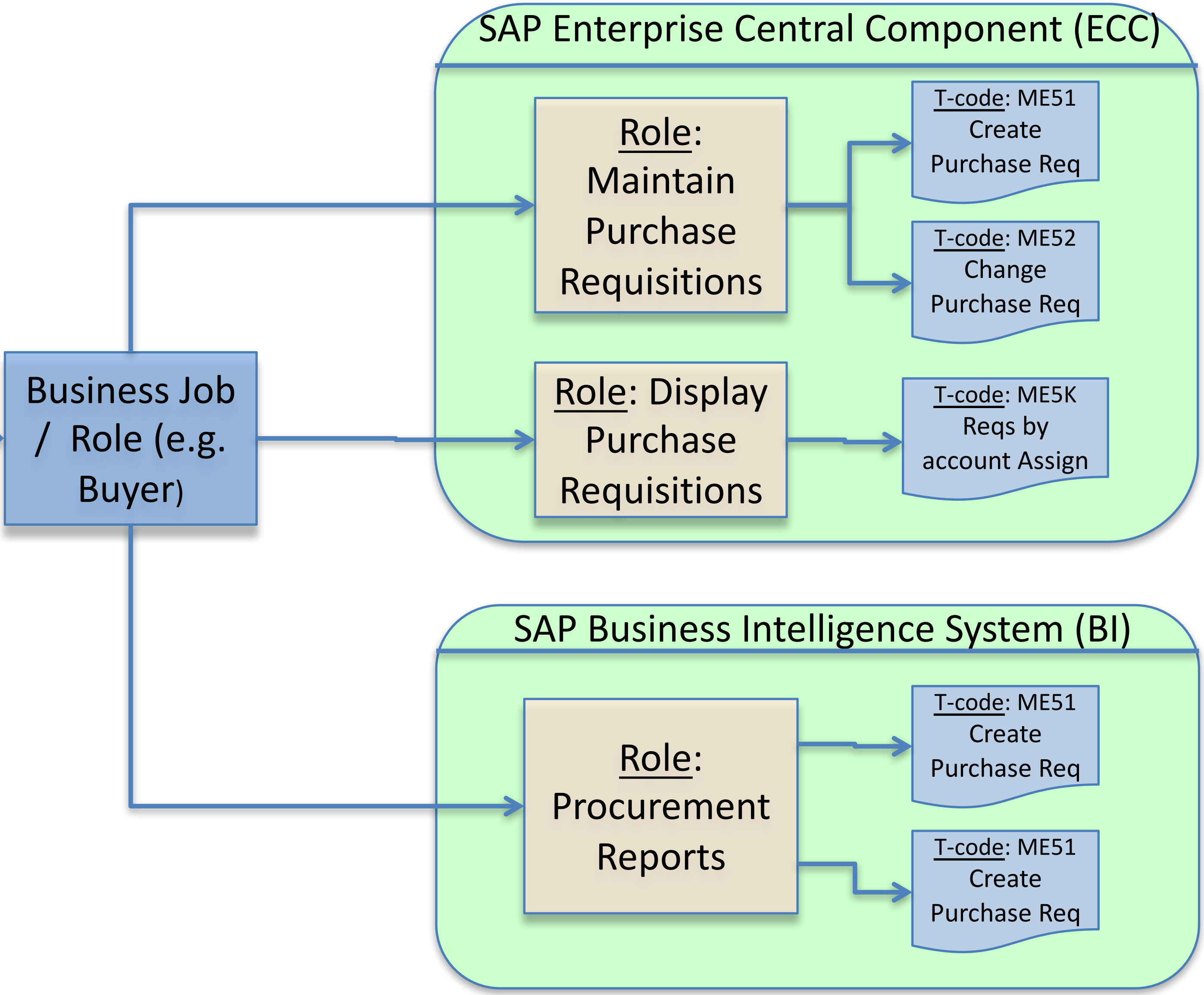
Assigned Authorization Profiles

Profile	Type	Text
IDES_DEVELOP		All authorizations without user authorizations
IDES_USER		Profile for IDES user (w/o development and customizing)
T-A4010009		Profile for role Z_GBI_SCC_US
T-A40100091		Profile for role Z_GBI_SCC_US
T-A40100092		Profile for role Z_GBI_SCC_US
T-A40100093		Profile for role Z_GBI_SCC_US
T-A40100094		Profile for role Z_GBI_SCC_US
T-A40100095		Profile for role Z_GBI_SCC_US

Application Security: Example



User



Business Job / Role (e.g. Buyer)

SAP Enterprise Central Component (ECC)

Role: Maintain Purchase Requisitions

T-code: ME51 Create Purchase Req

T-code: ME52 Change Purchase Req

Role: Display Purchase Requisitions

T-code: ME5K Reqs by account Assign

SAP Business Intelligence System (BI)

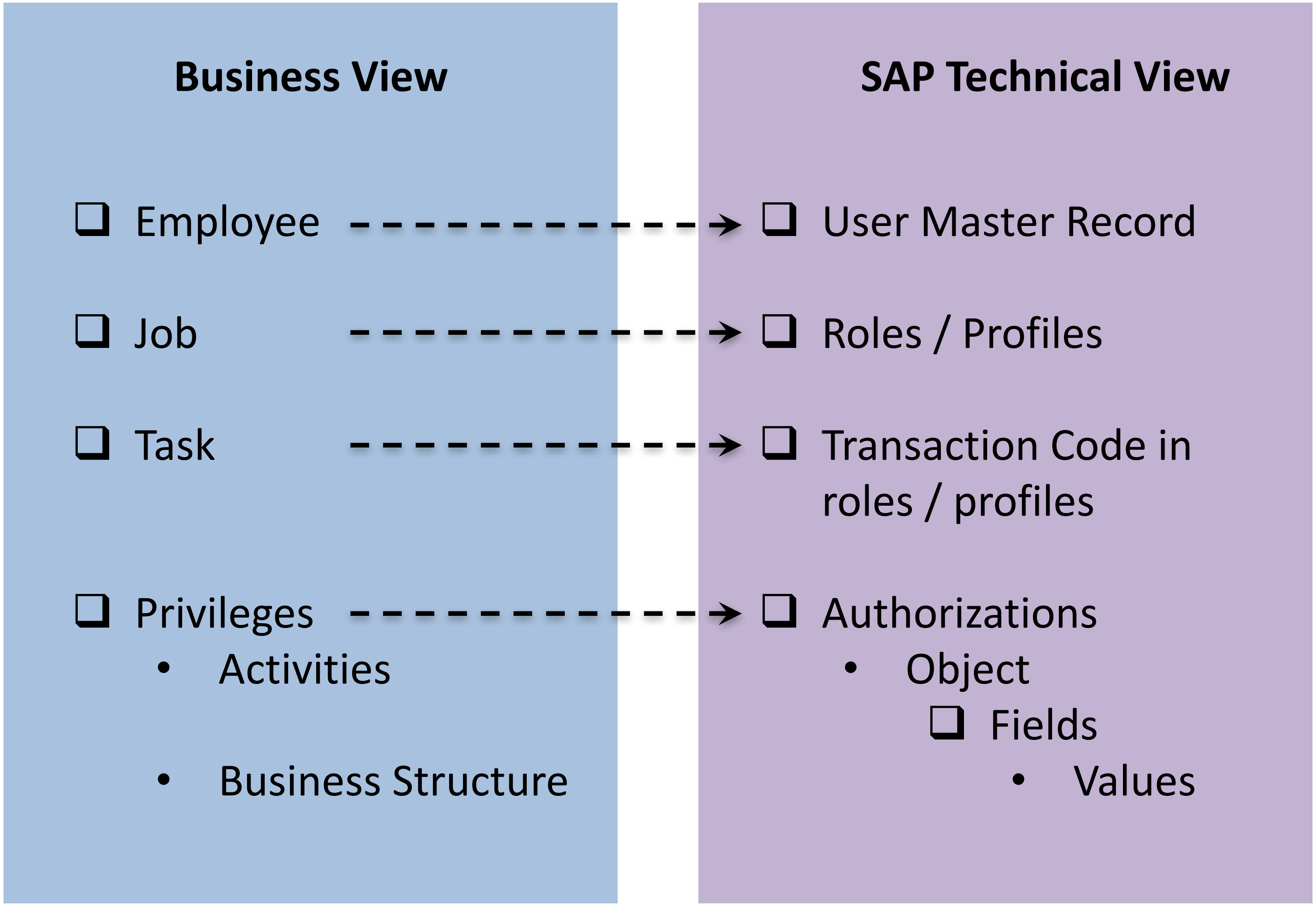
Role: Procurement Reports

T-code: ME51 Create Purchase Req

T-code: ME51 Create Purchase Req

I'VE ALWAYS WONDERED WHY YOU DECIDED TO BE A DOG..
I WAS FOOLED BY THE JOB DESCRIPTION..

SAP Security: Business vs. Technical View



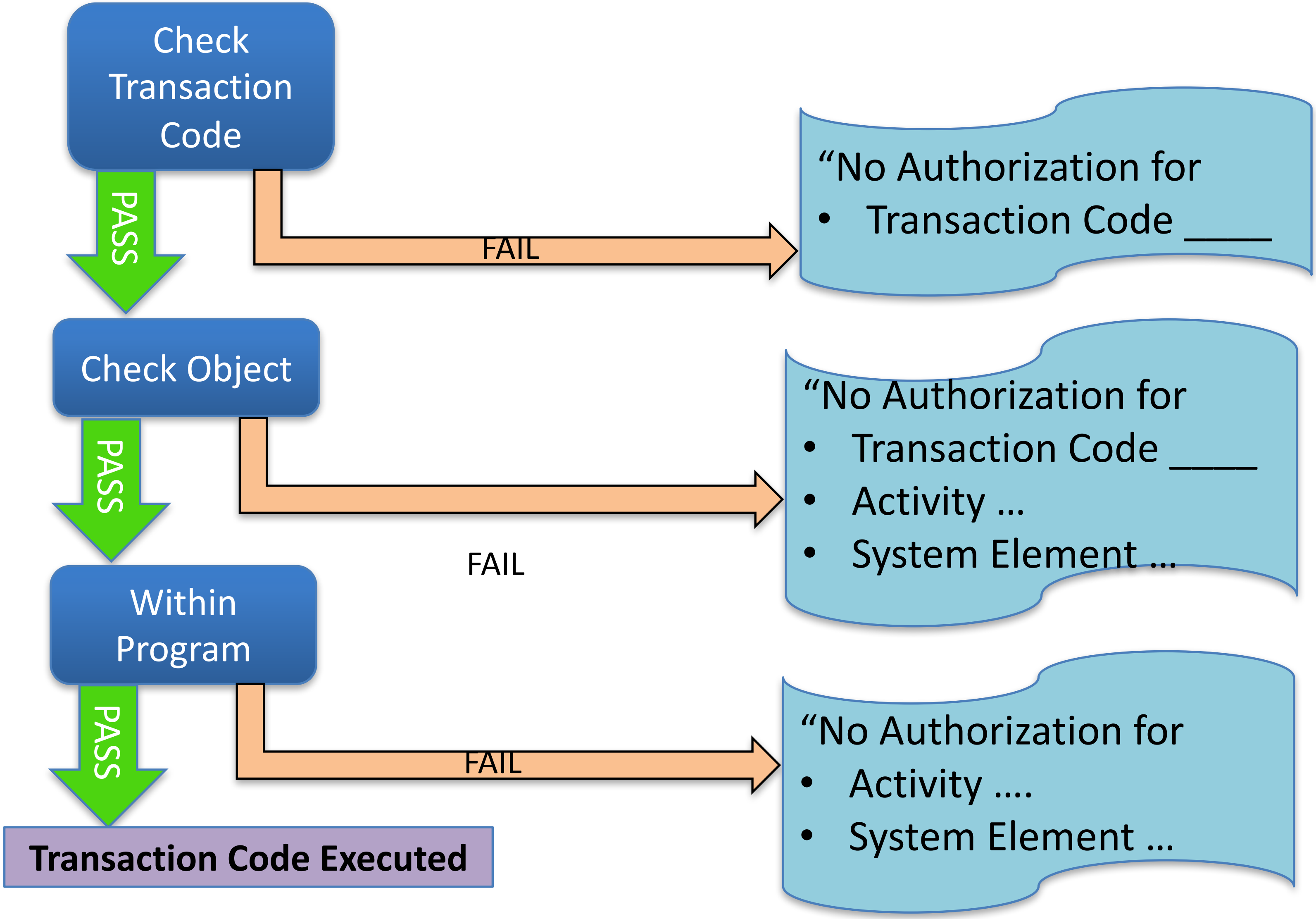
Business View

- □ 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

FAIL

“No Authorization for
- Transaction Code _____

Check Object

PASS

FAIL

“No Authorization for
- Transaction Code _____
- Activity …
- System Element …

Within Program

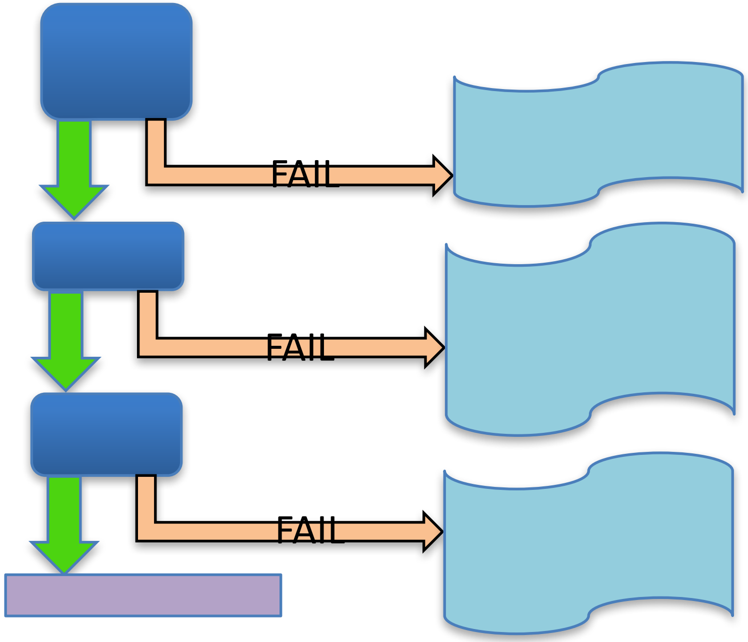
PASS

FAIL

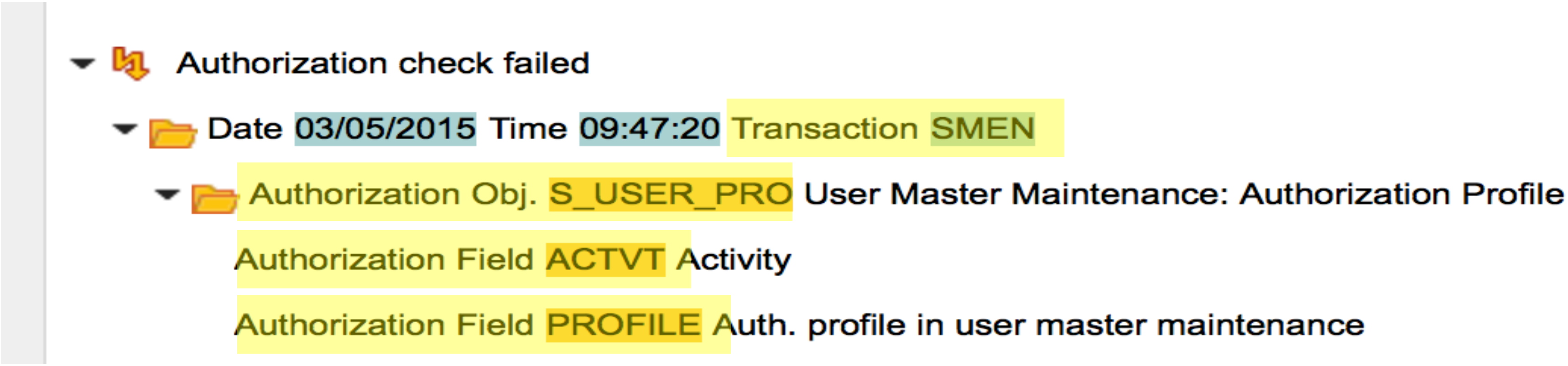
“No Authorization for
- Activity ….
- System Element …

Transaction Code Executed

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



Authorization check failed

Date 03/05/2015 Time 09:47:20 Transaction SMEN

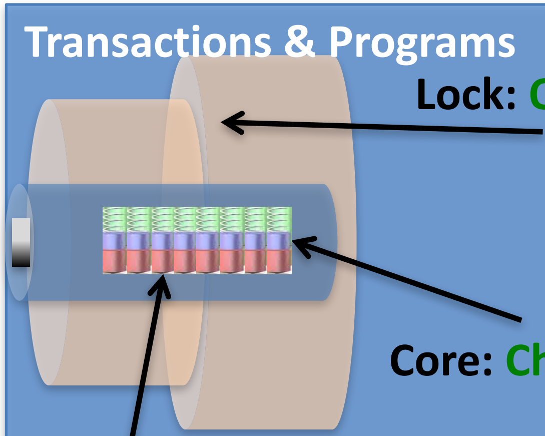
Authorization Obj. S_USER_PRO User Master Maintenance: Authorization Profile

Authorization Field ACTVT Activity

Authorization Field 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

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

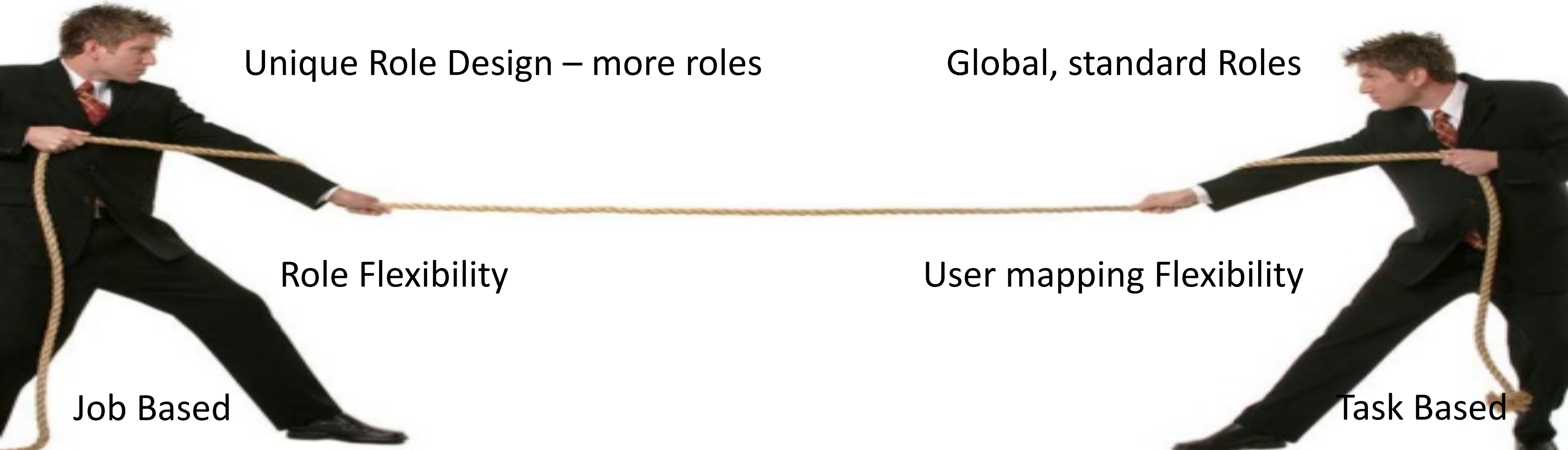
Job Based

Task Based

SAP Security Role Design

Managing the Tension

Role Complexity	User Role Mapping Complexity
Larger Roles	Smaller, more Roles
Maintenance ‘clean-up’	Simpler role maintenance
Risk of SOD in roles	Risk of SOD via multiple roles assigned
Unique Role Design – more roles	Global, standard Roles
Role Flexibility	User mapping Flexibility
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

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

Finance: Overview

- Risks / Controls in Finance
  - Document Parking
  - Manual Transactions
  - Fixed Assets
  - 1-time Business Partners
- Key configuration: Company codes
  - Definition Active vs. not (control tool)
- Financial Master Data
  - Chart of Accounts
  - Tolerances
- Real-time vs. Manual Postings
  - When each is used
  - How each is controlled
- Reconciliation: Control tool

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

Exercise 3: Journal Entries

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:

- ***Document Journal:*** *Information System → General Report Selection → Financial Accounting → General Ledger Reports → Document → General → Compact Document Journal → Compact Document Journal* **(S_ALR_87012289)**

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

- ***Line Item Journal:*** *Information System → General Report Selection → Financial Accounting → General Ledger Reports → Document → General → Line Item Journal → Line Item Journal* **(S_ALR_87012291)**

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