



*Overview of SAP Security  
Training Presented by: Karim Momin  
CISA, CISM, CGEIT, CRISC, CEH  
ISACA Houston 12/2/2011*



# Table of Contents

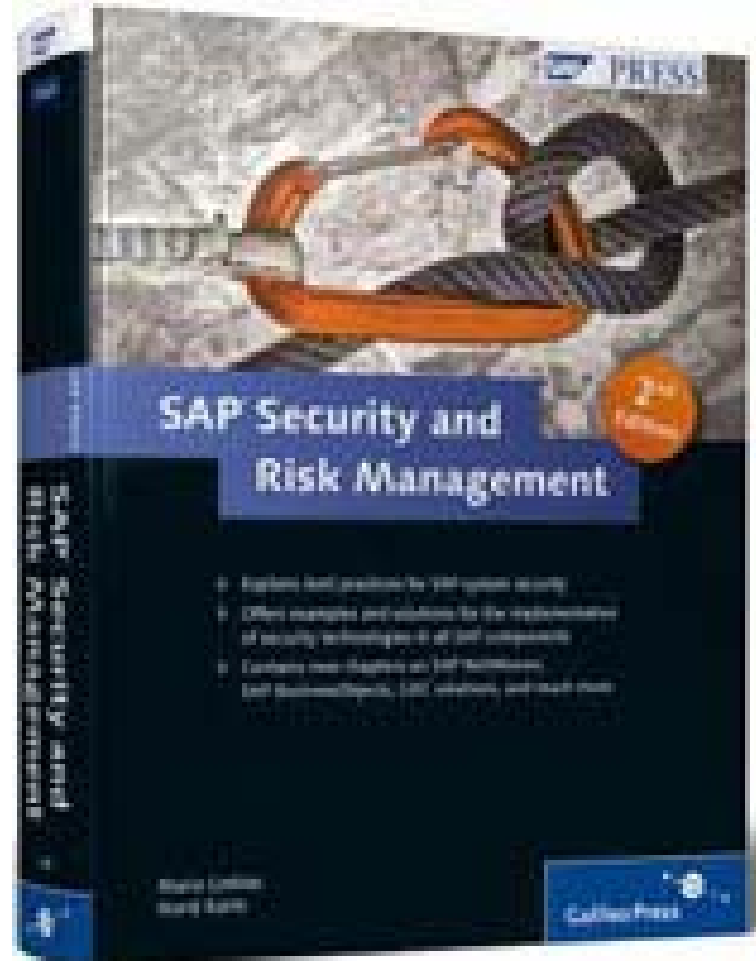
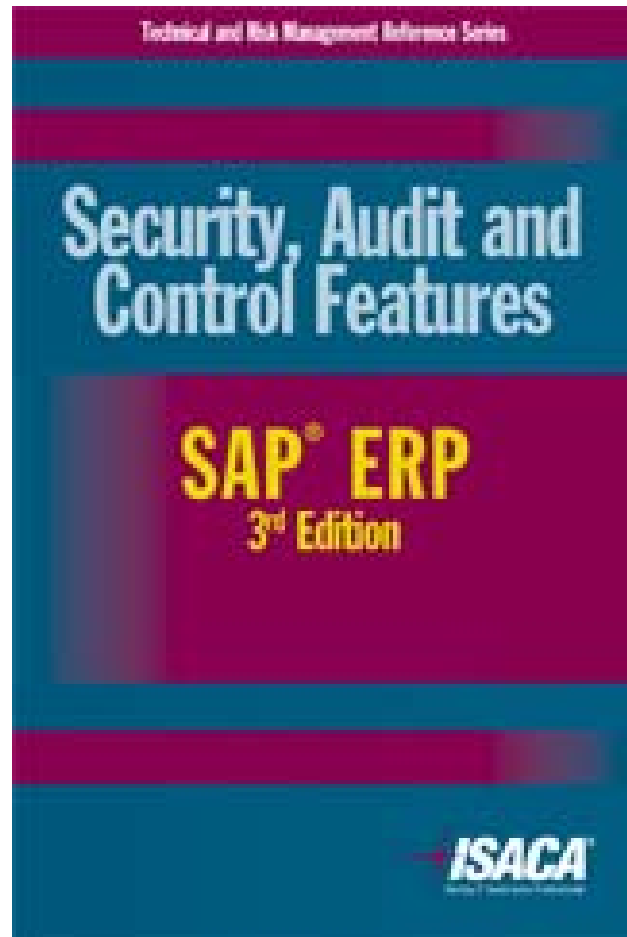
- **Overview of SAP Security Concepts**
- **Profile Generator**
- **Key Reports and Tables**
- **Questions?**



# Overview of SAP Security



# Resource Material from ISACA

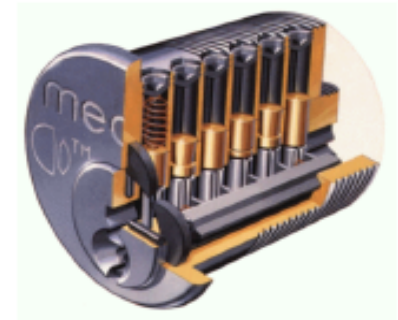
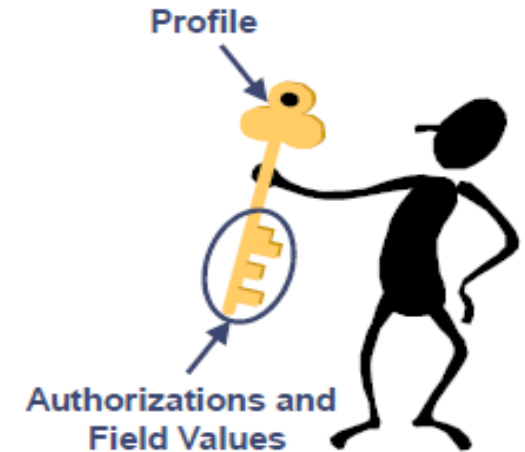




# Overview of SAP Security

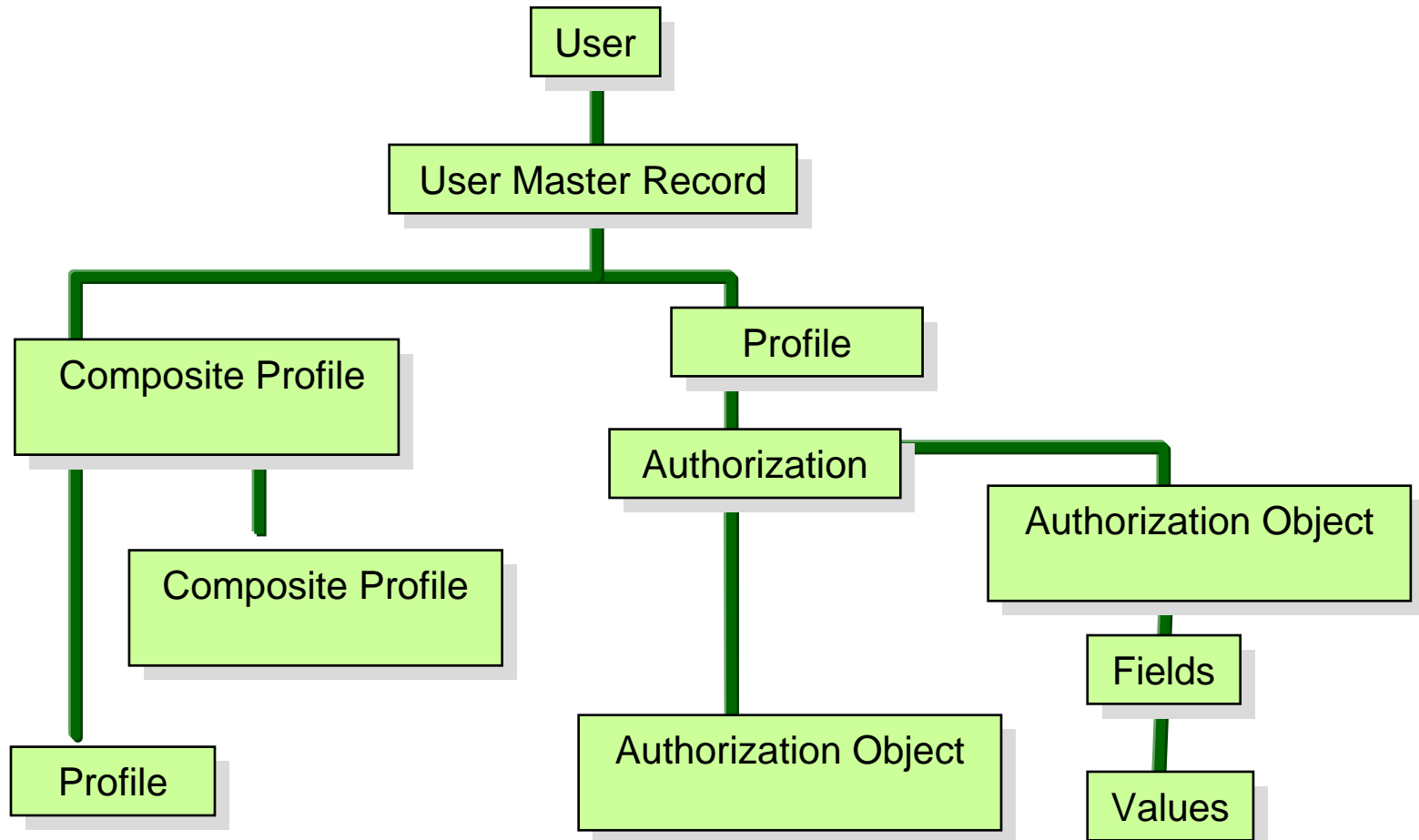
Roles, Profiles and Authority Checks

- A Role is a bucket containing:
  - Transaction Codes
  - Authorization Data (Authorization Objects and Field Values)
  - User assignments
- A Profile is a “key ring” that contains authorizations (cut keys)
- Authority Checks
  - Performed by SAP to ensure that a user ID has the correct authorization object and field value combination (cut key) to execute a particular task
  - There may be multiple authority checks in one program (typically one at the start of the program as well as throughout the program)





# Authorization Concept





# Overview of SAP Security

## Authorization Objects vs. Authorizations

- An authorization object is a template for security that contains fields with blank values (an uncut key)
  - Authorization Object may be reused for many transactions
  - Authorization Objects and Field Values are stored in two key SAP tables
    - > USOBX\_C: Transaction-to-object relationships
    - > USOBT\_C: Transaction-to-object field value relationships
      - » Both tables are maintained via transaction code SU24 and used by PFCG (Profile Generator)
- An authorization is an authorization object with completed fields (a cut key)
  - It takes one or more “keys” to open the doors to access a particular task, or transaction, within SAP



# Overview of SAP Security

Levels required to access a particular function in SAP



**Level 1: User ID Access**  
Login w/ UserID and Password

**Level 2: Transaction Code Access**  
Object: S\_TCODE  
Examples: FB01, MM01

**Level 3: Authorization Access**  
Examples: F\_BKPF\_BUK, M\_MATE\_BUK

User Master Record

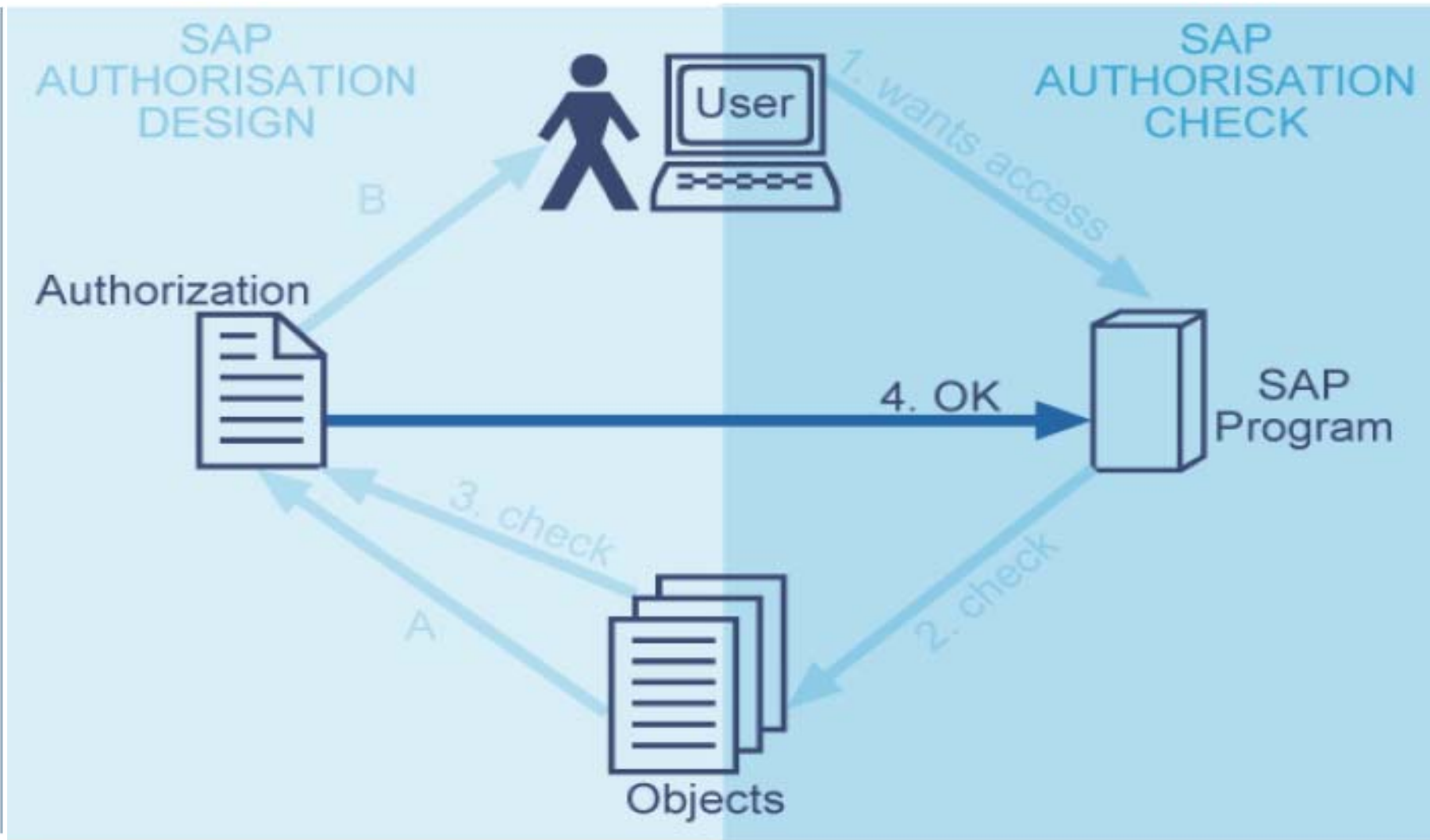
Role/Profile

Authorization Object Field Values



# SAP Security

## Authority Check





# Overview of SAP Security

## Authorization Concepts

Example: Object F\_BKPF\_BUK  
(Accounting Document: Authorization for company code)

In General, objects protect:

- a certain data element / function
- for a specific action
- in a specific context

This object protects:

- accounting document (= posting)
- activity (create, display, etc.)
- for company code (= of a legal entity)



# Overview of SAP Security

## Authorization Concepts

### Example of an SAP Authorization Object

<b>GENERIC BUILDING BLOCKS</b>		<b>EXAMPLE</b>
<b>Object</b>	F_BKPF_BUK	User wants to change a posting for Company Code 0001
<b>Field 1</b>	Activity (ACTVT)	Authorization XYZ
<b>Field 2</b>	Company (BUKRS)	Change (02)  (Company Code 0101)

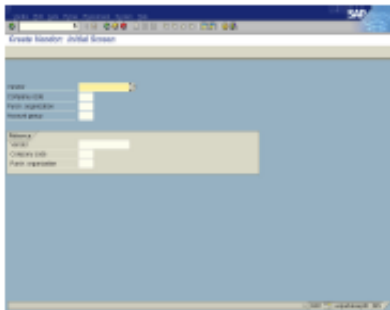


# Overview of SAP Security

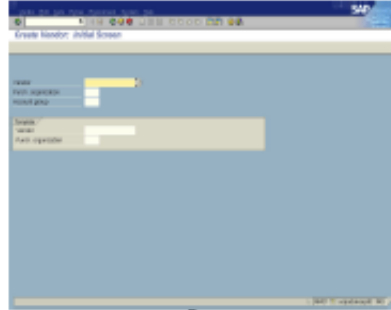
## Authorization Concepts

**Keep in mind!** In SAP, you can perform the same function with different transactions

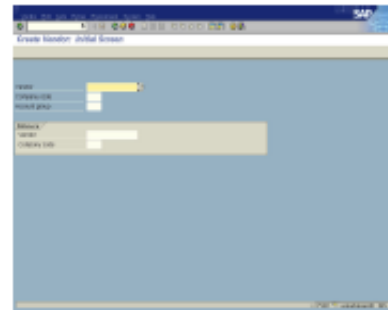
**MK01**



**Transaction  
FK01**



**XK01**



**Conventional  
approach  
protection via  
menu/function**

**Create Vendor**

**SAP approach  
protection once  
via authorization**



# Overview of SAP Security

SU24 – Relationship of authorizations to transaction codes

- USOBX\_C table

- T-code
- Object
- Flag (N = No Check, C = Check, CM = Check Maintain)
  - > Ignore U since it is essentially the same as C

- USOBT\_C table

- T-code
- Object
- Field
- Low
- High

*Maintaining these tables is the key to increasing efficiency, consistency, and integrity of the role design and future design changes by avoiding manual and changed authorizations in the roles.*



# Overview of SAP Security

SU24 – Relationship of authorizations to transaction codes

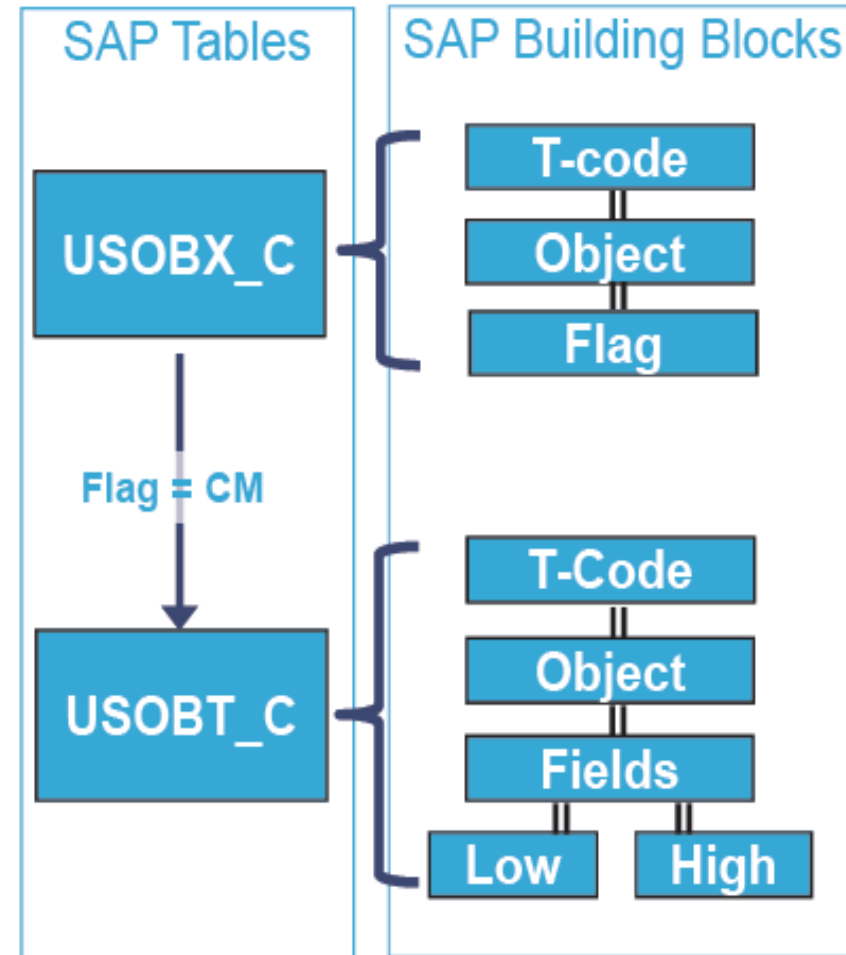
Maintains the USOBX\_C table

- T-code to object relationship and special handling flag

Maintains the USOBT\_C table

- T-code to object to default field value relationship

These tables are client independent. Modifications via transaction code SU24 modifications will affect all clients in an SAP system.



# T-CODE: SU24 (Authorization Objects)

SAP Data

Transaction Code: **FB01** Saved

Authorization Objects

Status	Authorization Object	Object Description	TSTCA	Check Int.
■	F_BKPF_BED	Accounting Document: Account Authorization for Customers		Check
■	F_BKPF_BEK	Accounting Document: Account Authorization for Vendors		Check
■	F_BKPF_BES	Accounting Document: Account Authorization for G/L Accounts		Check
■	F_BKPF_BLA	Accounting Document: Authorization for Document Types		Check
■	F_BKPF_BUK	Accounting Document: Authorization for Company Codes		Check
■	F_BKPF_BUP	Accounting Document: Authorization for Posting Periods		Check
■	F_BKPF_GSB	Accounting Document: Authorization for Business Areas		Check
■	F_BKPF_KOA	Accounting Document: Authorization for Account Types		Check
■	F_BNKA_BUK	Banks: Authorization for Company Codes		Check
■	F_BNKA_MAN	Banks: General Maintenance Authorization		Check
■	F_FAGL_LDR	General Ledger: Authorization for Ledger		Check
■	F_FAGL_SEG	General Ledger: Authorization for Segment		Check
■	F_FICA_CTR	Funds Management Funds Center		Check

Selection Result

Na...	Short Descriptio...
FB01	Post Document

Activity Types which grant the Type of Access

Default Authorization Values (F\_BKPF\_BUK)

Object	Field Name	Display	From	To
F_BKPF_BUK	ACTVT	⌘	01	
	DIKPCS		⌘DIKPCS	



# Available Activity Types

Define Values

Object: F\_BKPF\_BUK Accounting Document: Aut ...

Field name: ACTVT Activity

Activities

S...	Ac...	Text
<input checked="" type="checkbox"/>	01	Create or generate
<input type="checkbox"/>	02	Change
<input type="checkbox"/>	03	Display
<input type="checkbox"/>	06	Delete
<input type="checkbox"/>	07	Activate, generate
<input type="checkbox"/>	08	Display change documents
<input type="checkbox"/>	10	Post
<input type="checkbox"/>	22	Enter, Include, Assign
<input type="checkbox"/>	43	Release
<input type="checkbox"/>	77	Pre-enter
<input type="checkbox"/>	C4	Develop Payment Card

Activity types must be selected to grant access.

There are more activity types than what is listed.



# Overview of SAP Security

SU24 – Relationship of authorizations to transaction codes

## Why are These Tables “Misused” and “Underutilized”?

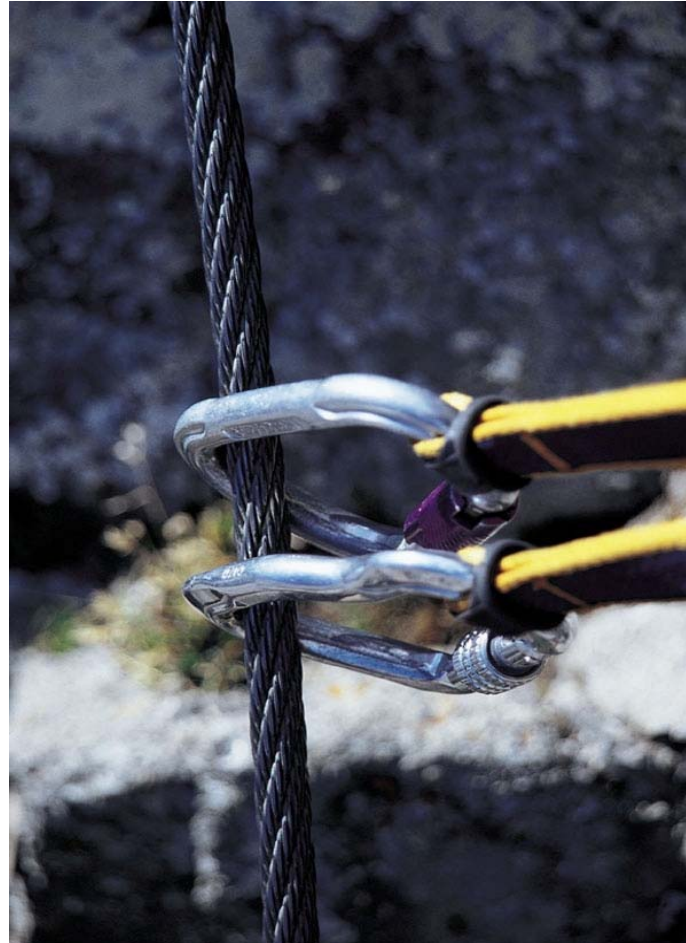
- Many companies do not even use transaction SU24 to maintain their customer tables (USOBX\_C and USOBT\_C)
- Others do some maintenance via transaction SU24, but do not fully understand the relationship between these underlying tables and the Profile Generator (PFCG)
- These tables are a key to reducing the maintenance and risk associated with roles!





# Overview of SAP Security

Profile Generator (PFCG)





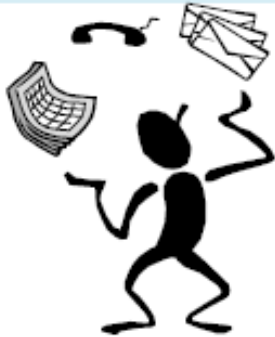
# Overview of SAP Security

Profile Generator (PFCG)

## Traditional Security Approach

Transaction Codes:

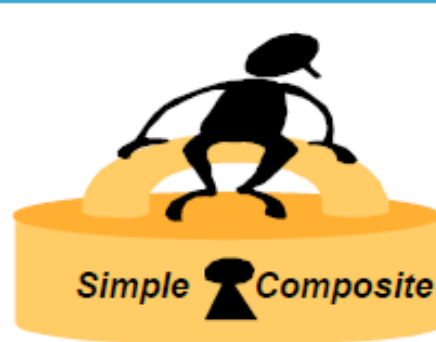
**SU01**



**End User Maintenance**

- Create User
- Change User
- Delete User
- Assign Profiles
- Setup Defaults

**SU02**



**Profile Maintenance**

- Create Profile
- Change Profile
- Delete Profile
- Assign Authorizations

**SU03**



**Authorization Maintenance**

- Create Authorization
- Change Authorization
- Delete Authorization



# Overview of SAP Security

Profile Generator (PFCG)

## Security Administration via Profile Generator

- The profile generator is an automated tool (transaction code PFCG) used to assist in the design, capture and maintenance of profiles
- Simplifies the Authorization process
- Uses transaction codes to define access
- Based on the TRANSACTIONS selected SAP determines the related AUTHORIZATION OBJECTS and, where applicable, the FIELD VALUES from tables USOBX\_C and USOBT\_C
  - The remaining FIELD VALUES for the selected AUTHORIZATION OBJECTS to create the AUTHORIZATIONS need to be filled in
- Role is therefore a collection of Authorizations
- When generated, a Role creates a corresponding Profile



# Overview of SAP Security

## Authorization Concepts

### Security Administration via Profile Generator

PFCG uses the USOBX\_C and USOBT\_C tables to pre-fill the Authorizations tab of a role based on the transaction codes entered on the Menu tab of a role



Based on the tcodes entered on the Menu tab...

PFCG will look up the objects with a Check/Maintain flag and populate the Authorizations tab



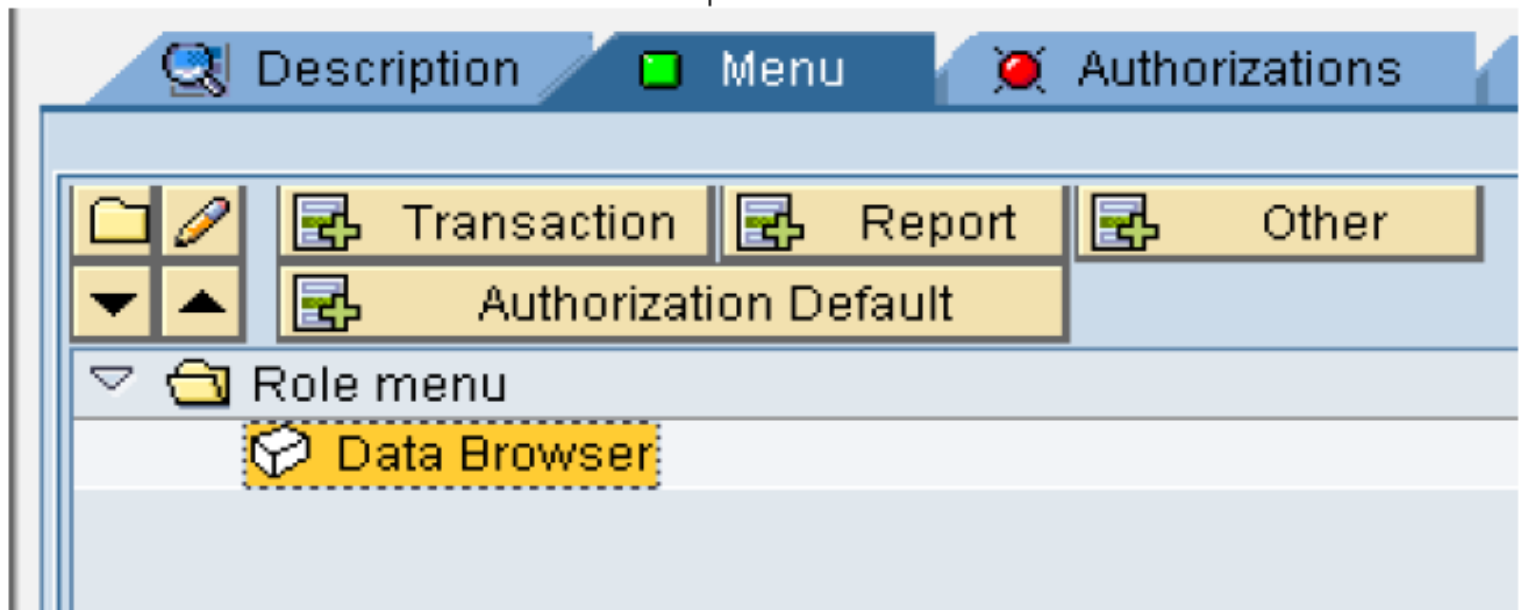
# Overview of SAP Security

Profile Generator (PFCG)

## Security Administration via Profile Generator

### Simple Role Example:

1. Create a simple role and add t-code SE16 “Data Browser” to the Menu tab





# Overview of SAP Security

Profile Generator (PFCG)

Security Administration via Profile Generator

Simple Role Example:

## 2. Assign Authorizations (objects & field values)

The screenshot displays the SAP Profile Generator (PFCG) interface, specifically the 'Authorizations' tab. The interface includes several sections:

- Created by:** Fields for User, Date, and Time (00:00:00).
- Last Changed On/By:** Fields for User, Date, and Time (00:00:00).
- Information About Authorization Profile:** Fields for Profile Name, Profile Text, and Status (No authorization data exists).
- Maintain Authorization Data and Generate Profiles:** A section containing a button labeled 'Change Authorization Data' (highlighted with a red box and arrow) and an 'Expert Mode for Profile Generation' option.



# Overview of SAP Security

## Profile Generator (PFCG)

### Security Administration via Profile Generator

#### Simple Role Example:

#### 2. Assign Authorizations (objects & field values)

Authorization objects which default into the role are defined in table USOBX\_C, these objects have their flag value set to "Check Maintain"

**General Table Display**

Background Number of Entries All Entries

Table: **USOBX\_C** Check Table for Table USOBT\_C

Text table:  No texts

Layout:

Maximum no. of hits: 500  Maintain entries

**Selection Criteria**

Fld name	O	Fr Value	To value	More	Output	Technical name
Name		SE16		→	<input checked="" type="checkbox"/>	NAME
Test status type				→	<input checked="" type="checkbox"/>	TYPE
Object				→	<input checked="" type="checkbox"/>	OBJECT
Changed by				→	<input checked="" type="checkbox"/>	MODIFIER
Modification date				→	<input checked="" type="checkbox"/>	MODDATE
Modification time				→	<input checked="" type="checkbox"/>	MODTIME
Check flag		Y		→	<input checked="" type="checkbox"/>	OKFLAG
Modification ID				→	<input checked="" type="checkbox"/>	MODIFIED
Name				→	<input checked="" type="checkbox"/>	ORNAME

Check fl	Short Descript.
N	No authorization check
X	Authorization check takes place
U	Not maintained
Y	Authorization check takes place; default values in USOBT
	Not maintained



# Overview of SAP Security

Profile Generator (PFCG)

Security Administration via Profile Generator

Simple Role Example:

## 2. Assign Authorizations (objects & field values)

Two authorization objects were found with their flag value set to “Check Maintain”: S\_TABU\_DISP & S\_TABU\_LIN

Table to be searched	USOBX_C	Check Table for Table USOBT_C
Number of hits	2	
Runtime	0	Maximum no. of hits 500

Name	Ty.	Object	Changed by	Date	Time	CheckFl.	Name
SE16	TR	S_TABU_DISP	JWHITEHURST	08/20/2009	11:41:39	Y	
SE16	TR	S_TABU_LIN	JWHITEHURST	08/20/2009	11:41:39	Y	



# Overview of SAP Security

Profile Generator (PFCG)

## Security Administration via Profile Generator

### Simple Role Example:

#### 2. Assign Authorizations (objects & field values)

Default fields & field values for the auth. objects are then defined on USOBT\_C, these are brought into Profile Generator automatically

#### Table (USOBT\_C)

Name	Tv	Object	Field Name	Value	Value
SE16	TR	S_TABU_DIS	ACTVT	03	
SE16	TR	S_TABU_DIS	DICBERCLS		
SE16	TR	S_TABU_LIN	ACTVT	03	
SE16	TR	S_TABU_LIN	ORG_CRIT		
SE16	TR	S_TABU_LIN	ORG_FIELD1		
SE16	TR	S_TABU_LIN	ORG_FIELD2		
SE16	TR	S_TABU_LIN	ORG_FIELD3		
SE16	TR	S_TABU_LIN	ORG_FIELD4		
SE16	TR	S_TABU_LIN	ORG_FIELD5		
SE16	TR	S_TABU_LIN	ORG_FIELD6		
SE16	TR	S_TABU_LIN	ORG_FIELD7		
SE16	TR	S_TABU_LIN	ORG_FIELD8		

#### T-Code (PFCG)

The screenshot shows the SAP PFCG authorization tree. The tree structure is as follows:

- Standard Basis: Administration
  - Standard Table Maintenance (via standard tools such as SM30)
    - Standard Table Maintenance (via standard tools such as SM30)
      - Activity Authorization Group Display
  - Standard Authorization for Organizational Unit
    - Standard Authorization for Organizational Unit
      - Activity Organization criterion for key Display
        - Org. crit. attribute 1
        - Org. crit. attribute 2
        - Org. crit. attribute 3
        - Org. crit. attribute 4
        - Org. crit. attribute 5
        - Org. crit. attribute 6
        - Org. crit. attribute 7
        - Org. crit. attribute 8



# Overview of SAP Security

Profile Generator (PFCG)

Security Administration via Profile Generator

Simple Role Example:

## 3. Generate the profile

**T-Code (PFCG)**

**Change role: Autho**

Assign Profile Name for Generated Authorization Profile

You can change the default profile name here

Profile name: T-ED554741

Text: Profile for role Z:FI:TABLE\_VIEW

Maint.: 0 Unmaint.

- Z:FI:TABLE\_VIEW
  - FI: Sample Role to Vie Tables
    - Standard Cross-application Authorization Objects
      - Standard Transaction Code Check at Transaction Start
    - Maintained Basis: Administration
      - Maintained Table Maintenance (via standard tools such as SM30)
      - Maintained Table Maintenance (via standard tools such as SM30)
        - Activity Display
        - Authorization Group \*
    - Maintained Authorization for Organizational Unit



# Overview of SAP Security

Profile Generator (PFCG)

## Security Administration via Profile Generator

- Simple Role Example:
  1. Create the Role
  2. Assign the Profile
  3. Generate the Profile

The screenshot displays the SAP Profile Generator (PFCG) interface. The main section shows the role details for 'Z:FI:TABLE\_VIEW'. The description is 'FI: Sample Role to Vie Tables'. Below this, there are tabs for 'Description', 'Menu', 'Authorizations', 'User', and 'MiniApps'. The 'Authorizations' tab is currently selected. The interface is divided into two main sections: 'Created by' and 'Last Changed On/By'. Both sections show the user 'STEPHENROSE' and the date '03/25/2010'. The 'Created by' section also shows the time '11:50:12', while the 'Last Changed On/By' section shows '11:50:22'. Below these sections is the 'Information About Authorization Profile' section, which shows the profile name 'T-ED554741', the profile text 'Profile for role Z:FI:TABLE\_VIEW', and the status 'Authorization profile is generated'.

Role	
Role	Z:FI:TABLE_VIEW
Description	FI: Sample Role to Vie Tables

Navigation: Description | Menu | Authorizations | User | MiniApps

Created by	
User	STEPHENROSE
Date	03/25/2010
Time	11:50:12

Last Changed On/By	
User	STEPHENROSE
Date	03/25/2010
Time	11:50:22

Information About Authorization Profile	
Profile Name	T-ED554741
Profile Text	Profile for role Z:FI:TABLE_VIEW
Status	Authorization profile is generated



# Overview of SAP Security

Profile Generator (PFCG)


## Relationship Between SU24 and the Profile Generator

Recommended

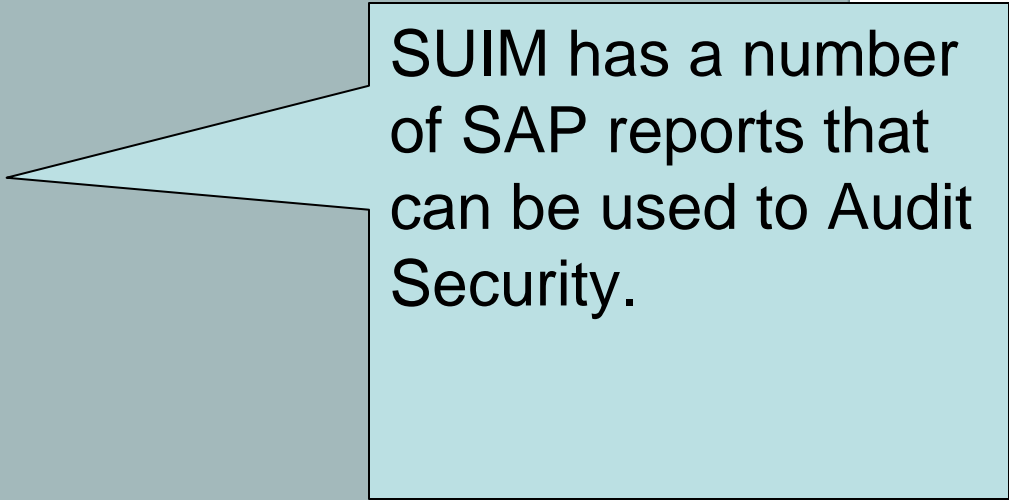
- Object status definitions
- Standard – Auth object was inserted from USOBT\_C, and all fields were filled in by default. (**“Nice, nothing to do”**)
- Maintained – Auth object was inserted from USOBT\_C, and the administrator filled in the “blank” fields, without changing the default values from USOBT\_C. (**“Working with the table”**)

Not Recommended

- Changed – Auth object was inserted from USOBT\_C, and the administrator changed a default field value from the recommended value in USOBT\_C. (**“Fighting with the table”**)
- Manual – Auth object was manually inserted into the role, and was not brought in by USOBT\_C. This object is not “related” to any tcode on the Menu tab and will not be removed when the Menu tab changes. (**“Ignoring the table”**)



# TCode: SUIM (User Information System)



SUIM has a number of SAP reports that can be used to Audit Security.



# T-Codes – User Access & SoD

Transaction Code	Description
SU03	Display Users
S_BCE_68001409	Profiles by Complex Selection Criteria
S_BCE_68001417	Authorizations by Complex Selection Criteria
S_BCE_68001429	Executable Transactions (All Selection Options)
PFCG	Profile Generator
<b>Programs executed using SA38</b>	
<b>RSUSR002</b>	<b>List of Users according to Complex Selection Criteria</b>
RSUSR008_009_NEW	Transaction Combinations Critical to Security (User Populated)
RSUSR100N	Change Documents for Users
RSUSR000	Listing of All Users Logged On



# Tables – User Access & SoD

Tables	Description
USR02	User Details
UST04	User Name to Profiles
UST10C	Composite Profile
UST10S	Simple Profile
UST12	Authorization Value
AGR_1251	Authorization data for the activity group
AGR_USERS	Assignment of roles to users



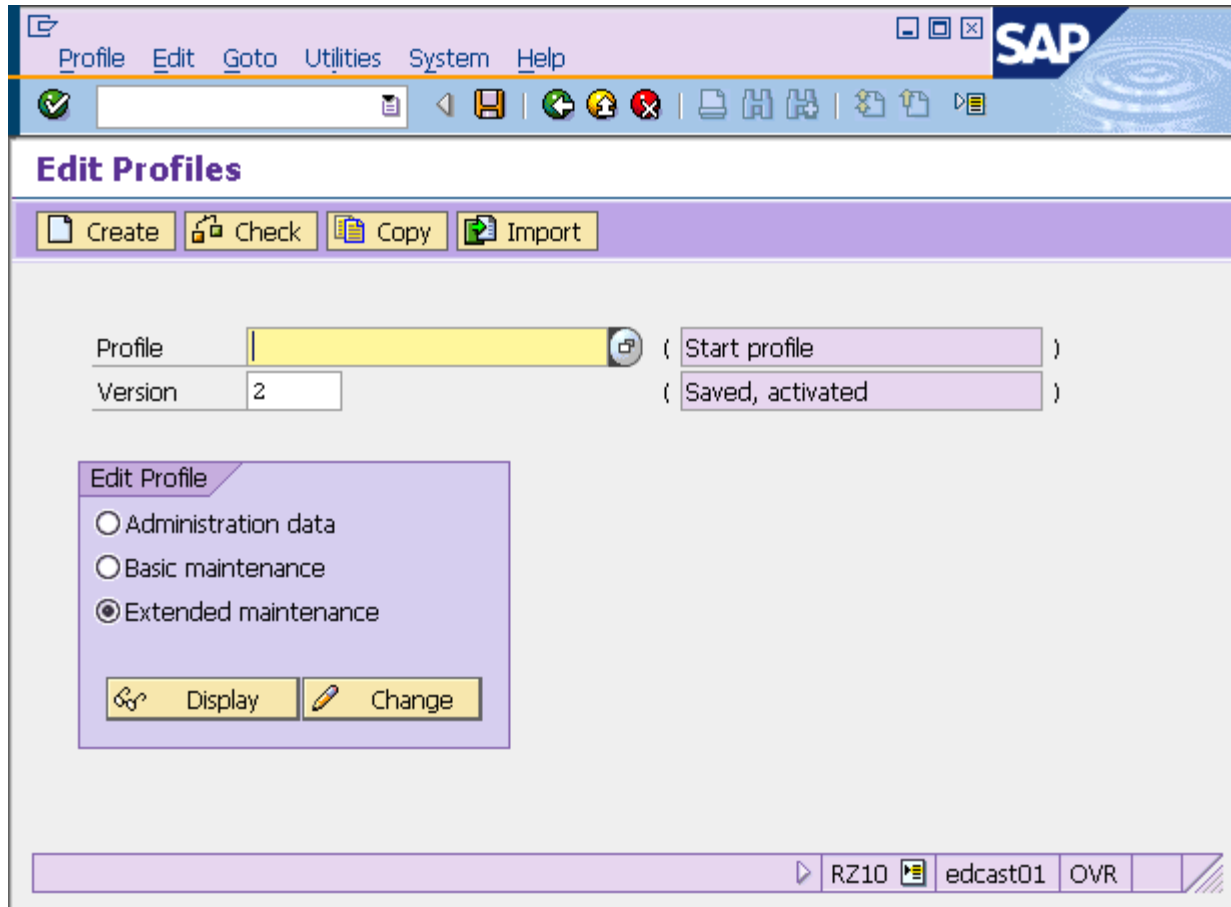
# T-Codes – Audit

Transaction Code	Description
SE16	Data Browser
SQVI	Quick Viewer (Dynamic Queries)
SQ01	SAP Query
SA38	Execute ABAP Programs
SE03	Transport Organizer Tools
ST01	System Trace
SM21	System Log
SLIN	ABAP Syntax Check
SM20	Security Log Audit
SM04	User Overview
AL08	Global Users



# Security Parameters Setting

System Parameters are set using T-Code **RZ10**. Select the appropriate Profile and Extended Maintenance



The screenshot shows the SAP RZ10 'Edit Profiles' interface. At the top, there is a menu bar with 'Profile', 'Edit', 'Goto', 'Utilities', 'System', and 'Help'. Below the menu is a toolbar with various icons. The main area is titled 'Edit Profiles' and contains a toolbar with 'Create', 'Check', 'Copy', and 'Import' buttons. The 'Profile' field is highlighted in yellow and contains the text 'Start profile'. The 'Version' field contains the number '2'. To the right of these fields are two status indicators: '( Start profile )' and '( Saved, activated )'. Below this is a section titled 'Edit Profile' with three radio buttons: 'Administration data', 'Basic maintenance', and 'Extended maintenance'. The 'Extended maintenance' radio button is selected. At the bottom of this section are 'Display' and 'Change' buttons. The status bar at the bottom right shows 'RZ10', 'edcast01', and 'OVR'.



# Security Parameters Setting

Auditor should run report RSPARAM via T-Code SA38.

## Display Profile Parameter



## Display Profile Parameter



Profile parameters valid in the current system: Substituted form  
Param. Name

Parameter name	User-defined value	System default value
DIR_ATRA		D:\usr\sap\TST\D01\data
DIR_AUDIT		D:\usr\sap\TST\D01\log
DIR_BINARY	D:\usr\sap\TST\D01\exe	\\edcast01\sapmnt\TST\SYS\exe\run
DIR_CCMS		D:\usr\sap\CCMS
DIR_CT_LOGGING	\\edcmst01\sapmnt\TST\SYS\global	\\edcast01\sapmnt\TST\SYS\global
DIR_CT_RUN	\\edcmst01\sapmnt\TST\SYS\exe\run	\\edcast01\sapmnt\TST\SYS\exe\UC\NTAMD64
DIR_DATA		D:\usr\sap\TST\D01\data
DIR_DBMS	\\edcmst01\sapmnt\TST\SYS\SAPDB	\\edcast01\sapmnt\TST\SYS\SAPDB
DIR_EPS_ROOT		\\edcmsd01\sapmnt\trans\EPS
DIR_EXECUTABLE	D:\usr\sap\TST\D01\exe	\\edcast01\sapmnt\TST\SYS\exe\run
DIR_EXE_ROOT	\\edcmst01\sapmnt\TST\SYS\exe	\\edcast01\sapmnt\TST\SYS\exe
DIR_EXTRACT		D:\usr\sap\TST\D01\data
DIR_GEN	\\edcmst01\sapmnt\TST\SYS\gen\dbg	\\edcast01\sapmnt\TST\SYS\gen\dbg
DIR_GEN_ROOT	\\edcmst01\sapmnt\TST\SYS\gen	\\edcast01\sapmnt\TST\SYS\gen
DIR_GLOBAL	\\edcmst01\sapmnt\TST\SYS\global	\\edcast01\sapmnt\TST\SYS\global
DIR_GRAPH_EXE	D:\usr\sap\TST\D01\exe	\\edcast01\sapmnt\TST\SYS\exe\run
DIR_GRAPH_LIB	D:\usr\sap\TST\D01\exe	\\edcast01\sapmnt\TST\SYS\exe\run
DIR_HOME		D:\usr\sap\TST\D01\work
DIR_INSTALL	\\edcmst01\sapmnt\TST\SYS	\\edcast01\sapmnt\TST\SYS
DIR_INSTANCE		D:\usr\sap\TST\D01
DIR_LIBRARY	D:\usr\sap\TST\D01\exe	\\edcast01\sapmnt\TST\SYS\exe\run
DIR_LOGGING		D:\usr\sap\TST\D01\log
DIR_MEMORY_INSPECTOR		D:\usr\sap\TST\D01\data
DIR_ORADEBS		RDBMS71
DIR_ORAHOME		unknown
DIR_PAGING		D:\usr\sap\TST\D01\data
DIR_PERF		D:\usr\sap\PRFCLOG
DIR_PROFILE	\\edcmst01\sapmnt\TST\SYS\profile	\\edcast01\sapmnt\TST\SYS\profile



# Security Parameters Setting

System Parameters(Descriptions)	Default Values	Suggested Values	Permitted Values
<b>Login/password_expiration_time</b> (The number of days after which a password must be changed. The default value 0 sets the password to never expire)	0-30	Days	0-999
<b>Login/min_password_lng</b> (Minimum password length)	3	8	3-8
<b>Login/fails_to_session_end</b> (The number of times a user can enter an incorrect password before the system terminates the logon)	3	3	1-99
<b>Login/fails_to_user_lock</b> (The number of times per day a user can enter an incorrect password before the system locks the user master records against further logon attempts)	12	5	1-99



# Security Parameters Setting

continued

System Parameters(Descriptions)	Default Values	Suggested Values	Permitted Values
<b>Login/failed_user_auto_unlock</b> (Used to specify whether a user who has been locked as a result of invalid password attempts must have the login reset manually [value 0] or automatically at midnight.)	1	0	0 or 1
<b>Auth/check_value_write_on</b> (Enables the transaction [SU53] for authorization analysis when this parameter is set to a value greater than 0.)	Blank	>0	0-
<b>Auth/no_check_in_some_cases</b> (Must be set to Y to allow authorization checks [apart from the check at the start of the transaction] to be deactivated for certain transactions usings T-Code SU24.)	N	Y	Y or N



# Security Parameters Setting

continued

System Parameters(Descriptions)	Default Values	Suggested Values	Permitted Values
<b>Auth/no_check_on_TCODE</b> (Since release 3.0E, the system checks for transaction code access [the S_TCODE authorization object]. Where available, setting this parameter to Y allows the authorization check for transaction code to be switched off.)	N	N	Y or N
<b>Auth/No_check_on_TCODE</b> (This parameter determines whether object S_RFC is checked during Remote Function Calls: Value=0; No check against S_RFC Value=1, Check active but no check for SRFC-FUGR Value=2; Check active and check against SRFC-FUGR	1	2	0-2



# Security Parameters Setting

continued

System Parameters(Descriptions)	Default Values	Suggested Values	Permitted Values
<b>Auth/system_access_check_off</b> (This parameter switches off the automatic AUTHORIZATION Check for particular ABAP/4 language elements [file operations, CPIC calls and calls to kernel functions]. This parameter may be used to ensure downward compatibility of the R/3 kernel [value=0, check remains active].)	0	0	0 or 1
<b>Rdisp/gui_auto_logout</b> (Specifies the number of seconds a user session can be idle before the user is automatically logged off. The parameter is deactivated when set to a value of 0.)	0	>900<2700	0-



**Questions ?**



# Contact Information

Karim Momin, CISA, CISM, CGEIT, CEH

[Kmomin@HornSolutions.Net](mailto:Kmomin@HornSolutions.Net)

832-545-8431 (Cell)



Karim.Momin

Linked .

[www.hornsolutions.net](http://www.hornsolutions.net)