

Auditing SAP IT General Controls (ITGCs)

Steve Biskie, Principal, SAP Risk & Automation Leader,
RSM US LLP

SAPinsider
Las Vegas

2023

SAPinsider

Steve Biskie

RSM's national practice leader for SAP risk services

25+ years working with SAP controls, data & security

Author of *Auditing SAP S/4HANA & Surviving an SAP Audit*

Expert reviewer for *Security, Audit, and Control Features: SAP ERP (3rd & 4th Editions)*

Teach intermediate & advanced SAP audit & security courses

Based in Denver, CO





In This Session

Learn how to properly assess Segregation of Duties (SoD) and Critical Access risks, while avoiding the "transaction code trap"

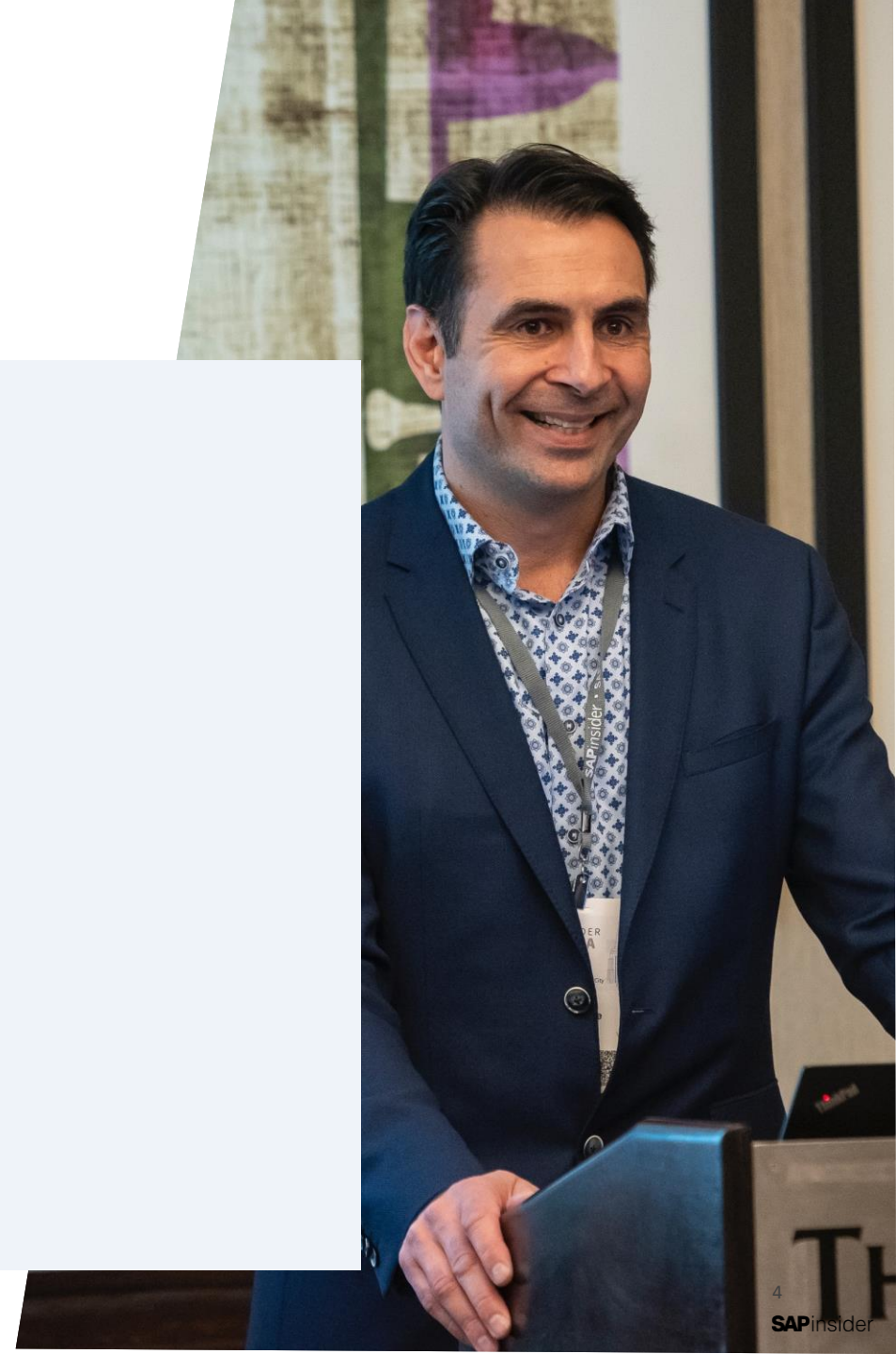
Understand the controls most important in the change control and transport process, including the type of documentation typically expected

Review the logs and log monitoring procedures that are enough to "get you by," and contrast those with the ones that should be in place regardless of any regulatory requirements

Explore how key tables and files related to ITGCs can be used to facilitate continuous monitoring in tools like Process Control

What We'll Cover

- A few basics
- SAP security
- Development and change control
- SAP logging
- New Considerations with SAP S/4HANA
- Continuous monitoring of ITGCs
- Wrap-Up



A Few Basics



Browsing the vendor master file

Key display transactions

In SAP S/4HANA, transaction BP

- Display in BP role:
 - “Business Partner (Gen.)” for general data
 - “Supplier (Fin. Accounting) for company code specific data

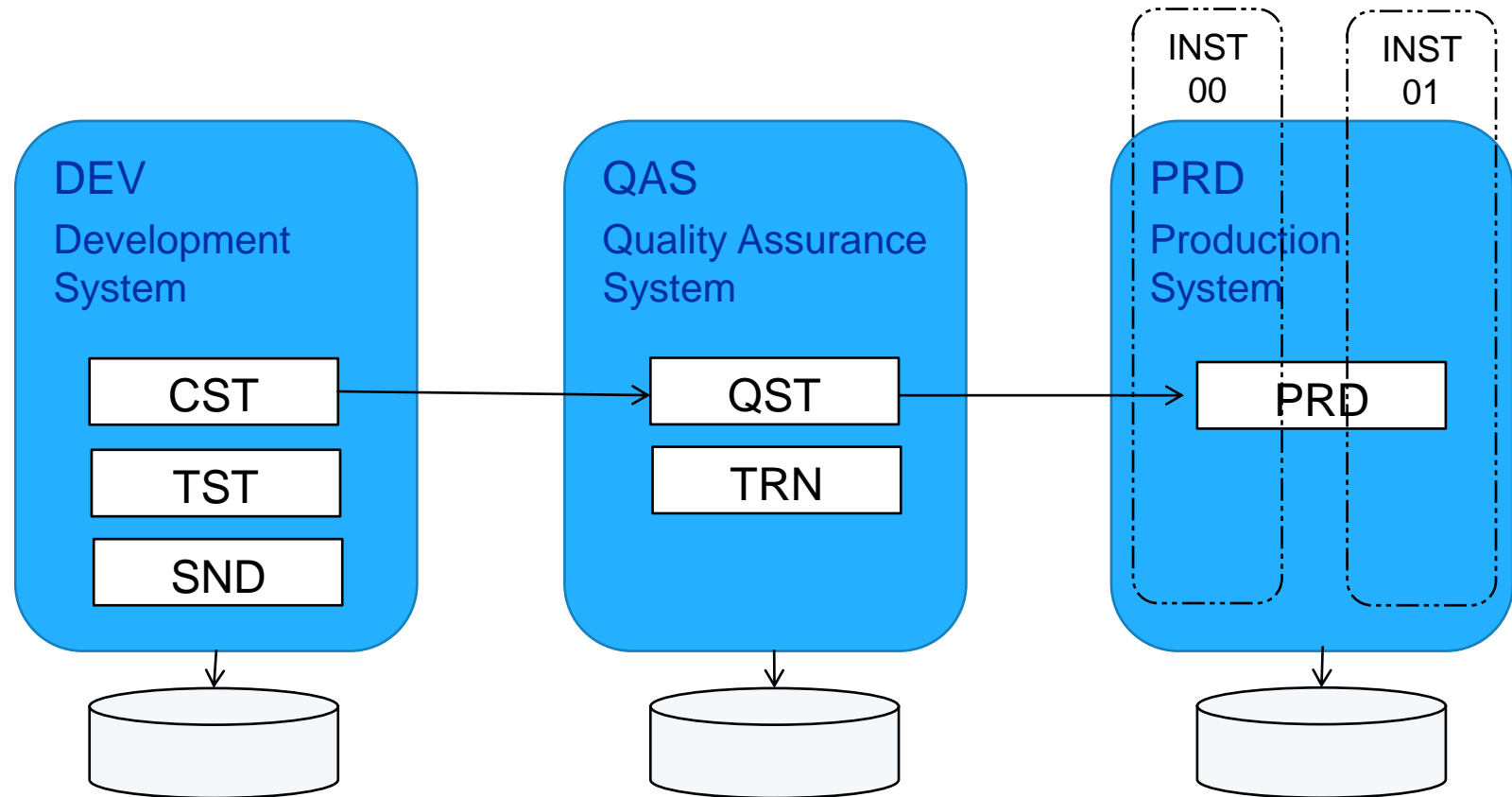
In ECC

- FK03 (Central + Company-Code)
- MK03 (Central + Purchasing Organization)
- XK03 (All)

Terminology

Details on the next slides:

- System
- Instance
- Client
- Transport Path



Terminology, Continued...

SAP System

- A discrete installation SAP software
 - Defined set of functionality, configured as a unit
 - Identified by a 3-character System ID (SID)
- Architecture...
 - Database (physical or logical)
 - 1+ application server instances (ABAP / JAVA)
 - Central Services (e.g., messaging, enqueue)

Common SAP System Types

S/4HANA (SAP Business Suite re-written to optimize on the HANA DB)

ECC (ERP Central Component)

EWM (Extended Warehouse Management)

BW (Business Warehouse)

GRC (Governance, Risk, & Compliance)

Solution Manager (centrally manage configuration)

Portal Systems (JAVA-based)

CRM, SCM, SRM, PLM

Terminology, Continued...

Application Server Instance (aka Instance)

- Administrative unit of an SAP system providing the actual data processing and corresponding services
 - group of resources (memory, work processes, etc. usually in support of a single application or DB)
- Often used interchangeably with "application server" or "server", although not technically the same
- Started, stopped, and monitored as a single unit
- multiple instances for load balancing
- Identified by a host name and a two-digit instance number

Terminology, Continued...

Client

- Means to logically separate complete SAP functionality within a single SAP system
 - e.g. QA, sandbox, training on same SAP system
- Represented by a 3-digit code, unique within the SAP system
- Entire group or corporation typically runs in a single client
- Logically separates configuration and other data
 - Client field (MANDT) in most tables
- Limited number of client-independent tables
 - Unknown to most users (no entry of client after initial login)

Terminology, Continued...

Transport

- SAP term used for the process of moving configuration and program changes from one Client to another (within or across SAP Systems)
- Individual change requests aggregated into a Transport Request in DEV
 - before being moved to a QA and production
- Transport Path defined during initial SAP setup
 - governs the rules for how changes can move between clients

More on this later

Terminology, Continued...

Transaction Code

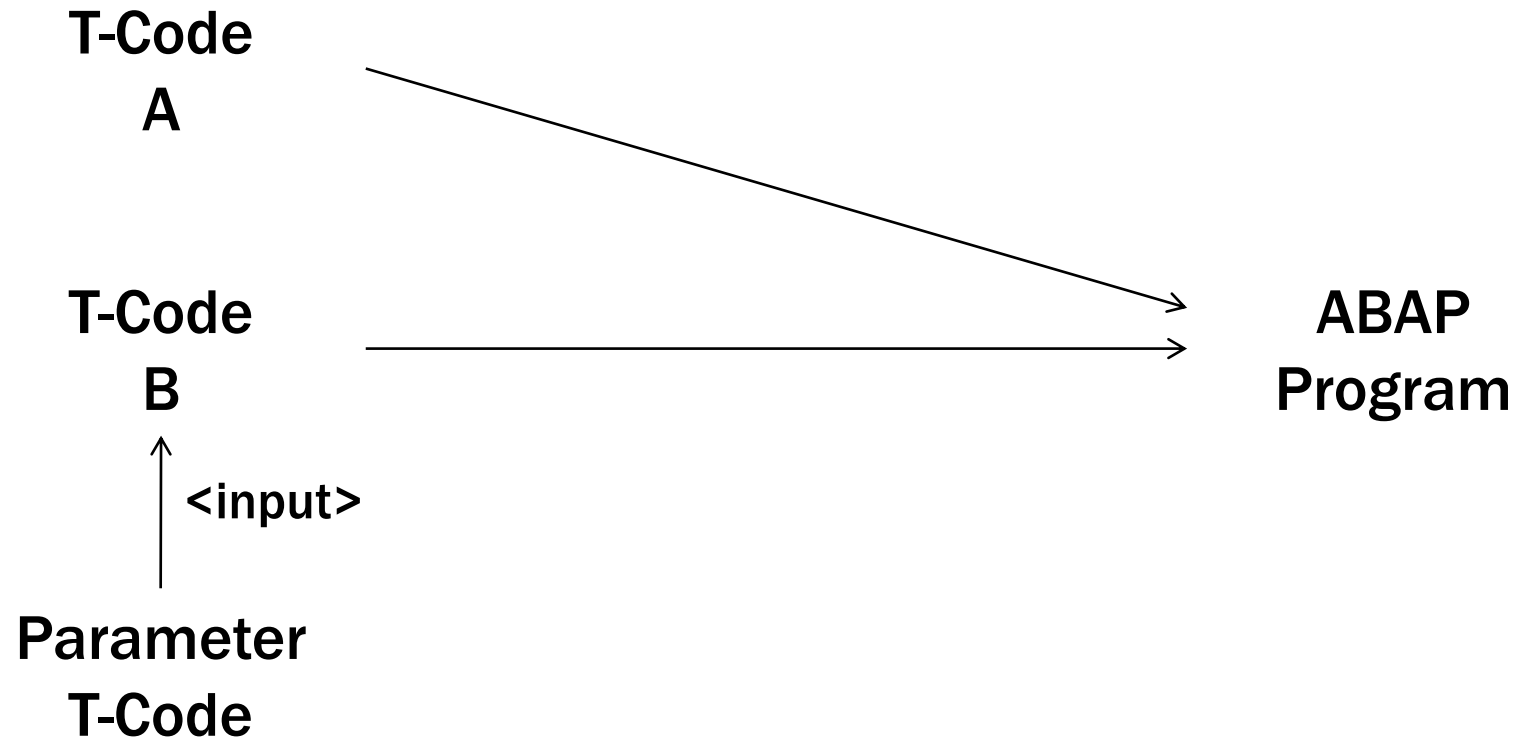
- Also known as a “T-Code”, or simply a “Transaction”
- Calls an SAP program
- First letter often represents the relevant SAP module
- Special Type called a Parameter Transaction:
 - Calls standard transaction with pre-defined values
 - Can skip first screen—means to enhance control

Terminology, Continued...

Program

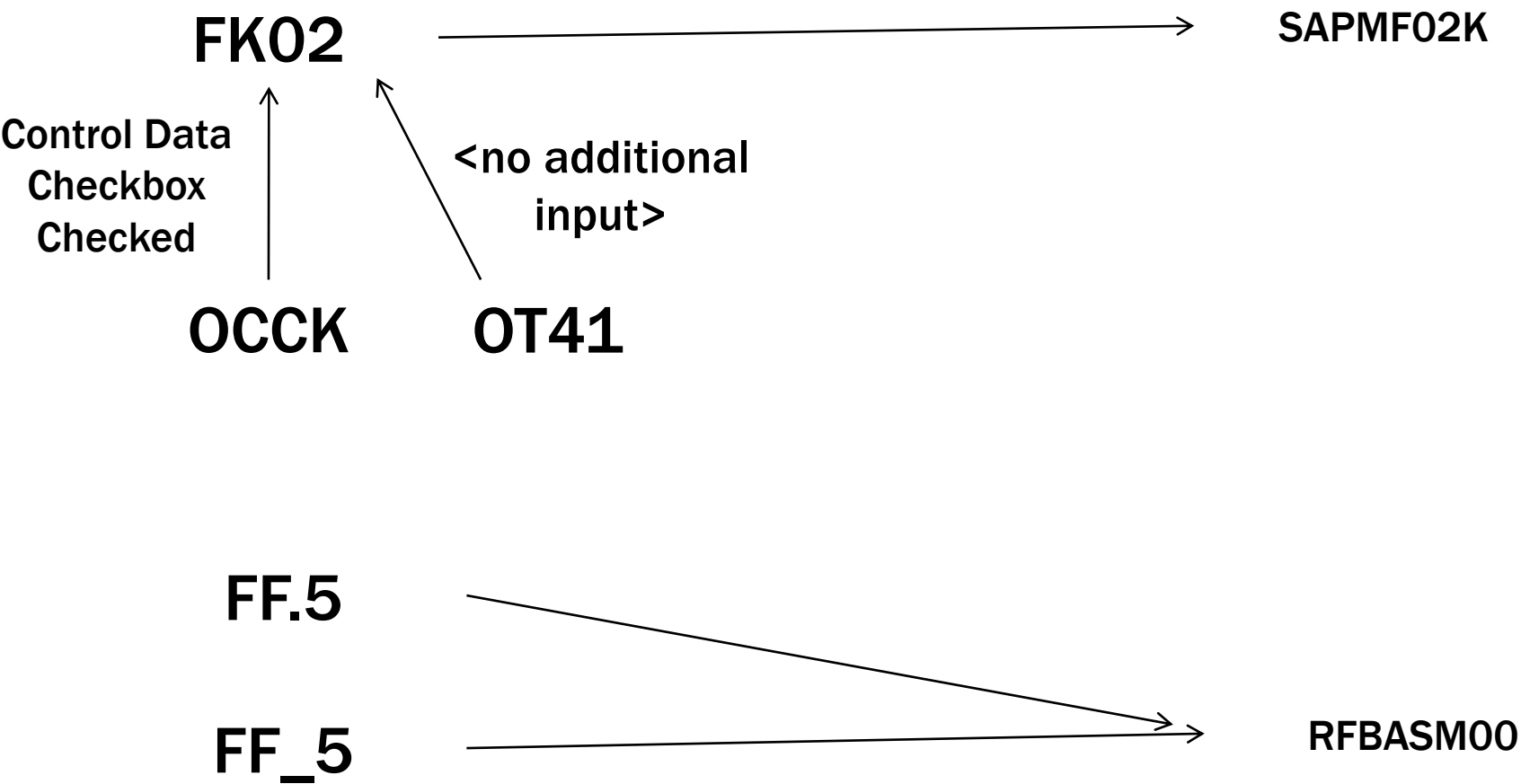
- Set of instructions written in ABAP/4
- Typically called by a T-Code, but can be executed directly by certain functions
- *Report* program typically has 3 stages
 - Data entry
 - Processing
 - Output

T-Codes vs. Programs



A T-Code is similar to a Microsoft Windows shortcut. It merely calls a program. Programs may be called by multiple T-Codes

T-Codes vs. Programs, actual examples



Special Transactions – Audit Usage

Viewing Table Data

SE16N (preferred)

- Some admins may raise security concerns; these are unfounded if audit access set up correctly

SE16H (HANA-specific)

- Allows table joins (2 tables)
- Allows summarizing data (e.g., total by doc type)

SE16, SE17 (outdated and much less efficient)

Regardless of transaction used, browsing tables can expose sensitive data

Consider what is required, restrict appropriately

General Table Display

Table: Sales Document: Header Data

Text table:

Layout:

Maximum no. of hits:

Get Field:

☐ No texts

☐ Maintain entries

Selection Criteria

Fld name	O...	Fr.Value	To value	More	Output	Technical name
Client						MANDT
Sales Document					<input checked="" type="checkbox"/>	VBELN
Created on					<input checked="" type="checkbox"/>	ERDAT
Time					<input checked="" type="checkbox"/>	ERZET
Created by					<input checked="" type="checkbox"/>	ERNAM

Special Transactions – Audit Usage, continued...

Reviewing Configuration

SPRO (highly useful, if not required)

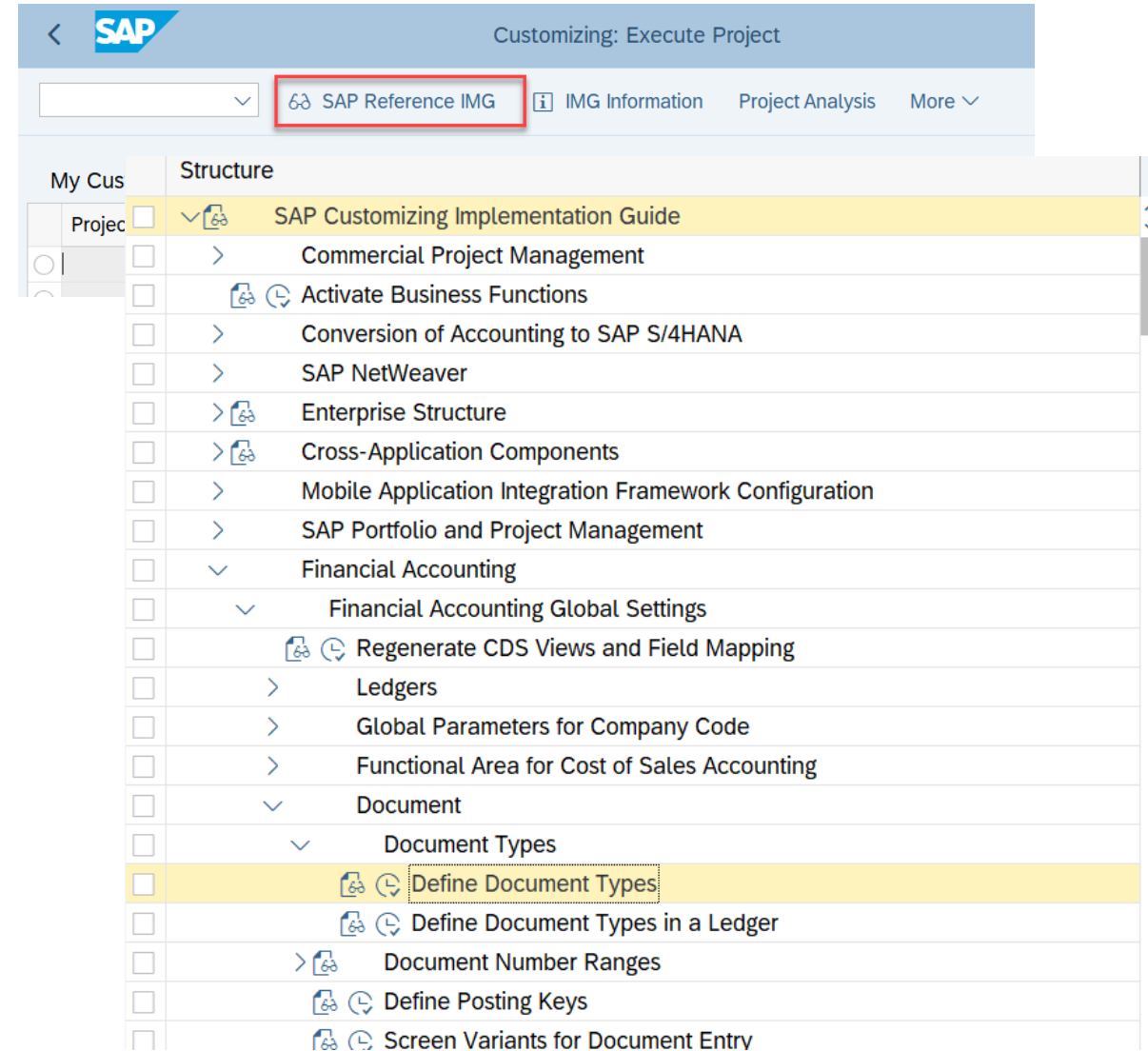
- Time-consuming to initially grant display access
- Many configuration settings can be viewed directly in tables via SE16N / SE16H

SPRO at times is easier to interpret than table data for certain configurations

- Field status groups
- Data validation rules
- Workflow

Use “Find” to quickly jump to a section if you know words in the title

- Tolerance
- Default
- Assign
- Set
- Check



Special Transactions – Audit Usage

AL01 – The Relationship Browser

From a given document, show all related SAP documents

Note the multiple sets of material documents for the given purchase order

Often not provisioned in audit roles (due to lack of knowledge about this transaction)

Relationship Tree	Descriptn
✓ Accounting document	1710 50000000000 2022
✓ Material Document	5000000000 2022
Inbound delivery	0180000000
✓ Purchase Order	4500000000
Quality notification	Packaging Damaged
Quality notification	Broken Packaging
Purchase requisition	3000000000
✓ Material Document	5000000041 2022
Accounting document	1710 50000000005 2022
Controlling Document	A000 A00000F700
✓ Material Document	5000000042 2022
Accounting document	1710 50000000006 2022
Controlling Document	A000 A00000F800
> Material Document	5000000043 2022
> Material Document	5000000044 2022
> Material Document	5000000045 2022
> Material Document	5000000046 2022
✓ Incoming Invoice	5105600125 2022
Workflow	Invoice: Release Blocked Invoices
Accounting document	1710 51000000027 2022
Controlling Document	A000 A000000100

Special Transactions – Audit Usage

The (FREE) Audit Information System

If granted access, AIS will appear in the user menu

Accessed by the SAP_AUDITOR role, or a variation

- Standard role requires cleanup, as it does grant some create/maintain privileges (not just display)

Standard in SAP S/4HANA, as well as SAP ECC and SAP R/3

✓	📁	User Menu for Steve Biskie
✓	📁	AIS - Audit Information System
	>	📁 AIS - Administration
	>	📁 System Audit
✓	📁	Business Audit - Individual Financial Statements
	>	📁 AIS - Organizational Overview
	>	📁 Financial Statements - General
✓	📁	Balance Sheet - Assets
	>	📁 AIS - Tangible Assets
	>	📁 AIS - Real Estate
✓	📁	AIS - Material Inventories
	✓	📁 Consistency Checks
		🔗 MB5L - List of Stock Values: Balances
		🔗 MB5K - Stock Consistency Check
		🔗 S_P6B_12000135 - List of Goods Receipt/Invoice Receipt Balances
		🔗 S_P6B_12000136 - MM/FI Balance Comparison
	>	📁 Material Master Data
	>	📁 Material Stocks
	>	📁 Physical Inventory
	>	📁 Balance Sheet Valuation
	>	📁 Ranking Lists/Key Figures
	>	📁 Price Calc.
	>	📁 Goods Movements and Documents

SAP security



Default User IDs

















Every SAP client has a well-known set of default user IDs

Default SAP clients depend on whether you are running SAP ECC or S/4HANA

Three Default Clients (SAP ECC)	
000	SAP R/3 base image. Used for release changes, updates, and special customizing tasks.
001*	A copy of client 000
066**	EarlyWatch. Used for technical monitoring by SAP AG.

- ***001 goes away with S/4HANA**
- ****066 no longer needed per recent SAP Notes**

RSUSR003: Auditing default user IDs

Client	User	Lock	Password Status	Reason for User Lock	Failed	Valid from	Valid to	Policy	Info
000	DDIC		Exists; Password not trivial.		1				
	SAP*		Exists; Password not trivial.	Locked by unsuccessful logons					
	SAPCPIC		Does not exist.						
	TMSADM		Exists; Password not trivial.						
010	DDIC		Exists; Password not trivial.						
	SAP*		Exists; Password not trivial.	Locked by unsuccessful logons					
	SAPCPIC		Does not exist.						
	TMSADM		Exists; Password not trivial.						
100	DDIC		Exists; Password not trivial.		2				
	SAP*		Exists; Password not trivial.	Locked by unsuccessful logons					
	SAPCPIC		Does not exist.						
	TMSADM		Exists; Password not trivial.						
110	DDIC		Exists; Password not trivial.						
	SAP*		Exists; Password not trivial.						
	SAPCPIC		Does not exist.						
	TMSADM		Exists; Password not trivial.						
120	DDIC		Exists; Password not trivial.						
	SAP*		Exists; Password not trivial.	Locked by administrator					
	SAPCPIC		Does not exist.						
	TMSADM		Exists; Password not trivial.						
130	DDIC		Exists; Password not trivial.						

- Shows default user ID status across all clients in the SAP system
- In addition to not having default passwords, all IDs excluding TMSADM should be locked

SAP System Parameters

Used to maintain configuration over the operation of the SAP system

Provide system-wide control over some aspects of Security

Several options for applying to SAP system

- Globally for all instances
 - Set in the system Default profile
DEFAULT.PFL
- Separately for each instance
 - Set in an Instance Profile

Defined via transaction RZ10

Parameters: logon behavior (typical SOX)

Parameter	How Used
Login/fails_to_session_end	Defines the number of times a user can enter an incorrect password before the system terminates the logon attempt
Login/fails_to_user_lock	The number of times a user can enter an incorrect password before the system locks the user.
Login/failed_user_auto_unlock	Enable automatic unlock of [auto] locked user at midnight
rdisp/gui_auto_logout	Maximum time (in seconds) allowed between input from the GUI before automatic logout. 0 = not active

Parameters: Password Characteristics (typical SOX)

Parameter	How Used
Login/min_password_lng	Sets the minimum password length. Values can be a minimum of 3, and a maximum of 40*.
Login/password_expiration_time	Number of days after which a password must be changed. A value of 0 indicates no password change required
Login/password_history_size	Controls the number of passwords SAP stores in password history for each user, rejecting new passwords that exist in the history file.
login/min_password_digits login/min_password_letters login/min_password_lowercase login/min_password_specials login/min_password_uppercase	Define the minimum standards for password composition

* While most passwords controlled by SSO or active directory these days, consider IDs that can bypass

Advanced Parameters: Special logon considerations

Parameter	Risk / What to look for
login/disable_multi_gui_login	If = 0, multiple logins to the same client by the same ID are allowed
login/multi_login_users	Regardless of above, exclusion list of user IDs that are authorized to log into the same client multiple times
login/disable_cpic	If not using CPIC communications, should be set to 1 (RFC communications still allowed, but CPIC will not be)

Advanced Parameters: Passwords & IDs

Parameter	Risk / What to look for
login/password_compliance_to_current_policy	If set to 0, user password does not need to comply with current password rules (if changed frequently) until next required password change
login/password_max_idle_initial	Time in days between initial password setup or password reset and next login before user ID automatically locked
login/password_max_idle_productive	Number of days a user-changed password can be inactive before the ID is automatically locked
login/password_change_waittime	Number of days required between user password changes

Auditing SAP Parameter Settings

Review key parameter settings via transaction RSPFPAR

- Similar to report RSPARAM that you will find in a lot of audit reports, but...
- RSPARAM does not have a standard transaction code, and...
- Unless a custom transaction is assigned to call RSPARAM...
- Then someone would need to run it via SA38...
 - ...And as we said...no one should have SA38 in production 😊
- Compare values to corporate security policies


Advanced Auditing – Use Transaction TU02

- Able to show changes by date, and changes since specified date

Understanding RSPFPAR

If the User-Defined Value is blank:

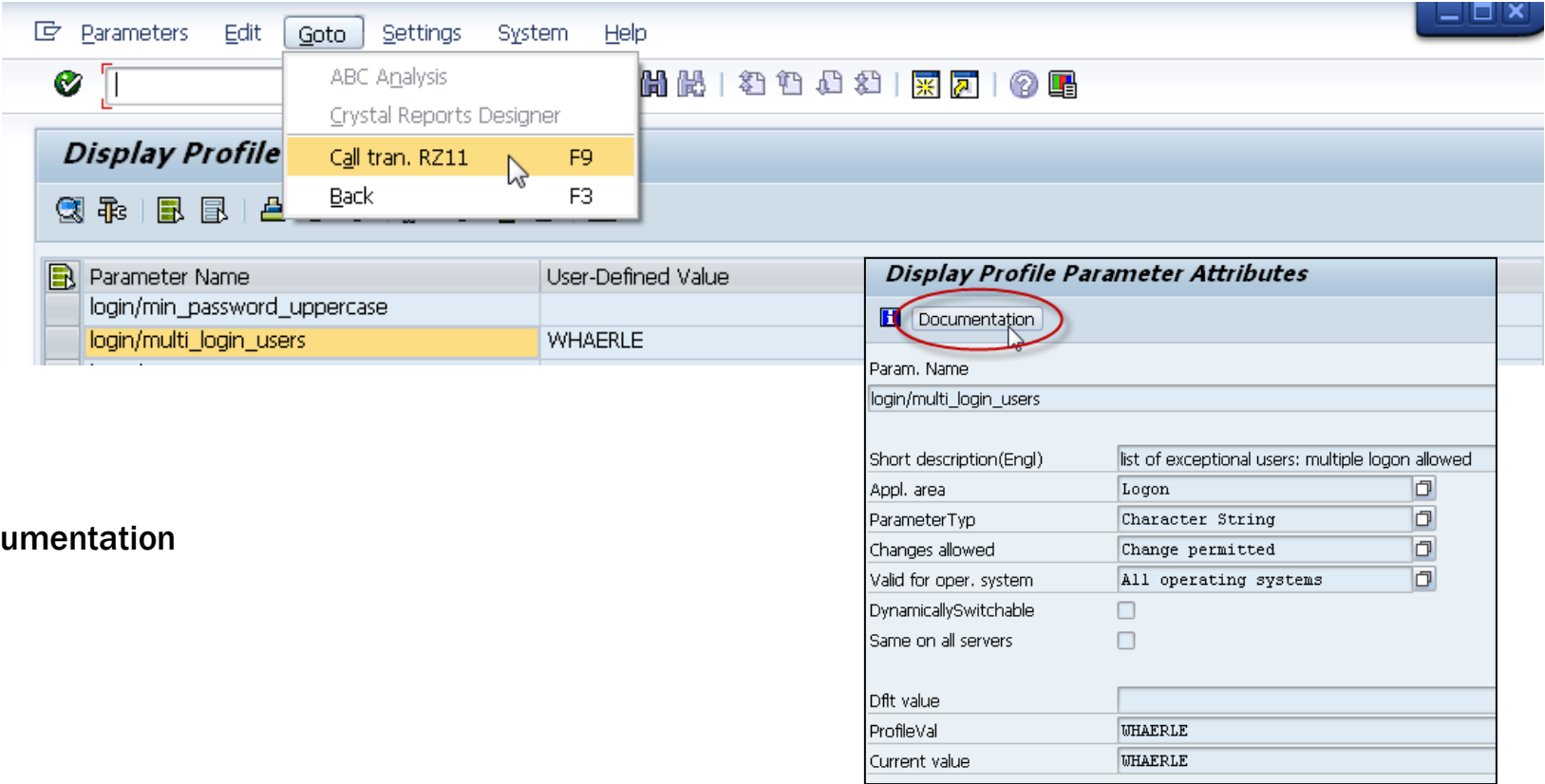
- The System Default Value applies
- Otherwise, the User-Defined Value applies

Display Profile Parameter		
		
Parameter Name	User-Defined Value	System Default Value
login/min_password_uppercase		0
login/multi_login_users	WHAERLE	

Parameter Documentation from RSPFPAR

Highlight the parameter you are interested in

Goto > Call Tran. RZ11



Click the Documentation
icon

TU02: Parameter Change Dates

The screenshot shows the SAP 'Parameter Changes in SAPSYSTEM' dialog box. The title bar includes menu options: List, Edit, Goto, Tune, Edit, Goto, System, Help. Below the title bar is a toolbar with various icons. The main area displays the date and time '08.06.2010 10:06:12 UG7' and the text 'Dates of most recent SAPSYSTEM parameter changes'. A table lists three systems with their host names, system IDs, and modification dates. The third system, 'suse10sap16', is highlighted. A pop-up window titled 'Choose Changed Parameters' is open, showing a date selection field labeled 'Date changed' with a calendar icon. A green checkmark is visible at the bottom of the pop-up.

Host Name	System ID	Modif.
iwd7yt4	59	13.08.20
iwd7yte	02	07.07.20
suse10sap16	00	08.06.20

TU02: Parameter Changes

The screenshot shows the SAP Parameter Changes interface for the system suse10sap16. The window title is "Parameter Changes in SAPSYSTEM suse10sap16 00". The menu bar includes List, Edit, Goto, Tune, Edit, Goto, System, and Help. The toolbar contains various icons for file operations and system functions. Below the toolbar, there are buttons for "Select Period", "Active parameters", "History of file", and "Display: INIT<SID>.ORA". The main content area displays the date and time "08.06.2010 10:14:39" and the user "UG7" for the system "suse10sap16". Below this, the parameter "DIR_ATRA" is listed. A table shows the parameter values for various directories.

Modif.	Parameter	New Parameter Value
08.06.2010	DIR_ATRA	/usr/sap/UG7/DVEBMGS00/data
	DIR_AUDIT	/usr/sap/UG7/DVEBMGS00/log
	DIR_BINARY	/usr/sap/UG7/DVEBMGS00/exe
	DIR_CCMS	/usr/sap/ccms
	DIR_CLIENT_ORAHOME	
	DIR_CT_LOGGING	/usr/sap/UG7/SYS/global
	DIR_CT_RUN	/usr/sap/UG7/SYS/exe/run
	DIR_DATA	/usr/sap/UG7/DVEBMGS00/data
	DIR_DBMS	/usr/sap/UG7/SYS/SAPDB

Authorization object

Key security element providing information about what user authorizations (credentials) *can* be checked

- if referenced by ABAP code or certain other processes, then the user authorizations will be verified before proceeding

Contains one or more *Fields* (up to 10), telling SAP security to look for a certain data element in the user's authorization

These fields then contain *Values*, defining the specific criteria that must be met

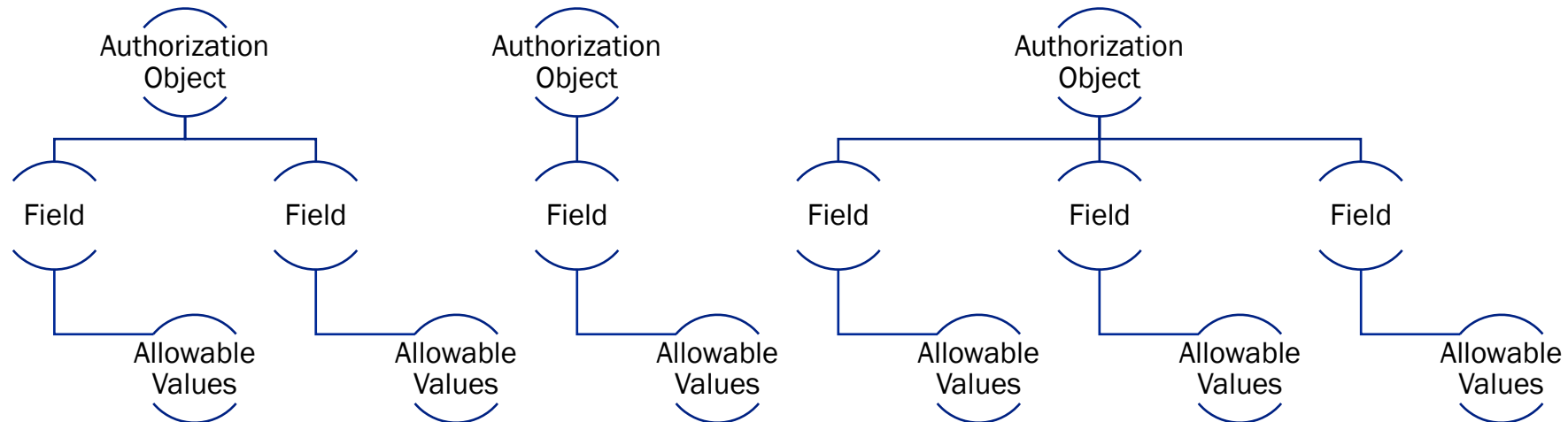
Provided by SAP, but custom objects can also be created

Authorization object, continued...

Within the authorization object, the value of a field often represents specific data or range of data

For example, an authorization object may contain the field BUKRS, which represents the data element Company Code

- The value for field BUKRS could be a specific company code, such as 1000
- The value could also be specified by a wildcard (*) which would be all company codes



ACTVT

A special type of *field* contained by some *authorization objects*

The field ACTVT has values which define the type of activity a user can perform

The most common audit-relevant values referenced by ACTVT include:

- 01 Create
- 02 Maintain
- 03 Display
- 06 Delete

Some activity values are unique to certain types of objects

- 22 Assign is used for security administration

F_BKPF_BUK & F_BKPF_BLA example

Table Entry Edit Goto System Help

Display of Entries Found

Table to be searched: BKPF Accounting Document Header

Number of hits: 500

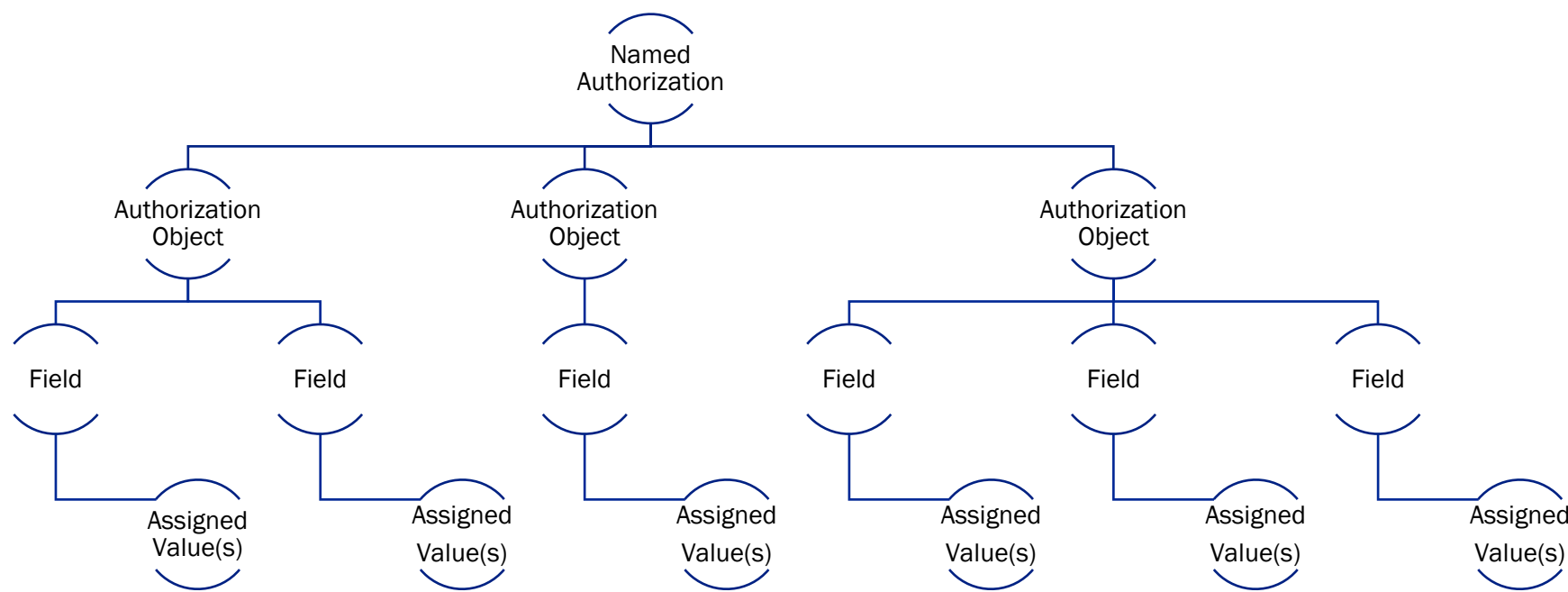
Runtime: 0 Maximum no. of hits: 500

BUKRS	BELNR	GJAHR	BLART	BLDAT	BUDAT	MONAT	CPUDT	CPUTM	AEDA
0001	100000000	1995	SA	06.06.1995	06.06.1995	6	06.06.1995	14:28:00	
0001	100000001	1998	KN	05.05.1998	05.05.1998	5	05.03.1999	17:05:29	
0001	4900000338	2012	WA	02.02.2012	02.02.2012	2	02.02.2012	11:06:20	
0005	6000000	2007	SA	31.12.2007	31.12.2007	12	10.01.2008	09:51:22	
0005	6000000	2008	SA	31.12.2007	01.01.2008	1	10.01.2008	09:51:24	
0005	100000000	2005	SA	31.12.2005	31.12.2005	12	17.05.2006	10:25:02	
0005	100000000	2006	SA	13.03.2006	13.03.2006	3	13.03.2006	15:15:25	
0005	100000000	2007	SA	01.01.2007	16.01.2007	1	16.01.2007	17:17:58	

SAP SE16N suse10sap16 OVR

Authorization

A named set of one or more authorization objects that have been assigned values

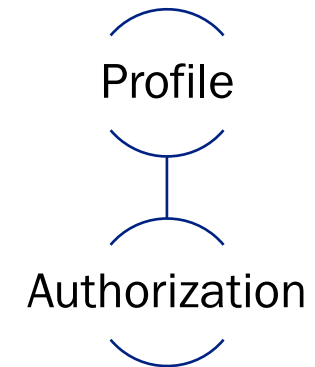
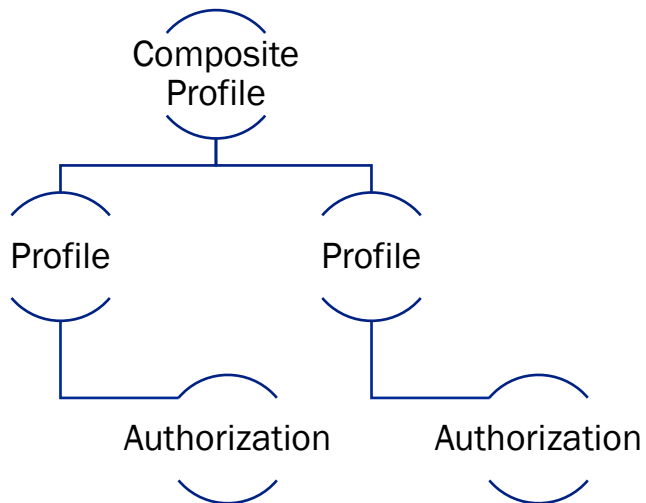


Profile

Defines the *authorization(s)* that will be granted to assigned users

Can only contain authorizations

Composite profiles only contain other profiles



Role

Allows grouping of one or many *Profiles*, typically into a job function or task

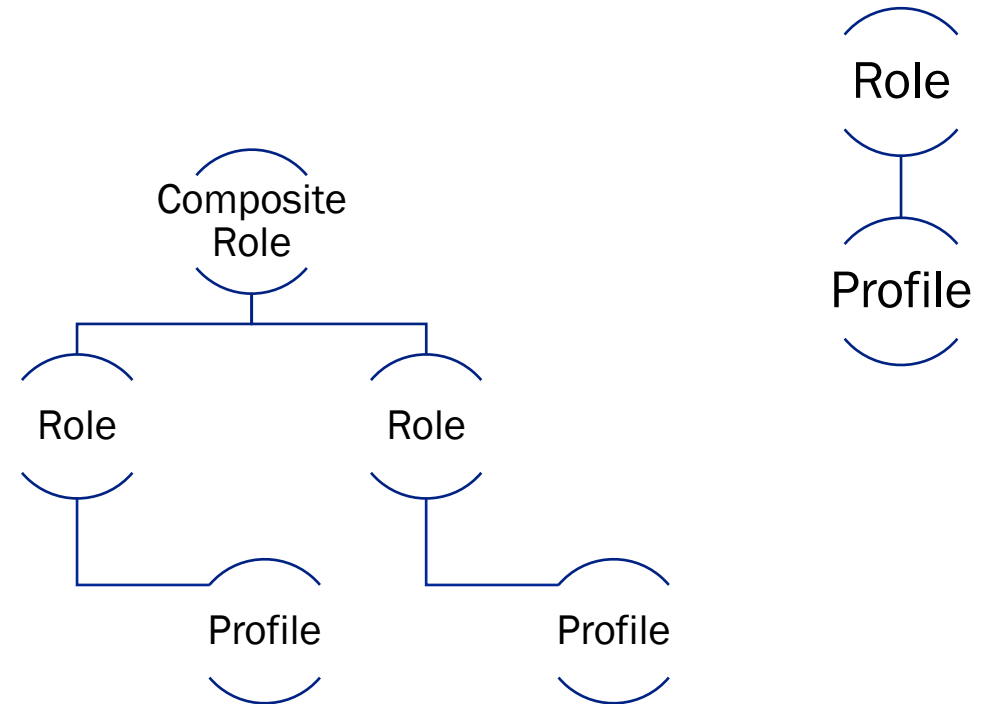
Include at least one *Profile*

Unlike a profile:

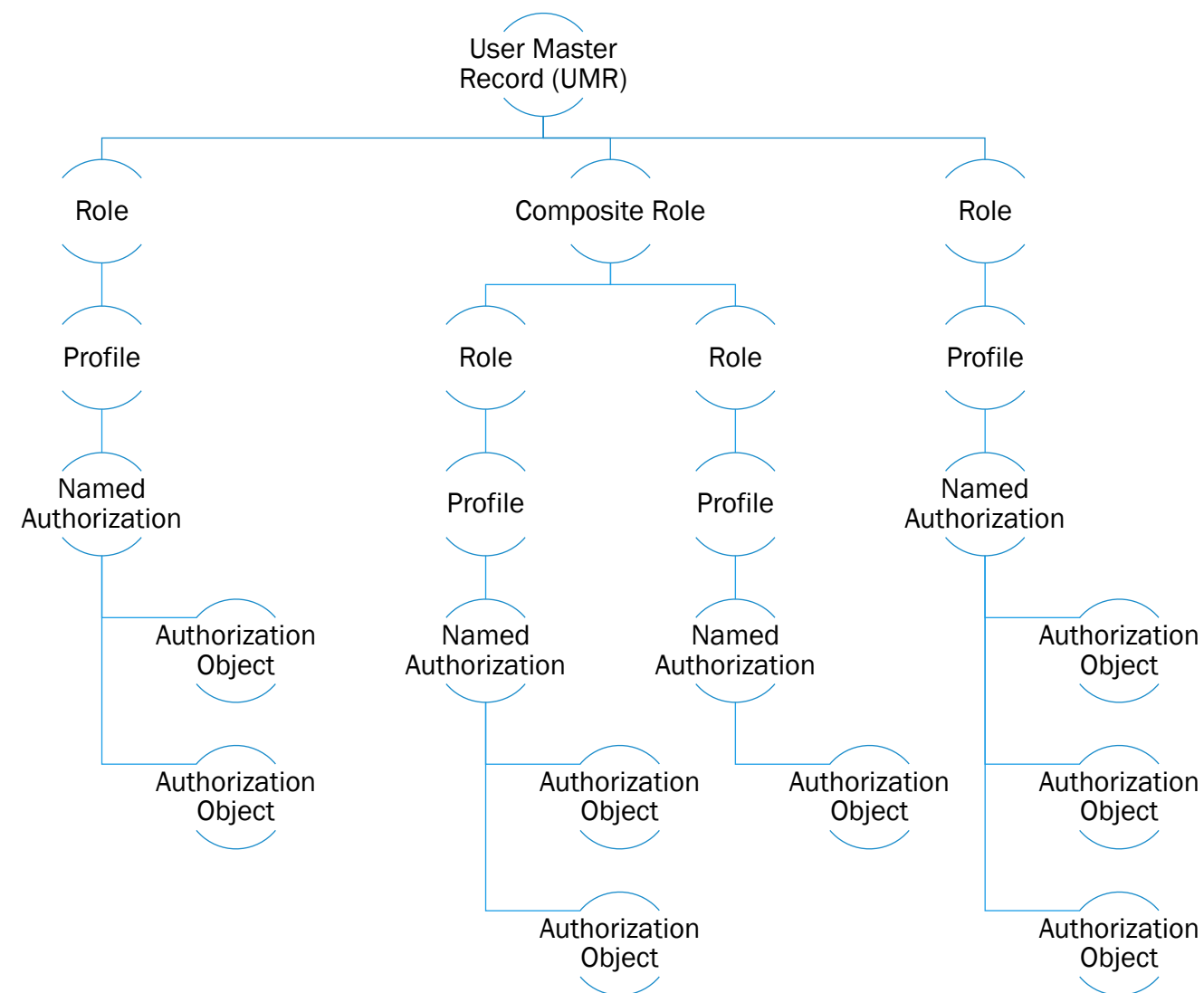
- can be effective-dated

Composite roles can contain one or many single roles

- Same effective dates

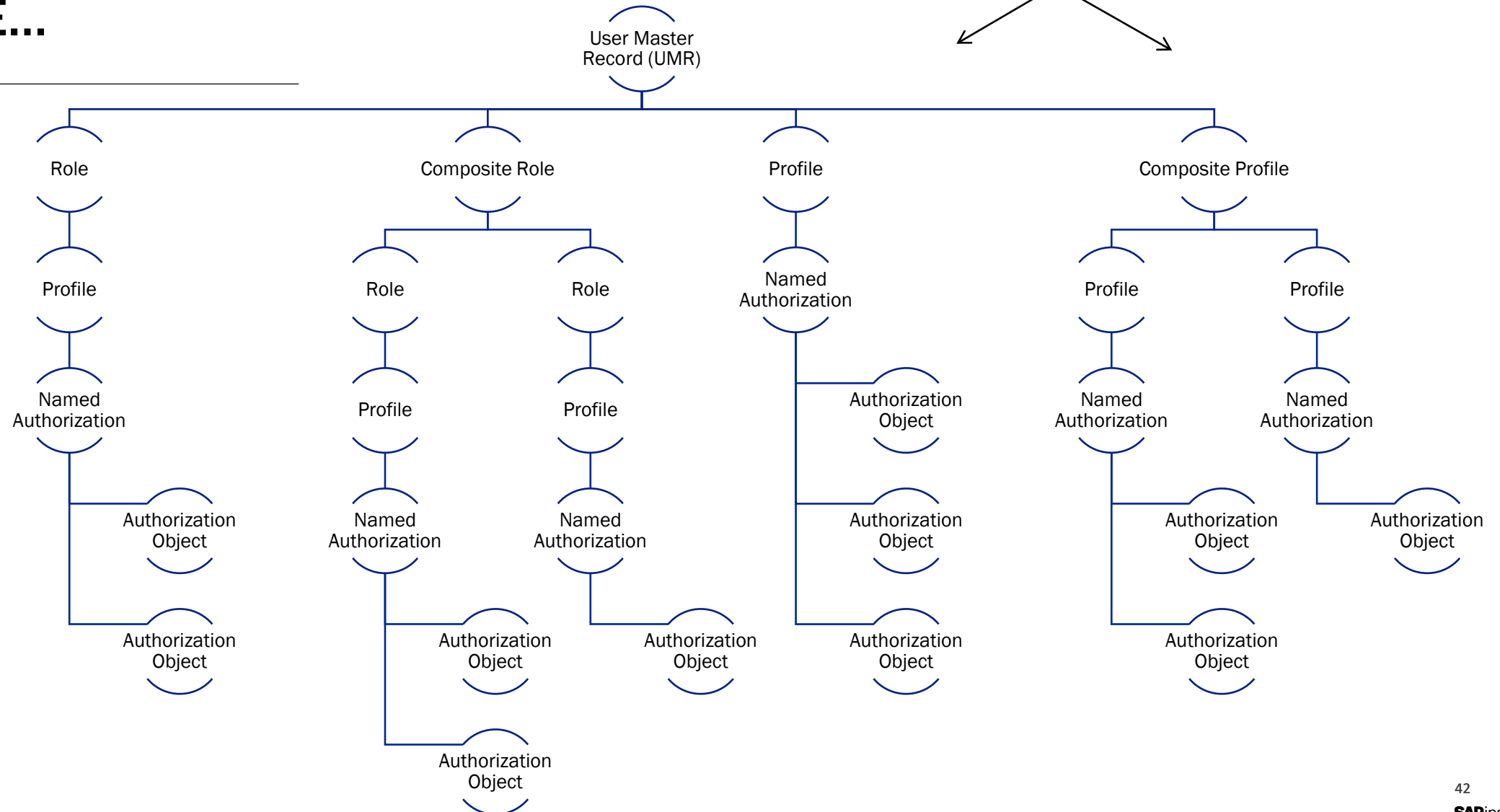


Typical Access



BEWARE...

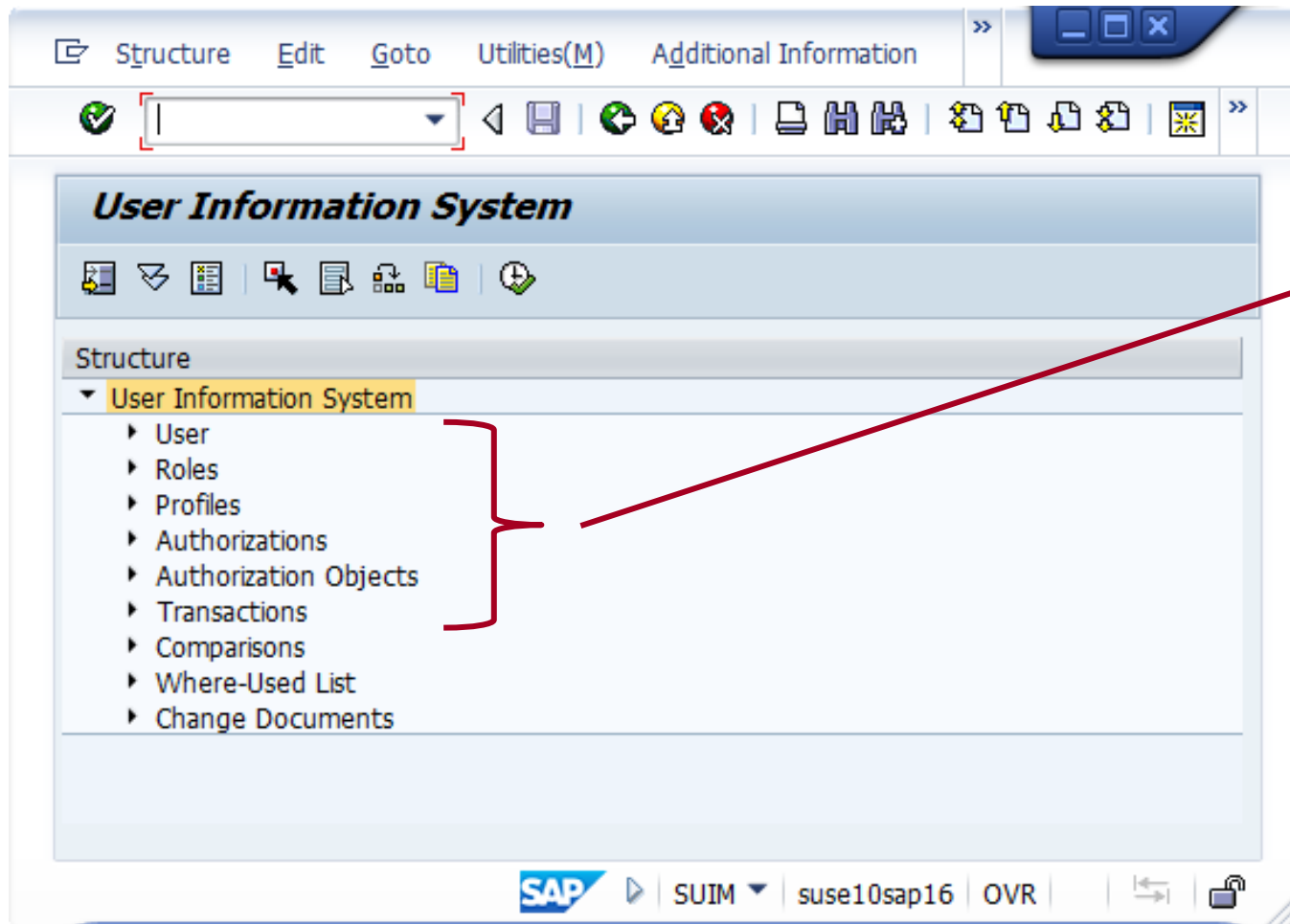
Should be uncommon,
but is possible



SUIM: User Information System

Much of your security audit time will be spent in SUIM

The key to where to start depends on what you want returned (think left column of results)



Ideas for Users by Complex Selection

Look up specific user IDs or groups of IDs

- Contractors
- Terminated/transferred employees

See who has been assigned a known sensitive role

Report on who has been granted specific values for an authorization object in any of their authorizations



The many options for selections with this screen, combined with the use of multi-select criteria, makes this one of the more powerful reporting areas of SUIM

Users By Complex Selection Criteria

Selection criteria for user

User

Group for authorization

User group (general)

Reference user

User ID alias

Role

Profile name

AND Profil

AND Profil

Transaction Code

Selection by Field Name

Field Name

Value

Selection by authorizations

Authorization object

Authorization

Selection by values

Entry values

Authorization object 1

Authorization object

AND authorization object 2

Authorization object

AND authorization object 3

Authorization object

Additional selection criteria

Account number

Start menu

Output Device

Valid until

User Type for Measurement

☐ Locked Users Only

☐ Unlocked Users Only

☐ CATT check ID

* Note: This is an older view of the selection screen to show relevant options more easily

Avoid a common mistake

Transaction Code	FK02
------------------	------

Instead of this...

Always use this:

The “Transaction Code” section on some SUIM screens is only looking for the T-Code in a role menu, and can miss manual assignments as well as T-Codes granted via a directly-assigned profile

Selection by values			
Entry values			
Authorization object 1			
Authorization object		S_ICODE	
Transaction Code			
Value	FK02	OR	
AND		OR	

Roles By Complex Selection Criteria

The screenshot displays the 'Roles By Complex Selection Criteria' dialog box, which is divided into several sections for defining search criteria:

- Standard Selection:** Includes a 'Role' dropdown, a 'Role Short Text' section with 'Description' and 'Language Key' fields, and checkboxes for 'Show Role Long Text', 'Single Roles' (checked), 'Composite Roles' (checked), and 'Only Obsolete Roles'.
- Selection according to user assignments:** Features radio buttons for 'All Roles Regardless of User Assignment' (selected), 'Without User Assignment', and 'With Valid Assignment Of'. Below are 'User(s)' and 'Display List of User/Role Assignments' checkboxes.
- Selection by Assigned Applications in Menu:** Contains a 'Type of Application' dropdown set to 'Transaction' and a 'Transaction code' field with a search icon. Below are four 'AND' fields for further filtering.
- Selection by Profiles and Authorization Objects:** Includes 'Profile name' and 'Authorization Object' fields with search icons.
- Selection according to authorization values:** Features an 'Always Convert Values' checkbox, an 'Input Values' button, and four 'Authorization Object' sections (Object 1 to Object 4) with corresponding value fields.
- Selection by Field Name:** Includes 'Field Name' and 'Value' fields.
- Additional Selection Criteria:** Includes 'Created By' and 'Changed' fields, and 'Changed since' and 'To' fields.
- List Format:** A section at the bottom for selecting the output format.

- Commonly used to find roles granting certain authorizations of audit-interest
- Can also be used to find “display” roles that contain more than display authorizations

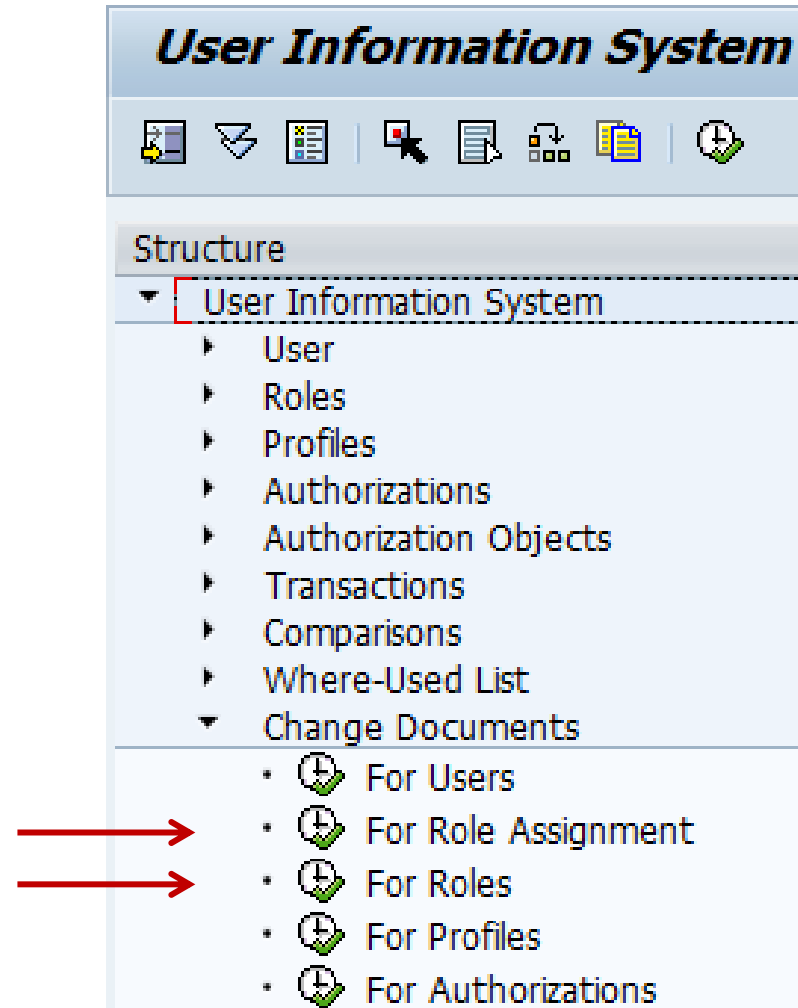
Security Change Documents

Last option in SUIM

Useful for comparing the timing of changes to expectations

- Near key dates
- NOT during certain time-periods

Note: depending on the client where changes are maintained, these may be in development rather than production



Using Access Control? Audit Considerations

Appropriate justification for any disabled rules?

Risk weightings customized?

Addition of organization-specific rules?

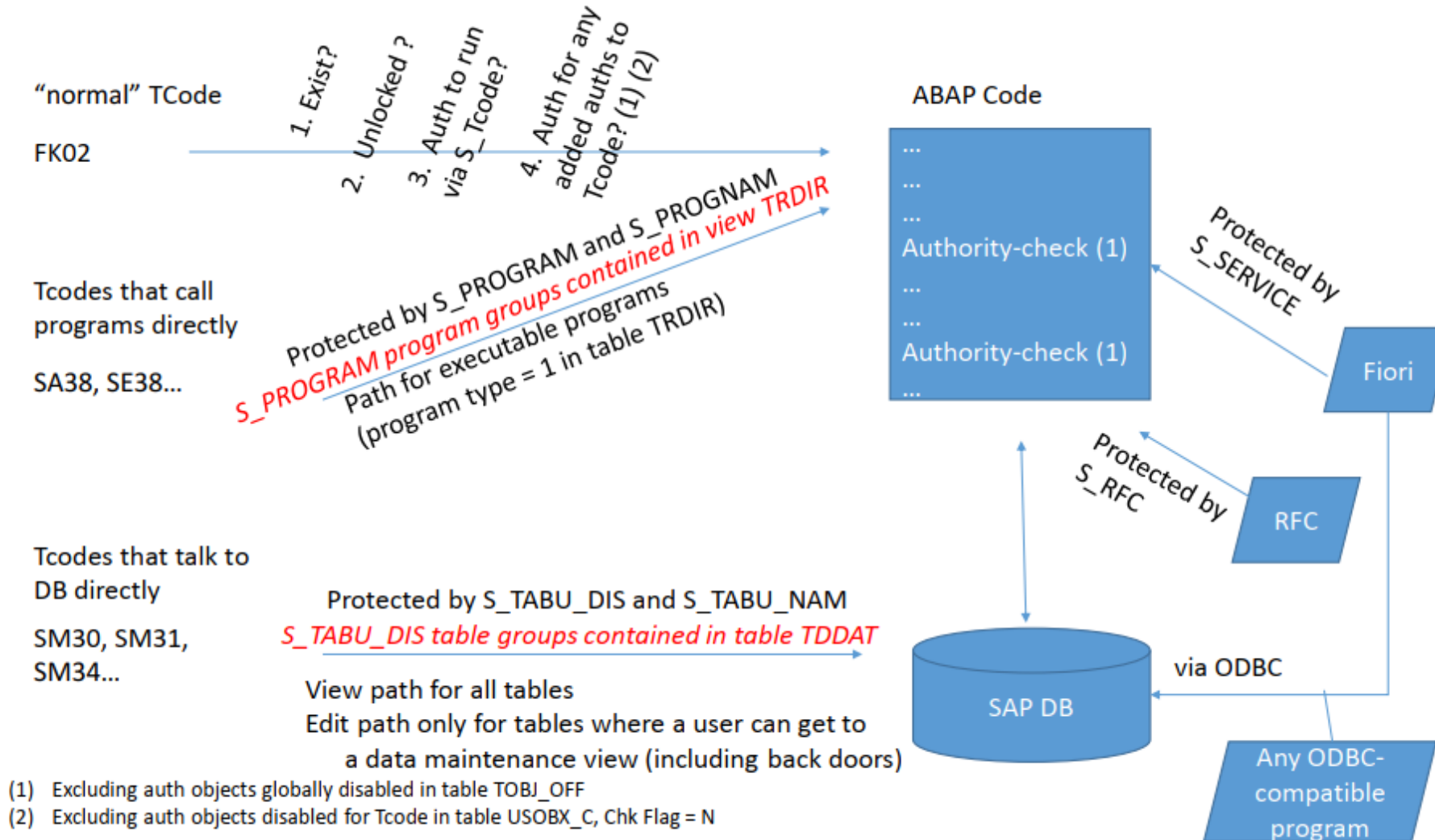
Updated for customizations?

- Transactions
- Authorization objects
- Custom objects used by fields in authorization objects
 - e.g. document types and movement types

Design and operation of mitigating controls

Ongoing process for maintenance

Security: What really happens in the background



Development and change control



Risk: Production Open for Editing

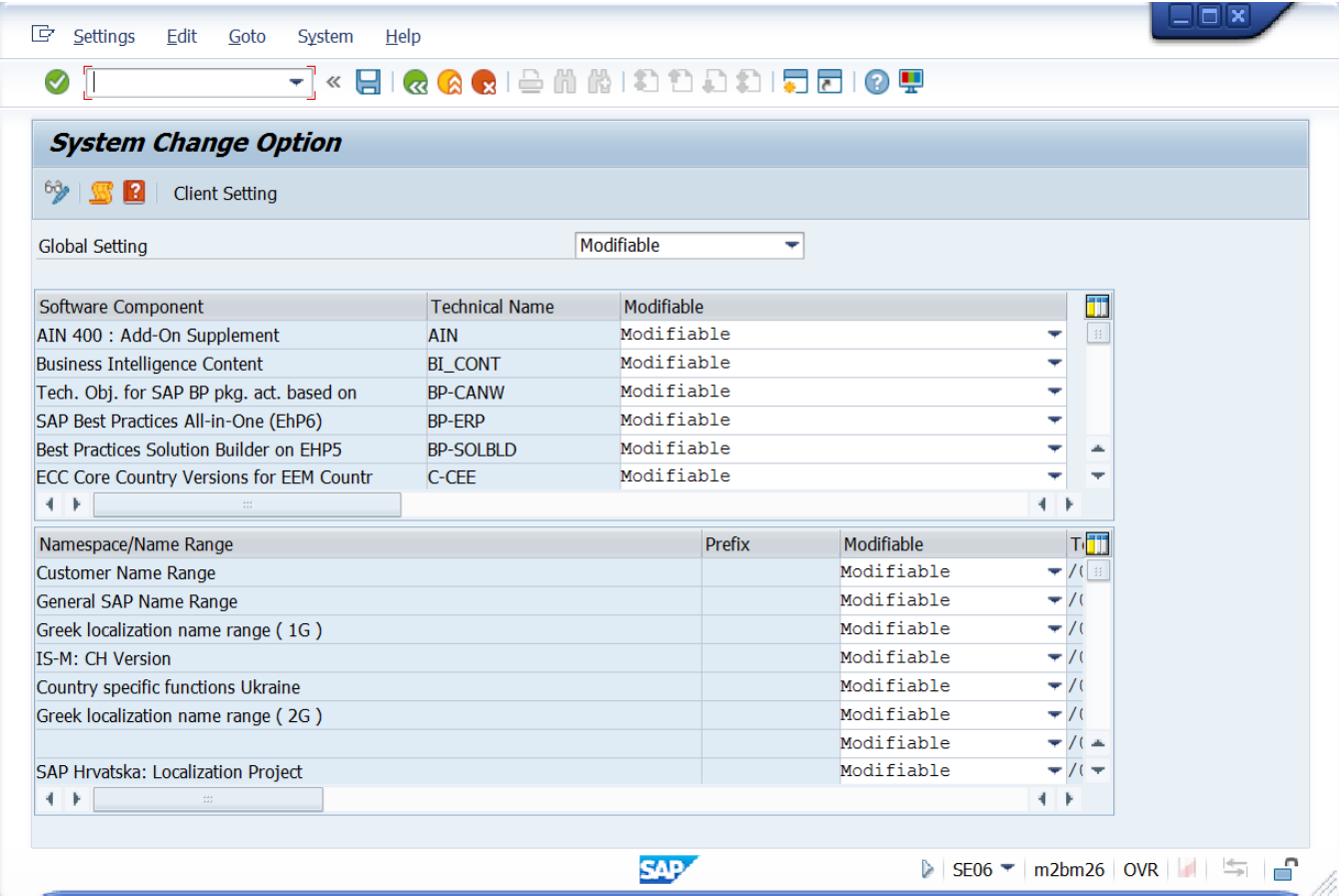
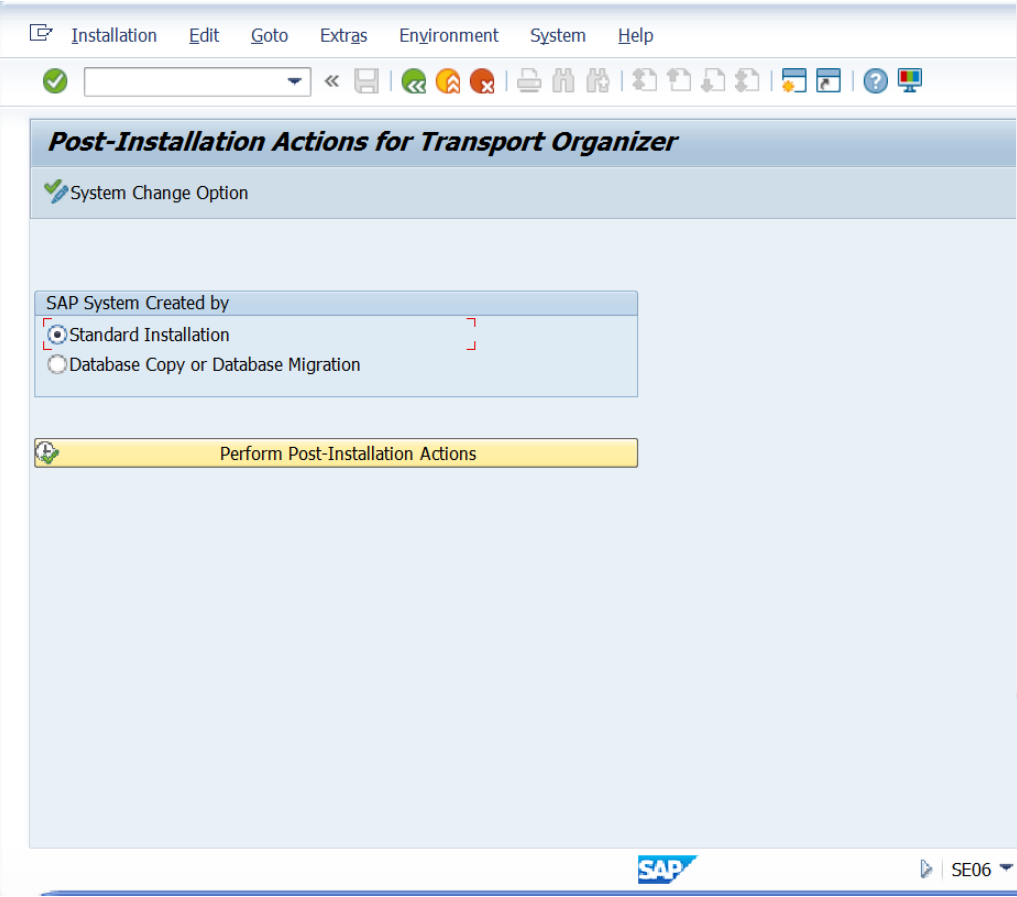
When initially established, programs and other objects can be edited within an SAP System & Client

For production, this violates common change control practices

Two “locks” available

- System lock via SE06 “System Change Option”
- Client lock via SCC4

SE06: System Change Option



SCC4 Review Production Client Lock

Client: 110 Client 110

City: Munich Last Changed By: STUDENT182

Logical system: S4MCLNT110 Date: 02/04/2022

Currency: EUR

Client Role: Production

Changes and Transports for Client-Specific Objects

- ☐ Changes without automatic recording
- ☐ Automatic recording of changes
- ☒ No changes allowed
- ☐ Changes w/o automatic recording, no transports allowed

Cross-Client Object Changes

No changes to repository/cross-client customizing objects

Client Copy and Comparison Tool Protection

Protection level 2: No overwriting, no external availability

CATT and eCATT Restrictions

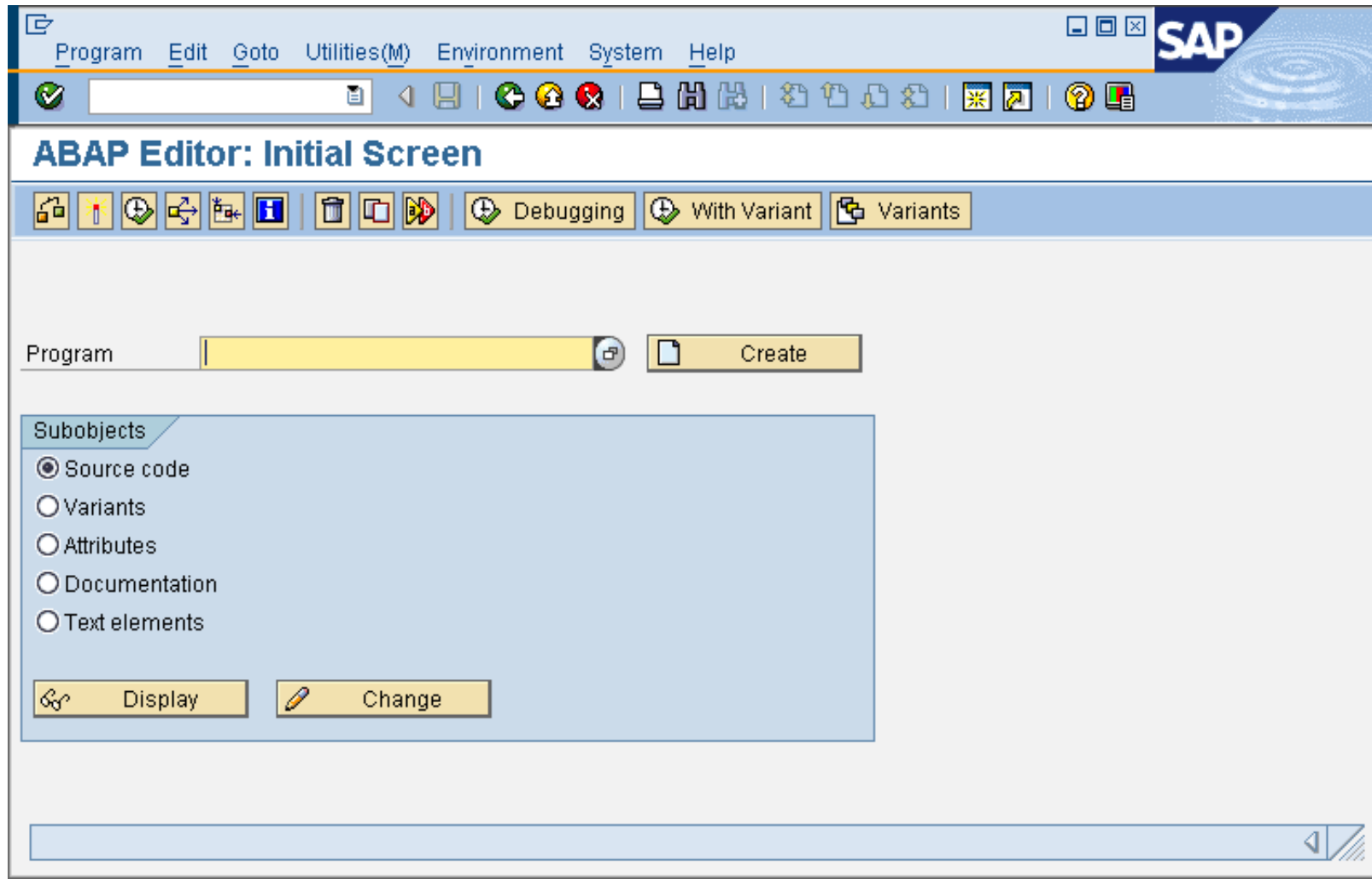
eCATT and CATT Allowed

Restrictions

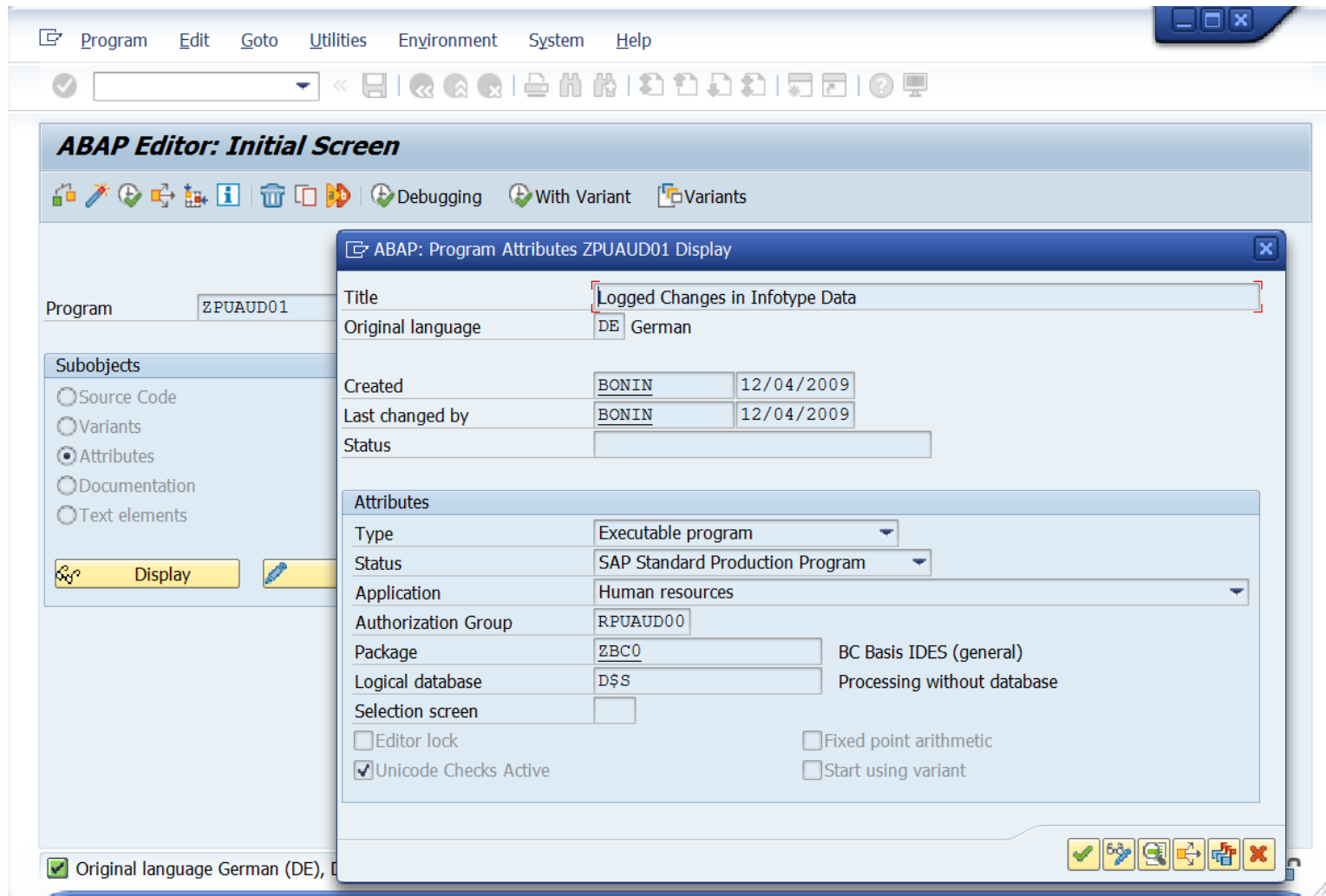
- ☐ Locked due to client copy
- ☐ Protection against SAP upgrade

- Additionally, review changes to the client lock setting during the audit period
- What control in SAP would allow us to see those changes?

SE38: ABAP Editor



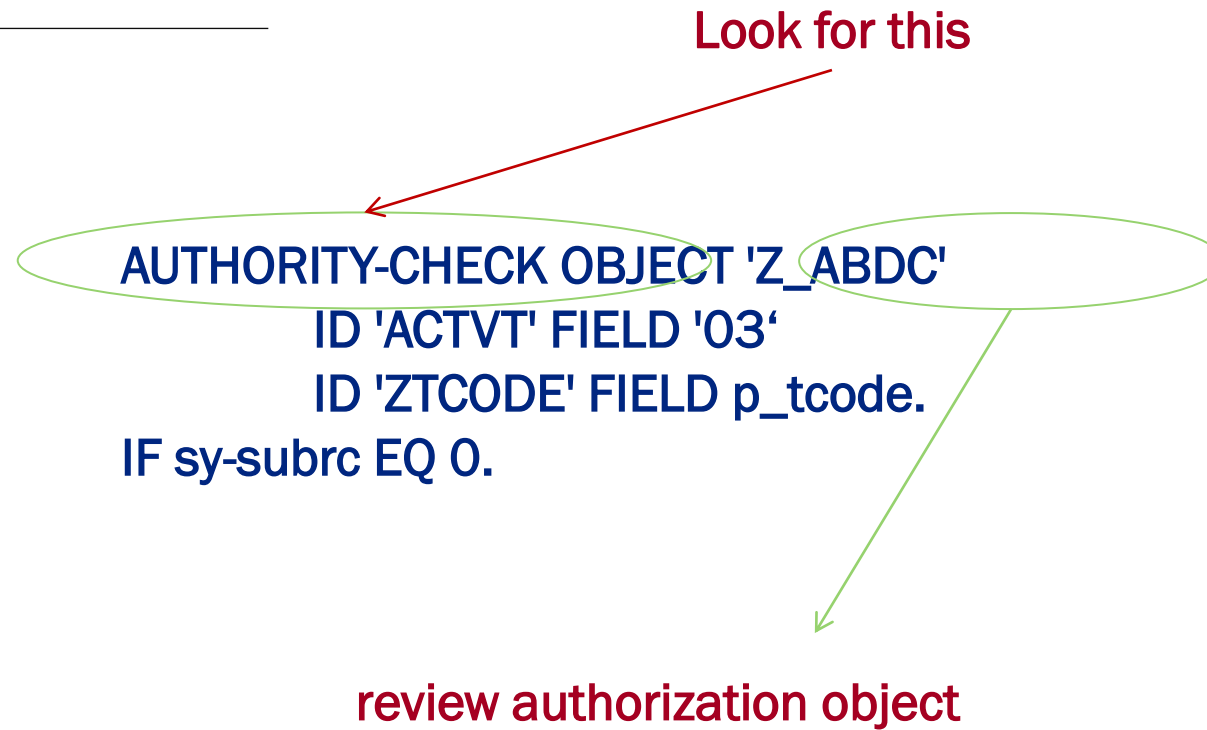
SE38: ABAP Editor - Attributes



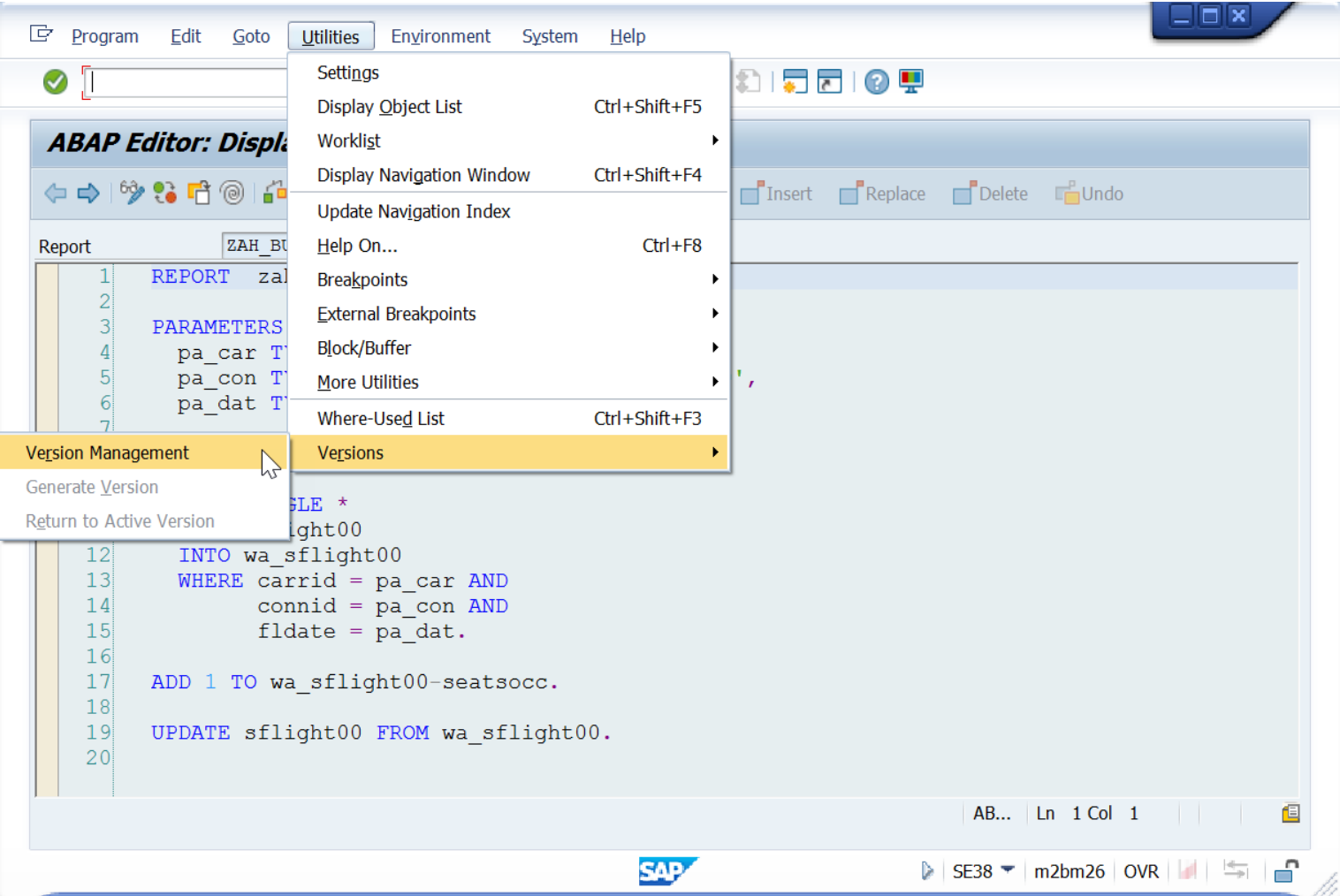
Authorization group used by the S_PROGRAM auth object

All attributes in table TRDIR

Authority Check



Review critical programs for changes



Compare prior versions of code

Versions

Edit

Goto

System

Help

Display

Compare

Retrieve

REMOTE comparison

Exit

F7

F8

Ctrl+F5

Shift+F8

Shift+F3

BUENDELUNG of Type Report Source Code

OTE comparison

Versions: Report Source Code ZAH_BUENDELUNG

Version	Cat	Fla	SAP	Rel.	Arch	Request	Project	Date	Time	Author
Version(s) in the development database:										
<input checked="" type="checkbox"/>	activ			731				07/16/2008	15:48:25	HERRMANNSPAH
Version(s) in the version database:										
<input type="checkbox"/>	00008			701		ID3K932146		12/07/2009	14:47:41	HERRMANNSPAH
<input type="checkbox"/>	00007	I		700		XD0K900996		07/16/2008	15:49:06	HERRMANNSPAH
<input type="checkbox"/>	00006			640		ID3K932078		06/17/2005	09:20:57	HERRMANNSPAH
<input type="checkbox"/>	00005			640		ID3K932073		06/16/2005	17:32:04	HERRMANNSPAH
<input checked="" type="checkbox"/>	00004			640		ID3K932027		06/06/2005	17:40:22	HERRMANNSPAH
<input type="checkbox"/>	00003			640		ID3K932025		06/06/2005	17:39:38	HERRMANNSPAH
<input type="checkbox"/>	00002			640		ID3K931934		05/19/2005	13:18:57	HERRMANNSPAH
<input type="checkbox"/>	00001	s		640				05/19/2005	13:18:32	HERRMANNSPAH

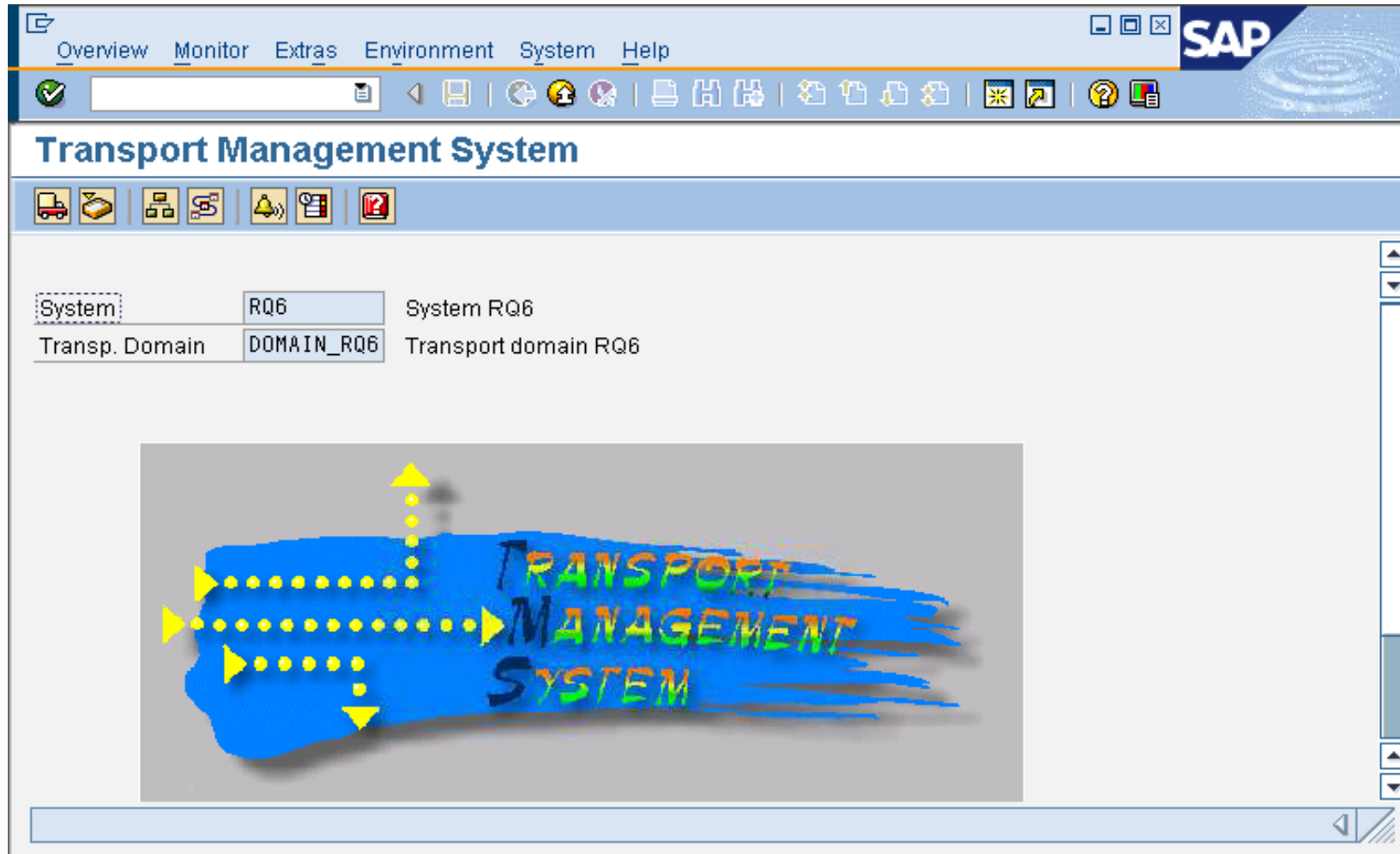
SAP

SE38

m2bm26

OVR

STMS: Transport Management System



Yes, this same graphic is used in SAP S/4HANA 2022

LOL

STMS > Truck Icon: Transports

Queue Edit Goto Request Extras Environment System Help

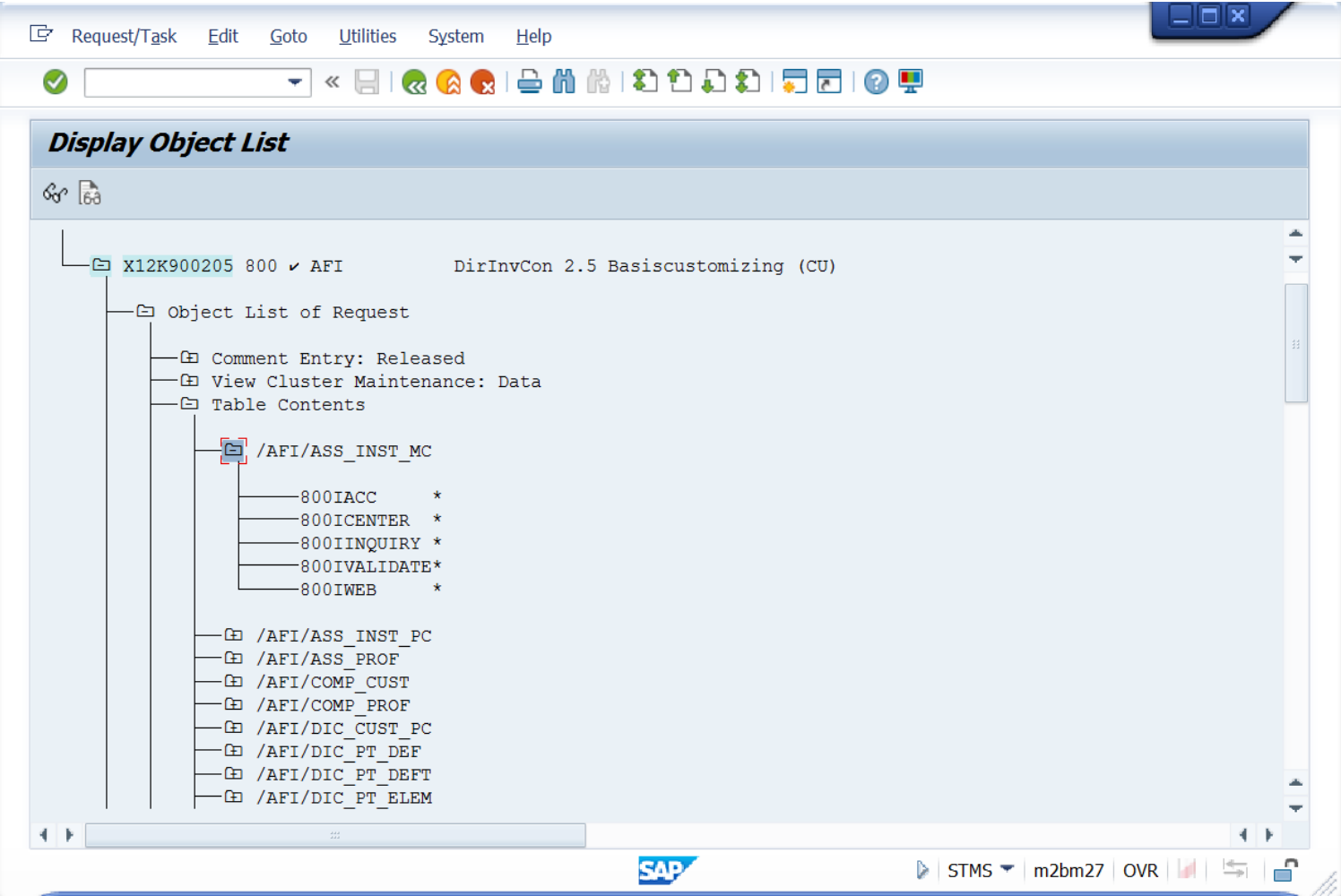
Import Queue: System M27

Requests for M27: 1 / 50 04/23/2018 16:38:23

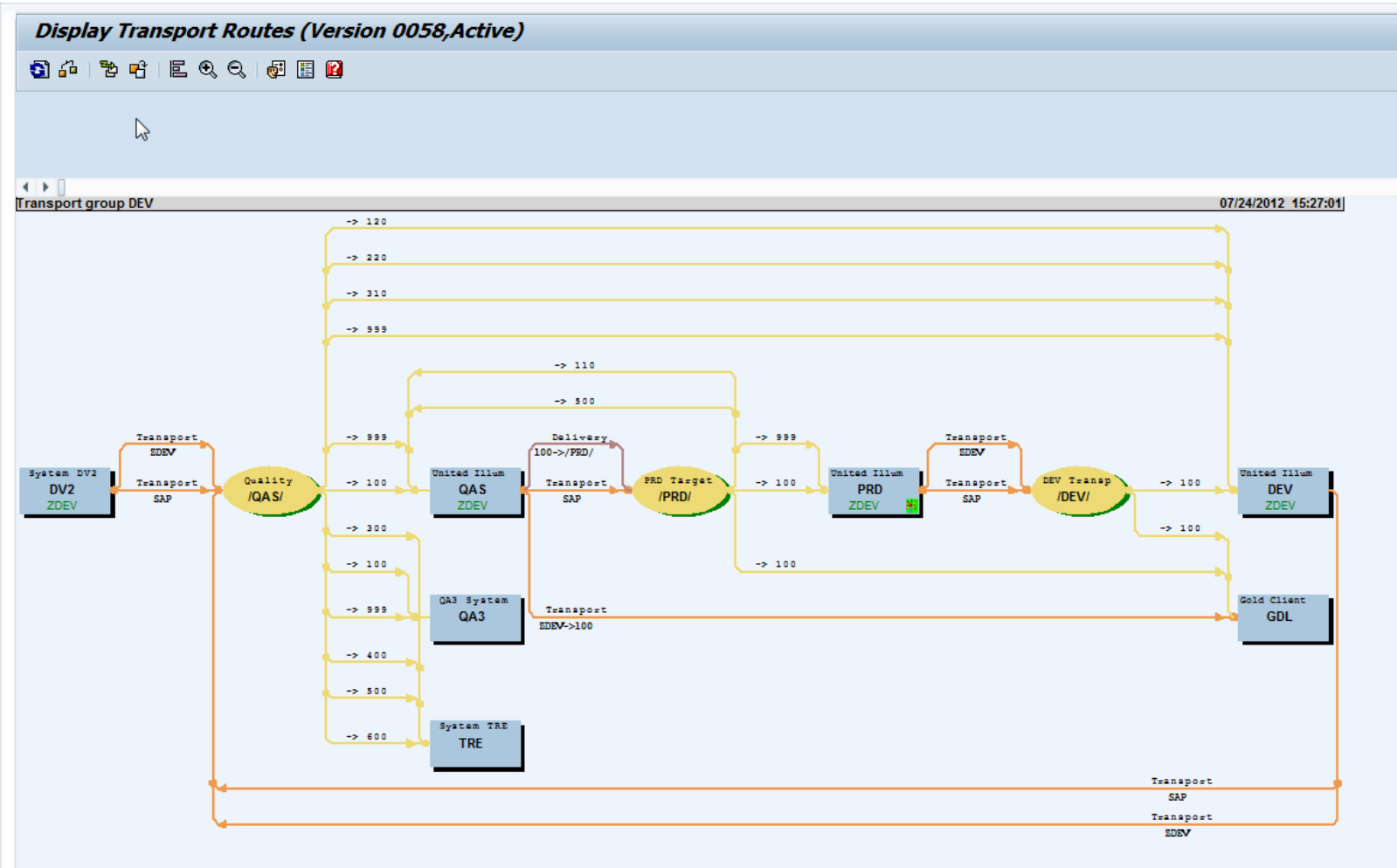
Number	Request	RC	Owner	Short Text	St
20	AF1K903456	✓	AFIPROD	DirectInvoiceControl 2.4 / 2.5 Build 187 Ass&Comp	✓
21	AF1K903989	✓	AFI	DirectInvoiceControl 2.4 / 2.5 build 187 Ass&Comp PL3	✓
22	X12K900205	✓	AFI	DirInvCon 2.5 Basiccustomizing (CU)	✓
23	X12K900201	✓	AFI	DirInvCon 2.5 Basiccustomizing (WB)	✓
24	AF1K903457	✓	AFI	DirectInvoiceControl 2.4-187.1 / 2.5 Steuerung	✓
25	E40K900039	⚠	AFIENTW	AFI/sm Migration des BAdI INVOICE_UPDATE für SAP ERP 6.0	✓
26	E20K907928	⚠	AFIPROD	DirectAgents 1.11	✓
27	AF4K908917	⚠	AFIENTW	AFI / DirInvCon 2.5 / CSK / Vorab DEV / 20170120	✓
28	LW1K901353	⚠	CONSULTSK	ZCSK Attachdown	✓
29	LW1K901401	⚠	CONSULTSK	ZCSK Attachdown korrektur	✓
30	M27K903012	⚙	STUDENT001	02 /CSK/ Commander Paket	⚙
31	M27K903017	⚙	STUDENT001	02 /CSK/ Commander Paket #2	⚙
32	M27K903020	⚙	STUDENT001	AFI DIC CU Brief für Weiterbererechnung	⚙
33	M27K903021	⚙	STUDENT001	AFI DIC CU Center BLART für Weiterber.	⚙
34	M27K903022	⚙	STUDENT001	AFI DIC Grundcustomizing CU TKA	⚙
35	M27K903023	⚙	STUDENT001	AFI CU DirectAgents TKA	⚙
36	M27K903024	⚙	STUDENT001	DIC Grundcustomizing WB TKA	⚙
37	M27K903033	⚙	STUDENT001	/CSK/ Entwicklungen	⚙
38	M27K903048	⚙	STUDENT001	AFI-Centerbeleg anlegen	⚙

SAP STMS m2bm27 OVR

STMS Transport Contents (double-click)



STMS Transport Routes Icon



Review Transports

Review transport path in STMS

Review actual transports in STMS

Review changes not started in development

- First 3 characters of transport request indicate the System ID of the system where the transport was initially created
 - Most easily viewed in table E070
 - Objects transported in table E071

Review changes to the transport path

Configuration Edit Goto Utilities Environment Settings System Help

Get Other Version Shift+F6
Display <-> Change F5
Check
Save
Distribute and Activate
Adjust with Controller
Adjust Transport Routes of System
Standard Configuration
Exit Shift

Single Sy 37

Select Configurations from M27

Vers	S	Short Description	Author	Activation
0006	A	Single System Configuration	SE06 Gener.	201406152201
0005	D	Single System Configuration	SE06 Gener.	201403271319
0004	D	Two System Landscape with cirtual Produc	DDIC	201402041027
0003	D	Single System Configuration	SE06 Gener.	201308200124
0002	D	Two System Landscape with cirtual Produc	DDIC	201207042103

SAP STMS m2bm27 OVR

SAP logging



Summary of Audit-Relevant Logs

Logging Framework	Data / Event Logged	Enabled by Default?
Change Documents	Master data + accounting-relevant transaction data	Yes
Version Management*	Repository objects (i.e., ABAP code)	Yes
Table Logs	Customizing data	No
Security Audit Log	Security-related events	No (ECC) Yes (S4)
System Log	System-related events	Yes
Gateway Logging	SAP Gateway configuration changes and activity	No

Change Documents

About

- Turned on by default
- Can be configured
 - Specified tables
 - Fields within those tables
- Intended for business data
 - But not high-volume transactional data

Common audit uses

- Sample changes to ensure authorized and accurately entered
- Look for high-risk changes
 - Low-risk data to high-risk data
 - “flip-flops”
- Identify abnormal change frequency / timing / user

To Be Reported on a Change Document

The following 3 items must each be in place

1. The field must be related to a *Data Element* that has been marked for writing change documents
2. The field must be in a table that is associated with a *Change Document Object*
3. The change document object must be referenced by a relevant change function module in the ABAP Code for the SAP application program causing the change based on the user input

Change Document Settings: SCDO

Change doc.object Edit Goto Utilities(M) System Help

Change Document Objects: Overview

Change Create Generate update pgm. Generation info

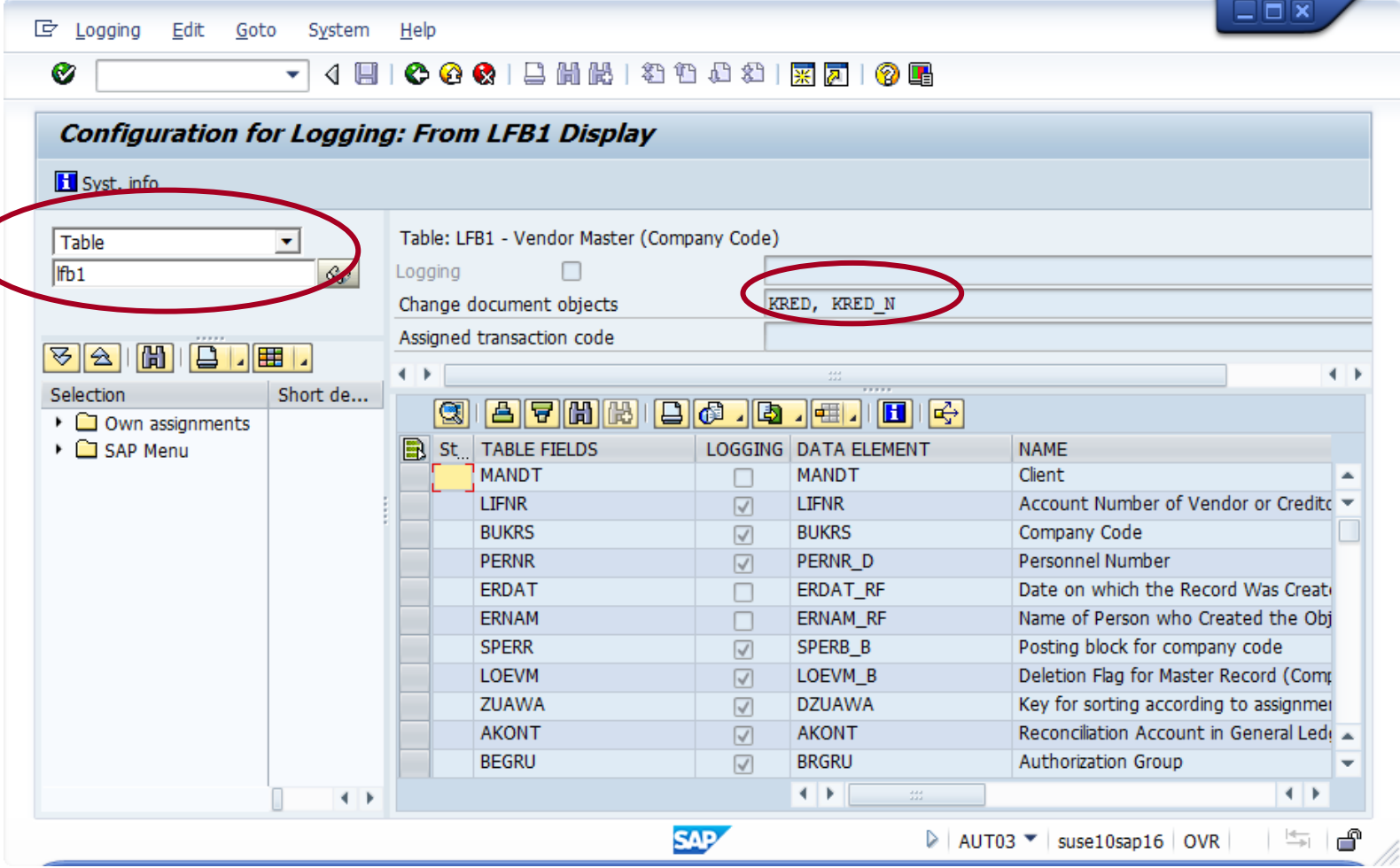
Object	Text
/IBS/RB_CD_KTO	RBD: Master Data Account
/IBS/RB_CD_KTOD	RBD: Account Key Date of a RBD Account
/ISDFPS/EX_BWUL	SDP-BW: External Batches for Batch Where-Used List
/ISDFPS/FLIGHT	Mission
/ISDFPS/FORCE	Force Element
/ISDFPS/FORCER	Reference Force Element
/ISDFPS/FOREPA	Force Element - Equipment Package Relationship
/ISDFPS/FORMC	Force Element - Material Container Relationship
/ISDFPS/FORMCH	HR - Material Container Relationship
/ISDFPS/FORMPH	HR - Material Planning Object Relationship

Object 1 /

SAP SAPMSCDO suse10sa

- BANF = Purchase Requisition
- BANK = Bank Master
- BELEG = Financial documents
- COND_A = Pricing conditions
- EINKBELEG = Purchasing Documents
- FAKTBELEG = Billing Document
- INCOMINGINVOICE = insert best guess ;-)
- VERKBELEG = Sales Document
- PFCG = Role Maintenance (security)

View Object Class with AUT03




The screenshot shows the SAP 'Configuration for Logging: From LFB1 Display' window. The 'Table' dropdown is set to 'lfb1'. The 'Change document objects' field contains 'KRED, KRED_N'. The 'Assigned transaction code' field is empty. The table below lists fields and their logging status.

St...	TABLE FIELDS	LOGGING	DATA ELEMENT	NAME
	MANDT	<input type="checkbox"/>	MANDT	Client
	LIFNR	<input checked="" type="checkbox"/>	LIFNR	Account Number of Vendor or Credit
	BUKRS	<input checked="" type="checkbox"/>	BUKRS	Company Code
	PERNR	<input checked="" type="checkbox"/>	PERNR_D	Personnel Number
	ERDAT	<input type="checkbox"/>	ERDAT_RF	Date on which the Record Was Creat
	ERNAM	<input type="checkbox"/>	ERNAM_RF	Name of Person who Created the Obj
	SPERR	<input checked="" type="checkbox"/>	SPERB_B	Posting block for company code
	LOEVM	<input checked="" type="checkbox"/>	LOEVM_B	Deletion Flag for Master Record (Comp
	ZUAWA	<input checked="" type="checkbox"/>	DZUAWA	Key for sorting according to assignme
	AKONT	<input checked="" type="checkbox"/>	AKONT	Reconciliation Account in General Led
	BEGRU	<input checked="" type="checkbox"/>	BRGRU	Authorization Group

The status bar at the bottom shows 'AUT03', 'suse10sap16', and 'OVR'.

Reviewing Change Documents

Display Changes to Vendors

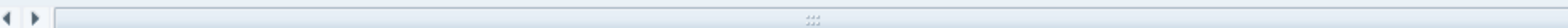
 Selections

IDES-ALE: Central FI Syst
Frankfurt - Deutschland

Display Changes to Vendors

Time 04:01:32
RFKABL00/STEVEN

Date	Time	Vendor	Changed By	Field Name	CoCd	POrg	New value	Old value
							New value	Old value
11.01.2013	12:58:42	3802	STEVEN	Chk double inv.	3000			X
08.10.2012	22:26:53	51235	MAHES	VSR relevant			X	
28.02.2012	04:39:34	T-K515B16	DECLAN	City			Dublin	Neustadt
28.02.2012	04:39:34	T-K515B16	DECLAN	Country			IE	DE
28.02.2012	04:39:34	T-K515B16	DECLAN	Name			Minola Supplies Inc.	Abbot Supplies Inc.
28.02.2012	04:39:34	T-K515B16	DECLAN	Postal Code			24	10032
28.02.2012	04:39:34	T-K515B16	DECLAN	Street			ITT Dublin	Mainstr.




 FK04 suse10sap16 OVR

Table Logging

About

- Disabled by default
- Numerous tables set to be logged by default
 - (if table logging gets turned on)
- Faulty belief that affects performance
 - Addressed by several SAP notes

Common audit uses

- Review when the production client has been opened for editing
- Review when posting periods have been opened/closed
- Set triggers to notify of key configuration changes

Using Table Logging

Step 1: Enable the table logging parameter

- rec/client: set to the client number of the production client

Step 2: Define the tables to be logged

- Transaction SE13
- Select the table
- Ensure the “Log” flag is set

Step 3: Review the logs

- Transaction SCU3

Table Logging: Relevant SAP Notes



SAP Note 608835 - Performance problems due to table logging?

Note Language: English

Version: 2 Validity: Valid Since 27.03.2003

Summary

Symptom

You want to activate table logging in your system profile parameter but you are not getting good performance.



SAP Note 1653464 - Enable Change Log Monitoring by Activating Table Logging

Note Language: English

Version: 1 Validity: Valid Since 16.11.2011

Summary

Symptom

SAP GRC provides monitoring tools to enable customers to analyze logged changes to configuration tables, and recommends that customers enable Basis logging to the DBTABLOG table via the rec/client setting. Customers point out that traditionally SAP has advised customers to turn logging off globally, and their IT departments have concerns in going against this standard practice of keeping logging off.

SAP GRC recommends that table logging be enabled in production systems, since the actual performance impact has been found to be low. This recommendation is consistent with all relevant prior guidance from SAP on this topic.

SE13 Table Log Flag

Dictionary: Display Technical Settings

Revised<->Active

Name	Z812_MP_PP_CTRL	Transparent Table
Short text	SF/MP Control Table	
Last Change	STUDENT001	08/07/2012
Status	Active	Saved

Logical storage parameters

Data class	APPL0	Master data, transparent tables
Size category	0	Data records expected: 0 to 3,300

Buffering


☒ Buffering not allowed
☐ Buffering allowed but switched off
☐ Buffering switched on

Buffering type

<input type="checkbox"/> Single records buff.	No. of key fields	0
<input type="checkbox"/> Generic Area Buffered		
<input type="checkbox"/> Fully Buffered		

☐ Log data changes
☐ Write access only with JAVA

SCU3 Log File Review

Evaluation of change logs																																		
 Techn. information Logging: Display status																																		
Tables: Change Logs																																		
Clients																																		
Technical Name: T000																																		
Date : 02/26/2016 User: STUDENT001																																		
<table><tr><th></th><th>Key Fields</th><th colspan="3">Function Fields, Changed</th></tr><tr><th>Time</th><th>Client</th><th>Field Name</th><th>Old</th><th>New</th></tr><tr><td>20:35:08</td><td>912</td><td>Corr. sys.</td><td>1</td><td></td></tr><tr><td></td><td></td><td>CHANGEDATE</td><td>02/06/2015</td><td>02/26/2016</td></tr></table>						Key Fields	Function Fields, Changed			Time	Client	Field Name	Old	New	20:35:08	912	Corr. sys.	1				CHANGEDATE	02/06/2015	02/26/2016										
	Key Fields	Function Fields, Changed																																
Time	Client	Field Name	Old	New																														
20:35:08	912	Corr. sys.	1																															
		CHANGEDATE	02/06/2015	02/26/2016																														
Date : 02/27/2016 User: STUDENT007																																		
<table><tr><th></th><th>Key Fields</th><th colspan="3">Function Fields, Changed</th></tr><tr><th>Time</th><th>Client</th><th>Field Name</th><th>Old</th><th>New</th></tr><tr><td>11:42:13</td><td>912</td><td>Copy lock</td><td></td><td>X</td></tr><tr><td>11:45:38</td><td>912</td><td>Copy lock</td><td>X</td><td></td></tr><tr><td>11:49:07</td><td>912</td><td>Copy lock</td><td></td><td>X</td></tr><tr><td>11:54:31</td><td>912</td><td>Copy lock</td><td>X</td><td></td></tr></table>						Key Fields	Function Fields, Changed			Time	Client	Field Name	Old	New	11:42:13	912	Copy lock		X	11:45:38	912	Copy lock	X		11:49:07	912	Copy lock		X	11:54:31	912	Copy lock	X	
	Key Fields	Function Fields, Changed																																
Time	Client	Field Name	Old	New																														
11:42:13	912	Copy lock		X																														
11:45:38	912	Copy lock	X																															
11:49:07	912	Copy lock		X																														
11:54:31	912	Copy lock	X																															

Security Audit Log

About

- Disabled by default in ECC
- Enabled by default in S4
- Once enabled, can configure what type of events to log
- Events categorized by SAP into different severity levels
 - Some require proactive monitoring, while others best left for investigation if an event occurs

Common audit uses

- Identify when changes to security-relevant configuration has occurred
- Review ID usage
- Look for patterns of rejection
 - Logon
 - Transaction starts

Using the Security Audit Log

Step 1: Set key parameters

- rsau/enable: Set to 1 to enable security logging
- rsau/local/file: set the location of the audit log on the application server
- rsau/max_diskspace_local: Set the maximum length of the audit log

Step 2: Define what to log

- Transaction SM19 to define logging “filters”
- Clicked the detail section to see specific events

Step 3: Review the logs

- Transaction SM20N

Example Security Audit Log: Dump to Excel

Date	Column1	Time	User Name	Terminal	Transaction Code	Program	Security Audit Log message text
3/1/2015		12:14:15	T-FRANK	USFRANK	SESSION_MANAGER	SAPMSYST	Password check failed for user T-FRANK in client 200
3/1/2015		12:14:15	T-FRANK	USFRANK	SESSION_MANAGER	SAPMSYST	Logon failed (reason=1, type=A, method=P)
3/1/2015		12:14:20	T-FRANK	USFRANK	SESSION_MANAGER	SAPMSYST	Password check failed for user T-FRANK in client 200
3/1/2015		12:14:20	T-FRANK	USFRANK	SESSION_MANAGER	SAPMSYST	Logon failed (reason=1, type=A, method=P)
3/1/2015		12:14:31	T-FRANK	USFRANK	SESSION_MANAGER	SAPMSYST	Logon successful (type=A, method=P)
3/1/2015		13:14:23	T-FRANK	USFRANK	SE16		User Logoff
3/3/2015		6:31:56	T-RENUKA	UR700CIS06	SESSION_MANAGER	SAPMSYST	Logon successful (type=A, method=P)
3/3/2015		6:54:37	T-RENUKA	UR700CIS06	FPL9	SAPMFKL9	Dynamic ABAP Coding: Event - Event Type: G! Checksum: -
3/3/2015		6:54:37	T-RENUKA	UR700CIS06	FPL9	SAPMFKL9	Dynamic ABAP Coding: Event - Event Type: G! Checksum: -
3/3/2015		7:03:18	T-RENUKA	UR700CIS06	FPL9	SAPMFKL9	Dynamic ABAP Coding: Event - Event Type: G! Checksum: -
3/3/2015		8:15:18	T-RENUKA	UR700CIS06	SESSION_MANAGER	SAPLSMTR_NAVIGATION	User Logoff
3/3/2015		8:15:18	T-RENUKA	UR700CIS06		SAPMSYST	User Logoff
3/3/2015		8:15:18	T-RENUKA	UR700CIS06		SAPMSYST	User Logoff
3/4/2015		12:11:15	T-RENUKA	UR700CIS06	SESSION_MANAGER	SAPMSYST	Logon successful (type=A, method=P)
3/4/2015		12:11:47	T-RENUKA			SAPMSSYC	Logon successful (type=B, method=P)
3/4/2015		13:22:01	T-RENUKA	UR700CIS06	EMMACLS		User Logoff
3/4/2015		16:35:21	T-RENUKA	UR700CIS06	SESSION_MANAGER	SAPMSYST	Logon successful (type=A, method=P)

SM19 Configuration (Screenshot from ECC)

Security Audit: Administer Audit Profile

Static Configuratio

DynamicConfigurati

Active profile

MYTEST

Activated By

STUDENT001

07/16/2014

Displayed profile

MYTEST

Changed By

STUDENT001

07/16/2014

Filter 1

Filter 2

☒Filter active

Reset

Detailed Display

Selection criteria	Audit classes	Events
<div>Client</div> <div>912</div>	<div><input checked="" type="checkbox"/>Dialog logon</div>	<div>All</div>
<div>User</div> <div>STUDENT001</div>	<div><input checked="" type="checkbox"/>RFC/CPIC logon</div> <div><input checked="" type="checkbox"/>RFC call</div> <div><input checked="" type="checkbox"/>Transaction start</div> <div><input checked="" type="checkbox"/>Report start</div> <div><input checked="" type="checkbox"/>User master change</div> <div><input checked="" type="checkbox"/>System</div> <div><input checked="" type="checkbox"/>Other events</div>	

Audit Class	Event Class	Recording	Message Text
Dialog Logon	Non-Crit.	✓	User Logoff
	Non-Crit.	✓	Test message CU1
	Important	✓	Logon Successful (Type=&A)
	Important	✓	Logon Failed (Reason = &B, Type = &A)
	Critical	✓	Logon Failed (Reason = &B, Type = &A)
	Critical	✓	User &B Locked in Client &A After Erroneous Password Check
	Critical	✓	User &B in Client &A Unlocked After Being Locked Due to In
RFC/CPIC Logon	Non-Crit.	✓	RFC/CPIC Logon Successful (Type = &A)
	Critical	✓	RFC/CPIC Logon Failed, Reason = &B, Type = &A
RFC Function Call	Non-Crit.	✓	Successful RFC Call &C (Function Group = &A)
	Critical	✓	Failed RFC Call &C (Function Group = &A)
Transaction Start	Non-Crit.	✓	Transaction &A Started
	Important	✓	Transaction &A Locked
	Important	✓	Transaction &A Unlocked
	Critical	✓	Start of transaction &A failed (Reason=&B)
Report Start	Non-Crit.	✓	Report &A Started
	Important	✓	Start Report &A Failed (Reason = &B)
User Master Change	Non-Crit.	✓	Password changed for user &B in client &A
	Important	✓	User &A Deleted
	Important	✓	User &A Locked
	Important	✓	User &A Unlocked
	Important	✓	Authorizations for User &A Changed
	Important	✓	User Master Record &A Changed
	Important	✓	Authorization/Authorization Profile &B Created
	Important	✓	Authorization/Authorization Profile &B Deleted
	Important	✓	Authorization/Authorization Profile &B Changed
	Critical	✓	User &A Created
	Critical	✓	Authorization/Authorization Profile &B Activated
Other Events	Important	✓	Download &A Bytes to File &C
	Important	✓	Digital Signature (Reason = &A, ID = &B)
	Important	✓	ICF recorder entry executed for user &A (Activity: &B)
	Important	✓	ICF Recorder entry executed by user &A (&B,&C) (activity: &
	Important	✓	Administration setting was changed for ICF Recorder (Activ
	Important	✓	Virus Scan Interface: Error "&C" occurred in profile &A (step
	Critical	✓	Digital Signature Error (Reason = &A, ID = &B)
	Critical	✓	Password check failed for user &B in client &A
	Critical	✓	Change Security Check During Export: Old Value &A, New V
	Critical	✓	Transport Request &A Contains Security-Critical Source Obje
	Critical	✓	Virus Scan Interface: Virus "&C" found by profile &A (step &
System	Critical	✓	Audit Configuration Changed
	Critical	✓	Audit: Slot &A: Class &B, Severity &C, User &D, Client &E, S
	Critical	✓	Application Server Started
	Critical	✓	Application Server Stopped
	Critical	✓	Audit: Slot &A Inactive
	Critical	✓	Audit: Active Status Set to &1

Event Class	Audit Class	Recording Message	Message ID System log message text (Before setting variables)	Report alert
Chill Chain Dialog Logon	AUS	Logoff (reason=AA, type=BA, method=BC)	AUS User AB Logged in Client Error: Password Checks	
	AUN	User AB In client AA Unlocked After Being Locked Due To Invalid Password Entered	AUN User AB in client AA Unlocked After Being Locked Due To Invalid Password Entered	
	BUI	Web Service Logon failed (type BA, WP AC). Refer to Web service log BA.	BUI SPNego reject after failed (type BA, WP AC) Refer to Web service log BA.	
	CIA	Client AB 2.0: Logged-on client user AA, assertion not same as parameter client ID AB	CIA Client AB 2.0: Logged-on client user AA, assertion not same as parameter client ID AB	
	CUB	Client AB 2.0: Client ID AB in SAML, assert none same as client ID AB in request	CUB Client AB 2.0: Client ID AB in SAML, assert none same as client ID AB in request	
	AUC	User Logout	AUC User Logout	
	BUE	Web Service Logon successful (type BA, WP AC). Refer to Web service log BA.	BUE Web Service Logon successful (type BA, WP AC). Refer to Web service log BA.	
	BUR	SA Assertion Used	BUR SA Assertion Used	
	BAI	Name	BAI Name	
	BEN	Attribute	BEN Attribute	
BUD	Authentication Assertion	BUD Authentication Assertion		
BUP	Signed LogoutRequest accepted	BUP Signed LogoutRequest accepted		
BUQ	Unsigned LogoutRequest rejected	BUQ Unsigned LogoutRequest rejected		
BUR	Unsigned LogoutRequest accepted	BUR Unsigned LogoutRequest accepted		
CIA	Client AB 2.0: Access token issued (client=BA, user=AB, grant type=BC)	CIA Client AB 2.0: Access token issued (client=BA, user=AB, grant type=BC)		
CIB	Client AB 2.0: Valid access token received for user BA	CIB Client AB 2.0: Valid access token received for user BA		
AUI	Logon successful (type BA, method=AC)	AUI Logon successful (type BA, method=AC)		
AUD	Logon failed (reason=BA, type=BA)	AUD Logon failed (reason=BA, type=BA)		
CIC	Client AB 2.0: Invalid access token received (reason=BA)	CIC Client AB 2.0: Invalid access token received (reason=BA)		
CID	Client AB 2.0: Insufficient Client AB scope for requested resource (user=BA)	CID Client AB 2.0: Insufficient Client AB scope for requested resource (user=BA)		
CIS	Client AB 2.0: Client AB requested invalid access grant type AB	CIS Client AB 2.0: Client AB requested invalid access grant type AB		
CIT	Client AB 2.0: Scope AB not permitted for client AC, user AD (cause=BA)	CIT Client AB 2.0: Scope AB not permitted for client AC, user AD (cause=BA)		
CJA	Rejected Assertion	CJA Rejected Assertion		
CIB	BA, AB	CIB BA, AB		
CIC	BA	CIC BA		
CIE	Name ID of a subject	CIE Name ID of a subject		
CIF	Attribute	CIF Attribute		
CIP	Authentication Assertion	CIP Authentication Assertion		
CJH	Signed LogoutRequest rejected	CJH Signed LogoutRequest rejected		
CJI	Unsigned LogoutRequest rejected	CJI Unsigned LogoutRequest rejected		
AUV	Digital Signature Error (Reason = BA, ID = AB)	AUV Digital Signature Error (Reason = BA, ID = AB)		
BCL	Password check failed for user AB in client BA	BCL Password check failed for user AB in client BA		
BBS	Change Security Check During Export: Old Value BA, New Value BB	BBS Change Security Check During Export: Old Value BA, New Value BB		
BUB	Virus Scan Interface: Virus "XAC" found by profile BA (step AB)	BUB Virus Scan Interface: Virus "XAC" found by profile BA (step AB)		
BUC	HTTP Security Session Management was deactivated for client BA	BUC HTTP Security Session Management was deactivated for client BA		
BUS	BA: Request without sufficient security characteristic of address AB:	BUS BA: Request without sufficient security characteristic of address AB:		
BUT	Certificate check for subject BA with profile BA failed (status BC)	BUT Certificate check for subject BA with profile BA failed (status BC)		
BVY	Field contents changed: XAS/XAS(XS/MS)	BVY Field contents changed: XAS/XAS(XS/MS)		
BUZ	> in program BA, use AB, event AC	BUZ > in program BA, use AB, event AC		
CIX	C debugging activated	CIX C debugging activated		
CJL	Field content changed: BA	CJL Field content changed: BA		
CJM	Jump to AB Debugger: BA	CJM Jump to AB Debugger: BA		
CJN	A manually caught process was stopped from within the Debugger (BA)	CJN A manually caught process was stopped from within the Debugger (BA)		
CJO	Explicit database content or rollback from debugger BA	CJO Explicit database content or rollback from debugger BA		
CJP	Non-exclusive debugging session started	CJP Non-exclusive debugging session started		
DON	Active scenario BA changed (ID)	DON Active scenario BA changed (ID)		
BDU	Active scenario BA changed (ID)	BDU Active scenario BA changed (ID)		
BHA	Dynamic ABAP Coding: Event AB Event Type: MB Checksums: AC	BHA Dynamic ABAP Coding: Event AB Event Type: MB Checksums: AC		
BUIF	HTTP Security Session Management was activated for client BA.	BUIF HTTP Security Session Management was activated for client BA.		
BAU		BAU		
CJG	Payload of PDU message BA was read (I)	CJG Payload of PDU message BA was read (I)		
CJT	> BA	CJT > BA		
CJK	Payload of postprocessing request BA read	CJK Payload of postprocessing request BA read		
DNE	EHS-SADN: Configuration of service BA changed on host AB	DNE EHS-SADN: Configuration of service BA changed on host AB		
DUF	EHS-SADN: File BA transferred from host AB	DUF EHS-SADN: File BA transferred from host AB		
DUG	EHS-SADN: File BA transferred to host AB	DUG EHS-SADN: File BA transferred to host AB		
DUH	Check for BA in whitelist AB was successful	DUH Check for BA in whitelist AB was successful		
DUX	Authorization check for object BA in scenario AB successful	DUX Authorization check for object BA in scenario AB successful		
DUP	Authorization check for object BA in scenario AB failed	DUP Authorization check for object BA in scenario AB failed		
DYO	Download BA bytes to file AC	DYO Download BA bytes to file AC		
BDI	Digital Signature (Reason = BA, ID = AB)	BDI Digital Signature (Reason = BA, ID = AB)		
BDJ	I/O recorder entry executed by user BA (Activity: AB)	BDJ I/O recorder entry executed by user BA (Activity: AB)		
BLG	I/O Recorder entry executed by user BA (Activity: AB)	BLG I/O Recorder entry executed by user BA (Activity: AB)		
BDP	Administration setting was changed for I/O Recorder (Activity: BA)	BDP Administration setting was changed for I/O Recorder (Activity: BA)		
BDQ	Virus Scan Interface: Error "XAC" occurred in profile BA (step AB)	BDQ Virus Scan Interface: Error "XAC" occurred in profile BA (step AB)		
BUA	WS: Signature check error (reason AB, WP AC). Refer to Web service log BA.	BUA WS: Signature check error (reason AB, WP AC). Refer to Web service log BA.		
BUB	WS: Signature insufficient (WP AC). Refer to Web service log BA.	BUB WS: Signature insufficient (WP AC). Refer to Web service log BA.		
BUC	WS: Time stamp is invalid. Refer to Web service log BA.	BUC WS: Time stamp is invalid. Refer to Web service log BA.		
BBH	HTTP Security Session of user BA (client AB) was hand ended	BBH HTTP Security Session of user BA (client AB) was hand ended		
BWT	OK, download failed with error code BA	BWT OK, download failed with error code BA		
CJ	Test Message	CJ Test Message		
CJQ	Logical file name AB not configured. Physical file name AB not checked.	CJQ Logical file name AB not configured. Physical file name AB not checked.		
CJR	Physical file name AB does not fulfill requirements from logical file name BA	CJR Physical file name AB does not fulfill requirements from logical file name BA		
CJS	Logical file name BA is not a valid alias for logical file name BA	CJS Logical file name BA is not a valid alias for logical file name BA		
CJU	Validation for logical file name BA is not active	CJU Validation for logical file name BA is not active		
DUA	EHS-SADN: Service BA created on host AB	DUA EHS-SADN: Service BA created on host AB		
DUB	EHS-SADN: Service BA started on host AB	DUB EHS-SADN: Service BA started on host AB		
DUC	EHS-SADN: Service BA ended on host AB	DUC EHS-SADN: Service BA ended on host AB		
DUD	EHS-SADN: Service BA deleted on host AB	DUD EHS-SADN: Service BA deleted on host AB		
DUE	Check for BA in whitelist AB failed	DUE Check for BA in whitelist AB failed		
DUM	Report BA Started	DUM Report BA Started		
DUN	Start Report BA failed (Reason = BB)	DUN Start Report BA failed (Reason = BB)		
AIA	Failed RFC Call AC (Function Group = AA)	AIA Failed RFC Call AC (Function Group = AA)		
AIB	Failed Web service access (reason=BA, type=BA, method=BC, reason = BA-C)	AIB Failed Web service access (reason=BA, type=BA, method=BC, reason = BA-C)		
AIC	Generic table access by RFC BA with activity BB	AIC Generic table access by RFC BA with activity BB		
ADJ	Server BA is not contained in the whitelist	ADJ Server BA is not contained in the whitelist		
DAH	Connection to server BA failed	DAH Connection to server BA failed		
DAB	There is no logical file name for path BA	DAB There is no logical file name for path BA		
DAD	Validation for BA failed	DAD Validation for BA failed		
AIK	Successful RFC Call AC (Function Group = AA)	AIK Successful RFC Call AC (Function Group = AA)		
CIV	Successful WS Call (service = AA, operation BB)	CIV Successful WS Call (service = AA, operation BB)		
DDE	Validation for BA is successful	DDE Validation for BA is successful		
DDB	FTP connection request for server BA successful	DDB FTP connection request for server BA successful		
DUJ	FTP server whitelist is empty	DUJ FTP server whitelist is empty		
DDB	FTP server whitelist is not active due to use of placeholders	DDB FTP server whitelist is not active due to use of placeholders		
AUE	RFCFCIP logon failed, reason=BA, type=BA, method=BC	AUE RFCFCIP logon failed, reason=BA, type=BA, method=BC		
AUS	RFCFCIP logon successful (type=BA, method=AC)	AUS RFCFCIP logon successful (type=BA, method=AC)		
System	AAC	Auth Configuration Change	AAC Auth Configuration Change	
	AUF	Auth: Slot BA: Class AB, Severity BC, User RD, Client BE, Wf	AUF Auth: Slot BA: Class AB, Severity BC, User RD, Client BE, Wf	
	AIA	Application Server Started	AIA Application Server Started	
AHI	Application Server Stopped	AHI Application Server Stopped		
AIO	Auth: Slot BA Inactive	AIO Auth: Slot BA Inactive		
AIS	Auth: Active Status Set to BA	AIS Auth: Active Status Set to BA		
Transaction-Transaction Start	AIA	Start of transaction BA failed (Reason=AB)	AIA Start of transaction BA failed (Reason=AB)	
	CJ	Failed to start application BA (reason=AB)	CJ Failed to start application BA (reason=AB)	
	AII	Transaction BA Started	AII Transaction BA Started	Non-Critical
Non-Critical	CIE	Application BA Started	CIE Application BA Started	
	AIP	Transaction BA Locked	AIP Transaction BA Locked	Severe
	AIOQ	Transaction BA Unlocked	AIOQ Transaction BA Unlocked	
User Master Change	BAU	Test Message	BAU Test Message	
	AUI7	User BA Created	AUI7 User BA Created	Critical
	AUI3	Authorization/Authorization Profile AB Activated	AUI3 Authorization/Authorization Profile AB Activated	
Non-Critical	BUS	Password changed for user AB in client BA	BUS Password changed for user AB in client BA	
	AUI8	User BA Deleted	AUI8 User BA Deleted	Severe
	AUI9	User BA Locked	AUI9 User BA Locked	
User Master Change	AUI8	Authorizations for user BA Changed	AUI8 Authorizations for user BA Changed	
	AUID	User Master Record BA Changed	AUID User Master Record BA Changed	
	AUI6	Authorization/Authorization Profile AB Created	AUI6 Authorization/Authorization Profile AB Created	
	AUI5	Authorization/Authorization Profile AB Deleted	AUI5 Authorization/Authorization Profile AB Deleted	
	AUI7	Authorization/Authorization Profile AB Changed	AUI7 Authorization/Authorization Profile AB Changed	
	AUI9	User BA Locked	AUI9 User BA Locked	
	DUN	Client AB 2.0: Token declared invalid (Client client=BA, user=AB, token type=BC)	DUN Client AB 2.0: Token declared invalid (Client client=BA, user=AB, token type=BC)	

Additional Logs - Discussion

System Log (SM21)

Gateway Log (SMGW)

New Considerations with SAP S/4HANA



S/4 Transition Impact

Simplifies the data model (reduction in tables and new tables)

Rewrite custom code

Account for new authorization objects

New business functions; Adds and removes transaction codes

Fiori

A large and growing library of Fiori mobile apps

Need to account for application catalogs that are available (Fiori ABAP system/gateway)

Broad business access within different applications, present SODs issues.

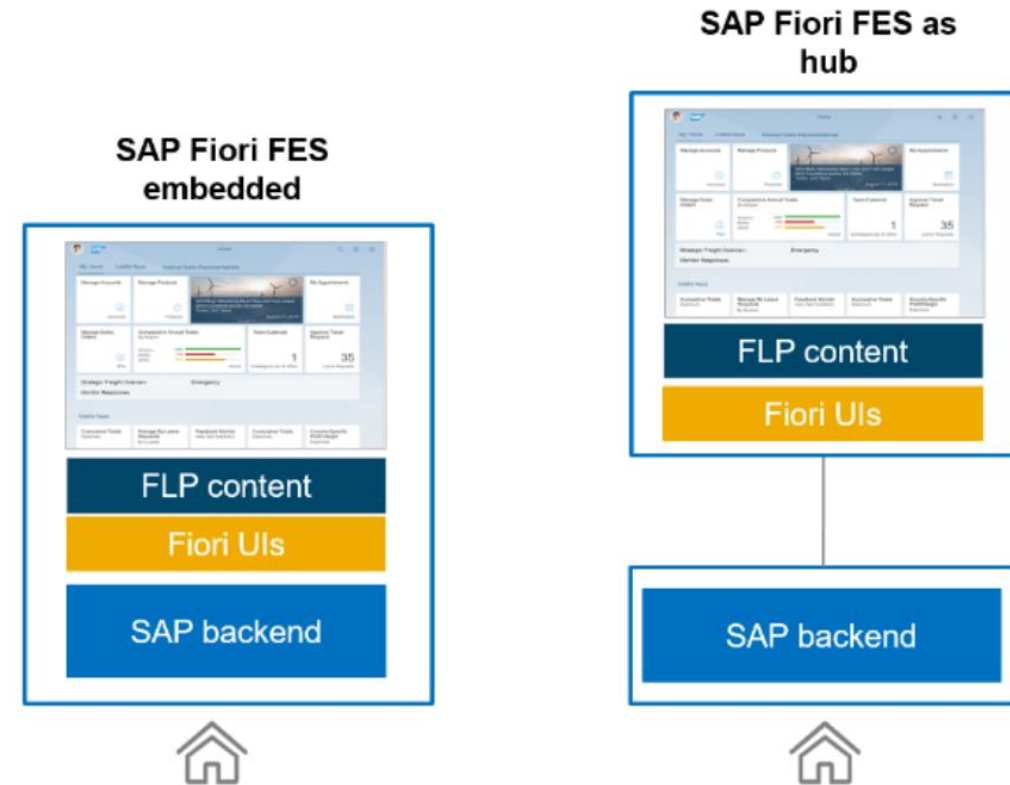
Filtered by: Product Suite (SAP S/4HANA) 	
All apps	>
by Line of Business	>
by Industry	>
by Roles	>
by Application Component	>
by Back-End Product	>
by Product Version	>
by SAP Best Practices	>

*Screenshot is the copyright of SAP AG.
Taken from the Fiori library.

Transactional	Analytical	Factsheet
Task based Access	Insights	Search & Explore
Access to tasks with guided navigation	Visual overview for KPI related analyses	View essential information about objects
Runs on Any DB, SAP HANA	Runs only on SAP HANA	Runs only on SAP HANA

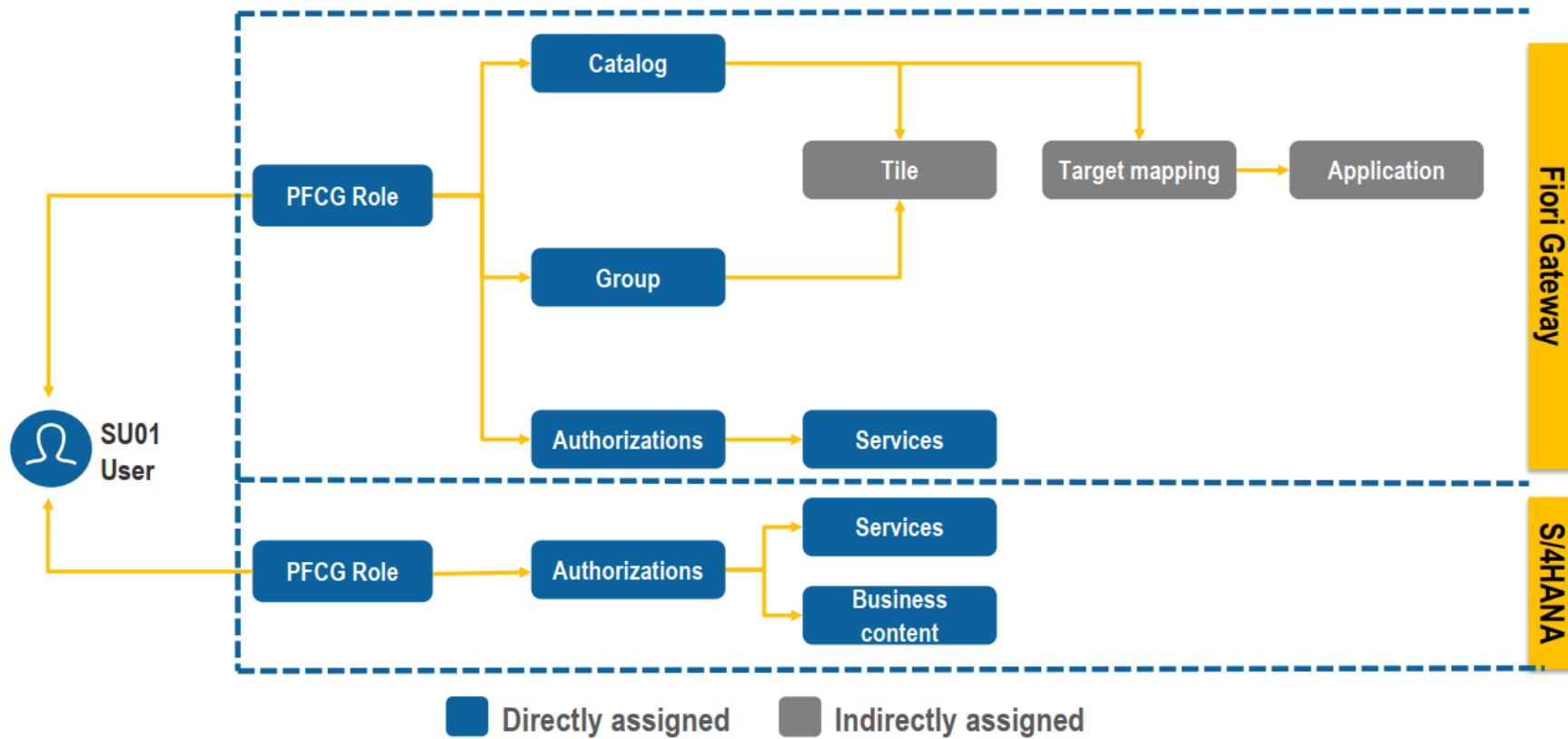
SAP Fiori Deployment Options

Initial recommendations for Fiori with Business Suite deployments was for a standalone front-end server (FES) deployment. With S/4 HANA an embedded deployment is recommended.



*Illustration is the copyright of SAP AG.

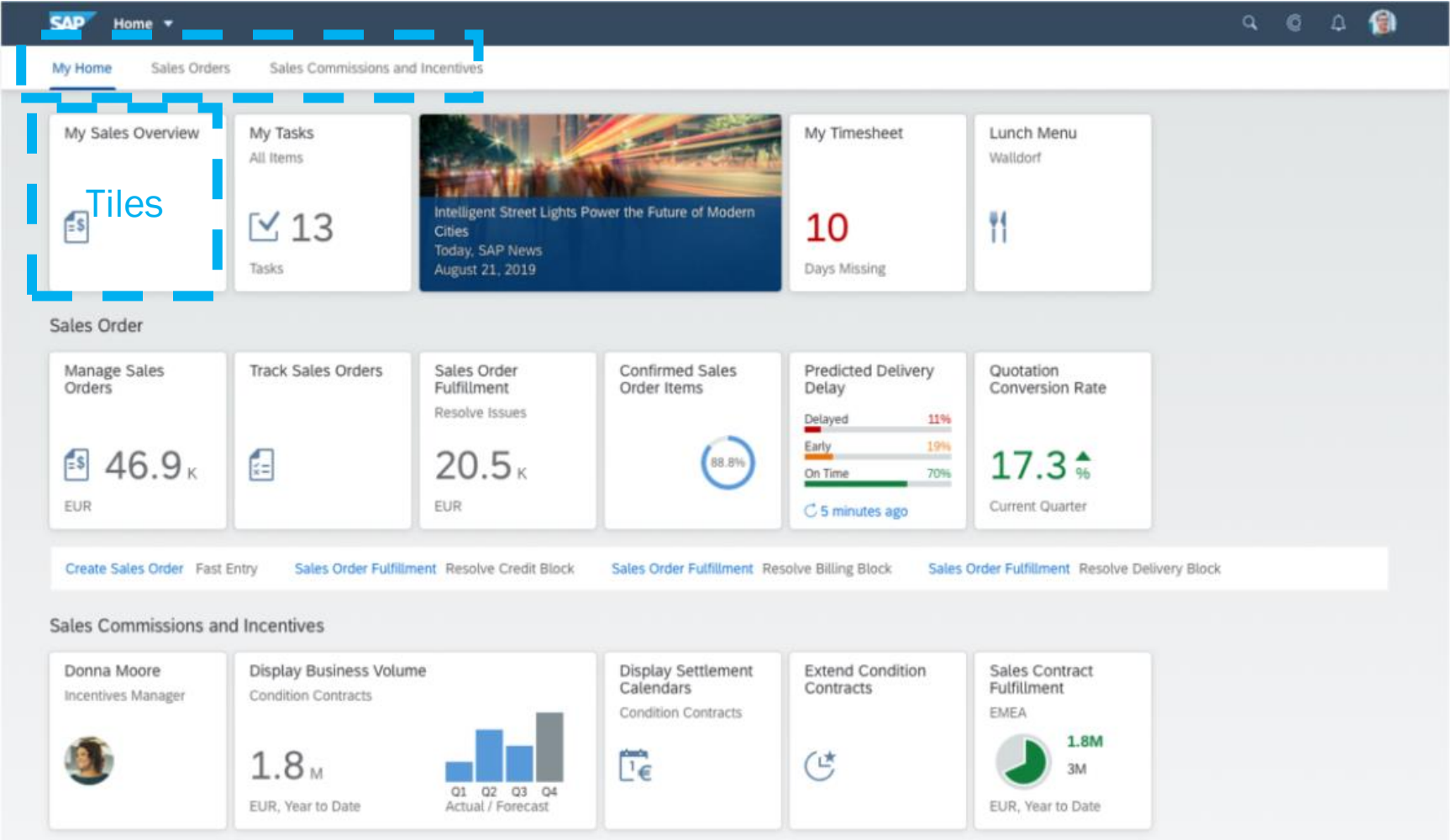
Fiori Authorization concept



*Illustration is the copyright of SAP AG.

Fiori Launch Pad

Fiori Groups



Review the Fiori Catalog

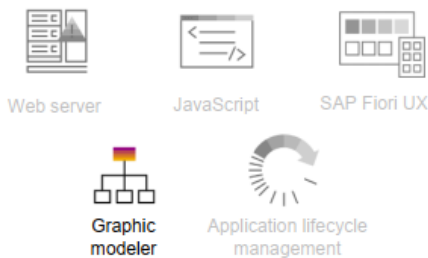
See how details in the Fiori catalog get carried over to the Fiori authorization concept

<https://fioriappslibrary.hana.ondemand.com/>

HANA Innovations

SAP HANA platform

Application development



Advanced analytical processing



Data integration and quality



Database management

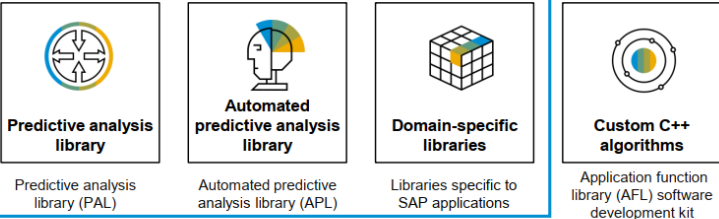


SAP HANA platform

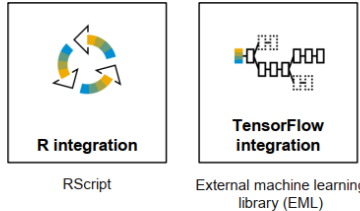
Enterprise edition

Runtime edition

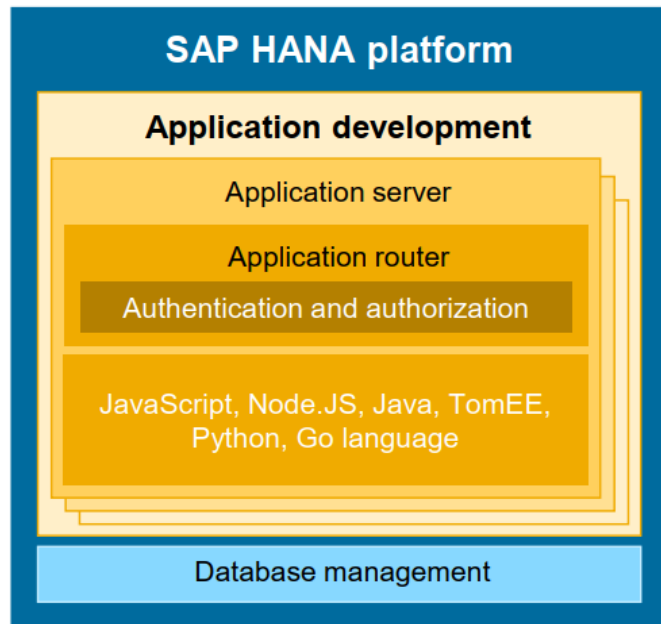
In-database capabilities



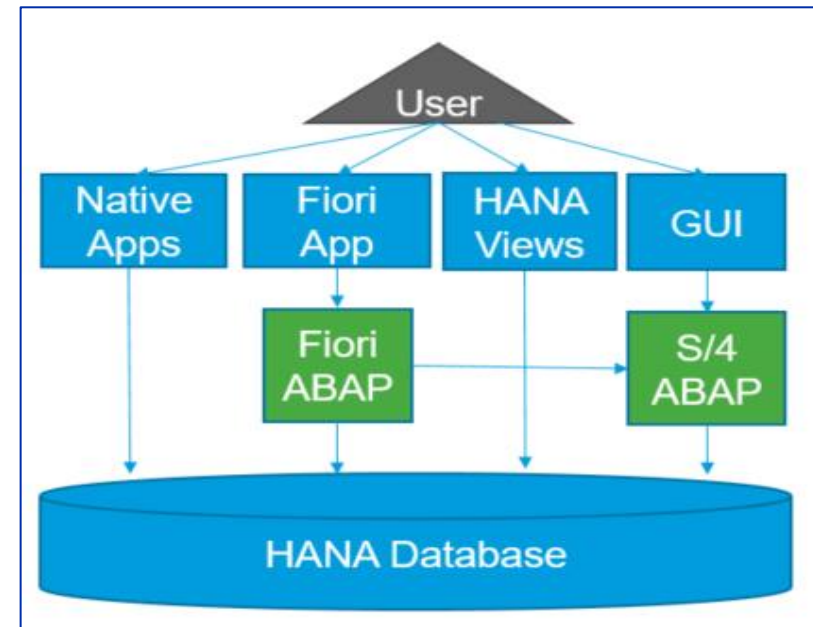
Database-level integration



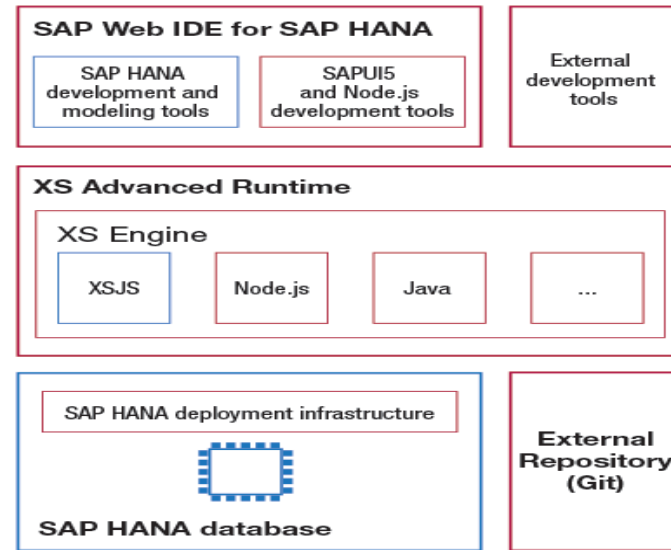
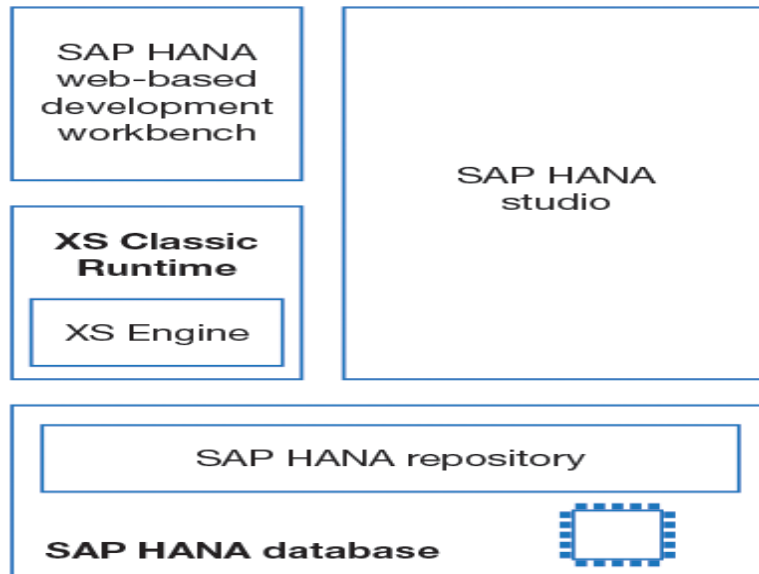
HANA Security Implications – Beyond a database



*Illustration is the copyright of SAP AG.



New development platform – Classic & Extended Application Services (XS)



*Illustration is the copyright of SAP AG.

HANA Potential User Interfaces, Administrative & Development Tools

Admin tools

- Native SAP HANA User Administration (SAP HANA Studio)
- SAP HANA Lifecycle Management Tool
- LDAP-Compliant Identity Management Server
- SAP Netweaver Identity Management
- SAP GRC Access Control
- Custom applications via SQL
- HANA Cockpit 2.0

Development Tools

- SAP HANA Studio (XS)
- SAP Web-based development Workbench (XS)
- SAP HANA Extended Application Services Advanced (XSA)

Potential User Interfaces

Fiori

- Native applications
- S/4, Business Suite, BW
- SAP Business Objects Explorer
- Microsoft Excel
- Other application via ODBC/JDBC

HANA Privileges

Privilege Types	Applicable To	Target Users
System Privileges	System, database <i>Administrative purposes, such as creating schemas, creating and changing users and roles, performing data backups, managing licenses, etc.</i>	Database administrators
Object Privileges	Specific database objects (schemas, tables, views, procedures, etc.) <i>Used to allow access to and modification of database objects such as tables, schemas, triggers, etc.</i>	Technical users
Analytical Privileges	Analytical views <i>Used to allow read access to data in SAP HANA information models (analytic views, attribute views and calculation views).</i>	Technical Users, End Users
Application Privileges	SAP HANA XS applications <i>Used to authorize access to SAP HANA Native XS Applications</i>	Application end users for custom developed applications.
Package Privileges (Deprecated)	Packages in the classic repository of the HANA database <i>Used to allow access to work in packages in the HANA database.</i>	Application and content developers (not recommended)

***Repository roles should be assigned to users rather than standard roles. If a standard role is used, when the grantor of the account is removed, it removes those privileges.

Continuous monitoring of ITGCs



The power of auditing ITGCs using SAP tables

See how audit issues can be quickly uncovered at the table level

Discuss high-value ITGC-related analytics

Advancing your continuous monitoring program

SAP Process Control 12.0 Master Guide 12.0 SP17 ▼

This document ▼



▼ Advanced Search



☆ Favorite Download PDF Share Next →

▼ Getting Started

About this Document

Planning Information

Further Useful Links

Related Documentation

Important SAP Notes

➤ SAP Process Control Overview

➤ Business Scenario of SAP Process Control

Getting Started

SAP Process Control 12.0 is an enterprise software solution for process control management. SAP Process Control is a customizable software solution that is delivered as an add-on and is based on SAP NetWeaver AS for ABAP 7.52.

SAP Process Control enables organizations to:

- Document their control environments
- Test and assess controls
- Track issues for remediation
- Certify and report on the state and quality of process controls
- Manage policies

Wrap Up



Where to Find More Information

https://www.sap-press.com/auditing-sap-s4hana_5526/

- SAP Press book on auditing SAP S/4HANA (largely also applicable to SAP ECC)

https://www.sap-press.com/authorizations-in-sap_2965/

- SAP Press book on both little-known and advanced security concepts

<https://support.sap.com/en/product/support-by-product/73554900100800000266.html>

- Documentation tab > Security Guide to access the SAP S/4HANA 2022 security guide

<https://launchpad.support.sap.com/#/notes/2253549>

- Link to SAP's security baseline template, including newest recommendations for security settings, about halfway down the page

Key Points to Take Home

- Your ITGC audit scope will depend on the audit objectives, which can vary widely
- SAP transaction codes are the **LEAST** reliable ways to audit security
- Auditing security in SAP S/4HANA, considering Fiori and the HANA DB, is significantly more challenging than in SAP ECC
- Many logging concerns are a myth (at least in 2022)
- Having access to browse SAP tables will make your audit much more efficient
- **There is not a great out-of-the-box audit role**
 - Starting with the Audit Information System roles (SAP_AUDITOR) can help, although it does require cleanup
 - Many of the IT audit functions in AIS are still relevant
- **You can step into continuous auditing now, and build the case for Process Control**

Thank you! Any Questions?

Steve Biskie

[Twitter.com/SteveBiskie](https://twitter.com/SteveBiskie)

[Linkedin.com/in/SteveBiskie](https://linkedin.com/in/SteveBiskie)

Please remember to complete
your session evaluation.



SAPinsider.org

PO Box 982Hampstead, NH 03841
Copyright © 2023 Wellesley Information Services.
All rights reserved.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies. Wellesley Information Services is neither owned nor controlled by SAP SE.

SAPinsider comprises the largest and fastest growing SAP membership group worldwide, with more than 600,000 members across 205 countries.
