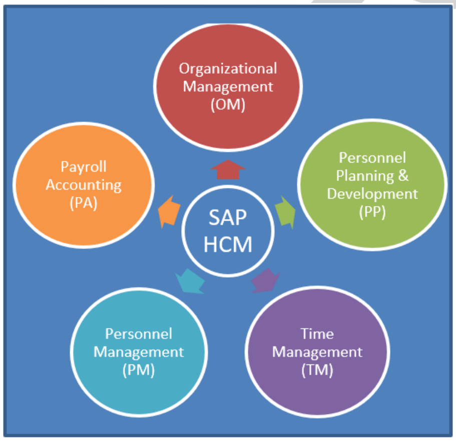
Authorizations in SAP ERP HCM

The area of personnel management is well suited for dealing with authorizations, because the Human Resources (HR) department has a highly distinct perception of authorizations. From the data protection point of view, the data saved here is particularly critical, because it concerns the employee´s privacy, which must be protected at all costs.

SAP HCM (Human Capital Management) System separate the information in five different sub-modules:


Organizational Management (OM)
Payroll Accounting (PA)
Personnel Planning & Development (PP)
SAP HCM
Personnel Management (PM)
Time Management (TM)

When we talk about authorizations, as in the rest of SAP systems, the key is the Segregation of Duties. SAP GRC offers a standard risk matrix with 21 segregation of duties risks (SoD) specific to the HCM module. If you want to know more details about SoD Risk Matrix for SAP GRC, we recommend reading our related article (Segregation of Duties: Risk Matrix for SAP GRC).

In order to have the minimum risks of SoD in our HCM system it will be important that we analyze the two main ways to set up authorizations HCM system:

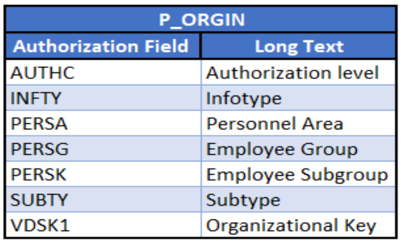
- General authorizations
- HR specific structural authorizations

General authorizations:

In this section we will define as based on the same authorization methodology as for the ECC systems in SAP. This option is based in Authorization Objects which defined the authorization fields to be checked during the transaction execution. You can use the Role Maintenance transaction (PFCG) to create authorization profiles and assign it to the users. These profiles can be made up of transactions through the "menu" tab and/or by authorizations objects through the "authorizations" tab.

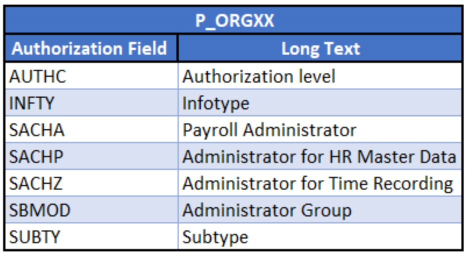
Now we will list the most important objects in the HCM system to perform an appropriate restriction of authorizations:

P_ORGIN: HR Master Data, that is used to provides the user with the necessary authorizations to access the specific personnel data they need:



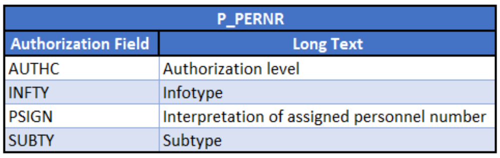
P_ORGIN	
Authorization Field	**Long Text**
AUTHC	Authorization level
INFTY	Infotype
PERSA	Personnel Area
PERSG	Employee Group
PERSK	Employee Subgroup
SUBTY	Subtype
VDSK1	Organizational Key

P_ORGXX: HR Extended Check, that is used to check authorization for personal data (HR infotypes):



P_ORGXX	
Authorization Field	**Long Text**
AUTHC	Authorization level
INFTY	Infotype
SACHA	Payroll Administrator
SACHP	Administrator for HR Master Data
SACHZ	Administrator for Time Recording
SBMOD	Administrator Group
SUBTY	Subtype

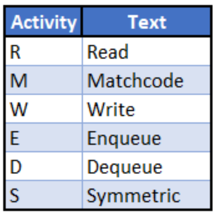
P_PERNR: HR Personnel Number Check, that is used to assign users different authorizations for accessing their own personnel number:



P_PERNR	
Authorization Field	Long Text
AUTHC	Authorization level
INFTY	Infotype
PSIGN	Interpretation of assigned personnel number
SUBTY	Subtype

As you can see, these three objects have two fields in common:

- **INFTY** which is a unique term to the SAP HCM module to group related data fields used to store employee data.
- **AUTH** through which you can restrict access to:



Activity	Text
R	Read
M	Matchcode
W	Write
E	Enqueue
D	Dequeue
S	Symmetric

If you want to check additional fields of Infotype, for example, cost center or personnel subarea, you can use the **P_NNNNN** authorization object. This object should be created by yourself and equip it with all fields of Infotype and customer specific additional fields.

Regarding with tables it is important to remark the authorization object **S_TABU_LIN** (Authorization for Organizational Unit). This object complements the authorization objects S_TABU_NAM, S_TABU_DIS and S_TABU_CLI. As you know, S_TABU_NAM works at the level of restrict access to viewing or modifying a specific system table. But the S_TABU_LIN controls access to individual table rows. Therefore, the existence of organizational criteria is a prerequisite for the use of this authorization object.

The HCM tables functionality can be identified by the following suffixes:

- PA*- PA Infotype Tables
- PCL* - HR Clusters
- PB* - Recruitment Tables

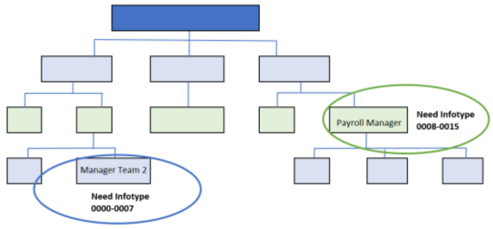
Furthermore, it is important to indicate that when we decided to restrict HCM authorization role model through "general authorizations" it is recommendable to combine a master-derived role model with Enabler Roles. These roles only have authorization objects, not transactions. This will make the model management more efficient.

The Enabler Roles are necessary since the fields that we want to restrict the authorizations (as we have seen in the previous objects like Infotype and Personnel Area) are not consider organizational value so you will need to have in one hand the roles with the transactions and objects derived by the corresponding organizational values (company code, plant, sales order ... ..) and in the other hand, enabler roles with only the specifics HCM objects that give you specific access to the different Infotype and Personnel area.

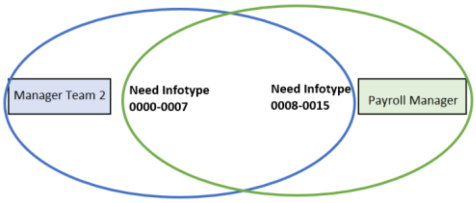
Structural Authorizations:

In addition to the general authorization check, which are based on authorization objects, you can define additional authorizations by hierarchical structures.

The technical separation of general and structural authorizations profiles can cause context problems for users who perform different roles in a company. For example, if the same person performs the Payroll Manager activity for which you need access to some infotypes and is the manager of a team that should be allowed to other different infotypes:



The result of giving this person the authorizations he requires for the two positions through the model explained in the previous section (General authorizations) will mean that the user will have additional access to Manager Team 2 in Infotypes 0008-0015 and Payroll Manager the Infotypes 0000-0007 by combination of authorizations:



This can be avoided separating the general and structural authorizations concepts.

It is important to highlight that to enable the use of structural profiles it is a prerequisite to activate the ORGPD check through the **OOAC** transaction.

Structural profiles are assigned in a different way to general authorization profiles (PFCG Transaction). To assign structural profiles, you use a specific transaction called Authorization Profiles (**OOSP**). Through this transaction profiles are initially created independently of the users and then assigned to them by User Authorizations Transaction (**OOSB**) instead of SU01 as general authorizations.

In relation to the SAP Tables, this information related with structural profiles authorizations can be found in the following tables:

- **T77PR** - Definition of Authorization Profiles Data
- **T77UA** - Assignment of Profiles to Users

On the other hand, the following tables allow you to restrict access to tables through organizational rules:

- **ORGCRIT** - Store Organization criteria data
- **V_ORGCRACT –** Organizational Criteria Activation

Key Points to Take Home:

- HCM system is having employee´s privacy information which must be protected.
- Restricting authorizations in an HCM system should be handled differently than in an SAP ECC system.
- Each company should evaluate its situation and know in which cases the general or structural authorization model should be used.