Preface

„Few are those who see with their own eyes and feel with their own hearts.”

Albert Einstein

Special thanks to my love Dirk,
who again has created this beautiful cover for me.

This little book shall help you to understand the various elements of SAP® security and their interaction. Hope you enjoy reading it as much as I have enjoyed writing it. I am planning to add more chapters over time, so I decided to go with the e-book version.

If you have any questions, I would be more than happy to answer them.
Please feel free to send me a mail:

info@mariewagener.de
No part of this publication may be reproduced, stored in retrieval systems or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise without prior written permission of the author.

SAP® and SAP R/3® are registered trademarks of the SAP® AG.

Disclaimer of warranty:
While the author has used her best efforts in preparing this book, she makes no representations or warranties with respect to accuracy or completeness of the content of this book. The book may include technical or other inaccuracies or typographical errors. The author will not be liable for any loss or profit or any other commercial damages, including but not limited to special, incidental, consequential or other damages.
1 Introduction to the general authorization concept of SAP® ....................... 6
  1.1 Requirements to an authorization concept......................................................... 6
  1.2 Functional structure............................................................................................ 7
2 Detail view: Components of the authorization concept............................. 10
  2.1 Authorization objects........................................................................................ 11
     2.1.1 Structure................................................................................................... 11
     2.1.2 Overview of authorization objects ............................................................ 13
  2.2 Authorizations .................................................................................................. 24
     2.2.1 Structure................................................................................................... 24
     2.2.2 Overview of authorizations....................................................................... 25
  2.3 Profiles ............................................................................................................. 32
     2.3.1 Structure................................................................................................... 32
  2.4 Overview of profiles.......................................................................................... 34
     2.4.1 Overview of composite profiles ................................................................ 39
  2.5 Roles ................................................................................................................ 40
     2.5.1 Structure................................................................................................... 40
     2.5.2 Overview of roles – the PFCG.................................................................. 40
     2.5.3 Additional interfaces of the PFCG ............................................................ 47
     2.5.4 Master - Derivation ................................................................................... 52
     2.5.5 Overview of composite roles .................................................................... 54
     2.5.6 Tables with role information ..................................................................... 55
  2.6 User.................................................................................................................. 59
     2.6.1 User master record................................................................................... 59
     2.6.2 The reference users ................................................................................. 67
     2.6.3 Basic user evaluations ............................................................................. 68
     2.6.4 System measurement data ...................................................................... 70
3 Basic mode of operations............................................................................. 75
  3.1 General relation transaction and authorization object................................. 75
  3.2 The authorization check for dialog users ......................................................... 84
  3.3 The matching authorization......................................................................... 88
4 Evaluation tools ................................................................. 94
4.1 Report RSUSR002................................................................. 94
4.2 Report RSUSR003................................................................. 98
4.3 Report RSUSR008 [transaction S_BCE_68001401] ................. 99
4.4 Report RSUSR009 [transaction S_BCE_68001403] .................. 100
4.5 Report RSUSR008_009_NEW ............................................... 101
4.6 Report RSUSR010................................................................. 103
4.7 Report RSUSR020 [transaction S_BCE_68001409] .................. 104
4.8 Report RSUSR030................................................................. 105
4.9 Report RSUSR040................................................................. 106
4.10 Report RSUSR050 [transaction S_BCE_68001433] .................. 107
4.11 Report RSUSR060OBJ.......................................................... 108
4.12 Report RSUSR070 [transaction S_BCE_68001425] .................. 110
4.13 Change documents ............................................................ 111
  4.13.1 Report RSUSR100.......................................................... 111
  4.13.2 Report RSUSR101.......................................................... 112
  4.13.3 Report RSUSR102.......................................................... 113
  4.13.4 Report RSSCD100_PFCG ............................................... 114
  4.13.5 SUIM – The User Information System.............................. 115
5 How to .................................................................................. 116
5.1 How to adapt authority-check in reports .................................. 116
5.2 How to add an authorization object to a customer created transaction code 119
5.3 Table access – table protection .............................................. 123
5.4 Protection of reports / ABAP®s ............................................. 127
5.5 Export of tables for an authorization check .............................. 134
5.6 The SAP® system trace ...................................................... 136
5.7 Transaction SE16N – risk and control .................................... 144
5.8 Transaction SE16 –risk and control ....................................... 148
5.9 SAP® NetWeaver security parameter ................................. 152
5.10 The evaluation of the SysLog – SM21 .................................... 158
5.11 Segregation of duties in the financial accounting (Asymmetric approach) .... 162
5.12 Table of content for the documentation of an authorization concept .... 166
5.13 Selected relevant Security tables ........................................... 170
1 Introduction to the general authorization concept of SAP®

1.1 Requirements to an authorization concept

A good authorization concept should have the following characteristics:

- **Reliability**
  
  The range of authorization has to correspond with the operational responsibility of the user.

- **Security**
  
  It has to be guaranteed, that no unauthorized users have access to sensitive data or programs.

- **Testability**
  
  The concept has to be comprehensible and transparent as well for internal as also external auditors.

- **Flexibility**
  
  It should be easily adaptable, if for example organizational changes occur or new modules have to be integrated.

- **Comprehensibility**
  
  It should be easily comprehensible for all those involved, as for example according to name conventions for users, authorizations and profiles.
1.2 Functional structure

The authorization concept of SAP® represents the fundamental security function of the system. All relevant security functions are controlled via the authorization concept, as for example the adjustments of system modifications or the segregation of duties within the modules. The main principle, on which the authorization concept is set up, is the protection of individual fields. Every user works with screens that again consist of several fields.

It should not be possible for every user to have unrestricted access to all fields including all potential values. The users should only get access to the individual fields in a way that this complies with a work related need. This way, the fields are protected from unauthorized accesses.

With regard to this, authorization objects were created in the SAP® system that again were laid over the individual fields the same as a mask. This mask can exist of up to ten fields. In this mask, the options that will be assigned to the user are maintained. In Release ECC 6 2.580, 4.7 there are about 1033, in 4.6C 947, in 4.6B 891 and in 4.0B 711 predefined authorization objects.

Analysis of an authorization object:

<table>
<thead>
<tr>
<th>Authorization object</th>
<th>Authorization field</th>
<th>Authorization value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F_KNA1_BUK</td>
<td>ACTVT</td>
<td>03</td>
<td>Determination Activity in which company code dependent part of the master data, the activity defined ahead, may be executed.</td>
</tr>
<tr>
<td></td>
<td>BUKRS</td>
<td>$BUKRS</td>
<td></td>
</tr>
</tbody>
</table>

In the above example an authorization object is listed that controls the access to the company code data of the general customer master data. This authorization object consists of two fields. First, the field ACTVT, in which is determined which activities may be executed. In this example 03, a display authorization is established. The second field BUKRS, enables that the access is only provided to
selected company codes with the assigned activity. The company codes can be explicitly entered to this field, for example 0001.

Are the just named values assigned to the authorization object, then the field company code can only be brought to display for the company code 0001.

With the assignment of values to the participating fields in this authorization object, an authorization to this object is created.

SAP® works transaction controlled. That means that basically every application within SAP® is represented by a transaction.

To every authorization object an unlimited number of authorizations can be created, resulting from the diverse combination possibilities of the field values with one another.

An authorization cannot be assigned directly to a user instead authorizations are collected in a profile. The profiles, in which authorizations are collected, are also called single profiles. Starting with the profile level, an assignment to users can succeed. SAP® allows furthermore that profiles may be combined in composite profiles. In composite profiles, no authorizations are combined, only other profiles. The most popular composite profile is the SAP_ALL profile, which contains (just about) all authorizations of the SAP®-System. The profile SAP_ALL contains no authorizations, but other profiles. In a profile, either authorizations or profiles can be entered, but a combination of both is not possible.

These composite profiles can also be nested in other composite profiles. Concerning the nesting depth on the composite profile level there are no limitations other than related to the database structure [300 profile entries per composite profile]. Composite profiles are assigned to users just like single profiles. The user then receives all authorizations that are contained in the profiles of the composite profiles.

With the integration of the profile generator into SAP®, profiles are created with the help of this tool. The profile generator creates roles. A role is similar to a container for one or more profiles that are generated and contain the defined authorizations. Roles may be combined as composite roles. The nesting depth is limited to one level only.

Roles as well as composite roles may be assigned to users.
Graphic display of the previous explanation:

Exhibit 1.1: The elements of the authorization concept
2 Detail view: Components of the authorization concept

The decisive components of the authorization concept are therefore:

- **Authorization objects**

  For objects that are to be protected, as applications within SAP®, there are authorization objects created in the ABAP/4® Workbench. These objects contain fields that are meaningful to protect, and that can be restricted within the authorizations, that are created based on the respective authorization objects. All the relevant elements are already equipped from SAP® with authorization objects per default. Additional authorization objects should only be created for company specific developments.

- **Authorizations**

  An arbitrary number of authorizations can be created based on every already existing authorization object. They are the actual carriers of the access key. Here also, authorizations are delivered by SAP® per default that is not limited on any organizational level.

- **Profiles**

  SAP® delivers standard profiles for all typical tasks within the SAP® environment. Single and composite profiles will be distinguished; the last-named contain again further single or composite profiles. Included in the profiles are the necessary authorizations for the individual conceptual task.

- **Activity groups / Roles**

  An activity group represents a collection of activities that describe a certain working area. It contains transactions as well as reports and can be extended through the creation of a user menu. A role is a release dependent synonym for an activity group. Activity groups can be combined in composite activity groups, roles in composite roles. Further nesting depths do not exist.
User master data

User master records have to be created and managed individually in every client, provided with authorization profiles or transported from the test client into the production client via CTS (Change and Transport management System). No users exist per default, other than some SAP® standard users like for example SAP* and DDIC.

2.1 Authorization objects

2.1.1 Structure

An authorization object is the central control element; it consists of up to 10 fields, (mostly two).

Authorization objects are sorted according to object classes. The authorization objects that are delivered per default can be identified by an underline on the second place of the technical name (for instance: F_BKPF_BED Accounting document: authorization for customers).

The result of this is that at a release change the authorization object is recognized as standard. Individual company authorization objects may not have an underline on the second place, so they will not be overwritten.

Any number of authorizations can be created based on authorization objects, so even several authorizations can have the same name, as long as they are created based on different authorization objects.

The naming convention of SAP® for the authorization elements serves for the sorting in the respective modules. A letter is set on the first place that refers to the module:

A  Assets Accounting
C  Classification System
E  Consolidation
In the second place an underline is located, for example F_KNA1_BUK.

Each of these authorization objects consists of several fields (one to ten) and the possible values for these fields. The assignment of an authorization object to an action procedure (transaction, posting, report,...) is predefined by SAP® per default. Resulting from the assignment of corresponding values to these fields, an authorization is created out of an authorization object.

Only for special company interfaces the creation of company specific authorization objects will be necessary. In this case, the SAP® naming conventions have to be followed; company specific objects should always start with “Y” or “Z”.

Important:

Never delete a standard authorization object!
2.1.2 Overview of authorization objects

An overview of the existing authorization objects can be received in two ways.

Call up the transaction **SU03**.

Exhibit 2.1: Authorization object classes

You directly reach the above displayed list. In this overview the authorization objects are sorted according to classes. With a double-click you come directly into the affiliated detail display:
Exhibit 2.2: Objects of the class FI

Mark a selected authorization object and press the button Display fields. In the opening dialog box, the fields of the corresponding authorization objects are listed.

Exhibit 2.3: Overview of authorization object
Mark an entry and press the button , an explanation to this object will be displayed. Additionally, you will receive information about the fields and their possible values:

**Definition**

Using this authorization object, you determine in which company codes documents can be processed. An employee can only call up the functions for posting if he/she has this authorization in at least one company code.

**Defined fields**

The object consists of the "Company code" and "Activity" fields. You take the possible input values for the "Activity" field from table TACTZ.

*Exhibit 2.4: Documentation of an authorization object*
Transaction SU21

The transaction SU21 provides a similar editing structure as the transaction SU03.

Overview of object classes:

<table>
<thead>
<tr>
<th>Class/Object</th>
<th>Text</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Not assigned to a class</td>
<td>Object...</td>
</tr>
<tr>
<td>AAAA</td>
<td>Obsolete Authorization Objects</td>
<td>Object...</td>
</tr>
<tr>
<td>AAB</td>
<td>Cross-application Authorization Objects</td>
<td>Object...</td>
</tr>
<tr>
<td>ACO</td>
<td>PLM ACOs</td>
<td>Object...</td>
</tr>
<tr>
<td>AM</td>
<td>Asset Accounting</td>
<td>Object...</td>
</tr>
<tr>
<td>BC_A</td>
<td>Basis: Administration</td>
<td>Object...</td>
</tr>
<tr>
<td>BC_C</td>
<td>Basis - Development Environment</td>
<td>Object...</td>
</tr>
<tr>
<td>BC_Z</td>
<td>Basis - Central Functions</td>
<td>Object...</td>
</tr>
<tr>
<td>BPCT</td>
<td>Partner Contact Management</td>
<td>Object...</td>
</tr>
<tr>
<td>BRF</td>
<td>BRF: Business Rule Framework</td>
<td>Object...</td>
</tr>
<tr>
<td>BVCH</td>
<td>Contract Handling</td>
<td>Object...</td>
</tr>
<tr>
<td>BVED</td>
<td>Excise Duty</td>
<td>Object...</td>
</tr>
<tr>
<td>BVM</td>
<td>Empties Management</td>
<td>Object...</td>
</tr>
<tr>
<td>BVSR</td>
<td>Sales Returns</td>
<td>Object...</td>
</tr>
<tr>
<td>BVTS</td>
<td>Beverage: Part Load Lift Orders</td>
<td>Object...</td>
</tr>
<tr>
<td>CACS</td>
<td>Commission System</td>
<td>Object...</td>
</tr>
<tr>
<td>CLAS</td>
<td>Classification</td>
<td>Object...</td>
</tr>
<tr>
<td>CM</td>
<td>Campus Management</td>
<td>Object...</td>
</tr>
<tr>
<td>CMSA</td>
<td>Collateral Management System</td>
<td>Object...</td>
</tr>
<tr>
<td>CMX</td>
<td>Manufacturing Execution: Authorization Objects</td>
<td>Object...</td>
</tr>
<tr>
<td>CO</td>
<td>Controlling</td>
<td>Object...</td>
</tr>
<tr>
<td>COND</td>
<td>Conditions</td>
<td>Object...</td>
</tr>
<tr>
<td>CSEA</td>
<td>Commissions: Application</td>
<td>Object...</td>
</tr>
<tr>
<td>CSEO</td>
<td>Commissions: Customizing and Generation</td>
<td>Object...</td>
</tr>
<tr>
<td>CV</td>
<td>Document Management</td>
<td>Object...</td>
</tr>
<tr>
<td>CVF</td>
<td>Customer/Vendor Integration</td>
<td>Object...</td>
</tr>
<tr>
<td>DFPS</td>
<td>Defence Forces &amp; Public Security</td>
<td>Object...</td>
</tr>
<tr>
<td>DSD</td>
<td>Direct Store Delivery</td>
<td>Object...</td>
</tr>
<tr>
<td>DSDM</td>
<td>DSD Connector</td>
<td>Object...</td>
</tr>
</tbody>
</table>

Exhibit 2.5: Overview of object classes
Open the folder for the object class where you want to review the objects.

Double click onto a selected entry to branch to the corresponding object details.

Exhibit 2.6: Overview of authorization objects

Exhibit 2.7: Detail view of authorization object
By push of the button [Display object documentation], you will get the detail documentation displayed:

Definition

Using this authorization object, you determine in which company codes documents can be processed. An employee can only call up the functions for posting if he/she has this authorization in at least one company code.

Defined fields

The object consists of the "Company code" and "Activity" fields. You take the possible input values for the "Activity" field from table TACTZ.

Exhibit 2.8: Documentation of authorization object

By pushing the button [Permitted activities], you get an overview of all permitted activities:

Exhibit 2.9: Activities per authorization object
A list of all available activities can be received from the table **TACT** through the transaction **SE16N**.

It is recommended to have this list on hand for a better understanding throughout an audit.

---

**Display of Entries Found**

<table>
<thead>
<tr>
<th>Activity</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Create or generate</td>
</tr>
<tr>
<td>02</td>
<td>Change</td>
</tr>
<tr>
<td>03</td>
<td>Display</td>
</tr>
<tr>
<td>04</td>
<td>Print, edit messages</td>
</tr>
<tr>
<td>05</td>
<td>Lock</td>
</tr>
<tr>
<td>06</td>
<td>Delete</td>
</tr>
<tr>
<td>07</td>
<td>Activate, generate</td>
</tr>
<tr>
<td>08</td>
<td>Display change documents</td>
</tr>
<tr>
<td>09</td>
<td>Display prices</td>
</tr>
<tr>
<td>10</td>
<td>Post</td>
</tr>
<tr>
<td>11</td>
<td>Change number range status</td>
</tr>
</tbody>
</table>

*Exhibit 2.10: Overview of activities*

Another possible display can be reached by the **Where-used-List**.

*Exhibit 2.11: Where-Used-Search*
This output generates a list of programs and transactions that use the selected authorization object.

**Where-used Authorization Object F_BKPF_BUK (212 Hits)**

<table>
<thead>
<tr>
<th>Program</th>
<th>Short description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAPFI100</td>
<td>Financial Accounting Comparative Analysis</td>
</tr>
<tr>
<td>SAPMFE05N</td>
<td>Maintain BR/IR Clearing Account</td>
</tr>
<tr>
<td>SAPRCM11R11</td>
<td>Deleting Master Data</td>
</tr>
<tr>
<td>USDALF01</td>
<td>PI Editor: Textsymbol anzeigen</td>
</tr>
<tr>
<td>WSDCCF01</td>
<td>Include WSCCF01</td>
</tr>
<tr>
<td>USDCCF01</td>
<td>Include USDCCF01</td>
</tr>
<tr>
<td>WSSSUMF01</td>
<td>Include WSSSUMF01</td>
</tr>
<tr>
<td>ZSDR_STS_INV</td>
<td>Program for downloading invoices - Chinese Golden Tax System</td>
</tr>
</tbody>
</table>

**Transaction code**

<table>
<thead>
<tr>
<th>Code</th>
<th>Short description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FBRR</td>
<td>Bundle FI Documents to Request</td>
</tr>
<tr>
<td>FBDS</td>
<td>Detail display of payent requests</td>
</tr>
<tr>
<td>FBDR</td>
<td>Display Payment Requests</td>
</tr>
<tr>
<td>FBBO</td>
<td>Reversal of Bank-to-Bank Transfers</td>
</tr>
<tr>
<td>FBDS</td>
<td>Reset Cleared Items: Payt Requests</td>
</tr>
<tr>
<td>FBDD</td>
<td>Post Document</td>
</tr>
<tr>
<td>FBDS</td>
<td>Change Document</td>
</tr>
<tr>
<td>FBDR</td>
<td>Display Document</td>
</tr>
<tr>
<td>FBDR</td>
<td>Document Changes</td>
</tr>
</tbody>
</table>

*Exhibit 2.12: Where-Used-Results*

With a double-click on a selected entry, you branch directly into the source code of the program in the below example, in fact into the section, in which it will be checked whether the required authorization is established for this object.

**Found Locations/short description**

<table>
<thead>
<tr>
<th>Program</th>
<th>300 AUTHORITY-CHECK OBJECT 'F_BKPF_BUK'</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ID ‘BUKRS’ FIELD TOGL-BUKRS</td>
</tr>
<tr>
<td></td>
<td>ID ‘ACTIVY’ FIELD ‘03’.</td>
</tr>
</tbody>
</table>

*Exhibit 2.13: Detail view for located object*
Via double-click onto a transaction you can review the corresponding integration in transaction SE93.

Exhibit 2.14: Transaction set up in SE93

Table of authorization objects

Call the transaction SE16N. Enter the table TOBJ into the field Table. You may add further selection options to the selection mask if required. The execution of the data preparation can be started with the key F8.
Exhibit 2.15: Table of authorization objects

Select an entry and push the button , this way you get to the detail display:

Exhibit 2.16: Detail view of authorization object

Empty fields will not be displayed.

An overview of all object classes is provided in the table **TOBC**. Texts for authorization objects are deposited in the table **TOBJT**.
Display of Entries Found

<table>
<thead>
<tr>
<th>Class</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAAA</td>
<td>AAAA</td>
</tr>
<tr>
<td>AAAB</td>
<td>AAAB</td>
</tr>
<tr>
<td>ACO</td>
<td>ACO</td>
</tr>
<tr>
<td>AM</td>
<td>AM</td>
</tr>
<tr>
<td>BC_A</td>
<td>BC_A</td>
</tr>
<tr>
<td>BC_C</td>
<td>BC_C</td>
</tr>
<tr>
<td>BC_Z</td>
<td>BC_Z</td>
</tr>
<tr>
<td>BPCT</td>
<td>BPCT</td>
</tr>
<tr>
<td>BRF</td>
<td>BRF</td>
</tr>
<tr>
<td>BVCH</td>
<td>BVCH</td>
</tr>
<tr>
<td>BVED</td>
<td>BVED</td>
</tr>
<tr>
<td>BVEM</td>
<td>BVEM</td>
</tr>
</tbody>
</table>

Exhibit 2.17: Table of object classes
2.2 Authorizations

2.2.1 Structure

The creation of users belongs to the functions of a SAP®-system administrator or to an user administrator. The assignment of authorizations is an incumbency of another person, the authorization administrator. The segregation of these working areas is recommendable for the reduction of security risks. If a user had the right to create new users and assign authorizations, he could then equip himself with a user including all authorizations for the SAP®-System and might get unrestricted access to all data this way. This can be prevented by dividing the corresponding working areas. The maintenance of authorizations can only succeed in close cooperation with the end-user department or lies totally in their responsibility.

Changes to the original authorizations may never occur. As a rule a copy may be taken form a standard authorization that may then be modified.

In the next step we will get an overview of the authorizations that exist within the system.

As already explained, authorizations are always based exactly on one authorization object. All authorizations that are based on the same object need different names. However, authorizations that are based on different objects can have identical names. The name of an authorization only has to be clear within one object. That is why many authorizations exist in the system that all have the same name. Here, as an example, a few standard authorizations from SAP® with the name F_ANZ are listed, that are based respectively on varying objects.
An authorization is therefore not identified only through the name, but through the name and the underlying authorization object.

If authorizations were created, then these cannot be utilized right away for the right assignment to the users. The authorizations have to be released first for further use. This procedure is called *Activation* in SAP®. After the activation procedure, the authorization is available for assignment.

### 2.2.2 Overview of authorizations

Our starting point for the authorization overview is therefore the authorization object. Call up the transaction **SU03**.

Select an object class per double-click and set the selection on an authorization object. With another double-click you might branch into the corresponding authorization list.

---

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Authorization</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>F_AVIK_AVA</td>
<td>F_ANZ</td>
<td>Financial Accounting Display Authorization</td>
</tr>
<tr>
<td>F_AVIK_BUK</td>
<td>F_ANZ</td>
<td>Financial Accounting Display Authorization</td>
</tr>
<tr>
<td>F_BKPF_BED</td>
<td>F_ANZ</td>
<td>Financial Accounting Display Authorization</td>
</tr>
<tr>
<td>F_BKPF_BEK</td>
<td>F_ANZ</td>
<td>Financial Accounting Display Authorization</td>
</tr>
<tr>
<td>F_BKPF_BES</td>
<td>F_ANZ</td>
<td>Financial Accounting Display Authorization</td>
</tr>
<tr>
<td>F_BKPF_BLA</td>
<td>F_ANZ</td>
<td>Financial Accounting Display Authorization</td>
</tr>
<tr>
<td>F_BKPF_BUK</td>
<td>F_ANZ</td>
<td>Financial Accounting Display Authorization</td>
</tr>
<tr>
<td>F_BKPF_GSB</td>
<td>F_ANZ</td>
<td>Financial Accounting Display Authorization</td>
</tr>
<tr>
<td>F_BKPF_KCA</td>
<td>F_ANZ</td>
<td>Financial Accounting Display Authorization</td>
</tr>
<tr>
<td>F_ENKA_BUK</td>
<td>F_ANZ</td>
<td>Financial Accounting Display Authorization</td>
</tr>
<tr>
<td>F_ENKA_MAN</td>
<td>F_ANZ</td>
<td>Financial Accounting Display Authorization</td>
</tr>
<tr>
<td>F_KNA1_APP</td>
<td>F_ANZ</td>
<td>Financial Accounting Display Authorization</td>
</tr>
<tr>
<td>F_KNA1_BED</td>
<td>F_ANZ</td>
<td>Financial Accounting Display Authorization</td>
</tr>
<tr>
<td>F_KNA1_BUK</td>
<td>F_ANZ</td>
<td>Financial Accounting Display Authorization</td>
</tr>
</tbody>
</table>

*Exhibit 2.18: Overview of authorizations F_ANZ*
Exhibit 2.19: Overview of authorizations related to an object

To get to the detail display you have to switch to the transaction **SA38/SE38** in a parallel mode. There you have to enter the report **RSUSR030** [transaction **S_BCE_68001414** or **S_BCE_68001417**]. Enter the authorization object that is to be reviewed into the selection mask, and generate your selection afterwards via **F8**.

**Authorizations by Complex Selection Criteria**

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Authorization</th>
<th>Text</th>
<th>Type</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>F_BKPF_BUK</td>
<td>B_ZV_ALL</td>
<td>Generated authorization for profile B_ZV_ALL</td>
<td>A Active version</td>
<td>G Generated</td>
</tr>
<tr>
<td>F_BKPF_BUK</td>
<td>F_ALL</td>
<td>All Financial Accounting Authorizations</td>
<td>A Active version</td>
<td></td>
</tr>
<tr>
<td>F_BKPF_BUK</td>
<td>F_ANZ</td>
<td>Financial Accounting Display Authorization</td>
<td>A Active version</td>
<td></td>
</tr>
<tr>
<td>F_BKPF_BUK</td>
<td>F_BKPF_KAEN</td>
<td>FI Authorizations for Changing Vendor Documents</td>
<td>A Active version</td>
<td></td>
</tr>
<tr>
<td>F_BKPF_BUK</td>
<td>F_DEBITOREN</td>
<td>Accounts Receivable Authorizations</td>
<td>A Active version</td>
<td></td>
</tr>
<tr>
<td>F_BKPF_BUK</td>
<td>F_KREDITOREN</td>
<td>Accounts Payable Authorizations</td>
<td>A Active version</td>
<td></td>
</tr>
<tr>
<td>F_BKPF_BUK</td>
<td>F_SACHKONTEN</td>
<td>General Ledger Authorizations</td>
<td>A Active version</td>
<td></td>
</tr>
<tr>
<td>T_A132010000</td>
<td>A Active version</td>
<td>Generated</td>
<td>A Active version</td>
<td></td>
</tr>
</tbody>
</table>

Exhibit 2.20: Overview of authorizations related to different objects

Double-click onto a selected authorization entry.

**Authorizations by Complex Selection Criteria**

![Diagram of authorizations in tree format]

Exhibit 2.21: Overview of authorizations in tree format
This way you have the possibility to get an overview of the shaping of the authorizations.

This procedure is available for every authorization.

Starting from the authorization overview you also have the possibility to get “Where-used lists” for two integrated questions, profiles and user master records.

Make your choice and confirm it with Enter.

We have selected the entry Profiles for the following view.

With another double-click on a selected line entry you reach a detailed itemized break down of the profile to which this authorization was assigned to.
Exhibit 2.24: Overview of authorization profile in tree format

This detailed overview is available for download as well as print out.

Additionally in the previous tabular preparation, you have the option to get the corresponding change documents displayed (button of the same name):

Exhibit 2.25: Overview of changes to profiles
If you click on an entry, you directly get to the detail display:

**Exhibit 2.26: Overview of changes to authorization**

For the selection according to user masters, you proceed the same way.

**Exhibit 2.27: Overview of assigned users**

With double-click onto a selected entry you branch directly to the detailed directory structure.

**Exhibit 2.28: Overview of user authorizations in tree format**
Exhibit 2.29: Overview of interfaces

In the button menu several options are available, as for example *List of profiles* as displayed below.

Exhibit 2.30: Overview of profile assignments

**Authorizations via table**

Select the table *USR12* for the transaction *SE16N* and enter your selection criteria:

Exhibit 2.31: Table of authorizations
In this example we let the authorization F_ANZ be prepared for us.

Exhibit 2.32: Overview of authorizations and their values

Texts for authorizations are located in the table USR13.
2.3 Profiles

2.3.1 Structure

As a SAP®-System is structured in a very complex way, the definition and assignment of all necessary authorizations for all individual users is only possible in theory. In practice, because of the great effort, this cannot be realized.

As a result, individual authorizations can be combined to an authorization profile. On the other hand, several authorization profiles can be combined into composite profiles.

SAP® already encloses an extensive number of authorization profiles that cover the needs in many cases. Through this the authorization design of the user masters is decisively simplified. According to the name convention of SAP®, the standard profiles also have on the second place of their technical name an underline.

It also has to be observed, that for company copies another sign has to be used, such as a colon or an equal sign. It is always possible to create company specific profiles resulting from new or existing authorizations.

Profiles can exist in different status in the SAP® system:

- active or inactive
- maintained (adapted to actual conditions) or left to standard.

Only active profiles can be used in the system. If new profiles are created, then these have to be activated before they are available within the system.
The authorizations contained in the profiles result in the authorization extent of the user, who got them assigned to his master record.

The name of the profile does not necessarily say anything about its real possibilities!

When restrictions are to become effective in profiles, the standard profiles will be copied, the concerned standard authorizations deleted from the copy and supplemented by company specific authorizations, as a copy of a profile contains initially all the identical authorizations of the original.

For a better overview, the profiles are classified according to working areas and typical scopes of duties. This way, a user of the vendor accounting can get in addition to his already assigned profiles of the vendor accounting for example, the profile for the data archiving assigned if necessary; another user might get the right for the user administration in addition.
2.4 Overview of profiles

With the transaction SU02 you can have the profiles displayed that exist in your system.

Exhibit 2.33: Entrance to profile maintenance
In the lower section Profile, press the Restrictions button. You will receive a list with all profiles.

**Exhibit 2.34: Profile overview**

Select an entry and confirm your choice with the Enter-key.

**Exhibit 2.35: Profile view**
For further information we have to go to the Transaction **SA38/SE38** again. There you have to enter the report name **RSUSR020** [transaction **S_BCE_68001409**].

Make your selection, as here for example the profile **A_ANZEIGE** and then start the preparation.

---

Exhibit 2.36: Profile overview in RSUSR020

Double-click onto a line:

---

Exhibit 2.37: Profile overview in tree format

With a composite profile we are only confronted with one additional instance and that is the information, which single profiles are assigned to this composite profile.

It is also possible to carry out a *Where-used list*, as already described.
Remark:

In the entry mask of the transaction you may also select the button for an overview of profiles. Do not register an entry to the field profile, to get a complete list.

Table overview

In the table **UST10S** via transaction **SE16N** all single profiles with their authorizations are registered.

This table is a transparent table to **USR10**. Let your entries be additionally sorted after the preparation.

**UST10S**

![Profile Where-Used List](image)

### Display of Entries Found

<table>
<thead>
<tr>
<th>Table to be searched</th>
<th>User master: Single profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>UST10S</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of hits</th>
<th>Runtime</th>
</tr>
</thead>
<tbody>
<tr>
<td>116,194</td>
<td>09:08:05</td>
</tr>
</tbody>
</table>

*Exhibit 2.39: Profile overview in UST10S*
Exhibit 2.40: Profile overview in USR10

Maintained texts to profiles are deposited in the table USR11.
2.4.1 Overview of composite profiles

We have already discussed composite profiles in the preceding section, concerning the overview with transaction SU02.

You can receive the tabular overview through the transaction SE16N with the table UST10C.

Exhibit 2.41: Composite profile overview in UST10C
2.5 Roles

2.5.1 Structure

Roles consist of one or more profiles. A role can be regarded as a container for one or more profiles that allow the profile generator to connect to these for creation and maintenance. The role name can have 30 characters.

SAP® provides a set of approx. 2.250 standard roles that can be used as templates. The SAP® standard role names start with SAP_.*.

2.5.2 Overview of roles – the PFCG

The main tool for the role creation is of course the profile generator – transaction PFCG.

Exhibit 2.42: The profile generator

In the button you can select according to different criteria such as: Single Roles, Composite Roles etc. and will get the corresponding results displayed:
Exhibit 2.43: View of Single Roles

If you click onto an entry the role name is transferred to the role name field.

Role Maintenance

Exhibit 2.44: PFCG

If you push the button you get to the display mode of the role.

The role information is ordered and can be reviewed by selecting the different tabs.

The Description tab can be used as a log book, and for storing content or business process descriptions. Here you can also find the information of the user who has created the role and last changed it. If this role is derived from a master role, you can find the corresponding information here also.

Exhibit 2.45: Description tab
The text information are stored in the table AGR_TEXTS.

The tab **Menu** has all menu entries that are part of the selected role.

---

**Display Roles**

<table>
<thead>
<tr>
<th>Role</th>
<th>SAP_FI_AR_MASTER_DATA</th>
<th>Role documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Maintenance of Accounts Receivable Master Data</td>
<td></td>
</tr>
</tbody>
</table>

---

**Exhibit 2.46: The menu tab**

The role menu is customizable. Personalized folders can be created and entries can be moved via drag and drop. Node names can be changes as well.

The menu structure is driven by the individual integration of transactions, reports etc..

---

**Exhibit 2.47: Buttons for role design**

Even complete menus can be taken from any of the below listed.

---

**Exhibit 2.48: Interfaces for menu integration**
The tab *Workflow* allows the assignment of workflow tasks to a role. With that assigned users would become possible agents of corresponding workflow tasks.

Exhibit 2.49: Workflow tab

The tab *Authorizations* leads to the profiles that are part of this role, where as a distinction between the integrated profiles will not become obvious. All profiles are loaded with their authorizations.

Exhibit 2.50: Role content

In display mode you get here:

Exhibit 2.51: Authorization set up
To get the technical information displayed such as authorization object name etc., go to the menu and select *Utilities – Technical names on.* The authorizations can have various statuses like e.g. *Open, Changed, Maintained, Standard, Old, New or Manual.*

*Open*: These authorizations are not yet fully maintained, and have open fields.

*Changed*: The SAP® default suggestion [USOBT_C] was changed.

*Maintained*: One of the fields that were delivered empty form the SAP® defaults was populated with a value.

*Standard*: This authorization is set up according to SAP default.

*Old*: No changes have occurred for this authorization while opening the role in editing mode.

*New*: This authorization was added when opening the role in edit mode.

*Manual*: At least one authorization was added manually.

**! Note**

If a standard SAP® suggestion was changed, the default value will automatically be integrated again when the role is changed the next time.

To reduce the maintenance effort, you may want to consider to reopen the role in expert mode after changing the SAP® defaults.

```
<table>
<thead>
<tr>
<th>Maintain Authorization Data and Generate Profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Authorization Data</td>
</tr>
<tr>
<td>Export Mode for Profile Generation</td>
</tr>
</tbody>
</table>
```

*Exhibit 2.52: Change modes*

Instead of selecting *Edit old status*, you switch to the merge status.
The profile generator will now bring in the SAP® standards again:

Exhibit 2.53: Maintenance options in expert mode

Exhibit 2.54: Import of standard values

Set them to inactive, if you want to go with your changed setting and save your changes. Regenerate the role, and open it again in expert mode as previously described.

The standards will no longer be automatically integrated. The role is stabilized.

The profile generator offers some additional features such as Merge Authorizations [menu path Utilities]. Duplicate authorization entries will be merged.

Another feature can be found in menu Utilities – Reorganize. This will lead to a reorganization of profile numbers. To get an overview of all profiles that are part of this role go to menu entry Authorizations – Profile overview.

When creating a role, the profile name can be adjusted.
The settings for the PFCG can be adjusted via menu path *Utilities – Settings*:

Another interesting feature is in the menu *Utilities – Authorization object assignments*. Position your cursor onto an authorization object within the role. Go to the menu entry just mentioned. You will get the origin of this authorization object displayed [transaction name incl. description] for this role:

<table>
<thead>
<tr>
<th>Name</th>
<th>Short Description</th>
<th>Authorization Id</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>F.2D</td>
<td>Customers: FI-SD mast data comparison</td>
<td>$SPART</td>
<td>$SPART</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$VKORG</td>
<td>$VKORG</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$VTWEG</td>
<td>$VTWEG</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ACTVT</td>
<td>03</td>
</tr>
</tbody>
</table>

*Exhibit 2.57: Authorization object assignments*
In the tab Users you get an overview of all users that have the particular role assigned, and you can also run the user master comparison from here.

![User assignment tab](image)

**Exhibit 2.58: User assignment tab**

The button for the Organizational Management leads to the indirect role assignment where established.

The tab MiniApps lists services or applications that are supposed to be used via web browser.

The tab Personalization stores the objects that are part of a framework for application development and allows the saving of user dependant data for an application.

The table information is valid for both the single roles and the composite roles and are therefore listed separately in section 2.5.6

### 2.5.3 Additional interfaces of the PFCG

The profile generator provides some additional helpful interfaces.

Go to the menu path Utilities in the below view.
Select the first entry *Overview Status*:

The status overview gives you helpful information like e.g. if a role has a menu, if the corresponding profile is generated, if the role is distributed, if the role is assigned to a user or a composite role, if the role is indirectly assigned or if the profile comparison is current etc.

Another interface is integrated to the mass comparison.
Roles: Mass generation of profiles

Which roles do you want to output?
- Roles with Non-Current Profiles
- Also Roles to Be Compared
- Also Roles with no Authorization Data
- All Roles
- Roles with Current Profiles for New Generation

Additional restrictions
- Role
- Last changed by

Presentation in the list
- Display Data When Created and Changed
- Display Role Texts

Generate all profiles to be generated?
- Generate automatically

Exhibit 2.62: Mass generation

This transaction **SUPC** also allows some evaluations as listed in the first section. As long as you do not set the checkmark for generate automatically, you can get the information without direct change.
The interface *Mass Comparison* directly leads to the report **RHAUTUPD_NEW**, transaction **PFUD** or **S_PH0_48000109**.

**User Master Data Reconciliation**

<table>
<thead>
<tr>
<th>Selection of roles</th>
<th>Role to</th>
</tr>
</thead>
</table>

**Selection of action**

- Schedule or check job for full reconciliation
- Perform User Master Comparison

**Editing type**

- Profile matchup
- Composite Role Reconciliation
- HR Organizational Management: Reconciliation
- Cleanups

**Options**

- Display Log

*Exhibit 2.63: PFUD*

This report helps to make the authorizations effective after a role is added to a user in the **PFCG** e.g. also profiles that are no longer current will be deleted from the user master.

The interface *Role comparison* allows the comparison of two roles and their menus [not their authorization]:

**Compare and adjust roles**

<table>
<thead>
<tr>
<th>Compare</th>
<th>Adjust</th>
</tr>
</thead>
</table>

- **Role**: ZZ_MW_TEST_FI_AR_MASTER_DATA
- **Comparison role**
- **Comparison destination**
- **Compare with template**
- **Compare with old customer version**

*Exhibit 2.64: Role menu comparison*
Additional interfaces allow you to read roles from systems that are connected via RFC; you can of course upload and download as well as transport roles. If the client is connected to a CUA [Central user Administration] you can perform the necessary text comparison.

The role menu is influenced by customizing settings in the table SSM_CUST. The switch CONDENSE_MENU set to YES will eliminate redundancies in the role menu. If no entry is listed, or the switch set to NO, the redundancies will not be eliminated. See OSS note 203994.

The switch SORT_USER_MENU will sort the menu entries regardless of their location in alphabetical order if set to YES. The functionality is deactivated if no entry is listed, or if the switch is set to NO. See OSS note 322853.

The switch DELETE_DOUBLE_TCODES set to YES, or without entry will delete transaction code duplicates from different roles. This is deactivated by NO. See OSS note 357693.
2.5.4 Master - Derivation

SAP® has integrated inheritance functionality into the profile generator. That allows the creation of master roles and the derivation of corresponding transaction and transaction related content to a number of derived roles that are connected via a join in the inheritance field.

Exhibit 2.66: Transaction Inheritance

Everything that is part of the master role will be pushed to the connected derived roles aside from the organizational value sets. Therefore this concept can be applied to environments where the only difference related to role activities is in the organizational area.

For example if the accountant A and accountant B have to perform identical tasks, but with split responsibilities as for the company codes. A is only supposed to work in company code 1000, B only in company code 2000.

You can now create a master role [single role], and inherit the content to two derived roles [single roles]. The organizational values need to be specified individually for any of the derived versions.

In case of future role changes, the changes only need to be executed in the master, and can then be pushed to all connected derived versions. This of course reduces the maintenance effort.
Exhibit 2.67: Master – derived concept

The organizational values are listed in table **USORG**. The organizational fields in the profile generator can be maintained with the help of the reports **PFCG_ORGFIELD_CREATE**, **PFCG_ORGFIELD_DELETE** and **PFCG_ORGFIELD_UPGRADE**.

The view **Inheritance Hierarchy** in **PFCG** provides a good overview of master roles and their derived versions.
2.5.5 Overview of composite roles

Composite roles are containers for single roles. In contrast to composite profile the nesting depth is limited. Composite roles may only contain single roles, but no composite roles.

If you call the profile generator and switch to the view Composite Roles you will get an overview of the composite roles.

<table>
<thead>
<tr>
<th>Comp. Roles</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_AUDITOR</td>
<td>AIS - Audit Information System</td>
</tr>
<tr>
<td>SAP_AUDITOR_TAX</td>
<td>AIS - Tax Audit</td>
</tr>
<tr>
<td>SAP_BC_LVC_ALL</td>
<td>LiveCache Administration Roles (Transport Help)</td>
</tr>
<tr>
<td>SAP_BC_TW2 DEVELOPER</td>
<td>Test Workbench: Test Case Creator</td>
</tr>
<tr>
<td>SAP_BC_TW2 DISPLAY</td>
<td>Test Workbench: Display</td>
</tr>
<tr>
<td>SAP_BC_TW2 ORG</td>
<td>Test Workbench: Test Organizer</td>
</tr>
<tr>
<td>SAP_BC_TW2_TESTER</td>
<td>Test Workbench: Tester</td>
</tr>
<tr>
<td>SAP_BC_USR_CUA</td>
<td>Roles for Service User of Central User Manager</td>
</tr>
<tr>
<td>SAP_BPT_ADMINISTRATION</td>
<td>BPT - Arbeitsplatz für Administratoren</td>
</tr>
<tr>
<td>SAP_BPT_CONTROLLER</td>
<td>BPT - Controller</td>
</tr>
<tr>
<td>SAP_BPT_EVERYONE</td>
<td>BPT - Arbeitsplatz für Jedermann</td>
</tr>
<tr>
<td>SAP_BPT_IMPLEMENTATION</td>
<td>BPT - Arbeitsplatz für Implementations-Team</td>
</tr>
<tr>
<td>SAP_CM_ADMIN_COORDINATOR</td>
<td>Admission Coordinator</td>
</tr>
<tr>
<td>SAP_CM_ADMIN_OFFICER</td>
<td>Admission Officer</td>
</tr>
<tr>
<td>SAP_CM_ASM_COORDINATOR</td>
<td>Assessment Coordinator</td>
</tr>
<tr>
<td>SAP_CM_ASM_OFFICER</td>
<td>Assessment Officer</td>
</tr>
<tr>
<td>SAP_CM_STREC_COORDINATOR</td>
<td>Student Records Coordinator</td>
</tr>
<tr>
<td>SAP_CM_STREC_OFFICER</td>
<td>Student Records Officer</td>
</tr>
<tr>
<td>SAP_EHS_IHS_SPECIALIST</td>
<td>Industrial Hygiene and Safety Professional</td>
</tr>
<tr>
<td>SAP_EMPLOYEE</td>
<td>Employee Self Service</td>
</tr>
<tr>
<td>SAP_EMPLOYEE_ERP</td>
<td>Employee Self-Service</td>
</tr>
<tr>
<td>SAP_EMPLOYEE_ERP05</td>
<td>Composite role for all country-specific functions</td>
</tr>
<tr>
<td>SAP_FMCA_ALL</td>
<td>Public Sector Vertragskontokorrent</td>
</tr>
<tr>
<td>SAP_ICC_KOREA_SUPER</td>
<td>Korea Super User</td>
</tr>
</tbody>
</table>

Exhibit 2.68: Composite Role View

If you switch to the view Roles in Composite Roles, you get the contained roles displayed.

<table>
<thead>
<tr>
<th>Roles in Comp. Roles</th>
<th>Description</th>
<th>Target Sys</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_AUDITOR_A</td>
<td>AIS - Central Authorizations</td>
<td>AIS</td>
</tr>
<tr>
<td>SAP_AUDITOR_ADMIN</td>
<td>AIS - Administration</td>
<td>AIS</td>
</tr>
<tr>
<td>SAP_AUDITOR_ADMIN_A</td>
<td>AIS - Administration (Authorizations)</td>
<td>AIS</td>
</tr>
<tr>
<td>SAP_AUDITOR_BA_A</td>
<td>AIS - Authorizations for SAP Applications (Except HR)</td>
<td>AIS</td>
</tr>
<tr>
<td>SAP_AUDITOR_BA_CO</td>
<td>AIS - Internal Activity Allocation</td>
<td>AIS</td>
</tr>
<tr>
<td>SAP_AUDITOR_BA_CO_A</td>
<td>AIS - Internal Activity Allocation (Authorizations)</td>
<td>AIS</td>
</tr>
<tr>
<td>SAP_AUDITOR_BA_EC_CS</td>
<td>AIS - Consolidation</td>
<td>AIS</td>
</tr>
<tr>
<td>SAP_AUDITOR_BA_EC_CS_A</td>
<td>AIS - Consolidation (Authorizations)</td>
<td>AIS</td>
</tr>
<tr>
<td>SAP_AUDITOR_BA_EC_PCA</td>
<td>AIS - Profit Center Accounting</td>
<td>AIS</td>
</tr>
</tbody>
</table>

Exhibit 2.69: Roles in Composite Roles View
2.5.6 Tables with role information

All tables can be displayed with the help of transaction SE16N, SE16 etc.

The table **AGR_DEFINE** contains all roles, and also the reference to the parent role if available.

Exhibit 2.70: AGR_DEFINE

An overview of composite roles and their assigned roles can be obtained in table **AGR_AGRS**.

<table>
<thead>
<tr>
<th>Composite role</th>
<th>Role</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_AUDITOR</td>
<td>SAP_AUDITOR_A</td>
<td></td>
</tr>
<tr>
<td>SAP_AUDITOR</td>
<td>SAP_AUDITOR_ADMIN</td>
<td></td>
</tr>
<tr>
<td>SAP_AUDITOR</td>
<td>SAP_AUDITOR_ADMIN_A</td>
<td></td>
</tr>
<tr>
<td>SAP_AUDITOR</td>
<td>SAP_AUDITOR_BA_A</td>
<td></td>
</tr>
<tr>
<td>SAP_AUDITOR</td>
<td>SAP_AUDITOR_BA_CO</td>
<td></td>
</tr>
<tr>
<td>SAP_AUDITOR</td>
<td>SAP_AUDITOR_BA_CO_A</td>
<td></td>
</tr>
</tbody>
</table>

Exhibit 2.71: AGR_AGRS

In table **AGR_1016** the roles together with their profiles are stored:

<table>
<thead>
<tr>
<th>Table to be searched</th>
<th>Name of the activity group profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGR_1016</td>
<td></td>
</tr>
</tbody>
</table>

Number of hits | 1,485 |
Runtime | 6 |

Exhibit 2.72: AGR_1016
The authorization objects for the individual roles are located in table **AGR_1250**.

Exhibit 2.73: **AGR_1250**

The authorization status of the object is listed left to the column **Variant**, as well as indicators if objects were deleted, copied, are old or new.

The authorization data including corresponding field values are listed in table **AGR_1251**.

Exhibit 2.74: **AGR_1251**
The table **AGR_1252** provides all organizational values that are part of the individual roles.

Exhibit 2.75: AGR_1252

The menu information is part of the table **AGR_HIER**.

Exhibit 2.76: AGR_HIER

Table **AGR_TCODES** provides an overview of the roles with their transaction codes.

Exhibit 2.77: AGR_TCODES
The table **AGR_PROF** has all the roles with their profiles and profile names:

**Display of Entries Found**

<table>
<thead>
<tr>
<th>Table to be searched</th>
<th>Role</th>
<th>Profile name for role</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGR_PROF</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Exhibit 2.78: AGR_PROF**

In table **AGR_NUM_2** the internal counter for profiles in roles is stored.

The table **AGR_TIME** contains the relevant time stamp information for menu, profiles and authorization.

**Display of Entries Found**

<table>
<thead>
<tr>
<th>Table to be searched</th>
<th>Role</th>
<th>Time Stamp for Role (Menu, Profile, Authorizations)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGR_TIME</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Exhibit 2.79: AGR_TIME**

The time stamp for profile generation is part of table **AGR_TIMEB**, for user assignments **AGR_TIMEC**, and **AGR_TIMED** for profile comparisons.

The overview of roles and their user assignments is part of table **AGR_USERS**.

The SAP® menu is stored in table **SMENSAPNEW**, the text in **SMENSAPT**.
2.6 User

2.6.1 User master record

The user master record consists of a client valid and clear, free selectable name. The name can be assigned in the corresponding address field to a specific employee. Also assigned here is the password, that is provided by the user administrator first of with an initial password (IPW-Initial-password). Furthermore, the user can be assigned to a user group; that does not indicate an increase of rights, but makes allows easier sorting as well as a segregation of duties in the user management organization [as a restriction field within an authorization].

The user record can be provided with validity time period, no entry indicates unlimited validity.

An accounting number can be registered for the CPU-time account.

A user record consists among others of the following elements:

- User name
- Assigned client
- Password
- Company address
- User type
- Start menu
- Logon language
- Personal output control
- Time zone
- Activity groups / roles
- Profiles
• Authorizations

• Parameter adjustments

Users can be displayed over the menu item Tools-Administration - User maintenance - Display user (Transaction SU01D). In the field User, you enter the user ID that you want to have displayed and then you click on the button Display.

![User Maintenance: Initial Screen](image)

Exhibit 2.80: SU01D

ALIAS serves as alternative user identification.

If you want to create a user with an alias, you have to assign the alias in the input field on the register card logon data. Through the use of alias names you have 40 signs available and with that you can utilize longer, self-explaining names. The user can then be identified either through the (12 character) user name or through his (40 character) alias. For the SAP®-GUI and RFC-logons to the system, alias names cannot be used at this time.
The user attributes are distributed over several register cards:

**Address:**

The company address data of the corresponding user is displayed on the first tab - followed by company and communication data.

---

*Exhibit 2.81: Address data*
**Logon data:**

The logon data of the user:

![Display User](image)

**Exhibit 2.82: Logon data**

The assignment to a user group is maintained in the context of the user administration. User administrators receive their responsibilities for the user administration through the assignment to a user group.

With the validity time period, the employee affiliation time can be limited. If no entry exists, then the employee is valid unlimitedly.
User types:

Dialog = regular SAP user
Communication = Implementation for a dialog-free communication (e.g., via RFC)
System = dialog-free communication within systems (e.g., CPIC user)
Service = Dialog user for a larger, anonymous user range [should only have minimum access authorizations].
Reference = separately discussed, see chapter 2.6.2.

Defaults:

Here the standard output devices, its spool control and the personal adjustments for the display of numbers and dates are displayed.

Exhibit 2.82: Defaults
Parameters:

The personal parameter adjustments of the users are displayed here.

### Display User

<table>
<thead>
<tr>
<th>Parameter ID</th>
<th>Parameter Value</th>
<th>Short Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F03</td>
<td>X</td>
<td>Accounting User Options (Single-Screen Transaction)</td>
</tr>
<tr>
<td>F21</td>
<td>SAF01</td>
<td>FL: Invoice/Credit Memo Fast Entry Line Layout</td>
</tr>
<tr>
<td>F22</td>
<td>SAF01</td>
<td>FL: GL Account Items Fast Entry Line Layout</td>
</tr>
<tr>
<td>F25</td>
<td>SAF01</td>
<td>FL: Document Parking Fast Entry (GL Account Line Layout)</td>
</tr>
<tr>
<td>KME</td>
<td>SAF01</td>
<td>FI Account Assignment Model: Screen Template Value</td>
</tr>
<tr>
<td>LE_SHIP_DEL_MON_LIST</td>
<td>HC</td>
<td>Delivery Monitor List Type</td>
</tr>
<tr>
<td>SCL</td>
<td>X</td>
<td>Upper and lower case in source code; X = lower, **</td>
</tr>
<tr>
<td>SU53_STYLE</td>
<td>TREE</td>
<td>Layout of SU53 and SU55 (CLASSIC or TREE)</td>
</tr>
<tr>
<td>WLS</td>
<td>X X XX X</td>
<td>Workflow: User-specific settings</td>
</tr>
</tbody>
</table>

*Exhibit 2.83: Parameters*
Roles:

Display of the roles that were assigned to the user:

Exhibit 2.84: Role assignments

Profiles:

Display of the profiles that were assigned to a user:

Exhibit 2.85: Profile assignments

The maximum number of profiles that can be assigned to a user is limited to 312 due to the structure of the underlying database. See OSS 410993.
Groups:

Display of groups, in which the user is listed as member:

Exhibit 2.86: Groups assignments

Personalization:

<table>
<thead>
<tr>
<th>Description</th>
<th>Personalization object key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line Maintenance - Flight: User Settings</td>
<td>/SDFFSILM_FLIGHT</td>
</tr>
<tr>
<td>Line Maintenance - Flight Plan: User Settings</td>
<td>/SDFFSILM_FPLAN</td>
</tr>
<tr>
<td>Line Maintenance - Status Board: User Settings</td>
<td>/SDFFSILM_STS</td>
</tr>
<tr>
<td>spare parts personalization key</td>
<td>/SAFDILSPP</td>
</tr>
<tr>
<td>Vehicle management’s personalization key for DI</td>
<td>/SAFDIIMWS</td>
</tr>
<tr>
<td>Personalization Key/For Warranty Application</td>
<td>/SAFDIWITY</td>
</tr>
<tr>
<td>Consolidator Portal - Page personalization key</td>
<td>/SPEICONS_CI</td>
</tr>
<tr>
<td>Consolidator Portal - Page personalization key</td>
<td>/SPEICONS_QR</td>
</tr>
<tr>
<td>Consolidator Portal - Page personalization key</td>
<td>/SPEICONS_NOLINE</td>
</tr>
<tr>
<td>Consolidator Portal - Page personalization key</td>
<td>/SPEICONS_FACE</td>
</tr>
<tr>
<td>Consolidator Portal - Page personalization key</td>
<td>/SPEICONS_QI</td>
</tr>
<tr>
<td>Consolidator Portal - Page personalization key</td>
<td>/SPEICONS_SO</td>
</tr>
<tr>
<td>Inbound Developer Utilities</td>
<td>/SPEINBDDEVUT</td>
</tr>
</tbody>
</table>

Exhibit 2.87: Personalization

Via double-click onto an entry you can branch to the corresponding details.

Licence data:

Exhibit 2.88: Licence data
2.6.2 The reference users

Reference users serve to pass on access rights to other users. A reference user gets rights assigned. Each user may have exactly one reference user assigned to him, whose authorizations he will receive at the logon in addition to his already existing rights. Reference user of the corresponding type cannot logon to a system. They are substantially used to equip internet users with identical authorizations.

In the context of user evaluations within SAP®, the authorizations that were obtained through a reference user will not be considered! The assignment of reference users to users is separately to be checked in the table USREFUS.

Reference users are assigned to user within the register sheet Roles:

Exhibit 2.89: Reference user assignments

With the flag REF_USER_CHECK within the table PRGN_CUST you can adjust, which message is to be displayed, in case a user who is not of the type reference is assigned as a reference user: 'W' (default) Warning, 'E' Error, 'S' Simple message, 'I' no message.

An overview of created reference users is prepared by the report RSUVM013.
2.6.3 Basic user evaluations

An overview of users, whose address data are only maintained incompletely can be received with the report RSUSR007 [transaction code RSUSR007 or S_ALR_87101200]

Exhibit 2.90: RSUSR007

Select the fields that have to be maintained according to your company guidelines and start the execution. The evaluation succeeds cross-client.

You can carry out a general selection according to user address data with the report RSUSR002_ADDRESS [transaction S_BCE_68001393].
Exhibit 2.91: RSUSR002_ADDRESS

All currently active users can be displayed with the help of the report RSUSR000. The report RSUSR200 contains further information that can be interrogated.

Exhibit 2.92: RSUSR200
Note:

With regard to the selection according to validity, a programming error exists in some releases. The selection fields were probably mixed up. OSS Information: 669023, 1007027.

This means: If you have selected putative valid users- you actually have selected the invalid ones and vice versa.

2.6.4 System measurement data

The user measurement data serve as basis for the calculation of the license fees. The standard user types are listed in the table TUTYP:

<table>
<thead>
<tr>
<th>Language</th>
<th>User Type</th>
<th>User Type Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN</td>
<td>01</td>
<td>Operational User</td>
</tr>
<tr>
<td>EN</td>
<td>02</td>
<td>Information User</td>
</tr>
<tr>
<td>EN</td>
<td>03</td>
<td>Requisitions/Confirmations</td>
</tr>
<tr>
<td>EN</td>
<td>04</td>
<td>Substitute</td>
</tr>
<tr>
<td>EN</td>
<td>05</td>
<td>Basis Only</td>
</tr>
<tr>
<td>EN</td>
<td>06</td>
<td>Development Workbench User</td>
</tr>
<tr>
<td>EN</td>
<td>07</td>
<td>Enterprise HR User</td>
</tr>
<tr>
<td>EN</td>
<td>11</td>
<td>Multi-Client/System User</td>
</tr>
<tr>
<td>EN</td>
<td>12</td>
<td>DECENTRALALE USER (GUEST)</td>
</tr>
<tr>
<td>EN</td>
<td>20</td>
<td>SAP APO-DO-ATP</td>
</tr>
<tr>
<td>EN</td>
<td>21</td>
<td>SAP APO-PP/DS</td>
</tr>
<tr>
<td>EN</td>
<td>22</td>
<td>SAP APO-SCP</td>
</tr>
<tr>
<td>EN</td>
<td>23</td>
<td>SAP APO-COLL</td>
</tr>
<tr>
<td>EN</td>
<td>24</td>
<td>SAP APO-TP</td>
</tr>
<tr>
<td>EN</td>
<td>25</td>
<td>SAP EBP Purchase User</td>
</tr>
<tr>
<td>EN</td>
<td>26</td>
<td>SAP EBP Requisitioner</td>
</tr>
<tr>
<td>EN</td>
<td>30</td>
<td>SAP BW</td>
</tr>
</tbody>
</table>

Display of Entries Found

<table>
<thead>
<tr>
<th>Table to be searched</th>
<th>TUTYP</th>
<th>SAP System User Type Texts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of hits</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>Runtime</td>
<td>0</td>
<td>Maximum no. of hits 500</td>
</tr>
</tbody>
</table>

Exhibit 2.93: TUTYP
According to the user type SAP® imposes license fees for the users. For the determination of how many users exist of all user types, the report of the system measurement RSUVM002 can be used. Call up this report with the transaction SA38 (System – Services - Reporting). For all clients, the number of existing user types will be displayed:

To review which user is of which user type, you may use the RSUVM005. All users with their user names and types are listed here, sorted by their client-affiliation.

Users, for whom no user type is displayed, are automatically of the user type: OPERATIONAL-USER.

**OSS Notes for system measurement:**

- 39307 Users priced separately during measurement
- 121366 System measurement in Release 4.5 und 4.6
- 94167 System measurement in Release 4.0
### Meaning of some selected user types:

<table>
<thead>
<tr>
<th>Id.</th>
<th>Description</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>OPERATIONAL-USER</td>
<td>User with the authorization to carry out SAP SAP® transactions for creating, deleting or changing data.</td>
</tr>
<tr>
<td>02</td>
<td>INFORMATIONAL-USER</td>
<td>User with the authorization to read-only data within SAP SAP®. Change or addition of data is not allowed.</td>
</tr>
<tr>
<td>03</td>
<td>REQUESTER / CONFIRMER</td>
<td>Users that only possess the authorization:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- To create a purchase requisition (Component MM)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- To create an order confirmation (Component PP)</td>
</tr>
<tr>
<td>04</td>
<td>SUBSTITUTE</td>
<td>A user, who executes the functions of another user for a certain time. The actual user is not allowed to be active in the system during that time. The substitute user is free of charge, because the actual user will be cashed up.</td>
</tr>
<tr>
<td>05</td>
<td>ONLY-BASIS-USER</td>
<td>Users that only execute administrative basic functions. They are also allowed to use all HR-transactions for their own purpose.</td>
</tr>
<tr>
<td>06</td>
<td>DEVELOPMENT WORKBENCH-USER</td>
<td>Users with the authorization to use the ABAP-Workbench. For these users usually a developer key was requested.</td>
</tr>
<tr>
<td>07</td>
<td>ENTERPRISE HR-USER</td>
<td>Users that may only perform the following actions for themselves:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- HR data maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Time and attendance recording</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Travel expense processing and expense accounting</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Who’s who</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Course registration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Internal job advertisement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Calendar resource</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Purchase requisition for employees</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Email incl. document filing</td>
</tr>
<tr>
<td>11</td>
<td>MULIT CLIENT/-SYSTEM-USER</td>
<td>Users that work in several client / systems, only have to be declared once with their real user type. In other clients / systems they will be declared as multi-client-system-users. This user-type is free.</td>
</tr>
<tr>
<td>91</td>
<td>TEST-USER</td>
<td>Users that are exclusively used for test purposes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The SAP ® standard user SAP*, DDIC,SAPCPIC and TMSADM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Users with developer keys, who exclusively carry out emergency functions and repairs (emergency users).</td>
</tr>
<tr>
<td>71</td>
<td>SPECIAL COMPONENT TYPE 1 9</td>
<td>Users that carry out functions that are not part of the general SAP®-standard. An individual contract settlement is to be agreed.</td>
</tr>
<tr>
<td>81</td>
<td>IS-USER TYP 81 85</td>
<td>User of IS-components. An individual contract settlement is to be agreed.</td>
</tr>
</tbody>
</table>
User evaluation in tables

First of all you can get yourself an overview of all tables that contain user data. Select the transaction **SE16N**, press the *Input help* button and there choose the button *Information System*. There you enter in the field *Table name*: **USR* or UST* or USH**.

![Exhibit 2.94: Table information system](image)

You will receive a list.
Exhibit 2.95: Search Result

For a relevant user overview, the following tables are required:

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USR01</td>
<td>User master record</td>
</tr>
<tr>
<td>USR02</td>
<td>Logon data</td>
</tr>
<tr>
<td>USR03</td>
<td>User address data</td>
</tr>
<tr>
<td>USR04</td>
<td>User master authorizations</td>
</tr>
<tr>
<td>UST04</td>
<td>User masters</td>
</tr>
<tr>
<td>USH04</td>
<td>Change history for authorizations</td>
</tr>
<tr>
<td>USR10</td>
<td>User master authorization profiles</td>
</tr>
<tr>
<td>USR12</td>
<td>User master authorization values</td>
</tr>
</tbody>
</table>
3 Basic mode of operations

3.1 General relation transaction and authorization object

Actually, a user is never confronted directly with an authorization object. He works with transactions. Now we have to get acquainted with the relation between transactions and authorization objects. The following aspects are generally valid for these relations:

- An authorization object can be integrated in the call of several transactions.
- At the call of a transaction, several authorization objects can be integrated.

The relation between transactions and authorization objects are deposited in the table **USOBT** (at the use of the profile generator in table **USOBT_C**). Enter the name of the transaction you want to dissolve, into the selection mask – field Name:

Exhibit 3.1: USOBT_C

The following display results from the example transaction **FK03** (Display of vendor master records):
Exhibit 3.2: FK03

Not every one of these authorization objects will inevitably be checked. Some are optional. In the next step it has to be reviewed which authorization objects are actually checked.

Call the transaction **SU22**: 

Exhibit 3.3: SU22
Exhibit 3.4: SU22 - detail

Mark an entry and double-click onto it or else push the button.
The type definition can be displayed via the Help (F1) in the field Type (TC).

**Type of transaction**

A transaction is defined here by an identification code with a maximum of three digits. The individual letters have the following meaning:

- T Transaction
- R Report transaction
- P Parameter transaction
- C Transaction defined by authorization object
- E Locked by entry in Transaction SM01
- M Area menu
If the transaction code is based on another transaction code, you will find a corresponding entry in the last column **TCod**.

For the evaluation of a transaction, mark the desired entry and push the button **Check indicator**.

### Exhibit 3.9: Check indicator

Three authorization objects will be checked altogether at the call of the transaction **FK03**, because the change authorization and the account group authorization, as well as the account authorization or business partner are optional. Via the **Help**, you can branch to the legend for the check indicators:

### Exhibit 3.10: Check indicator explanation
Via the button **Field values** you can get a detailed overview of the required field values of these authorization objects.

### Exhibit 3.11: SAP® standards

Via the button **Object desc.** you have the opportunity to get the object descriptions additionally displayed.

With the help of the button **Value list** you get the following overview:

### Exhibit 3.12: Detail view
For the execution of the transaction **FK03** it will be checked, if the user has the necessary authorizations for all three authorization objects. If the authorization for one object is missing, then he will not be allowed to execute the transaction.

Another possibility exists, if the user has received authorizations on all three objects, but with further restrictions. Has a user for example received authorizations on all three objects, but for the object **F_LFA1_BUK** he only got an authorization for the company code 1000, then he may execute this transaction and look at the 1000 customers in the company code. If he enters the company code 2000 at the display of customer master records, then he will receive the message “No authorization for the company code 2000”. The system will then not allow the display of the selected customer.

That an authorization object is checked at several transactions can be explained with the example of the object **F_LFA1_APP**. This object was used for the transaction **FK03**. The question displayed by this object (which actions may be carried out with the customer master records) will be frequently required, for example within the transaction **FK01** (Creation of vendor master records). For the transaction **FK01** there was naturally no new object created. Therefore an authorization on the object **F_LFA1_APP** will be inquired. The authorization object **F_LFA1_APP** is checked in about 331 transactions in ECC 6.
### Exhibit 3.13: USOB_C – object selection

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>To Value</th>
<th>Date</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIBLAPIOP</td>
<td>TR</td>
<td>F_LFA1_APP</td>
<td>ACTVT 03</td>
<td>SAP</td>
</tr>
<tr>
<td>FK01</td>
<td>TR</td>
<td>F_LFA1_APP</td>
<td>ACTVT 01</td>
<td>SAP</td>
</tr>
<tr>
<td>FK02</td>
<td>TR</td>
<td>F_LFA1_APP</td>
<td>ACTVT 02</td>
<td>SAP</td>
</tr>
<tr>
<td>FK03</td>
<td>TR</td>
<td>F_LFA1_APP</td>
<td>APPKZ F</td>
<td>SAP</td>
</tr>
<tr>
<td>FK04</td>
<td>TR</td>
<td>F_LFA1_APP</td>
<td>ACTVT 03</td>
<td>SAP</td>
</tr>
<tr>
<td>FK05</td>
<td>TR</td>
<td>F_LFA1_APP</td>
<td>APPKZ F</td>
<td>SAP</td>
</tr>
<tr>
<td>FK06</td>
<td>TR</td>
<td>F_LFA1_APP</td>
<td>ACTVT 06</td>
<td>SAP</td>
</tr>
<tr>
<td>FK07</td>
<td>TR</td>
<td>F_LFA1_APP</td>
<td>APPKZ F</td>
<td>SAP</td>
</tr>
<tr>
<td>FK08</td>
<td>TR</td>
<td>F_LFA1_APP</td>
<td>ACTVT 08</td>
<td>DDIC</td>
</tr>
<tr>
<td>FK09</td>
<td>TR</td>
<td>F_LFA1_APP</td>
<td>ACTVT 03</td>
<td>DDIC</td>
</tr>
<tr>
<td>FMCAV1</td>
<td>TR</td>
<td>F_LFA1_APP</td>
<td>ACTVT 01</td>
<td>DDIC</td>
</tr>
</tbody>
</table>

### Exhibit 3.14: USOB_C – transactions with objects F_LFA1_APP
This authorization object is part of the module FI (Financial accounting). It may be used in other modules as well, for example in the module SD (Sales and Distribution).

The tables with the change history for the tables **USOB_C** and **USOBX_C** are **USOB_C_D** and **USOBX_C_D**.
3.2 The authorization check for dialog users

Short introduction to the basic mode of operation

One has to deal with the following three steps.

I.
The user enters a transaction code like for example **FK01**.

Initially SAP® checks if the called transaction code is valid (comparison with table entries in table **TSTC**), it is also evaluated if the transaction code is locked (via **SM01** e.g.)

SAP® then checks whether the user has a correspondent authorization on the object **S_TCODE**.

The authorization object **S_TCODE** consists of only one field (**TCD**).

The called transaction has to be part of the existing entries.

If the assigned authorization does not meet the requirements, then the user will fail the authorization check already at this stage of procedure.

This is the message that will accompany this step.

![Exhibit 3.15: Error message](image)

If the user successfully passes this check, then SAP® continues with the next step (II.).

II.

SAP® then checks whether any values for transaction code authorizations were assigned to the called transaction. This can be looked up in the table **TSTCA**. For a successful pass the user needs a matching authorization.
The above described maintenance is executed with the help of the transaction SE93.
There one can define whether an additional authorization check on especially selected authorization objects has to be passed additionally.

And again if the user fails the way ends right up here. If this step was passed too, SAP® proceeds with the next step.

III.
SAP® checks whether the user has a match for the so-called application authorization.
Every call of a transaction leads to the execution of a SAP® program.
The program that is assigned to the transaction can also be reviewed with the call of the transaction `SE93`. And if further authorization checks are executed depends on the source code.

[You might check the source code with the help of the report `RSABAPSC`.]

Within the authority-check the object is listed together with the fields.

The authority-check is always executed with a logical `AND` as a joint of the listed field that are part of the listed authorization object.

One entry as an example of the integrated authority-checks is:

```plaintext
... 
AUTHORITY-CHECK OBJECT 'F_LFA1_BUK'
ID 'BUKRS' FIELD LFB1-BUKRS
ID 'ACTVT' FIELD B_ACTVT
IF SY-SUBRC <> 0.
   MESSAGE Exxx WITH xxx.
   ENDIF.
... 
```

In this case the object `F_LFA1_BUK` (vendor: authorization for company codes) with both of the defined fields is checked.

For the field BUKRS (company code) it is checked if the user has the same value assigned as provided by the variable `LFB1-BUKRS`.

For the field ACTVT (activity) it is checked if the user has the same value assigned as provided by the variable `B_ACTVT`.

Only when all values correspond with the requirements, the return value will be set to 0.

Otherwise the authorization check fails `IF SY-SUBRC <> 0` [means that the return value is not equal 0] and the user will get an error message.

The authority-check may be integrated as a part of the program or may else be executed within an integrated call of a function module. The execution of the authority-check relies on the pass through of the correspondent source code section of course.
If the dialog user has passed these authorization checks successfully, he will be able to execute the called transaction.

**Important exceptions**
As usual there are some exceptions from the rule.
In this case we have to look at two other adjustments.

1. **Disabling of authorization objects**
First of all SAP offers the possibility to deactivate checks on authorization objects globally. In case an object is listed in the table `TOBJ_OFF` this object is excluded from any authority-checks. Objects with the initials `S*` or `P*` cannot be switched off.

2. **Check indicator**
The second option that is to be considered is the adjustment for the individual transaction. With the help of the transaction `SU24/SU22` authorization objects can be maintained to the effect that they will not be checked at the call of a transaction. These settings are located in the tables `USOBX_C` (check table for `USOBT_C`) and `USOBT_C` (relation between transaction and authorization object).
These tables are the customer specific tables that are valid if the profile generator is activated for use. The equivalent SAP tables are the tables `USOBX` and `USOBT`.

The values the check indicator may adopt are:

- **Y** the authorization object is checked at the call of the transaction
- the default values are located in the table `USOBT_C`
- **N** the authorization object is NOT checked at the call of the transaction
- **X** the authorization check takes place
- **U** not maintained
- `<empty>` not maintained
3.3 The matching authorization

It is of no importance whether the matching authorization results from a profile in a role or a manually created profile. That means that the origin of a matching authorization is of no relevance.

I. Our first test case for a better understanding.
The following authorization is required for a successful pass of the authority-check:

for authorization object F_LFA1_APP
for field ACTVT value 02
for field APPKZ value F

Scenario 1:
The user has the following authorizations assigned.

Authorization A
for authorization object F_LFA1_APP
for field ACTVT value 03
for field APPKZ value F

Authorization B
for authorization object F_LFA1_APP
for field ACTVT value 02
for field APPKZ value M

The user has no matching authorization because the required values are not combined in one authorization.
Scenario 2:
The user has the following authorizations assigned.

**Authorization A**
- for authorization object: F_LFA1_APP
- for field: ACTVT value 02
- for field: APPKZ value F

**Authorization B**
- for authorization object: F_LFA1_APP
- for field: ACTVT value 02
- for field: APPKZ value M

The user has one matching authorization [Authorization A].

Scenario 3:
The user has the following authorizations assigned.

**Authorization A**
- for authorization object: F_LFA1_APP
- for field: ACTVT value 02
- for field: APPKZ value F

**Authorization B**
- for authorization object: F_LFA1_APP
- for field: ACTVT value *
- for field: APPKZ value *

The user has full authorization. He has even higher authorization [Authorization B] than required. That means that he is able to do whatever is possible within this context.
The highest assigned authorization that meets the requirements will always prevail.

II. Second test case for verification:

Required for a successful pass of the authority-check is the following authorization:

for authorization object  S_TABU_DIS
for field ACTVT value 02
for field DICBERCLS value FC01

Scenario 1:
The user has the following authorizations assigned.

Authorization A
for authorization object  S_TABU_DIS
for field ACTVT value 03
for field DICBERCLS value FC01

Authorization B
for authorization object  S_TABU_DIS
for field ACTVT value 02
for field DICBERCLS value FC32

The user has no matching authorization.
Scenario 2:
The user has the following authorizations assigned.

Authorization A
for authorization object  S_TABU_DIS
for field  ACTVT  value 02
for field  DICBERCLS  value FC01

Authorization B
for authorization object  S_TABU_DIS
for field  ACTVT  value 03
for field  DICBERCLS  value FC01

The user has one matching authorization [Authorization A].

Scenario 3:
The user has the following authorizations assigned.

Authorization A
for authorization object  S_TABU_DIS
for field  ACTVT  value *
for field  DICBERCLS  value FC01

Authorization B
for authorization object  S_TABU_DIS
for field  ACTVT  value 03
for field  DICBERCLS  value FC32

The user has one matching authorization [Authorization A].
Scenario 4:
The user has the following authorizations assigned.

**Authorization A**
for authorization object  **S_TABU_DIS**
for field  **ACTVT**  value 02
for field  **DICBERCLS**  value *

**Authorization B**
for authorization object  **S_TABU_DIS**
for field  **ACTVT**  value 03
for field  **DICBERCLS**  value FC32

The user has one matching authorization [Authorization A].

Scenario 5:
The user has the following authorizations assigned.

**Authorization A**
for authorization object  **S_TABU_DIS**
for field  **ACTVT**  value 02
for field  **DICBERCLS**  value FC01

**Authorization B**
for authorization object  **S_TABU_DIS**
for field  **ACTVT**  value *
for field  **DICBERCLS**  value FC01

**Authorization C**
for authorization object  **S_TABU_DIS**
for field  **ACTVT**  value *
for field  **DICBERCLS**  value *
The user has full authorization. He has even higher authorization [Authorization C] than required.

**Conclusion**

The authorizations are accumulated within the user master record. The user master data will be scanned during the different steps of the authorization check procedure. If a match or an even higher authorization is detected, the user will successfully pass the authorization check.
4 Evaluation tools

4.1 Report RSUSR002

This report is the core tool for user authorization evaluation.

Users by Complex Selection Criteria

<table>
<thead>
<tr>
<th>Selection criteria for user</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
</tr>
<tr>
<td>Group for authorization</td>
</tr>
<tr>
<td>User group (general)</td>
</tr>
<tr>
<td>Reference user</td>
</tr>
<tr>
<td>User ID alias</td>
</tr>
<tr>
<td>Role</td>
</tr>
<tr>
<td>Profile name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AND Profil</th>
<th>AND Profil</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Transaction Code</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Selection by Field Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field Name</td>
</tr>
<tr>
<td>Value</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Selection by authorizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization object</td>
</tr>
<tr>
<td>Authorization</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Selection by values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry values</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authorization object 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization object</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AND authorization object 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization object</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AND authorization object 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization object</td>
</tr>
</tbody>
</table>

Exhibit 4.1: RSUSR002
You can check which users have for example SAP® standard profiles such as SAP_ALL, SAP_NEW, S_A.SYSTEM, S_A.DEVELOP assigned.

**The profile SAP_ALL**

This composite profile contains almost all authorizations for the SAP® system. This includes basis administration, application maintenance, all customizing-functions and the table maintenance for all tables, including the cross-client tables. According to the aspect of a segregation of duties it is not necessary to assign this profile in practice. If at all, it should only be assigned to an emergency user, who is supposed to be protected with dual control.

**The profile SAP_NEW**

This composite profile contains all innovations of the latest SAP® releases, starting with 2.1C. Among others the authorizations for the administration of cross-client tables as well as the transaction authorization for all transactions is in this profile. This profile may be used for a limited time-period after a release change in a development environment, but is not feasible for the running productive operation mode.

**The profile S_A.SYSTEM**

This profile contains all basis authorizations, including the authorization for role and user administration. With this, no segregation of duties is possible in this area. A user with this profile has the right to assign for example, the profile SAP_ALL to himself or to any other user. Through this, he might gain complete access to all available data. Therefore this profile is regarded as backdoor to SAP_ALL.
The profile S_A.DEVELOP

This is a profile for developers. It contains comprehensive access to almost all data. This profile should not be assigned to anyone in the production system.

You can check if users have SAP® standard role assigned. You can evaluate which users have critical authorizations assigned.

In the section, you can review for example, which user has a certain field, as for example BUKRS [company code] assigned with a certain value, e.g. 1000. This way you can see, who generally has access to this organizational unit.

In the selection area Selection by values you can enter up to three authorization objects with corresponding field values for evaluation of critical authorizations. The objects are combined via logical AND. If your roles are menu based, you can use the as fourth element for your inquiry.

For queries on roles that are not menu based, you would need to check on S_TCODE.

Some evaluations are already predefined:

RSUSR002_AUDIT_ABAP [S_ALR_87101206] - Users with ABAP Authorization
RSUSR002_AUDIT_CTS [S_ALR_87101207] - Users who can use CTS
RSUSR002_AUDIT_OSCL [S_ALR_87101205] - Users who can call OS commands
RSUSR002_AUDIT_RFC - Users who can execute RFC functions
RSUSR002_AUDIT_UAP [S_ALR_87101208] - Update Accounting Periods
RSUSR002_AUDIT_UCA [S_ALR_87101210] - Update Chart of Accounts
RSUSR002_AUDIT_UCC [S_ALR_87101209] - Update Company Codes
If you want to combine more than three authorization into a query, you need to download the results of the first three and reconcile it with the result list of the second query by identifying the corresponding cut set.

In the meantime SAP® offers the GRC [Governance, Risk and Compliance] toolset. This toolset has approx 20,000 predefined rules for the evaluation of SOD [segregation of duties] conflicts. The ruleset is customizable. A variety of features is included as for example the interactive simulation of role changes to identify potential SOD conflicts right in the beginning, or the integration into profile generator or user maintenance. A Fire Fighter solution is also part of the set, as well as a user provisioning entity.

The general advantage is the full integration into the SAP® system including online reviews and checks.

- The security based part of the GRC toolset for Access Control consists of:
  - Access Enforcer
  - Compliance Calibrator
  - Risk Terminator
  - Fire Fighter
  - Role Expert
4.2 Report RSUSR003

The check of standard user passwords with report RSUSR003 [transactions RSUSR003 or S_ALR_87101194]. Call transaction SE38 and enter RSUSR003, after that push F8.

---

**Check the Passwords of Standard Users In All Clients**

- **Display Profile Parameters**

**List Format**
- **Title**
- **Layout**

---

**Exhibit 4.2: RSUSR003**

This report serves to review relevant login parameter as well as to review the password of the SAP® standard users [remove checkmark from box *Display Profile Parameters*].

<table>
<thead>
<tr>
<th>Client</th>
<th>User</th>
<th>Lock</th>
<th>Password Status</th>
<th>Reason for User Lock</th>
<th>Inc Logs</th>
<th>Valid from</th>
<th>Valid through</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>DDIC</td>
<td>✔</td>
<td>Exists; Password not trivial.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SAP</td>
<td>✔</td>
<td>Exists; Password not trivial.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SAPCIC</td>
<td></td>
<td>Exists; Password not trivial.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Exhibit 4.3: RSUSR003 - result**

The report usually checks for the following authorizations:

```
CALL FUNCTION 'VIEW_AUTHORITY_CHECK'
  AUTHORITY-CHECK OBJECT 'S_TABU_DIS' ID 'ACTVT' FIELD ACTIVITY ID 'DIBERCLS' FIELD TODAT-CLASS
  AUTHORITY-CHECK OBJECT 'S_TABU_CLI' ID 'CLIOMAINT' FIELD 'X'
  AUTHORITY-CHECK OBJECT 'S_USER_GRP' ID 'CLASS' FIELD 'SUPER' ID 'ACTVT' FIELD '02'
```

**Exhibit 4.4: RSUSR003 – authorization check**

The authorizations are critical authorizations; therefore the access to this report was formerly to be restricted to selected individuals only. SAP® has introduced an authorization object that now allows executing this report in display mode only. Therefore this report can now even be assigned to auditors.
The name of the object is S_USER_ADM. The object has only one field S_ADM_AREA and can have the following values assigned:

**CHKSTDPWD**: Display special users with their passwords

**PRGN_CUST**: Change of Customizing table PRGN_CUST

**SSM_CUST**: Change of Customizing table SSM_CUST

For executing the report in display mode, the value **CHKSTDPWD** needs to be assigned. If this authorization is established in the user master, the previously listed authorizations are no longer necessary to execute the report.

```
PERFORM CHECK_GLOBAL_REPORT_SECURITY
  AUTHORITY-CHECK OBJECT 'S_USER_ADM' ID 'S_ADM_AREA' FIELD 'CHKSTDPWD'
```

Helpful OSS notes are: 704307 and 717123.

4.3 Report RSUSR008 [transaction S_BCE_68001401]

**By Critical Combinations of Authorizations at Transaction Start**

An evaluation of users with critical combinations of authorizations for transaction start may take some time.

You can reduce the processing time by restricting the selection of critical combinations.

Select the corresponding pushbuttons to display or maintain the "Crit. comb."

- View by Critical Combinations
- View by Users

*Exhibit 4.5: RSUSR008*

This report, together with the RSUSR009, is a predecessor of report **RSUSR008_009_NEW** and is classified as obsolete with 7.0.
SAP® delivers a set of predefined critical transactions that can be maintained. The table underneath where the transactions can be defined is the table SUKRI, a cross-client table.

You have to be aware, that any result provided in this report only shows the transactions that are assigned to the user. It does not provide any insight about the corresponding application authorizations that are required to successfully execute the transaction. With 7.0 the report can no longer be executed.

### 4.4 Report RSUSR009 [transaction S_BCE_68001403]

#### List of Users With Critical Authorizations

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Analyzing users with critical authorizations may take several minutes.

You can reduce the processing time by restricting the selection of critical authorizations.

Select the corresponding pushbuttons to display or maintain “Crit. auth.”

When maintaining critical authorizations, you must refer to the documentation (choose “?”).

- Check Using Customer Data
- Check Using SAP Data

Exhibit 4.6: RSUSR009

This report allows up to 7.0 to execute a check on predefined, or customer defined critical authorizations. The table underneath is the table USKRIAT [client independent table].
4.5 Report RSUSR008_009_NEW

Exhibit 4.7: RSUSR008_009_NEW

The report is an interface for the evaluation of critical authorizations and combinations of critical authorizations.

The following tables are relevant for this report:

TABLES: usrvarcom, uscrcomo, uscrcomid, uscrauth, usrvar, usrcombt, sscenfields, usrvarcount, ust16s, ust16c, ust04, ust12, usrvart, usrvard, uscrauthid, uscraudit, usrcomo, usr02, usgrp, usrefus, str_agrs, usrl0, tobl.

Exhibit 4.8: RSUSR008_009_NEW - tables

The maintenance for the tables that are supposed to contain the evaluation information is performed with the help of views.
For the maintenance of critical authorizations, you need to maintain a variant first, then you establish the IDs for the critical authorizations, and finally the authorization data need to be maintained.

The variants are maintained per view VUSRVARCOM [table USRVARCOM].

With the help of view VUSRVARID [table USRVARID] the part lists of the variants are maintained.

The view VUSCRAUTH [table USCRAUTH] allows the maintenance of the values for the critical authorizations that are defined via VUSRVARID [USRVARID].

SAP® provides a default set of IDs and data based on RSUSR009.

Exhibit 4.9: RSUSR008_009_NEW - customizing

The critical combinations have a similar structure, and are based on the information from the previously explained critical authorizations.

The variants are maintained via view VUSRCRCOMB [table USRCRCOMB]. The part list of critical combinations is maintained in view VUSCRCOMID [table USCRCOMID], which refers to the IDs of critical authorizations. The critical combinations of these critical authorizations are maintained in VUSRCOMB [table USRCOMB].
4.6 Report RSUSR010

[transaction S_BCE_68001426, S_BCE_68001427, S_BCE_68001428, S_BCE_68001429, S_BCE_68002041]

Exhibit 4.10: RSUSR010

This report provides a list of transactions that are assigned in the context of the selected category.

Double clicking onto a selected entry does not provide the details of the corresponding authorization, but of the standard relation within SU24 [table USOBT_C].

Exhibit 4.11: RSUSR010 – detail view
4.7 Report RSUSR020 [transaction S_BCE_68001409]  
transactions S_BCE_68001404, S_BCE_68001405, S_BCE_68001406, S_BCE_68001407, S_BCE_68001408, S_BCE_68001767

Profiles by Complex Selection Criteria

<table>
<thead>
<tr>
<th>Selection criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
</tr>
<tr>
<td>Profile text</td>
</tr>
<tr>
<td>Active version</td>
</tr>
<tr>
<td>Maint. version</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Additional selection criteria for profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comp. prof.</td>
</tr>
<tr>
<td>Single prof.</td>
</tr>
<tr>
<td>Generated profiles</td>
</tr>
<tr>
<td>Last changed by</td>
</tr>
<tr>
<td>Last change since</td>
</tr>
<tr>
<td>Last change up to</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Selection by contained profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Selection by authorizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization object</td>
</tr>
<tr>
<td>Authorization</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Selection by values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization object 1</td>
</tr>
<tr>
<td>Authorization object 2</td>
</tr>
</tbody>
</table>

Exhibit 4.12: RSUSR020

This report allows searching for profiles that correspond with the entered selection criteria.
4.8 Report RSUSR030

[transactions S_BCE_68001414, S_BCE_68001415, S_BCE_68001416, S_BCE_68001417]

Exhibit 4.13: RSUSR030

With the help of this report you can evaluate authorizations.

A selection for example on the authorization F_ANZ delivers the following:

Exhibit 4.14: RSUSR030 – detail view
Per double-click you can branch into the corresponding details and review the documentation for the authorization object or the values that are part of the authorization.

You can also utilize the interfaces to review change documents of selected entries or check where the authorization is used.

Exhibit 4.15: Where-Used-Search

### 4.9 Report RSUSR040

[transaction S_BCE_68001410, S_BCE_68001411, S_BCE_68001412, S_BCE_68001413]

**Authorization Objects by Complex Selection Criteria**

Exhibit 4.16: RSUSR040

This report helps to search for authorization objects.
4.10 Report RSUSR050 [transaction S_BCE_68001433]
[transaction S_BCE_68001430, S_BCE_68001431, S_BCE_68001432, S_BCE_68001777]

**Comparisons**

<table>
<thead>
<tr>
<th>User</th>
<th>Roles</th>
<th>Profiles</th>
<th>Authorizations</th>
<th>Across systems</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Exhibit 4.17: RSUSR050**

After pushing the button *Across systems*, you can enter available RFC destinations to connect to a target system to compare user, roles, profiles or authorizations across systems.

This report is a good tool to check and validate role changes in development phases, or user set ups across systems.

**Comparisons**

<table>
<thead>
<tr>
<th>User</th>
<th>Roles</th>
<th>Profiles</th>
<th>Authorizations</th>
<th>Across systems</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Exhibit 4.18: Comparison across systems**
4.11 Report RSUSR060OBJ

Where-Used List: Authorization Object in Program and Transactions

Exhibit 4.19: RSUSR060OBJ

After entering the authorization object, you can select the search range:

Exhibit 4.20: Search range

Where-used Authorization Object S_ADMIN_FCD in Programs (367 Hits)

Exhibit 4.21: Result list
Per double-click you can branch into the corresponding details as for example program integration:

Exhibit 4.22: Detail view

Where-used Authorization Object S_ADMI_FCD in Transactions (142 Hits)

<table>
<thead>
<tr>
<th>Transaction code</th>
<th>Short description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/SEF/PE</td>
<td>Project browser &amp; test environment</td>
</tr>
<tr>
<td>AL08</td>
<td>Users Logged On</td>
</tr>
<tr>
<td>AL11</td>
<td>Display SAP Directories</td>
</tr>
<tr>
<td>AL11_OLD</td>
<td>Display SAP Directories</td>
</tr>
<tr>
<td>AL12</td>
<td>Display table buffer (Exp. session)</td>
</tr>
<tr>
<td>AL13</td>
<td>Display Shared Memory (Expert node)</td>
</tr>
<tr>
<td>AL15</td>
<td>Customize SAPSCONL destination</td>
</tr>
<tr>
<td>BOA1</td>
<td>Call RSAFCCS</td>
</tr>
<tr>
<td>BWMSSPROCS</td>
<td>Transaction for MSS SP Maintenance</td>
</tr>
</tbody>
</table>

Exhibit 4.23: Transaction result

Or the details of the transaction set up in SE93:

Display Report Transaction

<table>
<thead>
<tr>
<th>Transaction code</th>
<th>Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>AL11</td>
<td>SMDS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transaction text</th>
<th>Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display SAP Directories</td>
<td>RSAFATCHO</td>
</tr>
<tr>
<td>Selection screen</td>
<td>1986</td>
</tr>
<tr>
<td>Start with variant</td>
<td></td>
</tr>
<tr>
<td>Authorization object</td>
<td>S_ADMI_FCD</td>
</tr>
</tbody>
</table>

Exhibit 4.24: SE93
4.12 Report RSUSR070 [transaction S_BCE_68001425]

Exhibit 4.25: RSUSR070

The transaction check is menu based.

For queries on roles that are not menu based, you would need to check on S_TCODE. This report is an excellent tool for role research.
4.13 Change documents

The change documents contain the relevant information to the authorization history.

4.13.1 Report RSUSR100

This report provides the change history of user authorizations as well as header data. Via click onto profile entries you can branch through down to the authorization history level.

**Change Documents for Users**

<table>
<thead>
<tr>
<th>Standard Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
</tr>
<tr>
<td>Changes by</td>
</tr>
<tr>
<td>From Date</td>
</tr>
<tr>
<td>From Time</td>
</tr>
<tr>
<td>To Date</td>
</tr>
<tr>
<td>To Time</td>
</tr>
</tbody>
</table>

**Output**

- List of Change History
- Table of Status History (User Attributes Horizontal)
- List of Status History (User Attributes Vertical)
- Technical View

<table>
<thead>
<tr>
<th>Selection Criteria for Changed Authorizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added Profiles (Profile Name: to)</td>
</tr>
<tr>
<td>Deleted Profiles (Profile Name: to)</td>
</tr>
<tr>
<td>Created Users</td>
</tr>
<tr>
<td>Deleted Users</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Selection Criteria for Changed Header Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator Lock Set</td>
</tr>
<tr>
<td>Administrator Lock Removed</td>
</tr>
<tr>
<td>Incorrect Logon Lock Set</td>
</tr>
<tr>
<td>Incorrect Logon Lock Removed</td>
</tr>
</tbody>
</table>

*Exhibit 4.26: RSUSR100*
4.13.2 Report RSUSR101

Change Documents for Profiles

Standard selections:
- Profiles: A_ANZEIGE
- Changes by: 
- Changes since: 
- Changes up to: 18.05.2008
- Changes to composite profiles
- Changes to single profiles

Additional selection criteria for profiles:
- OR operation
- AND operation
- Profiles added: 
- Profiles deleted: 
- Add to auth. object: 
- Delete from auth. objects: 
- Authorizations added: 
- Authorizations deleted: 

Exhibit 4.27: RSUSR101

For the additional selection logical operators can be chosen.

Change Documents for Profiles

<table>
<thead>
<tr>
<th>Prof.name</th>
<th>Date</th>
<th>Time</th>
<th>No.</th>
<th>Changed by</th>
<th>Action</th>
<th>Object</th>
<th>Auth.</th>
<th>Profile name</th>
</tr>
</thead>
<tbody>
<tr>
<td>A_ANZEIGE</td>
<td>12.06.1996</td>
<td>15:19:42</td>
<td>1</td>
<td>SAP</td>
<td>Created Entry</td>
<td>A_ANZ</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A_IMPR_ALL</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>F_BUCH_ALL</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X_COBL_ALL</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Exhibit 4.28: RSUSR101 - Overview

By clicking onto a profile name, you branch into the details:
Exhibit 4.29: Branch to authorizations

By clicking onto an object or authorization, you get the corresponding details of the change history for these elements.

4.13.3 Report RSUSR102

Exhibit 4.30: RSUSR102

Exhibit 4.31: Authorization details
4.13.4 Report RSSCD100_PFCG

Display Change Documents for Role Administration

- Parameters
  - Role Name: [Input Field]
  - Changed By: [Input Field]
  - From Data: [Input Field]
  - To Data: [Input Field]
  - From Time: [Input Field]
  - To Time: [Input Field]
  - Document Change Number: [Input Field]

- Change Documents
  - Create and delete roles
  - Role Description
  - Single Roles in Composite Roles
  - Transactions in Role Menu
  - Other Objects in Role Menu
  - Authorization Data
  - Organizational Level Value
  - Authentication Profile
  - Attributes
  - MiniApps
  - Composite Role Homepage
  - User Assignment
  - All Change Documents (Technical View)

- You can use wildcards in your input

Exhibit 4.32: RSSCD100_PFCG

For using the technical view, you can select the change documents per table.

<table>
<thead>
<tr>
<th>Table Name</th>
<th>Long Field Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGR_DEFINE</td>
<td>Create and delete roles</td>
</tr>
<tr>
<td>AGR_TEXTS</td>
<td>Role Description</td>
</tr>
<tr>
<td>AGR_AGORS</td>
<td>Single Roles in Composite Roles</td>
</tr>
<tr>
<td>AGR_OBJ</td>
<td>Transactions in Role Menu</td>
</tr>
<tr>
<td>AGR_BUFF1</td>
<td>Other Objects in Role Menu</td>
</tr>
<tr>
<td>CD1251</td>
<td>Authorization Data</td>
</tr>
<tr>
<td>CD1252</td>
<td>Organizational Level Value</td>
</tr>
<tr>
<td>CD1018</td>
<td>Authorization Profile</td>
</tr>
<tr>
<td>AGR_FLAG15</td>
<td>Attributes</td>
</tr>
<tr>
<td>AGR_MINAPP</td>
<td>MiniApps</td>
</tr>
<tr>
<td>AGR_HPAG1</td>
<td>Composite Role Homepage</td>
</tr>
<tr>
<td>AGR_USERS8</td>
<td>User Assignment</td>
</tr>
</tbody>
</table>

Exhibit 4.33: Tables for change history
4.13.5 SUIM – The User Information System

The *User information system* contains almost all of the previously mentioned reports. Call the transaction **SUIM** or else the report **RSUSRSUIM** via **SE38**.

Exhibit 4.34: SUIM
5 How to

5.1 How to adapt authority-check in reports

The procedure concerning the integration of an authority check to an ABAP/4® report is basically as described. In this example a SAP standard program is copied into the customer name space, and modified to meet the company specific needs.

1. Copy the SAP® Standard program into the customer name space:
   The original program is the report RSUSR003, the name of the copy in this case e.g. is ZZ_RSUSR003.

2. The entry of a developer key is required as long as you are not registered with a corresponding entry in the table DEVACCESS.

3. To validate whether an authority check already exists you may search for the string “authority-check” within the source code of the report copy. (CTRL + F)

Exhibit 5.1: Authority-check
Exhibit 5.2: Authority-check – source code

Via double-click you will directly branch into the corresponding line within the source code.

Exhibit 5.3: Authority-check in SE38

In this case the original authority-check is changed, but of course you may add or even create a complete different authority check:

```
AUTHORITY-CHECK OBJECT 'S_USER_GRP'
   ID 'CLASS' FIELD 'SUPER'
   ID 'ACTVT' FIELD '02' 'Andern
IF SY-SUBRC NE 0.
  * 041 Keine Berechtigung zum Anlegen von Benutzergruppe &
  MESSAGE E041(01) WITH ".
endif.
```

In this case the authority-check based on the object S_USER_GRP is changed. It is checked if the user has an authorization to create [01] for the user group AUDIT.
Execute the syntax check, and save the modifications. Activate the report. After that the report is successfully changed.

If the user has no corresponding authorizations [S_USER_GROUP with CLASS "AUDIT" and ACTVT "01" he will now get the following message:

Exhibit 5.4: Error message

If you want to integrate another object for the authority check, you can enter the syntax accordingly, like in the next example with the object F_BKPF_BUK:

* Berechtigung zur Pflege des Buchungskreises

  AUTHORITY-CHECK OBJECT 'F_BKPF_BUK'
    ID 'ACTVT' FIELD '01'
    ID 'BUKRS' FIELD '1000'.
  IF SY-SUBRC NE 0.

You may also add a user message to the source code as in the example before. Now the user will need a corresponding authorization on F_BKPF_BUK to execute the adapted report.
5.2 How to add an authorization object to a customer created transaction code

Call the transaction SU24 / SU22 [or SU24_OLD / SU22_OLD] to start the maintenance.

The transaction in this example currently consists of only one authorization object (S_TCODE) and is not listed in the table USOBT_C yet. Select the transaction you want to maintain.

Exhibit 5.5: SU24_OLD

Confirm your choice via F8 and double click the selected entry. The following message will be displayed.

Exhibit 5.6: Customizing request
Confirm the message with Enter. Select the target client.

Enter your request ID and confirm via Enter.

Select the item **Authorization objects** from the menu bar, and there the entry **Insert**.

* Exhibit 5.7: Insert

Choose the corresponding authorization object from the list or enter it directly.

* Exhibit 5.8: Authorization object

* Exhibit 5.9: Add mode

Confirm your choice.

The selected authorization object will be transferred to the list.
If you want this object to be called by the profile generator for maintenance you have to adapt the Check ID.

When you are finished with the maintenance, do not forget to save the adjustments.

At the call of the transaction **SE16N** with selection of the table **USOBT_C**, the maintained values for the corresponding transaction are added to the table.

---

**Exhibit 5.10: SU24_OLD view**

**Exhibit 5.11: Validation**
At the call of the profile generator with selection of the previously maintained self-created transaction, the adapted check values are displayed for further maintenance.

Exhibit 5.13: PFCG select
5.3 Table access – table protection

There are various transaction codes to access tables. You may use the popular ones like e.g. SE16, SE16N, SE17, SM30, SM31 etc.

All these transaction codes have one thing in common. To access tables an authority check based on two authorization objects is executed.

In a 640 BC system you deal with approx. 155.000 tables.
The tables are listed in the table DD02L [SAP tables].

Aside from a lot of other differences the tables can be divided into two groups:
1. cross-client tables and

Cross-client tables are tables that are valid for the whole system, and not only for one client.

Client-dependent tables are always valid for one client.

The classification is documented by a technical setting that can be reviewed by looking up the table DD02L.

Exhibit 5.14: DD02L

The column “client-specific” is relevant. The entry X means, that this is a client-specific table. If the field is entry, the table is a cross-client table.

In SAP® we deal with something like a two step table protection for maintenance.
First step
The first step is the general protection of tables that is covered by the authorization object \texttt{S\_TABU\_DIS}.

Everyone who wants to have a table access needs a corresponding authorization on \texttt{S\_TABU\_DIS}.

The object \texttt{S\_TABU\_DIS} consists of two fields.

The field \texttt{ACTVT} [activity] and the field \texttt{DICBERCLS} [authorization group].

Valid values for the field \texttt{ACTVT} are:

02 – for create, change, delete
03 – for display
BD – override change lock for customizing distribution

All possible \texttt{ACTVT} values are listed in the table \texttt{TACT}.

Concerning the values for the field \texttt{DICBERCLS} the assignment and selection is a bit more complex.

Tables are protected by so called authorization groups. The defined groups are listed in the table \texttt{TBRG}.

The assignment of tables to authorization groups is listed in the table \texttt{TDDAT}.

Every table can only have one authorization group.

But every authorization group may protect a number of tables.

\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|}
\hline
Table & Authorization & Authorization Group \\
\hline
TOOS & 01 & BA \\
TOOSD & 0A & \\
TOOSDCM & FGB1 & \\
TOOSD & 0NCS & \\
TOOSF & FGB1 & \\
TOOSH & 0NCS & \\
TOOSO & 0C & \\
TOOSQL & 0C & \\
TOOSK & FKOB & \\
TOOSH & MORD & \\
\hline
\end{tabular}
\caption{Display of Entries Found}
\end{table}

\textit{Exhibit 5.15: TDDAT}
Tables that are not especially protected by an explicitly defined authorization group are protected by the authorization group &NC&. “NC” stands for hereby for “non classified”.

So that we can conclude as a rule, that for access to tables an authorization on the object S_TABU_DIS with a corresponding ACTVT as well as a matching authorization group is required.

**Second step**
The second step in the table access control is based on the object S_TABU_CLI. The object consists of only one field: CLIDMAINT. The value for this object is X [indicator for cross-client maintenance].

The object S_TABU_CLI is the object that especially protects the client-independent, means the cross-client tables. All cross-client tables experience additional protection through this object. The indicator X does not automatically allow maintenance, the access scope is still limited through the field values in ACTVT of the object S_TABU_DIS. But maintenance of cross-client tables cannot be executed without an authorization on S_TABU_CLI.
Summary
For accessing client dependent tables an authorization on the object S_TABU_DIS is required.

For accessing cross-client tables for maintenance an authorization on the objects S_TABU_DIS and S_TABU_CLI is required.

Remark
The object S_TABU_LIN was created for further table access limitation. S_TABU_LIN allows an access granularity down to the line level of the tables.
This is connected to special customizing adjustments, the definition and activation of so-called organizational criteria. With the predefinition of organizational criteria like e.g. a plant or a country, access to tables can then be limited to the lines of the organizational criteria only.

Because of the additional complexity of these fine tuning requirements [customizing on-line], this is rarely used in companies so far.
5.4 Protection of reports / ABAP®s

The protection of reports is set up according to the same principle as the protection of tables, only that SAP® does not provide many standard assignments. The assignment to users succeeds with the authorization object S_PROGRAM. The authorization object consists of two fields. First the field **User action ABAP/4 program** and secondly the field **authorization group ABAP/4 program**. The assignment succeeds with the latter.

You can get an overview of the already maintained assignments with the table **TRDIR** via transaction code **SE16N**. An authorization group would be entered to the field **SECU** (authorization group).

![TRDIR Table Display](image)

Exhibit 5.16: TRDIR

The maintenance for the assignment of reports to authorization groups can be executed with the report **RSCSAUTH** via transaction **SE38/SA38**.
SAP® does not provide many entries here, as already mentioned.

You can however enter the desired values in the field Customer with the help of this report and have it saved. These maintained values will then be directly transferred into the table TRDIR.

SAP® offers several options to analyze programs to check if an authority-check is integrated. Transaction SE38 allows calling the APAP/4® Editor for review of the source code and corresponding documentation.

Exhibit 5.17: RSCSAUTH

Exhibit 5.18: SE38
Enter the name of the report you want to analyze, activate the radio button for the desired information and push the button Display.

The report **RSANAL00** [can be called via transaction **SE38** or **SA38**] helps to analyze ABAP/4® programs.

**Exhibit 5.19: RSANAL00**

Other reports that are available for the source code analysis are **RPR_ABAP_SOURCE_SCAN** and **RSABAPSC** [both can be called via **SE38/SA38**]. These reports allow to search for specific strings, like e.g. “authority-check”, or “EXEC SQL”.

**RPR_ABAP_SOURCE_SCAN** checks through all recurrence levels.
### Exhibit 5.20: Source code scan

In RSABABSC you can enter the desired depth for the search.

### Statistical program analysis to find ABAP lang. commands

Exhibit 5.21: RSABAPSC
You can also call the transaction **SE38**. Enter the name of the program and click the button **Display**. Within the view of the source code you may select the menu item **Edit – Search/Display** or you click the button **Find** (CTRL+F).

Enter the string „authority-check“ and select the search area „in program“. As a result, in all included programs it will be searched for this string.

![String search](image)

**Exhibit 5.22: String search**

All detected entries will be displayed:

![Search result](image)

**Exhibit 5.23: Search result**
With double-click on one entry you directly branch to the source code of the corresponding point.

```
authority-check object 'F BKPF_BUK'
  id 'ACTVT' field l_actvt
  id 'BUKRS' field p_bukrs.
  if sy-subrc ne 0.
    case g_status.
      when char_1.
        message e083 with p_bukrs.
      when char_2.
        message e006(fp) with p_bukrs.
      when char_3.
        message e086(fp) with p_bukrs.
      when char_4.
        message e049(fp) with p_bukrs.
      endcase.
    endif.
endform.  " authority_bukrs
```

*Exhibit 5.24: Source code review*

Beside this kind of authorization check, it is possible that the authorization check is not directly executed within the source code but through the integration of function modules.

Some function modules for example are:

**VIEW_AUTHORITY_CHECK**

**AUTHORITY_CHECK_TCODE**

**AUTHORITY_CHECK_DATASET**

These function modules are used within other function modules as well as in programs. The „Where-used list“ can be checked with the help of the transaction SE37.
Enter the corresponding function module and activate the button „Where-used list“.

Make the following selection:

You get this hit list.

For a better distinction between programs and function modules you may refer to the name conventions of reports by SAP®.
5.5 Export of tables for an authorization check

The check of access authorizations with SAP® standard means is only possible to a certain extent. For more complex questions (who is allowed to post within the company code 1000, business area 2000, posting period 11 the document type DR) the call of several reports is required. These reports are then to be compared manually (in this example three times the report RSUSR002).

A more effective possibility for these kind of checks results from the export of the corresponding tables into a database (e.g. ACCESS, dBASE, IDEA or ACL).

The following aspects are to be considered at the export:

- the export should succeed via the transaction SE16N
- the export should succeed in an unconverted format
- prior to the display of tables a selection mask will be displayed. There, the maximum number of hits is restricted as a standard, to 500 data records. This value has to be set higher, set it on a high value that cannot be reached, such as 12,000, or delete the entry completely out of the field.

Every table can be saved as a file for further processing procedures. Please select the button.

Select the corresponding format:

Exhibit 5.29: Download
Confirm your choice and select the path for the local file transfer and enter a name for the file:

![Transfer List to a Local File](image)

**Exhibit 5.30: Download path**

Finally you activate the button *Transfer*. The data will now be transferred to the file and can be edited with an associated application.

Another possibility within the transaction **SE16N** is the direct data export through an integrated interface into associated programs like MS®Excel.

![Spreadsheet](image)

**Exhibit 5.31: Download options**

For the export to Excel® the following edit options will be at your disposal:

![Export list object to XSL](image)

**Exhibit 5.32: Excel® options**
As a rule, the entry table is to be preferred:

Exhibit 5.33: Table download

5.6 The SAP® system trace

SAP® offers with the system trace the opportunity to evaluate the authorization objects that are checked during the call of the different transactions.

With the help of the trace all authorization objects on which an authority check is executed while working with the system can be logged. This also includes the corresponding field values within the authorization objects.

Call the transaction **ST01** for the use of the system trace.

Exhibit 5.34: ST01 in 4.7

In the selection screen the different components can be activated via checkmark.
Exhibit 5.35: ST01 Filter

There are options for additional filter settings. Push the button *General Filters*. You can filter for the process you want to log, the user, the transaction, or the program.

Enter the required selection, push the key *Enter*, and then activate the trace.

**Note:** An activation of the trace for all system users should not be activated. For user evaluation always enter the username you want to analyze.

With activation of the trace all required access rights for the selected user will be logged.

When all actions are traced, and logged, then please switch the *Trace off*. After that you can evaluate the results by pushing the button *Analysis [or key F2]*.

The evaluation path varies in dependency of the current release level.

A. from release 4.7:

Exhibit 5.36: ST01 higher 4.7
Activate the integrated button *Analysis*. Enter the required selection for evaluation, and push the key *F8* for activation.

Aside from the selection of the different trace components, you can narrow down the selection according to users, transactions work process, or times. In the context of performance analysis you can select a restriction in the field duration, which is not very useful for an authorization trace. Additionally an evaluation with consideration of tables can be set up, which might be helpful for SQL or table buffer traces.

B. up to release 4.6D:

Exhibit 5.37: Trace analysis

Exhibit 5.38: Trace files
Double-click onto the displayed file name. Select the required information in the dialog box, and activate the button **Analysis**.

**Trace in a multiple instance environment**

In case you run SAP® on different instances you have to make sure that you activate the trace for the instance on which the user is executing the transactions that need to be logged for evaluation. Users can be active on more than one instance.

[The user instance information is displayed down on the right in the SAP status bar.] You can review, and even change to the corresponding instance, with the help of transaction **SM51**.

Select the instance you want to review. Activate the button **User Info** [CTRL+SHIFT+F7]. Select the user from the correspond list. Mark the entry. In the menu bar select the path **Goto – Terminals**. Select the user. In the menu bar select the path **Goto – Remote Server**. From here you can activate the trace for the instance on which the user is located.

The trace evaluation

![Trace results](image)

Exhibit 5.39: Trace results

For interpretation of the evaluation you can use the following overview of relevant information.
<table>
<thead>
<tr>
<th>Element</th>
<th>Info</th>
<th>Additional info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Exact million second.</td>
<td>Per double-click onto the selected entry you branch to the detail view.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of the corresponding trace entry</td>
<td>Display of the selected trace component. See component overview</td>
</tr>
<tr>
<td>Duration</td>
<td>Duration of the trace</td>
<td>Not useful for authorization trace</td>
</tr>
<tr>
<td>Object</td>
<td>Objekt in dependency of the related component</td>
<td>See: component overview</td>
</tr>
<tr>
<td>Trace-message text</td>
<td></td>
<td>Per double-click onto the selected entry, you branch into the detail view. From there, you can branch into the related ABAP source code.</td>
</tr>
</tbody>
</table>

Please find the component overview with corresponding acronyms.

<table>
<thead>
<tr>
<th>Component</th>
<th>Acronym</th>
<th>Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization check</td>
<td>AUTH</td>
<td>Authorization object</td>
</tr>
<tr>
<td>Kernel-Functionen</td>
<td>CMOD</td>
<td>Related C-function in kernel</td>
</tr>
<tr>
<td>Kernel general</td>
<td>USER</td>
<td>C-Modul in Kernel, in which the trace is written</td>
</tr>
<tr>
<td>DB-access (SQL-Trace)</td>
<td>SQL</td>
<td>DB-Table that was accessed</td>
</tr>
<tr>
<td>Table buffer-Trace</td>
<td>BUFF</td>
<td>DB- that was accessed</td>
</tr>
<tr>
<td>RFC-call</td>
<td>RFC</td>
<td>Called function module</td>
</tr>
<tr>
<td>Lock operation</td>
<td>ENQUE</td>
<td>Lock object</td>
</tr>
</tbody>
</table>
The return code
Successfully passed authorization check are marked in dark green already and have the value $RC=0$ added in the column next to the authorization object.

RC is the acronym for return code. The return values vary depending on the check result.
The return code 0 means that the authorization was successfully checked.
The return code 4 says, that the required authorization for the authorization object in the user master is not available.
The return code 12 says, that no authorization for the authorization object is available.

Saving of trace results
There are different ways to save trace evaluation results.
You can download the trace file in the evaluation display mode by saving the list locally.
If trace information are to be protected against overwriting, you have to branch to the button Save after tracing.

Exhibit 5.40: ST01

In the following window you can enter remarks as well as a file name.
### Restrictions on Saving Trace Records

<table>
<thead>
<tr>
<th>General Restrictions</th>
<th>Trace Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name: MLWAGENER</td>
<td>+ Authorization check</td>
</tr>
<tr>
<td>Client: 100</td>
<td>+ Kernel Functions</td>
</tr>
<tr>
<td>Work Process:</td>
<td>+ General Kernel</td>
</tr>
<tr>
<td>Transaction:</td>
<td>+ DB Access (SQL Trace)</td>
</tr>
<tr>
<td>Duration (&gt;us):</td>
<td>+ Table Buffer Trace</td>
</tr>
<tr>
<td>Mail. No. Records: 19,808</td>
<td>+ RFC calls</td>
</tr>
<tr>
<td>From: 12.05.2007 13:33:01</td>
<td>+ Lock operations</td>
</tr>
<tr>
<td>To: 12.05.2007 13:48:01</td>
<td></td>
</tr>
</tbody>
</table>

#### Exhibit 5.41: Trace saving

If you do not enter an absolute path when entering the file name manually, the file will be created in the log directory.

For the automatic file name creation, the system provides a file name, and creates the file in the log directory.

Automatically created file names can be selected with the *F4* search key in the future. This option is not available for manually created names.

Automatically created file names can be deleted within this application, manually created file names need to be deleted on the OS level separately.

Therefore the automatic file name creation is to be preferred.

#### Trace configuration

The system trace is configurable through different profile parameters. All trace relevant parameters are part of the category `rstr/`

To review the parameters the transaction **RZ11** can be used.

The following parameters are adjustable.
<table>
<thead>
<tr>
<th>Profile parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **rstr/buffer_size_kB**    | The SAP-Trace (SQL-Trace u.a.) writes the trace data into trace files. Because of performance issues this is not done directly but through a process internal buffer. The profile parameter 
**rstr/buffer_size_kB** determines the size of this buffer in kilobytes. |
| **rstr/filename**          | Since release 6.10 the SAP-Trace (SQL Trace etc..) saves the data in different files, that are sequentially written. The Parameter 
**rstr/filename** establishes the basic name of these files. There is always only one file with this name. If the file is full (parameter 
**rstr/max_filesize MB**), the file is renamed and a new file with the basic name is created. During the renaming a file extension with the numbers 00 to 99 is added to the file name. The parameter 
**rstr/max_files** determines, how many files there will be altogether. If this number is exceeded, the files will be overwritten. |
| **rstr/max_files**         |                                                                                                                                               |
| **rstr/max_filesize MB**   |                                                                                                                                               |

The system trace cannot only be used for the evaluation of authority checks, but also for evaluation of kernel functions, kernel modules, DB access, table buffer, RFC calls and lock operations. For system monitoring the developer trace is usually preferred.
5.7 Transaction SE16N – risk and control

The transaction code SE16N [report RK_SE16N] offers some options for table maintenance activities, if the corresponding authorizations are assigned as well. But together with this risk, SAP® provides an integrated control that can be used for review.

First of all we have to understand how the maintenance activities can be executed:

1. Call the transaction SE16N.

2. Enter the name of the table you want to maintain into the corresponding field.

Some tables already offer integrated maintenance functionality. This is then represented by an activation of the checkmark in the checkbox: Maintain entries.

For the tables that do not offer this option automatically you have to choose a different path.

To activate the general maintenance functionality you have to enter the following:
3. **&SAP_EDIT**

![Table Display](image)

**General Table Display**

<table>
<thead>
<tr>
<th>Table</th>
<th>TOB1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Testtable</td>
<td></td>
</tr>
<tr>
<td>Layout</td>
<td></td>
</tr>
<tr>
<td>Maximum no. of hits</td>
<td>500</td>
</tr>
</tbody>
</table>

**Exhibit 5.43: &SAP_EDIT**

Confirm your entry with “Enter”.

4. You will then get the following message displayed:

![Message](image)

**Exhibit 5.44: Message**

5. Generate the table view with the help of the key *F8*.

![Display of Entries Found](image)

**Exhibit 5.45: Edit mode**

This way the table fields can be maintained.
The above described table maintenance will only work for the tables that were already available when using the transaction SE16.

The maintenance protection is part of the technical adjustments for the table. Table maintenance in a production system always represents a critical risk, especially because not all changes are properly logged. Only changes to tables with tax relevant content are logged per default if the correspondent system adjustments [system parameter: rec/client] are correctly adapted. The advantage in using the transaction SE16N consists in the fact, that the accompanying changes are logged as well as the responsible users. The data changes are stored in the table SE16N_CD_DATA

![Table Display: Change Documents - Data](Image)

Exhibit 5.46: SE16N_CD_DATA

Exhibit 5.47: Data record

The responsible user is listed in the table SE16N_CD_KEY, together with the modification date and time.

![Table Display: Change Documents - Header](Image)

Exhibit 5.48: SE16N_CD_KEY
The change document tables are protected and cannot be maintained by this means.

Exhibit 5.49: SE16N_CD_KEY edit

Changes to the production system always require comprehensible documentation.

With the help of these tables system traceability is available.
5.8 Transaction SE16 – risk and control

The transaction code **SE16** in combination with critical authorizations allows some highly critical steps within a SAP® system.

For this example you call the transaction code **SE16**, and enter the table name **TGSB** to the selection field. After selecting one special entry via double-click, you will then get e.g. the following window displayed:

![Exhibit 5.50: TGSB](image)

The table fields are currently protected against maintenance. [This is represented by the grey colour].

In this next view the debugging function is activated via corresponding entry of /h to the command line [/*h – enter*/].

![Exhibit 5.51: Debug mode](image)
In the next step the string **CODE** is entered to the *Field name* and **EDIT** to *Field contents*.

After that the *Pencil Button* is activated and the settings are saved. At this moment an additional authorization check based on the object S DEVELOP for activity 02 [replace/change] is executed.

<table>
<thead>
<tr>
<th>Project</th>
<th>S DEVELOP</th>
<th>ABAP Workbench</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project class</td>
<td>BC_C</td>
<td>Basis - Development Environment</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity</td>
<td>C2</td>
</tr>
<tr>
<td>Package</td>
<td>FBASCORE</td>
</tr>
<tr>
<td>Object name</td>
<td>TGBG</td>
</tr>
<tr>
<td>Object type</td>
<td>TABL</td>
</tr>
<tr>
<td>Authorization group</td>
<td>ABAP/4 program</td>
</tr>
<tr>
<td></td>
<td>&lt;Dummy&gt;</td>
</tr>
</tbody>
</table>

*Exhibit 5.52: Authorization requirements*

After saving of the adjustments, and running of the function *F8*, the corresponding field entries are opened for maintenance.

*Exhibit 5.53: Edit*

A test change is executed and saved

*Browser: Table TGB Select Entries 1*

*Exhibit 5.54: Change*
This event is logged within the SysLog [SM21].
The event ID is **A19** change of field content for **A14** program, line, and event.
But you will not be able to trace the former setting of the field.
This is also valid for the transaction codes based on **SE16** that have a table directly assigned, like e.g.:

```
SE16RFCDESSECU
SE16T000
SE16TXCOMSECU
SE16USR40
SE16USRACL
SE16USRACLEXT
SE16V_T599R
SE16W3TREES
SE16WWWFUNC
SE16WWWREPS
SE16_ANEA
SE16_ANEK
SE16_ANEP
SE16_ANLA
SE16_ANLC
SE16_ANLP
SE16_ANLZ
SE16_BKPF
SE16_BSEG
SE16_BSID
SE16_BSIK
SE16_BSIS
SE16_ECMCA
SE16_ECMCT
SE16_KNA1
SE16_KNB1
```
SE16_LFA1
SE16_LFB1
SE16_MARA
SE16_MARC
SE16_RFCDESSECU
SE16_SKA1
SE16_SKB1
SE16_T000
SE16_T807R
SE16_T CJ_CHECK_STACK
SE16_T CJ_CPD
SE16_T CJ_C_JOURNALS
SE16_T CJ_DOCUMENTS
SE16_T CJ_POSITIONS
SE16_T CJ_WTAX_ITEMS
SE16_TXCOMSECU
SE16_USR40
SE16_USRA CL
SE16_USRACLE XT
SE16_V_T599R
SE16_W3TREES
SE16_WWWFUNC
SE16_WWWREPS
5.9 SAP® NetWeaver security parameter

The SAP® NetWeaver is a comprehensive application and integration platform that consists of several components and tools. Important components are e.g. the NetWeaver Application Server, NW Business Intelligence, NW Exchange Infrastructure, NW Master Data Management, NW Mobile, NW Portal, Auto-ID infrastructure, NW Identity management. Relevant tools are e.g. Adaptive Computing Controller, NetWeaver Composition Environment, NW Developer Studio, NW Visual Composer, and SAP® Solution Manager.

Just like for the former basis kernel the security of this platform is controlled by corresponding system security parameters. The following overview provides a short introduction in the relevant aspects of selected parameters.

You can review the current settings with the help of the report RSPFPAR or RSPARAM [via transaction SE38 e.g]. The parameter change history is available through transaction TU02.

The system profile parameters are stored in files on the operation system level [an instance, a start and default.pfl] and are supposed to configure the different instances.

Dynamic parameters can be changed on the fly, while for static parameters a restart of the corresponding instance is necessary to activate the setting.

---

1 NW = SAP® NetWeaver
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Recommended</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>login/min_password_length</td>
<td>6</td>
<td>6-8</td>
<td>Controls the minimum length of a password. Possible entries: 3-40 [until NW 6.4 up to 8]</td>
</tr>
<tr>
<td>login/min_password_digits</td>
<td>0</td>
<td>1-2</td>
<td>Controls the minimum number of digits [0-9] in a password. Possible entries: 0-40 [until NW 6.4 up to 8]</td>
</tr>
<tr>
<td>login/min_password_letters</td>
<td>0</td>
<td>1-2</td>
<td>Controls the minimum number of letters [A-Z] in a password. Possible entries: 0-40 [until NW 6.4 up to 8]</td>
</tr>
<tr>
<td>login/min_password_specials</td>
<td>0</td>
<td>1-2</td>
<td>Controls the minimum number of special characters in a password, such as !&quot;@ $%^&amp;/()=?’`*+~#-_.,;:{[]}&lt;] and space Possible entries: 0-40 [until NW 6.4 up to 8]</td>
</tr>
<tr>
<td>login/min_password_lowercase</td>
<td>0</td>
<td>1-2</td>
<td>Controls the minimum number of lower-case letters in a password. Possible entries: 0-40 [after NW 6.4]</td>
</tr>
<tr>
<td>login/min_password_uppercase</td>
<td>0</td>
<td>1-2</td>
<td>Controls the minimum number of upper-case letters in a password. Possible entries: 0-40 [after NW 6.4]</td>
</tr>
<tr>
<td>login/password_charset</td>
<td>1</td>
<td></td>
<td>0 – restrictive. Only letters, digits and the following special characters are allowed !&quot;@ $%^&amp;/()=?’`*+~#-_.,;:{[]}&lt;] and space in a password. 1 – downwards compatible. The password may consist of various characters [incl. national specialties, such as e.g. ä, ö] All characters aside from the above listed will then be stored as one special character, and can therefore not be differentiated. 2 – not downwards compatible. The password may consist of any character and will be stored in UTF-8 format [Unicode]. If the system does not support unicode, not every character can be entered during login. This parameter should only be set to 2, if the systems support the code.[with rel. 6.4]</td>
</tr>
<tr>
<td>Parameter</td>
<td>Default</td>
<td>Recomm.</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>login/min_password_diff</td>
<td>1</td>
<td>2-3</td>
<td>Controls the number of characters that have to be different from the previous password. Possible entries: 1-40 [until NW 6.4 up to 8]</td>
</tr>
<tr>
<td>login/password_expiration_time</td>
<td>0</td>
<td>30-90</td>
<td>Controls the number of days, after which a password change is required. Possible entries: 0-1000</td>
</tr>
<tr>
<td>login/password_history_size</td>
<td>5</td>
<td>12</td>
<td>Controls the number of passwords that are stored as history and cannot be used</td>
</tr>
<tr>
<td>login/password_change_waittime</td>
<td>1</td>
<td>&lt;30-90</td>
<td>Controls the number of days a user has to wait to be allowed to change his password again. Possible entries: 1-1000 [after NW 6.4]</td>
</tr>
<tr>
<td>login/disable_multi_gui_login</td>
<td>0</td>
<td>1</td>
<td>Controls whether multiple logins are enabled or disabled. 0 = enable 1 = disable</td>
</tr>
<tr>
<td>login/multi_login_users</td>
<td>No entry</td>
<td></td>
<td>Here a list [user ID] can be deposited that would allow users a multiple login even though the multi login is generally disabled. The multiple login information are stored in the table URSR41_MLD</td>
</tr>
<tr>
<td>login/system_client</td>
<td>Produ...</td>
<td></td>
<td>Controls the suggested client number for login. The common client for each system should be entered here.</td>
</tr>
<tr>
<td>login/fails_to_session_end</td>
<td>3</td>
<td>&lt;=</td>
<td>Controls the number of false login attempts after which the session is ended. The session can be restarted, with continuous login attempt until the user is locked by the corresponding setting in login/fails_to_user_lock.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Default</td>
<td>Recom.</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>login/fails_to_user_lock</td>
<td>5</td>
<td>3-5</td>
<td>Controls the number of false login attempts until the user is locked. Possible entries: 1-99</td>
</tr>
<tr>
<td>login/failed_user_auto_unlock</td>
<td>0</td>
<td>0</td>
<td>Controls if the user ID stays locked after false login attempts or not. 0- the ID will stay locked until manually unlocked 1 – the ID will automatically be unlocked after midnight.</td>
</tr>
<tr>
<td>login/no_automatic_user_sapstar</td>
<td>1</td>
<td>1</td>
<td>Controls the activation of the ID SAP* after deletion. [OSS note 2383 and 68048]. If the parameter is set to 1, no one can logon with SAP* and the password PASS in case the ID was for example accidentally deleted. SAP* is not recommended to be used as an emergency user. It is recommended to establish a separate, especially protected emergency user ID as part of an emergency user concept [please also see SAP Security Guide II].</td>
</tr>
<tr>
<td>rdisp/gui_auto_logout</td>
<td>0</td>
<td>900-1800 [maybe in combination with network security]</td>
<td>Number of seconds, after which an inactive user is automatically disconnected from the GUI. Possible entries: any numeric value</td>
</tr>
<tr>
<td>Parameter</td>
<td>Default</td>
<td>Recom.</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>---------</td>
<td>--------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>login/password_downwards_compatibility</td>
<td>1</td>
<td>0-2</td>
<td>Controls the downwards compatibility of password security. 0 – no downwards compatibility. The system only generates only new hash values that cannot be interpreted by older kernel versions. 1 – the system internally generates downwards compatible hash values, but does not evaluate them upon logon. This setting is required in a CUA controlled landscape with systems that have older kernel releases. 2 – the system generates downwards compatible hash values and checks them logged in system log upon failed login attempts to detect compatibility issues. The login fails. 3 – as 2, but with successful login 4 – as 3, but without system log entry. 5 – completely downwards compatible. [after NW 6.4]</td>
</tr>
<tr>
<td>login/password_compliance_to_current_policy</td>
<td>0</td>
<td>1</td>
<td>1 - The system check during login if the password is compliant with the password security settings. If not, a password change will be enforced. 0 – no check Users of type Service and system are generally excluded from password change requirements. [after NW 6.4]</td>
</tr>
<tr>
<td>login/disable_password_logon</td>
<td>0</td>
<td></td>
<td>Controls the deactivation of password logon, in case of Single Sign On integration e.g. 0- password enabled 1 – password logon only enabled for users that are listed in login/password_logon_usergroup 2 – password no longer possible</td>
</tr>
</tbody>
</table>
Parameter | Default | Recom. | Description
--- | --- | --- | ---
login/password_logon_usergroup |  |  | Here a list [user ID] can be deposited that would allow users a password login even though the password login is generally disabled.

login/password_max_idle_productive | 0 |  | Controls the number of days that may pass from the last password change of a user to his next logon. After that period of time, the password is rejected.
0 – unlimited validity
1 – only valid for same day
>1 – number of days before rejection

login/password_max_idle_productive | 0 | < 30 | Controls the number of days an initial password is valid after creation.
0 – unlimited
Possible entries: 0-24.000
[after NW 6.4]

The definition of illegal passwords is set up by maintaining entries for the table **USR40**.

There you can enter passwords that you want to exclude from usage in your company, as they might be easy guessed – for example the company name, address etc..

Wild cards can be used like *01, *02, or Quarter* etc.

⚠️ Please never enter a * as single entry.

Please be aware that a communication of the corresponding entries will help to reduce confusion; an additional short introduction into the risks of low level passwords security may also help to increase the level of user security compliance.
5.10 The evaluation of the SysLog – SM21

The SysLog is an acronym for “System Logging”. Selected events and problems within a SAP® system are generally logged. The information are written into text files that are saved on the operation system level. The exact location can be identified with the help of the system parameter DIR_LOGGING.

Call the transaction SA38, and enter the report name RSPFPAR, push the key F8.

Enter the parameter name, and activate the execution via F8.

<table>
<thead>
<tr>
<th>Display Profile Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="" /></td>
</tr>
</tbody>
</table>

Profile parameter: DIR_LOGGING
Display unsubstituted?
With short description

Exhibit 5.55: RSPFPAR

The name of the local file can be identified with the help of the parameter rslg/local/file.

The cross-client information are written sequentially into this file until the maximum file size is reached. The size is controlled via the parameter rslg/max_diskspace/local. When the maximum limit is reached a new file will be created, and the old file will be saved as copy. This copy can be identified with the help of the parameter rslg/local/old_file. SAP® only saves one copy at a time. That means if the new file has reached the maximum size, it will be saved as a copy, and with this, the former copy will be overwritten.

A system log is written for every instance. If you run on multiple instances you have to make sure that you look up all corresponding log information. UNIX systems allow a central logging in that way, that the locally saved information can be send to a central instance [parameter rslg/central/file].
For evaluation of the records, please call the transaction SM21 [the report RSLG0001 can be used as equivalent].

To check all remote instances at the same time [which is to be preferred due to efficiency] you have to select the menu path:

**System log – Choose - All remote system logs**

Select then the menu path: *Edit – Expert mode*.

![Exhibit 5.56: Expert mode](image)

You can modify the layout via the menu path *Goto – Layout*:

![Exhibit 5.57: Layout options](image)
The required authorizations for the evaluation are

S_TCODE with TCD value SM21
S_ADMI_FCD with S_ADMI_FCD value SM21

The following events and messages are important for audit and security reviews, and can be selected via the integrated button Message IDs.

**System Log: Further Restrictions**

<table>
<thead>
<tr>
<th>Further restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of Messages as Further Restriction:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Only these messages:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>All Except These Messages:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>R1 4</td>
</tr>
<tr>
<td>R1 9</td>
</tr>
<tr>
<td>R1 9</td>
</tr>
<tr>
<td>R8 3</td>
</tr>
<tr>
<td>B X</td>
</tr>
<tr>
<td>B X</td>
</tr>
<tr>
<td>F 4</td>
</tr>
<tr>
<td>G E</td>
</tr>
<tr>
<td>L C</td>
</tr>
<tr>
<td>R B</td>
</tr>
<tr>
<td>R B</td>
</tr>
<tr>
<td>U S</td>
</tr>
<tr>
<td>U S</td>
</tr>
<tr>
<td>U S</td>
</tr>
<tr>
<td>U S</td>
</tr>
<tr>
<td>U S</td>
</tr>
<tr>
<td>A U</td>
</tr>
<tr>
<td>A U</td>
</tr>
<tr>
<td>A U</td>
</tr>
<tr>
<td>A U</td>
</tr>
<tr>
<td>A U</td>
</tr>
</tbody>
</table>

**Exhibit 5.58: Log restrictions**

You can get the full scope of possible entries by calling the table TSL1D via transaction SE16N.
A19 allows to review if a field content was changed in debug mode e.g., which is not allowed in a production environment. Together with the entries in A14 you can even evaluate with which program, and which line.

With BXF you can see if the table logging was deactivated in a program by a user. GEW shows if the authorization check for the lock management via SM12 was deactivated.

LC0 displays if a user has executed logical os commands. F04 provides the information about deletion of DB tables. ROL allows you to see if a program was set to debug mode by a user.

ROS displays manually inactivation of the update, R0T the manual activation, and R0U shows if an update request was deleted. With R0W you can see if a terminated update was reposted. With R0Y you can show that terminated updates were displayed with SM13. And R65 shows, that an update was terminated. US2 shows if the user SAP* was deleted, and by whom.

AUP which transaction was locked, and with AUQ you can also see if, and which transaction was unlocked.

With AUE to AUI you can keep track of changes to the audit configurations of the Security Audit Log.

In the log, you can call the detail view via double click onto a selected entry.

Important note:

Please make sure that the access to the log files on the os level is restricted, and that the files are properly protected against unauthorized manipulations, or even deletion.
5.11 Segregation of duties in the financial accounting (Asymmetric approach)

In the financial accounting the change of bank data of vendor master data is usually regarded as a critical change, together with additional processing authorization even more so. Quite a number of departments try to leverage this risk by additional internal controls like e.g. signature authorizations that are part of an additional paper workflow.

To reduce the risk of the permeable controls to zero, the implementation of an asymmetric segregation of duties is to be considered.

In departments with lack of resources a fully system-controlled segregation of duties is not always applicable. All employees would need the authorization to create and change master data e.g.

With this methodology for segregation of duties, employee A can change the affected part of the master data. The master record is blocked for any further activities [payment run etc.], until a confirmation of this change is executed by employee B.

Information

Change to general data must be confirmed

Exhibit 5.59: Change vendor

Employee B has to validate the changes [Original of change notification compare to actual change including verification, e.g. telephone call].
Exhibit 5.60: Confirm changes

To check which data have been changed can be branched via the integrated button:

Vendor Changes: Overview

<table>
<thead>
<tr>
<th>Changed Fields</th>
<th>Entries</th>
<th>Deletions</th>
<th>Field Names</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Exhibit 5.61: Change overview

After successful validation employee B will confirm the changes and the master data is released for all succeeding actions after that.

In case of discrepancies employees B can decline the changes. The master data will be blocked for further activities until an agreed change is applied including confirmation.

The asymmetric approach results from the fact, that employee A cannot release his own changes.

As not all changes to vendor master data need to be considered as highly critical, the focus is usually on payment relevant data such as bank data.

The asymmetric approach allows the definition of fields that require additional protection in case of changes. The segregation of duties is then reduced to these fields only. Changes to telephone numbers e.g. can then be executed without additional control.
How can that be applied?

**Step 1:**

The fields that are supposed to be protected by the segregation of duties need to be defined. The definition is realized by maintaining the desired entries into the table **T055F**.

**Display of Entries Found**

<table>
<thead>
<tr>
<th>Account type</th>
<th>Field name</th>
</tr>
</thead>
<tbody>
<tr>
<td>K</td>
<td>LFBK-BANKL</td>
</tr>
<tr>
<td>K</td>
<td>LFBK-BANKN</td>
</tr>
</tbody>
</table>

The technical names are described in more detail in the field attributes, or else in the Repository.

In this example the fields **LFBK-BANKL** and **LFBK-BANKN** are defined. (Vendor master bank key and bank account.)

**Step 2:**

In a second step the transactions need to be established for future user master data assignment, so that changes to the master data can be confirmed. This is usually done with transaction **FK08**.

The transaction **FK09** (List) cannot be recommended, because of the higher risk in the permeability.

In addition the user needs to have the authorization values 08 (Display changes) und C8 (Confirm changes) established.
Note:
This protection method is not exclusively applicable to vendor master data. The protection of customer master data can be relevant as well, in case of high volume credit notes that are paid for example.
### 5.12 Table of content for the documentation of an authorization concept

This is an example for a possible documentation structure including special requirements for HR.

**Table of content**

1. Target / scope
2. Premise
   2.1. Protection of Data being transmitted across state and international borders [Non-violation of local and export laws]
3. Function structure
   3.1. Explanation of concept
   3.2. Integration in SAP system landscape with interfaces
   3.3. Description of system and data ownership
   3.4. Data classification
   3.5. Overview of relevant organizational units
4. Dependency of authorizations
   4.1. Segregation of duties
   4.2. Dual control principle [symmetric with OSS 151207 / asymmetric] – P_ORGIN, P_ORGXX or RPUAUD00 (master data log)
5. Functions
   5.1. Basic system adjustments
      5.1.1. Profile parameter of the function category login/* and auth/*
      5.1.2. Globally deactivated authorization objects
      5.1.3. Deactivation of individual authorization objects
   5.2. Name convention and Use
      5.2.1. User groups
         5.2.1.1. User of the User group SUPER
         5.2.1.2. User of the User group "XXX"
      5.2.2. User Name convention
   5.2.3. Roles
      5.2.3.1. Use of SAP Standard roles
      5.2.3.2. Single Roles
      5.2.3.3. Composite Roles
      5.2.3.4. Inheritance and Derivation [USORG]
   5.2.4. Indirect Role assignment
      5.2.4.1. Local
      5.2.4.2. Global
   5.2.5. Profiles
      5.2.5.1. Use of the profiles SAP_ALL, SAP_NEW, P_BAS_ALL
      5.2.5.2. Use of SAP standard profiles
   5.2.6. Reference users
   5.2.7. Central User Administration
6. Working place analysis [Job description - including transaction codes]
   6.1. User with the authorization to maintain personnel master data
   6.2. User of the business area Financial accounting / Cost center import
   6.3. User with display authorization within the personnel administration
   6.4. User with critical authorization
   6.5. Coordination function for Payroll
7. HR Specials

7.1. Infotypes

7.1.1. Description of used Infotypes
7.1.2. Use of Infotype 0130 [protection of master data from deletion]

7.2. Main authorization switches

7.2.1. AUTSW ORGIN
7.2.2. AUTSW ORGXX
7.2.3. AUTSW NNNNN
7.2.4. AUTSW ADAYS
7.2.5. AUTSW PERNR
7.2.6. AUTSW APPRO
7.2.7. AUTSW ORGPD

7.3. Context sensitive authorization switches

7.3.1. AUTSW INCON
7.3.2. AUTSW XXCON
7.3.3. AUTSW NNCON
7.3.4. AUTSW DFCON

7.4. Structural authorizations

7.4.1. Description
7.4.2. Use
7.4.3. Customizing and assignment [e.g. T77PR, TU77A]

7.5. System settings

7.5.1. Table T77SO

7.6. P_ORGIN

7.6.1. [INFTY, SUBTY, AUTHC, PERSA, PERSG, PERSK, VDSK1] especially authorization level, organizational key, time limitation responsibility
– time logic
ADAYS in table T77S0, indicator for access (T582AVALDT) in T582A

7.7. P_ABAP

7.7.1. “Degree of simplification for authorization check”
7.7.2. Reports to be protected

7.8. Log of HR report starts

[Table T599R - evaluation with report RPUPROTD]

7.9. Use of PFCG_ORGFIELD_CREATE [OSS Note 323817]

7.10. Calculation Rules

7.11. External check DEÜV [Table T5D4S]

7.12. Protection of tables REGUH, REGUP in FI – [Table T558A]

7.13. Protection of special transactions [S_TCODE and P_TCODE]

7.13.1. PU00
7.13.2. PU01
7.13.3. PU03

7.14. Integration of evaluation control
[e.g. RHUSERREALATIONS]

8. User education and training

8.1. Help Desk
8.2. Super User
8.3. User manual

9. User administration / role administration

9.1. Structure
9.2. Authorization administration
9.3. Administrator user accounts
9.4. Administration of user master records
   9.4.1. Creation
      9.4.1.1. Request
      9.4.1.2. User type
      9.4.1.3. Initial Password / Use of Wizard
      9.4.1.4. Approval procedure
      9.4.1.5. Archiving of request
      9.4.1.6. Guarantee privacy regulation / Data protection
      9.4.1.7. Initial Logon
   9.4.2. Change of responsibilities
   9.4.3. Change and deletion
   9.4.4. User master records in the system
9.5. Administration of roles
   9.5.1. Principle of menu control
      9.5.1.1. Exceptions from the menu control
   9.5.2. Changes of roles
      9.5.2.1. Documentation of role changes
   9.5.3. Creation of roles and profiles
   9.5.4. Testing of roles
      9.5.4.1. Positive Test
      9.5.4.2. Negative Test
   9.5.5. Deletion of roles and profiles
9.6. Logon procedure
   9.6.1. Regulations for complex passwords
   9.6.2. Multiple logon
9.7. Control activities within the user administration
   9.7.1. Locking and deletion of users
   9.7.2. Unlocking of users
10. Protection of Special user
   10.1. SAP Standard user
      10.1.1. User SAP*
      10.1.2. User DDIC
      10.1.3. Technical user (TMSADM, SAPCPI)
   10.2. Company specific special user
      10.2.1. Emergency user
      10.2.2. Support user
      10.2.3. Batch-User
      10.2.4. ALE-Remote User
   10.3. Auditing
      10.3.1. Audit Log
         10.3.1.1. Configuration (e.g. all dialog user with SAP_ALL)
         10.3.1.2. Evaluation
      10.3.2. Security Log
         10.3.2.1. Configuration
         10.3.2.2. Evaluation
11. Table logging
   11.1. General information
   11.2. Parameter
   11.3. Evaluation and check
      11.3.1. Display of logged table content
      11.3.2. Check of log status for individual tables
      11.3.3. Other evaluations
         11.3.3.1. List of all logged tables
         11.3.3.2. List of change history for logged tables
11.3.4. Determination and control of size for table DBTABLOG
11.4. Archiving / Deletion

12. System changeability in the production system
12.1. Security guideline for cross client settings

13. Client changeability in the production system

14. Special functions
14.1. Restriction of download [S_GUI, S_OLE_CALL]
14.2. Restriction of query and ad-hoc query
14.3. Restriction of printer access and authorizations
14.4. Customizing authorization / Table maintenance
14.5. Maintenance of system parameters

14.6. Reports
14.6.1. Name convention for self created reports
14.6.2. Deletion of self created reports that are not longer needed
14.6.3. Protection of self created reports
14.6.3.1. Authorization group
14.6.3.2. Authority-check in source code
14.6.4. Documentation for self created reports

14.7. Tables
14.7.1. Name convention for self created tables
14.7.2. Logging of self created tables
14.7.3. Protection of self created tables [authorization-group]
14.7.4. Documentation for self created tables

14.8. Transaction codes
14.8.1. Name convention for self created transaction codes
14.8.2. Assignment of authorization-objects within SE93
14.8.3. Maintenance of self created transaction codes
SU22/SU24
14.8.4. Documentation for self created transaction codes
5.13 **Selected relevant Security tables**

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADCP</td>
<td>Person/Address Assignment (Business Address Services)</td>
</tr>
<tr>
<td>ADRP</td>
<td>Persons (Business Address Services)</td>
</tr>
<tr>
<td>AGR_1251</td>
<td>Authorization data for the activity group</td>
</tr>
<tr>
<td>AGR_1252</td>
<td>Organizational elements for authorizations</td>
</tr>
<tr>
<td>AGR_AGRS</td>
<td>Roles in Composite Roles</td>
</tr>
<tr>
<td>AGR_DEFINE</td>
<td>Role definition</td>
</tr>
<tr>
<td>AGR_USERS</td>
<td>Assignment of roles to users</td>
</tr>
<tr>
<td>BAPIUSW01</td>
<td>User ID Table for Internet Application Components</td>
</tr>
<tr>
<td>D01T</td>
<td>Domain texts</td>
</tr>
<tr>
<td>DD01L</td>
<td>Domains</td>
</tr>
<tr>
<td>DD02L</td>
<td>SAP Tables</td>
</tr>
<tr>
<td>DD02T</td>
<td>SAP DD: SAP Table Texts</td>
</tr>
<tr>
<td>DD04L</td>
<td>Data elements</td>
</tr>
<tr>
<td>DD04T</td>
<td>R/3 DD: Data element texts</td>
</tr>
<tr>
<td>DD06L</td>
<td>Pool/cluster structures</td>
</tr>
<tr>
<td>DD09L</td>
<td>DD: Technical settings of tables</td>
</tr>
<tr>
<td>SMMAIN</td>
<td>Main Information for an Entry in the Monitor</td>
</tr>
<tr>
<td>SUKRI</td>
<td>Transaction Combinations Critical for Security</td>
</tr>
<tr>
<td>T000</td>
<td>Clients</td>
</tr>
<tr>
<td>T001</td>
<td>Company Codes</td>
</tr>
<tr>
<td>T001L</td>
<td>Storage Locations</td>
</tr>
<tr>
<td>T001W</td>
<td>Plants/Branches</td>
</tr>
<tr>
<td>T003</td>
<td>Document Types</td>
</tr>
<tr>
<td>T004</td>
<td>Directory of Charts of Accounts</td>
</tr>
<tr>
<td>TACT</td>
<td>Activities which can be Protected</td>
</tr>
<tr>
<td>TACTZ</td>
<td>Valid activities for each authorization object</td>
</tr>
<tr>
<td>TBRG</td>
<td>Authorization groups</td>
</tr>
<tr>
<td>TDDAT</td>
<td>Maintenance Areas for Tables</td>
</tr>
<tr>
<td>TGSB</td>
<td>Business Areas</td>
</tr>
<tr>
<td>TOBC</td>
<td>Class assignment of authorization objects</td>
</tr>
<tr>
<td>TOBJ</td>
<td>Authorization Objects</td>
</tr>
<tr>
<td>TOBJ_CD</td>
<td>Short Texts for Authorization Objects</td>
</tr>
<tr>
<td>TOBJ_OFF</td>
<td>Objects that were disabled</td>
</tr>
<tr>
<td>TOBJT</td>
<td>Objects that were disabled</td>
</tr>
<tr>
<td>TRDIR</td>
<td>Generated Table for View TRDIR</td>
</tr>
<tr>
<td>TSTC</td>
<td>SAP Transaction Codes</td>
</tr>
<tr>
<td>TSTCA</td>
<td>Values for transaction code authorizations</td>
</tr>
<tr>
<td>TSTCP</td>
<td>Parameters for Transactions</td>
</tr>
<tr>
<td>TUTYP</td>
<td>SAP System User Type Texts</td>
</tr>
<tr>
<td>USGRP</td>
<td>User Groups</td>
</tr>
<tr>
<td>USH02</td>
<td>Change history for logon data</td>
</tr>
<tr>
<td>USH04</td>
<td>Change history for authorizations</td>
</tr>
<tr>
<td>USKRIA</td>
<td>Entry of Critical Auths for Report RSUSR009</td>
</tr>
<tr>
<td>USOBT</td>
<td>Relation transaction &gt; authorization object</td>
</tr>
<tr>
<td>USOBT_C</td>
<td>Relation Transaction &gt; Auth. Object (Customer)</td>
</tr>
<tr>
<td>USOBT_CD</td>
<td>Change History for Field Values</td>
</tr>
<tr>
<td>USOBX</td>
<td>Check table for table USOBT</td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>USOBX_C</td>
<td>Check Table for Table USOBT_C</td>
</tr>
<tr>
<td>USOBX_CD</td>
<td>Change History for Check Indicator</td>
</tr>
<tr>
<td>USORG</td>
<td>Org. levels for profile generator</td>
</tr>
<tr>
<td>USOTT</td>
<td>Relation transactions –authorization objects [reports]</td>
</tr>
<tr>
<td>USVAR</td>
<td>Possible authorization fields as variables</td>
</tr>
<tr>
<td>USR01</td>
<td>User master record (runtime data)</td>
</tr>
<tr>
<td>USR02</td>
<td>Logon Data (Kernel-Side Use)</td>
</tr>
<tr>
<td>USR03</td>
<td>User address data</td>
</tr>
<tr>
<td>USR04</td>
<td>User master authorizations</td>
</tr>
<tr>
<td>USR05</td>
<td>User Master Parameter ID</td>
</tr>
<tr>
<td>USR06</td>
<td>Additional Data per User</td>
</tr>
<tr>
<td>USR07</td>
<td>Object/values of last authorization check that failed</td>
</tr>
<tr>
<td>USR10</td>
<td>User master authorization profiles</td>
</tr>
<tr>
<td>USR11</td>
<td>User Master Texts for Profiles (USR10)</td>
</tr>
<tr>
<td>USR12</td>
<td>User Master Authorization Values</td>
</tr>
<tr>
<td>USR13</td>
<td>Short Texts for Authorizations</td>
</tr>
<tr>
<td>USR21</td>
<td>Assign user name address key</td>
</tr>
<tr>
<td>USR40</td>
<td>Table for illegal passwords</td>
</tr>
<tr>
<td>USR41</td>
<td>User master: Additional data</td>
</tr>
<tr>
<td>USR41_MLD</td>
<td>Transaction Data for USR41</td>
</tr>
<tr>
<td>USREFUS</td>
<td>Reference user for internet applications</td>
</tr>
<tr>
<td>UST04</td>
<td>User masters</td>
</tr>
<tr>
<td>UST10C</td>
<td>User master: Composite profiles</td>
</tr>
<tr>
<td>UST10S</td>
<td>User master: Single profiles</td>
</tr>
<tr>
<td>UST12</td>
<td>User master: Authorizations</td>
</tr>
</tbody>
</table>