



SAP HCM Authorisations: Little known tips and pitfalls

Today's situation

- Role amount is terribly increasing, because
 - Rather create new role for new requirement instead of checking existing authorisation
 - Functional range of SAP HCM applications increases
 - Functions are becoming decentralised – more users need different access
 - General authorisation is used for both: access to data and access to persons

Agenda

- **Little known tips for reduced role maintenance**
 - Structural authorisation
 - P_NNNNN
 - Reference role
- **Avoid these pitfalls**
 - P_PERNR
 - P_ABAP
 - Time dependent check - T582a
 - Adding rights from different roles, particularly backend and XSS
 - PLOG_CON
 - Non-integrated persons

Reduce role maintenance

- **Implement or enhance use of structural authorisation**
- Use object P_NNNNN
- Reference roles

Are you using 1 profile for each location?



	Authoriz. profile	Auth.profile name
	2001	London
	2002	Cambridge
	2003	Portsmouth
	2004	Birmingham
	2005	Liverpool
	2006	Bristol
	2007	Coventry
	2008	Leeds
	2009	Glasgow
	2010	Edinburgh

Responsible for 2 locations:

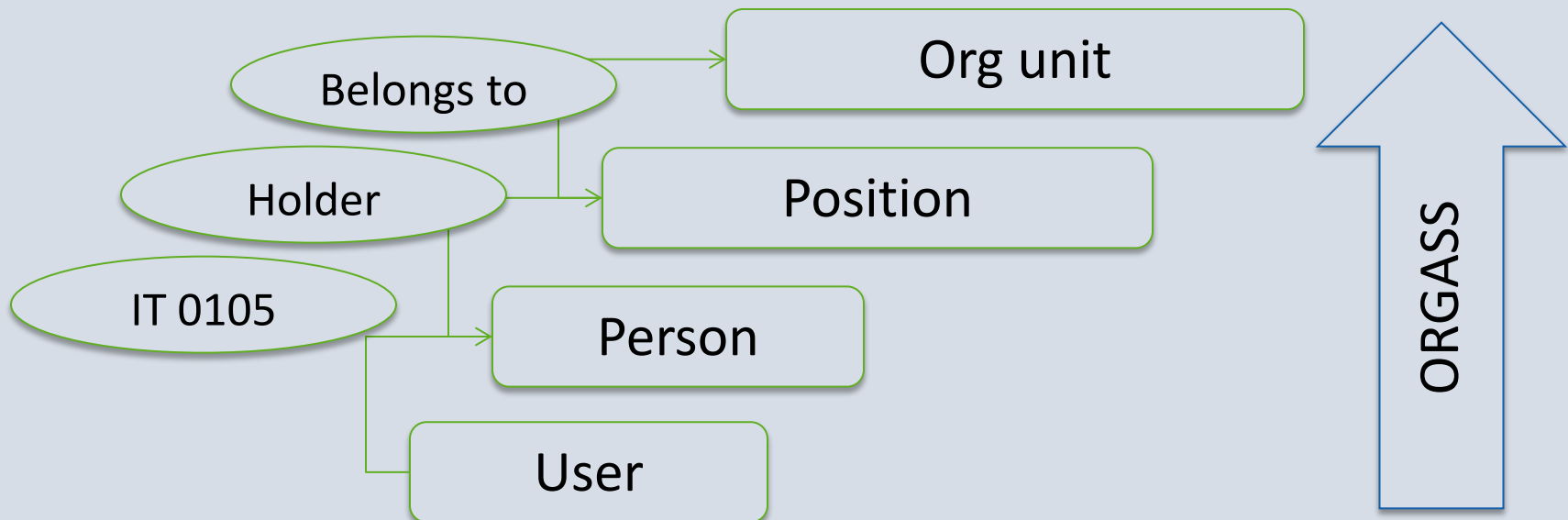
	User name	Auth.profile	Start date	End date	E
	IPROCON_AJ	2001	01.01.2012	31.12.9999	
	IPROCON_AJ	2002	01.01.2012	31.12.9999	

	Auth.profile	No.	Plan...	Ob...	Object I	Maint.	Eval.path	Statu...	Depth	Sign	Period
	2001	1	01	0	50000100	☐	0-0-S-P	1			D

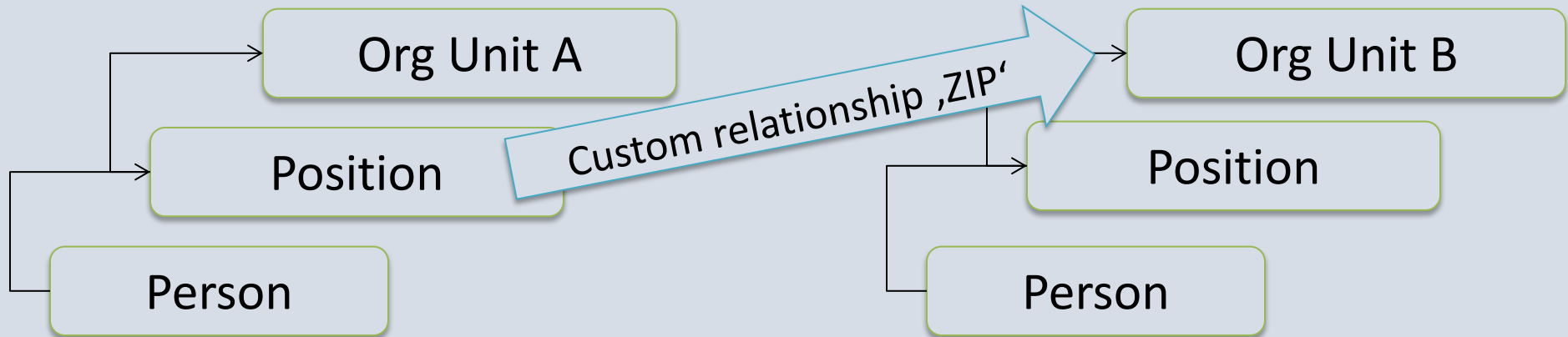
How to create dynamic profiles

Auth.profile	N..	Pla...	Obj....	Object I	Maint.	Eval.p...	S..	D..	P	Function module
2020	1	01	0		☐	0-0-S-P	12			RH_GET_ORG_ASSIGNMENT

Standard function module RH_GET_ORG_ASSIGNMENT dynamically identifies the assigned org unit.



Step 1: Create custom relationship



	OT	Object type text	A/B	Rel	Relationship name	RelObjType
	O	Organizational unit	B	ZIP	Is responsibility of	S
	S	Position	A	ZIP	Responsible for location	O

Step 2: Copy evaluation path ORGASS

Evaluation Path		ZORGASS	Determine organizational assignment				
	No.	Obj.Ty...	A/B	Relat'ship	Relationship name	Priority	Rel.obj.type
	1	P	B	008	Holder	*	S
	2	US	A	208	Is identical to	*	P
	3	S	A	ZIP	Responsible for location	*	O

Step 3: Copy function module

Function module: Z_RH_GET_ORG_ASSIGNMENT Inactive

Attributes Import Export Changing Tables Exceptions

```
22  
23 IF sy-subrc = 0.  
24   lv_wegid = 'ZORGASS'.  
25 ENDIF.  
26  
27 CALL FUNCTION 'RH_PBUILD_WORKFLOW'  
28   EXPORTING  
29     iv_evaluation_path = lv_wegid  
30   IMPORTING  
31     ev_mod_ev          = lv_wegid  
32     ev_is_internal     = lv_wegint.  
33  
34 CALL FUNCTION 'RH_STRUC_GET'  
35   EXPORTING  
36     act_otype          = 'US'  
37     act_objid          = uname
```



Tip for enhanced use

- If the access to persons can't be determined from org structure you can also develop a custom function module that may **identify all relevant persons** by
 - user parameter
 - master data (e.g. Time Administrator, Default Position)
 - customizing
 - ...
- In this case, evaluation path and start object remain empty.

Reduce role maintenance

- Enhanced use of structural authorisation
- **Use object P_NNNNN**
- Reference roles

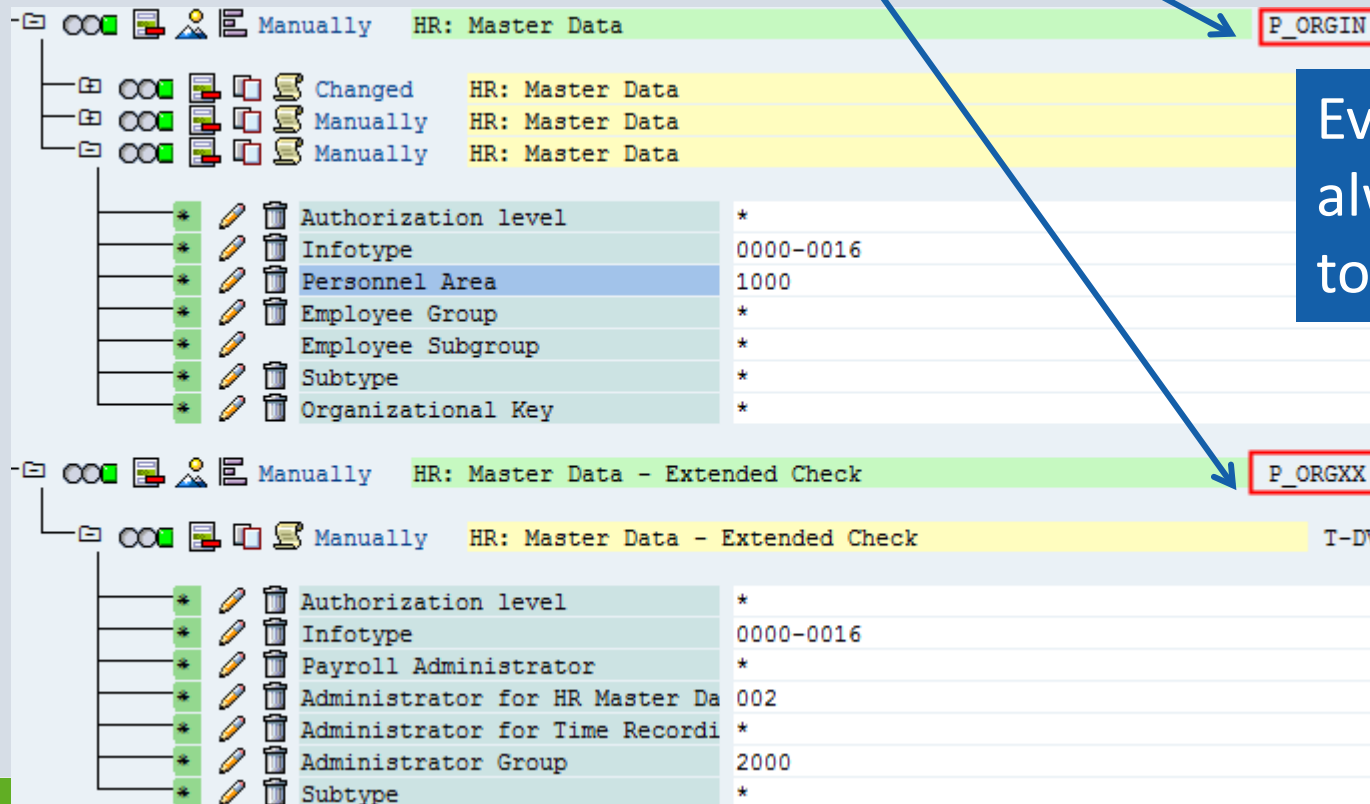


P_NNNNN

- Example: You need access to all persons of your own cost center.
- But: Cost center is missing in standard objects
- Organisational key leads to 1 role for each user.
- Instead: P_NNNNN with additional coding in generated Report -> 1 role for all users

Two HR objects for master data access

AUTSW	NNNN	0	HR: Customer-Specific Authorization Check
AUTSW	ORGIN	1	HR: Master Data
AUTSW	ORGP	1	HR: Structural Authorization Check
AUTSW	ORGXX	1	HR: Master Data - Extended Check
AUTSW	PERNR	1	HR: Master Data - Personnel Number Check



The screenshot displays the SAP HR Master Data configuration interface. It shows two main objects: 'HR: Master Data' and 'HR: Master Data - Extended Check'. Each object has a list of attributes with their respective values. The 'HR: Master Data' object includes attributes like Authorization level, Infotype, Personnel Area, Employee Group, Employee Subgroup, Subtype, and Organizational Key. The 'HR: Master Data - Extended Check' object includes attributes like Authorization level, Infotype, Payroll Administrator, Administrator for HR Master Data, Administrator for Time Recording, Administrator Group, and Subtype. Arrows from the table above point to the object names 'P_ORGIN' and 'P_ORGXX' in the interface.

Object	Attribute	Value
HR: Master Data (P_ORGIN)	Authorization level	*
	Infotype	0000-0016
	Personnel Area	1000
	Employee Group	*
	Employee Subgroup	*
	Subtype	*
	Organizational Key	*
HR: Master Data - Extended Check (P_ORGXX)	Authorization level	*
	Infotype	0000-0016
	Payroll Administrator	*
	Administrator for HR Master Data	002
	Administrator for Time Recording	*
	Administrator Group	2000
	Subtype	*

Every object always needs to be maintained.

Create ONE new object with necessary fields



Manually Z_HRSTAMM Z_HRSTAMM

Manually Z_HRSTAMM T-DV87

*			Authorization level	*
*			Personnel Subarea	*
*			Infotype	0000-0016
*			Cost Center	*
*			Personnel Area	1000
*			Employee Group	*
*			Payroll Administrator	*
*			Administrator for HR Master Da	002
*			Administrator for Time Recordi	*
*			Subtype	*

Unfortunately 10 fields, only.

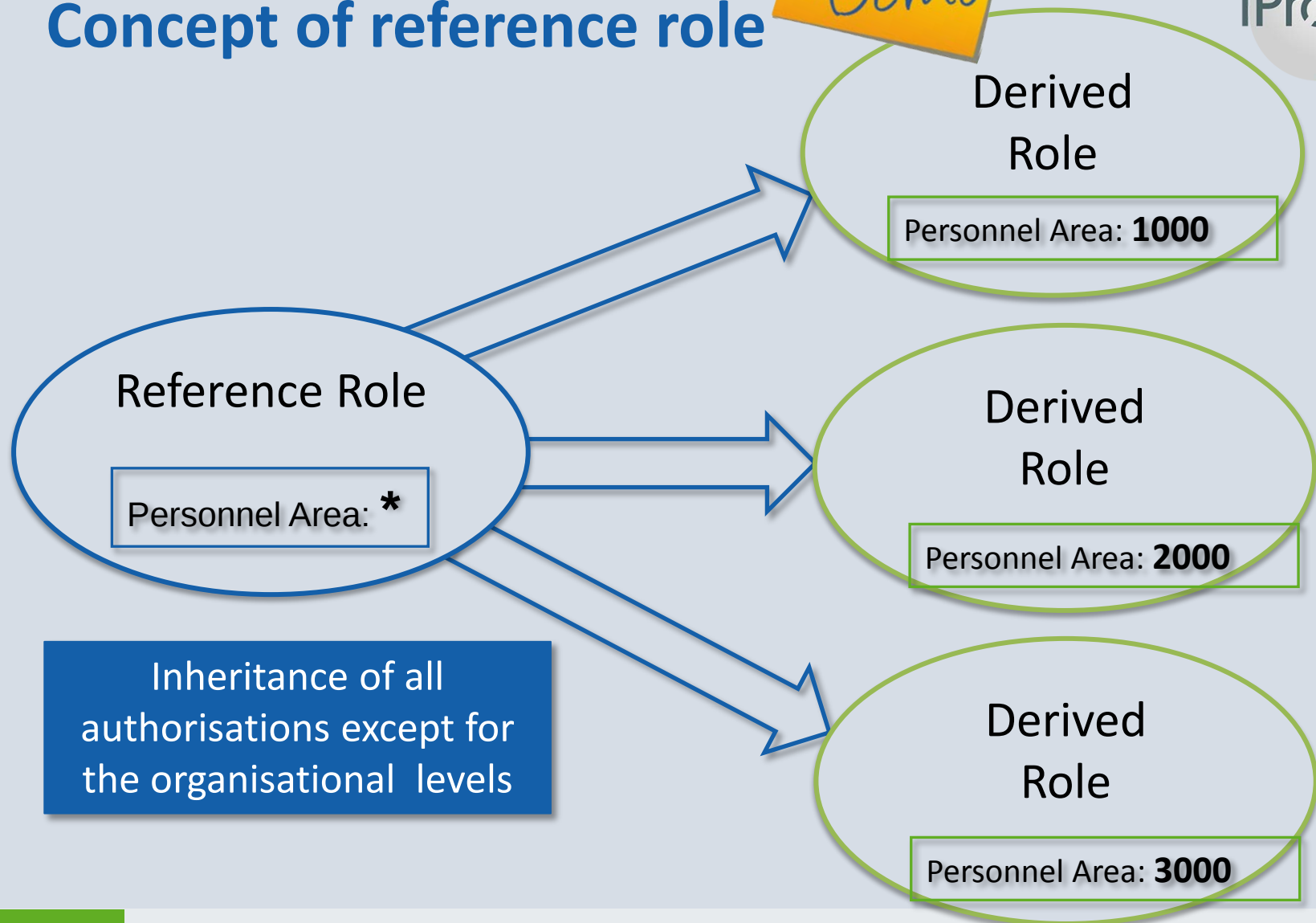
Reduce maintenance effort

- Enhanced use of structural authorisation
- Use object P_NNNNN
- **Reference roles**



Concept of reference role

Live-Demo



Agenda

- **Little known tips for reduced role maintenance**
 - Structural authorisation
 - P_NNNNN
 - Reference role
- **Avoid these pitfalls**
 - P_PERNR
 - P_ABAP
 - Time dependent check - T582a
 - Adding rights from different roles, particularly backend and XSS
 - PLOG_CON
 - Non-integrated persons

P_PERNR



Manually	HR: Master Data - Personnel Number Check	P_PERNR
Manually	HR: Master Data - Personnel Number Check	T-I655
	Authorization level	*
	Infotype	0006
	Interpretation of assigned per	*
	Subtype	*

Not like this!

Please note!

Basis is always ,normal' authorisation – P_PERNR is checked last

E: less rights for own personnel number (e.g. Change IT0008)

I: more rights for own personnel number (e.g. ESS)

P_ABAP



PFCG

SU53

Please note!

P_ABAP deactivates HR authorisation check for the report (if COARS = 2)

Never enter the Logical Database SAPDBPNP in the field REPID of P_ABAP

Display Authorization Data for User IPROCON_AM1

Description	Authorization values
▼ Date 17.04.2015 Time 11:38:15 Transaction S_AHR_61016369	
▼ Authorization Obj. P_ABAP HR: Reporting	
• Authorization Field COARS Degree of simplification for authorization check	2
• Authorization Field REPID ABAP Program Name	SAPDBPNP
▼ Date 17.04.2015 Time 11:38:15 Transaction S_AHR_61016369	

P_ABAP – Extra Tip

Manually	HR: Reporting	T-DV87003601	
* [edit] [delete]	Degree of simplification for a	1	COARS
* [edit] [delete]	ABAP Program Name	RPLMIT00, RPTEDT00	REPID
Manually	HR: Master Data	P_ORGIN	
Changed	HR: Stammdaten	T-DV87003601	
* [edit] [delete]	Authorization level	R	AUTHC
* [edit] [delete]	Infotype	*	INFTY
* [edit] [delete]	Personnel Area	NONE	PERSA
* [edit] [delete]	Employee Group	*	PERSG
* [edit] [delete]	Employee Subgroup	*	PERSK
* [edit] [delete]	Subtype	*	SUBTY
* [edit] [delete]	Organizational Key	*	VDSK1
Manually	HR: Master Data	T-DV87003600	
* [edit] [delete]	Authorization level	*	AUTHC
* [edit] [delete]	Infotype	ZZZZ	INFTY
* [edit] [delete]	Personnel Area	*	PERSA
* [edit] [delete]	Employee Group	*	PERSG
* [edit] [delete]	Employee Subgroup	*	PERSK
* [edit] [delete]	Subtype	*	SUBTY
* [edit] [delete]	Organizational Key	*	VDSK1



Time dependant check

Change View "Infotype attributes (Customizing)": Details

New Entries

Infotype: 0002 Personal Data

General attributes

Time constraint	1	☐ Subtype obligatory	☐ Accntng/log.data
Time cnstr.tab.		Subtype table	☐ Text allowed
Maint.aft.leave	☐	Subty.text tab.	☒ Copy infotype
☐ Access auth.		Subtype field	☒ Propose infotype

Display and selection

Select w/ start	3	Create w/o strt	1	Sort sequence	☐
-----------------	---	-----------------	---	---------------	--------------------------

Please note!

The date-dependent check is **not carried out for each infotype** by default. You can change the setting in table view V_T582A.



Rights from different roles adding up

- It is a common misconception that authorisations are only used together, when in the same role
 - E.g.: if one role allows to read infotype 0002 and a different role holds rights for transaction PA20, then the user cannot access infotype 0002 in PA20 → **WRONG!**
 - When a user wants to perform any action, authorisations from all roles assigned are applied
- Example: HR team leader
 - Role „HR Manager UK“ gives access to transaction PA30 and HR infotypes only for personnel areas in the UK
 - Role „Manager for MSS“ gives access to all HR infotypes without restrictions (assumption: MSS assigns right people only)
 - **Problem: combining both roles gives access to all HR data globally**

No context for org objects

PLOG-CON

A large, 3D-style red 'X' mark is superimposed over the text 'PLOG-CON', indicating that this object is deprecated or should not be used.

Definition

NOTE: Do NOT use this authorization object. It does not work.

This object is used by the authorization check for personnel planning data.

This authorization object comprises the same fields as object **PLOG** and has been enhanced with the new PROFL field (structural profile). The check for this object enables user-specific contexts to be represented in PD.

Non-integrated and context auth.

Note:

Only users with profile ALL always see all Non-integrated.

AUTSW	DFCON	3	HR: Default Position (Context)
AUTSW	INCON	0	HR: Master Data (Context)
AUTSW	NNCON	0	HR: Customer-Specific Authorization
AUTSW	NNNNN	0	HR: Customer-Specific Authorization
AUTSW	ORGIN	1	HR: Master Data
AUTSW	ORGPD	3	HR: Structural Authorization Check

Tip:

Grant infotype access for non-integrated via structural profile \$\$\$\$\$\$.

Organizational plan

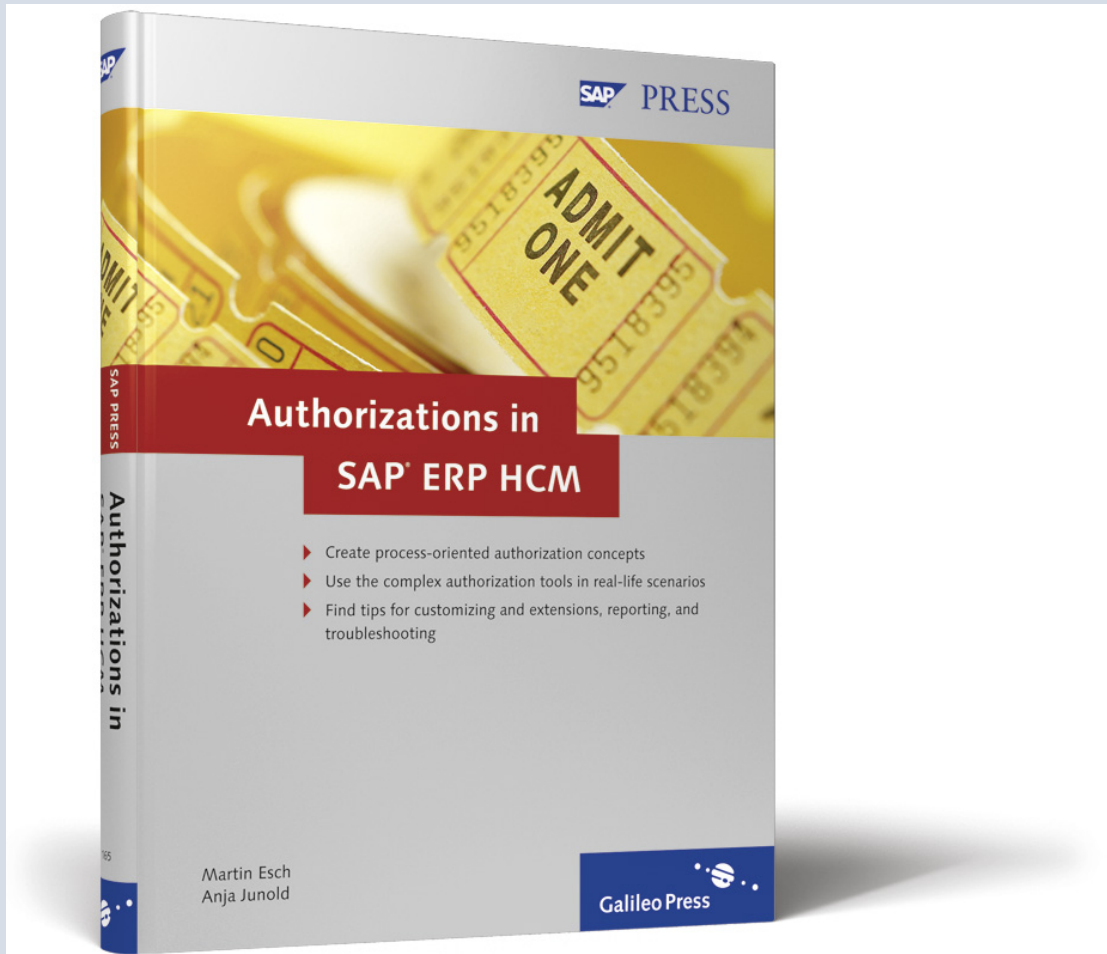
Position	99999999
Job key	50000041
Org. Unit	50000034 Private International ...
Org.key	100000000003000

Recommendation:

Evaluate organizational unit /
Grant authorization as default

Manually	HR: Master Data with Context
Authorization level	*
Infotype	0000-0016
Personnel Area	*
Employee Group	*
Employee Subgroup	*
Authorization Profile	\$\$\$\$\$\$
Subtype	*
Organizational Key	*

Book recommendation



Questions?!

