

# **AUDIT – manual**

## **Introduction to the SAP R/3™ system focusing on audit aspects**

***Roger Odenthal***

**Translation by Eva Romatzeck**

## DIRECTORY

	Site
I Introduction	1
II SAP R/3™ in audit focus	2
1 Audit relevance	2
2 Audit layers	5
III Organizational preparation of audits in an SAP R/3™ environment	7
1 Audit objective and scope	7
2 Auditor work place	7
3 Creating user IDs	8
4 Necessary authorizations for audit purposes	8
5 Installing the AIS™ audit work place	10
6 Creating an interface (USER-Exit) to audit software	10
7 Summary of organizational preparation	11
IV How to operate the system and analyze data	13
1 Historical development of the user interface	13
2 User interface and system operation options	13
2.1 The SAP™ screen	13
2.2 Menu layout	15
2.3 System operation options	15
2.3.1 Operation via menus	15
2.3.2 Operation via transactions	18
2.3.3 Personal menus / favourites	20
2.3.4 Operation via the AIS™ auditor work place	21
2.4 Summary on user interface	22
2.5 Tools for the user interface layout	23
3 Preparing and analyzing SAP™ data	25
3.1 Options for Preparing and analyzing data	25
3.2 Preparing and analyzing table data	26
3.2.1 Introduction to tables	26
3.2.2 Strategies for finding proper tables	29
3.2.2.1 Searching the logical databases	29
3.2.2.2 Generic table search	31
3.2.3 Calling and preparing table data	32
3.2.3.1 Amount of shown data items and selection fields	32
3.2.3.2 Selecting table fields	33
3.2.3.3 Sorting data	34
3.2.4 Downloading data and transfer it to Excel	35
3.2.5 Tools for preparing and analyzing SAP™ data	37
3.3 Analyzing and preparing information in reports	39
3.3.1 Introduction to SAP™ reports	39
3.3.2 Strategies for finding proper reports	39
3.3.2.1 Searching the SAP™ information systems	39
3.3.2.2 Generic search by report names	40
3.3.2.3 Additional criteria for finding reports	44
3.3.2.4 Summarized strategies	45
3.3.3 Calling and preparing reports	45
3.3.3.1 Selection screen layout	46
3.3.3.2 Fine tuning the selection	47
3.3.4 Utilizing report variant techniques for audit purposes	49
3.3.4.1 Basic variant techniques	49
3.3.4.2 Static variants	50
3.3.4.3 Dynamic variants	51
3.3.4.4 Calling report variants	54
3.3.5 Further options for using reports	54
3.3.6 Download and usage of list contents	56
3.3.7 Summary on reports	58
3.3.8 Tools for report layout	58

- II -

3.4.1	Introduction	60
3.4.2	Creating functional areas	61
3.4.3	Creating and changing user groups	64
3.4.4	SAP <sup>TM</sup> query list layout	65
3.4.5	The AIS <sup>TM</sup> system and SAP <sup>TM</sup> Query	67
3.4.6	Calling existing queries and their interactive layout	67
3.4.7	Downloading data from SAP <sup>TM</sup> query	70
3.5	List layout using the list generator Quick-Viewer	71
3.6	Tools for utilizing SAP <sup>TM</sup> query	72
V	Auditing in an SAP R/3 <sup>TM</sup> -environment	74
1	Introduction	74
2	Organizational preparations for audits in the SAP R/3 <sup>TM</sup> environment	74
2.1	The auditor's work place	74
2.2	Required extent of authorizations	74
3	Supporting audits for the migration in an SAP R/3 <sup>TM</sup> system	76
4	General IT operations	81
4.1	Structure of the IT department	81
4.2	Rules for organizational processes and documentation of IT operations	82
4.3	Overview of the IT related technical environment	83
4.4	Utilities for estimating the technical operating environment	84
4.5	Mapping the IT environment	86
4.6	Summary on general IT operations	86
4.7	Audit tools for general IT operations	86
5	Auditing SAP <sup>TM</sup> basis applications	87
5.1	Introduction	87
5.2	Overview of installed systems, system environment and active SAP <sup>TM</sup> components	87
5.2.1	Mapping the installed R/3 <sup>TM</sup> systems	87
5.2.2	Mapping the operating system and the database environment	89
5.2.3	Mapping the business structure	92
5.2.3.1	Created clients	92
5.2.3.2	Further elements of the company specific structure	96
5.4.2	Tools for system overview	97
5.3	Overview and assessment of in-house developments	100
5.3.1	Basics on in-house developments	100
5.3.2	Name ranges for in-house developments	101
5.3.3	In-house developed transactions	102
5.3.4	In-house developed programs/reports	106
5.3.4.1	Initial overview of in-house developed programs	106
5.3.4.2	Detailed analyses of in-house developed programs	108
5.3.4.2.1	Contents of the detailed analyses	108
5.3.4.2.2	Utilizing the SAP <sup>TM</sup> editor	108
5.3.4.2.3	Table TRDIR	114
5.3.4.2.4	Utilizing the SAP AIS <sup>TM</sup> system for detailed analyses	117
5.3.5	In-house developed tables	119
5.3.5.1	Introduction	119
5.3.5.2	Initial overview of in-house developed tables	119
5.3.5.3	Detailed analysis of in-house developed tables	122
5.3.5.3.1	Development and changing procedures	122
5.3.5.3.2	Logging data changes	122
5.3.4.4	Further detailed analyses	125
5.3.6	Summary on in-house developments	130
5.3.7	Tools for auditing in-house developments	131
5.4	Data flow and reconciliation procedures in the SAP <sup>TM</sup> financial accounting environment	137
5.4.1	Introduction	137
5.4.2	The user dialog with the SAP <sup>TM</sup> system	137
5.4.3	Update termination and its consequences	141
5.4.3.1	System reaction	141

- III -

5.4.3.2	User reaction	142
5.4.3.3	Recommended actions in cases of update termination	143
5.4.4	Tools for auditing data flow and reconciliation procedures	146
5.5	Protecting the SAP™ system from unauthorized access	149
5.5.1	Introduction to system protection	149
5.5.2	Critical user IDs	149
5.5.3	Authentication procedures	153
5.5.1	Tools for auditing system security	156
5.6	Auditing the authorization concept	159
5.6.1	Introduction to the authorization concept	159
5.6.2	Methods, elements and tools for configuring the SAP R/3™ authorization concept	159
5.6.2.1	Introduction	159
5.6.2.2	The authorization object	160
5.6.2.2.1	Authorization object structure	160
5.6.2.2.2	SAP R/3™ standard authorization objects versus in-house developments	162
5.6.2.2.3	Object classes and authorization objects	164
5.6.2.2.4	Preconditions for utilizing SAP™ authorization objects	167
5.6.2.2.5	Calling authorization objects in SAP™ programs	167
5.6.2.3	Authorizations, profiles and activity groups	168
5.6.2.3.1	Single authorizations and profiles	168
5.6.2.3.2	Standard authorization profiles versus in-house developments	170
5.6.2.4	The SAP user and the assigned authorizations	174
5.6.2.5	User oriented access controls in the SAP R/3™ system	178
5.6.2.6	Tools for the authorization elements overview	179
5.6.3	Techniques for auditing authorizations	182
5.6.3.1	Introduction to the audit technique	182
5.6.3.2	Mapping the environment	182
5.6.3.3	Auditing the written authorization concept	183
5.6.3.4	Analyzing authorization weaknesses within the SAP™ system	185
5.6.3.4.1	Introduction to weakness analysis	185
5.6.3.4.2	Visual check of assigned authorization profiles	185
5.6.3.4.3	Analyzing the contents of specific single profiles	190
5.6.3.4.3.1	Audit approach	190
5.6.3.4.3.2	Auditing activity groups	192
5.6.3.4.3.3	Auditing “programmed “ profiles	196
5.6.3.4.4	Additional audit activities on selected transactions	199
5.6.3.4.4.1	The audit approach	199
5.6.3.4.4.2	Procedure for transaction oriented auditing	199
5.6.3.4.5	Further tools for auditing authorizations	210
5.6.3.4.5.1	Optional audit approaches	210
5.6.3.4.5.2	Pre-configured reports	210
5.6.3.4.5.3	Determine critical authorization combinations	211
5.6.3.4.5.4	Comparing users, profiles and authorizations	212
5.6.3.4.5.5	Checking amount authorizations	213
5.6.3.5	Tools for auditing authorizations	214
5.7	Critical parameter settings in the SAP™ start-up profiles	221
5.7.1	Introduction	221
5.7.2	Parameters, affecting the processing of financial accounting data	221
5.7.3	Comprehending transports	222
5.7.4	Other logs	222
5.7.5	Locking invalid logins	223
5.7.6	Controlling the authorization check	224
5.7.7	Tools for auditing parameter settings	225
5.8	Selected audit activities related to program development and maintenance	228
5.8.1	Introduction	228
5.8.2	Change and transport system	229
5.8.3	ABAP/4™ programming authorization	231



- IV -

5.8.4	Backdoor o programming authorization	231
5.8.5	Tools for auditing program development	232
5.8	Tracking critical master record changes	235
5.9.1	Creating and logging master records	235
5.9.2	Auditing table protection	236
5.9.3	Logging table changes	238
5.9.4	Reports on master record change logs	238
5.9.5	Tools for tracking master record changes	239
5.10	Setting up and processing automated program flows (jobs)	242
5.10.1	Introduction	242
5.10.2	Auditing the job processing	242
5.10.2.1	Defined job concept in writing	242
5.10.2.2	Auditing in the SAP R/3™ system	243
5.10.3	Tools for job control	245
5.11	Checking the batch input procedure	247
5.11.1	Introduction to the batch input procedure	247
5.11.2	Auditing established procedures	247
5.11.3	Auditing the batch input procedure in the SAP R/3™ system	248
5.11.4	Checking sufficient segregation of duties for processing sessions	250
5.11.5	Tools for auditing the batch input procedure	250
5.12	Data protection of personnel related data	253
5.12.1	Introduction	253
5.12.2	File register for personnel related data	253
5.12.3	Human resources planning	255
5.12.4	Personnel administration	255
5.13	Summary of the SAP™ basic system audit	258
6	Utilizing the SAP R/3™ AIS system for business audits	259
6.1	Introduction	259
6.2	Setting up the AIS™ system	259
6.2.1	Customizing the user interface for the auditor's work	259
6.2.1.1	Customizing the user menu	259
6.2.1.2	User specific notes and support	263
6.2.1.3	Layout of menu display options	264
6.2.2	Customizing the AIS™ system to company specific requirements	265
6.2.2.1	Introduction	265
6.2.2.2	Table TVARV – maintaining report system variants	266
6.2.2.3	Customizing the general ledger information system	267
6.2.2.4	The analysis system “BAETGE”	268
6.2.2.4.1	Introduction	268
6.2.2.4.2	Number of employees	268
6.2.2.4.3	Customizing the BAETGE analysis form	269
6.2.2.5	Customizing the interface “general ledger account balances” for further systems	270
6.2.2.6	Setting up the customer and vendor information systems	271
6.2.2.6.1	Introduction	271
6.2.2.6.2	Creating specified report variants	271
6.2.2.3	Tools for setting up the AIS™ system	277
6.3	Utilizing the AIS™ in business audits	279
6.4	Mapping the business / organizational parameters	280
6.4.1	Business structure	280
6.4.2	Information on account assignment elements	281
6.4.2.2	Details on account assignment elements	283
6.4.2.2.1	Document types	283
6.4.2.2.2	Number ranges	285
6.4.2.2.3	Posting key	287
6.4.2.2.4	Tax codes and tax keys	288
6.4.3	Special general ledger	290
6.4.4	Reconciliation accounts	291

6.4.5	Automatic account determination	292
6.4.6	Quantity structure (database)	293
6.4.7	Summary on the organizational overview	293
6.4.8	Tools for creating an organizational overview	294
6.5	Functions for auditing balance sheet items	300
6.5.1	Introduction	300
6.5.2	Functions in the menu closing (FI-GL)	302
6.5.2.1	Reconciling accounts and documents	302
6.5.2.2	Balance sheet and profit and loss account	304
6.5.2.3	Balances	306
6.5.3	General ledger account information	306
6.5.3.1	Overview	306
6.5.3.2	Creating and changing general ledger accounts	307
6.5.3.3	Analyzing general ledger accounts	308
6.5.4	Document information	308
6.5.4.1	Overview	308
6.5.4.2	Checking document completeness and single items	310
6.5.4.3	Detailed document analyses	311
6.5.4.4	Document changes	312
6.5.4.5	Exporting data to the auditor's software	312
6.6	Other functions for auditing assets and liabilities & equity	313
7	Exporting AIS <sup>TM</sup> data to audit software	314
7.1	Requirements for the export	314
7.1.1	Setting up a private folder	314
7.1.2	Requirements for exporting data from SAP <sup>TM</sup> Query and Quick View	315
7.1.3	Requirements for the audit software	316
7.2	Data export and import	317
7.2.1	Data export from the AIS <sup>TM</sup> system	317
7.2.2	Data export from SAP <sup>TM</sup> Query and Quick View	320
7.3	Importing SAP <sup>TM</sup> AIS data to audit software	322
7.3.1	Import to ACL audit software	322
7.3.2	Import to WinIDEA audit software	325
7.4	Importing SAP <sup>TM</sup> data to audit software via file store	327
7.4.1	.Introduction	327
7.4.2	Import to ACL audit software	327
7.4.3	Import to WinIDEA audit software	329
7.5	Overview of transferred document fields	331
7.6	Summary	333
VI	Final remark	334

## Enclosures

Tables for the user administration	Enclosure 1
Controlling tables for the financial accounting	Enclosure 2
Important tables for the financial accounting	Enclosure 3
Reports on user administration and authorization checks	Enclosure 4
Company and staff	Enclosure 5

## APPENDICES

Appendix 1:	Tables for the user administration
Appendix 2:	Controlling tables for the financial accounting
Appendix 3:	Important tables for the financial accounting
Appendix 4:	Reports on user administration and authorization checks
Appendix 5:	Company and staff

### Note

**This document is not meant to be read and understood by itself, but to support a class on audits in an SAP R/3 environment. The author would be pleased to receive your suggestions for changes and additions. This document or parts of it may not be copied without permission by the author. This also applies for the accompanying software and prints of it, in particular for teaching purposes.**

### Note from the translator

**In order to keep the document as clear and readable as possible, the translator refers to “the auditor” and “the user” as “he”, “him” or “his”. Obviously, all auditors and users – male and female – are being equally addressed by these terms.**

### Trademark

**SAP, R/2, R/3, ABAP, ABAP/4, SAP-Earlywatch are registered trademarks of SAP AG, Walldorf, Germany. Most other hard and software products mentioned in this manual are also registered trademarks and are protected by corresponding laws.**

## FOREWORD

Our staff have carried out manifold audits in co-operation with internal and statutory auditors, and their experiences are reflected in this manual. During audits and training sessions we have noted reoccurring issues like

- How should the user operate this complex IT system?
- How can the user generate information in the different SAP R/3<sup>TM</sup> release versions, which meets his requirements?
- What should the IT auditor focus on, in order to obtain a correct impression of the complete system, the data processing and the resulting business information?
- What about the auditor's workplace?
- What are the options for downloading data to personal computers?

With this manual, we try to provide some of the answers and hope that the manual will be useful to the readers in their daily work. This manual focuses on selected issues of major importance, as it is not possible to discuss every audit relevant aspect. There are several additional manuals, publications and other literature, where the reader may find further aspects though.

The following – rather detailed – sections will discuss the topics

- 1 organizational requirements for efficient auditing
- 2 basic instructions on the user interface and options for operating the system
- 3 options and techniques for preparing and analyzing SAP<sup>TM</sup> data
- 4 audit activities for the initial SAP<sup>TM</sup> system audit
- 5 utilizing the SAP R/3<sup>TM</sup> AIS system to support audits of financial statements
- 6 downloading SAP<sup>TM</sup> data to the auditor's personal computer

Depending on the reader's interest and knowledge, different sections of this manual will be of particular interest. For the business auditor, who deals with the system for the first time, the sections on how to operate the system and analyze data may be of relevance. The statutory auditor may want to know more about the benefits of the AIS<sup>TM</sup> system, and the experienced IT auditor may only find the section on system audits interesting.

After each section, the reader will find an overview of tools in the SAP<sup>TM</sup> system for generating the intended outcome. Optional ways are presented in many cases, depending on the auditor's access to an AIS<sup>TM</sup> system or if he works with transactions, tables and programs. There are exercises, which are meant to increase the understanding of discussed topics. The reader has to adapt the exercises to company codes etc. in his training environment.

The reader will find a checklist at the end of each section, which summarizes the discussed audit issues and details.

In addition to the hardcopy you can obtain this manual on an interactive CD-ROM upon request, where the text and figures are linked to motion picture sequences from a live SAP™ system.

Details on further available manuals and documentation as well as information about our company can be found in the appendices. At this point we would like to attract your attention to our download service on our website

**[www.roger-odenthal.de](http://www.roger-odenthal.de)**

where you can find several utilities, checklists and supporting programs, not only for SAP™ but also for other topics related to internal and statutory auditing.

Please feel free to forward your suggestions for further improvements of this manual to us.

We hope this document will be useful to you, and to your successful work.

Cologne in January 2002

Roger Odenthal

## I Introduction

SAP AG, Walldorf, Germany, has become one of the leading suppliers of integrated business standard software world-wide. The company is providing a powerful and complex system, covering all aspects of the business. Internal and statutory auditors consequently need to take a very close look at it.

In order to analyze the SAP<sup>TM</sup> and the saved, processed and reported data according to audit specific standards, auditors have to deal with organizational and technical problems, which often seem impossible to solve. This is not only unfortunate because of the risks connected to the data processing within SAP<sup>TM</sup>, but is in fact dangerous *as the auditors are partly responsible for the proper implementation of and processing in the SAP<sup>TM</sup> system*. This proper utilization of the system is the basis for a software certification by statutory auditors.

As for any comparable system, SAP<sup>TM</sup> must contain

- Complete and correct master data
- Complete and correct transaction data
- Proper and logical processing

before correct results can be ensured.

This manual should give an introduction to the SAP R/3<sup>TM</sup> system, taking audit relevant aspects into particular consideration. The focus is put on the structure and features of the SAP<sup>TM</sup> system. Basics for the handling of the system and advice for useful audit steps in SAP R/3<sup>TM</sup> will be given. Additionally, alternative methods of processing saved data for audit purposes will be presented.

R/3<sup>TM</sup> release upgrades are taken into consideration where possible. *Please note however, that the use of different hard and software, as well as different releases may result in deviations from this manual.*

## II SAP R/3™ in audit focus

### 1 Audit relevance

Auditors, who want to take a closer look at the SAP R/3™ system often hear comments from the IT and other departments, such as

- The SAP R/3™ system is secure
- SAP™ does not allow improper data input
- Programming errors would be detected promptly due to the large amount of implementations
- The auditors are obstructing the project
- The system has been reviewed and certified by statutory auditors

Auditors have to be very critical about such comments. No doubt, the SAP R/3™ system is being developed by a big software company with competent programmers and great business know-how. There are plenty of users and certificates issued by statutory auditors, confirming the compliance of the different SAP R/3™ modules.

In spite of these arguments, there are several good reasons for auditors to deal intensively with the SAP™ processing and the data saved in the system.

#### ❑ Installation environment and operation

The SAP R/3™ system is based on a complex client-server-technology, where various computers, operating systems and databases are employed.

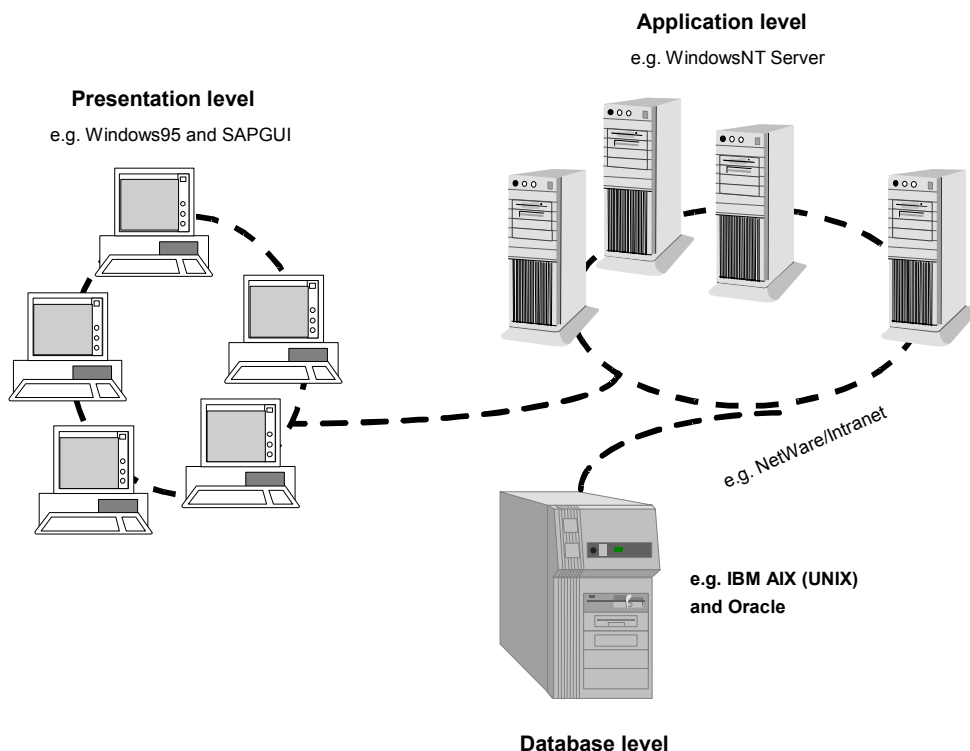


Figure 1: a typical installation environment

The function of the system, as well as the protection and security of the processed transactions, are substantially depending on the physical and logical precautions for securing the computers and other components of the operating system. The direct impact on data in the databases must be ruled out and the user work stations must be secured in order to avoid interference with the system itself. Additionally, the SAP R/3<sup>TM</sup> administrators and hereto assigned consultants have to ensure the proper processing within the system, which automatically results in a row of audit tasks.

#### ☐ **Customizing and table management**

SAP<sup>TM</sup> provides a standard system for the processing of business transactions, which has to be customized to the specific requirements of each company implementing the system. The table settings are controlling the transaction processing. SAP R/3<sup>TM</sup> is a so called "system controlled by parameters", which gets its information about obligatory processes, checking procedures, calculations and data of accounts and taxes from table settings as defined by the user. These table settings determine the actual processing of business transactions and the function of the system. The initial setting and subsequent changes therefore need to get special attention from the auditor.

#### ☐ **SAP R/3<sup>TM</sup> standard versus modification of the source code**

Where the controlling of SAP<sup>TM</sup> processes are reaching its limits, and the software still has to be customized to the specific requirements of the company, changes of the SAP<sup>TM</sup> standard source code are necessary. This is often the case in the sales module, where such topics as specific customer relations, rebates and discounts can not be sufficiently reflected based on table settings only.

Changes of the SAP<sup>TM</sup> standard source code are not recommended by SAP<sup>TM</sup>, as the subsequent maintenance, service and release upgrades require additional manual customizing and tests. Additionally, the certificates issued by statutory auditors are only valid for the original standard system without changes. The objective and financial benefit of such changes, along with their documentation and comprehension open new audit fields.

#### ☐ **SAP<sup>TM</sup> system enhancement based on ABAP<sup>TM</sup> programming**

A further possibility in order to consider customer aspects in the system, is to develop partial programs or even complete sub-ledgers, based on the programming language ABAP<sup>TM</sup> (Advanced Business Application Programming), provided by SAP<sup>TM</sup>. Without restraint, every company can decide whether to use this possibility for developing SAP R/3<sup>TM</sup> and create new files and applications, which have only vague reminiscence to the standard software as provided by SAP<sup>TM</sup>.

Information, which has been created in such partial programs and possibly will be used for other purposes relevant to the accounting records, are to be assessed according to the same criteria as every other (non SAP R/3<sup>TM</sup>) in house developed program. Here too, is the special attention from the auditor needed.



#### ❑ **System settings and security**

A computerized accounting system which saves data for accounting purposes has to fulfil certain requirements according to commercial and tax legislation (documentation requirements, storage and document purposes, prohibited erasing, efficient internal control system etc.). The installation of such a system, the initial input of information and subsequent test phases can be performed with system settings, which would not meet the legal requirements in case the SAP R/3™ would go live and be utilized as a production system. The SAP R/3™ system offers possibilities to companies - also regarding different functions of developing, test and productive operations - which have to be reviewed critically by auditors.

#### ❑ **Hardware failure and programming errors**

The SAP R/3™ software is delivered with several control mechanisms, which should ensure the data integrity even in problematic situations. Nevertheless, hardware failure, errors in the operating system or in the program can not be ruled out, resulting in incomplete postings, erroneous document numbers or other data inconsistencies, which make an audit inevitable.

#### ❑ **Interfaces**

SAP R/3™ will rarely cover every need of information in a company completely. Usually the system is surrounded by additional programs, used for specific purposes. These systems are communicating with the SAP™ system via defined interfaces. The smooth exchange of data via the interfaces has to be ensured by developers, administrators and users. In this area additional controls by auditors are required.

#### ❑ **SAP™ basic data**

The basic data determines the quality of the numerical data, the results and reports in SAP R/3™. SAP R/3™ provides a database with a data dictionary, including almost every field required for business applications. Which fields are actually used and which contents is input is decided by the users. If absurd information is input to the system, only absurd information will come out of it too. It is therefore the duty of the auditor to assess the quality of the data.

#### ❑ **Process view and complex integration**

The accounting data in the financial accounting records in SAP R/3™ is *automatically generated from the computerized processing of business transactions to a great extent, and can hardly be affected by the accounting department*. The quality of the business transactions, reflected in the system in accordance with the software customizing, the related organizational circumstances, the sufficient user knowledge and the integrated authorization concept as well as the resulting internal controls, determine the quality of the numerical data.

For reasons mentioned, it is a must to include the related functions of SAP R/3™ in an audit of business processes. *Without considering both elements, no reliable statement on risks or security of a partial business process can be made.* The audit of the SAP™ system is not a task for (a few) IT auditors alone. The professional business auditor has to deal with the system as well. Additionally, the audit of SAP™ is not a static, nonrecurring task. The dynamic and the process oriented view of the system requires continuous reviews by business as well as IT auditors.

Summarized we conclude: for several reasons, auditors have to deal with the processing in SAP R/3™ and the data managed by the system.

## **2      *Audit layers***

The risks of protection, security, integrity and compliance of data have increased due to the described features of the SAP R/3™ system. A few years ago, an auditor was able to make a qualified statement on the IT system security standards within an acceptable time frame, auditing a centralized mainframe computer, put in a secured area and protected from unauthorized access by Remote Access Control Function. This is not possible with modern client-server systems, since the sources of risk have multiplied.

IT operations, in past times reserved for the elite at computer centers, has turned democratic as a result of the use of personal computers. The users consider themselves to be sufficiently proficient for processing individual data with their personal computers. Due to the described flexibility and openness of SAP R/3™ and the option of easy data transferal to personal computers, *every work station connected to the SAP R/3™ system makes out a potential risk* as far as looking out for and smuggling confidential information on discs, via telephone lines or e-mail connections.

The modularity and the related trend towards a miniature platform in SAP R/3™ gives the IT environment a tremendous dynamic. A competent statement on which computers the complete R/3™ system consists of is momentarily and can only be made with reservation. An R/3™ application can not permanently be assigned to one specific or several servers. *The complete network, including linked mainframe computers, UNIX, MicrosoftNT, Novell and other servers, as well as personal computers connected to the network, make up an ever changing audit environment.*

The desire for supplier independent applications has been fulfilled with SAP R/3™ and is of importance for the audit. The suppliers can obviously optimize the protection and security of IT data only in their own applications, which means the supplier of the financial accounting system optimizes his program, the other supplier of the required related database does it for his database, the supplier of the hardware is in charge of the operating system. For all layers of the IT system, equally complex and often object oriented authorization concepts are offered. *The assessment of the security as a whole, and of the interdependence between these different layers in particular, is extremely difficult for the auditor.*

The described integration of data and processes can be good or bad news for the auditor, depending on the system design. It requires a proper setting and customizing of the provided SAP R/3™ standard system for the specific purposes of each company. The necessary parameters have to be clear and their reciprocal dependencies have to be transparent, providing appropriate and sufficient controls in order to contribute to an efficient internal control system and the smooth processing of business transactions. However – who can guarantee that in a continuously developing SAP R/3™ system, which includes multiple programs?

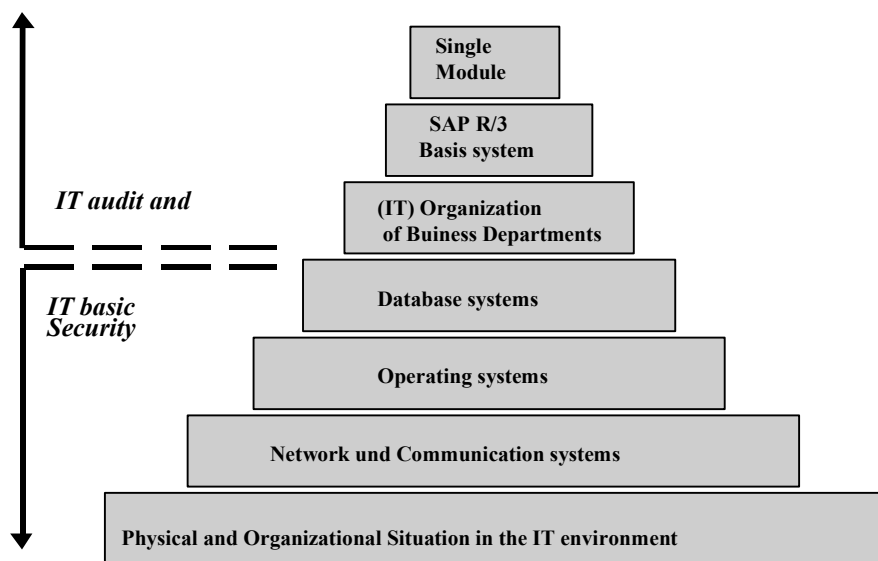


Figure 2: audit layers in a complex SAP R/3™ implementation

One does not have to be pessimistic in order to recognize, that the progress in IT technology increases the difficulties to secure and audit the systems. Even in an economic situation, where companies are depending on a reliable and secure IT environment in order to survive, auditor are lagging 10 or 15 years behind security technology.

Computer servers are often located in accessible areas without security locks, and a separation comparable to remote access control functions between the users and the network operating system or specific applications is rarely to be found. Additionally, confidential data such as account balances are exchanged without security codes via local modems, e-mail and non-secured networks.

The standards of secure and compliant IT processing as developed in co-operation between statutory and internal auditors are increasingly being neglected. This is unfortunate for the auditor. In many cases he finds himself in a situation – unless he was involved in the design of and processing in the SAP R/3™ system at an early stage – where protection, security and compliance can be audited only with great effort.

Knowing this, *audit support during the implementation phase* has proved to be an extraordinary efficient tool for increasing security with acceptable staff efforts.

The review of an already implemented SAP R/3<sup>TM</sup> system should be designed as a *cross-sectional audit*, which considers all layers of the IT system. Limited reviews on the levels of the operating system, databases and hardware will often be sufficient for increasing the overall level of security significantly.

Beside the *basic audit* of the SAP R/3<sup>TM</sup> system, a focused, *risk oriented audit of the IT operations and processes* should be carried out.

### **III Organizational preparation of audits in an SAP R/3<sup>TM</sup> environment**

#### **1 Audit objective and scope**

Internal and statutory auditors need to have access to the SAP R/3<sup>TM</sup> system in order to carry out audit activities. The *audit of IT procedures* includes reviews of table settings, processes, authorizations and programs. Complete process sequences are reviewed in order to ensure an efficient internal control system and to assess the numerical data resulting from the processing in SAP. During the statutory audit, the auditor is dealing with compliance aspects of the *financial accounting* in SAP and audits the numerical data generated by the system in the accounting system and in the balance sheet.

The system is offering comprehensive support for all audit field mentioned. Nevertheless, the *auditor is required to co-ordinate the timing* and other organizational matters with the administrators and other employees. The following has to be organized prior to the audit:

- Setting up a necessary (SAP) audit work place
- Creating necessary user IDs in the network and in SAP R/3<sup>TM</sup>
- Assigning required authorizations
- Installing and setting up the necessary SAP<sup>TM</sup> audit work place (AIS, Audit Information System)

These aspects will be discussed in detail.

#### **2 Auditor work place**

It is necessary to provide access to the SAP<sup>TM</sup> system to the auditor. Usually this can be done via a personal computer. It is useful to discuss with the administrators prior to the audit, which other programs – except SAP<sup>TM</sup> - will be needed. In most cases standard office software, including word processing, spreadsheet and database, need to be available. Auditors often also use specific audit software, such as WinIDEA and ACL, which should be installed on their personal computers prior to the audit.

The support of administrative staff is usually required. The CD-ROMs for installing required software have to be provided on a timely basis. This also applies if further specialized software will be used, such as Audit Agent or Monarch, a common tool for data conversion.

In cases where the auditor needs to exchange data with his own laptop, he will need a *computer with a disc drive* at his work place. The disc drive has to be released for use, which may need to be co-ordinated with the administrators.

### **3      *Creating user IDs***

User IDs are required for access to the network and to the SAP™ system. It should be clarified if a personalized ID or a group ID can be used. The user ID should be agreed beforehand and if possible, the same user ID and password should be valid for the network and the SAP™ system. Network access can be limited to certain weekdays or daytimes. If this is the case, the auditor should make sure his has access to the systems during regular working hours.

### **4      *Necessary authorizations for audit purposes***

Internal and statutory auditors need extensive authorizations within the SAP™ system in order to perform required audit activities, strictly excluding any possibilities of changing data though. For this purpose, every SAP™ installation is offering standard profiles for each business application and for the basis module. These can usually be recognized by the suffix "ANZ" or "SHOW" at the end (meaning display authorization).

Such as following profiles:

- A\_ANZ   all display authorizations for fixed assets
- F\_ANZ   all display authorizations for accounting
- M\_ANZ   all display authorizations for materials and logistic
- S\_A\_SHOW   all display authorizations for the basis module
- .....

It makes sense to use these standard profiles, since they ensure exclusion of data changes *and at the same time* provide display authorizations to the required extent. Experience shows, that in-house developed profiles usually do not enable auditors to fulfil their tasks. In particular is the often required display authorizations for the basis module missing.

If the AIS™ module has already been installed in the production system and the profile generator is being used as the common tool for allocating authorizations, the SAP™ system offers standard activity groups called “SAP\_CA\_AUDITOR\_XXX”<sup>1</sup>

Activity group	Activity group name
SAP_CA_AUDITOR_APPL_ADMIN_AG	CA: Audit Administration
SAP_CA_AUDITOR_APPL_AG	CA: Auditor SAP Applications (except HR)
SAP_CA_AUDITOR_DS_AG	CA: Data Protection Auditor
SAP_CA_AUDITOR_HR_AG	CA: HR Auditor
SAP_CA_AUDITOR_SYSTEM_AG	CA: Auditor System

Figure 3: overview of standard activity groups for audit purposes

The authorization administrators have to change the activity groups slightly before they are allocated to the auditor’s user ID.

The administrators can find precise procedures for allocating authorizations in the AIS™ system.

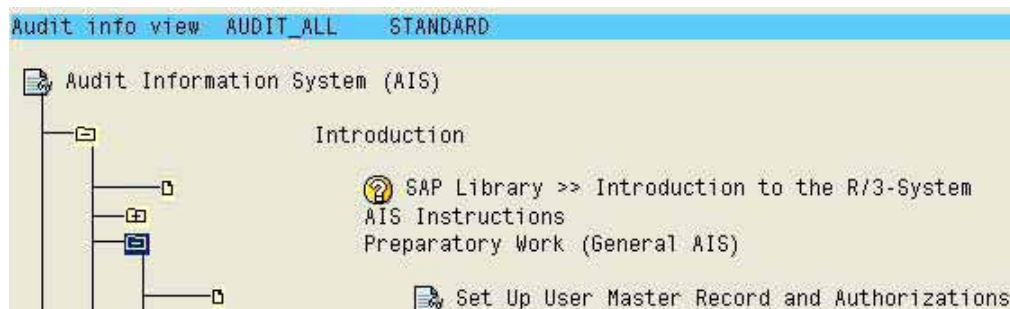


Figure 4: guide for administrators to the allocation of authorities

SAP has created this log showing which activities are required by the authorization administrators in order to set the authorizations properly for the auditors.

Activities
<ol style="list-style-type: none"> <li>Copy the SAP standard activity groups from client 000 to the current client. AIS initial screen: -&gt;Extras -&gt;Installation -&gt;Activity groups</li> <li>Call up transaction <b>PFCG</b> <ol style="list-style-type: none"> <li>Copy the activity group to the customer name range (such as Z_CA_AUDITOR_ALL_AG).</li> <li>Change the authorization data of the new activity group. (From the authorizations tab select the function "Change authorization data")</li> <li>Assignment of organizational level authorization. (Start the "Org. levels" function) Simple recommendation: Entire authorization All fields of the organizational levels are thus covered.</li> <li>Assignment of special authorizations for the fields still open. Start "Open fields" function and edit all the yellow-colored fields: * Enter entire authorizations</li> </ol> </li> </ol>

Figure 5: required activities for the authorization administration

<sup>1</sup> XXX shows the type of audit for the activity group, such as business audit, system audit, data protection audit etc.



It is recommendable *to check if the audit work can be carried out* as intended after creating the user master data and allocating the authorizations. The AIS™ system can be accessed with the transaction “SECR”, and different functions within the system audit and the business audit areas can be checked. A refused access due to lack of authorization is usually a sign of an insufficient extent of required authorizations.

## **5      *Installing the AIS™ audit work place***

The Audit Information System is not automatically installed in every SAP environment. In release 4.6C it is provided with the SAP™ standard. In earlier releases (from release 3.0D) a separate installation is necessary. The program is available for transferal to the production SAP™ environment on the SAP™ service computers (SAP\_SERV) and is free of charge. The installation is supported by SAP™ with the OSS directives No. 13719 and No. 77503.

The separate installation of the AIS™ system is possible with little effort. Nevertheless, the auditors *should allow 2-4 weeks time for the required preparations*. After the installation, the administrators have to enter necessary forward information and controlling data for specific reports with the function “Customizing AIS”. Additionally, the transaction code “SECR” for calling the AIS™ system, has to be entered in the table TSTC.

## **6      *Creating an interface (USER-Exit) to audit software***

The direct *transfer of document data and of information from query* reports into common audit software works via a standard interface provided by SAP, the so called USER-EXIT (SQUE010101), which has to be installed by the system administrators by calling the transaction CMOD. Further information is available in the AIS menu path and the attached text document

Business audit  
    Closing  
        Export data  
            Export document data

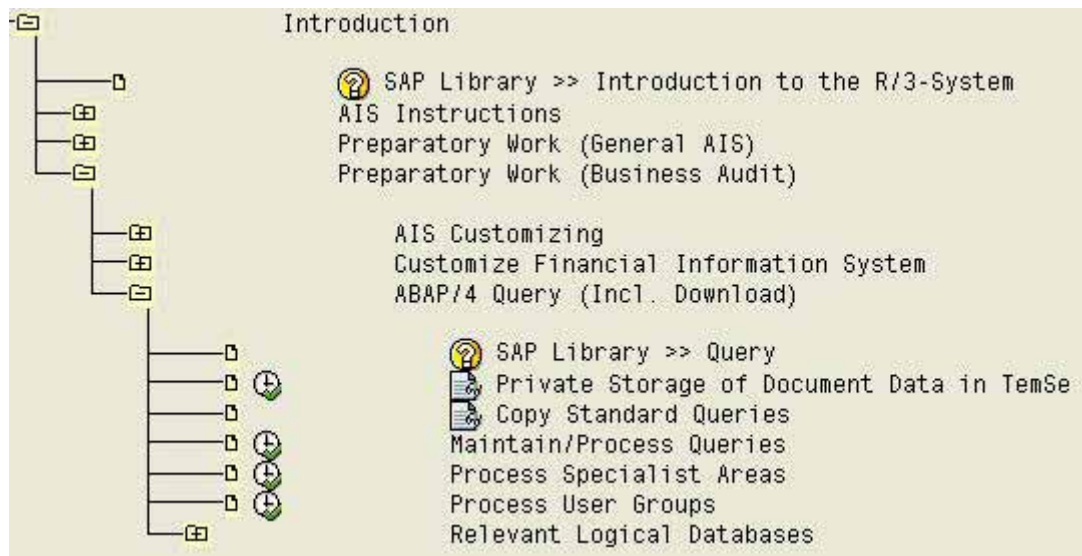


Figure 6: context sensitive support menu for data transfer

In order to activate the interface, an INCLUDE component called RXQUEU00 has to be allocated to the mentioned interface. *The private folder is now activated and enables a direct data transfer into the audit software.*

## 7 Summary of organizational preparation

The listed tasks only have to be performed once in order to enable a continuous and appropriate use of the SAP™ system for audit purposes. The preparations *have to be coordinated with the proper people on a timely basis*, and not when the audit is about to begin. Experience also show, that tests of the functions mentioned above are essential. If no problems occur in the tests, all audit activities can be carried out as described in this manual.



### **Audit preparation checklist**

#### ☐ **audit work place equipment**

- personal computer with SAP™ access
- Installing other required programs
  - word processing
  - spreadsheet
  - audit software for data analysis
  - special software for data conversion
  - special software for managing work papers
- released disc drive, ready to use
- installing a local printer

#### ☐ **creating user IDs**

- user ID for the SAP™ system
- user ID for the network

#### ☐ **assigning required SAP™ authorizations**

- display authorization for the basis module and business applications or
- activity groups SAP\_CA\_AUDITOR\_XXX, noting that the activity groups for both system and business audits usually are required

#### ☐ **separate installation of the AISTM system**

- only necessary if not existing and for releases prior to 4.6C
- customizing of the IAS™ system, as described in the OSS directives

#### ☐ **installing the interface to common audit software (USER-Exit)**


## IV How to operate the system and analyze data

### 1 Historical development of the user interface

SAP R/3™ has reached the current extent of functions and the status of user interface, passing several developing stages. Due to this, there are many alternative paths for reaching the same function. The resulting complexity is sometimes making it difficult for the auditor to find his way through the system. In the following sections, basic user options will be presented. Additionally, ways of generating audit relevant information from the SAP R/3™ system without assistance from the IT administrators or the audited departments will be presented. These are the basics for the business and system audit activities described in this manual.

### 2 User interface and system operation options

#### 2.1 The SAP™ screen

The SAP R/3RM functions are available to the auditor, using an SAP™ partial program on his computer, the so-called “SAP™-GUI” (Graphical User Interface). “SAP™-GUI” enables the smooth system operation across platforms according to windows standards. The screen display layout can be altered before entering SAP™ using the symbol , where classic or modern layouts are optional.

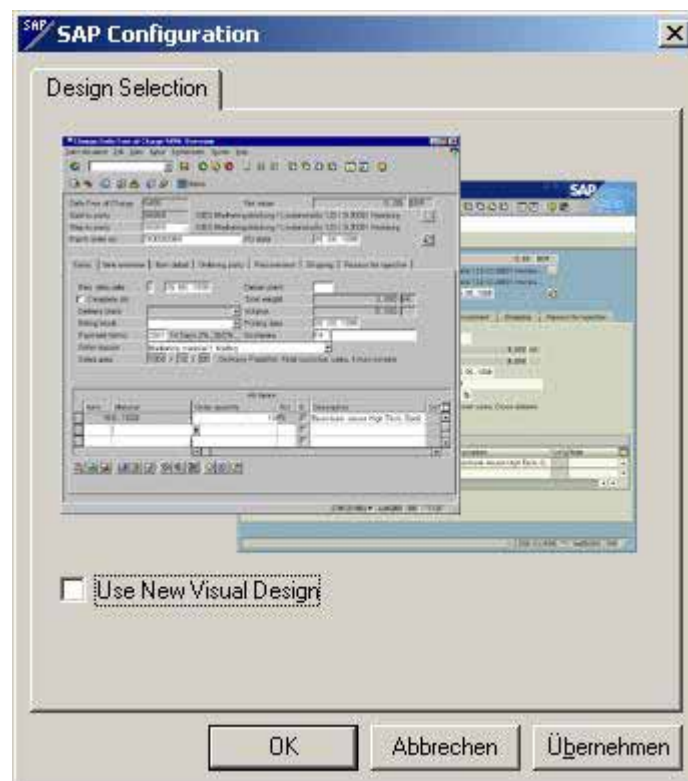


Figure 7: SAP™ screen layout options

In this manual, the modern layout with gray background has been chosen.

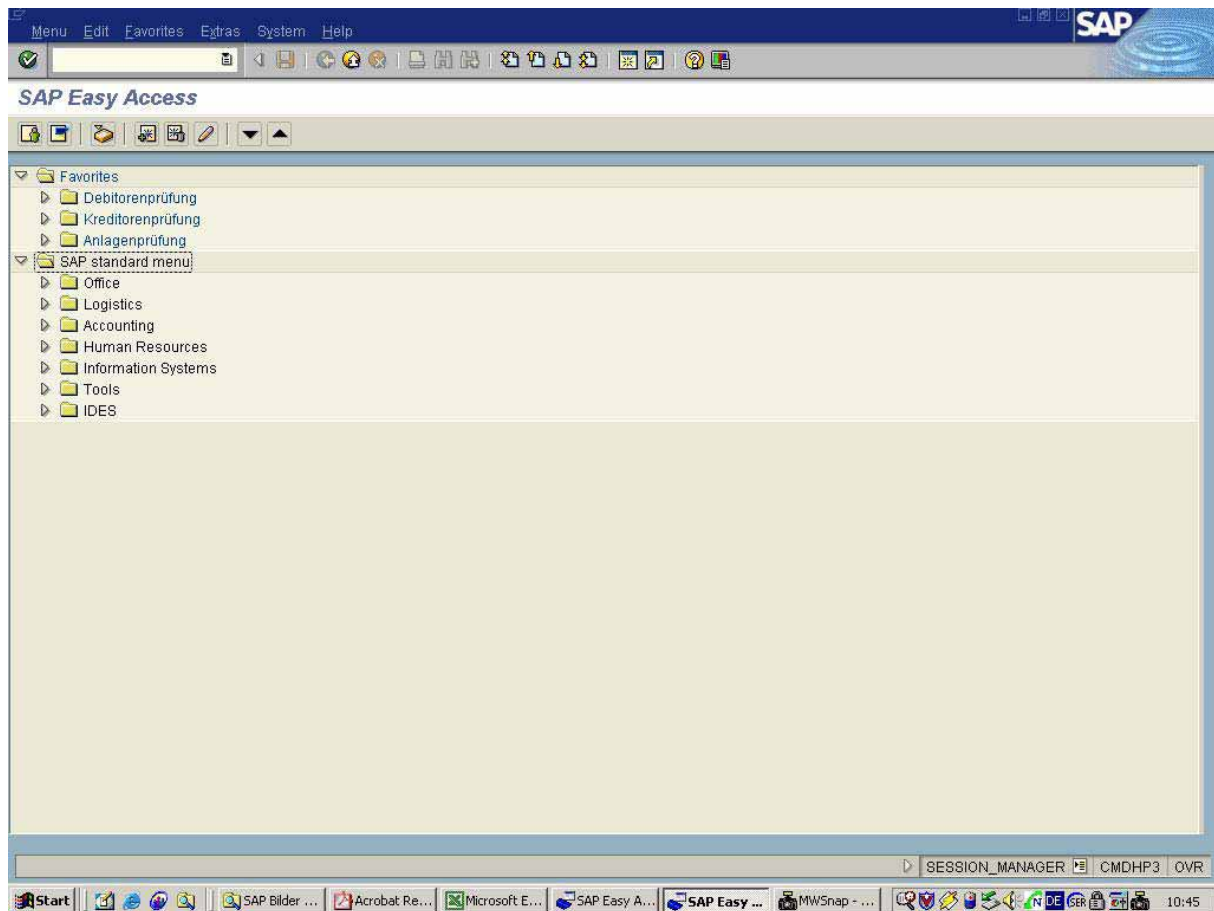


Figure 8: View of an opening screen of SAP R/3™

In the upper screen border, in blue, there is a *title bar* showing the user in which transaction he is currently working. A *menu area* is in the second line on the screen, showing basic functions for using the system, for specific settings and for report layout to the screen.



The third line on the screen contains *the command field and the buttons for saving*, browsing, cancelling transactions, creating new sessions or call for help.

The fourth line is the *title bar*, displaying the current function.

The *application toolbar* is in the fifth line, with buttons for application functions, relevant for the function currently in use. The screen body can be seen below, where relevant functions, fields for selecting screens or reports are displayed.

The menu interface ends with the *status bar* in the lower screen border, where the user finds indications for information, warning and errors. The program or transaction currently in process can also be displayed in the status bar.

## 2.2 Menu layout

The user has several options for changing the user interface layout, e.g. menu font and color of, display or hide menu bars etc. The changes are made by selecting "option" in the menus of the buttons  , depending on the selected interface layout.

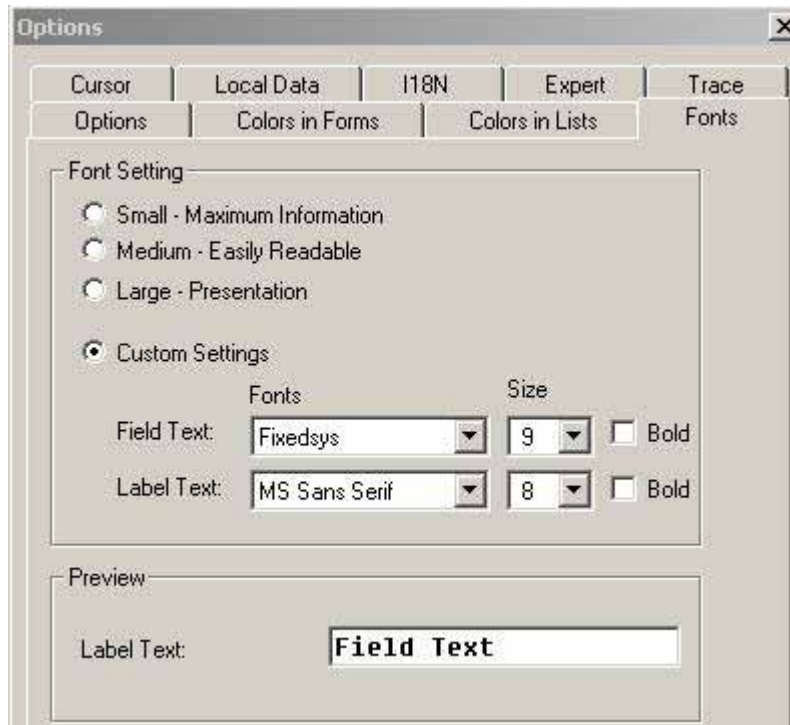


Figure 9: Changing the font on the screen

## 2.3 System operation options

### 2.3.1 Operation via menus

The user can select the function of his interest, using the mouse in the hierarchically structured easy access menus. The availability of functions is depending on the displayed menu. There is a difference between

- User menu  
Only SAP™ functions are displayed, which the user is able to operate based on his authorities
- SAP™ standard menu  
The SAP™ standard menu is displayed, regardless of the user's authorization for operation

Depending on the configuration of the complete system, the user can alter the displayed menu calling

Menu

User menu

SAP standard menu

The availability of specific functions in the menu structure is based on the module and process oriented concept of SAP R/3™.

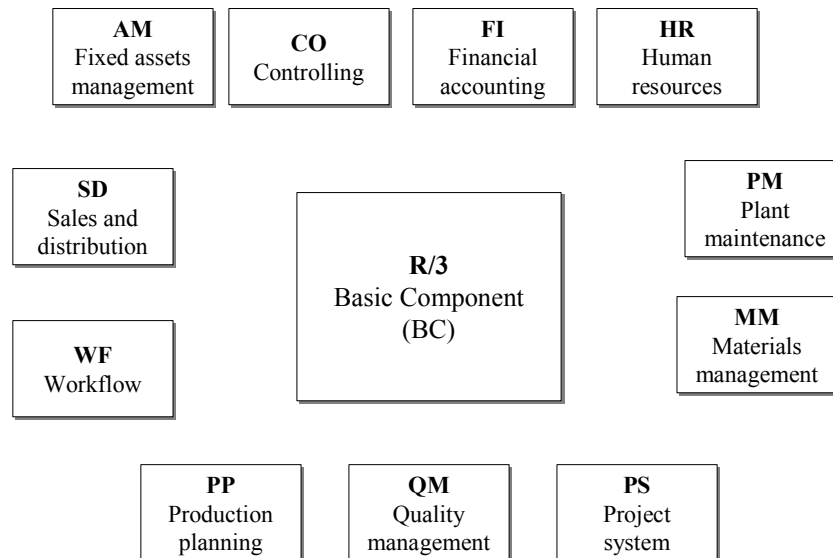


Figure 10: The module oriented concept of an R/3™ system

The functions in the modules MM and SD can be found in the menu “logistics”. The modules FI and CO are assigned to the menu “accounting”. The module HR has its own menu “human resources” and the basis module BC, containing functions for system administration, customizing, authorization maintenance and the data dictionary, is in the menu “tools”.



Figure 11: hierarchically structured menu in SAP™

In addition to the technical menus, the menu “system” is placed in the upper screen border. This menu is displayed at all times, and contains several functions of practical importance. Some examples are

- **Printer selection and setting**

A suitable printer can be selected and set in the menu

System

User profile

Own data

Default (Output Device)

- **Reports and lists**

Reports and lists are created in the menu

System

Services

Reporting

and input of the report name.

- **Transferring information in lists to the local personal computer**

Screen information in reports can be saved to the personal computer, stating the path and the file name, calling

System

List

Save

Local file

- **Managing own print jobs**

Print jobs can be managed, e.g. changed, deleted or printed, in the menu

System

Own spool requests

stating the selected print job.

- **Documenting failed authorization checks**

If a function can not be utilized due to lack of authorization, the auditor can print a document, stating which authorization is missing in order to operate this function, calling

System

Utilities

Display authorization check

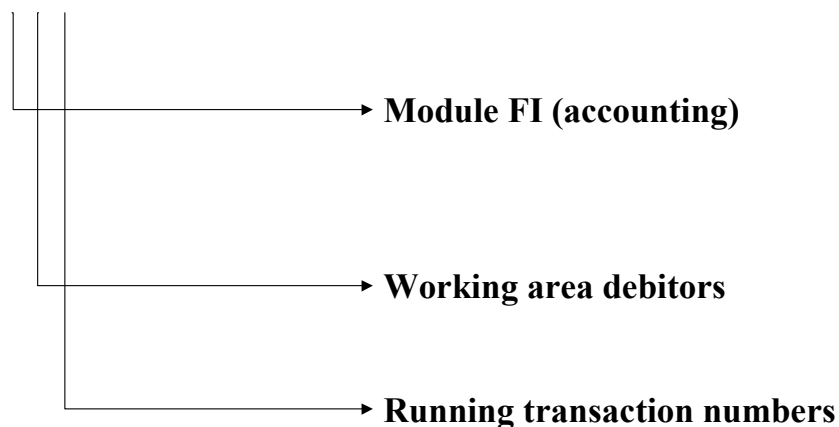
### 2.3.2 Operation via transactions

Transaction codes are short descriptions for SAP<sup>TM</sup> functions and were originally developed for the character oriented processing in SAP R/2<sup>TM</sup> mainframe computer systems, where operations with a mouse were unfeasible. They enable the user to go directly to any transaction, regardless of menu path. This possibility makes it a lot easier to operate the system. The audit should note the most important and audit relevant transaction codes. Different ways are available:

- **SAP<sup>TM</sup> basic functions and transaction names**

The names of the transactions for basic functions are descriptive. The transaction name usually consists of four characters, two letters followed by two numbers. The first letter describes the module, the second letter describes the working area and the two numbers states the extent of authorization needed for the transaction. An example:

**FD03**



- **01** = create
- **02** = change
- **03** = display
- **04** = display changes
- **06** = delete

Transactions are input in the command field in the third line of the upper screen, and confirmed with the enter key.

Calling a new transaction means the previous transaction has to be cancelled. The transaction can be cancelled by input of “/n”. Cancelling the previous transaction has to be connected with the call for the new transaction, so the input for the transaction “display document” would be “/nFB03”. This procedure is valid for all transactions.

- **Identifying transactions via the SAP™ menu**

A rather simple method for learning transaction codes during the operation via menus, is to set SAP™ to display the transaction code during the processing via menus. The auditor has to select the option “show technical name” calling,

Extras

Settings

in the upper menu bar of the opening screen of SAP™. The transaction codes will now be shown in addition to the menu items.

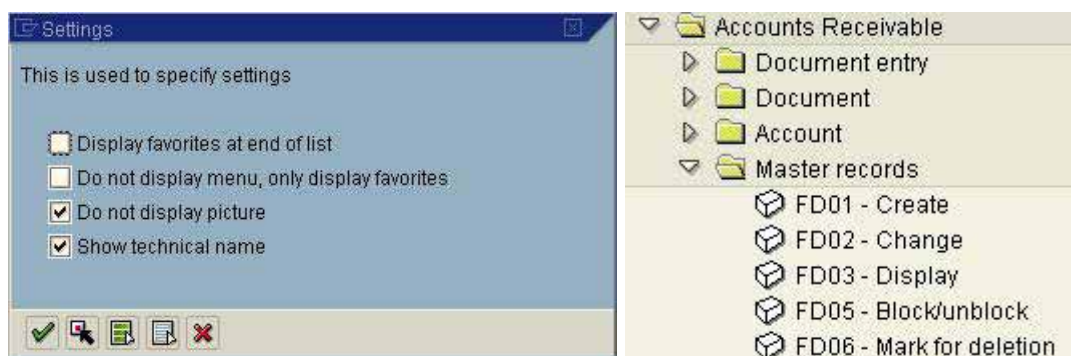


Figure 12: Activating the display of transaction codes in menus

- **Display of transactions in the status bar**

The transactions called via menus will be shown in the status bar on the lower screen, if the user selects the option “transaction”.

- **Display of transaction codes in table “TSTC”**

All transactions within the SAP™ system are controlled in the table TSTC. To obtain an overview, the auditor can use the data browser by calling transaction SE16, and input the table name TSTC. The overview of requested transactions can be limited by a generic search in the field “transaction code”. In order to display all transactions related to accounts receivable the code “FD\*” would be input.



In order to reduce the displayed items on the screen to the relevant fields transaction code and transaction text, those fields only should be activated by calling

- Settings
- List format
- Choose fields

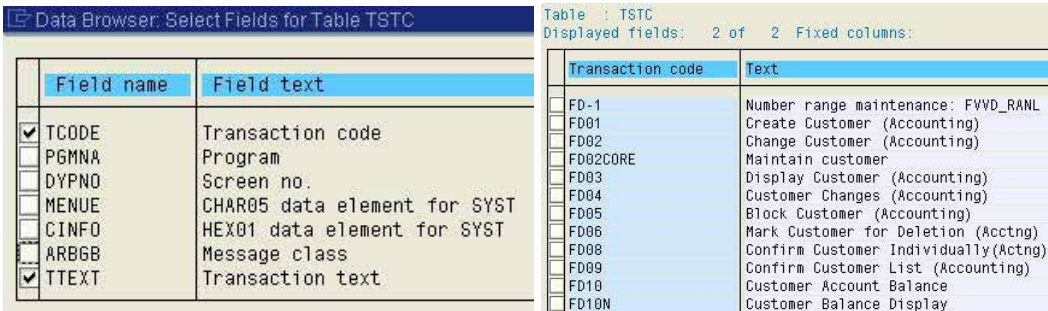


Figure 13: Display of transaction codes related to accounts receivable

2.3.3 Personal menus / favourites

Personal menus connected to the user ID can be created for specific audits in the menu “favourites”. In order to keep clarity, these functions can be kept in folders, created by calling

- Favourites
- Insert folder

in the opening screen. Once the folder has been created, suitable transactions or transaction bundles are marked and then dragged and dropped to the new folder in the menu “favourites”. A copy of the transaction will be created.



Figure 14: Transfer of transactions the menu favourites

The favourites can be placed before of after the standard menus. Additionally, it is possible to show only the newly created menu, reflecting the requirements of the current work phase, calling

Extras

Settings

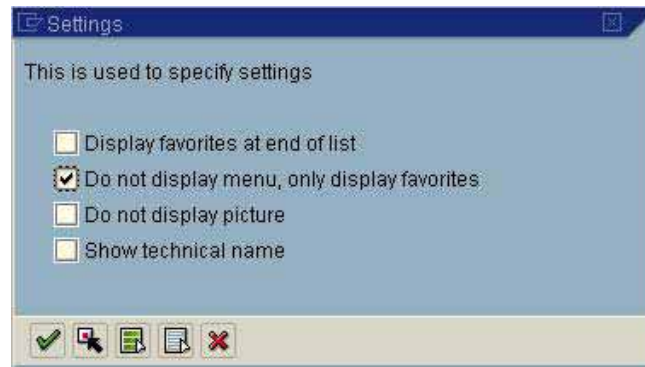


Figure 15: Configuration of the favourite menu

in the opening screen.

### 2.3.4 Operation via the AIS™ auditor work place

The explicit work place for auditors, the AIS™ system, is provided as a standard with SAP R/3™ releases from 4.6. In previous releases this additional function can be installed separately.

In this manual, the AIS™ system will be discussed thoroughly. At this point should merely be noted, that the standard AIS™ system is called in the menu

SAP standard menu

Information systems

Audit Info System

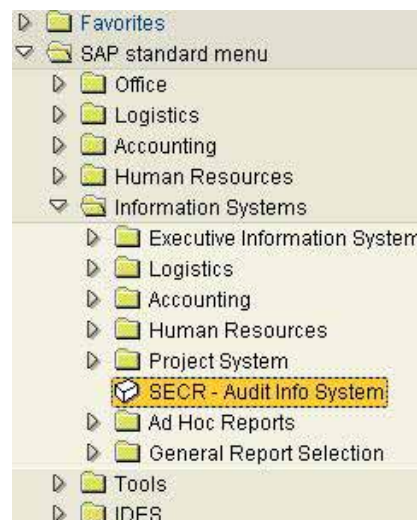


Figure 16: Calling the AIS™ system in the opening screen

Another option for calling a separately installed AIS system, where this menu is not available, is to call *transaction* "SECR"

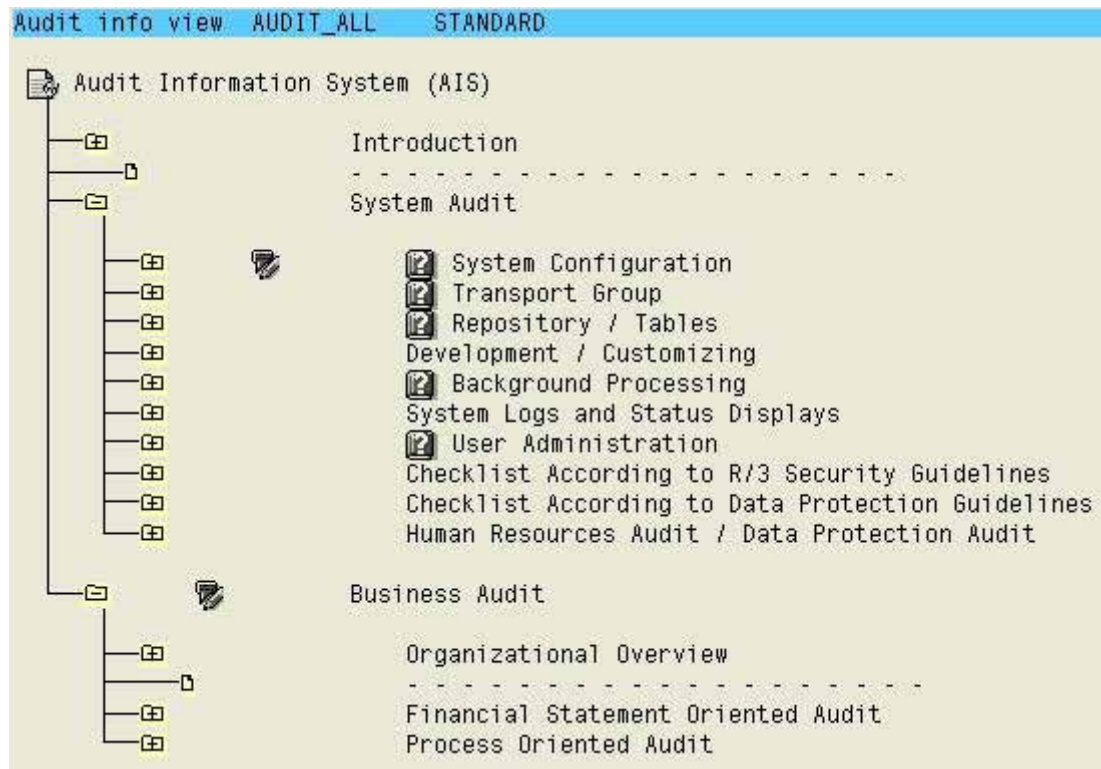




Figure 17: Menu structure in the AIS system

## 2.4 Summary on user interface

Summarized we conclude: the auditor can choose between several options when operating an SAP™ system. In order to achieve the desired outcome, he should chose the option which suits him best.

## 2.5 Tools for the user interface layout

Purpose	Transaction/function	Table	Program
Selecting screen layout	Button "SAP configuration"		
Fonts and colors	Button  		
Menus	Opening screen/user menu/ SAP standard menu		
Printer selection and setting	System/user profile  SU3 and defaults		
Calling reports and lists	System/services/reporting  SA38		Program name
Transferring information in lists to the local personal computer	System/list/save/local file		
Managing own print jobs	System/own spool requests SP01		
Documenting failed authorization checks	System/utilities/display authorization check		
Display of transactions in the SAP <sup>TM</sup> menu	Extras/settings/ show technical name		
Calling the AIS system	Information systems/Audit Info System		

### Exercises on the user interface

1. Printer configuration

Set the printer "LOCL" as default output device, request "delete after output" and "output immediately"

---

---

---

---

---

---

2. Create an overview of all display transactions within financial accounting

---

---

---

---

---

---

3. Expand the SAP<sup>TM</sup> menu by a folder "reports on accounts payable" and add the transactions

- accounts payable – display master records
- accounts payable – display account
- accounts payable – display changing documents

---

---

---

---

---

---

### 3 **Preparing and analyzing SAP™ data**

#### 3.1 **Options for Preparing and analyzing data**

One of the major issues of audit related activities in the SAP™ system is to prepare and analyze the processed and saved data for audit purposes. This will give the auditor useful hints for manual audit work, which has to be carried out. Basically, the following options are available,

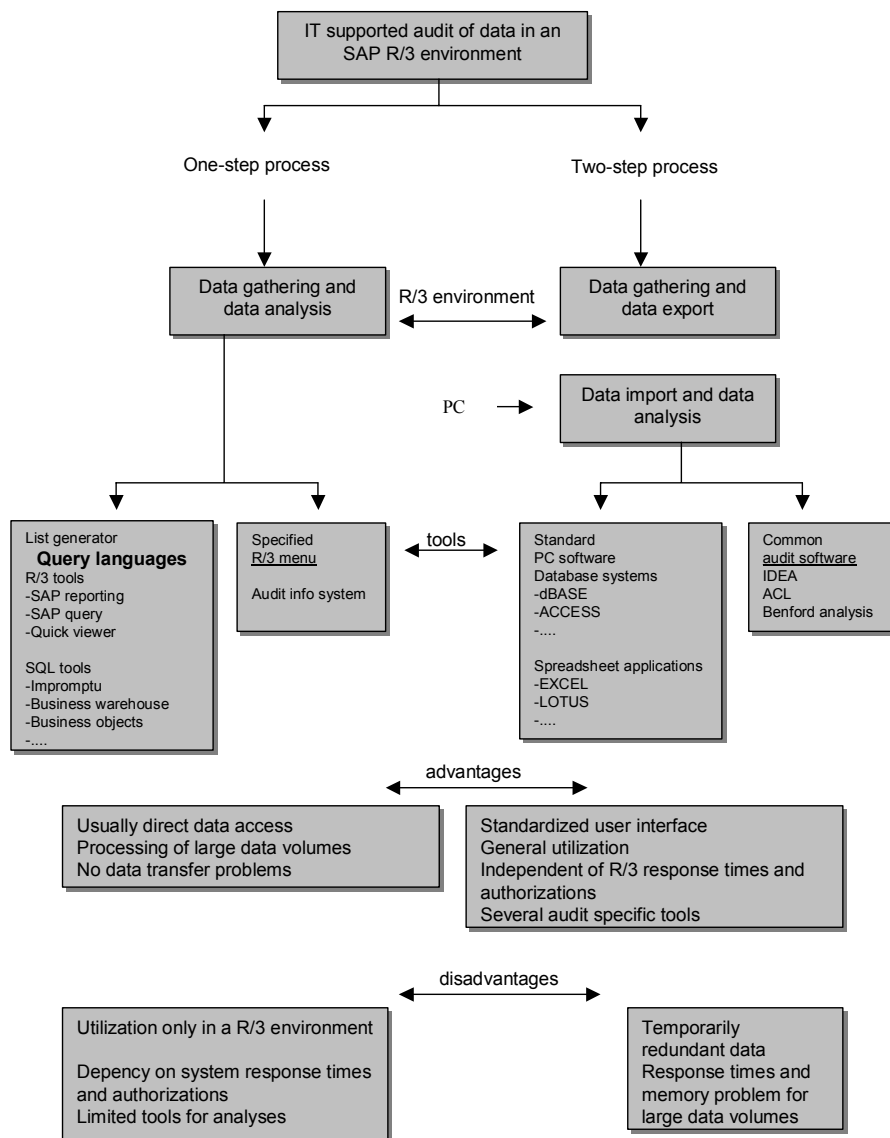


Figure 18: Options for preparing and analyzing SAP™ data

which can be described as processes in one and two steps, and are connected to certain advantages and disadvantages.

#### ❑ **One-step processes**

The analyses of the SAP<sup>TM</sup> data can be done directly in the system. For this purpose, SAP<sup>TM</sup> has developed reports which enable a specifically structured selection, using the selection screen and all options. Additionally, reports can be generated by tools provided for the users, such as the SAP<sup>TM</sup> list generators "SAP<sup>TM</sup> QUERY" and "Quick-Viewer", which are highly interactive and the basic functions are comparable to spreadsheet applications.

In particular the Audit Information System (AIS<sup>TM</sup>) is a great help for auditors. AIS<sup>TM</sup> is summarizing standard reports and specific queries in one set of menus, providing a specialized work place for audit activities.

In addition to the tools mentioned, the auditor can call transaction SE16 or access SAP<sup>TM</sup> table data using secondary tools in order to generate analyses of interest.

The advantages of the one step processes are the direct access to the SAP<sup>TM</sup> data, the possibility to handle large quantities of data with enough memory capacity and avoiding the system straining data transfers to the auditor's personal computer. On the other hand, lack of authorizations for some of the necessary tools, obstructions caused by system delays, the system workload and the lack of audit specific functions have to be considered as disadvantages.

#### ❑ **Two-step processes**

The analysis of SAP R/3<sup>TM</sup> data can also be done in a two-step process. The audit relevant data is gathered in the R/3<sup>TM</sup> system and then leaves the world of SAP<sup>TM</sup>, being transferred to the auditor's personal computer. The auditor analyses the data using a well known spreadsheet application or specific software. For analyzing the data, the auditor is not depending on the running times in the R/3<sup>TM</sup> system or any authorizations. However, during the time of the analyses, he is creating redundant data files and needs to have a sufficiently dimensioned computer and an appropriate analyzing program.

In practice, both kinds of processes are usually combined. In the following sections the described options will be presented in detail.

### **3.2      *Preparing and analyzing table data***

#### **3.2.1.    *Introduction to tables***

For saving data, SAP<sup>TM</sup> is utilizing an external relational database system where the operative application data as well as the program controlling information is stored in tables. Basically it is possible, and under certain circumstances it makes sense, to access the data directly in specific tables.

It has to be noted however, that data related to one and the same topic is allocated to several different tables, which are subsequently communicating via key connections. The data is structured by hierarchy, organizational characteristics and IT supported processes. For example:

*Vendors of a corporate group (client) can be administered, using different terms and bank details in different companies (company codes). Additionally, transaction data such as monthly turn over differs between the companies. Regarding the company processes, it has to be kept in mind that vendor information concerns not only purchasing, but also the financial accounting and the processing of the resulting bookkeeping transactions.*

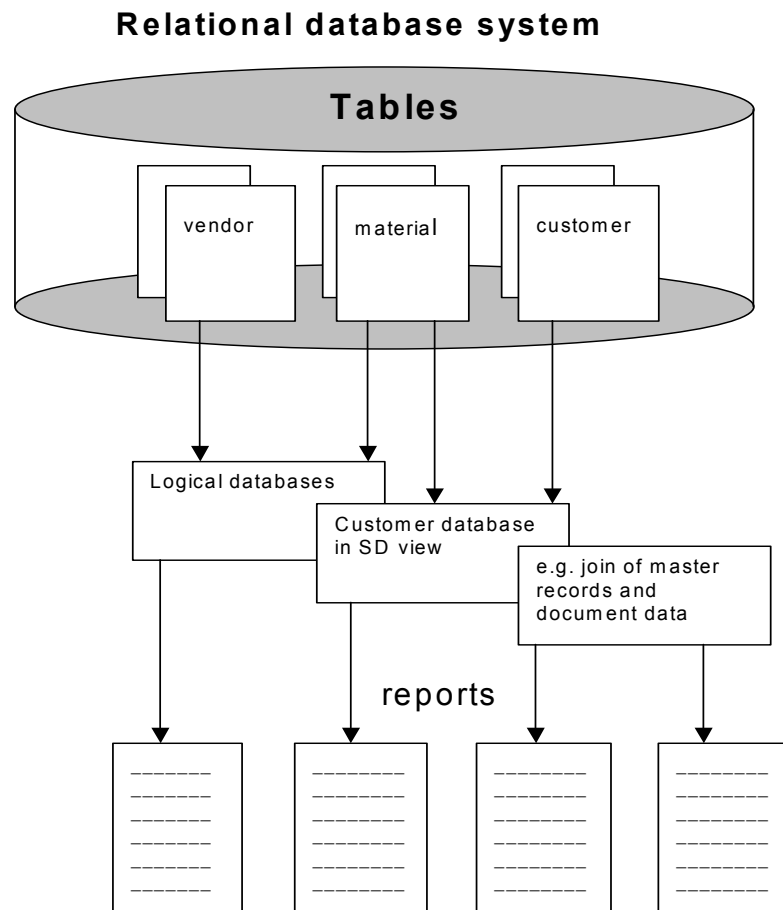
In order to avoid redundant data, several tables are needed to administer all vendor information.

data						
Organization	G/L accounts	Customers	Vendors	Fixed assets	Materials	
Clients (A table)		Customer name Address	Vendor name Address		Material number Material name Vendor	Cross area unit
Chart of accounts	Account name Account no.					Financial accounting
Management accounting						Controlling
Company code (B tables)	Currency Account assignment	Conditions Reconciliation account Bank	Conditions Reconciliation account Bank	Asset name Historical cost		Financial accounting
Business area	Transaction data for financial year					Financial accounting
Sales organization		Turnover, posting authorization Transaction data				and
Purchasing organization			Turnover, conditions, transaction data, discounts			Business data
Plant					Allocation data Valuation prices Buyer	Logistics
Storage location					Inventories Phvsical count data	Storage management

**Figure 19: Structure of data organization and master data administration in the SAP™ system (depending on the system)**

To enable the gathering of useful information in order to respond to a business inquiry, SAP™ is utilizing “logical databases” where technically related tables are brought together. SAP™ reports usually get the data from logical databases.





**Figure 20: Connecting relational tables, logical views and reports**

The above said is meant to explain, why direct preparation of data in SAP<sup>TM</sup> tables is interesting for the auditor only in the rare cases, where the data he needs is kept in one or at the most two tables, and he can connect the data on his personal computer. The advantages of the technically simple generation of table data and the easy transfer to the auditor's personal computer are outweighed by the fact, that the process of transforming table data into useful business information requires further work such as links, calculation and queries in order to create a useful report.

### 3.2.2. Strategies for finding proper tables

Considering the vast amount of tables and their very heterogeneous functions in the SAP™ system, it is not easy to find the proper tables, if the table names are not known. Below, a few strategies for finding the proper tables will be presented:

#### 3.2.2.1 Searching the logical databases

As explained, technically related tables are connected in logical databases by SAP™. By analyzing the logical databases, the proper tables for audit relevant inquiries may be found.

Calling the menu

Tools

ABAP™ Workbench

Development

Programming Environment

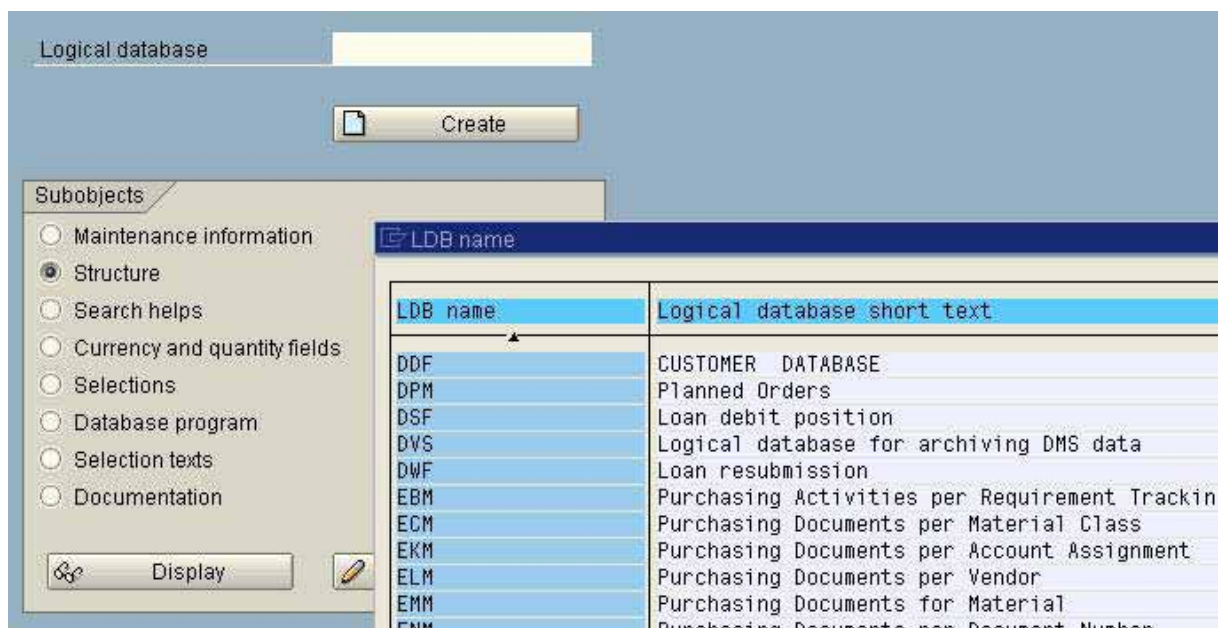


Figure 21: Selecting logical databases

(transaction SE36) will display the logical databases with a short description on the screen. The AIS™ system also offers a limited overview of the logical databases in the menu

Introduction

Preparatory Work (Business Audit)

ABAP/4 Query (incl. Download)

Relevant Logical Databases

Some important databases are listed below with their names and short description:

Name of database	description
ADA	assets database
BRF	document database
BRM	accounting documents
CKM	material master
KDF	vendor database
LMN	stock movements
DDF	customer database
PNP	HR master data
SDF	G/L account database

There is a whole string of additional logical databases.

Node name	Table / Type	Node type	Short text
▼ KNA1	KNA1	Table	General Data in Customer Ma
ADDR1_VAL	ADDR1_VAL	DDIC cat.	Address Data
KNAS	KNAS	Table	Customer Master (VAT Regist
KNKA	KNKA	Table	Customer Master Credit Mana
KNKK	KNKK	Table	Credit Management Cust. Mst
KNBK	KNBK	Table	Customer Master (Bank Detail
▼ KNB1	KNB1	Table	Customer Master (Company C
KNB4	KNB4	Table	Customer Payment History
KNB5	KNB5	Table	Customer Master (Dunning D:
KNC1	KNC1	Table	Customer Master (Transaction
KNC3	KNC3	Table	Customer Master (Special G/L
▼ BSID	BSID	Table	Accounting: Secondary Index f
BSIDEXT	BSIDEXT	Table	Secondary Index & Additions E
▼ BKPF	BKPF	Table	Accounting Document Header
BSEG	BSEG	Table	Accounting Document Segme
WITH_ITEM	WITH_ITEM	Table	Withholding Tax Info.per W/Tax
GSEG	GSEG	Table	Offsetting Items for B-Segmer

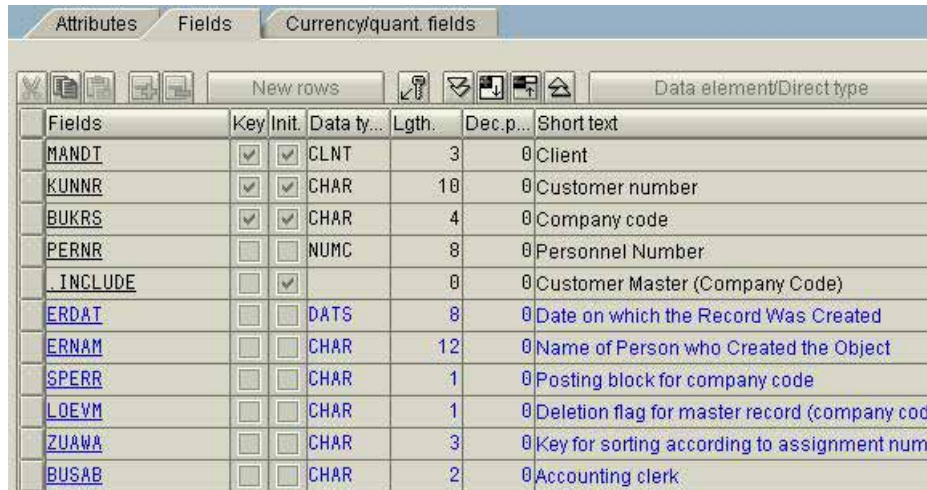
Figure 22: Structure of the logical database "customer database"

Within the display of the logical database structure, the related tables are shown according to their hierarchical structure

A-tables	client level
B-tables	company code level
C-tables	transaction level

The structure of document data shows two stages, document header and document segment.

After marking the proper table, the table fields and their short text can be shown by clicking the right mouse button. Additionally, the report “RDD00DOC” gives detailed documentation and descriptions of the contents in the table data fields.



Fields	Key	Init.	Data ty...	Lgth.	Dec.p...	Short text
MANDT	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	CLNT	3	0	Client
KUNNR	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	CHAR	10	0	Customer number
BUKRS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	CHAR	4	0	Company code
PERNR	<input type="checkbox"/>	<input type="checkbox"/>	NUMC	8	0	Personnel Number
INCLUDE	<input type="checkbox"/>	<input checked="" type="checkbox"/>		0	0	Customer Master (Company Code)
ERDAT	<input type="checkbox"/>	<input type="checkbox"/>	DATS	8	0	Date on which the Record Was Created
ERNAM	<input type="checkbox"/>	<input type="checkbox"/>	CHAR	12	0	Name of Person who Created the Object
SPERR	<input type="checkbox"/>	<input type="checkbox"/>	CHAR	1	0	Posting block for company code
LOEVM	<input type="checkbox"/>	<input type="checkbox"/>	CHAR	1	0	Deletion flag for master record (company cod
ZUAWA	<input type="checkbox"/>	<input type="checkbox"/>	CHAR	3	0	Key for sorting according to assignment num
BUSAB	<input type="checkbox"/>	<input type="checkbox"/>	CHAR	2	0	Accounting clerk

Figure 23: Fields in the accounts receivable database "KNB1"

### 3.2.2.2 Generic table search

SAP™ tries to use descriptive names throughout the system. This may be useful when developing a strategy for finding tables, using generic search terms. After calling transaction SE16 and the DATA-BROWSER, partial table names are input, followed by “\*”. By clicking the arrow next to the command field, the command field will expand. The following are examples of partial table names:

LF*	vendors/accounts payable data
KN*	customers / accounts receivable data
SK*	general ledger data
AN*	fixed assets data
US*	user and authorization data
T0*	data controlling the financial accounting
PA*	human resources data



**Data Browser: Initial Screen**

Table name: kn\*

Tables (30 Hits)

Table name	Short text
KNA1	General Data in Customer Master
KNAS	Customer master (VAT registration nu
KNAT	Customer Master Record (Tax Grouping
KNB1	Customer Master (Company Code)
KNB4	Customer Payment History
KNB5	Customer master (dunning data)
KNBK	Customer Master (Bank Details)
KNBW	Customer master record (withholding
KNC1	Customer master (transaction figures

Figure 24: Generic table search calling transaction SE16

### 3.2.3 Calling and preparing table data

Several transactions such as SM30, SM31 and SE16 can be used for calling tables. Since SM30 and SM31 are transactions for table maintenance, only tables which are maintained by calling these transactions can be accessed. The auditor is therefore advised always to view *table contents by calling transaction SE16 (DATA-BROWSER)*, which will access every table in the system.

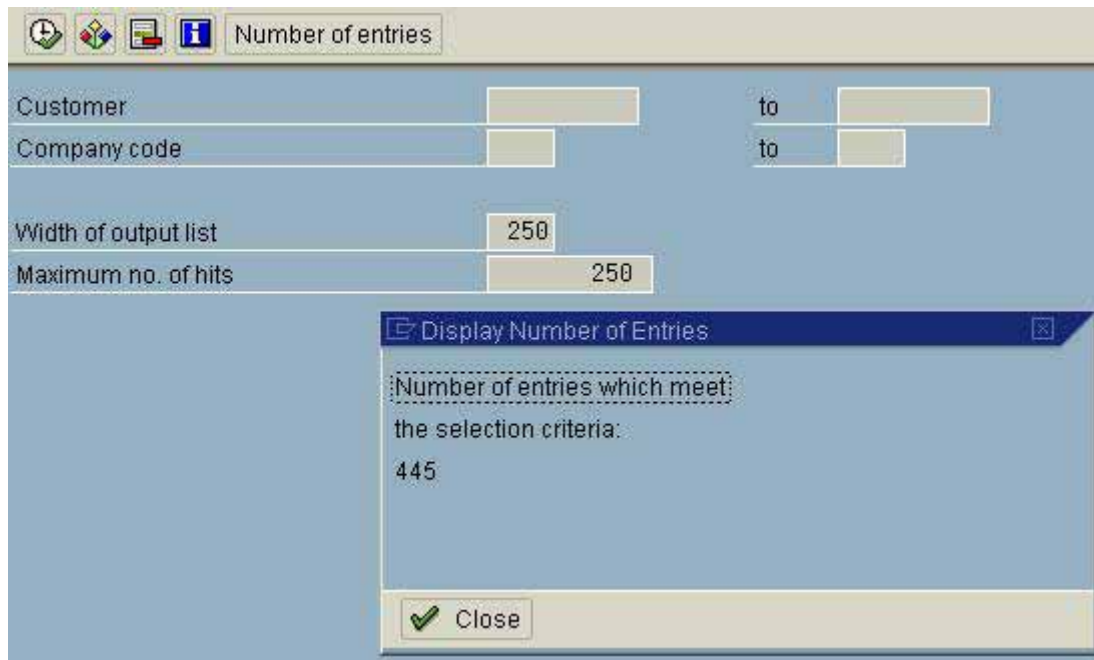


Figure 25: Selection screens and input parameters

Calling the transaction will route the user to a selections screen, which limits the extent of data items to be displayed. The auditor has several options for modifying the selection.

#### 3.2.3.1 Amount of shown data items and selection fields

In every selection screen, the volume of selected items from the database are shown in the lower screen in terms of character width of output list and the maximum number of hits. Both parameters affect the display on the screen. If a table is wider than the stated width of the output list, not all columns will be displayed. The selection of data items is restricted to the stated maximum number of hits. Prior to selection, the auditor should enter his search parameters, using the button "number of entries" in the upper screen and change the maximum no of hits in the input field in the lower screen.

The parameters can be changed generally calling the menu

Settings

User parameters

The maximum number of hits should not be set much higher than the default, in order to avoid unnecessary system load.

In the selection screen as in the displayed table, the technical, and usually incomprehensible, SAP™ field names or the more comprehensive descriptive explanations are shown.

The auditor should choose the comprehensive explanations, calling the menu

Settings

User parameters

Keyword "field text"

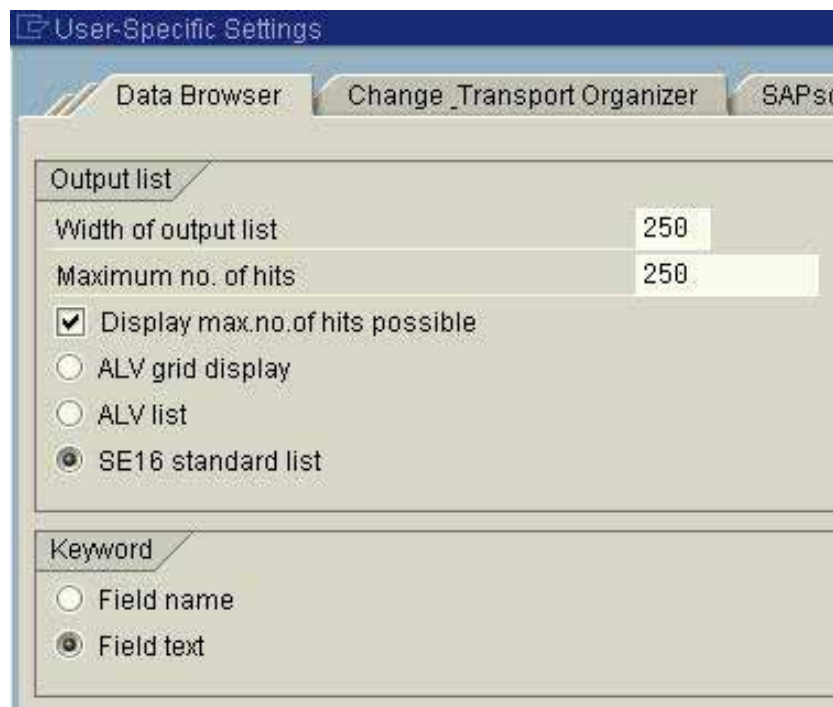


Figure 26: User parameters affecting the screen display

As a tip, all interesting fields that could be selected are rarely shown in the selection screen. However, the auditor can include every table field in the selection screen, which he marks in the menu

Settings

Fields for selection

### 3.2.3.2 Selecting table fields

In the list oriented display of the table fields on the screen, all table fields are shown in chronological order, or are restricted by the width of output list. The user gets a notification in the second table line, "displayed fields", and has the option to widen the list.



Considering, that possibly only a few of the displayed table fields are of interest for the current analyses, the auditor can decide which fields he prefers to see on the screen, calling the menu

Settings

List format

Choose fields

The fields can not be restructured in this menu.



Figure 27: Selecting table fields

An other option is the index oriented display of specific selected data items. These have to be marked by the auditor beforehand. Then the index oriented display of specific data items can be shown, using the magnifier button.

### 3.2.3.3 Sorting data

The system enables not only column headers layout, selection of specific fields and options for displaying data but also quick sorting of any field or combination of fields in a table. Following options are available:

#### ☐ Sorting by one table field

The table field is marked by the field name in the upper screen and the symbol for ascending or descending sorting is clicked. The table will be sorted by the selected field.

#### ☐ Sorting by several table fields

The table can be sorted by several table fields, calling the menu

Settings

List format

Sort

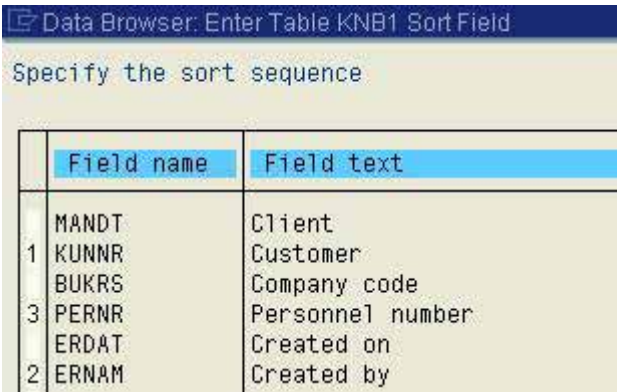


Figure 28: Selecting sorting order in tables

In the displayed screen, fields can be sorted in complex hierarchic order by entering the preferred sorting order.

3.2.4 Downloading data and transfer it to Excel

Once the data is displayed and structured according to the auditor’s requirements, it can be downloaded to his personal computer; where it can be analyzed in depth in Excel for example.

The standard menu

Edit

Download

is available for tables.

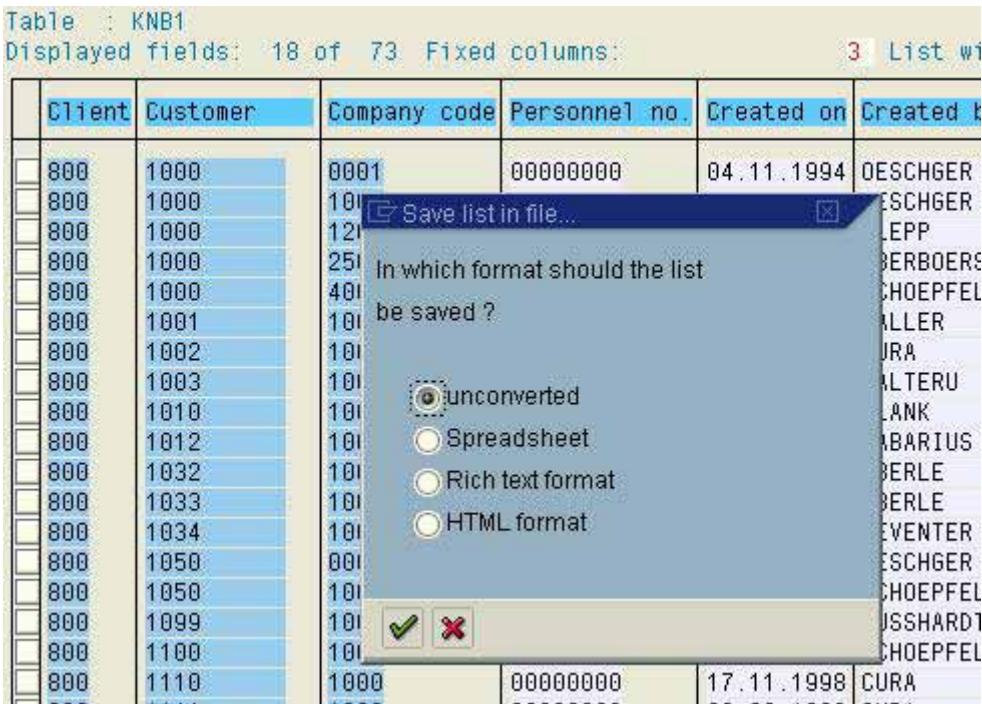


Figure 29: Downloading table data



### The formats

- Unconverted
- Spreadsheet
- Rich Text Format
- HTML format

can be selected. Selecting unconverted or spreadsheet formats will bring identical results. The data will automatically be transferred to the spreadsheet application, e.g. Excel, in the proper columns but will require simple adjustments of the lines. Then the data can be analyzed in depth with the spreadsheet application.

	A	B	C	D	E	F
1	Table :		KNB1			
2	Displayed fields:				Fixed columns:	
3						
4		Client	Customer	Company code	Created on	Created by
5						
6		800	1000	1	04.11.1994	OESCHGER
7		800	1000	1000	04.11.1994	OESCHGER
8		800	1000	1200	30.09.2002	KLEPP
9		800	1000	2500	08.11.1999	OBERBOERSCHG
10		800	1000	4000	07.11.1994	SCHOEPPFEL
11		800	1001	1000	01.12.1994	BALLER
12		800	1002	1000	28.11.1996	CURA
13		800	1003	1000	14.10.1998	WALTERU
14		800	1010	1000	20.03.1998	BLANK
15		800	1012	1000	27.11.1996	FABARIUS
16		800	1032	1000	23.06.1995	OBERLE
17		800	1033	1000	14.06.1995	OBERLE
18		800	1034	1000	03.02.1999	DEVENTER
19		800	1050	1	04.11.1994	OESCHGER
20		800	1050	1000	07.11.1994	SCHOEPPFEL
21		800	1099	1000	04.04.2001	BUSSHARDT
22		800	1100	1000	07.11.1994	SCHOEPPFEL

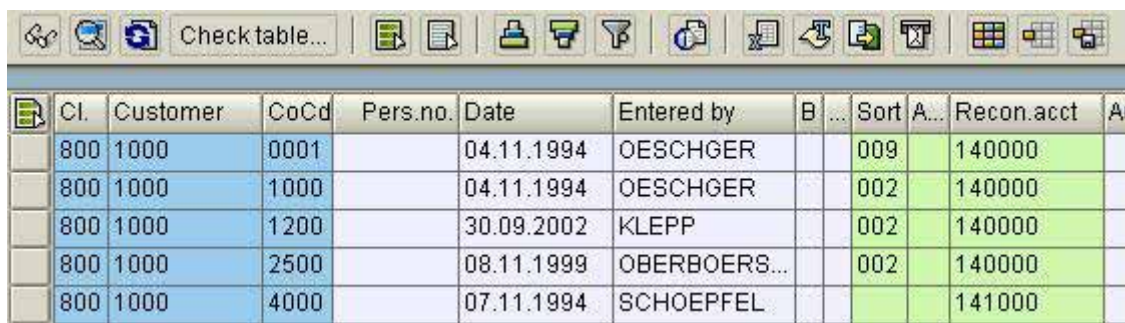
Figure 30: Transferring table data into Microsoft EXCEL

Interactive elements in a table, including a convenient download into Excel, can be obtained by changing the table display, calling the menu

### Settings

#### User parameters

#### ALV grid display (ALV list)



Cl.	Customer	CoCd	Pers.no.	Date	Entered by	B...	Sort A...	Recon.acct	A...
800	1000	0001		04.11.1994	OESCHGER		009	140000	
800	1000	1000		04.11.1994	OESCHGER		002	140000	
800	1000	1200		30.09.2002	KLEPP		002	140000	
800	1000	2500		08.11.1999	OBERBOERS...		002	140000	
800	1000	4000		07.11.1994	SCHOEPPFEL			141000	

Now direct sorting, filtering and similar options are available in the attached symbol bar.

### 3.2.5 Tools for preparing and analyzing SAP™ data

Purpose	Transaction/Function	Table	Program
overview of logical databases	SE36		
generic table search	SE16 and Table	table name with substitute character	
amount of data entries in tables	SE16 and table, button "number of entries"		
changing the number of hits when calling tables	settings/user parameters		
changing "coded" table field names into "descriptive" names	settings/user parameters/"field text"		
additional table fields for selection	settings/ fields for selection		
selecting table fields	settings/list format/choose fields		
sorting table data	settings/list format/sort		
Downloading table data	edit/download		

### Exercises on tables

1. Create an overview of the logical database “assets database”

---

---

---

2. Which tables contain document information

---

---

---

3. Create an overview of vendor master data from a table with the fields

- Vendor - number
- Vendor - name
- Vendor - city
- Vendor – postal code

sorted by “name” and “city”

---

---

---

4. Download the data in the spreadsheet application EXCEL

---

---

---

5. Determine the number of customers in company code 1000

---

---

---

### 3.3. Analyzing and preparing information in reports

#### 3.3.1 Introduction to SAP<sup>TM</sup> reports

Information from the SAP R/3<sup>TM</sup> system is usually generated by calling the huge amount of standard reports, supplemented by internally developed company analyses. An advantage of the pre-structured reports, as opposed to information generated from table data, is that all needed information is integrated in the reports and the user does not have to deal with technical details of the data structure. Additionally, most pre-designed reports present the information in a way, which provides the necessary business sense. The reports have been prepared in a way, which is useful for the auditor and further information has already been added. The disadvantage for the auditor on the other hand, is the inflexible structure, which restricts the possibilities of sorting and selecting specific options. If the auditor utilizes all available options for layout, sorting and selecting report data, a great deal of his audit focused inquiries will be answered by calling the standard reports though. The options will be discussed in detail.

#### 3.3.2 Strategies for finding proper reports

The SAP R/3<sup>TM</sup> system is delivered with a vast amount of standard reports, and it is not always easy for the auditor to find the proper analysis. There are several strategies:

##### 3.3.2.1 Searching the SAP<sup>TM</sup> information systems

Every SAP<sup>TM</sup> application, such as the financial accounting, logistics, the human resources and sales modules, has its own information system, which can be accessed from the application menu in the opening screen. The menu

Accounting

Financial accounting

Accounts receivable

Information system

reports for accounts receivable accounting

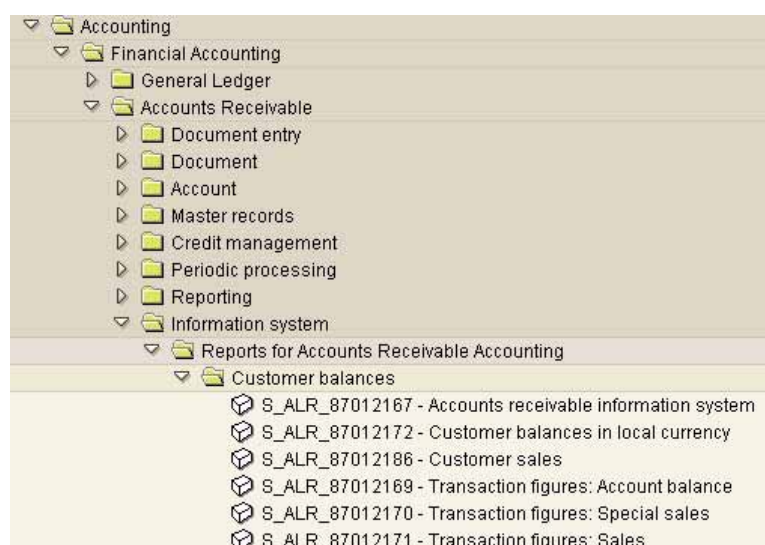


Figure 31: Accounts receivable information system

will take the user to analyses on accounts receivable master records and transactions. Similar analyzing possibilities can be found in all other application areas.

In order to simplify the search, SAP™ shows the menu item “information systems” on the opening screen menu, which takes the auditor to interesting reports in the areas of logistic, accounting, human resources etc.

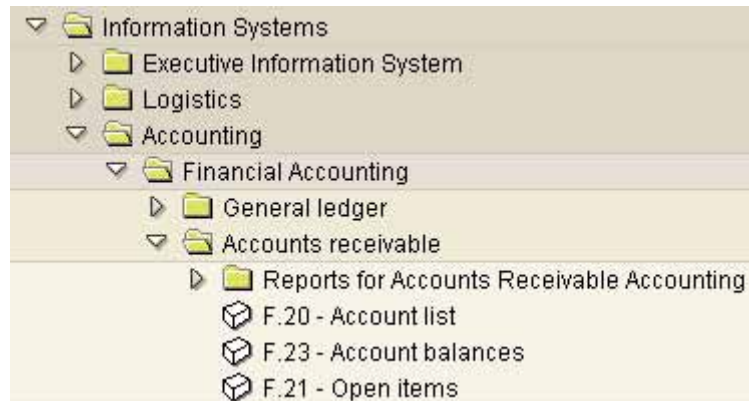


Figure 32: Calling the menu item „information systems“ on the opening screen

Both information systems should be searched in order to find proper reports, as different reports can be found in the specific business areas and in the general information system.

### 3.3.2.2 Generic search by report names

In the presented information system, only those reports can be found, which have been assigned to menus. This is usually only of a part of the reports, which are in fact available in the SAP™ system. The auditor should therefore also include “general reporting” in his search, calling transaction SA38 or the menu in the upper screen bar

System

Services

Reporting

The user will be requested to enter a report name

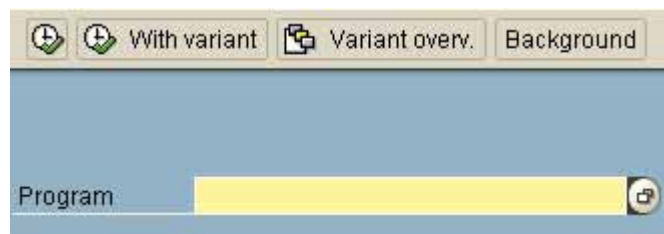


Figure 33: Reporting by calling transaction SA38

Finding reports by their names requires the display of the selection screen in the menu

Utilities

Find program

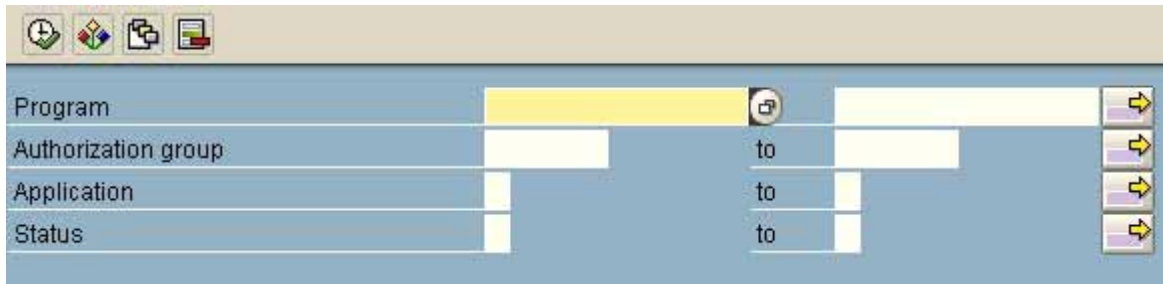


Figure 34: Calling the report selection screen

The following systematic naming convention applies to the SAP™ standard report names:

- *first letter*

SAP™ reports begin with the letter “R”. For customized reports, SAP™ reserves the letters “Y” and “Z”.

- *second letter*

The second letter of the standard report name represents the related application

- F financial accounting
- P human resources
- M materials
- V sales
- A fixed asset reports
- S basis module and system applications

etc. It has to be checked, if in-house developed reports are consistent with this systematic, otherwise the search strategy will be limited to the first letter.

- *third letter*

The third letter of the report name usually identifies the area of information more specifically, even though this systematic is not consistent throughout the system. Some examples are

- RFB document reports
- RFK vendor reports
- RFD customer reports
- RFS general ledger reports

- *fourth and following letters*

The fourth and following letter give additional details on the report contents. Some examples here are:

- RFSKVZ00 general ledger account list
- RFKEPL00 list of vendor line items
- RAABGA01 asset retirements

The generic search is very reliable for the first two letters, and is also sufficiently reliable for the third letter. The search should be limited to the first three letters. The following letters can be substituted by “\*”.

In the selection screen, the user can add the letters representing the required information to the first letter according to the SAP™ reporting systematic. For reports on accounts payable, the search for “RFK\*” will be input in the field “program”.

Program	RFK*		
Authorization group		to	
Application		to	
Status		to	


Figure 35: Search for accounts payable reports in the selection screen

and is confirmed with the execute button. An overview of all reports corresponding to this naming convention is given.

Execute Documentation	
Name	Title
RFKABL00	Display Changes to Vendors
RFKANZ00	List of Down Payments Open On Key Date - Vendors
RFKAP000	List Of Cleared Vendor Items
RFKBLIW0	Belgium : BLIW_IBLC : Open Items of Foreign Vendors
RFKCON00	Display/Confirm Critical Vendor Changes
RFKEPL00	List of Vendor Line Items
RFKFXN20	SWIFT Log Vendor Foreign Payment
RFKKAG00	Vendor Master Data Comparison
RFKKAK00	Open Item Balance Audit Trail by Alternative Account Number
RFKKB000	Open Item Account Balance Audit Trail from the Document Fil
RFKKBUI0	Accts Detailed Listing from Open Item Account Accumulated A
RFKKET00	Extract for Accumulated Open Item Balance Audit Trail
RFKKVZ00	Vendor List
RFKLAK00	Historical Balance Audit Trail by Alternative Account Numbe
RFKLBUI0	Account Details from Historical Accumulated Balance Audit T
RFKLET00	Extract for the Accumulated Historical Balance Audit Trail
RFKOFI02	Print Report for T0336 / Account Determination
RFKOFI05	Reverse Account Determination Simulation
RFKOFW00	Open Items - Vendor Due Date Forecast
RFKOP000	List of Vendor Open Items
RFKOPR00	Vendor Payment History with OI Sorted List
RFKORB00	Internal Documents
RFKORD00	Print Program: Payment Notice

Figure 36: Overview of accounts payable standard reports



Depending on the search term, a *huge amount of reports* corresponding to the naming convention may be displayed. In order to find the relevant reports, the *binocular button*  may be used for a detailed search in the report descriptions.

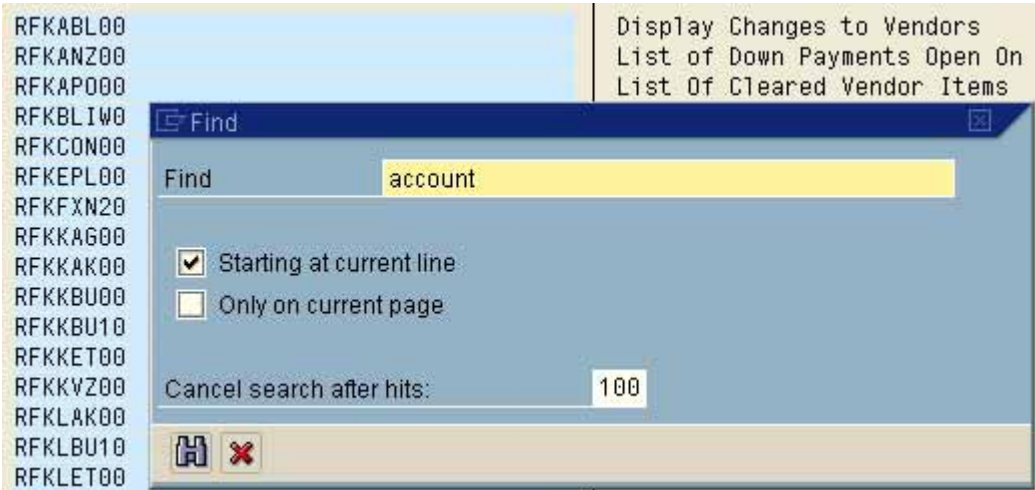
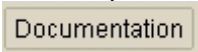


Figure 37: Searching for "account" in the report descriptions

All reports containing this term in their names or descriptions will be displayed separately.

No. of hits: 10	
RFKKAK00	Open Item Balance Audit Trail by A1
RFKKBU00	Open Item Account Balance Audit Tra
RFKKBU10	Accts Detailed Listing from Open It
RFKLAK00	Historical Balance Audit Trail by A
RFKLBU10	Account Details from Historical Acc
RFKOFI02	Print Report for T0336 / Account De

Figure 38: Overview of vendor reports including the term "account"

The relevant report can be called directly by double clicking it. The auditor should make sure, this is the relevant report he is looking for. To do so, he marks the program title and requests the documentation for the particular report by clicking the button  in the upper screen. Additional, in particular technical information, can be called in the menu "goto".



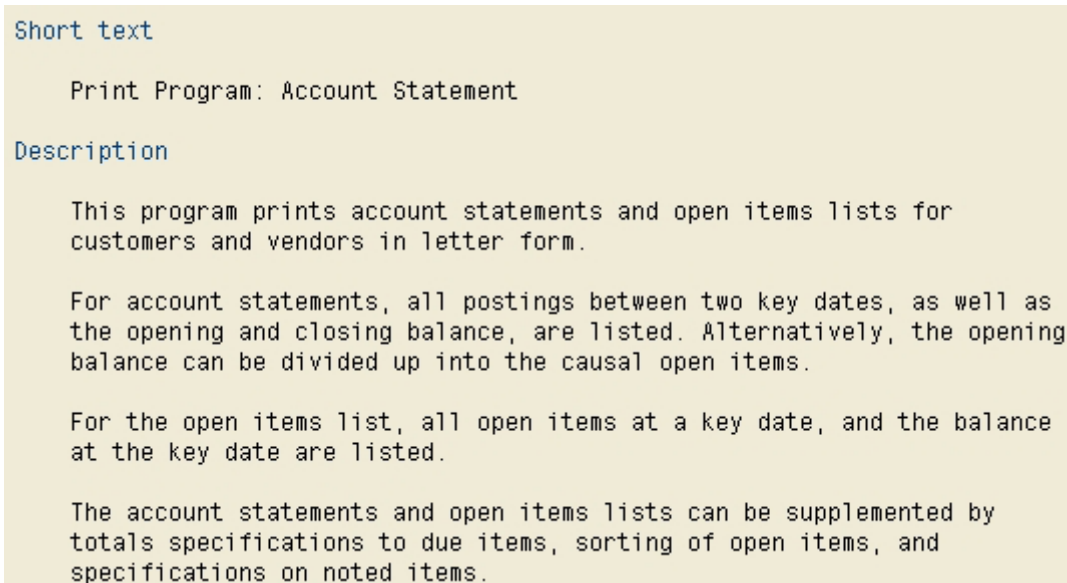


Figure 39: Displaying program documentation

The last step is now to mark the relevant program and start it by using the button "execute".

### 3.3.2.3 Additional criteria for finding reports

In the program selection screen the following additional selection criteria are available

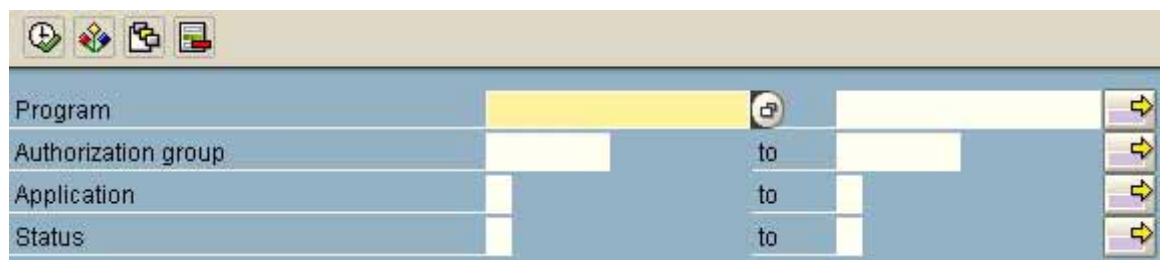


Figure 40: Selection criteria for finding reports

#### - Authorization group

If specific reports have been protected and assigned to particular authorization groups, the auditor can obtain an overview of these reports by entering the authorization group. He will find the created *authorization groups* by calling table *TPGP* in transaction *SE16*.

- *Assigned application*

All SAP™ standard applications are assigned to specific applications such as

- F financial accounting
- P human resources
- M logistics
- S basis / system areas

during development. By entering this application characteristic to the field “application”, an overview of all assigned programs can be obtained.

- *Program status*

Every SAP™ reporting program is created with a specific status.

Program status	Short text
P	SAP standard production program
K	Customer production program
S	System program
T	Test program

Figure 41: Program status overview

The search can be limited to an overview of all SAP™ standard reports, that can be executed by entering the character “P”.

### 3.3.2.4 Summarized strategies

The auditor can specify his search for interesting and relevant information considerably by combining the strategies presented. Additionally, he can print the generated program overviews in order to obtain written documentation of the audit work. This is of particular interest for the occasional user, who is auditing specific areas.

### 3.3.3 Calling and preparing reports

At first glance, SAP™ standard reports seem rather inflexible regarding the possibilities for data selection and preparation and may not appear to be very well suited for answering specific audit relevant inquiries. Taking a closer look, the auditor will find manifold setting options however, which allow fine tuning of reports and even the auditor’s needs for information will be satisfied. This will be discussed in detail.

### 3.3.3.1 Selection screen layout

Every SAP™ standard report is being called in an assigned selection screen.

The screenshot shows an SAP selection screen with the following sections and fields:

- Customer selection:**
  - Customer account: [ ] to [ ]
  - Company code: [ ] to [ ]
- Selection using search help:**
  - Search help ID: [ ]
  - Search string: [ ]
  - Complex search help: [ ]
- Line item selection:**
  - Open items at key date: 03.12.2002
- Output control:**
  - ☐ Summary sheet only
  - ☐ Corporate group version
  - Column I due in: 8
  - Column II due in: 30
  - Rdg factor/decimal places: 0 / 0

Figure 42: Example of a report selection screen

The screen has two major purposes:

- *Selecting data items*

The common input fields are in the upper selection screen. The number of fields displayed is depending on the area of information and differs for every report. The field input is supported by the keys

- F1 notes on input options
- F4 company specific match code search

The match code search is very useful in cases where only partial information for the input is known, such as partial account numbers, names or cities.

- *Report layout and output controls*

The “output control” can usually be seen only after scrolling to the very bottom of the screen. The report layout can be modified here, by changing elements like report layout, sorting, subtotals etc.

### 3.3.3.2 Fine tuning the selection

The selection screen does not consider the specific requirements of internal and statutory auditors regarding audit inquiries such as

*Which employee processed credit notes for the customer Smith exceeding a total of EUR 10.000 on December 25?*

*In a stratified selection of payment documents, only credit postings, payments in the range of EUR 10.000 to EUR 20.000 as well as all payments exceeding EUR 100.000 should be included.*

The selection screen offers additional options in order to provide answers:

- *Dynamic selection*

Using the button  or calling the menu

Edit

Dynamic selection

all interesting data fields related to the topic of the report can be selected.

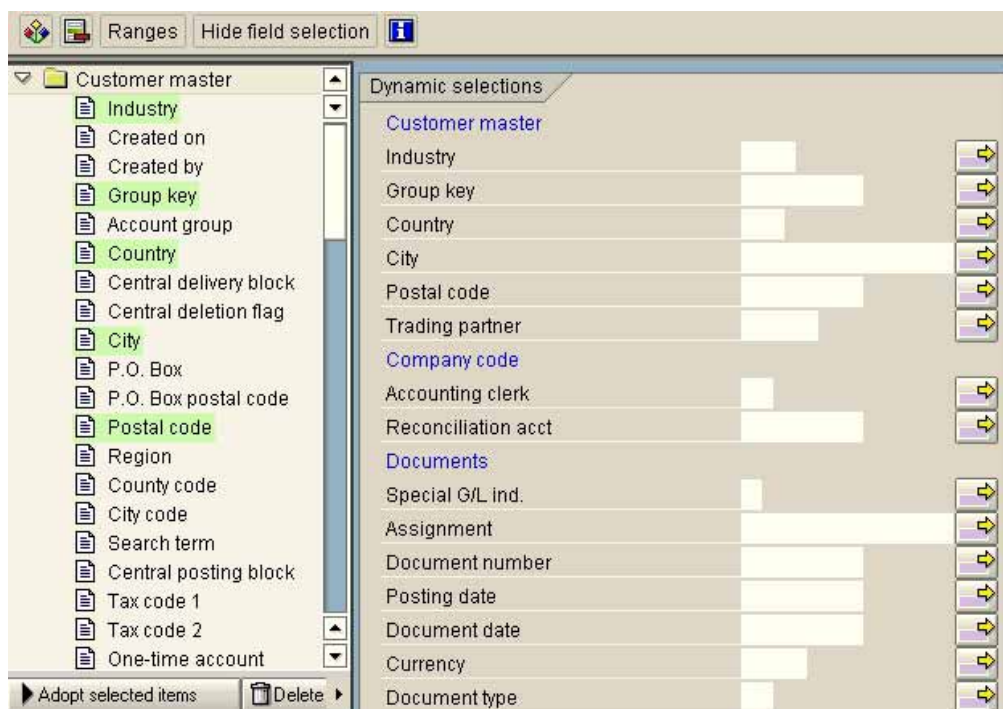



Figure 43: Input screen for dynamic selections

The fields on the left side of the screen can be added to the selection screen displayed to the right.

- *Multiple selection*

The button  offers multiple selection in every field. This enables a simultaneous differentiated input for one and the same field

- Single vals >0
- ranges 10.000 to 20.000
- single vals < 100.000

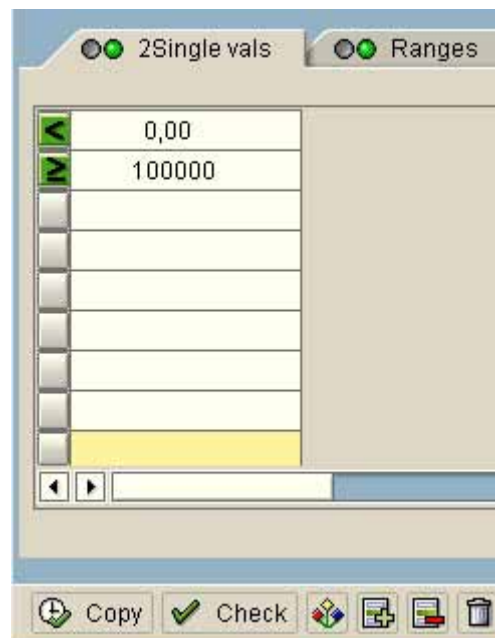



Figure 44: Example for multiple selection in a field

If a multiple selection has been activated, the button turns green.

- *Selection options*

A third possibility for fine tuning the reports are the selection options, which also can be utilized for every selection field. These are called by using the button  or the menu

Edit

Selection options

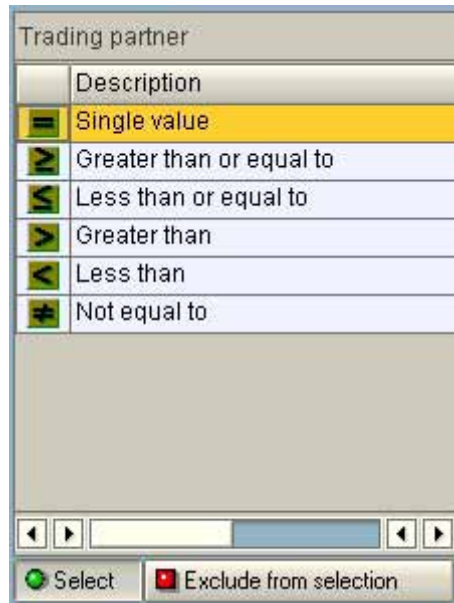


Figure 45: Selection options

Since the elements for report layout

- dynamic selection
- multiple selection
- selection options


can be combined, there are only few remaining audit inquiries, which can not be covered by standard reports.

### **3.3.4 Utilizing report variant techniques for audit purposes**

#### **3.3.4.1 Basic variant techniques**

The fine tuning of reports, taking audit specific reporting requirements into consideration, takes a lot of effort in many cases, and the auditor may want to save the outcome in the SAP<sup>TM</sup> system for future purposes. This is of particular importance, if the control awareness within the user departments of the company is increased as conspicuous issues are revealed on a regular basis. The R/3<sup>TM</sup> system offers interesting possibilities, which will be discussed in detail.

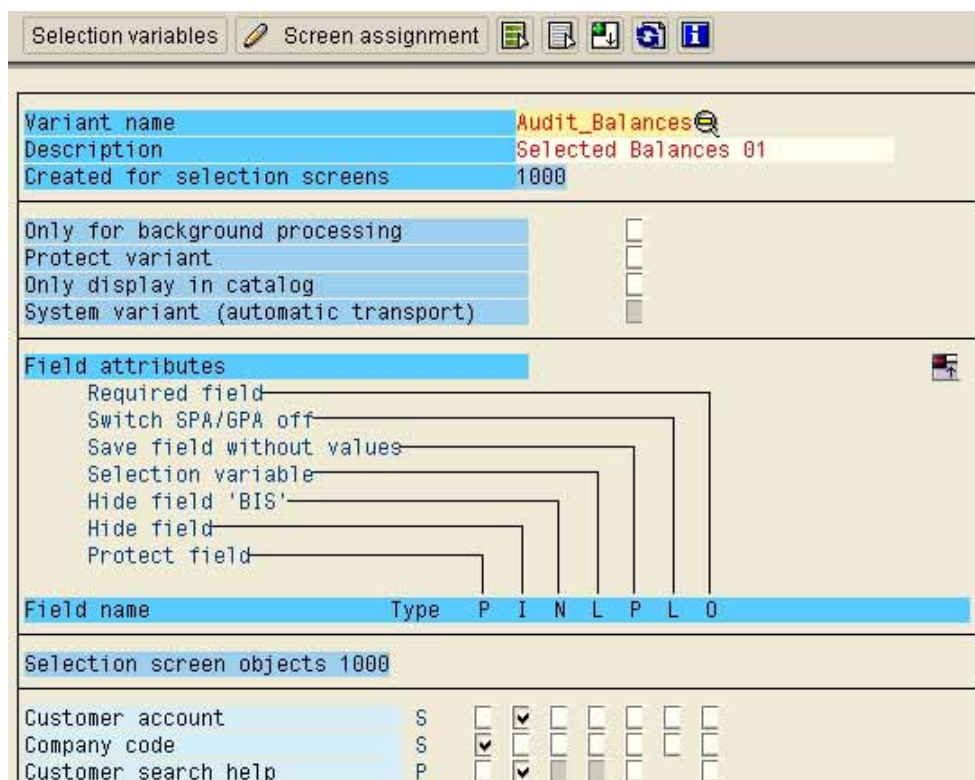
### 3.3.4.2 Static variants

After completing all selection criteria in the selection screen, the outcome can be saved by using the button  or calling the menu

goto

variants

save as variant



Field name	Type	P	I	N	L	P	L	O
Customer account	S	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Company code	S	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Customer search help	P	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 46: Input screen for saving variants

The user specific variant name and a note on the purpose and the contents of the variant is input in the field "description". The auditor now has several options, which will influence the call of the variant.

#### ☐ general protection "protect variant"

If the auditor prefers to get the same outcome every time the variant is called, based on the settings in the variant, he should mark this field. The variant can be changed by the auditor alone, and the input fields in the selection screen can not be overwritten when the variant is opened.

#### ☐ Field specific settings

In addition to the general variant protection, there are options for every field in the selection screen and for the unlimited selection.

##### - protect field

If a selection field is protected, the auditor can still see the settings of the variant, but they can not be overwritten when opening the variant.

- *hide field*

To strictly avoid input in a field when opening a variant, the field can be hidden in the selection screen. This is useful for audit purposes, if third parties should not be able to identify the selection criteria or if the fields are of no importance at all for the report.

*Examples of usage:*

If the regular reports should include documents with certain amounts for a specific company code, the corresponding items should be input in the selection screen. The variant should have general protection, fields without input should be hidden and field input should be protected from overwriting.

The advantage of static variants are the fixed report links within the system, which are used on a regular basis. The disadvantage on the other hand, is the necessity of creating and maintaining various variants for similar reports if they regard different company codes.

### **3.3.4.3 Dynamic variants**

In order to keep the advantages of the variant technique, but still limit the quantity and adjust the variants to regularly changing selection options, it is possible to obtain selection field input using data from the external table TVARV. The AIS audit work place is utilizing this technique, as AIS consists of dynamic variants of standard reports in large parts.

Two steps are required for dynamic variants:

- *Create the variable and input data in the table TVARV*

The TVARV is a cross client table. Auditors do usually not have the authorizations to maintain cross client tables, and the creation and data input in such variables have to be co-ordinated with the administrators.

The auditor has to decide if he wants to create his own variables in the table, which then should be identifiable by their names.

Example:

- RV\_BUK
- RV\_BALANCE
- RV\_fin\_year

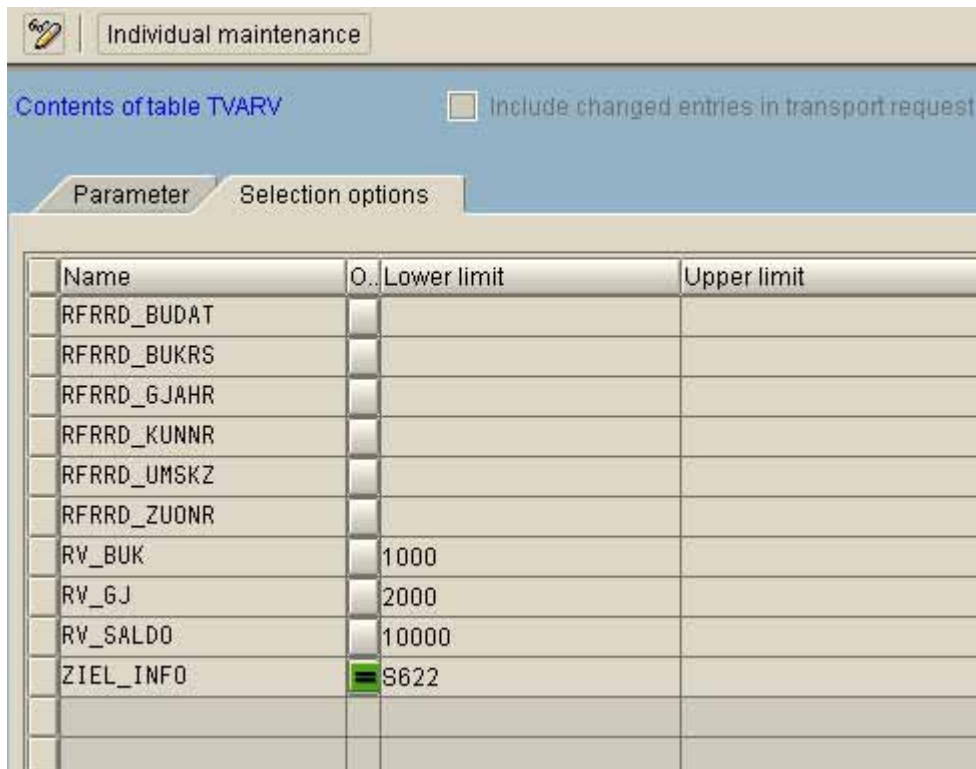
Alternatively, he can use the pre-prepared variables in the AIS (Audit Information System), which are identifiable by the prefix "AU".



Example:

- AU\_BUK
- AU\_financial\_year
- AU\_receivable\_exceeding\_n

Which option to use should be decided by the purpose of the variable. If the statutory auditor is using the variables in the Audit Information System, he will input them when the audit begins, regardless if they serve the purposes of the internal auditors. In this case it may be useful for the internal auditors to create their own variables, otherwise they should use the variables already available.



Name	O.	Lower limit	Upper limit
RFRD_BUDAT	<input type="checkbox"/>		
RFRD_BUKRS	<input type="checkbox"/>		
RFRD_GJAHR	<input type="checkbox"/>		
RFRD_KUNNR	<input type="checkbox"/>		
RFRD_UMSKZ	<input type="checkbox"/>		
RFRD_ZUONR	<input type="checkbox"/>		
RV_BUK	<input type="checkbox"/>	1000	
RV_GJ	<input type="checkbox"/>	2000	
RV_SALDO	<input type="checkbox"/>	10000	
ZIEL_INFO	<input checked="" type="checkbox"/>	S622	

Figure 47: Maintaining selection variables in table TVARV

The selection variables are assigned within the variants in a second step.

- Assignment of table variables to selection fields in the variant

In order to use the variables listed in the table TVARV in a variant, the button "selection variables" in the variant screen has to be marked for that field when saving the variant.

Field name	Type	P	I	N	L	P	L	O
Company code	S	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Customer search help	P	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alternative local currency	P	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Translation date	P	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fiscal year	S	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 48: Marking variant selection fields as selection variables

The button “selection variables” in the upper screen is clicked, and all selection variables are shown. In the column T (table variable), the variables in the table can be selected and assigned by clicking the arrow pointing downwards.

Selection criterion	T	D	B
Variable name			
Company code	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
AUDI_BUCHUNGSKREIS	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fiscal year	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
AUDI_BERICHTSJAHR	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Account balance	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
AUDI_FORDERUNGEN_GROSSER_N	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Choose selection variables**

- AUDI\_FORDERUNGEN\_GROSSER\_N
- AUDI\_FREMDWAHRUNG
- AUDI\_KONTENPLAN
- AUDI\_KREDITKONTROLLBEREICH
- AUDI\_L\_AUSLAND
- AUDI\_L\_INLAND
- AUDI\_PRUEFUNGSDATUM
- AUDI\_STICHTAG-VON/BIS
- AUDI\_STICHTAG\_BIS
- AUDI\_VERBINDLICHK\_GROSSER\_N
- RESPONSIBLE COST CENTER
- RFRD\_AUGDT
- RFRD\_BUDAT
- RFRD\_BUKRS

Continue Values X

Figure 49: Assigning table variables to a selection field

After assigning all variables, the variant can be saved in the SAP™ system by clicking the disc button. For future purposes, all dynamic variants, which are related to these table data can be updated by adjusting only the table variable to the current audit situation.

#### 3.3.4.4 Calling report variants

Report variants are called by selecting the sought program using the buttons “with variant” or “variant overview” in the upper screen. The available variants are shown and can be selected and started without further entries.

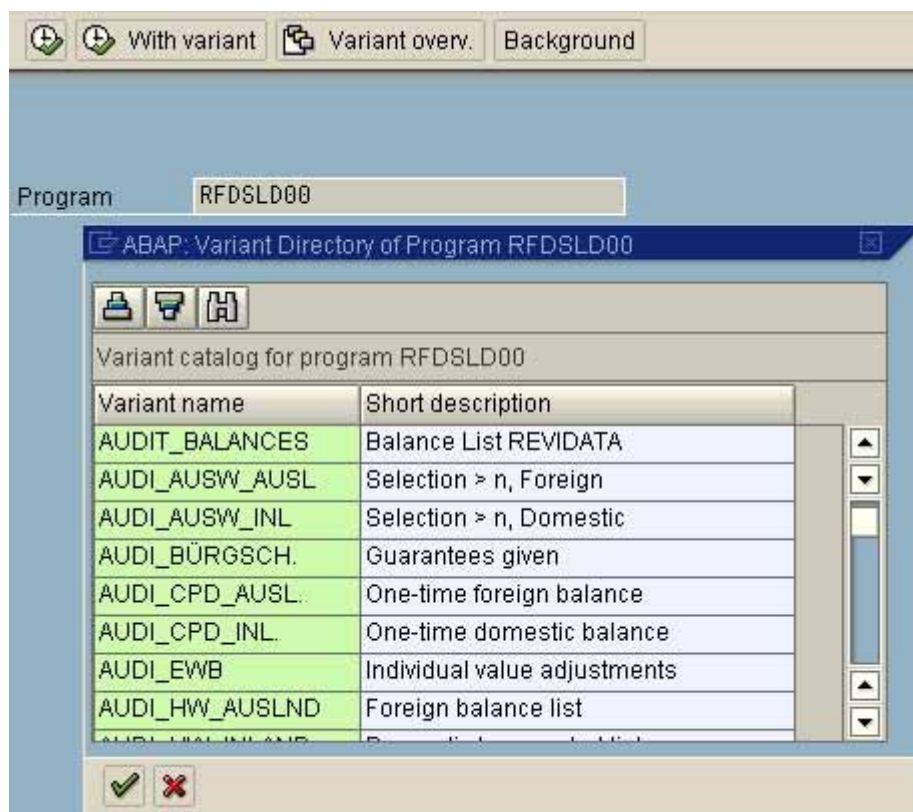


Figure 50: Further options for using reports

#### 3.3.5 Further options for using reports

Voluminous analyses by statutory or internal auditors may cause undesirable load on the system performance. The response times for dialog programs is therefore limited, and no output can be obtained if the processing exceeds the time limit. The user can run these programs during periods of low system load, however. For this purpose the button “Background” **Background** in the upper screen is clicked after entering the program to be run.

As soon as the user has input his reports, he should notify the administrators, who will see to the starting of the scheduled program.

The auditor still can save generated lists for continuous usage in the SAP™ system, as soon as the list contents appear on the screen, by calling the menu

System  
List  
Save  
Office folders  
Private folders



Figure 51: Saving a list in the private folder

Lists saved this way can be found in the opening screen menu

Office  
Workplace  
Private folders

sorted by topic and listing necessary information.

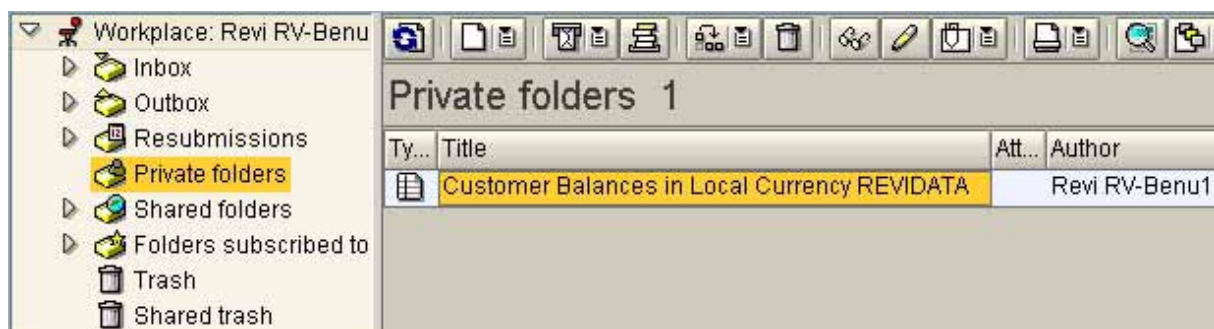


Figure 52: Overview of the auditor's private folders

By double clicking a selected list, the contents can be printed or displayed on the screen.

Comp	Reconcil.	Customer	Search tm	Sp.	Balance at	Reporting period	Reporting period	Debit balances
code	account	number	(short rme)	G/L	start of period	debit total	credit total	
1000	140000	Trade Receivables - domestic			347.086,66	9.887.654,80	10.226.832,41	7.909,05

Figure 53: Calling a list in the private folders

### 3.3.6 Download and usage of list contents

All reports displayed on the SAP™ screen can be transferred to a personal computer, if the authorization has been provided, using the menu

System  
List  
Save  
Local file

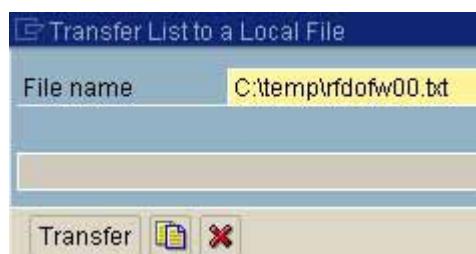


Figure 54: Transfer of a list file to the personal computer

The result is a print file with all list elements, such as headers, page breaks, sub-totals and totals.

If the file is to be analyzed further in Excel or in a specific audit software, it is necessary to transform the hierarchic structure into a database format and eliminate all undesired list elements prior to analyzing the data. Specific programs, such as Monarch or DataImport or the foreseen functions in the audit software WinIDEA (import print file) or ACL (import report file) enable the transfer.

The first step is to mark and select all data elements in the list, which are required for the input.



- 57 -

A:CC	B:BA	C: BALANCE
03.12.2002		Open Items - Customer Due Date Forecast
1000		Becker Berlin
		Insurance limit.....
		Open items per 03.12.2002
CC	BA	Open In total
		In 8 days
		In 30 days
		Over 30 Days
1000		135.455,56
1000	0001	46,40
1000	9900	58.000,00
1000	****	193.409,16
03.12.2002		Open Items - Customer Due Date Forecast

Figure 55: Selecting data items, using the software WinIDEA

In the second step, the layout can be switched to show a table oriented layout, displaying the data in the preferred format.

	NUMBER	NAME	CC	BA	BALANCE
1	1000	Becker Berlin	1000	0001	-46,40
2	1000	Becker Berlin	1000	9900	58.000,00
3	1012	Autohaus Franzl GmbH	1000	0001	116.510,40
4	1032	Institut fuer Umweltforschung	1000	8000	571,00
5	1034	ERL Freiburg	1000	8000	571,00
6	1050	Becker AG	1000	0001	106.596,00
7	1172	CBD Computer Based Design	1000	8000	638,00
8	1200	Minerva Energieversorgung GmbH	1000	0001	16.918,75
9	1360	Amadeus	1000	0001	1.520,07
10	2130	COMPU Tech. AG	1000	0001	225,02
11	2140	N.I.C. High Tech	1000	7000	3.743,78
12	2141	Jaspers Computers	1000	8000	3.016,00
13	2152	Bit Market	1000	7000	1.890,80
14	2300	Enjoy Motomarkt Heidelberg GmbH	1000	0001	6.397,90
15	3450	Norbert Neumann	1000	9100	-10.470,75
16	3450	Norbert Neumann	1000	9900	-3.984,75
17	3452	Karin Keller	1000	9900	-310,50
18	3453	Susanne Schenk	1000	9100	1.667,50

Figure 56: Displaying the data from a list in a table format

In the final step, the transformed file can be saved in any common format, used by spreadsheet applications and database programs.

### 3.3.7 Summary on reports

As the presented reports show, almost any audit relevant report can be generated in the system, based on SAP™ standard reports. Additionally, the possibility of saving reports in the system, in order to enable the calling of specified reports on a regular basis is of particular interest. As a result of consistent utilization of this possibility, the auditors will build up a powerful information system in due time. If additional analyses of report information are required, the presented audit software can be used for such purposes.

### 3.3.8 Tools for report layout

Purpose	Transaction/Function	Table	Program
Calling reports	SA38 and programs		
Finding reports	SA38 and selection screen and program name with substitute character		
Selection screen for finding reports	Utilities/find program		
Report documentation	Button "documentation" or goto/documentation		
Additional field for selection	Dynamic selections		
Input several different values for one field	Multiple selection		
Fine tuning of field input	Selection options		
Downloading list data	System/list/save/local file		
Create variant	Goto/save as variant and variant parameters		
Processing reports in the background	Button "background" and notification to administrators		
Saving reports in the personal SAP folders	System/list/save/office folders (personal folders)		
Calling the personal folders	Office/workplace/personal folders		

### Exercises on reports

1. Find the report “open items – customer due date forecast”

---

---

---

---

2. Choose the report and add values exceeding EUR 100, 2 decimals and ranges of 60 and 90 days to the selection

---

---

---

---

3. Save the report as a variant. Set the company code for the table variant AUDIT\_company\_code

---

---

---

---

4. Call the saved variant and save the list in the “private folders”

---

---

---

---

5. Download the list from the private folders to your personal computer and transfer the file to Excel or audit software.

---

---

---

---



### 3.4 Using the list generator SAP™-Query

#### 3.4.1 Introduction

SAP provides ABAP/4™ query, a so called “list generator”, which enables the user to create his own reports without having detailed knowledge of the programming language ABAP/4. The utilization of the list generator requires some administrative effort in order to set up the tool for audit purposes.

The related functions for calling SAP™ query in releases later than 4.6 can be found in the menu

System

Services

Quick viewer

and the button “SAP-query” (transaction SQ01).



Figure 57: Calling the list generator "SAP™-query"

The philosophy behind the list generator is to allow users in the business units to easily create their own reports based on data, which has been pre-structured and pre-defined by topic. In order to enable that, the functional areas and the related sphere of necessary data have to be defined and created. The functional areas are assigned to user groups, which have to be defined.

The individual user has to register in one or more groups. The assignment to user groups and their related functional areas will determine, which data the user can select within the list generator.

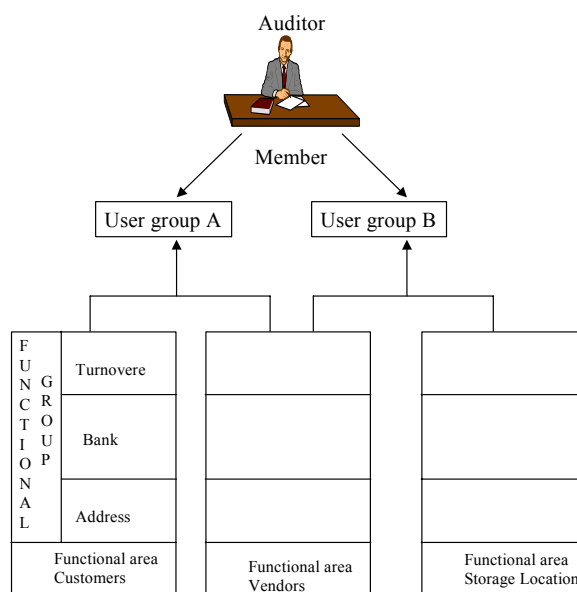


Figure 58: Connection between functional areas, user groups and user within ABAP/4™-query

Since auditors are interested in all business areas, they should have their own user group, which is assigned to all functional areas. That will give the auditors comprehensive access to R/3™ data, if the user group is set up properly by the administrators.

The possibilities of analyzing data generated in ABAP/4™ query reports are somewhat unusual. The data in these reports can be analyzed, using tables and their integrated functions, or be prepared graphically. Additionally, a direct transfer of information to audit software or spreadsheet applications is possible, if an interface has been installed.

### 3.4.2 Creating functional areas

For the user to be able to create reports, it is impossible to expect him to deal with the vast amount of data fields, table and the data dictionary in SAP™. He is working with a pre-structured sphere of data, selected by topic. Typical, flexible reports within financial accounting reflect customers, vendors, materials, general ledger accounts and documents. For these topics, functional areas are created.

Functional areas are created with transaction SQ02, the following window will open up:

Funct. area	Title	Logical data
AM01	FIAA - Inventurangaben	ADA
AM02	FIAA - Grundstücke	ADA
AM03	FIAA - Fuhrpark	ADA

Figure 59: Creating functional areas

For the functional area to be created, a description has to be entered. In the next menu the functional area is given an additional name. The format of the available data has to be defined. Specific tables can be accessed. Additionally, tables can be linked via key fields, such as customer number. The most common case, is data access in pre-structured logical databases.

Figure 60: Assignment of tables and databases to functional areas

The selected table or logical database with related tables is displayed in the next screen. Useful functional groups should be created prior to selecting specific table fields, by calling the menu

Edit

Functional group

Create functional group

FG	Description
M1	Material Description
M2	Supplier Data
M3	Other

Figure 61: Creating functional groups for a functional area

Finally, the specific tables are expanded, and the related data fields with descriptions appear. These can now be assigned to the preferred functional group by a simple mouse click.

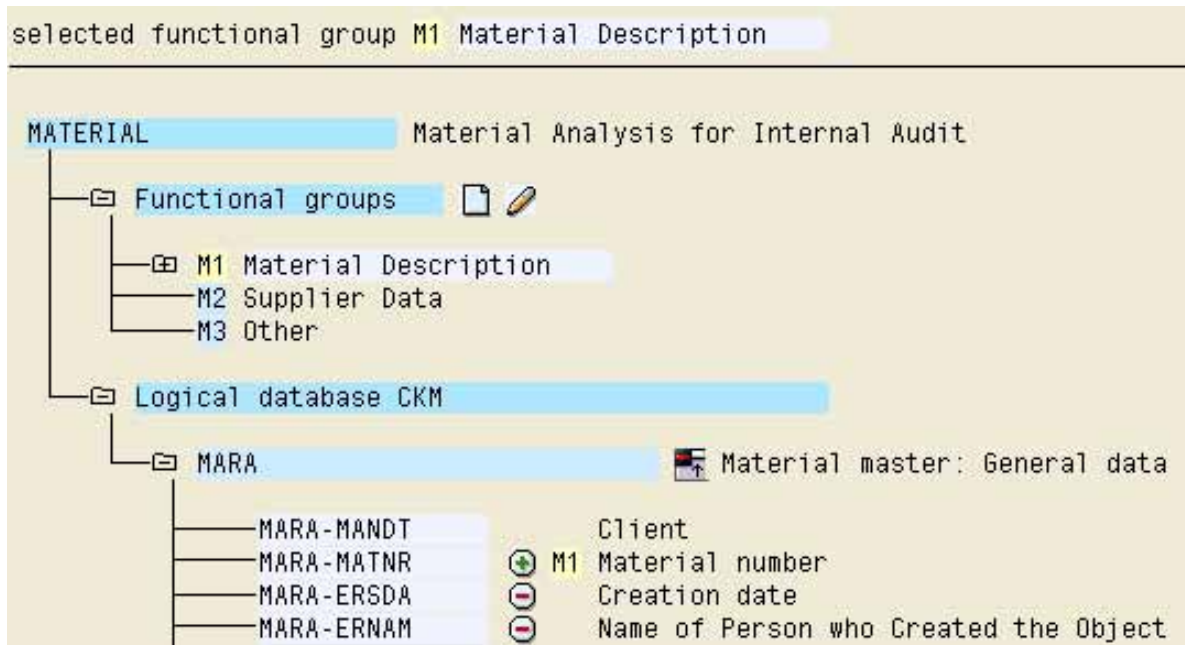


Figure 62: Assigning table fields to the pre-selected functional groups

The data sphere has now been completed and structured, and has to be saved and generated as follows.



Figure 63: Saving and generating a functional area

Now the functional area can be utilized for creating any list with ABAP/4 query.

3.4.3 Creating and changing user groups

Since individual users should only be able to create certain reports related to their work, user groups are created with transaction SQ03

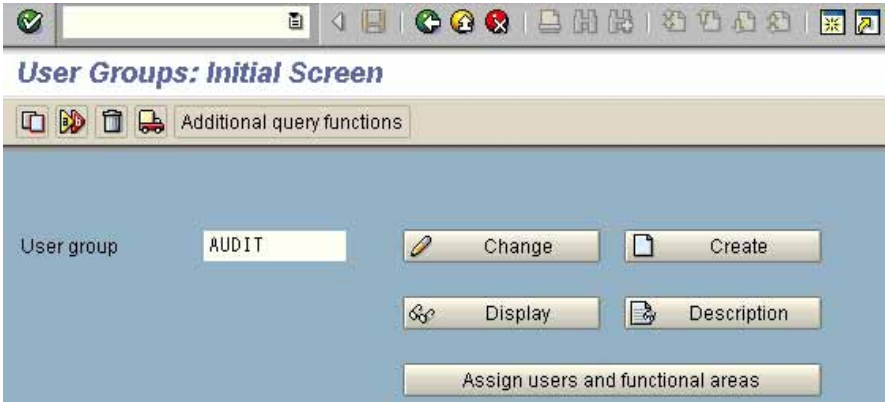


Figure 64: Creating a user group

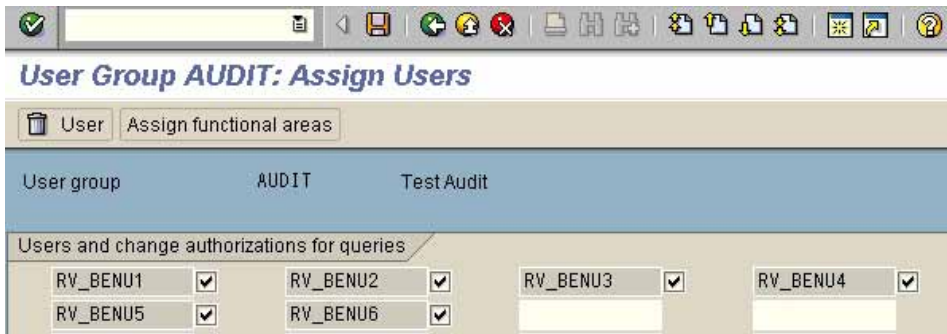


Figure 65: Assigning users to a user group

The auditors should have their own user group. In this user group, the user master records are assigned to the individual auditors. The proposed functional areas for this user group are marked.

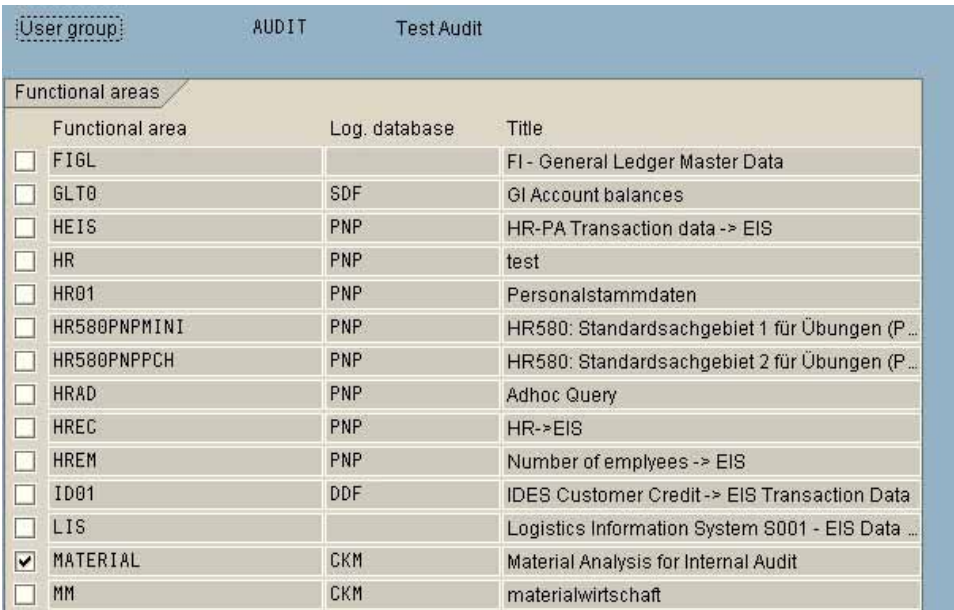


Figure 66: Assigning functional areas to the user group "audit"



Finally, the user group “audit” should be able to use the options of the “expanded folders”

### 3.4.4 SAP™ query list layout

Creating functional areas and user group is a task for the system administration. Creating lists with transaction SQ01 can only be done by users with knowledge of the business. The user logs on to his user group. He gives the new list a name and clicks “create”.



Figure 67: Crating new QUERY-lists

In the next menu he selects the functional area, which includes the necessary data fields for his report.

Name	Logical database	Description of functional area
AUBR	BRF	Audit, Document Analysis
AUDD	DDF	Audit, Customer Analysis
AUKD	KDF	Audit, Vendor Analysis
AUSD	SDF	Audit, General Ledger Analysis
MATERIAL	CKM	Material Analysis for Internal Audit

Figure 68: Selecting a functional area of the user group "audit"

The new list is given a name, and the parameters for the number of lines and columns of the list layout are entered.

The arrow pointing to the right in the upper screen (function key F6), can be used for browsing the selection of functional groups and fields to be listed.

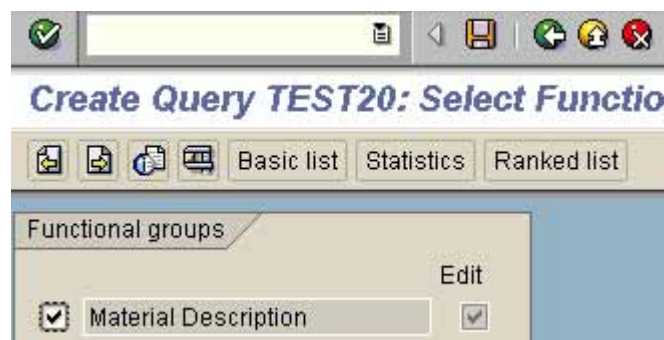


Figure 69: Selecting functional groups



Material Description	
<input type="checkbox"/>	Order unit
<input checked="" type="checkbox"/>	Material group
<input checked="" type="checkbox"/>	Material number
<input type="checkbox"/>	Industry sector
<input type="checkbox"/>	Base unit of measure
<input checked="" type="checkbox"/>	Material type

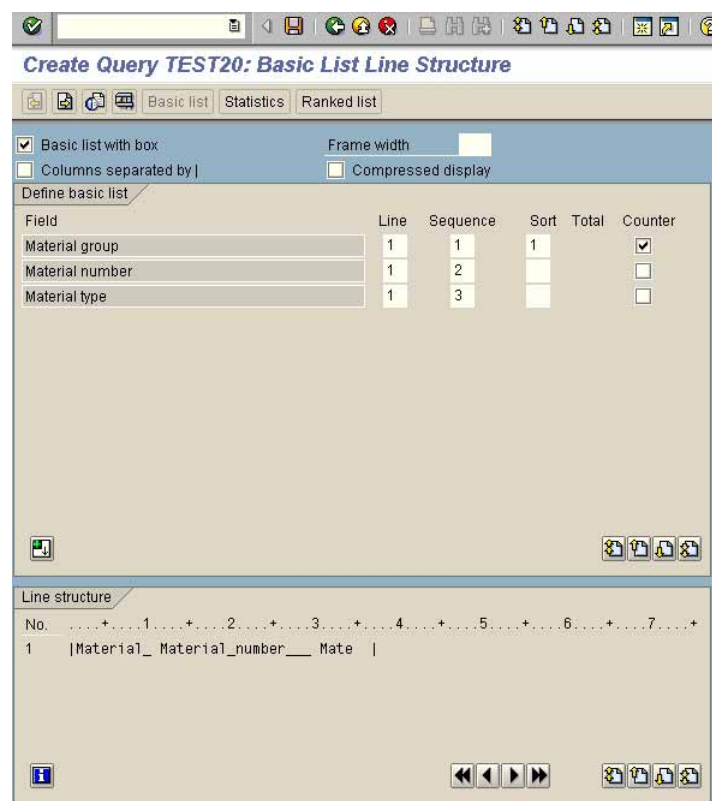
Figure 70: Selection fields to be listed

The list types

- Basic list
- Statistics
- Ranked list

can be chosen. The basic list is usually chosen for audit purposes.

The following screens, which are activated with the arrow pointing to the right, include all options for the list layout. This includes the alignment of fields, sorting, control breaks and group totals as well as additional headers for lines and columns.



**Create Query TEST20: Basic List Line Structure**

☒ Basic list with box      Frame width:

☐ Columns separated by |      ☐ Compressed display

Field	Line	Sequence	Sort	Total	Counter
Material group	1	1	1		<input checked="" type="checkbox"/>
Material number	1	2			<input type="checkbox"/>
Material type	1	3			<input type="checkbox"/>

**Line structure**

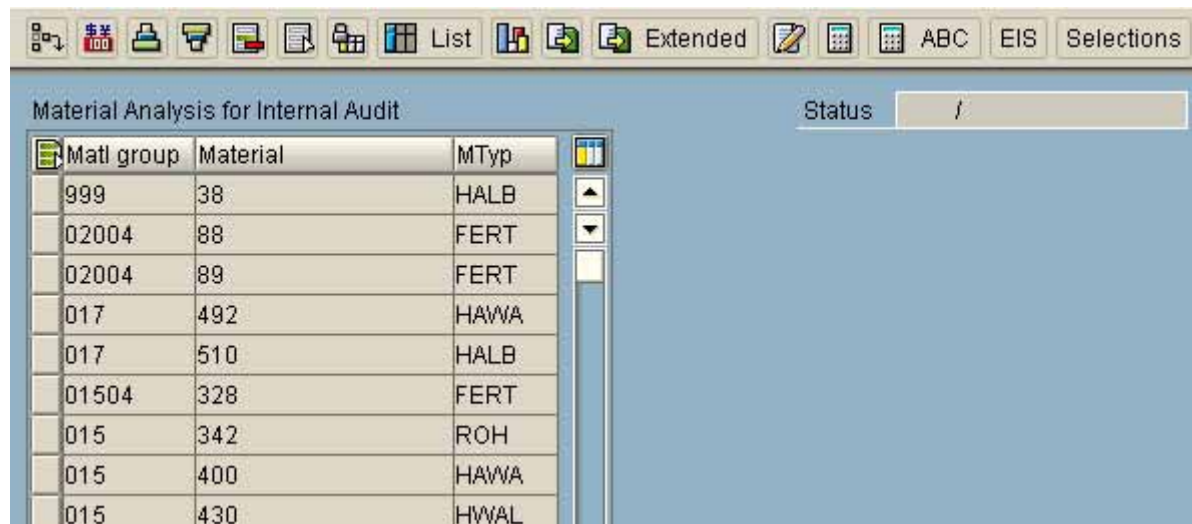
No. ....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+

1 |Material\_ Material\_number\_\_ Mate |

Figure 71: List layout



After finalizing the report, the list can be displayed and printed in any format, e.g. as spreadsheet, text file or graphic.

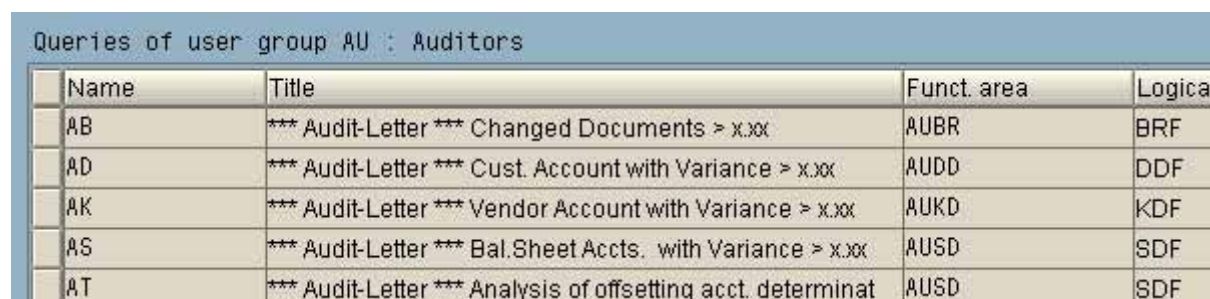


Matl group	Material	MTyp
999	38	HALB
02004	88	FERT
02004	89	FERT
017	492	HAWA
017	510	HALB
01504	328	FERT
015	342	ROH
015	400	HAWA
015	430	HWAL

Figure 72: Display of the report in a table format

### 3.4.5 The AIS™ system and SAP™ Query

The user group “AU\*” is automatically created when installing the AIS™ system. This user group already contains four functional areas, beginning with “AU\*”. These enable flexible reports on document level via the related databases in the areas of customers, vendors and general ledger accounts.



Name	Title	Funct. area	Logical
AB	*** Audit-Letter *** Changed Documents > x.xx	AUBR	BRF
AD	*** Audit-Letter *** Cust. Account with Variance > x.xx	AUDD	DDF
AK	*** Audit-Letter *** Vendor Account with Variance > x.xx	AUKD	KDF
AS	*** Audit-Letter *** Bal.Sheet Accts. with Variance > x.xx	AUSD	SDF
AT	*** Audit-Letter *** Analysis of offsetting acct. determinat	AUSD	SDF

Figure 73: Functional areas of the user group AU

In cases where the audit activities are restricted to these functional areas, the auditors merely have to be assigned to the user group AU (audit) and obtain authority for transaction SQ01. They can then create any required report in the mentioned functional areas.

### 3.4.6 Calling existing queries and their interactive layout

Existing queries can be called by the respective user group by calling transaction SQ01. Every report will show a large amount of interactive features, which can be activated with the button bar in the upper screen.



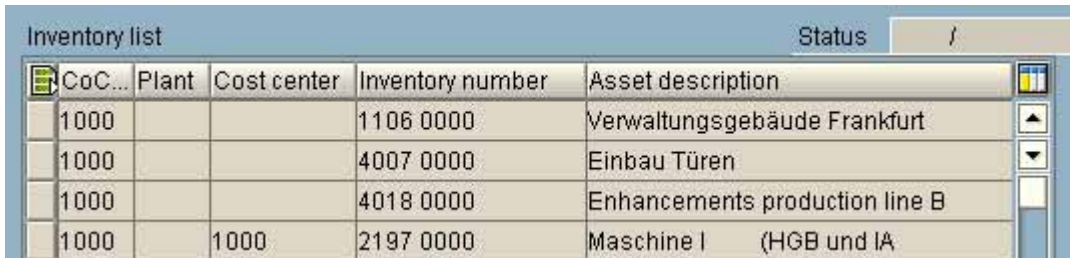
Figure 74: Interactive features in a ABAP-query list

The options will be presented briefly:

#### ☐ **Display as table**

The list contents are displayed in table format. Following options are available:

- Show or hide lines and columns
- Sorting order
- Fix columns
- Edit sub-totals and totals
- Adjust width of columns



The screenshot shows a SAP 'Inventory list' window. It has a title bar with 'Inventory list' and a 'Status' field with a slash. Below the title bar is a table with the following columns: CoC..., Plant, Cost center, Inventory number, and Asset description. The table contains four rows of data:

CoC...	Plant	Cost center	Inventory number	Asset description
1000			1106 0000	Verwaltungsgebäude Frankfurt
1000			4007 0000	Einbau Türen
1000			4018 0000	Enhancements production line B
1000		1000	2197 0000	Maschine I (HGB und IA

Figure 75: SAP™-query list in a table format

#### ☐ **Interactive list** List

The following options are available for interactive lists:

- Set filter with user defined criteria
- Sorting order
- Edit sub-totals and totals
- Adjust width of column / optimized width



The screenshot shows a SAP 'Interactive list' window. It has a title bar with 'Inventory list' and a 'Status' field with a slash. Below the title bar is a toolbar with icons for search, filter, print, save, and other functions. The table below has the following columns: Inventory number, Asset description, Acquisition value, Quantity, Year, and Comm... The table contains eight rows of data:

Inventory number	Asset description	Acquisition value	Quantity	Year	Comm...
1005 0000	Betriebsgelände Stuttgart	3.000.000,00		1993	
1006 0000	Grundstück Parkstraße	500.000,00		1994	
1105 0000	Distributionszentrum Stuttgart	800.000,00		1993	
1106 0000	Verwaltungsgebäude Frankfurt	19.500.000,00		1993	
1107 0000	Vertriebsbüro Region Süd	750.000,00		1994	
1109 0000	Erweiterung Laderampe Süd	126.000,00		1995	
1113 0000	NB-Fabrikgebäude 5	13.000.000,00		1996	
2001 0000	Fraesmaschine Maho 2323	212.173,91		1994	

Figure 76: SAP™-query as interactive list

## □ ABC analysis of any chosen field

The dynamic ABC analysis can be based on any field in the SAP™ query.

Analysis strategy: Key figures (percentage)				
A segment: 50%      B segment: 30%      C segment: 20%				
ABC	Cost center	Inventory number	Asset description	Acquisition value
A		1106 0000	Verwaltungsgebäude Frankfurt	19.500.000,00
A	4220	1113 0000	NB-Fabrikgebäude 5	13.000.000,00
A				32.500.000,00
B	1000	1005 0000	Betriebsgelände Stuttgart	3.000.000,00
B	1000	1105 0000	Distributionszentrum Stuttgart	800.000,00
B	1000	1107 0000	Vertriebsbüro Region Süd	750.000,00
B	4275	2021 0000	Produktionslinie Speicherchip-Herstell	598.005,00
B	4200	2141 0000	Produktionslinie Rahmen, Stoßfänger, R	556.500,00

Figure 77: ABC analysis based on SAP™-query data

## □ Spreadsheet

The final option is to download the SAP™ query list to the personal computer and transform it automatically into a spreadsheet.



Figure 78: Transfer of data to the spreadsheet application EXCEL

If the configuration is correct and there is enough memory, an Excel spreadsheet will be created, which enables any necessary analysis or processing.

Microsoft Excel - Mappe9								
	A	B	C	D	E	F	G	H
1	CoCode	Plant	Cost center	Inventory number	Asset description	Acquisition value	Quantity	Year
2	1000			1106 0000	Verwaltungsgebäude Frankfurt	19.500.000,00	0,000	1993
3	1000			4007 0000	Einbau Türen	6.000,00	0,000	1995
4	1000			4018 0000	Enhancements production line B34200	21.739,13	0,000	1996
5	1000		1000	2197 0000	Maschine I (HGB und IAS)	1.000,00	0,000	2001
6	1000		4100	2205 0000	Fräsmaschine	85.652,17	0,000	2001
7	1000	1000	1200	2015 0000	Geschirrabräumanlage	24.689,33	0,000	1995
8	1000	1000	1200	2016 0000	Geschirrspülanlage	33.685,01	0,000	1995
9	1000	1000	1200	2047 0000	Geschirrspülautomat	20.998,00	0,000	1995
10	1000	1000	1230	2105 0000	Transformator GNT 56	249.565,22	0,000	1994
11	1000	1000	3100	3224 0000	Faxgerät UTAX LF30	1.500,00	0,000	1997

Figure 79: Transferred SAP™-query data in an EXCEL spreadsheet

Summarized we conclude: the major part of the functions within SAP™ query are comparable to those in spreadsheet applications. In cases where the auditor can find the required information in SAP™ query, this option should be preferred to tables or SAP™ standard reports.

### 3.4.7 Downloading data from SAP™ query

There are different ways of downloading SAP™ query data to the personal computer. The possibility to create a spreadsheet automatically has been described.

Additional alternatives are offered as “further processing options” in the lower screen.

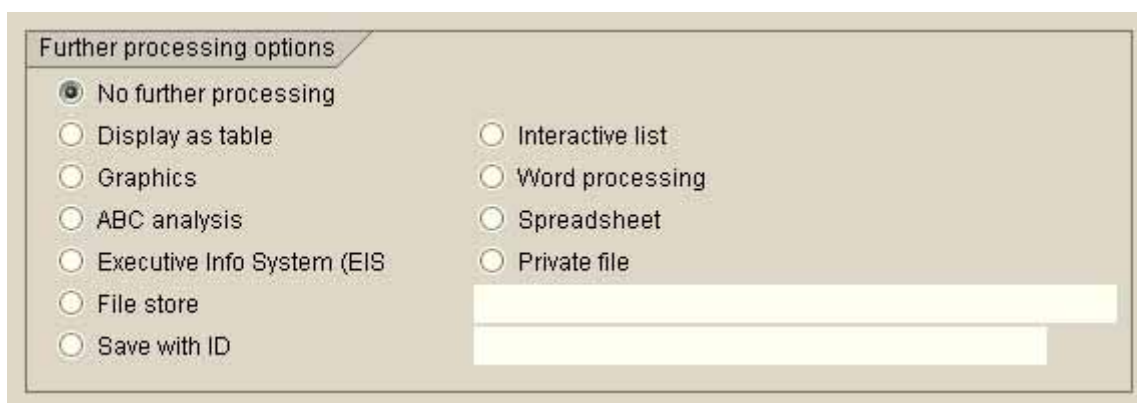


Figure 80: Processing options in the SAP™-query selection screen

The “private file” is of particular interest. Under certain circumstances, this is the interface to common audit software, such as WinIDEA and ACL. The necessary preparations will be discussed further on, in connection with the SAP AIS™ system.

By clicking on “file store”, SAP™ query data can be downloaded to any common computer program in an ASCII delimited file format, with tabulators separating the fields. No preparation is needed for this download.

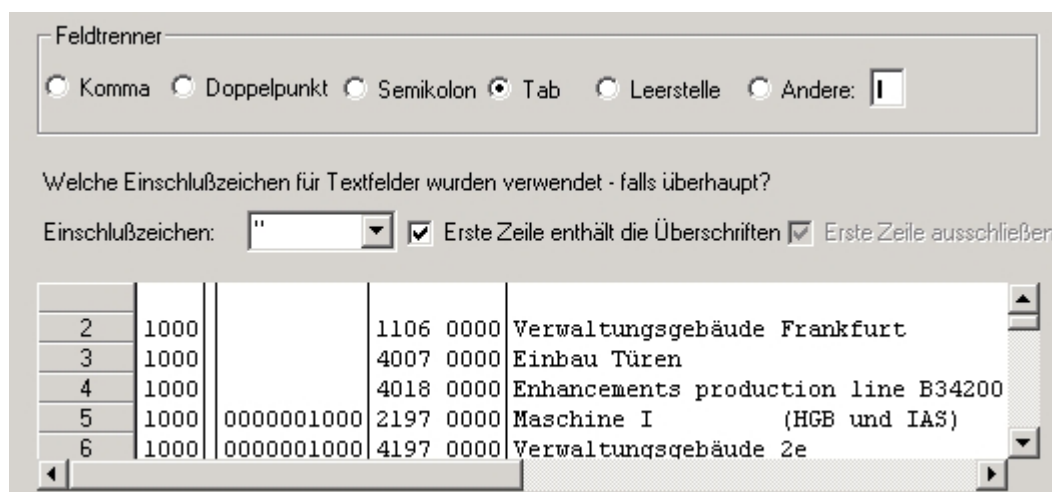


Figure 81: Transfer of an SAP™-query list, using “file store”



In addition to the described interactive ways of downloading data to the software on the personal computer, SAP™ query offers very simple options.

### 3.5 List layout using the list generator Quick-Viewer

The utilization of SAP™ query for list layout is depending on the system organization (functional areas and user groups). The quick viewer was added to the query function in releases from 4.6. It enables every user to generate individual lists with maximum support by the system. The function can be found in the menu

System

Services

Quick viewer

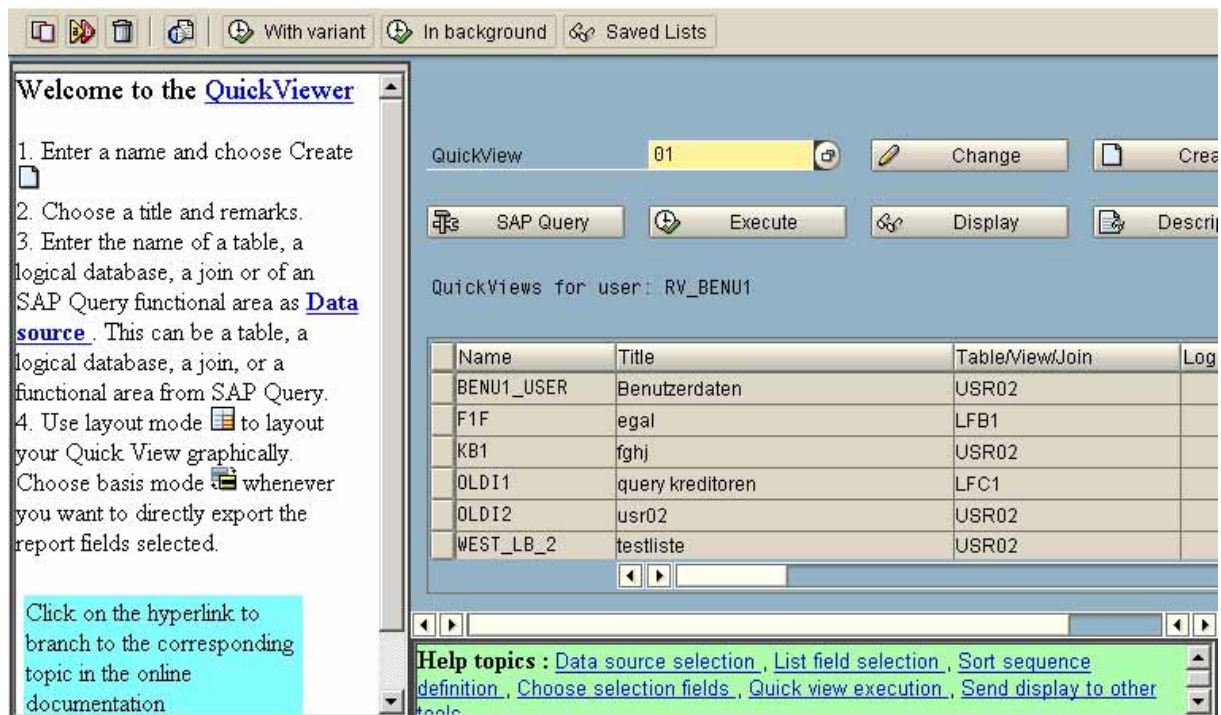


Figure 82: Opening screen to the Quick Viewer

Lists are created in two steps. In the first step a data source is entered, this could be a logical database, a table or joined tables. The necessary fields for the list are selected. In the second step the list is edited and coversheets, headers, sorting orders, sub totals and totals etc. are defined. After completion, Quick Viewer and its list generator creates a query with the same functions and options as described in the previous section.

### 3.6 Tools for utilizing SAP<sup>TM</sup> query

Purpose	Transaction/function	Table	Program
Calling SAP™ query or Quick Viewer	System/services/Quick Viewer		
Table options for interactive list, such as width of columns	“Display as table” button		
Filter/selection from interactive list	Filter button in “interactive list”		
Totals and sub totals	“Display totals” button		
Sorting in tables and interactive lists	“Sorting” button		
Data transfer to Excel from interactive lists	Spreadsheet button and “Excel display”		

Notes:

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

### Exercises on Quick Viewer and SAP™ query

1. Select table USR02 (logon data) as data source and create a list containing the fields (quick view)
  - User name
  - User type
  - Creator
  - Date of creation
  - Last logonSort the list by user group and user name

---

---

---

2. Call the created list and display it as a table. Sort the list descending by last logon.

---

---

---

3. Display the list in an interactive list format and exclude all users, who never logged on to the system by filtering.

---

---

---

4. Download the SAP™ query to a spreadsheet

---

---

---

5. Load the SAP™ query generated data to your audit software.

---

---

---



## **V Auditing in an SAP R/3™-environment**

### **1 Introduction**

In the previous sections it has been made clear, that SAP R/3 is a complex integrated flexible program, which can be customized to suit many specific company and business situations. This reduces the transparency of the system and makes it difficult to audit. *Not even the most experienced auditor will be able to audit the system and make a competent statement on every inherent risk aspect within an acceptable time frame.* A satisfactory statement on the system can only be made if the auditor focuses on certain aspects as defined in an audit plan, which will cover several years. Not only the SAP™ basis system and the linked applications have to be audited, but also the connected sub systems (operation system, databases, hardware, IT organization)<sup>1</sup>. The audit approach for an SAP R/3™ system is ranging from the implementation support and the audit of basic operations, to the review of complete processes. The audits have to be risk oriented and be performed within a defined time frame. The audit approach will be presented in detail.

### **2 Organizational preparations for audits in the SAP R/3™ environment**

#### **2.1 The auditor's work place**

The auditor should have his own access to the SAP™ system. In addition to the SAP™ access, this should include common standard office software. Further, the auditor needs reserved hard disc space for downloads of SAP™ data on his personal computer. Prior to the audit, data conversion software; such as Monarch or DatalImport, should also be installed, just as common audit software, such as WinIDEA or ACL. A printer should be set up properly to enable the auditor to print his work papers.

These preparations should be checked before the audit begins.

#### **2.2 Required extent of authorizations**

The auditor's authorizations should be as extensive as possible, but strictly limited to display only. The SAP™ system provides standard profiles in all audit relevant applications for this purpose, recognizable by the suffix "ANZ" or "SHOW". Some examples are:

- S\_A\_SHOW all display authorizations for the basis module
- F\_ANZ all display authorizations for accounting
- M\_ANZ all display authorizations for the MM module

---

<sup>1</sup> Details on this topic are stated in the manual on audits of operating systems and networks by the same author

Prof.name	Text	Type
M_ANZ	MM Materials management - Display everything	Comp.profile
M_BANF_ANZ	MM Purchasing: Requisitions: Display Authorization	Sgle profile
M_BEFU_ANZ	MM Inventory Management: Display authorization	Sgle profile
M_BEST_ANZ	MM Purchasing: Purchase Orders: Display Authorization	Sgle profile
M_BILA_ANZ	MM Balance Sheet Valuation: Display Authorization	Sgle profile
M_DGM_SHOW	MM Dang. Goods Management: Display DG-Mat Master & DG Texts	Sgle profile
M_EBEL_ANZ	MM Purchasing - Display order documents	Sgle profile
M_EINF_ANZ	MM Purchasing: Info Records: Display Authorization	Sgle profile
M_EINK_ANZ	MM Purchasing - complete: Display authorizations	Sgle profile
M_ESTA_ANZ	MM Purchasing: Display Vendor and Material Master	Sgle profile
M_LPET_ANZ	MM Purchasing: Sched. Agmt. Delivery Schedules: Displ. Auth.	Sgle profile
M_MATE_ANZ	MM Material master: Display authorizations	Sgle profile
M_ORDR_ANZ	MM Purchasing: Source List: Display Authorizations	Sgle profile
M_QUOT_ANZ	MM Purchasing: Quota Arrangement: Display Authorizations	Sgle profile
M_RAHM_ANZ	MM Purchasing: Outline Agreements: Display Authorization	Sgle profile
M_REPR_ANZ	MM Invoice Verification: Display authorizations	Sgle profile
S_A.SHOW	Basis: Display Authorizations Only	Sgle profile
S_ABAP_ANZ	BC: ABAP/4 - Processing authorizations	Sgle profile
S_KLAS_SH...	Profile for Displaying all Classes/Characteristics	Sgle profile
S_SYST_ANZ	BC for user department - Display (ABAP/4, tables)	Comp.profile
S_TABU_ANZ	Table display authorization	Sgle profile

Figure 83: Overview of standard profiles for display only in SAP R/3™

*In-house developed audit profiles can usually not be recommended for auditors*, since it is difficult to clearly define which authorizations will be needed for the specific audit, before the auditor begins his work. A mixture of in-house developed audit profiles and standard display profile is usually problematic as well, resulting in more authorizations than required.

In systems where the auditor's work place AIS (*Audit Information System*), is installed, SAP™ provides *standard audit activity groups*, named SAP\_CA\_AUDITOR\_XXX (XXX = relevant audit function).

Act. group	Name
SAP_CA_AUDITOR	CA: Auditor
SAP_CA_AUDITOR_APPL_ADMIN_AG	CA: Audit Administration
SAP_CA_AUDITOR_APPL_AG	CA: Auditor SAP Applications (except HR)
SAP_CA_AUDITOR_DS_AG	CA: Data Protection Auditor
SAP_CA_AUDITOR_HR_AG	CA: HR Auditor
SAP_CA_AUDITOR_SYSTEM_AG	CA: Auditor System

Figure 84: Standard audit activity groups, utilizing the AIS system

The corresponding activity groups are equipped with the same authorizations as the standard display profiles. Further information for auditors and administrators on how to proceed can be found in the *menu "preparatory work"* in the AIS™ system.

Since the auditor may need to create reports with SAP<sup>TM</sup> Query or Quick Viewer, it is useful to assign the necessary authorizations for transaction "SQ\*" (standard profile S\_QUERY\_ALL) in order to enable the auditor to edit functional areas, user groups and lists. If the authorizations for functional areas and user groups should remain only with the administrators, a functional area for the auditors should be created, or they should be assigned to the user group "AU", in order to enable the auditors to create reports for audit purposes within relevant functional areas.

### 3 **Supporting audits for the migration in an SAP R/3<sup>TM</sup> system**

Strategies for migration and related audits in an SAP R/3<sup>TM</sup> system environment are depending on the company specific circumstances and the prevailing IT structure. For the project support audit, it makes a difference if data is migrated from an SAP R/2 system or from a completely different system. Additionally, it is important to know which modules are to be implemented, due to the complex module integration within SAP R/3<sup>TM</sup>.

Some problematic migration related issues and corresponding audit approaches are presented below.

#### □ **Reflecting the company organization structure and the process organization in the SAP<sup>TM</sup> system**

- *process organization*

SAP<sup>TM</sup> is providing a reference model, which has to be customized to fit the specific company requirements. To ensure the proper *processing of business activities like purchasing, orders, invoice postings and payments etc.*, the business processes have to be properly reflected in the SAP<sup>TM</sup> system. This is possible by *customizing the SAP<sup>TM</sup> system* accordingly, or the company uses the opportunity of the system implementation for *reengineering the business processes*.

In both cases, *inconsistencies* between the actual business processes in the company and the corresponding processing within the SAP<sup>TM</sup> system *have to be avoided*. They would result in security gaps and a poor internal control system.

A *data model* is developed, based on the business processes as reflected in SAP<sup>TM</sup>. The model should ensure, that every document carries all necessary data and that required data for company controlling purposes is aggregated.

**Audit:**     ⇒     Are business processes documented properly and with sufficient quality, and are the processes reflected correctly in the system?

- *company organization structure*

*Several employees on different positions* take part in the business processes in the company. The *company organization structure* without names of the staff should be reflected in the SAP<sup>TM</sup> system, in particular if the company will utilize *work flow functions* in order to ensure *segregation of duties* and the *4-eye-principle* etc. The HR module (human resources) offer several functions in this area.

An advantage is, that *specified authorizations can be assigned to the positions (roles) at a later stage*. As soon as an employee is taking a certain position, he will obtain the *specified system authorizations required for the job*. The same applies for newly hired or internally transferred staff. This procedure increases the *company transparency and control*, and it decreases the administrative effort of maintaining authorizations in the system. The procedure requires a *clear documentation of the company organization structure*, and that the *tasks and responsibilities for each position are known*.

- Audit:**     ⇒     Has the company organization structure been properly documented and are the responsibilities known?
- ⇒     Have the roles been reflected properly within the SAP<sup>TM</sup> system?

- **Business structure definition**

It is necessary to reflect the business structure of the company in the R/3<sup>TM</sup> system. Which *clients, company codes and business areas* are used? Are business areas and data for controlling the company *related to a company code*, or is data *generated across company codes*? Are there *other organizational units*, such as purchasing or sales (including controlling possibilities)? How many plants and storage locations (for materials) are there? Which projects are created?

- Audit:**     ⇒     Is the business structure appropriate and does the generated information meet the requirements of management?

## □ **Data transfer**

As explained, the SAP R/3<sup>TM</sup> system consists of more complex organizational structures than SAP R/2<sup>TM</sup>. As a result, the *master records may have to be deleted and then assigned again*, depending on the business structure. The data field semantics have changed in many areas. This is a critical issue. SAP supports the migration of master records with tools, but the *auditor still has to check the data* to make sure that both the old and the new system are reflecting *“the identical company”* after the migration has been completed. The master records have a major impact on the business process controls and on valuation procedures. Therefore, the *system administration* must be able to prove the immaculate migration of master records, using *correct and comprehensible reconciliation procedures*.

- Audit:**     ⇒     Is there a concept for migrating master records?
- ⇒     Which ways are used for the migration of master records and the transfer to the SAP R/3<sup>TM</sup> database?
- ⇒     Is the migration of master records sufficiently documented?
- ⇒     Are master records from the old and the new system reconciled, and was the migration immaculate?

## ❑ Authorization system and user administration

Only a *thoroughly planned authorization concept* and a proper user administration can *ensure the sufficiency of the internal control system after implementing an SAP R/3™ system*.

There are *numerous elements* within the *protective systems* in the SAP R/3™ system, which have to be planned before they can be reflected in an authorization system. For example assigning the following:

- tables - to *table groups* and access authorizations
- transactions - to *roles* (company organization structure)
- executable ABAP/4™
- programs - to *program groups* and access authorizations
- user IDs - to *user groups* and user administration
- accounts - to *account groups* and authorizations for access and posting
- *amounts* - to user groups (invoices, documents, payments)
- *tolerance limits* - to user groups (invoice deviations, rounding)
- SAP™ objects - to *protection category* and access authorization

A differentiated protection can be created for each element. This requires thorough planning of the listed protective mechanisms beforehand, and that these are customized accordingly. This has to be *discussed with the user departments* in the company. *If this is neglected, the mechanisms can not be utilized in the authorization system*, resulting in a weakened system security.

The *assignment of specific authorizations* to individual authorizations, profiles, composite profiles or activity groups and their naming also has to be defined. The *naming convention* has to be fixed and defined to the last digit in order to enable audits as well as maintenance of profiles and activity groups by authorized staff only.

A *centralized or decentralized user administration* has to be considered. Both can be good or bad, more will not be said on this topic at this point.

- Audit:*
- ⇒ Is there a comprehensive and clear concept for creating and administer authorizations?
  - ⇒ Is there a clear naming convention for activity groups and profiles?
  - ⇒ Is there a clear description of the roles and the assigned authorizations?
  - ⇒ Is there a concept for the user administration?



#### ❑ Implementation work groups

SAP™ provides a *standard procedure* for implementing and *customizing the system*, which can be divided into *projects with work groups*. The auditor should make sure, that these work groups consist of *sufficiently qualified employees*, who are able to grasp *issues across modules* as well. Due to the fact, that authorizations often are defined on a decentralized basis in the different work groups, authorization systems are rarely *homogenous and conclusive*. A *strong project controlling* has to make sure, that the work groups are working according to a mutually defined guideline.

*Audit:*      ⇒      Sufficiently qualified employees in the work groups!

#### ❑ Test procedures

*Integration tests* have to be run after completion of the customizing and the *data transfer*. The staff in the user departments have to perform the tests according to a *specified test procedure*. The tests must meet sufficient quality standards and have to be documented. Only when the company is absolutely certain, that the SAP R/3™ system is working as expected, the system can go live.

*Audit:*      ⇒      Is the test procedure detailed enough and is it understandable to the users?  
                 ⇒      Is the test documentation comprehensible and detailed?

#### ❑ Project plan

Practical experience gathered during many audits show, that *SAP™ projects with complexity and timing according to plan are rare*. Either the project takes much longer than expected, or the requirements for system functionality and security were drawn back far enough to meet a fixed deadline. Cost overruns are not unusual. In an audit of cost effective aspects, the *project administration* should get suitable attention, beginning with *detailed project and cost plans* which state dated milestones and expected costs.

#### ❑ User training

We have noticed, that *user training does not get enough attention* during implementation projects, resulting in improper handling and lack of knowledge, causing problems in the business processes and system errors when the system goes live.

*Audit:*      ⇒      Is there a detailed *training schedule* with fixed dates and contents for every relevant module and process?  
                 ⇒      Has the *training organization*, stating internal and external trainers, responsibilities for each module and master user for each department been documented in writing?  
                 ⇒      Are user specific *manuals and user documentation* available?

#### ❑ **Final basic check**

After the system goes live, *start-up support and maintenance by external consultants* is required for some time. The know-how transfer should take place as soon as possible in order to transfer necessary knowledge to the system administrators. Additionally, the system load in the production system should be analyzed and the system tuning should be finalized.

The auditors have to convince themselves during a quick basic system audit, that the system is in compliance with generally accepted accounting standards, also regarding security standards and comprehensible processing.

- Audit:
- ⇒ Has there been a know-how transfer from the external consultants to the *system administrators*?
  - ⇒ Has a *system load analysis and a fine tuning* of the system been carried out, and do the response times meet the user requirements?
  - ⇒ Analyze the settings and organizational processing of security, protection and compliance aspects!

#### ❑ **Special audit: contractual agreements**

One aspect deserves the auditor's attention, even if it is not really a part of the project support audit. Several implementation projects are not satisfactory, especially towards the end of the project. The auditor should be prepared for problems between external consultants and the internal project team, which can be expected to occur. Proper contractual agreements are useful for such cases, and the auditor should make sure to review the contracts.

- Audit:
- ⇒ Has the project management (preferably external) been clearly defined?
  - ⇒ Are all formal criteria for contracts met?
  - ⇒ Are all terms of the contract clearly described, defined and restricted?
    - Basic services
    - Guarantee services
  - ⇒ Are the responsibilities clearly defined for
    - Exceeded project time limits
    - Poor system customizing
    - Performance problems after implementation?

Further audit activities in a production SAP R/3™ system will be presented in the following sections of this manual.



## **4 General IT operations**

### **4.1 Structure of the IT department**

For the implementation of the SAP R/3™ system, there is usually a small work group in addition to the regular IT department, which supports the system until it goes live and in some cases longer. The common segregation of duties in a mainframe computer environment does not apply to SAP R/3™ and is often non-existing. An careful overview of the staff dealing with the system should be obtained. The auditor should pay particular attention to the segregation of duties in areas relevant to system security, in order to avoid security gaps in the system itself and during system operation, resulting from bundled duties.

The following functions should be reflected by *independent organizational units* in a complex R/3™ implementation:

#### ☐ **RZ-system administration**

Responsibilities in the areas of standard installations, system operations and system libraries.

#### ☐ **Operating**

Monitoring of the running RZ-operations, starting jobs, often responsibility for the data storage area. Many companies have *automated system operations with staff on call* during time of low system load, e.g. during batch runs at night or weekend. This procedure should be audited, in particular how remote panel access is provided and how the system is secured.

#### ☐ **Preparing and wrapping up jobs**

Responsible for the job control in the SAP™ system. Here is the sequence for running programs on a daily, weekly or monthly basis decided. The outcome of specific runs is checked and corrected if necessary. Specific SAP™ logs are checked and parameters for automatic runs and information in advance are maintained. In R/3™ operations, these duties are usually assigned to the user departments.

#### ☐ **System programming**

System programmers are usually customizing the standard system, by e.g. changing the source code or certain system relevant settings. System programmers should as a rule have *no access to the production system*.

#### ☐ **Application programming**

The application programmers are creating new, or change existing applications. This is done in the development environment (programming language ABAP/4) provided by SAP™ or by using database tools. The *organizational set up for such developments* is a wide audit area. Also the application programming should *be strictly segregated from the production environment*.

❑ **Database administration**

The relational databases of the SAP R/3™ system are usually administered by an independent service provider, responsible for the reliability, efficiency and database protection.

❑ **Network administration**

Networks are gaining importance in a complexly distributed IT environment. The network administrator is managing the network. He has far reaching rights and protects the communication environment from unauthorized access.

❑ **IT support**

The computer intelligence of the SAP™ system is not concentrated to the servers alone. Data is forwarded to the users, who process the data further with database or spreadsheet applications on their personal computers. The support for these audit relevant applications are usually allocated to independent units (help desks).

#### **4.2 Rules for organizational processes and documentation of IT operations**

In order to secure the IT systems satisfactorily, legal requirements should be used as a basis for internal *policies and procedure* regarding business activities, and these should be given to the employees.

The auditor needs to know *which policies and procedure* are available. These have to be assessed and *considered during audits*. Examples are

- Work place descriptions for IT staff
- Work process descriptions
- Development guidelines for system and application programmers
- Naming convention / SAP™ norm manual
- Documentation guideline
- Test guideline
- Data ownership rules
- User creation and administration rules
- Data storage and archiving guidelines
- Computer center rules
- Advice for catastrophic situations
- Rules for log evaluation

This list is not exhaustive. Depending on the computer operations, a whole string of further documentation and regulations may be required.

#### 4.3 Overview of the IT related technical environment

The auditor should check the *security awareness* of the R/3<sup>TM</sup> operations in the company. A *negative influence*, caused by the introduction of a client server system with *mid size computers* can be noted in many cases. Expensive mainframe computers were, as one would expect, kept in hermetically sealed areas, but today's small manageable servers components get – unjustifiable – little attention.

An *audit of the R/3<sup>TM</sup> system* has to include how the *computer centers* manage cases like:

- Attacks and catastrophes
- Physical access security
- Power loss and other obstruction of operations
- Fire
- Storage of the computer and peripheral equipment
- System access security
- Storage of data media

*Network operations* bring another set of risks, which also need to be analyzed:

- Protection of the lines , including tapping
- Analysis of logged in personal computers
  - Not secured drives
  - Risky third party programs
  - Theft protection
- Access authorization for files and programs
- External interfaces and their security
- Virus problems
- Monitoring of the user work place
  - Automatic stand by modus with blank screen
  - Password access
  - Log of login failures

Finally, the *audit of the operating system and the databases* linked to SAP<sup>TM</sup> components should be mentioned. Usually, a *UNIX-derived system* or WindowsNT is utilized and its security settings have to be audited:

- Protection from unauthorized access to files and programs

Are critical UNIX-sub programs such as

NIS (Network Information System)

NFS (Network File System)

rLogin (remote Login)

protected from unauthorized access?

- Is there an early protection system analogous to RAC/F?
- Are system data and program libraries protected from unauthorized access and program manipulation?
- How is data exchange and communication with external bodies, if any, protected?
- Is the direct access to databases by SQL or ODBC techniques, where the data may be at risk, controlled and protected?

There are plenty of other interesting aspects in this area, but they will not be discussed at this point.

#### 4.4 Utilities for estimating the technical operating environment<sup>2</sup>

The auditor will hardly be able to estimate the IT environment regarding e.g. compliance with the security standards stated in the Orange-Book, without *technical utilities* supporting his analyses.

The issues of the previous sections will be discussed in detail (with integrated *audit checklists*) in the following sections:

- Generally accepted accounting principles when utilizing IT technology
- Manuals for IT system audits
- IT user manuals
- Generally accepted standards for IT data processing

Relational database systems can be analyzed, using programs such as SQL-Secure.

Username	Status	Pwd Minlen	Pwd Lifetime	Account Expires	Password Age	Last Login	Last LogFail	LogFails	Administrator 1
CHAPMAN	Unused Account	6	150	05-05-1995	4				SYS
DAVE	Active	8	90		0	04-11-1995 10:46			SYS
DAVETEST	Unused Account				5				
DTEST2	Pwd Expired				65	02-03-1995 17:01			
ED	On Hold				1	04-07-1995 11:39			DAVE
EEEE	Disabled				7				
JSMITH	Unused Account			12-31-1995	5				DAVE
JULIE	Unused Account				5				
OPS\$DAVE	Unused Account				1				
ORACLE7	Breakin!				6	04-06-1995 13:17	04-06-1995 13:20	4	
SQLCQR_DBA	Unused Account				7				
SYS	Active				11	04-12-1995 14:34			

Figure 85. Password analysis for a database system, using SQL Password Manager

<sup>2</sup> See Roger Odenthal, „IT audit: supporting procedures and tools“, KES, Magazine for communication and IT security, number 6, December 1997

There are specially developed tools for network audits, such as

- Novell / Network Auditcon
- BaynView/NCS
- SofTrack
- LAN Auditor
- NetDirector
- NORTON-Administrator for networks
- Kane Security Analyst

The listed product have been designed for *NOVELL and NT environments*. For *UNIX and AS400 operating system audits* there are supporting programs such as:

- SecurMax
- COPS (Computer ORACLE and Password System)
- RAXCO Security Toolkit
- DEC/UNIX-Audit
- AUDIT Master (IBM AS/400)
- DB or network analyses according to checklist AIS

Additionally, different UNIX derived products contain several utilities, which can be used for audit activities



Figure 86; Analyzing a network environment, using the program "Kane Security Analyst"

#### 4.5 Mapping the IT environment

The development of audit approaches and focuses requires *extensive knowledge about the complete IT environment* in the company. Only few companies utilize all SAP<sup>TM</sup> applications. Usually, the company will run programs from other suppliers or in-house developed applications in addition to R/3<sup>TM</sup>, which *exchange data via interfaces*. The auditor needs detailed graphics of the IT environment, showing

- ❑ The technical structure and
  - Stand alone computers
  - Peripheral equipment
  - Lines and multiplexes
  - External interfaces
  - Locations
  - Structure and performance details
- ❑ The organizational structure
  - Programs and their functions
  - Input and output interfaces
  - Communication between programs
  - Allocation of software solutions to computers

#### 4.6 Summary on general IT operations

The security gaps and risks in R/3<sup>TM</sup> system operations usually result from lack of administrative staff, insufficient policies and procedure in the IT area, lack of documentation and lack of security awareness.

The auditor should therefore convince himself of secure and compliant system operations, taking the described circumstances into consideration, before he starts his specific audit activities within the SAP<sup>TM</sup> system.

#### 4.7 Audit tools for general IT operations

Purpose	Transaction	Table	Program
Support for mapping the system	AIS/system audit and checklists according to R/3 <sup>TM</sup> security manual with questions		

## **5 Auditing SAP<sup>TM</sup> basis applications**

### **5.1 Introduction**

The SAP<sup>TM</sup> basis application audit is a task for the IT audit department. With their support, typical weaknesses of SAP<sup>TM</sup> implementations should be found and eliminated. The IT auditors deal with basic security and compliance settings within the SAP R/3<sup>TM</sup> system, including related organizational processes. The audit can be performed *using SAP<sup>TM</sup> standard transactions* or the *“system audit” in the AIS system*. This manual will use both methods for showing useful functions and transactions for audit purposes.

### **5.2 Overview of installed systems, system environment and active SAP<sup>TM</sup> components**

#### **5.2.1 Mapping the installed R/3<sup>TM</sup> systems**

The R/3 typical client server architecture is more fragile and exposed to errors than a monolithic mainframe computer environment, due to multiple communicating elements and their operating systems. Independent SAP<sup>TM</sup> systems for different purposes are run parallel, the systems are interconnected to one group, and make up the complete SAP<sup>TM</sup> environment.

Such an SAP<sup>TM</sup> group usually consists of the

- *Development system*  
Development of new programs, utilizing the programming language ABAP/4<sup>TM</sup> and development test runs
- *Test / consolidation system*  
Installation of SAP<sup>TM</sup> standards including company specific developments and R/3<sup>TM</sup> customizing. Test environment for users and mass tests. Data in the test system has to be similar to data in the production system.
- *Production system*  
Live system, production financial accounting, where all data resulting from the business processes is created, processed and saved.

The systems exchange programs, tables and data on precisely defined routes (change and transport system).

An SAP<sup>TM</sup> production system can not be operated on its own. The required system developments would enable changes of data without audit trail. This would not be in compliance with commercial or tax legislation (erasing is prohibited). Additionally, the required test runs would affect the stability of the complete system to such an extent, that nobody would be able to ensure the integrity of the production data.



A compliant system environment requires at least two corresponding SAP™ systems. The described three system environment is an advisable standard, which should be applied.

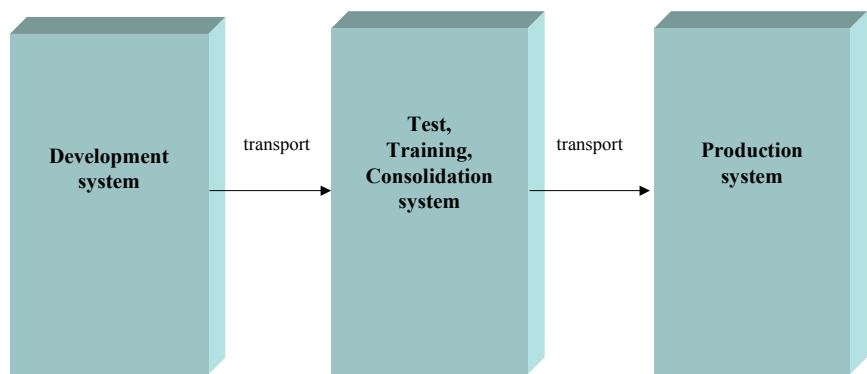


Figure 87: Group of interconnected SAP™ systems


The auditor obtains an overview of installed systems in the AIS menu

System audit

Transport group

Transport management system (TMS)

Transport management system (entry point)

(transaction STMS), which routes the user to the TMS. The auditor can obtain a list of the systems in the group with the button “system overview”  or in the TMS entry screen by calling menu

Overview

Systems



No. of systems: 2		04.12.2002 16:20:58	
System	Description	Release	Status
CMD I46	Virtuelles PRD-System IDES 4.6B Demo System	46B 46B	

Figure 88: Overview of installed SAP™ system

A graphic overview of the configured transport routes can be obtained with the button “transport routes”  in the TMS entry screen or by calling the menu

Overview

Transport routes

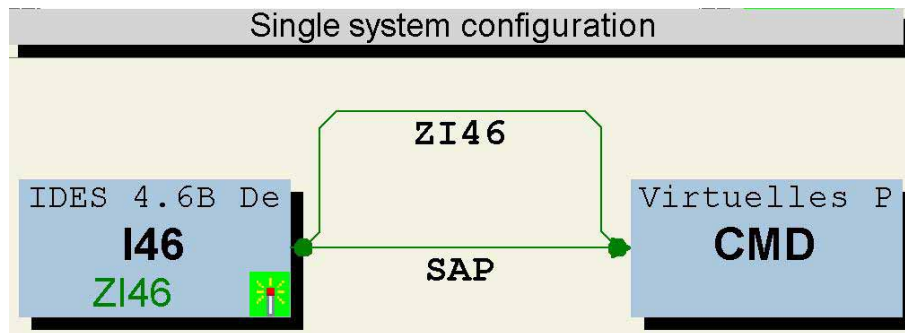


Figure 89: Graphic overview of transport routes in an SAP™ group

The displayed overviews should be printed to complete the work papers. Already at this point, the auditor can see if an *appropriate SAP™ group* has been installed, taking the complexity of the system and its applications into consideration. The *overview is also useful for the audit of authorizations*, which have to be specifically defined and created for each system. Additionally, the work papers from this area will be used later, for the *audit of the change and transport system*.

### 5.2.2 Mapping the operating system and the database environment

The auditor should not only know which SAP™ systems are available, but also which *hard and software the system is based on*, which *database* is being utilized and which *SAP™ release version* is installed.

This information can be obtained in different ways, depending on assigned authorizations. The “Computer Center Management System” (CCMS) in *transaction RZ20* gives a quick overview. With the following steps in the displayed menu

CCMS monitor sets

CCMS monitor templates

System configuration

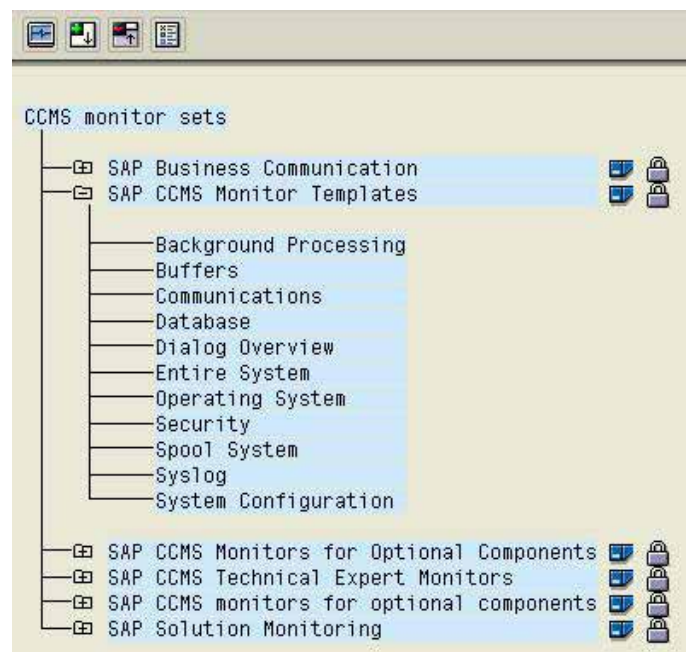


Figure 90: Display of system configurations in CCMS

A complete overview of all configuration details regarding hardware, operating system, database and SAP™ components

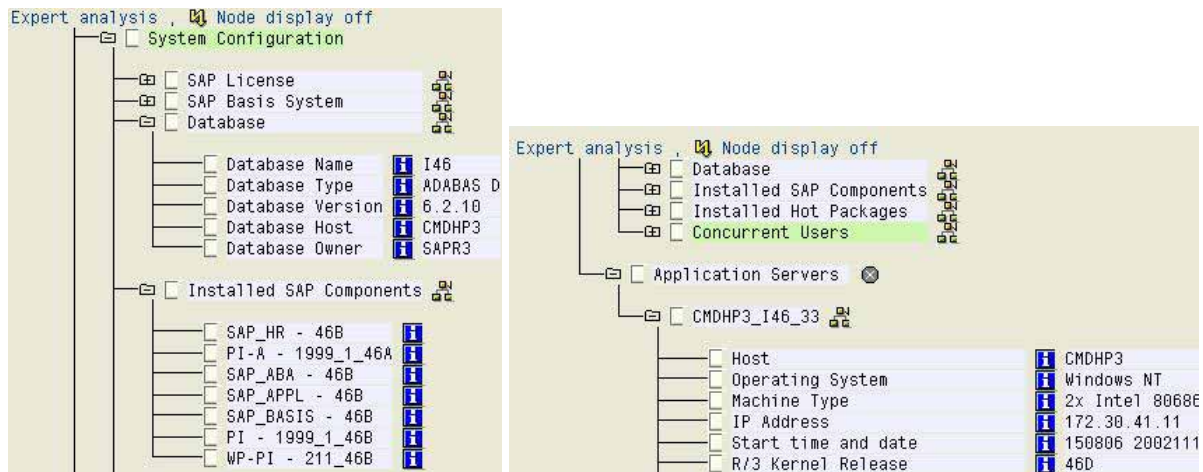


Figure 91; Display of system configurations in CCMS

is displayed on the screen and can be printed. At the same time, this information can be downloaded to the personal computer for reporting purposes, calling the menu

Monitor

Save to PC file

If the user does not have CCMS display authorization, the described information can be obtained in the following two steps:

#### ❑ SAP™ server overview

From the AIS opening screen, calling

System audit

System configuration

System

SAP server overview

(transaction SM51), the servers connected to an SAP™ implementation and their functions (type) are displayed.

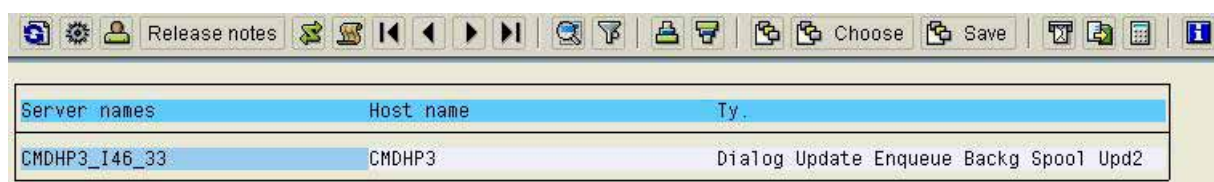


Figure 92: Display of the SAP™ server

The button “release notes” in this screen routes the user to a log, where all required information can be found.

SAP Release information	
Application server CMDHP3_I46_33	
SAP R/3 Kernel information	
SAP R/3 Kernel	46D
Database library	LiveCache_714_b16
created in	NT 4.0 1381 Service Pack 5 x86 MS VC++ 12.00
created on	Feb 5 2001 20:28:29
Patch level	432
Supported environment	
SAP database version	46A

Figure 93: Log of SAP™ release information

In addition to the log, further details are given in the menu

System

Status

The screenshot shows two overlapping SAP windows. The background window is 'System: Status' and the foreground window is 'System: Kernel Information'.

**System: Status**

- Usage data:** Client 800, User RV\_BENU4, Language EN, Previous log, Logon, System time.
- SAP data:**
  - Repository data:** Transaction SM51, Transaction variant, Program, Program (GUI) RSM51000\_ALV, GUI status SAPREL.
  - Host data:** Operating system Windows NT, Machine type 2x Intel 8, Server name CMDHP3\_I46\_33, Platform ID 560, Codepage 1100.

**System: Kernel Information**

- Kernel information:**
  - Kernel release 46D
  - Compilation NT 4.0 1381 Serv
  - Patch level 432
  - ABAP Load 1258
  - CUA load 12
  - Mode opt
  - Rsyn file
- Database data:**
  - System ADABAS D
  - Release 6.2.10
  - Name I46
  - Host CMDHP3
  - Owner SAPR3

Figure 94: Additional SAP™ status information

The presented functions give the auditor a *sound overview of the system installation to be audited* during the basis application audit.

### 5.2.3 Mapping the business structure

A useful basis application audit of the SAP™ system requires information on how the company structure has been reflected in the SAP™ system. This raises questions like

- Which clients (group of companies) have been created in the production system and for which purposes are they being used?
- In which company codes (companies) are relevant transactions for financial statements (balance sheet, profit & loss account) being processed?
- In which organizational units (business areas) could additional business transactions be reflected?
- Which levels exist for stock evaluation (plants) and physical stock management (storage locations)?
- Are there organizational sub-units (purchasing or sales organizations), which could deal with vendors or customers in different ways?

In particular when assessing the efficiency of the internal control system, based on the authorization system in the SAP™ system, the auditor is depending on the detailed knowledge about the reflected business structures.

#### 5.2.3.1 Created clients

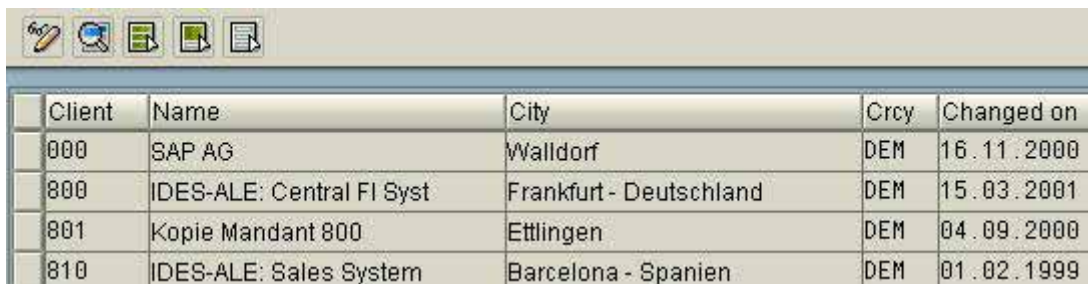
Information on the created clients in a system can be obtained via the AIS opening screen, calling the menu

Business audit

Organizational overview

Client

(transaction SCC4)



Client	Name	City	Crcy	Changed on
000	SAP AG	Walldorf	DEM	16.11.2000
800	IDES-ALE: Central FI Syst	Frankfurt - Deutschland	DEM	15.03.2001
801	Kopie Mandant 800	Ettlingen	DEM	04.09.2000
810	IDES-ALE: Sales System	Barcelona - Spanien	DEM	01.02.1999

Figure 95: Overview of the existing clients in a system, calling transaction SCC4

Client information can also be obtained via transaction SE16, in the table "T000".

The auditor should pay particular attention to the following facts:

## ❑ Purpose of the created clients

In a production system the following clients have usually been created:

- *Client 000*     *SAP<sup>TM</sup> delivery client*

The SAP<sup>TM</sup> delivery client is utilized as a reference for subsequently created production clients. A number of table details related to system control are referenced to the delivery client, and are of importance for the production client. Changes made by SAP in the delivery client will automatically change the production client, without overwriting modifications. Therefore, it is important to protect the delivery client from unauthorized access. The number of authorized users should be restricted only to employees, who are absolutely necessary for installation work.

- *Client XXX*     *production client*

All data required for the financial statements and the processing of business transactions are handled by the production client. Users with required authorizations are created for employees in this client. The auditor will put the focus of his audit activities on the production client.

- *Client 066*     *Early<sup>TM</sup>-Watch*

The client Early<sup>TM</sup>-Watch is created if the company is taking advantage of the Early<sup>TM</sup>-Watch service provided by SAP. SAP can be requested by the company to log on to its production system in order to analyze technical settings, without having access to production data.

Additional clients, in particular for *test or training purposes should not be created in the SAP<sup>TM</sup> production environment*. The unavoidably extensive user authorizations (e.g. for changing cross client tables) could otherwise endanger the system protection and security as well as the data integrity. Other systems in the SAP<sup>TM</sup> system group should be used for these purposes, as explained.

## ❑ Overview of created users in client 000

The auditor is usually busy with the production client, and gets an overview of *created users only in this client*. Additional information on created users in the delivery client can be obtained in the *system measurement* via the AIS opening screen, calling the menu

AIS opening screen

System audit

System configuration

System measurement

(transaction USMM) if he has the authorization.





Figure 96: Opening screen to system measurement


The button user list  is in the upper screen. In the following selection screen

Figure 97: Selection screen for the user list for system measurement

client 000 (delivery client) is entered. All users in client 000 are displayed on the screen.

User list for system measurement		
Clnt	User Name	User Type
000	BRAUN	
000	CCMS	
000	COMPARE	
000	CSMREG	
000	DDIC	
000	LOTUS	
000	MONSNG	
000	MONUSA	
000	RFC_IDESREPO	
000	SAP*	
000	SAPCPIC	
000	SCHAUER	
000	SCHUNTER	
000	TMSADM	

Figure 98: Overview of users in client 000

The auditor should make sure, that only the narrowest circle of administrative staff is listed.



## ❑ System and client modifiability

As already explained, no changes may be made in a production SAP™ system without audit trail, if the changes affect the financial statements. Audit relevant settings are required in two areas:

- *System modifiability*

The production system should generally be protected from changes. Necessary changes should be done in the system set up for customizing and be transported to the production client via the change and transport system. In order to control the settings for system changes, the function

System audit

Transport group

Configuration and status

Transport system configuration

(transaction SE06) can be called via the *AIS opening screen*.

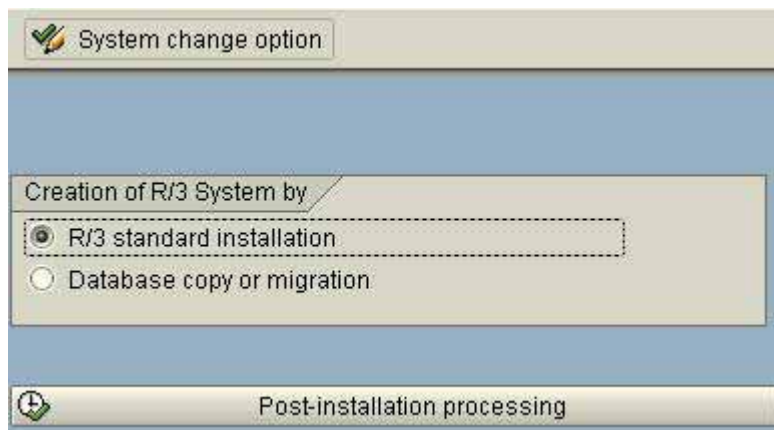



Figure 99: Opening screen to transaction SE06

With the button “system change option”  System change option in the upper screen, the “modifiable” technical settings can be displayed on the screen. In the menu “global settings” should the system be set to “not modifiable”.

Global setting			Not modifiable
Software component	Technical name	Modifiable	
Customer developments	HOME	Not modifiable	
Local developments (no automatic trans...	LOCAL	Not modifiable	
PI 99: Installation 1999_1_46B.	PI	Not modifiable	
R3_Plugin_99_46A_for_BW_BBP	PI-A	Not modifiable	
Cross-Application Component	SAP_ABA	Not modifiable	
Logistics and Accounting	SAP_APPL	Not modifiable	
SAP Basis Component	SAP_BASIS	Not modifiable	
Namespace/name range	Prefix	Modifiable	
Customer name range		Not modifiable	
General SAP name range		Not modifiable	

Figure 100: Modifiable system settings


- **Client modifiability**

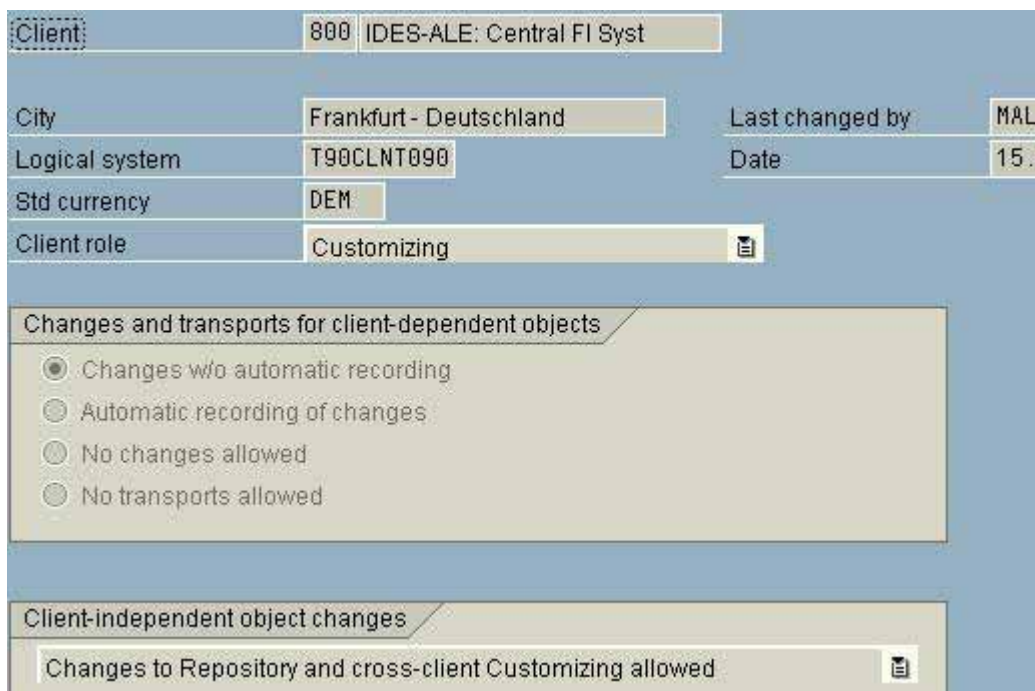
No changes on business objects in a client should be done without audit trail either. The auditor can enter the required settings in the AIS system, calling the menu

Business audit

Organizational overview

Client

(transaction SCC4). After marking the client, clicking the button  will show details. In the next screen the key word “changes” will show the settings.



Client	800	IDES-ALE: Central FI Syst	
City	Frankfurt - Deutschland	Last changed by	MAL
Logical system	T90CLNT090	Date	15.1
Std currency	DEM		
Client role	Customizing		

Changes and transports for client-dependent objects

- ☒ Changes w/o automatic recording
- ☐ Automatic recording of changes
- ☐ No changes allowed
- ☐ No transports allowed

Client-independent object changes

Changes to Repository and cross-client Customizing allowed

Figure 101: Details on client settings

The clients should be configured with settings to either *not allow any changes*, or *allow changes with automatic recording*.

### 5.2.3.2 Further elements of the company specific structure

The easiest way to map further elements of the company specific organization structure in the production client, such as company codes, business areas, plants and storage locations, is to call transaction SE16 and the tables

T001	company codes
TGSB	business areas
T001W	plants
T001L	storage locations

Table : T001  
Displayed fields: 17 of 69 Fixed columns:

	Client	Company code	Company name
<input type="checkbox"/>	800	0001	SAP A.G.
<input type="checkbox"/>	800	0100	CP COMPAS
<input type="checkbox"/>	800	0200	CP PLANTA
<input type="checkbox"/>	800	0300	CP PHARMA
<input type="checkbox"/>	800	0400	CP VITAL
<input type="checkbox"/>	800	1000	IDES AG
<input type="checkbox"/>	800	1100	test
<input type="checkbox"/>	800	1111	Test KOPLAN TRan

Figure 102: Created company codes in table T001

Generally, all tables beginning with "T0\*" are interesting for the auditor, as they contain the system information for controlling the financial accounting.

#### 5.4.2 Tools for system overview

Purpose	Transaction/function	Table	Program
Mapping the system	AIS + Transport Management System  SE16 and STMS	TSYST TASYS TWSYS  DEVL	
Operating system and database environment	Computer Management System  RZ20  SM51 + log  System/status		
Business structure	SCC4  SE16 and tables	T000  T001 TGSB T001W T001L	
System modifiability	AIS + Transport Management System  SE06		
Client modifiability	AIS + client  SCC4		
System measurement	USMM		

### Exercises on mapping the system

1. Check if client 066 Early<sup>TM</sup>-Watch has been created in your system, and if changes without audit trail are possible.

---

---

---

2. Which users have been created in client 000? Assess the risks!

---

---

---

3. Which type of computer and which databases is being used for operating the production system?

---

---

---

4. Which was the latest "hot package" to be transferred to your system?

---

---

---

5. Which settings are valid for the system modifiability?

---

---

---

6. Which storage locations have been created in your system and to which plants have they been allocated?

---

---

---

### **Checklist for system audits (mapping the system)**

- ❑ **Audit preparation**
  - Work place
  - Authorizations
  - Printer
  - AIS configuration
  - Contact person
- ❑ **Audit activities in the run-up to SAP**
  - Organizational structure of the IT department (segregation of duties)
  - Organizational policies and procedures and documentation for IT and system operations
  - Computer center security
  - Network security
  - Operating system security
  - Database security
  - Work station security
  - Rules for operating personal computers
- ❑ **Audit activities within the SAP system**
  - Overview of system group and transport routes
  - Installed servers
  - System overview and technique
    - SAP release version
    - Operating system
    - Database
    - Computer type (server)
  - Installed clients
  - Business structure
    - Company codes
    - Business areas
    - Plants
    - Storage locations
    - Etc.

### 5.3 Overview and assessment of in-house developments

#### 5.3.1 Basics on in-house developments

The setting of parameters for the complete system in controlling tables allows extensive customizing of the SAP<sup>TM</sup> standards to the specific requirements of a company, without utilizing the SAP integrated development environment for modifications or enhancements. In areas where the customizing does not enable a satisfactory reflection of the business processes, and the processes are not to be re-engineered according to SAP<sup>TM</sup>, the SAP<sup>TM</sup> standard system can be modified or enhancing functions like programs, tables and transactions can be developed in-house.

*Changes of the SAP<sup>TM</sup> standard programs* are generally possible. A development key has to be provided by SAP<sup>TM</sup>, which enables SAP<sup>TM</sup> to trace the changes. However, this kind of *modifications should be avoided* as far as possible, since they have to be tested manually with great effort after subsequent release upgrades. The certification by statutory auditors is not valid any more for applications, which are modified. Auditors should pay particular attention to this kind of modification, and critically assess the necessity and implementation.

Figure 103: Required development key for modifications

*Enhancing the system by additional functions*, which are not provided in the SAP<sup>TM</sup> standard, is common practice. For example complete sub-ledger for specific purposes are developed, utilizing the integrated programming language ABAP/4<sup>TM</sup>, or in-house developed tables are created and integrated to the system. For the auditor, the same quality standards apply for such in-house developments as for any other (non SAP) programming.

According to commercial and tax legislation, the SAP<sup>TM</sup> system has to be transparent when it goes live and during running operations. The system documentation has to be *sufficient and be of such quality*, that a competent third party is able to comprehend the processes within an acceptable (short) time frame. Additionally, for security and compliance reasons, the *development work has to be controlled*, the outcome has to be *sufficiently tested* and the integration in production operations has to be *comprehensible*.

### 5.3.2 Name ranges for in-house developments

In order to avoid collisions between SAP™ standard programs and customer specific in-house developments, SAP™ has released name ranges for in-house developments.

Object	Length	Customer name range
Change document object	10	Y..., Z...
Authorization / profile	12	No underscore at second digit
Authorization object	10	Y..., Z...
Data element	10	Y..., Z...
Data element supplement number	4	9000 - 9999
Domain	10	Y..., Z...
Screen number	4	9000 – 9999
Development class	4	Y..., Z...
Function module	30	Y..., Z...
Function group	4	Y..., Z...
Logical database	2	Y..., Z...
Menu	8	MENUY..., MENUZ...
Module pool screen	8	SAPMY..., SAPMZ...
INCLUDES	8	MY..., MZ...
Module pool dialog	8	SAPDY..., SAPDZ...
INCLUDES	8	DY..., DZ...
Module pool sub routine	8	SAPFY..., SAPFZ...
INCLUDES	8	FY..., FZ...
Module pool update	8	SAPUY..., SAPUZ...
INCLUDES	8	UY..., UZ...
Number range document object	10	Y..., Z...
Report	8	Y..., Z...
Report category	4	Y..., Z...
Lock object	10	Y..., Z...
SYSLOG messages	2	Y..., Z...
Table	10	Y..., Z..., T9..., P9...
Transaction code	4	Y..., Z...
View	10	Y..., Z...

It is of utmost importance for the system stability and auditability to adhere to the released name ranges for in-house developments. The name ranges protect the in-house developments from being accidentally overwritten by SAP™ standard programs at a release upgrade and enables recognition of in-house developments by the naming convention.

The auditor should make sure, that the development policies include binding rules for naming in-house developments



A few examples:

❑ **In-house developed transactions (example: ZFANLAAB)**

- First letter
  - Y transactions for administrative purposes
  - Z transactions for business purposes
- Second letter
  - F related application (here financial accounting)

❑ **In-house developed reports (example: ZFK3)**

- First letter
  - Y reports for administrative purposes
  - Z reports for business purposes
- Second letter
  - F related application (here financial accounting)
- third and following letters
  - - K... details on report contents (here vendors)

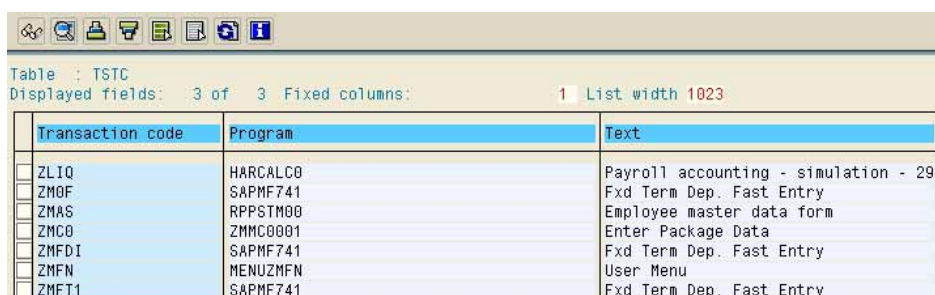
❑ **In-house developed tables (example: ZFKRED\_KON)**

- First letter
  - Y tables for administrative purposes
  - Z tables for business purposes
- Second letter
  - F related application (here financial accounting)
- third and following letters
  - - K... details on table contents (here vendors)

The presented examples are being used in many companies, but are not compulsory. For the auditor, it is only important to know if a company specific systematic for naming in-house developments has been established and if this systematic is being adhered to.

### 5.3.3 In-house developed transactions

An overview of in-house developed transactions, which adhere to the company specific naming convention, can be created by calling table TSTC in transaction SE16 (display tables) and entering "Z\*" in the field transaction code.



Transaction code	Program	Text
ZLIQ	HARCALC0	Payroll accounting - simulation - 29
ZMOF	SAPMF741	Fxd Term Dep. Fast Entry
ZMAS	RPPSTM00	Employee master data form
ZMCO	ZMMC0001	Enter Package Data
ZMFDI	SAPMF741	Fxd Term Dep. Fast Entry
ZMFN	MENUZMFN	User Menu
ZMFT1	SAPMF741	Fxd Term Dep. Fast Entry

Figure 104: Overview on in house developed transactions in the company's name range

For the first review, the generated table should be limited to the fields transaction code, program and transaction text by calling

Setting


List format

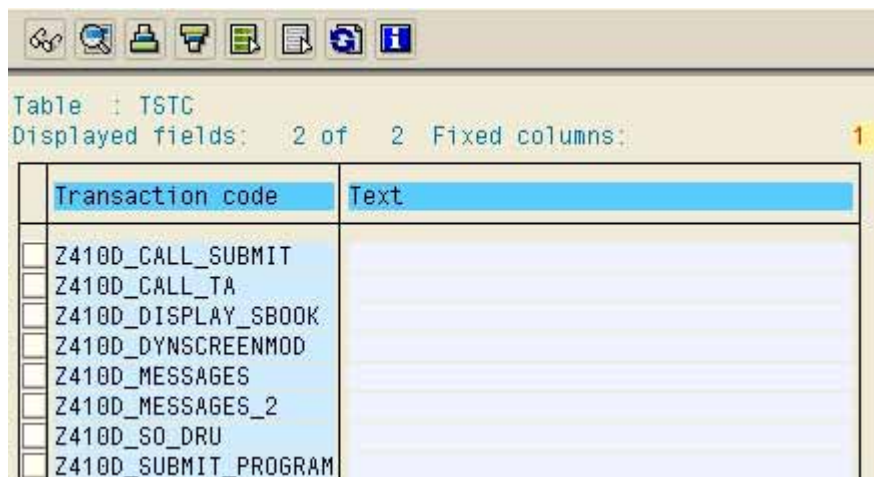
Choose fields

The auditor should take following audit aspects into consideration during the first review:

#### ❑ Sufficient description

Every listed transaction in the table TSTC should have a sufficient description of the purpose of the transaction. Missing descriptions affect system transparency and auditability, and should be criticized accordingly.

Transactions without description can be put at the beginning of the table, by using ascending sorting order  for the field transaction text.



The screenshot shows the SAP Table TSTC with the following data:

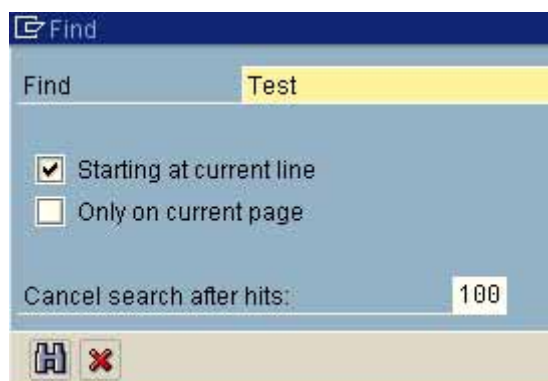
Transaction code	Text
<input type="checkbox"/> Z410D_CALL_SUBMIT	
<input type="checkbox"/> Z410D_CALL_TA	
<input type="checkbox"/> Z410D_DISPLAY_SBOOK	
<input type="checkbox"/> Z410D_DYNSCREENMOD	
<input type="checkbox"/> Z410D_MESSAGES	
<input type="checkbox"/> Z410D_MESSAGES_2	
<input type="checkbox"/> Z410D_SO_DRU	
<input type="checkbox"/> Z410D_SUBMIT_PROGRAM	

Figure 105: Transactions without sufficient description

#### ❑ Test transactions

No test procedures – as already mentioned - should be carried out in the production environment. Most test procedures are coded in the transaction name or in the description.

By clicking the binoculars  and enter "TST" or TEST" in the displayed screen

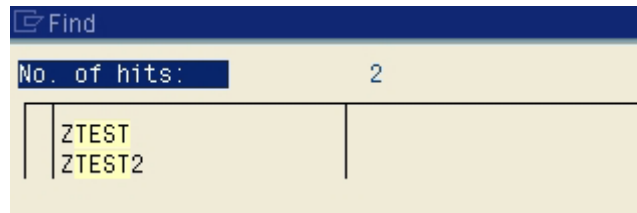


The screenshot shows the SAP Find dialog box with the following details:

- Find: Test
- ☒ Starting at current line
- ☐ Only on current page
- Cancel search after hits: 100

Figure 106: Finding test transactions

the auditor should know, it recognizable transactions for test purposes were carried out in the production system



Find	
No. of hits:	2
ZTEST	
ZTEST2	

Figure 107: Transactions for test purposes

The window displayed above, showing the number of hits, can be printed for the *work papers, using the right mouse button*.

#### ❑ Transactions with critical functions (e.g. delete)

Test and customizing procedures, which have to be carried out during the pre-production (configuration) phase of the SAP™ system, are often combined with complex deleting procedures, e.g. of complete company codes. These deleting procedures are mostly assigned to in-house developed transactions, which are not deleted from the system before the *system goes productive*. The auditor should search such transactions with terms like “DEL” or “REMOVE”.

#### ❑ Further conspicuous transactions

Blocked transactions can be found in the *Audit-Information-System*, calling the menu

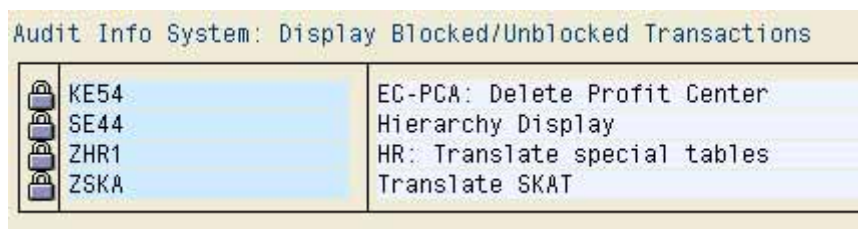
System audit

Development / Customizing

Transactions

Blocked transaction

(transaction SA38 and report RSAUDITC).



Audit Info System: Display Blocked/Unblocked Transactions	
KE54	EC-PCA: Delete Profit Center
SE44	Hierarchy Display
ZHR1	HR: Translate special tables
ZSKA	Translate SKAT

Figure 108: Overview of blocked transactions

Here the auditor should inquire about the reasons for the blocks. In many cases, *blocked transactions indicate insufficiently tested program functions, which are not acceptable in the production system.*

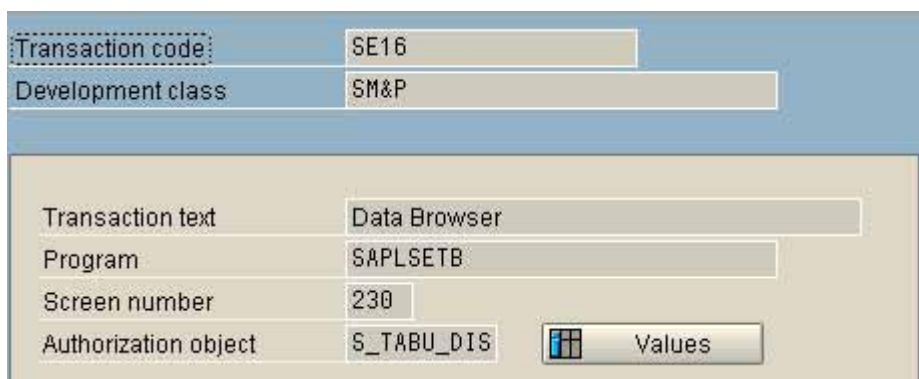
#### ❑ Assigned programs

In addition to the transaction names, table TSTC shows the assigned programs, which are called when a transaction is selected. At this point, it should be checked if incriminating transactions are connected to a executable program / report, and if these need to be audited in more detail, as will be described later on in this manual.

#### ❑ Authority checks after calling transactions

The authority check after calling a transaction is usually coded within the assigned programs. *In in-house developed programs, such an authority check is rarely implemented.* In stead, the option of connecting the transaction directly to an authorization object with protective function is chosen, in order to restrict the user's possibilities to execute the assigned program.

The auditor can convince himself, if an in-house developed transaction is connected to a protective authorization object by calling transaction SE93.



Transaction code	SE16
Development class	SM&P
Transaction text: Data Browser	
Program	SAPLSETB
Screen number	230
Authorization object	S_TABU_DIS
	Values

Figure 109: Display of transaction, connected to a protective authorization object

The *presented protection of program functions*, by connecting a *protective authorization object to a transaction is usually critical*, since many of the called programs are directly executable. In this case, the direct program start, by calling the widely spread reporting authorization (transaction SA38) and input the report name, would enable the user to pass the transaction oriented mechanisms for program protection.

### 5.3.4 In-house developed programs/reports

#### 5.3.4.1 Initial overview of in-house developed programs

The auditor can obtain an initial overview of in-house developed programs in the company's name range by calling the menu

System

Services

Reporting

(transaction SA38). In order to see all programs beginning with "Y" and "Z" on the screen, he must call the selection screen in the menu

Utilities

Find program

Program	YA	to	ZZ	[Arrow]
Authorization group		to		[Arrow]
Application		to		[Arrow]
Status		to		[Arrow]

Figure 110: Creating an overview of in-house developed reports in the company's name range

A complete overview of all such programs can be obtained by entering

Field from    YA


Field to        ZZ.

The auditor should look out for the following:

#### ❑ Sufficient titles

All presented programs should have a sufficiently descriptive title, stating the purpose of the program. Missing descriptions affect system transparency and auditability, and should be criticized accordingly.

#### ❑ Test programs

No test procedures should be carried out in the production environment. Most test procedures are coded in the program name or in the description. By clicking the binoculars  and enter "TST" or TEST" in the selection screen the auditor should know, if recognizable programs for test purposes were carried out in the production system

No. of hits: 79	
ZAUFK001	Test
ZBC400_00_TEST	
ZEMATEST	Show icon codes
ZFLEXIBEN	Test report Flexi Benefits
ZGRTEST	

Figure 111: Programs for test purposes

The window displayed above, showing the number of hits, can be printed for *the work papers*, using the *right mouse button*.

#### ❑ Programs with critical functions (e.g. delete)

Test and customizing procedures, which have to be carried out during the pre-production (configuration) phase of the SAP™ system, are often combined with complex deleting procedures, e.g. of complete company codes. These deleting procedures are mostly assigned to in-house developed programs, which are not deleted from the system before it goes productive. The auditor should search for such programs with terms like “DEL” or “REMOVE”.

No. of hits: 63	
ZA93DDEL	Delete Data From a Company Code in
ZABUCDEL	Delete Data From a Company Code in
ZALEDLE	De-activate ALE Data Model(s)
ZCATTDEL	Deleting CATTs
ZCATTFILE	Up- / Download- / Delete von CATTs
ZCB_USER_DEL	Lock User in a Client
ZDEL0002	
ZDELETE	Summarization: Sales Info System
ZDELTADIR	
ZEQUIDEL	Delete Serial Numbers

Figure 112: Critical programs

#### ❑ Further conspicuous reports

In addition to the presented strategies, all in-house developed programs in the company's name range should be printed and searched for conspicuous or critical functions in the descriptions. Practical experience show, that critical programs often are hidden in production systems, and are recognizable by e.g. exclamation marks, since they are related to deleting and similar procedures. The auditor should inquire about their benefit and security.

### 5.3.4.2 Detailed analyses of in-house developed programs

#### 5.3.4.2.1 Contents of the detailed analyses

The initial overview of the in-house developed reports has given the auditor an accurate impression of the document quality and the related system transparency. The detailed analysis will verify the (good or bad) impression by specific findings. The following aspects are relevant:

- Are in-house developments *documented* in a sufficient and comprehensive way?
- Are the in-house developments sufficiently *protected* from erroneous or unauthorized user access?
- Are only intended *developers* actually dealing with in-house developments?
- Have SAP<sup>TM</sup> *standard programs* been modified?

The detailed analysis consists of varied audit steps and requires plenty of time. The analysis should be restricted to a randomly selected sample of in-house developed programs. It is rarely necessary to analyze more than six to ten in-house developments in detail, in order to obtain a correct impression about all programs, including those, which were not in the sample.

Prior to the detailed analysis in the SAP<sup>TM</sup> system, the auditor should review the *written policies and procedures for development and documentation, as well as any available program files*, taking the following aspects into consideration

- Is a *procedure* for new development applications in place?
- Are there *naming conventions* for naming in-house developments?
- Are there instructions for the *utilization of protective authorization objects* within in-house developments or the assignment of such programs to *authorization groups*?
- Are defined *documentation requirements* available in writing?

If such procedures are not in place or if they are not sufficiently clear or of the required quality, no satisfactory results within the SAP<sup>TM</sup> system can be expected either.

#### 5.3.4.2.2 Utilizing the SAP<sup>TM</sup> editor

A string of audit relevant issues can be clarified by utilizing the SAP<sup>TM</sup> editor, which can be called in the menu

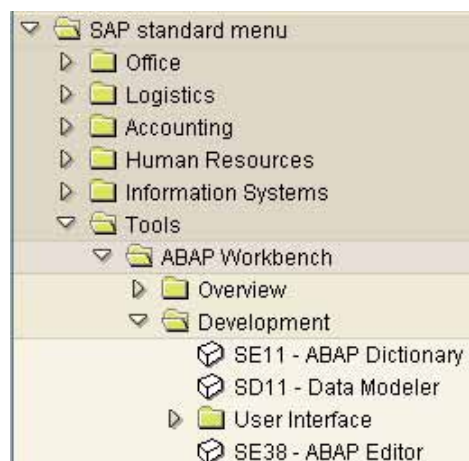


Figure 113: Menu for calling the editor



(transaction SE38). The reports in the randomly selected sample are input in the displayed selection screen.

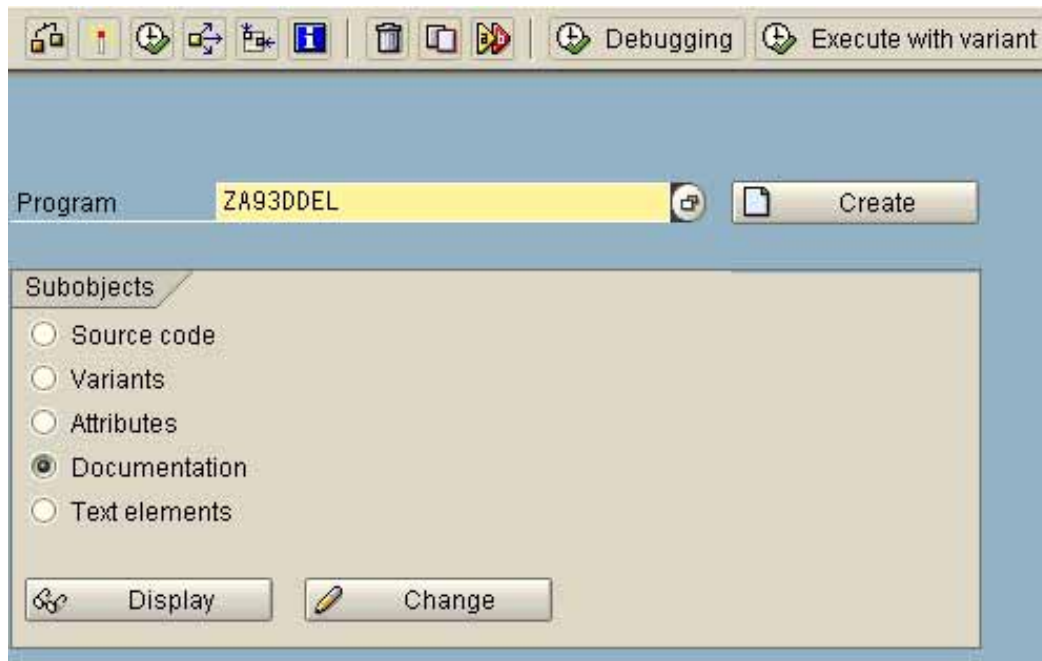


Figure 114: Options in the editor selection screen

In the selection screen, the options

- Documentation
- Attributes
- Source code

are available. They are useful for the following audit aspects:

#### ❑ Sufficient user help

A sufficient user help is of particular importance for users in the business departments. As soon as the user starts a program or a report of his interest, he should be able to get more information about the program, calling the menu "goto / documentation". This should include a *description of the program functions*, or the contents of the reports. The *conditions for starting the program* should also be stated. The same applies to *explanations of useful parameters or selection criteria*, which have to be input when starting a program.

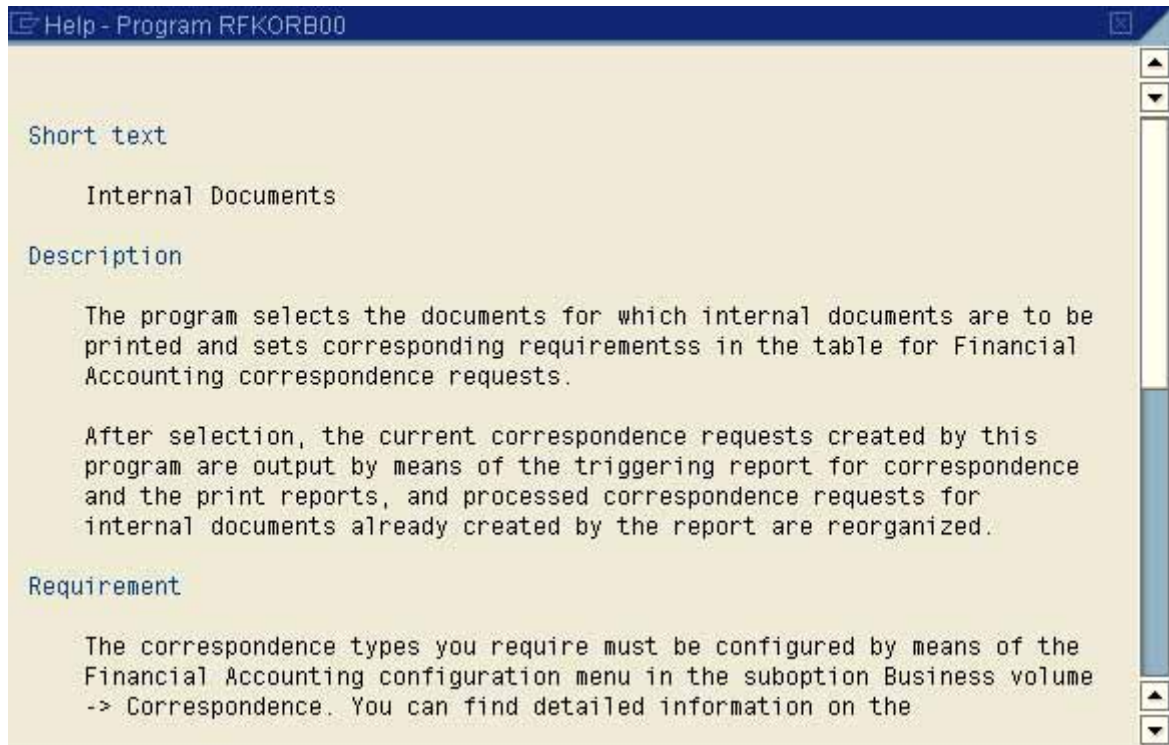


Figure 115: Example of proper SAP™ documentation of the report "RFKORB00"

Zur Ermittlung der Anwenderhilfe ist innerhalb des Auswahlbildschirms die Option "Dokumentation" zu markieren. Anschließend wird der Button „Anzeigen“ betätigt.

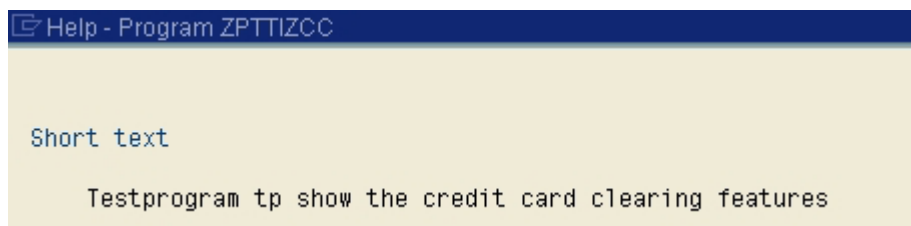
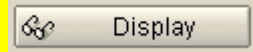


Figure 116: Example of insufficient user help

The displayed program help can be printed for the *work papers*, using the right mouse button.

#### ❑ Program attributes and program authors

More information – in particular about insufficiently described and documented programs – can be obtained by activating the option "*attributes*".

The displayed screen

ABAP: Program Attributes ZPTTIZCC

Title: Testprogram tp show the credit card clearing features

Original language: EN English

Created: 02.02.1997 PENNING

Last changed by: 24.09.1998 PENNING

Status: Active

Attributes

Type: Executable program

Status:

Application: Human resources

Authorization groups:

Development class: ZCAT Training CATTs for Walldorf/International use

Logical database: D\$\$ Processing without database

Selection screen:

☐ Editor lock ☒ Fixed point arithmetic ☐ Start using variant

Figure 117: Attributes of a selected in-house developed program

gives answers to questions about

- The program author and the date of creation  
Is the developer / consultant approved and when was the program created or changed?
- The program type  
Is it an independently executable program (in transaction SA38)?
- The program status  
Is it a customer production program, an SAP<sup>TM</sup> standard production program, a system program or a test program?
- The assigned application  
To which application area has the program been assigned, e.g. financial accounting, materials management, basis system etc.?
- The assigned authorization groups  
Is the program start secured by assignment to an authorization group, which can be checked in the authorization system?

SAP<sup>TM</sup> does not give the auditor a print option for the program attributes at this point. *Work papers* have to be created as a *screen copy* or by using the *clipboard*.

## ❑ Documentation in the source code

As a final step, the auditor can review the program code with the *option "source code"*. Experienced IT system auditors with knowledge of the programming language ABAP/4™ may find out the purpose of the program. However, the business auditor may also obtain additional information. This would include

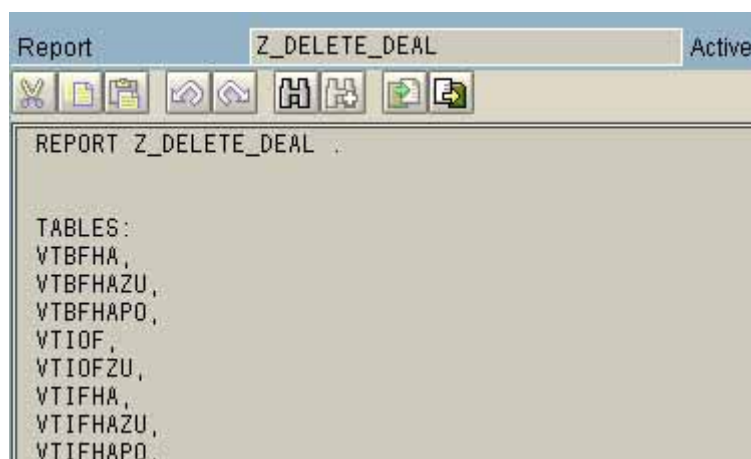
- Inline documentation

The complete documentation for in-house developments include the relevant program file, the described program help and the comment lines on the purpose and contents of the program and its life cycle in the source code.

```
*****
* report rpabri00_delete                                     *
* Purpose:                                                 *
* Delete entries in the payroll infotype before a certain *
* key date - instead of archiving them.                  *
*                                                         *
* VRMPH4xxxxx 120698 New report                          *
*****
REPORT RPABRI00_DELETE MESSAGE-ID RP.
TABLES: PERNR, T52IA, T777D, PA0402.
```

Figure 118: Describing inline documentation

In-house developed programs, with neither a program file, a meaningful program help nor a meaningful inline documentation are affecting the system transparency and audit ability. Additionally, the system is not in compliance with commercial and tax legislation regarding financial accounting records.



```
Report      Z_DELETE_DEAL      Active
[Icons]
REPORT Z_DELETE_DEAL .

TABLES:
VTBFHA,
VTBFHAZU,
VTBFHAPO,
VTIOF,
VTIOFZU,
VTIFHA,
VTIFHAZU,
VTIFHAPO,
```

Figure 119: Critical in-house developments without sufficient inline documentation


- Coded authority check

*Critical in-house developments*, which e.g. change databases or controlling information or are related to deleting procedures can be *protected from unauthorized user access in two ways*. One option is to assign the program to privileged *authorization groups*, as already explained. The second, more elegant option is to implement a *check of authorization objects with protective function in the source code*. Only those users, who have the adequate authorization for the protective authorization object in their user master record will be able to call such programs. The importance of the protective authorization objects and the authority checks will be described at length later in this manual. At this point it is of interest to the auditor, if the *calling of protective authorization object was coded in the source code*.

The required programming line is

“AUTHORITY-CHECK”

followed by the name of the protective authorization object and the required field values for starting the program, which have to be included in the user authorization profile.

The auditor can find out if the authority check is in the source code by clicking the binoculars  and search for “AUTHORITY-CHECK”.

Program	Found locations/short description	
<input type="checkbox"/> RFKORB00	214	AUTHORITY-CHECK OBJECT 'F_BKPF_BUK'
		ID 'ACTVT' FIELD '03'
		ID 'BUKRS' FIELD BKPF-BUKRS.
	244	AUTHORITY-CHECK OBJECT 'F_BKPF_BLA'
		ID 'ACTVT' FIELD '03'
		ID 'BRGRU' FIELD T003-BRGRU.

**Figure 120: Example of a coded authority check**

All executable *in-house developed programs* with unclear or problematic contents are *critical*, if they are not protected from unauthorized access by *neither an assigned authorization group nor a coded authority check*.

### 5.3.4.2.3 Table TRDIR

Detailed information on in-house developed programs / reports can not only be obtained in the editor but also by calling *table TRDIR (report directory) in Transaction SE16*. The table contains the following fields,

Field name	Field text
SQLX	Source code protection
EDTX	Editor lock flag
VARCL	Upper/lower case
DBAPL	Application database
DBNA	Logical database
CLAS	Program class
TYPE	Selection screen
OCCURS	Automatically generated program
SUBC	Program type
APPL	Application
SECU	Authorization group
CNAM	Created by
CDAT	Created on
UNAM	Last changed by
UDAT	Last changed on
VERN	Version number
LEVL	Level
RSTAT	Status
RMAND	Client
RLOAD	Original language
FIXPT	Fixed point arithmetic
SSET	Start only via variant
SDATE	Standard selection screen generation: Date
STIME	Standard selection screen generation: Time
IDATE	Selection screen generation: Date
ITIME	Selection screen generation: Time
LDBNAME	LDB name
UCCHECK	Unicode checks active

Figure 121: Data fields in tabl TRDIR

which can be used for varied audit activities.

The programs in the company's name range should be input in the selection screen

Program name: from <-> YA to <-> ZZ

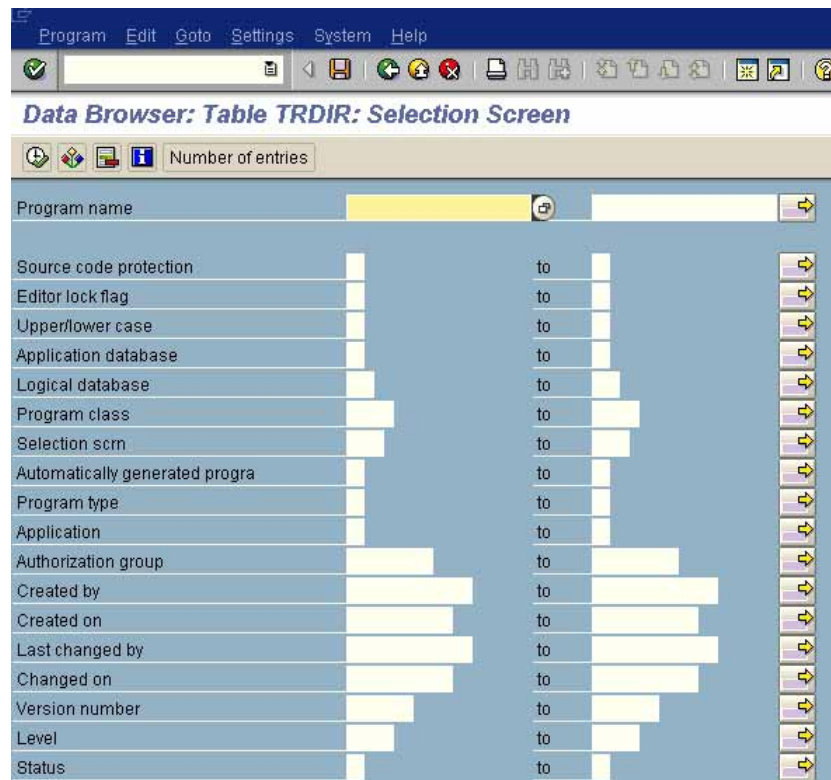


Figure 122: Selection screen for tabel TRDIR

Important fields are

- Program name
- Automatically generated program
- Program type
- Application
- Authorization group
- Created by
- Created on
- Last changed by
- Last changed on

which can be marked and selected in the menu

Settings

List format

Choose fields

Now summarized statements to the following questions are possible:

☐ **Assignment of in-house developed programs to authorization groups**

In-house developed programs, which have been assigned to authorization groups show entries in this field. Available authorization groups can be displayed by calling *table "TBGP" in transaction SE16*. The auditor should make sure, that only few users in privileged authorization groups can access critical programs.



#### ❑ Program type “executable programs”

Directly executable programs can be started immediately by calling general reporting (transaction SA38). They are *marked by “1” in the field “program type”*. With this program type, transaction oriented program start protection can possibly be ignored.

#### ❑ Assigned application

The field “application” states the first letter of the application, to which the program has been assigned (F – FI, financial accounting, M – MM, materials management, S – basis system). Here the auditor can see, if critical in-house developments are assigned to e.g. financial accounting and have to fulfill specific protection / compliance requirements.

#### ❑ Program development and changes

The auditor can *compare the listed names* to approved program authors. If recent programs have been created or changed by unknown authors or by authors, who should not have programming authorization, the auditor needs to clarify such matters.

The auditor should also make sure, that *group names*, such as

Developer  
Administration  
Programmer

are *not used* for in-house developments and changes, since they usually can not be traced to one individual. This would violate legal requirements of documentation, and decrease the system auditability.

The same applies for the special users in every SAP™ system

SAP\*  
DDIC

which should generally not be used for development purposes.



The characteristics of these special users will be described later on.

Table : TRDIR  
Displayed fields: 11 of 11 Fixed columns: 1 List width 1023

Program name	Program type	Application	Authorization group	Created by
<input type="checkbox"/> ZXMCBU02	I	S		D019512
<input type="checkbox"/> ZXMCDTOP	I	*		SCHAFER
<input type="checkbox"/> ZXMCDU01	I	*		SCHAFER
<input type="checkbox"/> ZXNIWU05	I	M		GRUNEWALDK
<input type="checkbox"/> ZXPCAU03	I	S		BEUTELS
<input type="checkbox"/> ZXQUEU01	I	S		BUCHHOLZF
<input type="checkbox"/> ZXSOPU20	I	S		MURAYAMA
<input type="checkbox"/> ZXSOPU21	I	S		MURAYAMA
<input type="checkbox"/> ZXUSRF01	I	S		CURA
<input type="checkbox"/> ZXUSRTOP	I	S		CURA
<input type="checkbox"/> ZXUSRU01	I	S		CURA
<input type="checkbox"/> ZXUSRU01_01	I	S		STADEL
<input type="checkbox"/> ZXUSRU01_02	I	S		STADEL
<input type="checkbox"/> ZXUSRZZZ	I	S		CURA
<input type="checkbox"/> ZXV46U01	I	S		SZABADI1711
<input type="checkbox"/> ZXV51U01	I	S		DEVENTER
<input type="checkbox"/> ZXV51U02	I	S		DEVENTER
<input type="checkbox"/> ZYIDES_USER_EXITU01	I	S		STADEL
<input type="checkbox"/> ZYIDES_USER_EXITU01_TOP	I	S		STADEL
<input type="checkbox"/> ZZ	1	S		TEST-03

Figure 123: Overview of the contents in table TRDIR for company in-house developed programs

#### ❑ Changes of SAP™ standard programs by company in-house program authors

The auditor will find indications of *changed SAP™ standard programs* in the name range reserved for SAP, if he *excludes all program names beginning with “Y” and “Z”* in the field for program name selection with the selection options  inputs *selection criterion “P”* (SAP™ standard application program) in the *status field*, *excludes automatically generated programs* and *enters the approved in-house developers / consultants* in the field “created by” (using multiple selection ).



The screenshot shows the SAP selection criteria screen with the following fields and values:

Field	Value	Operator	Field	Value
Program name	YA	to	ZZ	
Automatically generated progra	X	to		
Created by		to		
Created on	01.01.2000	to		
Last changed by	RV_BENU1	to		
Changed on		to		
Status		to		

Figure 124: Limiting the selection in order to find changes of SAP™ standard application programs

The results are to be questioned. Such changes can occur e.g. in connection with a release upgrade, at a larger extent. These changes are recognizable by the same date. For other changes in the SAP name range, there have to be OSS errors and notes on corrections.

#### 5.3.4.2.4 Utilizing the SAP AIS™ system for detailed analyses

For some of the presented audit activities, additional functions are available within the AIS™ system, calling the menu

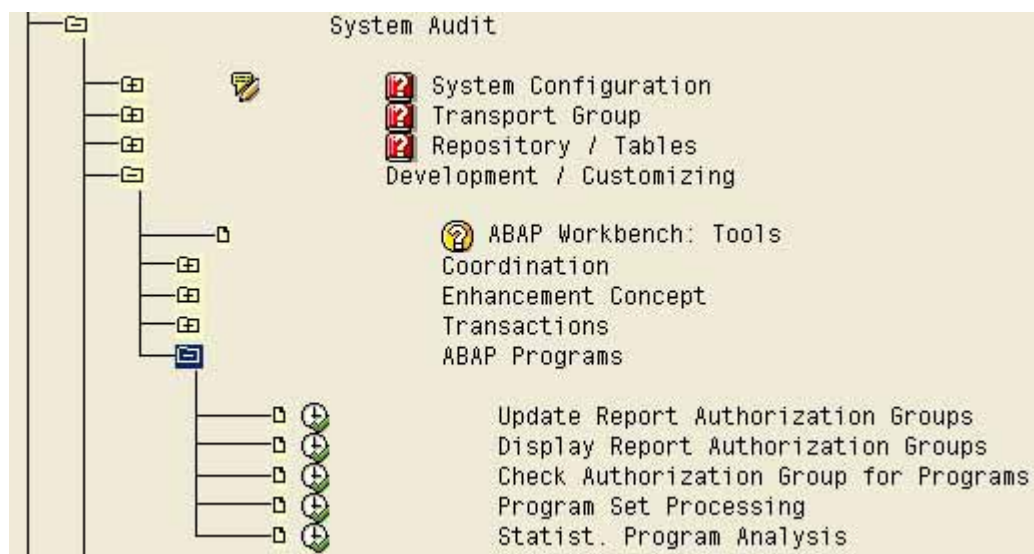
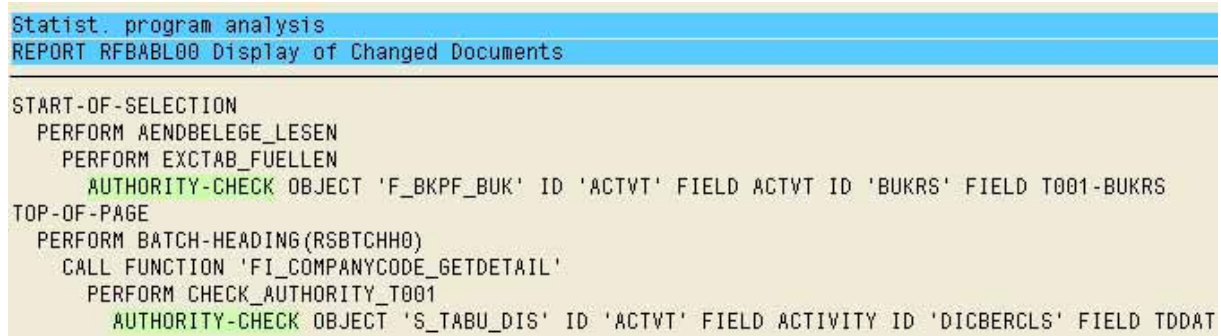


Figure 125: AIS™ functions for ABAP™ program analyses

The functions will be described in detail.

- Display report authorization groups  
This command displays a list of created authorization groups, which in-house developed reports can be assigned to (table TBGP).
- Check authorization group for program  
This function displays, if and where applicable, which authorization groups have had programs assigned to them.
- Statistical program analysis  
This *function is important for the auditor*, as he can find ABAP™ language commands, such as the instruction “AUTHORITY-CHECK”.



```
Statist. program analysis
REPORT RFBABL00 Display of Changed Documents

START-OF-SELECTION
  PERFORM AENDBELEG_LESEN
  PERFORM EXCTAB_FUELLEN
  AUTHORITY-CHECK OBJECT 'F_BKPF_BUK' ID 'ACTVT' FIELD ACTVT ID 'BUKRS' FIELD T001-BUKRS
TOP-OF-PAGE
  PERFORM BATCH-HEADING(RSBTCHHO)
  CALL FUNCTION 'FI_COMPANYCODE_GETDETAIL'
  PERFORM CHECK_AUTHORITY_T001
  AUTHORITY-CHECK OBJECT 'S_TABU_DIS' ID 'ACTVT' FIELD ACTIVITY ID 'DICBERCLS' FIELD TDDAT
```

Figure 126: Finding the ABAP™ language command "AUTHORITY CHECK" in the report RFBABL00

This function is of particular interest for the analysis of a *transaction authorization check*, which usually includes several programs. This will be described in detail in the section “authorization checks”.

### 5.3.5 In-house developed tables

#### 5.3.5.1 Introduction

Tables, in combination with their **protection and security**, control the performance of the SAP<sup>TM</sup> system and influence the **proper processing** of SAP<sup>TM</sup> supported **business processes** as well as the **quality of generated data**. At the same time, the tables save the **application data**, beginning with the company and process organizational structures, and ranging to the outcome of the financial accounting. The transparency of the complete financial accounting processes, including changes, has to be ensured, not only due to company interests for protecting the company, but also for purposes stated in commercial and tax laws. The same applies for tracking changes of saved application data.

The documentation for table contents, changes of contents or changes of structure has to be kept (recording and archiving) as required by commercial and tax laws.

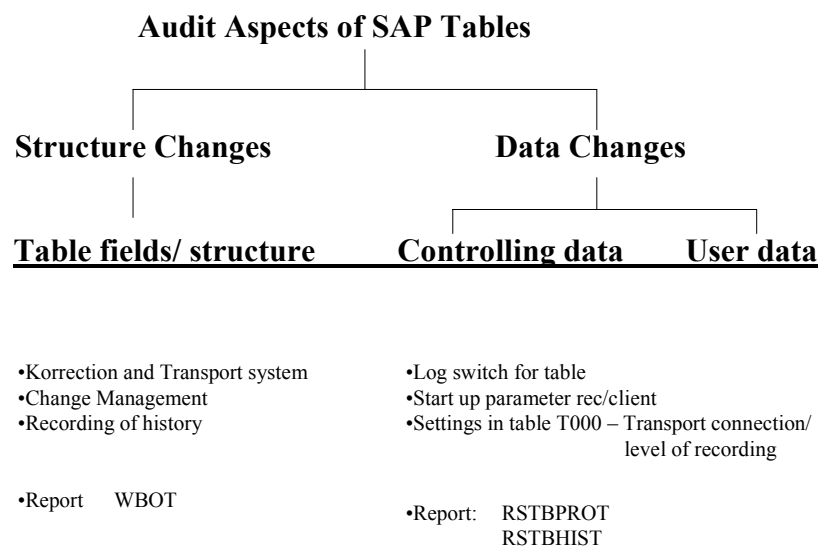


Figure 127: Audit aspects of an SAP<sup>TM</sup> table

In order to meet the described requirements, the SAP<sup>TM</sup> system is providing several protective mechanisms, which need to be critically assessed by the auditor. The assessment includes *review of current and previous settings for table logs, identification of critical tables and their purpose, documentation evaluation and tracking structural changes in central tables*.

#### 5.3.5.2 Initial overview of in-house developed tables

The auditor can create an *overview of in-house developed tables*, or track *audit relevant issues*, by calling “repository / tables” in the “system audit” in the AIS<sup>TM</sup> system, where several functions and programs are provided.

An overview of in-house developed tables can be obtained with the functions  
System audit  
Repository / tables  
Repository information system  
(transaction SE84). In the displayed menu

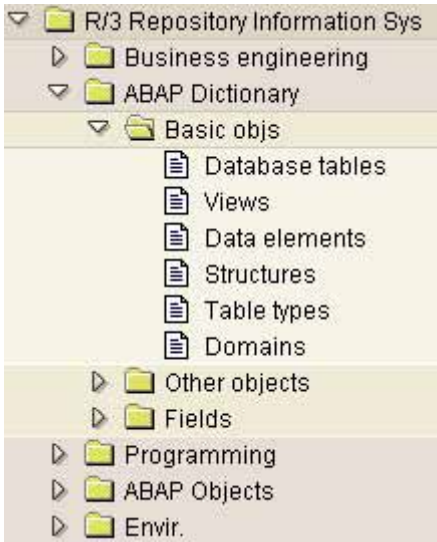


Figure 128: Selection screen in the repository information system  
“database tables” is activated.

SAP™ has released name ranges for company specific in-house tables, which begin with “Y” and “Z”. By entering “Z\*” in the displayed selection screen

Standard selections	
Table name	Z*
Short description	
Development class	


Figure 129: Selecting in-house developed tables  
an overview of in-house developed, company specific table can be created.

Table name	Short text
<input checked="" type="checkbox"/> ZABW01	Allowed deviation for period
<input type="checkbox"/> ZADRUSAB	Adress Data for Usability Example
<input type="checkbox"/> ZARIXC01	
<input type="checkbox"/> ZARIXPP1	
<input type="checkbox"/> ZARTJ	RT Article Table for Data Generation


Figure 130: in-house developed, company specific tables

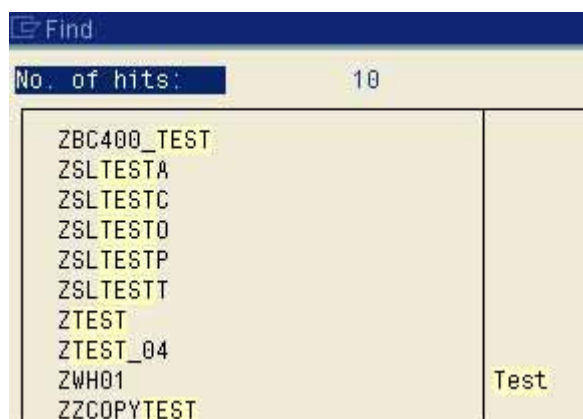
Tables have to meet the same requirements as in-house developed programs, as they influence the business processes and the quality of generated financial accounting data, due to their information and controlling structure. The auditor must obtain information on the following:

#### ❑ Sufficient texts

All presented tables should have a *sufficiently descriptive text, stating the purpose of the table*. Missing descriptions, which can be listed by marking and sorting the field “short text” in ascending order with , affect system transparency and auditability, and should be criticized accordingly.

#### ❑ Test tables

No test procedures should be carried out in the production environment. Most test procedures are *coded in the table name or in the text*. By clicking the binoculars  and enter “TST” or TEST” in the selection screen the auditor should know, it recognizable tables for test purposes were created and used in the production system



Find	
No. of hits:	10
ZBC400_TEST	
ZSLTESTA	
ZSLTESTC	
ZSLTEST0	
ZSLTESTP	
ZSLTESTT	
ZTEST	
ZTEST_04	
ZWH01	
ZZCOPYTEST	Test

Figure 131: Identifying tables for test purposes

The window displayed above, showing the number of hits, can be printed for the work papers, using the right mouse button.

#### ❑ Tables with critical functions or contents

*In-house developed tables* often serve in-house developed sub ledgers or *reports with specific data from the production financial accounting system*, which are relevant for the financial audit. It is important to identify such tables already during this initial overview, since they may have to meet *specific requirements for protection, security and comprehension* of data changes.

Table name	Short text
<input type="checkbox"/> ZKRBRT	Text Table for Material Area Values
<input type="checkbox"/> ZKRMA	Value Table for Material Criteria
<input type="checkbox"/> ZKRMAT	Text Table for Status Value Table
<input type="checkbox"/> ZKRSD	Value Table for Material Areas
<input type="checkbox"/> ZKRSDT	Text Table for Material Area Values
<input type="checkbox"/> ZKSTA	FB01 Postings cost types
<input type="checkbox"/> ZKSTL	Cost centers to be ignored in actual postings

Figure 132: Overview of tables with potentially important contents, relevant to the financial accounting



### **5.3.5.3 Detailed analysis of in-house developed tables**

#### **5.3.5.3.1 Development and changing procedures**

Structural changes (e.g. new fields) of in-house developed tables are to be categorized as development activities. *The development of tables should not be assessed any differently than that of programs*, and there have to be comparable procedures for creating and changing tables. This includes *defined development and documentation procedures in writing as well as program files*, which can answer the following questions:

- Is a *procedure* (application, test and release) for creating tables in place?
- Are there *naming conventions* for naming in-house developed tables?
- Is there a procedure for assigning in-house developed tables to *authorization groups*?
- Are clearly defined *documentation procedures* available?
- Have the circumstances for required *logging* of data changes in in-house developed tables been clearly defined?

If such procedures are not in place or if they are not sufficiently clear or of the required quality, no satisfactory results within the SAP™ system can be expected either.

For structural changes in tables and changes of their “technical settings”, the listed documentation must be available. The technical implementation within the SAP™ system takes place, utilizing the change and transport system. The changes are recorded in logs and can be tracked.

#### **5.3.5.3.2 Logging data changes**

The tables and their administered data are in charge of different tasks within the SAP™ system. They contain and control

- Reflecting the company specific *organizational structure*  
Created clients, company codes, business areas, cost centers, purchasing and sales organizations, storage locations etc.
- System *access*  
User master records and access authorization as well as checking procedures
- Automated, *pre-configured processes*  
Selecting accounts for automated posting procedures, utilization of calculation models etc.
- *Business transaction data*

and are assigned to different *delivery classes*, depending on their purpose.



**TABLE CLASSIFICATION**

Delivery class	Type	Example	Maintenance
A	User table	Master and transaction data	Company (transaction)
C	Company table	BUK	Company
L	Temporary file		Company
E	System table		Company for SAP™
G	Protected customer table	Number ranges	SAP™ + company
S	System table (program character)		SAP™
W	System table for maintenance		Correction and transport table

Figure 133: Classification of SAP™ tables

The obligation to keep logs on in-house developed tables is derived from relevant commercial and tax laws on comprehensive accounting data. It is important to note, that logs are to be kept *not only for data directly linked to the financial accounting but also for so called secondary data*, which are of importance for finding accounting relevant data. A detailed classification will be difficult for the auditor, as he needs to evaluate the complete context of the table utilization. *Usually, all data changes in all in-house developed tables should be kept in logs*, to ensure compliance with legal regulations.

Data changes are recorded under two conditions:

☐ **Activating the parameter “rec/client” in the SAP™ start-up profile**

The “general switch” for table logs has to be activated. The auditor can check this, calling the menu

System audit

Repository / tables

Table recordings

System parameters

(transaction SA38 and report RSPARAM).

Profile parameters valid in the current system: Substituted form		
Parameter name based on selection		
rec/client		
Parameter name	User-defined value	Sys.
rec/client		OFF
Activate/Deactivate table auditing		

Figure 134: Setting of the parameter rec/client for table logging

The proper setting requires an *entry for the delivery client "000" and the production system or "ALL"* in the field for user-defined value. It has to be noted, that the log parameter is set to "OFF" in the standard delivery version.

The setting "OFF" *can only be justified during the pre-production phase*, where manifold tests and customizing procedures would cause an unnecessary great volume of data. When the *system goes live*, it is a *compulsory requirement* to activate the log parameter, in order to enable a proper SAP™ operation.

#### ❑ Activating the log switch in specific in-house developed tables

In addition to the general switch, it has to be *decided for every single table, if data changes are to be logged*. This is done in the technical settings of each table, which will be discussed in detail.

A complete overview of the in-house developed tables without table log is the displays in the AIS™ report

System audit

Repository / tables

Table recordings

Tables with/without table log

(transaction SA38 and report RDDPRCHK), which takes the user to the following selection screen.

Table name	ya	to	zz	➔
Component ID		to		➔
Development class		to		➔
Delivery class		to		➔
Logging	<input type="radio"/> All	<input type="radio"/> available	<input checked="" type="radio"/> Not avlble	
Customizing activity	<input checked="" type="radio"/> All	<input type="radio"/> available	<input type="radio"/> Not avlble	
Current settings	<input checked="" type="radio"/> All	<input type="radio"/> available	<input type="radio"/> Not avlble	
Change doc. object	<input checked="" type="radio"/> All	<input type="radio"/> available	<input type="radio"/> Not avlble	
Client-dependence	<input checked="" type="radio"/> All	<input type="radio"/> available	<input type="radio"/> Not avlble	
Table maintenance using SE16	<input checked="" type="radio"/> All	<input type="radio"/> available	<input type="radio"/> Not avlble	
<input checked="" type="checkbox"/> Display Customizing activity				
<input checked="" type="checkbox"/> Consider exceptions				

Figure 135: Selection screen for audit of log switches in specific tables

The logging of important tables is shown with this function. For the audit of *in-house developed* tables, the table selection should be restricted to the company's name range

From YA to ZZ

The other parameters in this selection screen such as logging, customizing activities, table maintenance etc. concern critical aspects and require no particular setting in this initial overview.



The *flag* “currency/quantity fields” displays available data fields. These gives the auditor hints, if this table needs to be logged.

#### ❑ Data class and who changed the table

The *flag* “attributes” displays who created or changed the table structure, the date, the data class and the delivery class.

Transparent table: ZTRC01 Active

Short text: RIS/ABC: Weighting Factors for Purchase Order Processing

Attributes Fields Currency/quant. fields

Last changed on/by: FREITAG 19.01.2000

Development class: ZRCO

Original language: DE

Data class: Transparent table

Delivery class: Customizing table, maintenance only by cust., not SAP import

☒ Table maintenance allowed

Figure 138: Overview of table attributes of an in-house developed table

Here can also be seen, if “table maintenance allowed” has been activated to enable data changes with the standard transactions SM30 – 32.

#### ❑ Assigning tables to authorization groups

The assignment of tables to *authorization groups* is displayed in the *field* “auth” in the report “table logging”

Check Table Logging				
	Development class	TabType	Clt	SE16 Auth
Change document object/Customizing activity				
<input type="checkbox"/> ZST_DOC_EXCL	Exception List Documents			
	ZZST	TRANSP	■	&NC&
	No change document object for this table			
	No Customizing activities for this table			
<input type="checkbox"/> ZST_MAKT	Material Descriptions			
	\$TMP	TRANSP	■	&NC&
	No change document object for this table			
	No Customizing activities for this table			
<input type="checkbox"/> ZSWM01	Results table for workflow mail demo			
	\$TMP	TRANSP	□	
	No change document object for this table			
	No Customizing activities for this table			
<input type="checkbox"/> ZTEST				
	\$TMP	TRANSP	■	
	No change document object for this table			
	No Customizing activities for this table			

Figure 139: Extract from the report “table logging”



The table can be changed by any user, who is authorized to maintain tables, if no authorization group is listed (red display). This also applies to tables, which are protected by the authorization group "&NC&", since this is not a privileged class.

In order to assess if an appropriate privileged authorization class has been assigned to the table, the auditor can call *table TBRG* in transaction SE16,

Table : TBRG  
Displayed fields: 4 of 4 Fixed columns:

	Client	Object	Authorization	Description
<input type="checkbox"/>	800	S_TABU_DIS	&NC&	w/o auth. group
<input type="checkbox"/>	800	S_TABU_DIS	0SBC	Set country version
<input type="checkbox"/>	800	S_TABU_DIS	AA	RA:Application table
<input type="checkbox"/>	800	S_TABU_DIS	AC	RA:User-controlled
<input type="checkbox"/>	800	S_TABU_DIS	ACIN	FI/CO Interface
<input type="checkbox"/>	800	S_TABU_DIS	ALE0	ALE: Table maint.
<input type="checkbox"/>	800	S_TABU_DIS	AS	RA:SAP-controlled
<input type="checkbox"/>	800	S_TABU_DIS	ATES	Test
<input type="checkbox"/>	800	S_TABU_DIS	B0SD	System data maint.

Figure 140: Authorization classes in table TBRG

which displays *all authorization classes for tables*. If the AIS™ system has not been installed, the assignment of specific tables to authorization groups can be checked by *calling table TDDAT* in transaction SE16.

Table : TDDAT  
Displayed fields: 4 of 4 Fixed columns: 1

	Table name	Authoriz.class	Authorization
<input type="checkbox"/>	AD01C_CHK		&NC&
<input type="checkbox"/>	AD01C_CHK1		&NC&
<input type="checkbox"/>	AD01C_CT		AC
<input type="checkbox"/>	AD01C_CTT		AC
<input type="checkbox"/>	AD01C_MAT		AC
<input type="checkbox"/>	AD01C_MATA		AC
<input type="checkbox"/>	AD01C_PROF		&NC&
<input type="checkbox"/>	AD01C_PRTX		AC

Figure 141: Overview of tables and their assignment to authorization classes in table TDDAT

❑ **Technical setting for specific tables**

Calling information on data fields and table structure was already described. It was also mentioned, that a table log is kept only if the individual table log switch is activated, in addition to the general switch (rec/client). This can be checked in the technical table settings, calling the AIS™ menu

System audit  
Repository / tables  
Table recordings  
Technical table settings

**Technical settings** In the lower screen is the option “log data changes”, which has to be marked.

The screenshot shows the 'Technical settings' dialog for table ZST\_DOC\_EXCL. The 'Log data changes' checkbox at the bottom is highlighted, indicating it should be checked.

Figure 142: Technical settings ?????


If there is no AIS™ system, the auditor can obtain a *summarized overview of the technical settings* and missing log marks by calling *table DD09L* (field “log”) in transaction SE16.

Table : DD09L  
Displayed fields: 6 of 6 Fixed columns: 3 List width 1023

Table name	Data class	Log	Last changed by	Date	Time
<input type="checkbox"/> ZABW01	APPL0	X	YANG	19.01.2000	10:24:33
<input type="checkbox"/> ZADRUSAB	APPL0		KREICHGAUER	19.01.2000	10:24:34
<input type="checkbox"/> ZARIXC01	APPL2		HOLLAUS	21.03.2001	12:02:19
<input type="checkbox"/> ZARIXPP1	APPL2		KUNITZ	19.01.2000	10:23:04
<input type="checkbox"/> ZARTJ	APPL2	X	BOLLINGER	19.01.2000	10:27:52
<input type="checkbox"/> ZAUFRAG	APPL0	X	YANG	19.01.2000	10:23:04
<input type="checkbox"/> ZAUTOTR	APPL1		D000195	19.01.2000	10:23:05
<input type="checkbox"/> ZBC400_TEST	APPL1		HOLETZEK	26.06.2002	10:27:52
<input type="checkbox"/> ZBGR	USER	X	YANG	19.01.2000	10:24:35
<input type="checkbox"/> ZC001	USER		I015895	24.02.2000	14:27:59
<input type="checkbox"/> ZC003	USER		I015895	25.02.2000	13:50:47
<input type="checkbox"/> ZC005	USER		I015895	19.01.2000	10:25:56

Figure 143: Information on table logs in table DD09L

#### ❑ Where-used list for in-house developed tables

The auditor will find the usage of in-house developed tables, for example in in-house developed programs, by clicking the button “where-used list” , which will take him to the selection screen

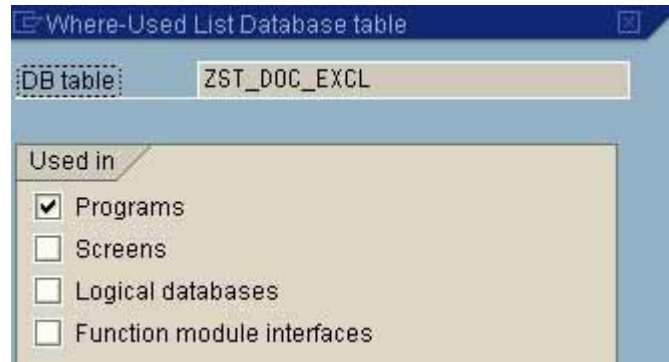


Figure 144: Selection screen and outcome for tracking the usage of in-house developed tables

The outcome gives the auditor further indications, if this table is to be considered as critical and needs to be sufficiently protected by authorization classes and if the table contents needs to be logged.

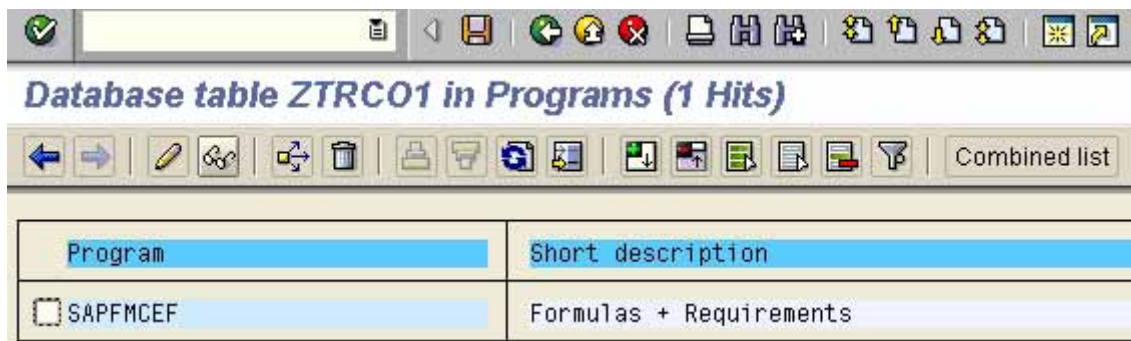


Figure 145: Where used list for a selected table

#### ❑ Change documents for in-house developed and other critical tables

Data changes in critical tables during a specified period of time can be obtained in the AIS™ system – if the log switch has been activated – by calling the menu

System audit

Repository / tables

Table recordings

Analysis table history

(transaction SA38 and reports RSTBHIST and RSTBPROT).



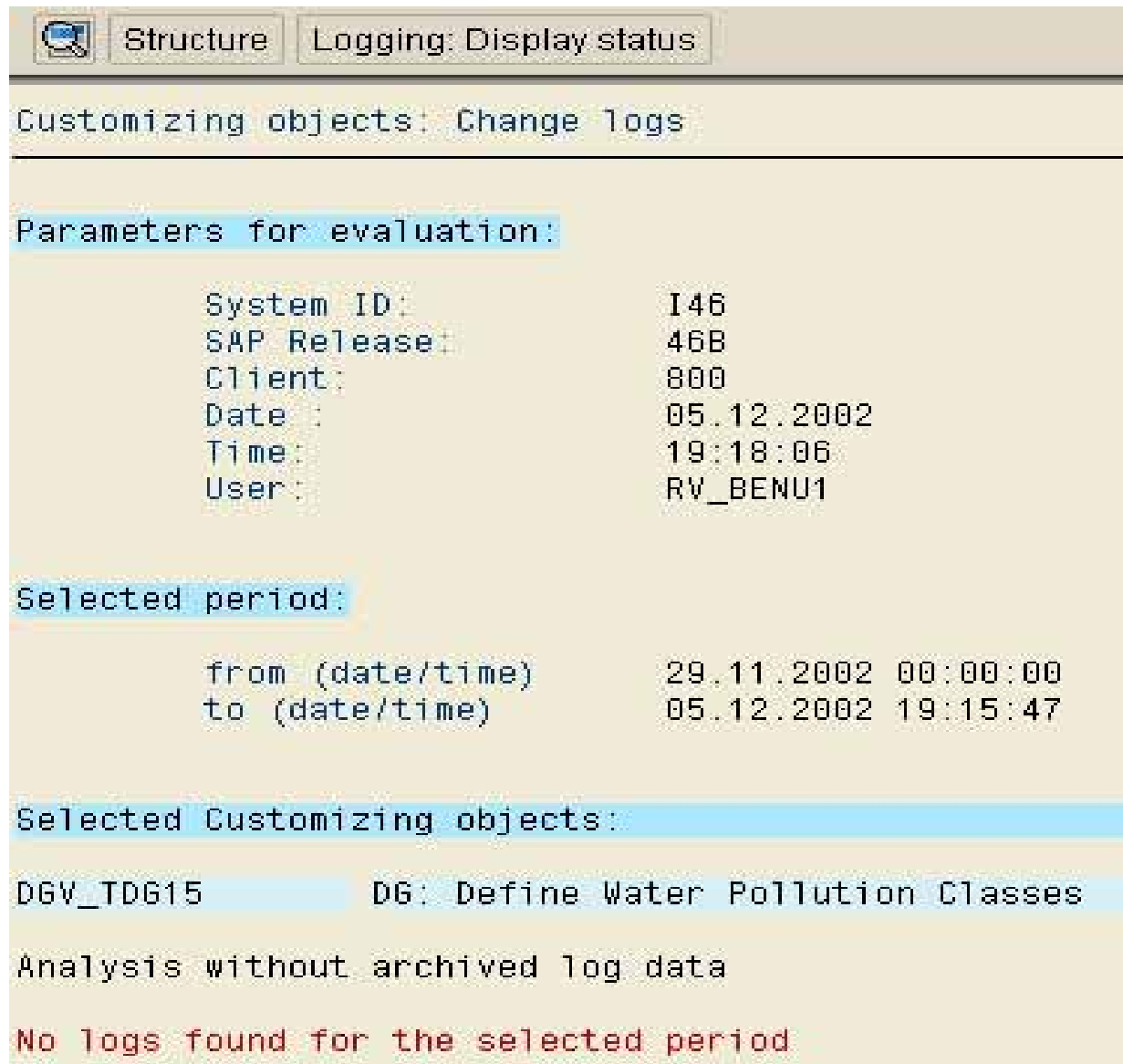


Figure 146: No change documents if the log switch has not been activated

If the general or table specific switch has not been activated, this is the output to be expected.

### 5.3.6 Summary on in-house developments

Auditing in-house developments in an SAP<sup>TM</sup> environment gives an accurate impression on the proficiency of the system operations and of the importance put on compliance, transparency and comprehensiveness. If the SAP<sup>TM</sup> system shows major weaknesses in this area, it will take quite some time to put them right.

### 5.3.7 Tools for auditing in-house developments

Purpose	Transaction/function	Table	Program
Transaction overview	SE16 and	TSTC	
Blocked transactions	AIS + blocked transactions SA38 and		RSAUDITC
Transactions with protective authorization objects	SE93		
Report overview	SA38 (selection screen) and		Z*, Y*
Detailed analysis of reports	SE38 Documentation Attributes Source code SE16 and	TRDIR	
“Authority-check” in reports	SE38 Source code AIS + Statistical program analysis		
Report authorization groups	SE16 and AIS + display authorization groups	TRDIR	
Table overview	SE84		
Detailed analysis on tables	AIS + table recordings SE11 Attributes Fields Technical settings Where-used list		
Log parameter rec/client	SA38 and AIS + table recordings		RSPARAM
Tables and authorization groups	AIS + table recordings SE16 and	TBRG TDDAT	
Table logs	AIS + table recordings SE11 Technical settings SE16 and	DD09L	
Table changes	AIS + table recordings SA38 and		RSTBPROT RSTBHIST

### Exercises on in-house developments

- 1 Create an overview of in-house developed transactions, which are linked to in-house developed programs

---

---

---

---

- 2 Which in-house developed transactions are blocked?

---

---

---

---

- 3 How many transactions are assigned to the financial accounting?

---

---

---

---

- 4 Are there transactions with deleting functions?

---

---

---

---

- 5 Which authorization object is connected to the transaction SM30?

---

---

---

---

- 6 Download a list of in-house developed programs in an Excel spreadsheet.

---

---

---

---

7 How many in-house developed programs are there in your system?

---

---

---

8 Which authorization object is connected to the SAP<sup>TM</sup> standard program RFKORB00?

---

---

---

9 Are user IDs of special users or of user groups used for developing in-house programs?

---

---

---

10 Are these programs directly executable?

---

---

---

11 Which authorization groups have these programs been assigned to?

---

---

---

12 Which programs were created in 2001?

---

---

---

13 Are there in-house developed tables for test purposes?

---

---

---

14 Which program (where-used list) have these tables been assigned to?

---

---

---

15 How many in-house developed tables in the system have insufficient descriptions?

---

---

---

16 Are there in-house developed tables, without assigned authorization groups?

---

---

---

17 Which in-house developed tables are not logged, as the log switch has not been activated?

---

---

---

18 Has the general log switch been activated?

---

---

---

- 19 Which fields does table T001 have, who created the table and are data changes recorded?

---

---

---

---

- 20 Which delivery class has this table been assigned to?

---

---

---

---

- 21 Which authorization groups have been created for tables in the system, and which authorization group has table T001L been assigned to?

---

---

---

---

- 22 Which report gives an overview of table changes and under which condition?

---

---

---

---



### **Checklist for system audits (in-house developments)**

#### **❑ In-house developed transactions**

- Overview
- Sufficient description
- Test procedures
- Blocked transactions

#### **❑ In-house developed programs**

- Policies and procedures on developments, documentation and tests
- Overview
- Sufficient titles
- Test and deleting procedures
- Other critical programs
- SAP<sup>TM</sup> help (documentation)
- Inline documentation
- Coded authorization checks
- Acceptable parameters
  - No special users
  - No group names
- Changes of SAP<sup>TM</sup> standard programs

#### **❑ In-house developed tables**

- Policies and procedures on developments, documentation and tests
- Overview
- Sufficient text
- Test procedures
- Log parameter rec/client
- Tables without log
- Assigned authorization groups
- Where-used list
- Critical data changes

## 5.4 Data flow and reconciliation procedures in the SAP™ financial accounting environment

### 5.4.1 Introduction

The auditor needs to have basic knowledge of the data processing and the data flow in order to determine audit relevant factors and the required reconciliation procedures within the SAP™ supported financial accounting. Only when the auditor acquires transparency of the route of a posting, from the user screen via different interfaces to the database tables, he can ask the proper questions on system security and reconciliation procedures and check appropriate settings.

### 5.4.2 The user dialog with the SAP™ system

The data input by users, e.g. a posting transaction, is usually made online via a linked *work station* or – in sub systems – via the standardized *batch input interfaces*, which is comparable to an automated dialog oriented data input. There are additional ways of filling the accounting relevant database tables, but these will not be discussed at this point.

In a dialog oriented *posting transaction*, the document is structured in two stages. In the first stage, general information is input in the *document header*, in particular document type and posting key (controlling elements). Depending on the posting key and chosen document type, the system will automatically input further items to the document header, such as posting date and document number. The system provides the required input fields for the *items in this document type*, such as amount, account number etc. The document items vary depending on document type and posting key.

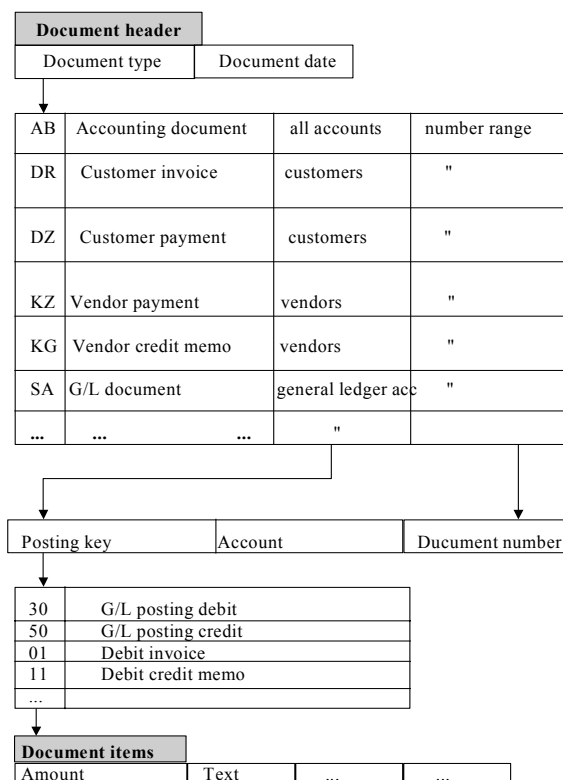


Figure 147: Controlling elements at document entry

During and after the input of document relevant information, a sequence of plausibility checks is performed

- Is *all* required document information entered?
- Are all entries in the input fields in the *proper* format?
- Has all *tax relevant information* been considered?
- Does the *debit* entry *equal* the *credit* entry?
- Does the user have the proper *authorizations* for posting the transactions, including all data and amounts?
- ...

in order to avoid erroneous or incomplete postings in the SAP™ system.

The input posting is reflected in a so called “log record” and a internal SAP™ document number is created. This checked and consistent posting record will be accepted in the database system.

For the technical forwarding of the log record in the system, SAP™ is utilizing the so called “*asynchronous update*” via *two separate interfaces* for performance reasons, which will be discussed in detail.

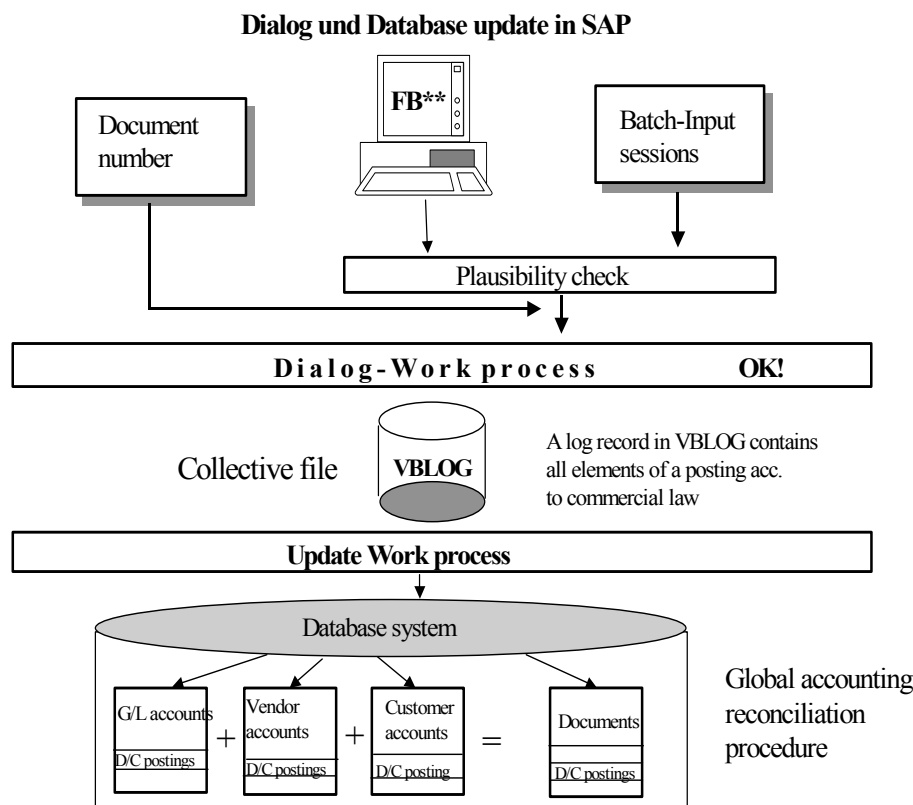


Figure 148: Asynchronous update

The user is communicating with the SAP™ system via the *dialog interface*. The interface is performing the plausibility checks, assigns the internal document numbers and generates the log record. *The system confirms the acceptance of the posting – at this point - to the user and the dialog ends.*

In a second step, the *log record* is marked with the update indicator “not updated” and is *parked* in a *collective file* called “VBLOG” (update log) via the dialog interface. At the same time, the separately working update interface is automatically notified about the posting record parked in the VBLOG. Since multiple users are posting business transactions simultaneously in the system and the users are competing about system processing, it has to be ensured, that the data remains consistent and the transactions are processed in a defined timely sequence. *Simultaneous changes of one and the same data object (account / table) by different users have to be avoided*. During the processing of one specific business transaction, the posting relevant *objects have to be locked for other users*. For this problem, which occurs in every database, SAP™ is utilizing its own *locking concept*, which enters the posting relevant objects into a separate *lock table*.

The update interface picks the log records from the VBLOG in the same sequence they were entered, and forward them to the relevant tables (accounts and documents) within the database system.

Only when the *database update has been performed successfully*, the system categorizes *the document as actually posted*, and it is deleted in the VBLOG. At the same time, the lock key is reset.

The technical process is displayed in detail below:

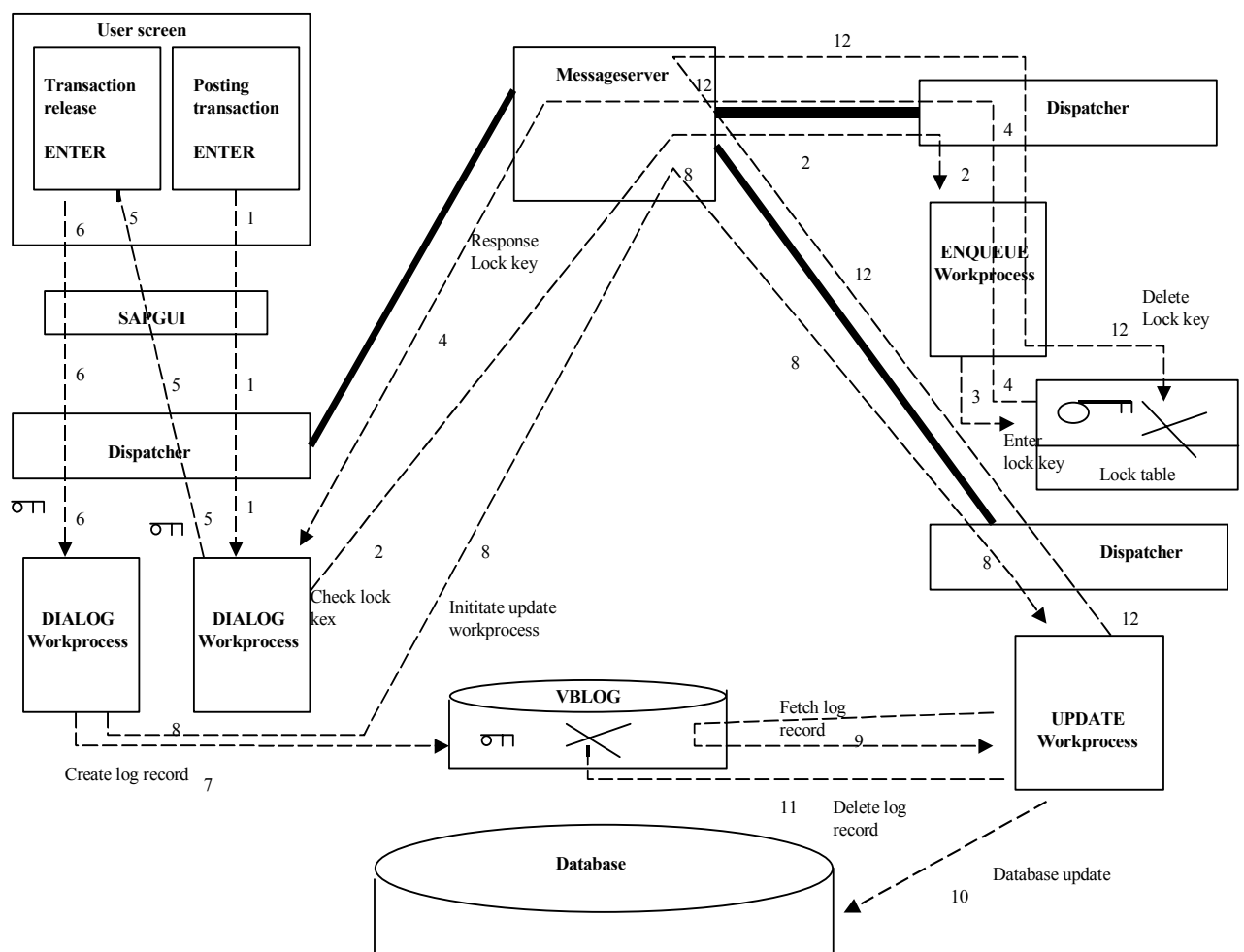


Figure 149: Posting a business transaction in the SAP™ system

The routes in the figure show the following processes:

- 1     *Entering a transaction (ENTER)*  
Forwarding the transaction via SAP-GUI and a dispatcher to a free dialog work process
- 2     Contacting an enqueue server via a message server, its dispatcher and a *free enqueue work process*
- 3     Checking the lock table and – if possible – *entering a lock key* for the current transaction
- 4     *Return of the lock key* to a free dialog work process via the message server and a dispatcher
- 5     *Forwarding the lock key* to the user via SAP-GUI
- 6     User is *confirming* the released *transaction* (ENTER), this information is sent to a free dialog work process via SAP-GUI and a dispatcher
- 7     *Creating a log record* and parking the log record in the VBLOG
- 8     The dialog work process forwards the lock key to the specialized *update work process*, via dispatcher and message server
- 9     The *update work process* uses the lock key for identifying the *log record* in the VBLOG
- 10    The update work process *updates the database*
- 11    After the database update, the update work process triggers the *deletion of the log record* in the VBLOG
- 12    After completed deletion in the VBLOG, the update work process forwards the lock key to an enqueue server via dispatcher and message server, where it is forwarded to a free enqueue work process, which deletes the *entry in the lock table*. Now the next user can work with the relevant data.

In the displayed process, there are quite a few risk sources, such as

- Update termination caused by system or database failures
- Erroneous lock handling
- Erroneous reconciliation procedures

which possibly affect the proper processing of postings. This will be discussed in detail.

### 5.4.3 Update termination and its consequences

#### 5.4.3.1 System reaction

During a timely staggered (asynchronous) update transaction, hardware or software failures, such as buffer overflow or line interference, may cause errors, resulting in anything from rejected postings and ranging to data inconsistencies.

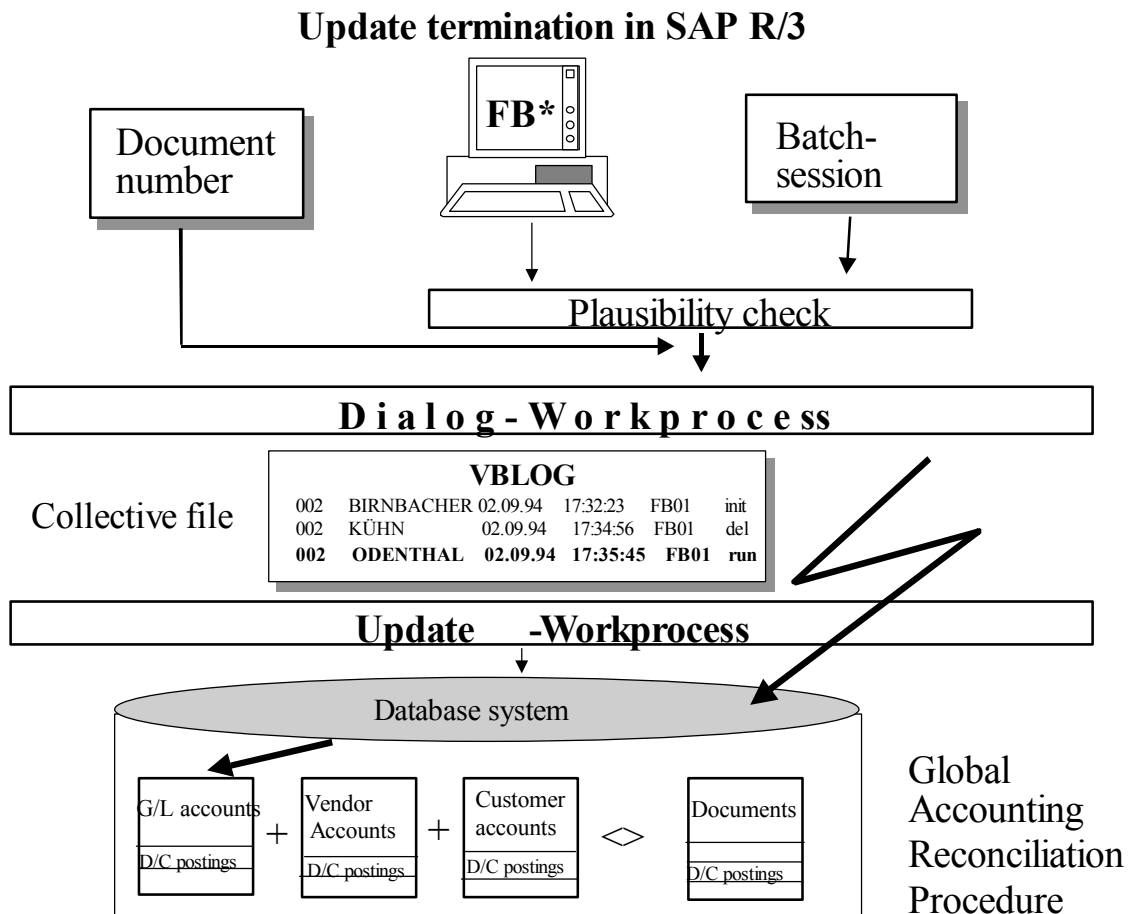


Figure 150: Update termination in the SAP R/3™ system

If *disruptions occur* - for whatever reason - during the transfer of the log record to the database via the update interface, this will result in data inconsistencies followed by e.g. missing recordings on accounts or incomplete document data. SAP™ is reacting with a self-healing process, where the unsuccessful *incomplete database update is cancelled* (rollback). If the rollback is properly executed, the relevant *log records are indicated as erroneous* and are *not deleted in the VBLOG*. In order to enable the further processing of accurate log records in the VBLOG, the *lock keys for the rolled back transactions* are reset. There is an *automated entry in the system log file (SYSLOG)*; an error message appears on the user screen and the user is notified by *express mail* about the unsuccessful update procedure, if the system parameters have been set accordingly.

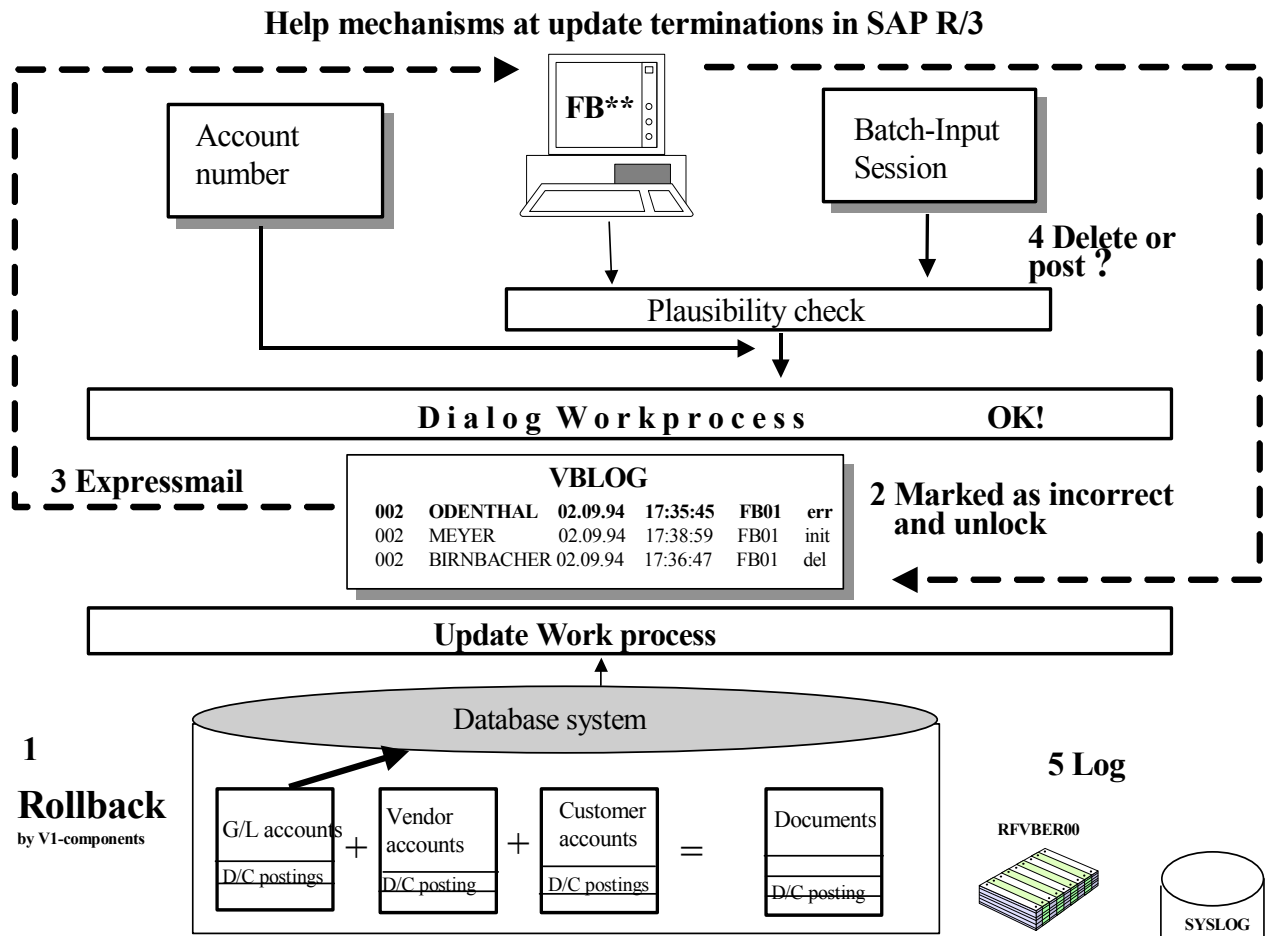


Figure 151: Update termination and the self-healing process

Since the log record has been entered with a document number, but was not accepted by the database system, the SAP™ system offers several possibilities for reacting to the erroneous situation.

#### 5.4.3.2 User reaction

If the user receives the update termination error message on a *timely basis*, and he recognizes it on his screen, he can react with *transaction SM13*:

- Display terminated updates

Analysis of the terminated updates regarding log record details, to determine if a technical failure or the actual log record caused the termination.

- Supplementary update

If the log record was not erroneous and no other user changed the relevant object (e.g. account) in the meantime (the lock key has been reset), the update transaction will be started again.



- Delete

In cases where a supplementary update is not possible, since the log record is erroneous or another user changed the relevant data in the meantime, the log record has to be deleted and re-entered.

Figure 152 Overview and analysis of update records

The presented options should be supported by organizational measures, since they have different consequences:

☐ Option: Supplementary update

*A supplementary update on a timely basis is to be recommended wherever possible, as the posting will be recorded in the system transaction data with its original document number.*

☐ Option: Delete

The plain deletion of the posting decreases the processing transparency and creates a gap in the internal document number sequence, which is not complete any more. Such gaps may have different reasons, (preliminary postings, document number buffering, data manipulation) which will be difficult for the auditor to determine without adequate organizational measures.

#### 5.4.3.3 Recommended actions in cases of update termination

*The user should be familiarized with the topic in a written guideline, which instructs the user to update any rollbacks supplementary on a timely basis. If the database update was enabled by the lock key reset and the database was actually updated in the meantime, the data integrity may be endangered and the supplementary update will be rejected. The user then must call the menu*

Tools

Administration

Monitor

Update

(transaction SM13), which displays the log record on the screen. This so called “skip log” can be printed. In the menu

Goto

Update header or RF documents (in FI)

additional analysis relevant information can be displayed and printed.

The data in terminated business transactions can be re-entered and posted based on this information. After posting this substitute document, the invalid rollback log record has to be deleted.

A written guideline does not ensure that all users react as intended. At the end of every day, the report “RFVBER00” should be run automatically by the administrators. All erroneous log records remaining in the VBLOG will be printed in this report. *This report* should be handed to the relevant user, to be used as a *substitute document*. The report documents the erroneous posting, which now can be deleted.

The described procedure documents the complete sequence within the financial accounting, as required by commercial and tax laws, and *has to be archived* accordingly.

The described SAP<sup>TM</sup> mechanism may result in *gaps in the sequence of automatically assigned internal document numbers*, which can be analyzed with the SAP<sup>TM</sup> standard program “RFBNUM00”. The program should include financial accounting documents and be run on a *regular basis*, e.g. for the *monthly closing*, and the logs should be kept. On a sample basis, the auditor can determine if the described procedures are being followed by the users and assess if comprehensiveness is ensured.

IDES AG		Gaps in Document Number Assignment		Date	04.12.2002
Frankfurt				Page	1
Number range 01 of 1994 to year 1999					
Interval of		0100000000	To	0199999999	Number 0100013157
Fehlende Belegnummern		Mehrfach vergebene Belegnummern			
100000041 ... 100000044					
100000285 ... 100000287					
100000295 ... 100000296					
100000307 ... 100000309					

Figure 153: Log of missing documents for vendor payments

Data inconsistencies should rarely occur, considering the various control mechanisms in an SAP R/3<sup>TM</sup> system. Nevertheless, the *accounting relevant data should be reconciled on a regular basis*, e.g. for the *monthly closing*. In a *global accounting reconciliation procedure* (transaction F.03) the debit and credit business volumes on the accounts are compared and agreed to the corresponding document data. The created *log should be reviewed by the accounting department* and be kept with other *accounting documentation*. If differences are noted in the accounting reconciliation, the reaction has to be comprehensible and on a timely basis.

During the SAP™ system audit, the auditor can review the regular reconciling procedures and their status in the AIS™ system, calling the menu

Business audit

Financial statement oriented audit

Closing (FI-GL)

Reconciliation

Accounting reconciliation (automatic)

Comparative analysis -> historical display

(transaction SA38 and report SAPF190). In the displayed log

Totals		Accounts	
11.11.1999	15:02:47	OLBERT	OK
25.05.1999	08:56:11	SCHUNTER	Errors
19.05.1999	12:35:09	SCHUNTER	OK
28.12.1998	13:37:11	SCHUNTER	OK

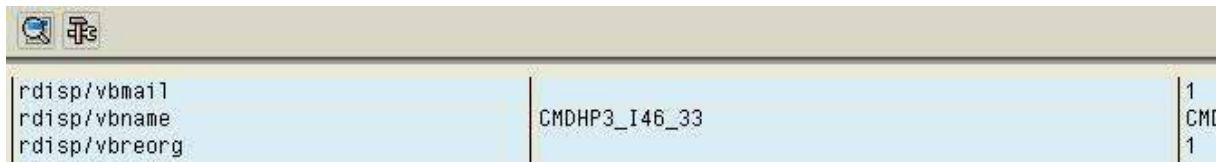
Figure 154: Log of reconciling procedures and their status

the completed reconciliation and the status are shown. Erroneous reconciling procedures and their consequences can be analyzed in detail, clicking the buttons Totals Accounts.

Display Totals			
Documents/transaction figures			
CoCd Year Periods			
AT Curr.	Debit items	Debit master	Credit
0001 1999 01 - 16			
S DEM	0,00	0,00	
1000 1999 01 - 16			
D DEM	51.514.735,69	51.514.735,69	57.840,4
K DEM	56.852.149,81	56.852.149,81	56.316,2
S DEM	1.380.183.469,00	1.379.488.410,92	1.380.183,4

Figure 155: Erroneous accounting reconciliation

As a final audit activity on this topic, the auditor should inquire, if the users are notified about update terminations by express mail, in addition to the error message.



rdisp/vbmail		1
rdisp/vbname	CMDHP3_I46_33	CM
rdisp/vbreorg		1

Figure 156: Parameter settings for ensuring express mail notification to the users

The transmission is controlled by the parameter “rdisp/vbmail”, which has to be set to “1”. The setting can be checked in the report “RSPARAM” in transaction SA38.

#### 5.4.4 Tools for auditing data flow and reconciliation procedures

Purpose	Transaction/function	Table	Program
Accounting reconciliation Current and historical and error analysis	F.03 SA38 and AIS + closing/ reconciliation		SAPF190
Determine update termination	SA38 and AIS + documents/ interrupted updates		RFVBER00
Determine gaps in document number sequence	SA38 and AIS + documents/ document number gaps		RFBNUM00
Check express mail parameter “rdisp/vbmail”	SA38 and		RSPARAM
Documentation of update terminations	Printed and kept SKIP-logs Written guidelines		

### Exercises on reconciliation procedures

- 1 Check if there are terminated log records in the VBLOG at the time of the audit.

---

---

---

---

- 2 Determine, if an accounting reconciliation was completed on a regular basis in the past, and if errors occurred. Analyze any errors.

---

---

---

---

- 3 Check if there are gaps in the sequence of vendor payment documents (document type VP) in the relevant number range (here 15) prior to 1999.

---

---

---

---

- 4 Determine if users are notified about terminated updates by express mail.

---

---

---

---

### **Checklist for system audits (reconciliation procedures)**

- ☐ **Accounting reconciliation**
  - Regular completion with SAPF190
  - Audit of history
  - Consequences of errors
  - Reconciliation by financial accounting
  
- ☐ **Update termination**
  - Regular check with RFVBER00
  - Print of SKIP-logs
  - Archiving
  - Written guidelines
  - System setting for express mail
  
- ☐ **Gaps in document number sequence**
  - Check a sample of critical document types
  - Regular check with RFBNUM00
  - Reconciliation by financial accounting
  - Consequences of gaps and duplicates
  - Archiving of logs

## **5.5 Protecting the SAP™ system from unauthorized access**

### **5.5.1 Introduction to system protection**

The SAP™ system is offering manifold opportunities for manipulating data or initiating unauthorized business processes. IT layers in sub systems, such as the database, the network, and the operating system, are popular targets. This was mentioned in previous sections. Additionally, the system may have poorly secured critical user IDs and improper protective settings may facilitate unauthorized intrusion. In particular the latter aspects should be included in the basic audit of the SAP R/3™ system, and will be discussed in detail.

### **5.5.2 Critical user IDs**

Every SAP™ system contains user IDs, which will facilitate intrusion if they are not sufficiently protected. This applies to the standard “special users” for specific purposes and to user IDs, which are created by the IT administrators.

#### **❑ Special user “SAP\*”**

A critical user in every R/3™ system is the so called initial user “SAP\*”. It is created at system installation and automatically has lower security standards than any other user ID, as it is created in every system and is commonly known. After the initial system installation the password is “06071992” and has same authorizations as a super user. The purpose of “SAP\*” is to provide initial system access to the administrators. SAP™ recommends this to be its sole purpose, after the initial access a new individual administrator ID should be created, and super authorizations should be assigned to this new user. For security reasons the following measures should be taken:

- Change the initial password
- Cancel all authorizations
- Lock the user SAP\* in the system
- Assign the user to the user group “SUPER”

Administrative tasks should not be performed with any user ID, which is not directly linked to one individual natural person. SAP\* can not be deleted in the user master records, since it still can be used for enabling access to the system, being a hard-coded user. The standard password is then “PASS” and the user ID has the super authorizations.

#### **❑ Special user “DDIC”**

The user ID “DDIC” is also created in almost every SAP™ system. It is used for software administrative purposes and has the commonly known password “19920706” and the authorizations of a super user.



In order to avoid related risks, SAP™ recommends to change the password immediately, assign this user also to the user group “SUPER” and assign only a standard authorization profile, specified for the intended purposes, “S\_DDIC\_ALL”.

#### ❑ Special user “SAPCPIC”

SAPCPIC is a dialog user, and any user can log on to the system with this ID. The standard password “ADMIN” is also commonly known, and is used for administrative tasks in the related programs. There is a risk of developers using this user ID. SAP™ recommends to assign a new password to this user too, or to lock the user during inactive periods.

#### ❑ Special user “EARLYWATCH™”

The user ID “EARLYWATCH™” is only used in client 066. It is created in the production system if the company is taking advantage of the “EARLYWATCH™” services provided by SAP™. SAP™ in Walldorf, Germany, is analyzing system settings and performance via a network line. An “EARLYWATCH™” analysis is performed at company request, and the system is connected to SAP™. The SAP™ support staff logs on to client 066 in the production system with the user ID “EARLYWATCH™” and the password “SUPPORT”.

In order to avoid manipulations with this commonly known user ID, SAP™ recommends to change the standard password. This might cause some administrative problems, as SAP staff will expect the standard password. An option is not to change the standard password, but to lock the user ID in the production system and only release it for “EARLYWATCH™” sessions.

Below is an overview of the presented special users and their commonly known standard passwords:

User	Client	Initial password
SAP*	000, 066, 001	06071992, PASS
SAPCPIC	000, 066, 001	Admin
DDIC	000, 001	19920706
EARLYWATCH	066	Support

Figure 157: Special users and initial passwords

The special users can be checked, preferably with functions in the AIS™ system

System audit

User administration

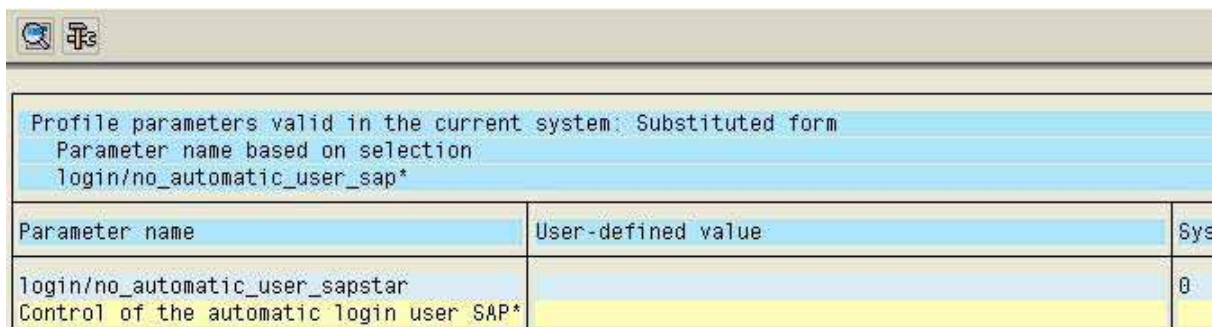
Authentication

Special user

(transaction SA38 and reports RSUSR003 and RSPARAM).

The special status of “SAP\*”, which enables a log on with this user ID even if the master records are deleted, can be inactivated with the system parameter

Login/no\_automatic\_user\_sapstar



Profile parameters valid in the current system: Substituted form  
Parameter name based on selection  
login/no\_automatic\_user\_sap\*

Parameter name	User-defined value	Sys
login/no_automatic_user_sapstar Control of the automatic login user SAP*		0

Figure 158: System settings for the status of the special user SAP\*

The auditor should check this setting.

Critical situations related to the special users and their passwords, and if the special users are locked or not, can be determined in a detailed log with the function “check passwords of special users”.

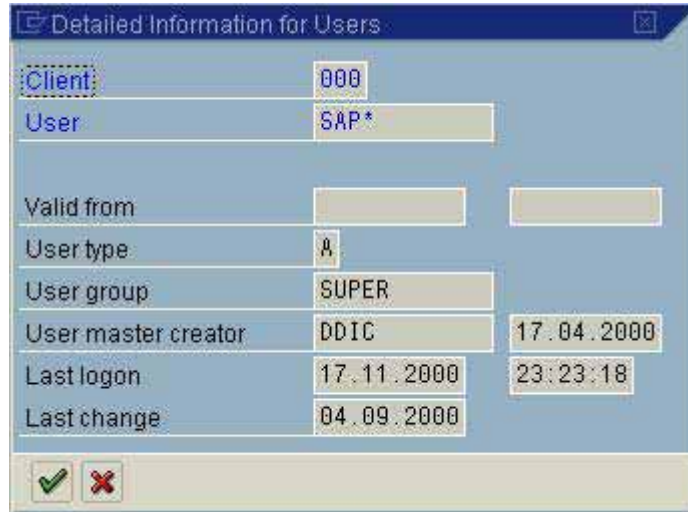
Cl.	User	State
000	SAP*	Exists; Password not trivial. 1 unsuccessful logins
000	DDIC	Exists; Password not trivial.
000	SAPCPIC	Password ADMIN well known. See note 29276
800	SAP*	Exists; Password not trivial. 3 unsuccessful logins
800	DDIC	Exists; Password not trivial.
800	SAPCPIC	Password ADMIN well known. See note 29276

Figure 159: Overview of SAP™ special user security settings

The log is created in the report “RSUSR003”, and shows the status of the special users in different clients. This requires an authorization for cross-client tables, which most auditors do not have, and there is no log output. In this case, the auditor should ask the administrator to print the log, and add it to the work papers.

Critical facts, such as a missing user ID or a commonly known standard password, are highlighted in the displayed log. An open or locked lock next to every user ID shows, if it has been locked according to SAP™ recommendations.

With the binoculars  the auditor can view detailed information of specific created user IDs



Client	000		
User	SAP*		
Valid from			
User type	A		
User group	SUPER		
User master creator	DDIC	17.04.2000	
Last login	17.11.2000	23:23:18	
Last change	04.09.2000		

Figure 160: Additional information on the special users

and see if they were assigned to the user group “SUPER” as recommended by SAP<sup>TM</sup>. This is of importance in order to prevent every authorization administrator from maintaining critical user IDs. For maintaining the user group “SUPER” additional administration authorizations are required. The date of the last login is displayed, which shows if the user ID is being used or not, and the date of the last password change. If intrusion was attempted with any of the presented special IDs, this will be recorded and displayed.

#### ❑ Critical company specific user IDs

In addition to the presented user IDs, user master records created by the company for users, which never logged on to the system bring particular risks. Since the users were not required to change password at an initial login, they usually still have the initial password. Initial passwords tend to be similar for all users and are usually well known, and could be used for attempted intrusions.

This can be audited in the AIS<sup>TM</sup> system, calling the menu

System audit

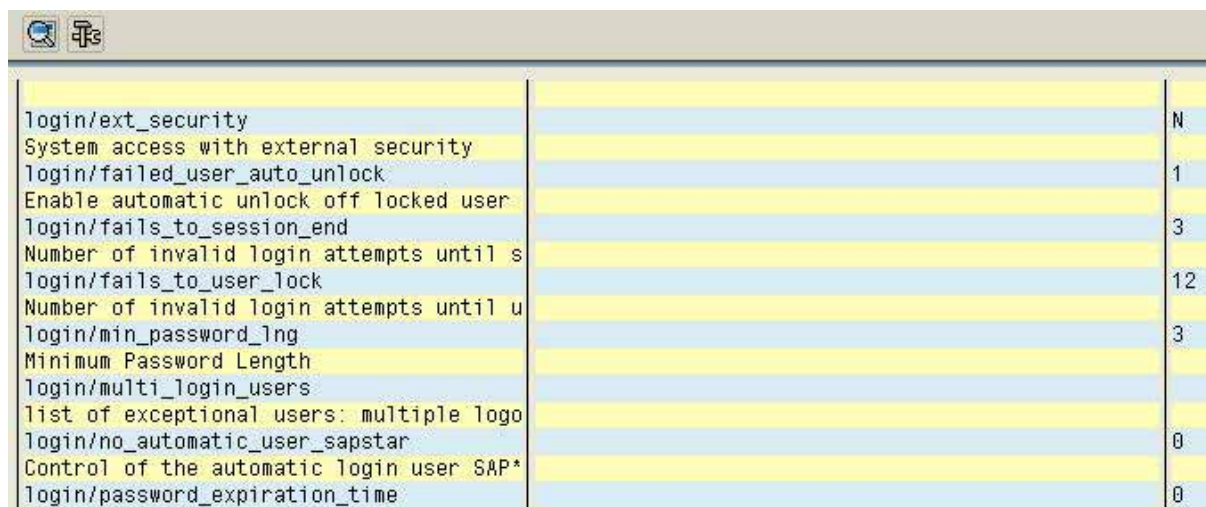
User administration

Overview of users

Users who have not logged in during the last 30 days

(transaction SA38 and report RSUSR200). The option “users with initial password” should be marked in the selection screen.





Parameter	Value
login/ext_security	N
System access with external security	
login/failed_user_auto_unlock	1
Enable automatic unlock off locked user	
login/fails_to_session_end	3
Number of invalid login attempts until s	
login/fails_to_user_lock	12
Number of invalid login attempts until u	
login/min_password_lng	3
Minimum Password Length	
login/multi_login_users	
list of exceptional users: multiple logo	
login/no_automatic_user_sapstar	0
Control of the automatic login user SAP*	
login/password_expiration_time	0

Figure 162: Logon rule parameters



The most important parameters, their function, the SAP™ standard settings and recommended settings are presented below:

System parameter	Function	Recommended security settings
Login/fails_to_session_end	Invalid login attempts	5 attempts
Login/fails_to_user_lock	User lock	7 attempts
Rdisp/gui_auto_logout	Automatic logoff	900 seconds
Login/min_password_lng	Password length	6 characters
Login/password_expiration_time	Password change	40 days

Figure 163: Overview with recommended logon rule parameters

The overview shows, that the security settings in the SAP™ system at installation are absolutely insufficient, and have to be customized in order to provide protection for the production system.



Detailed information about the security parameters can be obtained by marking the parameter and clicking the choose button . To display the parameter documentation, the help button  is clicked in the next window.

Parameter : login/fails\_to\_user\_lock

Short description: Number of invalid login attempts until use

Parameter description :

Number of incorrect logons allowed for a user master record until logon is rejected for this user. An entry is written to the system log.  
The lock is released at midnight.

Work area: Logon

Unit :

Default value: 12

Figure 164: Documentation for SAP™ profile parameters

For additional system security, the most common and simple passwords and combinations of passwords, can be listed as invalid in table “USR40”

Table : USR40  
Displayed fields: 1

<input type="checkbox"/>	Password
<input type="checkbox"/>	FIRMA
<input type="checkbox"/>	TEST

Figure 165: Overview of invalid passwords in table USR40

The auditor can view the company specific invalid passwords in the function “invalid passwords” or by calling table USR40 in transaction SE16.

### 5.5.1 Tools for auditing system security

Purpose	Transaction/function	Table	Program
Overview special user security Password User group Lock	AIS + special user SA38 and		RSUSR003
Deactivating special SAP* special status	AIS + special user/parameters SA38 and		RSPARAM
Overview USER with initial password	AIS + overview of users/users who have not logged in SA38 and SE16 and	USR02	RSUSR200
User parameters Password length Password change Etc	AIS + logon rule parameters SA38 and		RSPARAM
Invalid password	AIS + invalid passwords SA16 and	USR40	



### Exercises on system security

- 1 Determine of the special user ID SAP\* is in the system, has a new password and is locked in the SAP delivery client.

---

---

---

- 2 When was the user ID SAP\* active last time?

---

---

---

- 3 Create documentation on the start-up parameter "rdisp/gui\_auto\_logout". Which settings are possible?

---

---

---

- 4 Does the initial user SAP\* have a special status in your system?

---

---

---

- 5 Which users were never active in the system and still have their initial password?

---

---

---

- 6 Create an overview of the invalid passwords in your system.

---

---

---

### **Checklist for system audits (system security)**

#### ☐ **Securing the special users**

- SAP\*
  - New password
  - Lock
  - No authorizations
  - No special status
  - User group "super"
- DDIC
  - Profile "S\_DDIC\_ALL"
  - New password
  - User group "super"
- SAPCPIC
  - New password or lock
- EARLYWATCH
  - New password or lock

#### ☐ **Critical company specific user IDs**

- Never logged on
- With initial password

#### ☐ **Logon rule parameters "login"**

- No SAP standard parameter
- Settings according to company policy

#### ☐ **Invalid passwords in table USR40**

## **5.6 Auditing the authorization concept**

### **5.6.1 Introduction to the authorization concept**

Companies implementing SAP R/3™ install an extremely complex structured software system. In most cases, companies expect the implementation to contribute to the re-engineering of various business processes. The system supports not only the automatic processing of business transactions, paperless data exchange with other companies as well as the handling of digital documents, but also internet activities, such as – metaphorically speaking – relocating the desks of the sales force to the customers' offices.

This new process oriented view of the SAP-R/3™ system, the complex integration of business processes, business transactions and the essentially automated recording of related data and accounting procedures, has to be reflected in an eligible and sophisticated authorization concept. SAP R/3™ supports such an authorization concept. The configuration and auditing of this concept is very complex though, as various administrators and auditors have experienced.

The basics of the SAP R/3™ authorization concept will be discussed in detail in the first section below. Once the auditor grasps the basics, he can develop his own audit strategy, which suits the specific requirements of his company. In the second section, the (Odenthal) model procedure for auditing the authorization concept is presented, taking both risk and cost-effective aspects of the audit into consideration. In this context, techniques for auditing the authorization concept will be presented. The presented techniques are restricted to the various tools, which are implemented within the SAP R/3™ system for this purpose. Other tools, which are offered by third party suppliers or auditing companies, are not presented in this manual.

### **5.6.2 Methods, elements and tools for configuring the SAP R/3™ authorization concept**

#### **5.6.2.1 Introduction**

Within the SAP R/3™ authorization system there are four major elements

- authorization objects (with protective functions)  
SAP resources and processes to be protected
- authorizations (single profiles, composite profiles, activity groups)  
defined authorizations based on SAP™ protective authorization objects
- transactions and programs  
SAP™ processes and functions requiring authorization checks
- user master records  
users, who can start a function or a program based on their assigned authorizations

which are discussed below.

An efficient authorization audit requires the auditor to deal intensively with the mentioned elements in order to understand their meaning and functions.

### **5.6.2.2    *The authorization object***

#### **5.6.2.2.1   *Authorization object structure***

The authorization object is the basic element of the R/3™ authorization concept. For each business resource accessible via the SAP™ system and each business transaction processed in the system, which the company considers to be of interest and worth protecting, there is an SAP™ standard authorization object, or one can be created by the company. Authorization objects are therefore multifaceted and topic related. Examples are

- Company data
  - document data, master data, data on human resources
- organizational structure
  - clients
  - company codes
  - accounts and group of accounts
  - accounting periods
- tools and processes within the SAP™ system
  - tables
  - transactions
  - programs
- areas of activity in the SAP™ system
  - administrative activities
  - business processes
  - automated work flows
- technical system parts of SAP™
  - flow controls
  - interfaces
  - controlling elements

and more. Everything worth protecting in an SAP™ system usually has an authorization object. Authorization objects are therefore the indispensable precondition for realizing an efficient protection of the SAP™ system. The reverse of this fact is, that business resources without SAP™ authorization objects (standard or in-house developed), can not be protected from unauthorized access.

It is important for the auditor to understand the structure and the function of the authorization objects. Here is an example, based on the administration of vendor master records.

For the SAP™ system to strengthen the internal control system, enabling users to create and change vendor master records only within a predefined company code, the required authorization object has to take the

- activities (create, change, display, delete, etc.) but also
- the company (company code)

into consideration in its structure.

Such an authorization object can be used for coding pre-defined authorizations within programs, which control the changing procedures of vendor master records. It can also be used in the task specific user master record.

The SAP™ authorization objects are structured accordingly. The most important elements are the assigned “authorization fields” which define the characteristics of the authorization object, i.e. what is to be controlled and protected. The authorization area of the authorization object is described by these fields.

Most authorization objects define a possible authorization area in two fields

- activity and
- organizational unit (company code, account, document type, user group, etc.)

even though specific authorization objects may consist of up to ten authorization fields.

Below are three examples:

Object:	access to SAP-transactions	
Authorization field:	transaction code	<input type="text"/>

Figure 166: Simple structure of an SAP R/3™ standard authorization object

Object:	creating master records in company codes	
Authorization field:	activity	<input type="text"/>
	company code	<input type="text"/>

Figure 167: Twofold structured SAP R/3™ standard authorization object

Object:	access to HR applicant data	
Authorization field:	authorization level	<input type="text"/>
	Infotype	<input type="text"/>
	group of persons	<input type="text"/>
	person subgroup	<input type="text"/>
	administrator of HR master data	<input type="text"/>
	subtype	<input type="text"/>
	organizational key	<input type="text"/>
	plant	<input type="text"/>

Figure 168: Complex structured SAP R/3™ authorization object

#### 5.6.2.2.2 SAP R/3™ standard authorization objects versus in-house developments

In order to ensure efficient system security when implementing an SAP R/3™ system, SAP has programmed standard authorization objects for any thinkable protective option. These are automatically loaded in the system at initial installation or release upgrades.

SAP offers options for extensive protection of system elements, based on these standard authorization objects. The protection mechanisms offer multiple options for creating a specifically customized authorization concept for each company. Usually, the in-house developed company specific authorization concept is based on SAP™ standard authorization objects. In-house developed authorization objects are only found in very few implementations, for example in cases where the SAP™ system was enhanced by major in-house developed programs, and the SAP™ standard authorization objects do not offer sufficient protection.

SAP™ differentiates between SAP™ standard authorization objects and in-house developed authorization objects in the pre-defined naming convention. The authorization object name can consist of up to ten characters and is structured as follows:

Character	Contents
1	Description of the work area or the SAP module, e.g.: F – Finance area P – Human resources area A – asset area M – Materials area S - System area
2	underscore
3 - 6	four characters for characterizing the business or work area
7	underscore
8 – 10	three characters for the detailed description of the authorization object contents

Figure 169: SAP™ naming conventions for standard authorization objects

An example hereof:

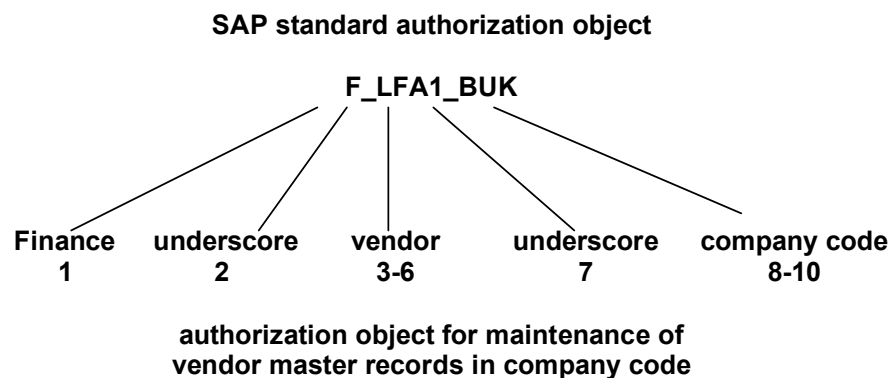


Figure 170: Example of the naming of a standard authorization object

SAP™ recommends, in-house developed authorization objects to start with the letter “Y” or “Z” in order to differentiate them from the delivered standard authorization objects.



### 5.6.2.2.3 *Object classes and authorization objects*

In order to improve the user handling and the structure of the various authorization objects, they are assigned to authorization classes sorted by topic. The auditor can obtain an overview by calling the menu:

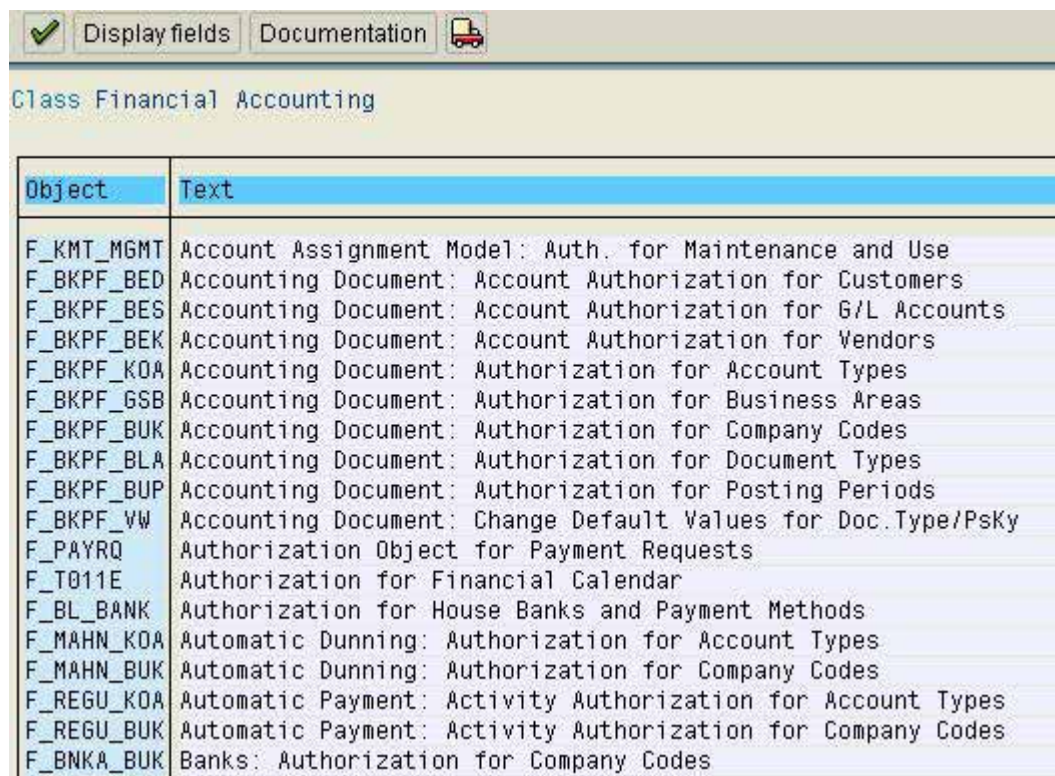
Tools  
Administration  
User maintenance  
Manual maintenance  
Edit authorizations manually

(transaction SU03).

Object Class	
	Not assigned to a class
AM	Asset Accounting
BC_Z	Basis - Central Functions
BC_C	Basis - Development Environment
BC_A	Basis: Administration
CLAS	Classification System
COND	Conditions
CO	Controlling
AAAB	Cross-application Authorization Objects
CV	Document management
ECCS	EC-CS: Consolidation
FI	Financial Accounting


Figure 171: Object classes in the SAP R/3™ system

The single authorization objects in the object classes, which are sorted by topic, can be displayed by double clicking the object class.



Object	Text
F_KMT_MGMT	Account Assignment Model: Auth. for Maintenance and Use
F_BKPF_BED	Accounting Document: Account Authorization for Customers
F_BKPF_BES	Accounting Document: Account Authorization for G/L Accounts
F_BKPF_BEK	Accounting Document: Account Authorization for Vendors
F_BKPF_KOA	Accounting Document: Authorization for Account Types
F_BKPF_GSB	Accounting Document: Authorization for Business Areas
F_BKPF_BUK	Accounting Document: Authorization for Company Codes
F_BKPF_BLA	Accounting Document: Authorization for Document Types
F_BKPF_BUP	Accounting Document: Authorization for Posting Periods
F_BKPF_VW	Accounting Document: Change Default Values for Doc.Type/PsKy
F_PAYRQ	Authorization Object for Payment Requests
F_T011E	Authorization for Financial Calendar
F_BL_BANK	Authorization for House Banks and Payment Methods
F_MAHN_KOA	Automatic Dunning: Authorization for Account Types
F_MAHN_BUK	Automatic Dunning: Authorization for Company Codes
F_REGU_KOA	Automatic Payment: Activity Authorization for Account Types
F_REGU_BUK	Automatic Payment: Activity Authorization for Company Codes
F_BNKA_BUK	Banks: Authorization for Company Codes

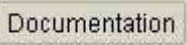
Figure 172: Authorization objects in the object class Finance

At this point, the auditor can obtain more information about the fields assigned to the authorization object and its structure by marking the object and using the button “display fields” .



Authorization Object: Fields
Account Assignment Model: Auth. for Maintenance and Use
Authorization group
Activity

Figure 173: Structure of the authorization object F\_LFA1\_BUK

Additional information about the functions of an authorization object, if the check is compulsory or optional, which system related or organizational preconditions are required for the check and which entries are possible, can be obtained by clicking the button “documentation”  after marking the authorization object.

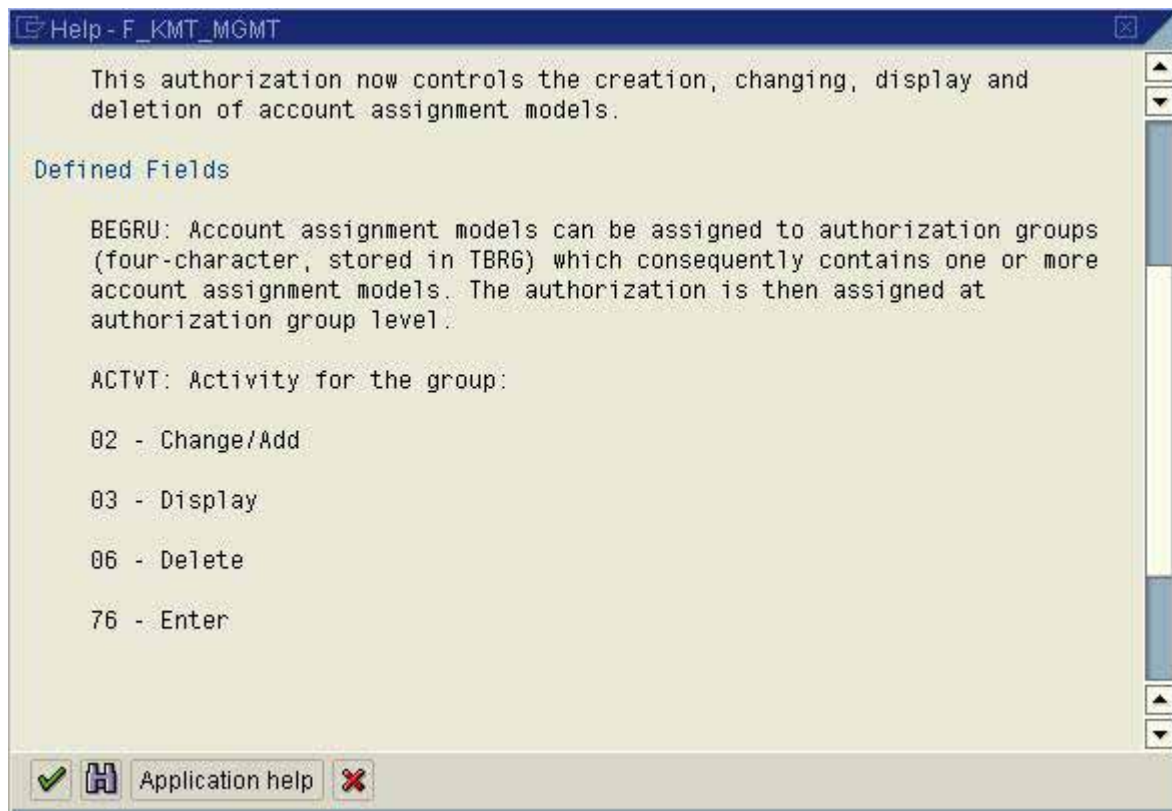


Figure 174: Documentation to the authorization object F\_LFA1\_BUK

The documentation to the authorization object can be printed by clicking the right mouse button.

#### 5.6.2.2.4 *Preconditions for utilizing SAP™ authorization objects*

Authorization objects only enable the customizing of an efficient and sophisticated authorization system in the first step. If the resulting optional protection is actually utilized in the system to be audited largely depends on two preconditions:

##### ❑ **Organizational configuring of authorization elements**

Several authorization objects refer to organizational configuration options, which have to be customized in such a way, that the authorization objects are included in the authorization check. As an example, protecting critical accounting tables from unauthorized access is depending on the assignment to privileged protection categories during the customizing process. To restrict the access to specific accounts, the accounts have to be assigned to certain groups of accounts. The same applies to many other configuration options. For SAP™ implementations without comparable specific organizational characteristics, protection by authorization objects is not ensured. The auditor therefore has to know the authorization objects and their characteristics very well.

##### ❑ **Specific deactivation of authorization objects**

The SAP™ system enables the administrators to deactivate specific authorization objects on a transaction basis or globally. In these cases, there is no protection. Technical and audit aspects of such a deactivation will be described later.

#### 5.6.2.2.5 *Calling authorization objects in SAP™ programs*

The authorization check for specific authorization objects is done within SAP™ programs, which are activated after an SAP™ function (transaction) is called. The coded command is "AUTHORITY-CHECK", followed by the name of the authorization object and the required authorization values in specific authorization fields for running the program.

```

AUTHORITY-CHECK OBJECT 'F_BKPF_BUK'
  ID 'ACTVT' FIELD '03'
  ID 'BUKRS' FIELD BKPF-BUKRS.
AUTHORITY-CHECK OBJECT 'F_BKPF_BLA'
  ID 'ACTVT' FIELD '03'
  ID 'BRGRU' FIELD T003-BRGRU.
  
```

Figure 175: Authorization check for an SAP™ authorization object within an SAP™ program

It was already mentioned, that in-house developed programs rarely are coded with sufficient authorization checks.

The connections between complex SAP™ work processes and the related authorization objects are important for the understanding and audit of protective mechanisms.

The posting of, for example, an accounting document is bound to involve several authorization objects. A document is created, containing following elements:

<b>Document</b>	→	account type
		and
	→	document type
		and
	→	accounting period
		and
	→	company code

Each element is protected by authorization objects within defined authorization areas. Each of the defined authorization areas for these authorization objects has to be passed successfully (AND connection) in order to enable the user to change the document. If the user is not sufficiently authorized for only one of the required authorization objects, the transaction will be rejected by the system.

### **5.6.2.3 Authorizations, profiles and activity groups**

#### **5.6.2.3.1 Single authorizations and profiles**

While the authorization objects – just like locks – are put in front of SAP elements to be protected, authorizations can be compared to the keys, which enable the access and the efficient work with these elements.

A single authorization to a specific authorization object always contains defined entries in the specific authorization fields.

Entry options for the authorization fields in an authorization object can be shown in the related documentation (see figure 169),

Basic recurring entries in the field “Activity” are:

01	=	create
02	=	change
03	=	display
06	=	delete
08	=	display change documents

A complete overview can be obtained by calling these tables in transaction SE16:

- TACT activities which can be protected
- TACTZ valid activities for each authorization object



	Activity	Text
<input type="checkbox"/>	01	Create or generate
<input type="checkbox"/>	02	Change
<input type="checkbox"/>	03	Display
<input type="checkbox"/>	04	Print, edit messages
<input type="checkbox"/>	05	Lock
<input type="checkbox"/>	06	Delete
<input type="checkbox"/>	07	Activate, generate
<input type="checkbox"/>	08	Display change documents
<input type="checkbox"/>	09	Display prices
<input type="checkbox"/>	10	Post
<input type="checkbox"/>	11	Change number range status
<input type="checkbox"/>	12	Maint. and gen. change document
<input type="checkbox"/>	13	Initialize number levels
<input type="checkbox"/>	14	Field select.: Generate screen
<input type="checkbox"/>	15	Field select.: Assign table
<input type="checkbox"/>	16	Execute
<input type="checkbox"/>	17	Maintain number range object
<input type="checkbox"/>	18	Deliveries from coll. proc.
<input type="checkbox"/>	19	Invoices from coll. proc.
<input type="checkbox"/>	20	Transport without translation
<input type="checkbox"/>	21	Transport

	Object	Activity
<input type="checkbox"/>	A_B_ANLKL	01
<input type="checkbox"/>	A_B_ANLKL	02
<input type="checkbox"/>	A_B_ANLKL	03
<input type="checkbox"/>	A_B_ANLKL	77
<input type="checkbox"/>	A_C_AFAPL	01
<input type="checkbox"/>	A_C_AFAPL	02
<input type="checkbox"/>	A_C_AFAPL	03
<input type="checkbox"/>	A_C_AFAPL	05
<input type="checkbox"/>	A_C_AFAPL	06
<input type="checkbox"/>	A_M_ANLKL	01
<input type="checkbox"/>	A_M_ANLKL	02
<input type="checkbox"/>	A_M_ANLKL	03
<input type="checkbox"/>	A_M_ANLKL	05
<input type="checkbox"/>	A_M_ANLKL	06
<input type="checkbox"/>	A_S_ANLGR	01
<input type="checkbox"/>	A_S_ANLGR	02
<input type="checkbox"/>	A_S_ANLGR	03
<input type="checkbox"/>	A_S_ANLGR	05
<input type="checkbox"/>	A_S_ANLGR	06
<input type="checkbox"/>	A_S_ANLKL	01
<input type="checkbox"/>	A_S_ANLKL	02

Figure 176: Content of the tables TACT and TACTZ

After having explained that every activity, like for example posting a document, involves several authorization objects, it should be obvious that it would be impossible to assign single authorizations to every user which cover the complete scope of the different work processes. The required administrative work load would have a negative cost-benefit effect. The user administration is working on a higher aggregated level, like for example

- Authorizations for all accounts receivable postings in company code 10
- Authorizations for all accounts receivable postings in company code 20
- Authorizations for all postings to accounts payable and accounts receivable
- Authorizations for changing customer master records etc.

created as “profiles”. The chosen level of aggregation, beginning with simple work processes to the reflection of complete work places, has to be defined individually by each company. Definition criteria may be the option to reuse the profiles (work processes) for different administrators, the amount of organizational units, which have to be reflected in the work processes, the amount of user administrators, the complexity of the company or the amount of user master records. There are no fixed rules. The important thing is to keep the administrative effort of creating authorization profiles and assigning the profiles to the users in a positive cost-benefit relation to the requirements of safety and segregation of duties.

The higher aggregated level of single profiles are the so called composite profiles, which usually reflect more complex work processes or complete work places. Composite profiles again can be aggregated to the next level of composite profiles.

While authorizations, single profiles and composite profiles were created with programming techniques in the past, it is now possible to create them by utilizing the “profile generator”, a new tool where authorizations are created with menu support. There are also new terms and definitions.

More complex work processes, with defined authorizations are called “activity groups”. In addition to single activity groups there are also composite activity groups. Based on the activity groups, profiles are created and assigned to user master records.

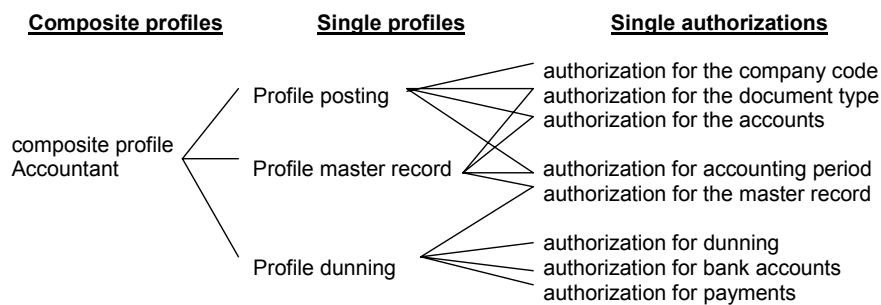


Figure 177: Example of aggregated single authorizations to a composite profile

#### 5.6.2.3.2 Standard authorization profiles versus in-house developments

Just as authorization objects are delivered when installing a new SAPTM R/3™ system, standard authorization profiles are too. These are provided for administrative tasks and users like

- system administrator
- operator
- developer

as well as for staff in the business departments

- accounts receivable clerk
- financial coordinator
- warehouse staff
- buyer
- sales staff



The delivered standard authorization objects, especially the ones for the business department staff, primarily serve the purpose of a template and have to be customized in order to meet company specific requirements. An SAP™ standard authorization profile for a business area will never meet the specified data protection and access security requirements of a particular company. From an auditor's point of view the authorization "standard version" will always be too wide-ranging. For this reason, it is absolutely necessary to reflect the company specific organizational regulations and powers in a written authorization concept, in order to create in-house developed authorization profiles and activity groups based on this document. It is necessary to strictly adhere to the SAP™ naming conventions, in order to meet the requirements for integrity and transparency. SAP™ standard names should never be used for in-house developed authorization profiles. SAP™ reserves the first underscore in the profile name for its standard profiles only.

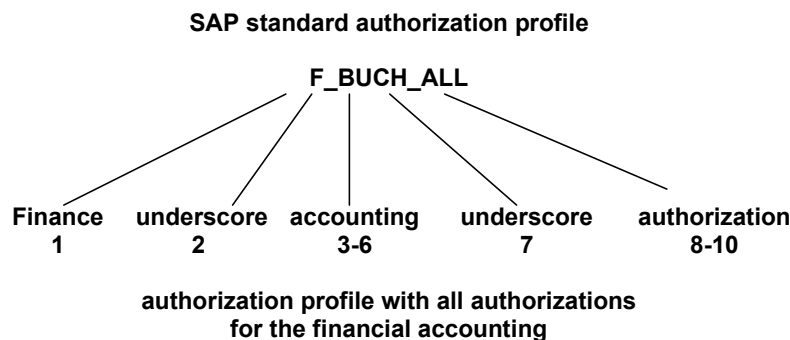


Figure 178: Name of an SAP™ standard profile according to the SAP™ naming convention

SAP™ recommends in-house developed authorization profiles to have another defined character, for example a colon, as a first separator in their names, and not an underscore, which is used in the standard authorization profiles.

In the menu

Tools

Administration

User maintenance

Information system

Profiles

List profiles by complex selection criteria

By profile name, -text

(SA38 and report "RSUSR020") an overview can be created, showing single and composite profiles in a system with related descriptions.

Prof.name	Text	Type
F_ANLAGEN	FI authorizations for an Assets Management accountant	Sgle profile
F_ANZ	FI Display Authorization Model Profile	Sgle profile
F_BANK	FI Additional authorizations for a bank accountant	Sgle profile
F_BANK_ALL	Sample additional profile for a bank accountant	Comp.profile
F_BKPF_KAEN	FI authorizations for changing vendor documents	Sgle profile
F_BKPF_KANZ	FI authorizations for displaying vendor documents	Sgle profile
F_BUCHHAL...	Sample profile for an accountant	Comp.profile
F_BUCH_ALL	FI: Financial Accounting - all maintenance authorizations	Comp.profile
F_DARL_ALL	Darwin: All authorizations for loan administration	Sgle profile
F_DEBITOREN	FI authorizations for an Accounts Receivable accountant	Sgle profile
F_DEBI_ALL	Model profile for an Accounts Receivable accountant	Comp.profile

Figure 179: Overview of SAP™ standard profiles

If the auditor is interested in the structure and authorization contents of a profile, he can double click on the item to “drill down” to the valid authorization values of each authorization fields, via single profiles, authorization objects and authorization fields.

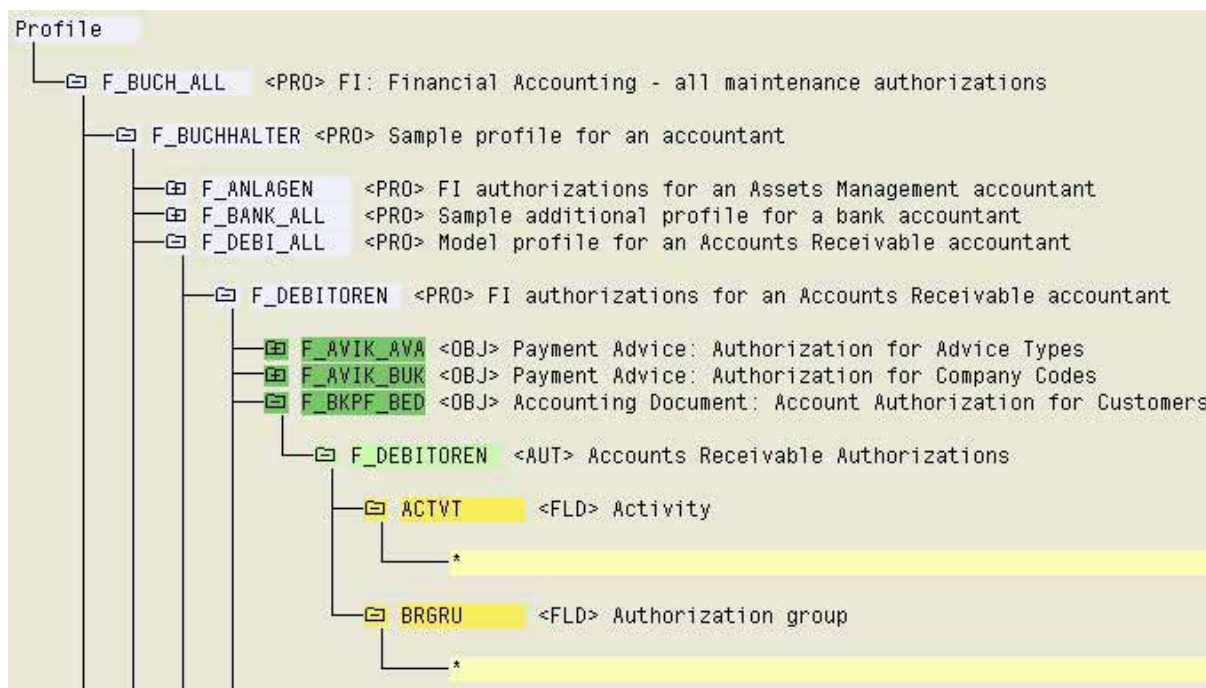


Figure 180: Analysis of an SAP™ standard authorization profile

The figure above shows the extensive authorization range of an SAP™ standard profile for an accountant.

Note that automatically generated profiles, derived from the activity groups when utilizing the profile generator, are usually saved with a technical name like “T-105736”.

With the menu

Tools

Administration

Information system

Profiles

List profiles by complex selection criteria

List profiles by complex selection criteria

and the selection limited to “generated profiles” in the next screen

Prof.name	Text	Type
T-00000001	Profile for activity group Z_SAP_ESSUSER	Generated
T-00000004	Activity group Z_IDES_ESS profile	Generated
T-000000041	Activity group Z_IDES_ESS profile	Generated
T-000000042	Activity group Z_IDES_ESS profile	Generated
T-000000043	Activity group Z_IDES_ESS profile	Generated
T-000000044	Activity group Z_IDES_ESS profile	Generated
T-79000005	Activity group MS_3020 profile	Generated
T-B2B_EMPL	Activity group IDES_B2B_EMPLOYEE.COM profile	Generated
T-DI550019	Profile for Activity Group IDES_EMPLOYEE_SELF_SERVICE	Generated
T-DI550039	Activity group IDES_BUYER profile	Generated
T-I3030002		Generated

Figure 181: Generated profiles

will convince the auditor.

Using such technical profile names is not obligatory. However, it is often done for simplicity reasons but with negative effects for the audit. If such technical profile names are assigned to user master records, additional effort is required in order to do a visual check of the assigned range of authorizations. It is possible to get from the technical profile name to the descriptive name of the activity group in several steps, but the auditor will always recommend to use “descriptive” profile names, even if the profile generator is being utilized.

#### 5.6.2.4 The SAP user and the assigned authorizations

Another element of an SAP™ authorization concept is the user master record, which is assigned to the user. By assigning profiles and composite profiles to a created user master record, the user obtains the authorizations required for his work. The following graph should clarify that:

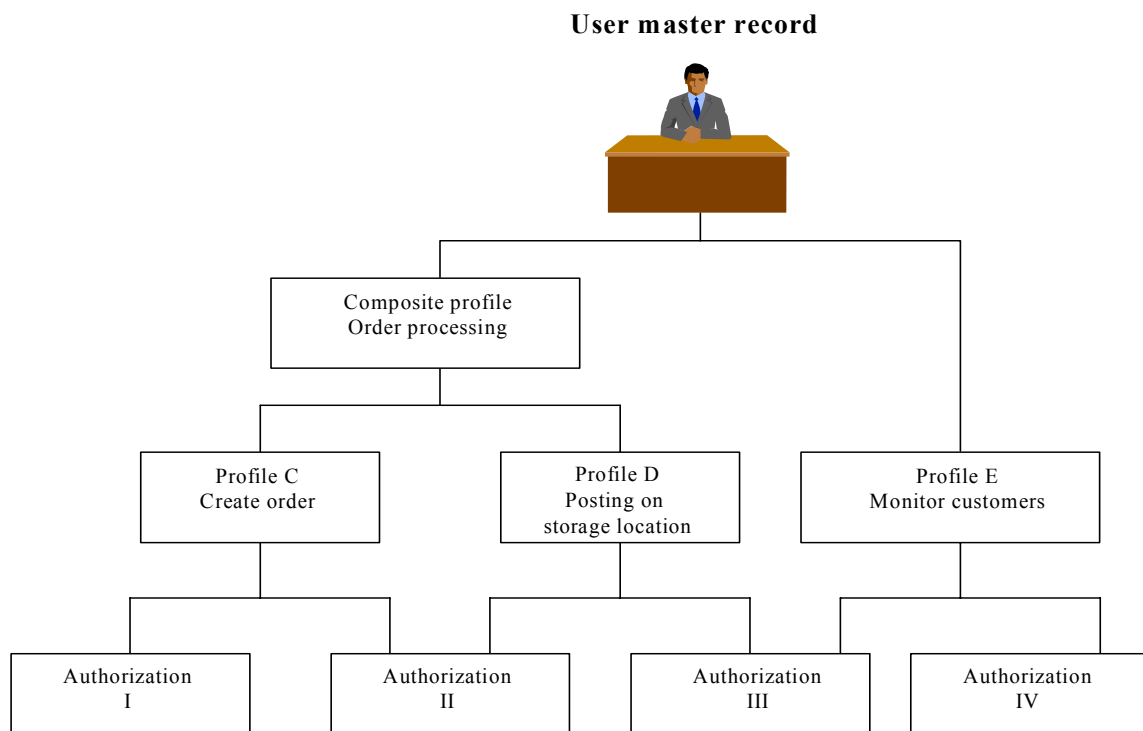


Figure 182: Diagram of a user master record

(Different) single authorizations which are related to the same authorization object - with different values – can be assigned to the same user, if this has been defined in the profiles. In an authorization check, the widest ranging authorization – an OR connection – decides if the check is passed.

Technically, the authorization check in the SAP™ system is done as follows: The single authorizations in all profiles which are assigned to authorization objects are loaded in the so called “user buffer” for the duration of the logged on session. This can be viewed in the menu:

Tools

Administration

Monitor


User buffer

(transaction SU56)



Display with values		
User: RV_BENU4 System: I46 Client: 800 Date: 02.12.2002 Time: 19:21:12		
Object	Authorizatio	Object text
A_A_VIEW	T-I655004200	Asset: View
A_A_VIEW	T-I655004201	Asset: View
A_B_ANLKL	T-I655004200	Asset Postings: Company Code/Asset Class
A_B_BWART	T-I655004200	Asset Postings: Asset Class/Transaction Type
A_C_AFAPL	T-I655004200	Asset Customizing: Chart of Depreciation
A_IMA_ART	T-I655004200	Request Type for Appropriation Requests
A_IMA_ART	T-I655004201	Request Type for Appropriation Requests
A_IMA_BUK	T-I655004200	Company Codes for Appropriation Requests
A_IMA_BUK	T-I655004201	Company Codes for Appropriation Requests
A_IMA_GSB	T-I655004200	Business Areas for Appropriation Requests
A_IMA_GSB	T-I655004201	Business Areas for Appropriation Requests
A_IMA_KOK	T-I655004200	Controlling Areas for Appropriation Requests
A_IMA_KOK	T-I655004201	Controlling Areas for Appropriation Requests
A_IMA_MSTA	T-I655004200	User Status of Appropriation Requests
A_IMA_MSTA	T-I655004201	User Status of Appropriation Requests

Figure 183: Overview of authorizations in the private user buffer

By clicking the button display with values  Display with values it is possible to display the authorization values in the authorization profiles for specific authorization objects.

Display with values		
User: RV_BENU4 System: I46 Client: 800 Date: 02.12.2002 Time: 19:26:10		
Object	Authorizatio	Object text
A_A_VIEW	T-I655004200	Asset: View
Asset view		*
A_A_VIEW	T-I655004201	Asset: View
Asset view		*
A_B_ANLKL	T-I655004200	Asset Postings: Company Code/Asset Class
Activity		*
Asset class		*
Company code		*

Figure 184: Authorization values in the user buffer

Programs are started when the SAP™ user calls a linked transaction. Within the started program the system checks if there are coded authorization objects and which authorization values are required for running the program.

The required authorization values for the authorization objects are compared to the entries in the user buffer. If the required authorization values of each involved authorization object can be matched, the program runs and the user is able to complete the transaction. If the SAP™ system identifies only one required authorization value of an authorization object as missing in the user buffer, the transaction will be terminated. The user receives a message about insufficient authorizations. Every SAP™ auditor knows this situation!

The user can obtain more information about the missing authorization as soon as the transaction has been terminated by calling the menu

System  
Utilities  
Display authorization check

(transaction SU53).

User: RV\_BENU4  
System: I46 Client: 800

The following authorization object was checked:

Object Administration Functions in the Change and Transport System ( S\_CTS\_ADMI )  
Object class Basis: Administration ( BC\_A )

Field	Value
Administration tasks for Change and Transport System	
TABL	

Available authorizations for the object in the master record:

**Figure 185: Display of a failed authorization check**

Below you will find a summarized overview, which explains the connections between various elements of the authorization system in the SAP™ system.

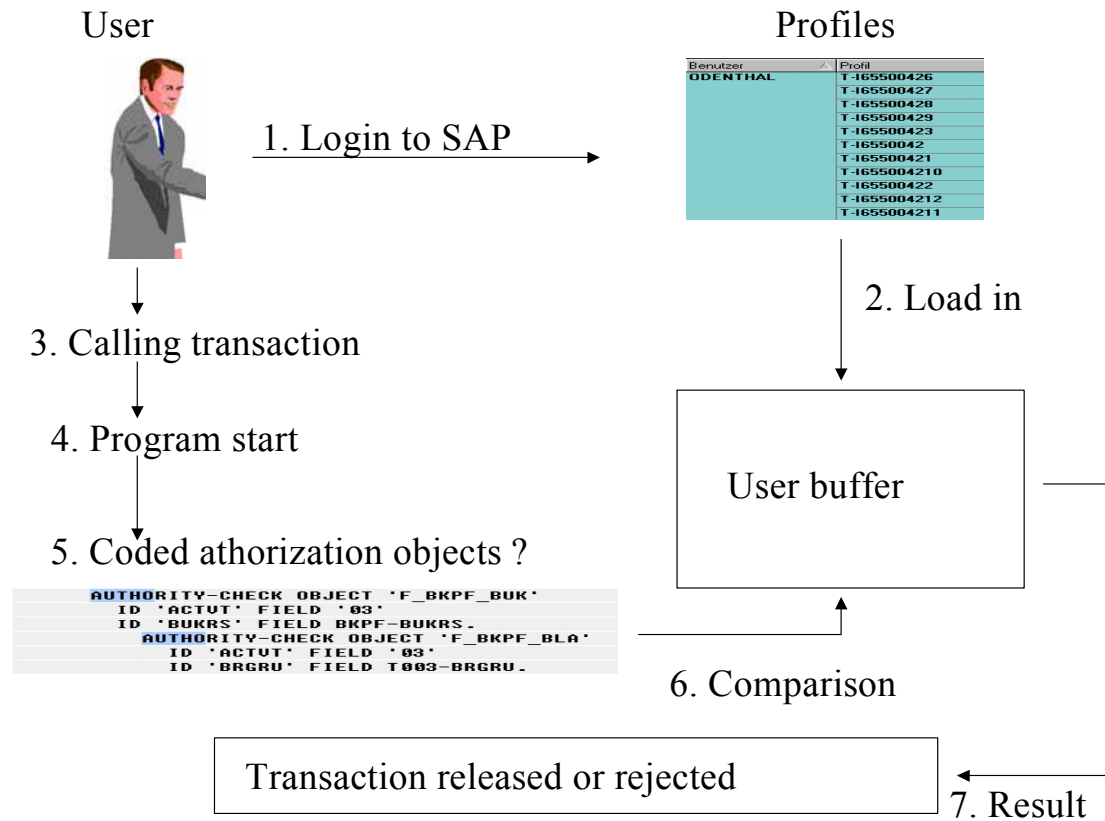


Figure 186: Elements of the authorization system in the SAP™ system



### 5.6.2.5 User oriented access controls in the SAP R/3™ system

The entirety of access controls, beginning with the log on of the user up to the release of specific transactions, is showed in the figure below.

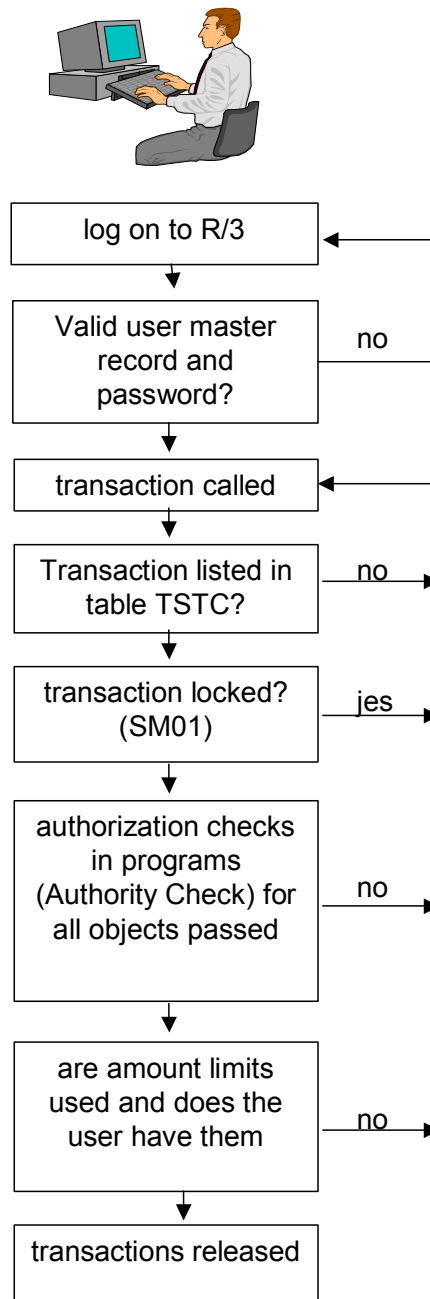


Figure 187: Access controls in the SAP R/3™ system

### 5.6.2.6 Tools for the authorization elements overview

Purpose	Transaction/Function	Tables	Programs
object classes overview	SU03		
single objects overview	SU03 and double click "class"		
object fields	Marking the object and button "display fields"		
objects documentation	Marking the object and button "documentation"		
determine authorization objects with protective functions in programs	SE38 and "source code" and find "Authority-Check"		selected program
determine authorization objects with protective functions in programs	AIS + development/ABAP programs (statistical program analysis)		selected program
Values for authorization field "Activity"	SE16 and	TACT TACTZ	
overview of SAP™ standard profiles	SA38 and		RSUSR020
Content analysis of single profiles	SA38 and (select profile, drill down)		RSUSR020
Overview of "generated profiles" (profile generator)	SA38 and "generated profiles" in the selection screen		RSUSR020
Viewing the user buffer	SU56		
Display specific authorization values in the user buffer	SU56 and button "Display values"		
Form "failed authorization check"	SU53		

### **Exercises on tools for the authorization system**

1. Which authorization objects protect the processing of a posting document?

---

---

---

---

2. Which fields contain the authorization object F\_LFA\_APP and what does the authorization object protect?

---

---

---

---

3. Explain the function of the authorization object S\_TCODE!

---

---

---

---

4. Create an overview of standard SAP™ profiles, with only display authorizations!

---

---

---

---

5. Which activities (values) can be entered in an authorization for the authorization object F\_LFA\_BUK?

---

---

---

---

6. Create an overview of the in-house developed authorization profiles!

---

---

---

---

7. Check (in samples) if the SAP™ standard profile M\_ANZ only contains values for display authorizations!

---

---

---

---

8. Create an overview of “generated profiles” (profile generator)!

---

---

---

---

9. Determine if your user profile has authorization for the authorization object F\_BKPF\_BUK!

---

---

---

---

10. Explain the purpose of an “amount authorization”!

---

---

---

---

### **5.6.3 Techniques for auditing authorizations**

#### **5.6.3.1 Introduction to the audit technique**

The presented process model for analyzing and evaluating individually designed SAP R/3™ authorization systems is based on methodical procedures as well as practical experiences from multiple audits in various companies of different sizes and fields of business. In order to reduce the audit staff effort, it is structured in separate steps, which can be adapted to any required level of detail. It is risk oriented regarding information system and business processes. The main audit focus is the sufficiency of the internal control system. The objective is to review the SAP R/3™ supported business processes to ensure that formal and legal requirements are met, just as company specific requirements for a sufficient internal control system as well as on data protection and security are met. Based on that, process improvements can be suggested as a result of the audit, which will be accepted by employees, by business departments and by internal and statutory auditors.

#### **5.6.3.2 Mapping the environment**

There is no such thing as a “correct” SAP authorization system. Instead, it has to be individually customized according to the prevailing system environment and has to be designed in line with the given management philosophy, from supervised and strictly segregated working steps to self guided and trust based responsibilities.

In a first step the system environment to be audited has to be mapped. The objective is to establish, how the company’s organizational structure has been reflected in the SAP R/3™ System. In which company codes are business transactions posted and which modules are utilized? Which data is entered into the system, including the interfaces to linked sub systems? The auditor should try to get an overview of which functions are utilized and how manual processes are connected to the IT-systems. The acting persons are of his particular interest, especially in the IT-administration, in the business departments and the consultants.

A part of the required information can be obtained – as indicated above – from the SAP™ system. Besides that, available paperwork like organization charts or job descriptions can be useful. Personal judgements and individual issues will be discussed in interviews.

The result of this initial overview is a risk matrix, where IT related business processes are classified by risk aspects. Additionally, the audit scope and strategy are defined, and the required budget is quantified.

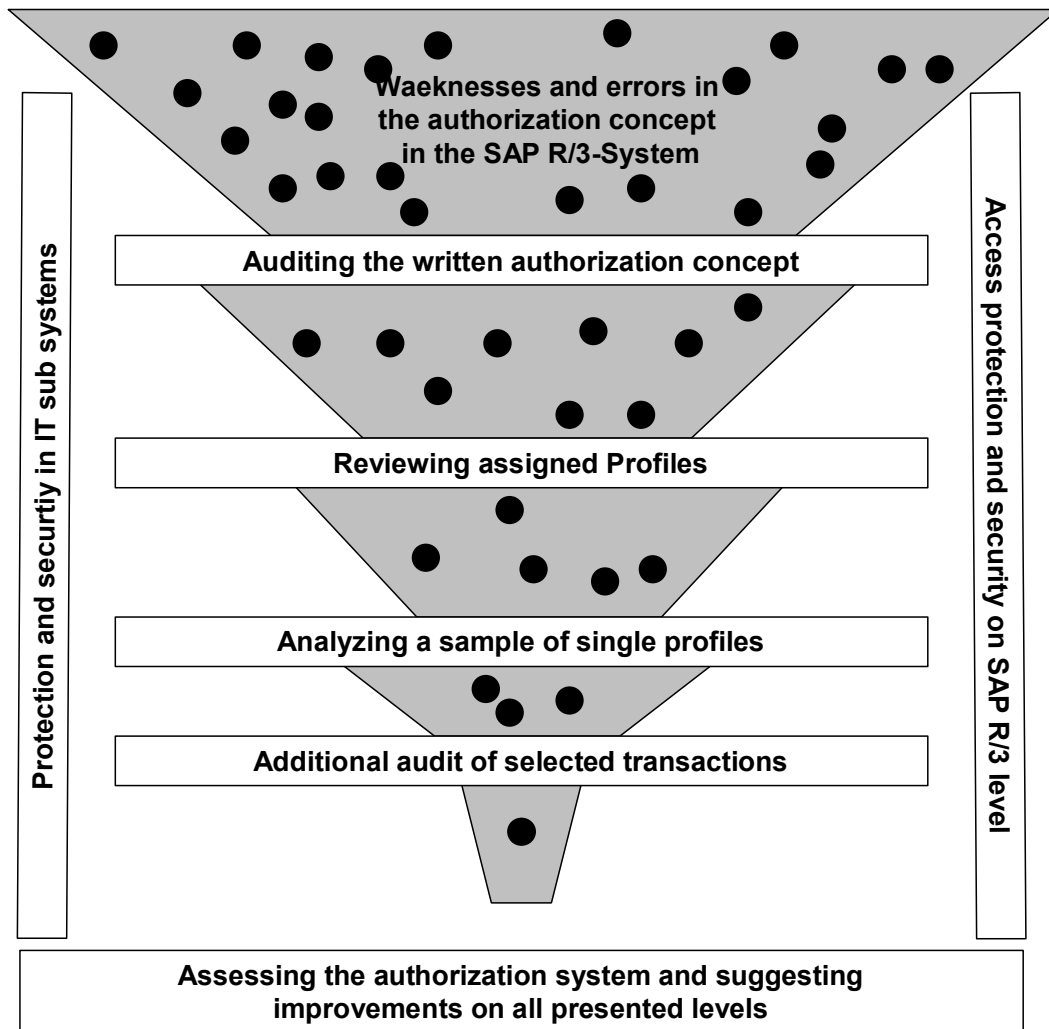


Figure 188: Cascade structured audit concept for an SAP R/3™ authorization system

#### 5.6.3.3 Auditing the written authorization concept

In order to ensure a sufficient internal control system in the company even after implementing the SAP R/3™ system, an immaculate desk planning is required, which has to be documented in a clear, closed and consistent written authorization concept. The existence of a written authorization concept, its contents, the clarity and timeliness are also within the audit scope, as well as its system implementation and the related authorization and user administration.

There are numerous elements within the protective systems in the SAP R/3™ system, which have to be planned before they can be reflected in an authorization system. For example assigning the following:

- tables - to table groups and access authorizations
- transactions - to roles (company organization structure)
- executable ABAP/4™ programs - to program groups and access authorizations
- user IDs - to user groups and user administration
- accounts - to account groups and authorizations for access and posting
- document types - to authorization groups and access authorizations
- amounts - to user groups (invoices, documents, payments)
- tolerance limits - to user groups (invoice deviations, rounding)
- SAP™ objects - to protection category and access authorization (materials, vendors)

A differentiated protection can be created for each element. This requires thorough planning of the listed protective mechanisms beforehand, and that they are customized accordingly. This has to be discussed with the user departments in the company. If this is neglected, the mechanisms can not be utilized properly in the authorization system, resulting in a weakened system security.

Further, the levels of aggregation (work process, work place, role of the employee) for the authorizations have to be defined in the authorization concept, as well as the authorization contents and names of authorizations, profiles or activity groups. Naming conventions, defined to the last character, are required in order to keep the system auditable, the administration effort at an acceptable level and to ensure that only authorized staff are able to maintain profiles within their work area.

The authorization concept should define the authorization maintenance, and assign it to organizational areas. It should also state if the user administration is to be centralized or decentralized.

The written authorization concept is the most important basis for the proper implementation of an authorization system and the administration in the production SAP™ system. At the same time, it is the benchmark for the audit. If the concept is not in place, or if it shows major weaknesses, the auditor can be certain to find security gaps in the production system. The audit activities in the system can then be limited to spot checks in order to confirm the hypothesis, resulting from practical experience.



#### **5.6.3.4 Analyzing authorization weaknesses within the SAP™ system**

##### **5.6.3.4.1 Introduction to weakness analysis**

By auditing the authorization system in the SAP R/3™ system, the implementation of the planned written authorization concept in the “live” system is analyzed. Are defined authorization implemented as intended and do the employees have adequate authorizations? Do the specific profiles bear weaknesses or risks? After assigning profiles to user-IDs, are there cumulated functions, which endanger protection, security and compliance? Which options can be activated in the system or with additional organizational measures in order to minimize risks resulting from lack of segregation of duties, where this is not feasible?

These and similar topics will be discussed in detail.

##### **5.6.3.4.2 Visual check of assigned authorization profiles**

The created user master records and the assigned single profiles and composite profiles are checked visually in the first step. Hereby is to be determined, if

- critical standard system profiles with super, administration and development authorizations are restricted to the small group of system administrators only,
- no functional standard profiles are used (for example in financial accounting) where the internal control system would not be sufficient,
- the names of in-house developed profiles adhere to the naming conventions in the authorization concept
- the profiles assigned to the user IDs agree to the function / user group to be carried out
- the assignment of incompatible profiles results in an accumulation of functions.

If major weaknesses or discrepancies to the written concept are detected at this early stage, it should be assessed if further audit activities are required, in order to enable a reliable statement on protection and security in the system environment.

#### **❑ Step 1: Creating an overview of users, user groups and assigned authorization profiles**

For this initial overview the auditor needs the written authorization concept and a system generated description of all users, their functions and their assigned profiles. It will be useful to utilize the AIS™ system and its comprehensive functions for the authorization audit.

The auditor can obtain an interactive list with created user IDs, their user groups and their user type by calling the menu:

System audit

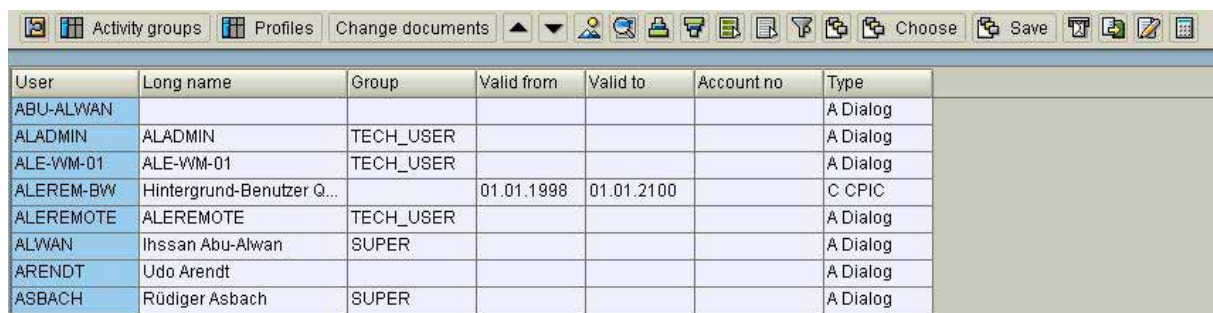
User administration

Information system users and Authorizations

User

By user ID

(transaction SA38 and report "RSUSR002")



User	Long name	Group	Valid from	Valid to	Account no	Type
ABU-ALWAN						A Dialog
ALADMIN	ALADMIN	TECH_USER				A Dialog
ALE-WM-01	ALE-WM-01	TECH_USER				A Dialog
ALEREM-BW	Hintergrund-Benutzer Q...		01.01.1998	01.01.2100		C CPIC
ALEREMOTE	ALEREMOTE	TECH_USER				A Dialog
ALWAN	Ihssan Abu-Alwan	SUPER				A Dialog
ARENDT	Udo Arendt					A Dialog
ASBACH	Rüdiger Asbach	SUPER				A Dialog

Figure 189: Overview of created users

## □ Step 2: Checking group IDs

In the created overview the auditor should determine, if critical SAP™ functions in the administrative and business areas have been assigned to individual user names and not to user groups. Popular user group IDs like for example:


- Admin
- Operator
- Author
- Developer
- Accountant
- Buyer

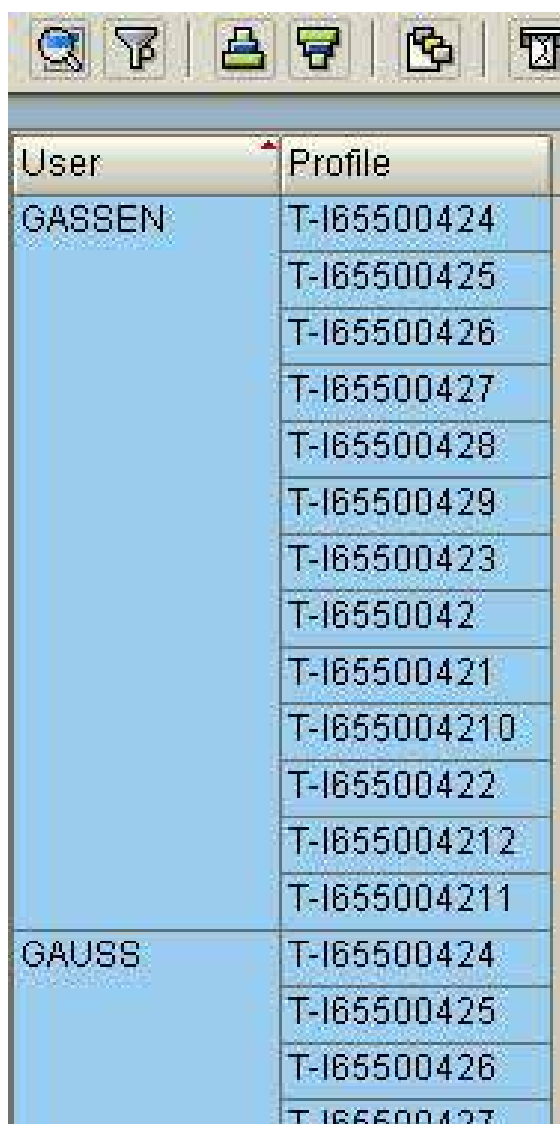
show, that several users use this ID. If these users process personal data, the data protection laws are violated. Commercial and tax laws state, that the processing of financial accounting data must enable the tracking to the originator. Additionally, it must be of basic interest to the company, to be able to name the user if system manipulations or erroneous processing occurs.

### ❑ Step 3: Checking user groups

The user groups should also be checked visually during the review. Every SAP™ user should be assigned to a task oriented user group. In a decentralized user administration this is an essential criterion for the user ID to be maintained only by the assigned administrator. The user group will also give hints about the required extent of authorizations. If the authorization concept is up to date can be checked by the fact, that only user groups which are specifically mentioned in the authorization concept can be found in the SAP™ system.

### ❑ Step 4: Comparing defined and assigned authorization profiles

By clicking the button “profiles”  Profiles in the report on the screen, the user IDs and their assigned profiles are displayed.



User	Profile
GASSEN	T-I65500424
	T-I65500425
	T-I65500426
	T-I65500427
	T-I65500428
	T-I65500429
	T-I65500423
	T-I6550042
	T-I65500421
	T-I655004210
	T-I65500422
	T-I655004212
	T-I655004211
GAUSS	T-I65500424
	T-I65500425
	T-I65500426
	T-I65500427


Figure 190: Overview of the SAP™ user master records and their assigned authorization profiles


Based on the written authorization concept, the auditor should make sure during this first visual check, that only defined profiles and activity groups are assigned to the user master records and that the names adhere to the naming convention. If major discrepancies are detected, like

- not defined profiles and activity groups
- deviations to the naming conventions
- usage of SAP™ standard profiles, especially for users in the business departments (example: F\_BUCH\_ALL)

it would indicate major system weaknesses, which are not very promising for subsequent detailed audit activities.

#### ❑ Step 5: Checking users without authorization


By marking the field “profile” and an ascending sorting order , users without assigned authorization profiles are identified. There is no reason for them to be listed in the user master file.



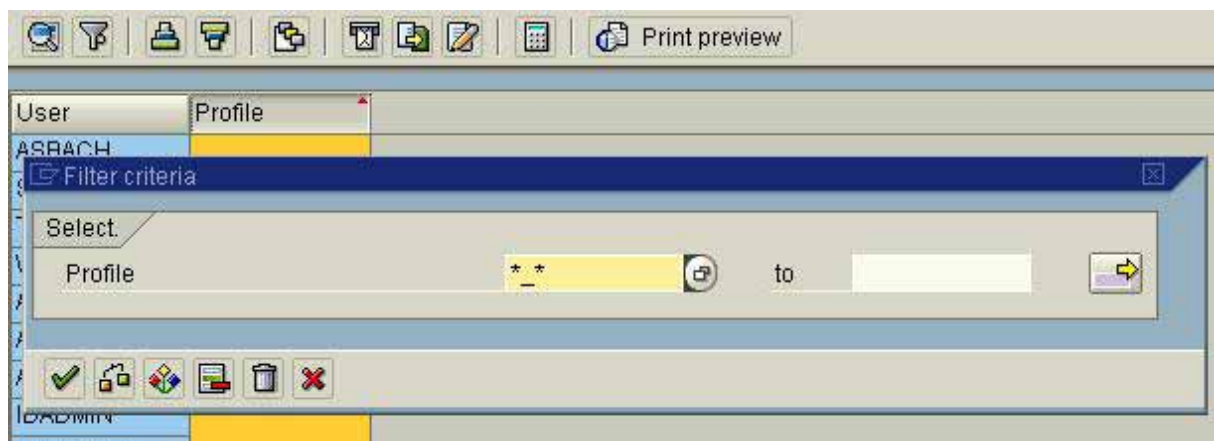
User	Profile
ASBACH	
SHCR3	
TESTBC	

Figure 191: User master records without authorization

#### ❑ Step 6: Checking SAP™ standard profiles

The displayed interactive list allows the filtering of line items in any table field, which enables the auditor to determine, if critical SAP™ standard profiles have been assigned to user master records. The field “profile” is marked and the button  is clicked.

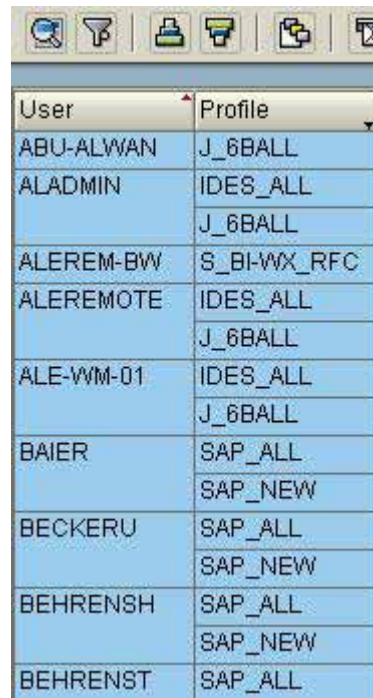
Within the displayed selection screen he can find profiles with an underscore in the profile name.



The screenshot shows the SAP selection screen for user master records. The 'Profile' field is selected, and the 'Filter criteria' dialog is open. The dialog shows a search for profiles containing an underscore. The search criteria are: Profile \* \_ \* to [empty field].

Figure 192: Entry in the selection for finding SAP™ standard profiles

As a result all users with assigned standard profiles are shown.



User	Profile
ABU-ALWAN	J_6BALL
ALADMIN	IDES_ALL
	J_6BALL
ALEREM-BW	S_BI-WX_RFC
ALEREMOTE	IDES_ALL
	J_6BALL
ALE-WM-01	IDES_ALL
	J_6BALL
BAIER	SAP_ALL
	SAP_NEW
BECKERU	SAP_ALL
	SAP_NEW
BEHRENSH	SAP_ALL
	SAP_NEW
BEHRENST	SAP_ALL

Figure 193: User master records with SAP™ standard profiles

A differentiated assessment of this fact is required:

- Administrative SAP™ standard profiles (for example SAP\_ALL)

Just like in every other IT-system, SAP™ system administrators require a widespread authorization range in order to fulfil their duties. All user profiles assigned to the administrators, no matter if they are SAP™ standard or in-house developed, enable them to manipulate the system. The auditor must critically ask, if the frequent discussions with administrators about the well known standard profile "SAP\_ALL" really make sense. The critical characteristics of this profile (amongst other administrative profiles) is commonly known and the risk awareness consequently high. The replacement by sufficiently wide ranging in-house developed administrative profiles result in a unjustifiable sense of security. In our opinion, it is much more important (if administrative SAP™ standard profiles like SAP\_ALL are maintained) to minimize the utilization of such profiles and restrict their assignment only to a very small group of administrative staff. This means:

- a restriction to two to three administrators
- no assignment of these profiles to
- employees in business departments
- group IDs
- developers
- external consultants.

Experience shows that these actions can be taken quickly and without conflicts.

- Standard display only profiles (for auditors)

Pre-configured standard profiles are provided by SAP, i.e.

- F\_ANZ,
- M\_ANZ,
- A\_ANZ,
- S\_A.SHOW

which contain only display authorizations. For specific tasks, like those of the auditors, these standard display authorizations, recognizable by the suffix "ANZ" or "SHOW", should be used. In-house developed profiles usually do not include all authorizations which are necessary for an audit.

- SAP™ -standard profiles for business departments

The risks of business oriented SAP™ standard profiles have been discussed already. The authorization range included in profiles like

- F\_BUCH\_ALL
- F\_BUCHHALTER
- F\_DEBI\_ALL,
- F\_KREDI\_ALL,
- M\_ALL

is not compliant with any legal requirements of a sufficient internal control system. Such SAP™ standard profiles should be avoided in the user master records of business departments.

#### **5.6.3.4.3 Analyzing the contents of specific single profiles**

##### **5.6.3.4.3.1 Audit approach**

The contents analysis of specific single profiles can be carried out in a sample, depending on if a written authorization concept is in place and if major deviations were noted during the previous audit steps. Profiles to be analyzed are randomly selected or according to their risk factors. The auditor should determine, if a defined profile is actually implemented with the intended contents and if the authorization range is appropriate, considering legal requirements for data protection and compliance.

The analytical review of specific profiles is time consuming. With high reliability however, it shows if the defined authorizations are created and assigned as intended. If no major deviations or issues of high risk are noted in a sufficient sample, it can be concluded with very high probability, that the authorization system is efficient. There is a remaining but manageable risk of critical authorization ranges within individual profiles, which were not included in the sample.

Depending on the quality and volume of noted deviations from the written authorization concept, the sample size may have to be increased in order to obtain reliable results. In cases of doubt, every profile, e.g. in accounting, may have to be analyzed in detail, causing an increased work load.

The following criteria should be met by profiles in the sample:

- Conspicuous profiles and activity groups
  - Lack of description in the written authorization concept
  - Deviation from defined naming conventions
  - Conspicuous descriptions indicating test and development activities
- Profiles with only uncritical authorizations, for example “display”
- Random selection from remaining inconspicuous profiles and activity groups

There are two optional approaches for the content analysis, depending on if normal programmed profiles are to be analyzed, or profiles generated from activity groups within the profile generator.

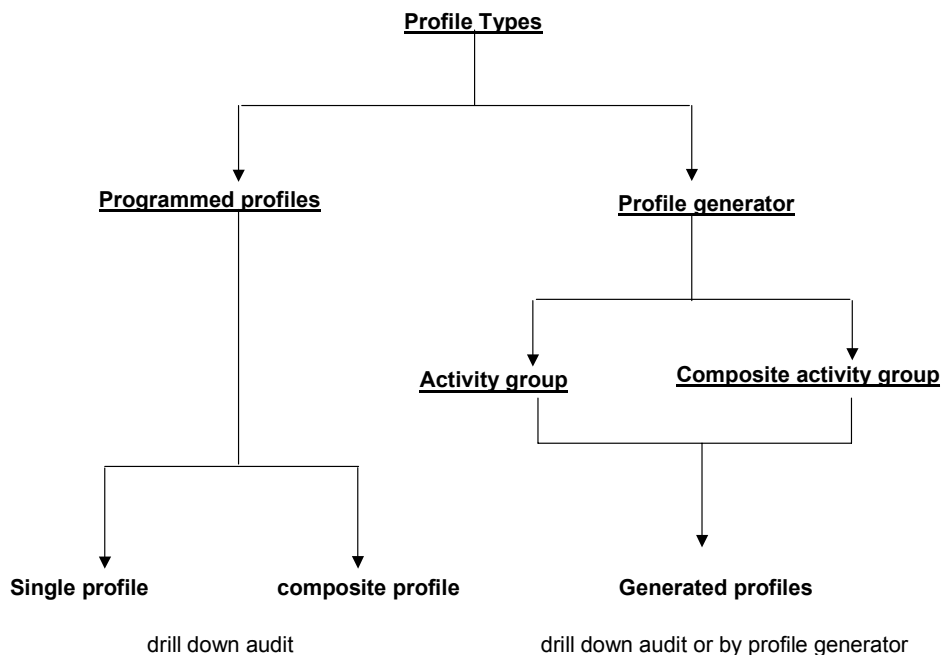


Figure 194: Types of authorization profiles



#### 5.6.3.4.3.2 Auditing activity groups

For analyzing generated profiles derived from activity groups the “profile generator” will be useful. The auditor first has to create an overview, displaying the connection between generated profiles and profiles assigned the user master record (with technical names) and the related activity groups. This overview is obtained in the AIS system by calling the menu

System audit

User administration

Information system users and authorizations

Profiles

by activity group

(transaction SA38 and report “RSUSR020”). The displayed selection screen can be extended with

Edit

All selections.

The selection should be restricted to

- active versions and
- generated profiles.

Selection criteria

Profile

Profile text

☒ Active version

☐ Maint. version

Additional selection criteria for profiles

☐ Comp. prof.

☐ Single prof.

☒ Generated profiles

Last changed by

As a result the single profiles and the related activity groups will be shown on the screen.



Prof.name	Text	Type	Version	Changed by
T-I3550001	Activity group WP_SAP_ESSUSER profile	Generated	Active versn	MIERZWA
T-I3550002	Activity group WP_SAP_B2BUSER profile	Generated	Active versn	MIERZWA
T-I3550004	Activity group ZZTESTWP_IDES_BUYER profile	Generated	Active versn	HAMED
T-I3550020	Activity group IDES_B2B_EMPLOYEE.COM profile	Generated	Active versn	GRAUENHOR...
T-I3550021	Activity group IDES_B2B_MANAGER.COM profile	Generated	Active versn	GRAUENHOR...
T-I3550023	Activity group IDES_BUYER profile	Generated	Active versn	GRAUENHOR...
T-I3550024	Activity group IDES_PURCHMANAGER profile	Generated	Active versn	GRAUENHOR...
T-I3550025	Activity group IDES_TRANSLATION profile	Generated	Active versn	CURA
T-I3550026	Activity group IDES_TRANSCoord profile	Generated	Active versn	CURA
T-I3550027	Activity group IDES_AUDITOR profile	Generated	Active versn	GRAUENHOR...

Figure 195: Overview of generated profiles and related activity groups

Once the profiles which are assigned to the user master records and the related activity groups are identified, the subsequent review should be carried out in the profile generator. The profile generator is called from the AIS-menu with

System audit

User administration

Profile generator

Activity group maintenance

(transaction PFCG). Activity groups to be selected are entered in the selection screen.




Activity group: Z-REVI-ENDUSER\_AG

Description: Z-REVI AUF BASIS SAP\_BC\_ENDUSER\_AG

Buttons: Display, Change, Create

Figure 196: Name of the selected activity group

With the button display  Display, details of the selected activity group are shown.

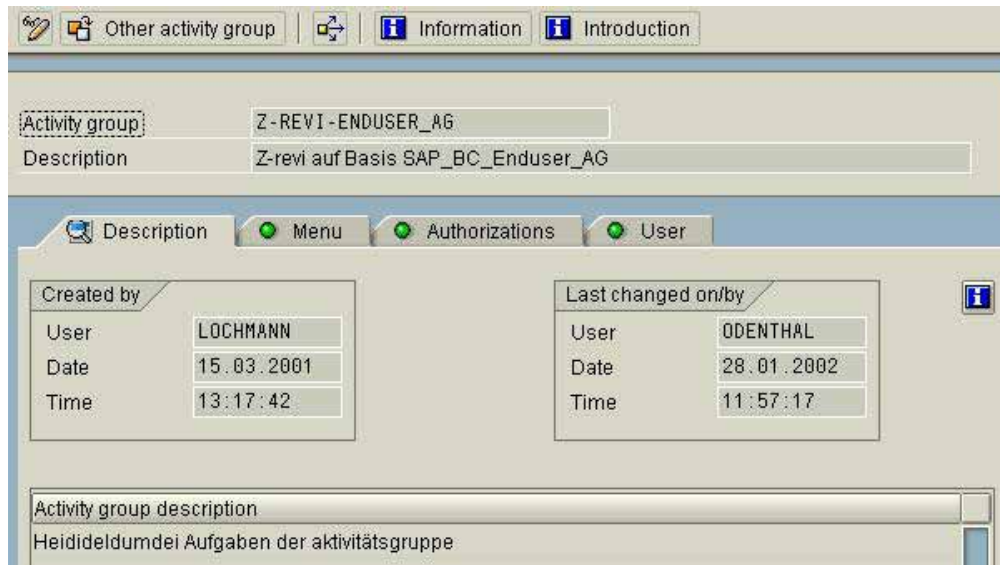


Figure 197: Entry screen for the analyzing a selected activity group

The contents analysis includes the following issues:

#### ❑ Sufficient description and documentation

Transparency within the authorization system requires the selected activity group to have a meaningful brief description which gives a correct impression of the assigned authorization range in tabular overviews. Further, the purpose of the activity group, the assigned authorization range and the intended user group, has to be stated in the documentation.

In this case there is an adequate short description, but the documentation is still not satisfying.

#### ❑ Assigned SAP™ functions (transactions)

The flag “Menu” shows an overview of the SAP™ functions (transactions) assigned to this activity group.

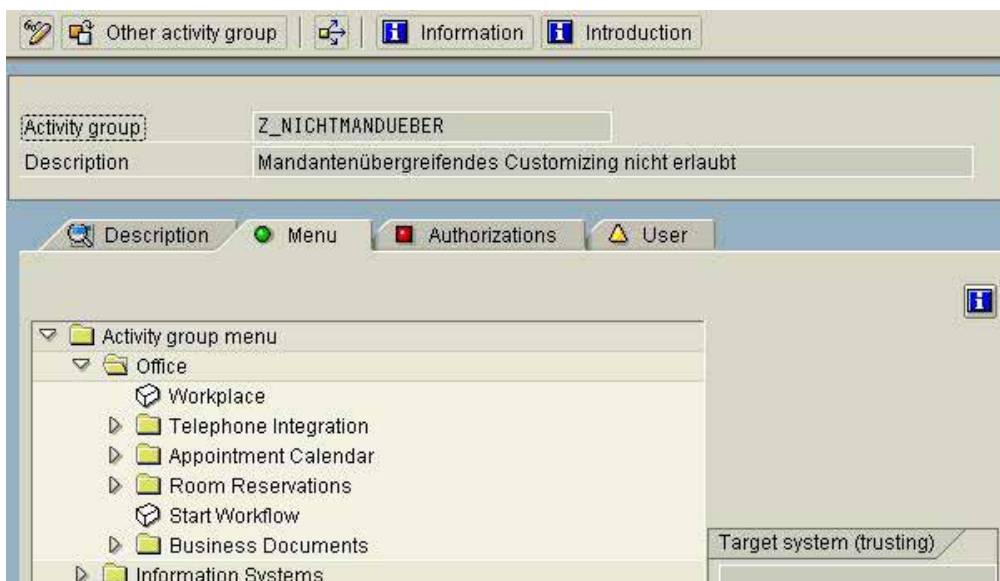



Figure 198: Transactions of an activity group

Here the auditor should make sure, that only those transactions have been assigned, which can be found in the written authorization concept.

#### ❑ Assigned business and administrative authorizations

The flag “Authorizations” and the function “display authorization data” , in the lower screen, routes the auditor to the specific authorization objects and to the assigned authorization values.

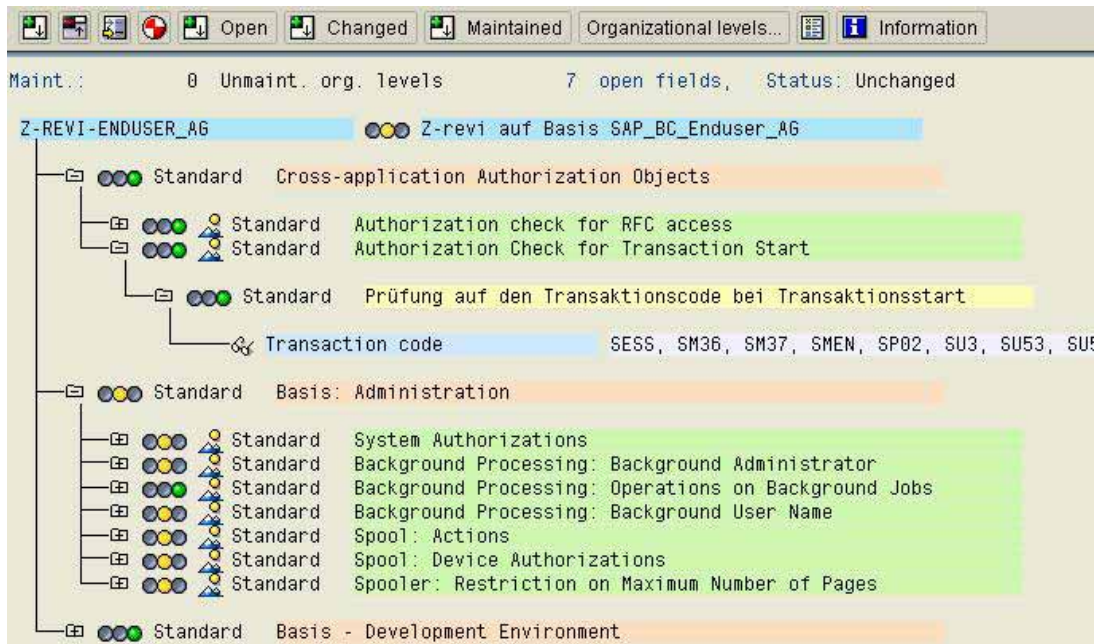


Figure 199: Activity groups with authorization objects and authorization values

At this point the auditor is able to make sure that only intended authorization values have been assigned the activity groups. It is also possible to search for critical authorization values.

#### ❑ Assigned user master records

The flag “user” shows the auditor, which users are assigned to the listed activity group and if the authorizations are assigned to only intended users as defined in the written authorization concept.

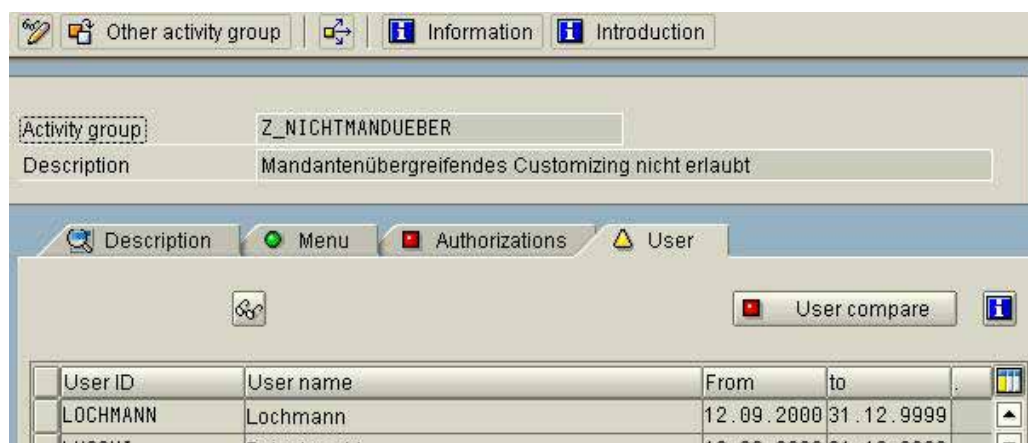


Figure 200: Activity groups and assigned users



#### 5.6.3.4.3.3 Auditing “programmed “ profiles

Programmed conventional profiles, which were not derived from activity groups in the profile generator, can not be analyzed by utilizing the profile generator. The method below can be used for these analyses, and can also be applied to generated profiles (from activity groups). This is especially useful, when the auditor does not have required authorizations for utilizing the profile generator.

In the AISTM system, the auditor can obtain an overview of created single profiles and composite profiles by calling the menu

System audit

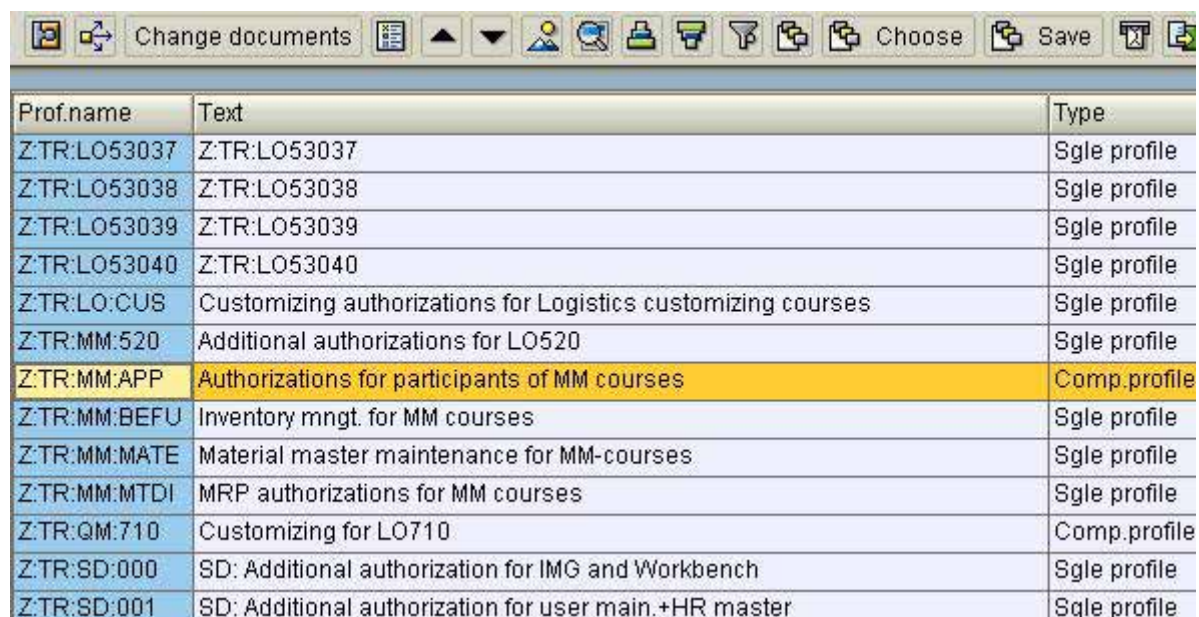
User administration

Information system users and authorizations

Profiles

By profile name or text

(transaction SA38 and program “RSUSR020)



Prof.name	Text	Type
Z:TR:LO53037	Z:TR:LO53037	Sgle profile
Z:TR:LO53038	Z:TR:LO53038	Sgle profile
Z:TR:LO53039	Z:TR:LO53039	Sgle profile
Z:TR:LO53040	Z:TR:LO53040	Sgle profile
Z:TR:LO:CUS	Customizing authorizations for Logistics customizing courses	Sgle profile
Z:TR:MM:520	Additional authorizations for LO520	Sgle profile
Z:TR:MM:APP	Authorizations for participants of MM courses	Comp.profile
Z:TR:MM:BEFU	Inventory mngt. for MM courses	Sgle profile
Z:TR:MM:MATE	Material master maintenance for MM-courses	Sgle profile
Z:TR:MM:MTDI	MRP authorizations for MM courses	Sgle profile
Z:TR:QM:710	Customizing for LO710	Comp.profile
Z:TR:SD:000	SD: Additional authorization for IMG and Workbench	Sgle profile
Z:TR:SD:001	SD: Additional authorization for user main.+HR master	Sgle profile


Figure 201: Overview of single profiles and composite profiles

The auditor can check the following facts:

#### ☐ Sufficient short description?

All listed profiles should have sufficient description of the authorization range and the purpose of the profile to ensure transparency.

#### ☐ Appropriate Authorization values?

By clicking the button display details  or by double clicking the selected profile, a contents analysis of assigned profiles, authorizations for authorization objects and the valid authorization values can be obtained.

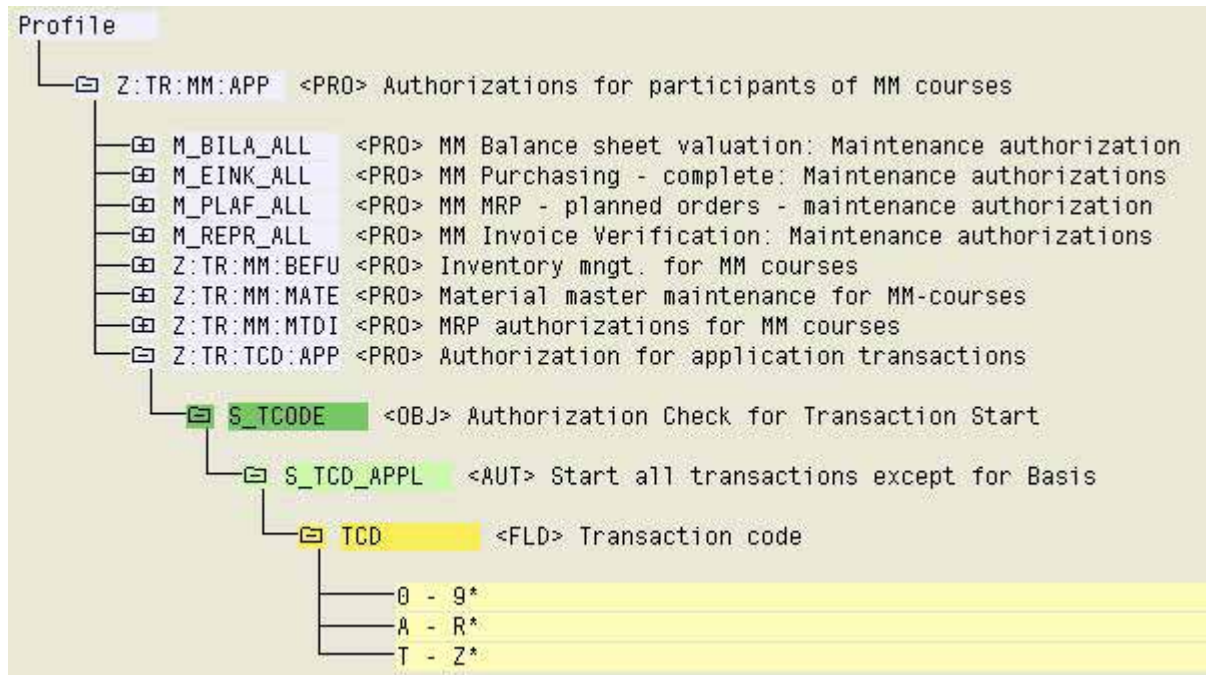


Figure 202: Detailed analysis of valid authorization values of a selected profile

A complete analysis is usually not recommendable, since a profile may consist of authorizations for multiple authorization objects. It can quickly be determined if a profile has a systematic structure, based on few indicators such as:

- Transaction authorizations for the authorization object S\_TCODE  
The entries in the field transaction code (TCD) should be restricted to transactions which are included in the written authorization concept for this profile.
- Authorizations for organizationally restricted authorization objects  
If the authorization profile is defined for working in a particular company code, only authorizations with authorization values for the particular company code should be included in the authorization objects which protect the company code (\_BUK).
- Assignment of appropriate activities  
Authorization profiles intended for display only, should only contain the entry "03" (display) in the field activity (ACTVT) in every authorization object.
- Authorization for only task related authorization objects  
If the authorization profile has been created for a clearly defined task, for example in the financial accounting, the authorizations for authorization objects should primarily be related to the object class finance (F\_XXX).

## ❑ Assigned user

Task related profiles should only be assigned to users, which are defined to perform this certain task in the authorization concept.

By clicking the button where-used list 



Figure 203: Selection screen for the where-used list

the auditor can determine, which user the selected profile has been assigned to.

Activity groups   Profiles   Change document		
User	Long name	Group
ABU-ALWAN		
ALWAN	Ihssan Abu-Alwan	SUPER
ARENDT	Udo Arendt	
BAUMGARTEN	Oliver BAUMGARTEN	
BAYDOUN	Baydon	
BAYER	J. Bayer	
BECKERU	Uta Becker	
BERTSCH	Bertsch	
BEUTELS	Jürgen Beutelspacher	

Figure 204: Finding users with certain profiles in the where-used list

In addition to the users, other profiles and activity groups which include the particular profile can be found in the where-used list.



#### **5.6.3.4.4 Additional audit activities on selected transactions**

##### **5.6.3.4.4.1 The audit approach**

Major deviations to a written coded authorization concept or weaknesses due to too extensive authorization ranges in cases where no written authorization concepts are in place, should have been detected during the previous audit phases. If no weaknesses were noted so far, only the minor audit risk remains, that the selected profile sample was not statistically representative and did not give the auditor a correct impression of the audit field "authorizations". This remaining risk can be minimized by checking if selected critical transactions or critical combinations of transactions, such as

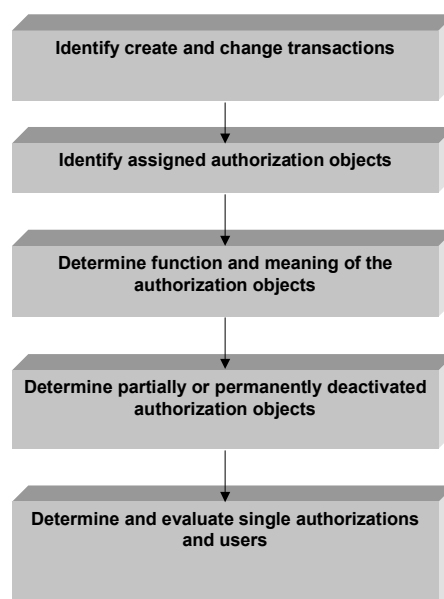
- changing customer and vendor master records
- checking documents
- changing bank information
- invoice checking and payment runs
- authorization administration and user administration
- changing controlling parameters

are assigned to user IDs or profiles, which should not have them.

Auditing transactions is also time consuming and should only be carried out in spot checks for transactions considered to bear risks. Inappropriate authorizations in not yet analyzed profiles are certain to be noted, and would result in the recursive audit step to analyze the relevant profiles in order to determine, if it is an individual erroneous case, or if there is an unrecognized system weakness.

##### **5.6.3.4.4.2 Procedure for transaction oriented auditing**

To check if critical transactions are only assigned to intended authorized users, the following steps are required:



**Figure 205: Model for determining critical authorizations for transactions**

#### ❑ **Step 1: Identify critical transactions**

First of all, transactions have to be identified, where the task oriented assignment to specific users should be checked in samples. This procedure was already discussed in section 2.3.2 (operation via transactions). Optional ways are

- activating technical names in the SAP™ menu or
- display transactions in table TSTC

It is usually useful to select critical transactions from different SAP™ modules. For example:

Transaction	Description
FK02	change vendor master records (accounting)
FB01	post document
F110	parameter for automatic payment
MR21	price change (materials)
VF11	cancel billing document
SE38	ABAP editor (development)
SCC4	client administration

**Figure 206: Selected critical SAP™ transactions**

Type and quantity of the selected transactions has to be defined for each company.

#### ❑ **Step 2: Identify assigned authorization objects**

The authorization objects involved when calling a transaction in the SAP™ system can only be determined with difficulty. A completely reliable statement about the extent and the characteristic of the checked authorization objects with protective functions can only be provided by the “authorization trace”, but auditors rarely have access to this function. Fortunately, the auditor can help himself and get sufficiently reliable results.

- Analyzing authorization codes in programs:

In the AISTM system, calling the menu

System audit

Development /Customizing

ABAP™ Programs

Statistical program analysis

(transaction SA38 and program “RSABAPSC”) an analysis by transaction can be done. The following example shows how the authorization objects with protective functions are determined in the transaction “FK02 –changing vendor master records”.

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

Report  
Function module  
**Transaction code** fk02  
Dialog module

ABAP language commands AUTHORITY-CHECK to

Recurrence level of the analy. 5

☐ Display program name  
☒ Only display selected commands  
☒ Call path of chosen commands

Figure 207: Selection screen for analyzing protective authorization objects in transaction FK02  
with following result:

```

Statist. program analysis
TRANSACTION FK02 Change Vendor (Accounting)

MODULE TRANSAKTIONS_INIT OUTPUT
  PERFORM BERECHTIGUNG_PBO
    AUTHORITY-CHECK OBJECT 'F_LFA1_APP' ID 'ACTVT' FIELD B_ACTVT ID 'APPKZ' FIELD CHAR1
    PERFORM AUTHORIZATION_GENERAL_DATA
    AUTHORITY-CHECK OBJECT 'F_LFA1_GEN' ID 'ACTVT' FIELD P_ACTVT
MODULE KONTO_LESEN
  PERFORM KREDITORENSTAMM_LESEN
  PERFORM BERECHTIGUNGS_PRUEFUNGEN
    AUTHORITY-CHECK OBJECT 'F_LFA1_BEK' ID 'BRGRU' FIELD LFA1-BEGRU ID 'ACTVT' FIELD B_ACTVT
    AUTHORITY-CHECK OBJECT 'F_LFA1_GRP' ID 'KTOKK' FIELD HLP_KTOKK ID 'ACTVT' FIELD B_ACTVT
    AUTHORITY-CHECK OBJECT 'F_LFA1_BUK' ID 'BUKRS' FIELD LFB1-BUKRS ID 'ACTVT' FIELD B_ACTVT
    AUTHORITY-CHECK OBJECT 'F_LFA1_BEK' ID 'BRGRU' FIELD LFB1-BEGRU ID 'ACTVT' FIELD B_ACTVT
    AUTHORITY-CHECK OBJECT 'M_LFM1_EKO' ID 'EKORG' FIELD LFM1-EKORG ID 'ACTVT' FIELD B_ACTVT
MODULE DYNTAB_AUFBAUEN
  PERFORM X055_AUFBAUEN
    AUTHORITY-CHECK OBJECT 'F_LFA1_AEN' ID 'VGRUP' FIELD T055G-GRUPP

Statist. program analysis limited 5 to levels
  
```

Figure 208: Listing of authorization objects for transaction FK02

- Identifying the authorization objects in table USOBT\_C

Table USOBT\_C provides comparable results, showing the connection between transaction, protective authorization object and required authorization values.

After calling the table in transaction SE16 the selected transaction name (FK02) is input in the appearing selection screen. The authorization objects and values are displayed.

- 202 -

Number of entries

Name FK02 to

ReportTyp to

Object to

for field to

Value to

Value to

Figure 209: Selection screen for table USOBT\_C

Table : USOBT\_C  
Displayed fields: 10 of 10 Fixed columns: 5 List width 0250

	Name	ReportTyp	Object	for field	Value
<input type="checkbox"/>	FK02	TR	F_LFA1_AEN	VGRUP	
<input type="checkbox"/>	FK02	TR	F_LFA1_APP	ACTVT	02
<input type="checkbox"/>	FK02	TR	F_LFA1_APP	APPKZ	F
<input type="checkbox"/>	FK02	TR	F_LFA1_BEK	ACTVT	
<input type="checkbox"/>	FK02	TR	F_LFA1_BEK	BRGRU	
<input type="checkbox"/>	FK02	TR	F_LFA1_BUK	ACTVT	02
<input type="checkbox"/>	FK02	TR	F_LFA1_BUK	BUKRS	\$BUKRS
<input type="checkbox"/>	FK02	TR	F_LFA1_GEN	ACTVT	02
<input type="checkbox"/>	FK02	TR	F_LFA1_GRP	ACTVT	02
<input type="checkbox"/>	FK02	TR	F_LFA1_GRP	KTOKK	

Figure 210: Protective authorization objects for transaction FK02 in table USOBT\_C

This overview should be printed for further analyses.

### □ Step 3: Determine function and meaning of the authorization objects

The auditor requires information about the function and meaning of the authorization objects. The required documentation can be obtained in the AISTM system

System audit

User administration

Information system users and authorizations

Authorization objects

By object name, text

(transaction SA38 and program "RSUSR040").

In the selection screen

Figure 211: Selection screen for calling authorization objects

the authorization object name is entered. The displayed overview

Object	Obj.class	Auth. object text
F_LFA1_AEN	FI	Vendor: Change Authorization for Certain Fields
F_LFA1_APP	FI	Vendor: Application Authorization
F_LFA1_BEK	FI	Vendor: Account Authorization
F_LFA1_BUK	FI	Vendor: Authorization for Company Codes
F_LFA1_GEN	FI	Vendor: Central Data
F_LFA1_GRP	FI	Vendor: Account Group Authorization

Number of authorization objects selected = 6

Figure 212: Overview of authorization objects for vendor master records

enables the display of detailed documentation with the button “documentation”

Documentation

Help - F\_LFA1\_AEN

Using this authorization object, you can define a change authorization for selected vendor master record fields. Using this object, you can also protect the fields from being blocked and the delete flag from being set. Only an employee who has been allocated this authorization can change these fields.

**Note**

This authorization is optional. You do not therefore have to assign this authorization if no fields are to be specifically protected from being changed.

The contents of a protected field can still be displayed by all users.

This authorization is not checked when creating a master record.

This authorization is valid for all company codes.

**Defined Fields**

The object consists of the field "Change group".

Figure 213: Documentation of authorization object F\_LFA1\_AEN



This shows if the authorization check is optional or mandatory and which preconditions are required.

**❑ Step 4: Determine partially or permanently deactivated authorization objects**

The authorization administration can deactivate the authorization checks of particular protective authorization objects in general – for all transactions – or for specific transactions. In these cases it is not necessary to include the authorization objects in the transaction oriented detailed audit.

- Determine deactivated authorization objects to transactions

Authorization objects, which are deactivated for specific transactions, can (transaction SE16) be displayed in table USOBX\_C. In the selection screen

Figure 214: Selection screen to table USOBX\_C

the transaction and the object name, have to be entered.

The field “check flag” shows, if the authorization check is done for the particular object in the selected transaction. If the entry is “N”, no authorization check is done.

Check table...							
Table : USOBX_C							
Displayed fields: 9 of 9 Fixed columns: 3 List width 0250							
	Name	ReportType	Object	Changed by	Modification date	Modification time	Check flag
<input type="checkbox"/>	FK02	TR	F_LFA1_AEN	SAP	02.09.1997	20:33:52	Y
<input type="checkbox"/>	FK02	TR	F_LFA1_APP	SAP	05.01.1996	10:44:37	Y
<input type="checkbox"/>	FK02	TR	F_LFA1_BEK	ODENTHAL	19.04.2002	20:28:50	Y
<input type="checkbox"/>	FK02	TR	F_LFA1_BUK	ODENTHAL	19.04.2002	19:48:45	Y
<input type="checkbox"/>	FK02	TR	F_LFA1_GEN	KIRK	05.09.2001	17:54:53	Y
<input type="checkbox"/>	FK02	TR	F_LFA1_GRP	KIRK	05.09.2001	17:54:53	Y

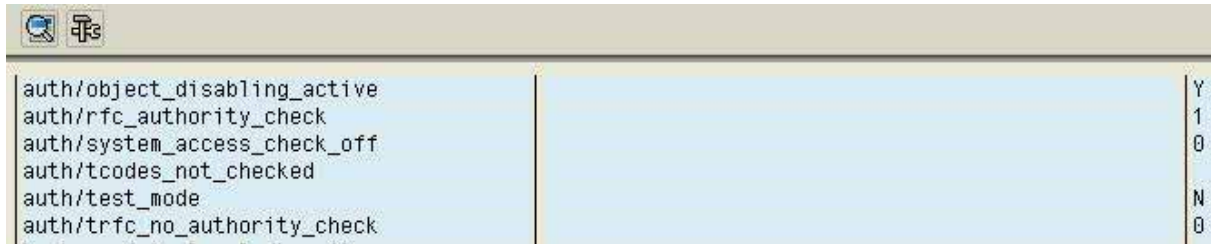
Figure 215: Contents of table USOBX\_C to transaction FK02

- General deactivation of authorization objects

Particular authorization objects can only be generally deactivated if “Y” is entered in the related system profile parameter

auth/object\_disabling\_active

This is checked by calling report “RSPARAM” in transaction SA38.



auth/object_disabling_active	Y
auth/rfc_authority_check	1
auth/system_access_check_off	0
auth/tcodes_not_checked	N
auth/test_mode	0
auth/trfc_no_authority_check	

Figure 216: Settings of system parameters in the authorization system

If the setting is “Y”, the authorization objects with globally deactivated authorization check have to be determined by calling the AISTM menu:

System audit

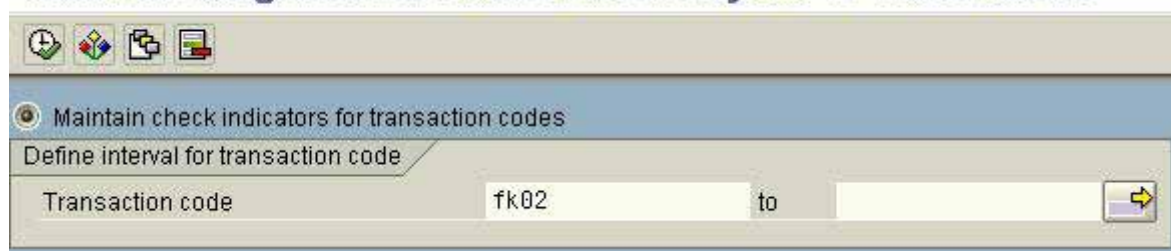
User administration

Profile generator

Authorization objects customer check ID

(transaction SU24)

### Maintain Assignment of Authorization Objects to Transactions



Maintain check indicators for transaction codes

Define interval for transaction code

Transaction code  to

Figure 217: Selection screen for checking check indicators for transaction codes

Any transaction can be shown. By clicking the button “check indicator”

 Check indicator

a log by transaction is shown on the screen.



### Display Check Indicator for FK02

Field values				Auth.obj.	Auth.obj.	SAP defaults
U	N	C	CM	Check ID	Object	Object name
		✓		Check	C_DRAW_TCD	Authorization for document activities
		✓		Check	C_KLAH_BKP	Authorization for Class Maintenance
		✓		Check	C_TCLA_BKA	Authorization for Class Types
		✓		Check	C_TCLS_BER	Authorization for Org. Areas in Classification System
		✓		Check	F_BNKA_BUK	Banks: Authorization for Company Codes
		✓		Check	F_BNKA_MAN	Banks: General Maintenance Authorization
		✓		Check/maintain	F_LFA1_AEN	Vendor: Change Authorization for Certain Fields
		✓		Check/maintain	F_LFA1_APP	Vendor: Application Authorization
		✓		Check/maintain	F_LFA1_BEK	Vendor: Account Authorization
		✓		Check/maintain	F_LFA1_BUK	Vendor: Authorization for Company Codes
		✓		Check/maintain	F_LFA1_GEN	Vendor: Central Data
		✓		Check/maintain	F_LFA1_GRP	Vendor: Account Group Authorization
		✓		Check	P_ORGIN	HR: Master Data
		✓		Check	P_PERNR	HR: Master Data - Personnel Number Check

Figure 218: Display of check indicators to transaction FK02

Globally deactivated authorization objects are colored (red).

The button field values  routes the auditor to the required authorization values (corresponding to table USOBT\_C).

### Display Field Values for FK02

SAP defaults

Object descr.

Auth.obj.

Object	Field	Value (interval)
F_LFA1_AEN	VGRUP	
F_LFA1_APP	ACTVT APPKZ	02 F
F_LFA1_BEK	ACTVT BRGRU	
F_LFA1_BUK	ACTVT BUKRS	02 \$BUKRS
F_LFA1_GEN	ACTVT	02
F_LFA1_GRP	ACTVT KTOKK	02

Object globally switched off

Object globally switched off

Figure 219: Authorization objects with assigned field values

- Lack of organizational characteristics

If certain organizational characteristics, which are of interest for the internal control system, such as customer groups, authorization groups etc. are not reflected in the system, the auditor should inquire about it with the authorization administration and review the written authorization concept. Authorization objects, with field values related to non-existing characteristics do not need to be included in the audit.

#### □ Step 5: Determine users of selected transactions

The start of a selected transaction in the SAP™ system is secured in a twofold respect.

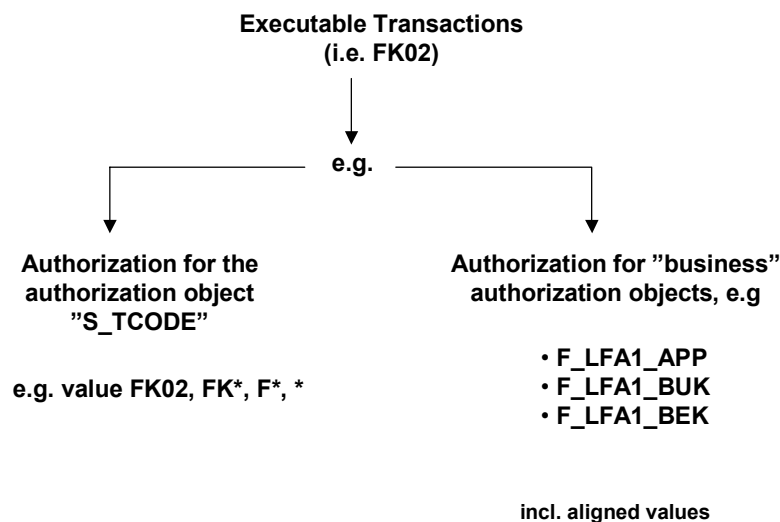


Figure 220: Access protection of SAP™-transactions

The auditor must have the adequate authorization for the authorization object S\_TCODE (FK02, FK\*, \*).

#### Definition

Whenever a transaction is started, the kernel uses the transaction code as the value to check against the authorization object. This check always takes place (from Rel. 3.0E) and cannot be deactivated by the developer.

#### Defined Fields

TCD: Transaction code

Figure 221: Documentation to the authorization object S\_TCODE

Additionally, he needs the authorization values for the authorization objects assigned to the transactions.

This can be checked in the AIS-System by calling the menu.:

System audit

User administration

Information system users and authorizations

User

By complex search criteria

(transaction SA38 and program "RSUSR002").

The transaction name to be checked is input in the field "transaction" in the selection screen. This entry ensures the analysis of the authorization object S\_TCODE.

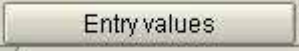
The involved authorization objects also have to be input in the area "selection by values".

The screenshot shows the SAP selection screen for user authorization search, organized into three main sections:

- Selection criteria for user:** Contains input fields for User, Group for authorization, User group (general), Profile, AND profile, and Transaction (with the value 'fk02' entered).
- Selection by authorizations:** Contains input fields for Authorization object and Authorization.
- Selection by values:** Contains a button labeled 'Entry values' and two sections for authorization objects:
  - Authorization object 1:** Authorization object field with the value 'F\_LFA1\_APP'.
  - AND authorization object 2:** Authorization object field with the value 'F\_LFA1\_BUK'.

Figure 222: Input of the selection screen "user by complex search criteria"

Please note, that the authorizations can be checked for only three authorization objects at the time. Therefore it makes sense to identify not used authorization objects beforehand.

In a third step the input screen has to be extended for the authorization objects by clicking the button . After that the authorization values required for calling the transaction have to be input.

Entry values

Authorization object 1

Authorization object: F\_LFA1\_APP

Activity: 02

Value: F OR

AND: OR

Customer and Vendor Master Data Application A

Value: F OR

AND: OR

AND authorization object 2

Authorization object: F\_LFA1\_BUK

Activity: 02

Value: OR

AND: OR

Company code

Value: OR

AND: OR

Figure 223: Input of selected authorization values for selected authorization objects

Please note, that the specified query of "\*" in quotation marks has to be entered for global authorizations! Otherwise, every user who has any authorization value for the particular authorization field are shown.

The system is utilizing the presented program and the input entries, in order to identify all users, who are able to call the selected transaction.

User	Long name	Group
ABU-ALWAN		
ALADMIN	ALADMIN	TECH_USER
ALE-WM-01	ALE-WM-01	TECH_USER
ALEREMOTE	ALEREMOTE	TECH_USER
ALWAN	Ihssan Abu-Alwan	SUPER
ARENDT	Udo Arendt	
BAIER	Günther Baier	
BAUMGARTEN	Oliver BAUMGARTEN	
BAYDOUN	Baydon	
BAVER	I. Baver	

Figure 224: User ID with the authorization vendor master records

Based on the displayed list the auditor has to make sure that only intended users can call the analyzed transaction, based on their tasks and on the defined written authorization concept. Additionally, administrative staff who have comprehensive profiles for controlling the complete system will be listed.

If the analysis identifies inappropriate assignments of the audited transaction authorizations, the not yet analyzed profiles and activity groups have to be analyzed for the employees, who normally should not have these transaction authorizations. By doing that, profiles with too wide authorization ranges, will be detected quickly.

#### **5.6.3.4.5 Further tools for auditing authorizations**

##### **5.6.3.4.5.1 Optional audit approaches**

The introduced audit approach and the presented tools describe one possible procedure for auditing the SAP™ authorization system. In the “Information system users and authorizations” there is a variety of additional reports, which support any thinkable view of authorizations and suit any individual audit strategy. Therefore we recommend every auditor to take a very close look at these reports.

In the following sections, additional special SAP™ reports will be introduced, which provide additional insights.

##### **5.6.3.4.5.2 Pre-configured reports**

Within the AISTM System menu “which user is allowed to...” pre-configured reports can be found, which refer to users with critical authorizations to selected authorization objects. This concerns for example

- users who can call operating system commands
- users who can update company codes
- users who can update accounting periods
- etc.

The results of these reports provide a first overview of the system security status.

Similar insights can be obtained in the report

System audit

User administration

Information system users and authorizations

User

With critical authorizations

(transaction SA38 and program “RSUSR040”) which in particular shows users, who can fulfill administrative tasks within the SAP™ system. The risk level is indicated by color (red).

The above mentioned report can be supplemented by functions, which are considered to be critical within the company.



User: ABU-ALWAN	
Administration:	All rights for background jobs
Administration:	Release background jobs
Administration:	Start background jobs with each user
Administration:	Start background jobs with each user
Administration:	Network, processes, update task administration, ...
Administration:	Network, processes, update task administration, ...
Administration:	CCMS maintenance
Administration:	Operations on secured print requests
Administration:	Print on critical printers
Administration:	Operations on other TemSe-Objekts
Revision:	Authorization display
Revision:	Profile displ.
Revision:	User displ.
Customizing:	Table maintenance
Customizing:	Table maintenance all basic tables
Development:	Program and ABAP Dict. maintainance
Development:	Transport system
User: ALADMIN	
Administration:	All rights for background jobs
Administration:	Release background jobs
Administration:	Start background jobs with each user
Administration:	Start background jobs with each user

Figure 225: Critical authorizations by user

5.6.3.4.5.3 Determine critical authorization combinations

A report which is limited to the analysis of assigned transactions (Object S\_TCODE) but displays critical combinations, can be called in the AISTM menu

System audit  
User administration  
Information system users and authorizations  
User  
By critical combinations

Critical combination						
FK01 Create Vendor (Accounting)						
FB01 Post Document						
Number of users found: 244						
User group : (not maintained)						
ABU-ALWAN	ARENDT	BAIER	BAUMGARTEN	BAYDOUN	BAYER	BECKERU
BEHRENGH	BEHRENST	BEILMANN	BERTSCH	BEUTELS	BORZIM	BRADLER
CMDDMO	CSUSER	DIEBOLD	DMITRIJEVIC	DOERLITZ	DOERR	DONNER
ERNSHAUS	EVERLING	FALZ	FECHNER	FESL	FISCHER	FISWICK
FITTERER	GASSEN	GAUSS	GEIGER	GELBARTH	GEYER	GOEDICKE
GOERLITZ	GRABETZ	GUANG	HEIDRICH	HENEKA	HERF	HILDEBRANDT
HOLETZKE	HOLLAU	HUNOLD	HUWIG	IHL	JOESEL	JORCZYK
KAULL	KLEIN	KLOBER	KNELL	KNIERIM	KNOLL	KRAPF
KRELL	KRIEG	KRIEG2	KRTEST	KUNKELM	KUNZE	KUHN
LANGENHORST	LEISSNER	LOCHMANN	LOEFFLER	LUCCHI	LUDWIG	MAIER
MELLATI	MERKLE	MERZ	METZ	MICKA	MINDERMANN	MOECKEL
MORALES	MUHLER	MUNSCH	NIEHAUS	NITSCHKE	NTSRVBE_TEL	ODENTHAL
PAAPE	PACHUR	PENG	PHILIPP	PREHN	PUCHALAPALLI	REICHELT
REMSEN	RFCUSER	RIEDENKLAU	RITT	ROTTER	RRZKA	RV_BENU1
RV_BENU2	RV_BENU3	RV_BENU4	RV_BENU5	RV_BENU6	SANDEEP	SANNA
SCHADOMSKY	SCHAUER2	SCHEUNEMANN	SCHIMANSKI	SCHMATZER	SCHNEIDER	SCHNEIDERM
SCHNELLE	SCHOENHERR	SCHULD	SCHULUNG1	SCHULUNG2	SEEBER	SEHLMAYER
SPENRATH	STEIN	STEPPE	SUPPORT	TEAM4	TEST_NICHT	THUM
TRISCH	WAEHNER	WALDHAUER	WEHDE	WIECHERS	WILD	WILMANS
WIRTH	WISCHNEWSKI	ZANDT	ZITZMANN			
User group : DEVELOPER						
DEVELOPER						

Figure 226: Users with authorization combinations

This report provides a first impression of possible authorizations of a user, but requires additional audit activities in order to verify the business related authorization objects. Any combination of transactions can be entered.

#### 5.6.3.4.5.4 Comparing users, profiles and authorizations

In an SAP™ system with multiple users, a continuous control can be facilitated by creating template user and profiles (with a defined authorization range) related to certain activities.

By calling the AIS™ menu

System audit

User administration

Information system users and authorizations

Comparisons

User

(transaction SA38 and program "RSUSR050") the template user can be compared with operating users of the same user group, in order to determine in which areas the authorization range differs.

Documentation		
User:	LOCHMANN	BAIER
Client:	800	800
System:	I46	I46
Different values	W_TRAN_CCR	W_TRAN_CCR
Different values	V_VTTK_TDS	V_VTTK_TDS
Different values	V_VFKK_FKA	V_VFKK_FKA
Different values	V_VBUK_FRE	V_VBUK_FRE
Different values	V_VBSK_GRA	V_VBSK_GRA
Different values	V_VBRK_VKO	V_VBRK_VKO
Different values	V_VBRK_FKA	V_VBRK_FKA
Different values	V_VBKA_VKO	V_VBKA_VKO
Different values	V_LIKP_VST	V_LIKP_VST
Different values	V_KONG_VWE	V_KONG_VWE
Different values	V_KOND_VEA	V_KOND_VEA

Figure 227: Authorization comparison for two user

The summarized shown values can be tracked in detail by the clicking the button .



#### 5.6.3.4.5.5 Checking amount authorizations

In addition to the presented mechanisms for separating critical SAP™ transactions from unauthorized users, the SAP R/3™ system offers the option to restrict users by so called "tolerance groups". By utilizing these tolerance groups, authorizations for e.g. postings to a general ledger account or an open items posting, can be restricted to predefined amounts.

A similar protection, which enables the system to operate in accordance with the company's defined delegation of authorities, is reflected in the system customizing. In a first step the tolerance groups are defined, stating the maximum amounts. In a second step, the users are assigned to specific tolerance groups.

Tolerance groups and assigned users are administered in tables named "T043\*".

Table name	Short text
T043	Assign Accounting Clerks —> Tolerar
T043G	Tolerances for Groups of Customers/V
T043GT	Name of Business Partner's Tolerance
T043I	Tolerance Groups for Persons Process
T043K	Control of Payment Notices to Custom
T043S	Tolerances for Groups of G/L Account
T043ST	Name of Business Partner's Tolerance
T043T	FI tolerance groups for employees

Figure 228: Overview of relevant tables for amount authorizations

By calling transaction SE16 and entering table T043T the auditor can check, if the system contains tolerance groups for financial accounting and which amount limits have been defined.

Table : T043T  
Displayed fields: 6 of 6 Fixed columns: 2 List width 0250

	Tolerance group	Company code	Revenue	Expense	Amount per document	Amount per C/V item
<input type="checkbox"/>		2400	1.000,00	1.000,00	9999.999.999.999,99	9999.999.999,99
<input type="checkbox"/>		2500	1.000,00	1.000,00	1000.000.000.000,00	1000.000.000,00
<input type="checkbox"/>		3000	1.000,00	1.000,00	1000.000.000.000,00	1000.000.000,00
<input type="checkbox"/>		4000	1.000,00	1.000,00	1000.000.000.000,00	1000.000.000,00
<input type="checkbox"/>		4200	1.000,00	1.000,00	1000.000.000.000,00	1000.000.000,00
<input type="checkbox"/>		5000	1,00	1,00	10.000.000.000,00	99.999.999,99
<input type="checkbox"/>		6000	1.000,00	1.000,00	1000.000.000.000,00	1000.000.000,00
<input type="checkbox"/>		F100	1.000,00	1.000,00	1000.000.000.000,00	9999.999.999,99
<input type="checkbox"/>		F300	1.000,00	1.000,00	1000.000.000.000,00	9999.999.999,99
<input type="checkbox"/>		GR01	1.000,00	1.000,00	1000.000.000.000,00	1000.000.000,00
<input type="checkbox"/>		MS01	1.000,00	1.000,00	1000.000.000.000,00	9999.999.999,99
<input type="checkbox"/>		R100	1.000,00	1.000,00	1000.000.000.000,00	9999.999.999,99
<input type="checkbox"/>		R300	1.000,00	1.000,00	1000.000.000.000,00	1000.000.000,00
<input type="checkbox"/>		S300	1.000,00	1.000,00	1000.000.000.000,00	9999.999.999,99
<input type="checkbox"/>	1000	1000	1.000,00	1.000,00	1000.000.000.000,00	1000.000.000,00
<input type="checkbox"/>	1000	1200	1.000,00	1.000,00	1000.000.000.000,00	1000.000.000,00
<input type="checkbox"/>	1000	1500	1.000,00	1.000,00	1000.000.000.000,00	1000.000.000,00
<input type="checkbox"/>	1000	2200	1.000,00	1.000,00	1000.000.000.000,00	1000.000.000,00

Figure 229: Created tolerance groups and their amount limits in table T043T

In table T043 he can determine which users in financial accounting have been assigned to certain tolerance groups.

Table : T043  
Displayed fields: 4 of 4 Fixed columns:

	Client	User name	Tolerance group	PhInv.tol.group
<input type="checkbox"/>	900	RV-BENU1	1000	

Figure 230: Overview of users assigns to tolerance groups

Utilizing tolerance groups is an elegant instrument for minimizing risks, because it is not connected to the presented mechanisms of the authorization system (objects, profiles), but is employee oriented. It is for example possible to keep extra critical groups of persons, trainees or administrators away from posting transactions with high risks without restricting them in other respect. It has to be noted though, that they should have no authorizations for maintaining the tables "T043".

#### 5.6.3.5 Tools for auditing authorizations

Purpose	Transaction/Function	Table	Program
Auditing the authorization concept	Written documentation		
Overview of users, user groups, profiles	AIS + Information system users and authorizations SA38		RSUSR002
Utilizing SAP standard profiles	SA38 Filter * _ *		RSUSR002
Contents analysis of activity groups	AIS + Information system users and authorizations (activity groups) SA38 generated profiles and drill down or PFCG		RSUSR020
Contents analysis of programmed profiles	AIS + Information system users and authorizations (profile, profile name) SA38 and drill down		RSUSR020
Determine transactions	Activate technical names SE16	TSTC	

Purpose	Transaction/Function	Table	Program
Identify transactions and authorization objects	AIS + development, customizing (statistical program analysis)  SA38  SE16	   USOBT_C	  RSABAPSC
Determine the meaning of authorization objects SA38	AIS + Information system users and authorizations (authorization objects, name)  SA38 "and documentation"		RSUSR040
Determine "partially" deactivated authorization objects	SE16	USOBX_C	
Determine "generally" deactivated authorization objects	1. SA38 (auth/object disabling_active = Y) 2. AIS + user administration (authorization objects, customer check ID)  SU24		RSPARAM
Determine users for transactions	AIS + Information system users and authorizations (user, by complex search criteria)  SA38		RSUSR002
Pre-configured report "which user is allowed to....."	AIS + Information system users and authorizations (user, with critical authorizations)  SA38		RSUSR050
Critical authorization combinations	AIS + Information system users and authorizations (comparisons, users, profiles)  SA38		RSUSR050
Determination amount limits	SE16	T043*	

### Exercises on the authorization audit technique

1. An authorization administrator tells you during your audit, that there is no need for a written authorization concept since only "uncritical transactions" have been assigned to the users. Your reply ?

---

---

---

2. Determine, which users have not been assigned to user groups in the client to be audited.

---

---

---

3. Create an overview of SAP standard profiles assigned to created users.

---

---

---

4. Identify created users without authorizations in the client to be audited.

---

---

---

5. Create an overview of active user profiles, which were derived from activity groups by utilizing the profile generator.

---

---

---

6. Check the authorization range of the SAP-standard profile "F\_buchhalter".

---

---

---

7. Check an activity group you find interesting, due to its authorization range.

---

---

---

8. Identify activity groups without sufficient short descriptions.

---

---

---

9. Which user groups has the profile "SAP\_ALL" been assigned to?

---

---

---

10. Which objects are checked when transaction "SM31" is called? What is the meaning of these objects?

---

---

---

11. Which users are authorized to change table "T043"?

---

---

---

12. Has an authorization object, which is checked when transaction SU02 is called, been (partially) deactivated for this transaction?

---

---

---

13. Determine, if the parameter for “general” deactivation of authorization objects has been activated.

---

---

---

14. Are there objects, which are generally excluded from authorization checks?

---

---

---

15. Which tolerance groups have been defined for posting financial accounting documents and which created users have been assigned to tolerance groups?

---

---

---

16. Check the “change documents” for your own user ID.

---

---

---

17. Determine standard display profiles within the system

---

---

---

18. When implementing the AIS system, standard activity groups named “SAP\_CA\_AUDITOR\_XXX” are provided for different audit activities. Determine these activity groups, analyze them (in a sample) regarding their authorization contents and check their documentation.

---

---

---

### **Checklist for system audits (Authorization system)**

- ❑ Mapping the environment
  - Utilized SAP™ modules and processes
  - Utilized company codes
  - Overview of business and administrative user
  - Work place and process description
  - Risk matrix
- ❑ Evaluating the written authorization concept
  - Level of detail and timeliness
  - Commitment
  - Utilizing protection categories and groups
  - Level of aggregation for activity groups and profiles
  - Clearly defined tasks (roles)
  - Considering the requirements for a sufficient internal control system
- ❑ Visual check of users and assigned authorizations
  - Utilizing SAP™ standard profiles
    - for the administration
    - for the business departments
  - Utilizing in-house developed profiles and activity groups
    - described in concept?
    - adhered to naming conventions (descriptive names)?
    - meaningful short descriptions?
    - assignment to proper users?
  - Selecting critical users
    - without authorizations
    - without user groups
    - with group Ids
    - with SAP™ standard profiles
  - Check change documents for conspicuous users and authorizations



- ❑ Contents analysis of selected profiles and activity groups
  - Display authorization with only “display” activities (example)
  - Company code specific authorizations with entries for only the particular company code (example)
  - Restriction to described transactions (S-TCODE)
  - Critical “sub-profiles”
  - Where-used-list of users
  - Sufficient documentation
- ❑ Detailed audit of executable transactions for specific users (samples)
  - Determine critical transactions
  - Determine authorization objects
  - Check general or transaction specific deactivation of objects
  - Determine users
- ❑ Additional checks on critical authorizations
  - Standard reports
    - “Which user is allowed to....”
    - “Critical authorizations”
    - “Critical combinations”
  - Comparisons of (template) users and profiles
  - Check amount authorizations / tolerance groups
- ❑ Summarized statement on the complete authorization system

## **5.7 Critical parameter settings in the SAP™ start-up profiles**

### **5.7.1 Introduction**

The parameter settings in the SAP™ start up profiles are affecting the SAP R/3™ system control in situations relevant to security, protection and compliance. The auditor should pay particular attention to some of the manifold controlling parameters.

Even though some parameter settings and their audit relevancy have already been discussed in this manual, a summarizing overview of audit aspects and recommended settings will be presented in the following sections.

The audit activities can be carried out utilizing report RSPARAM in transaction SA38.

### **5.7.2 Parameters, affecting the processing of financial accounting data**

- Activating automatic supplementary updates

In order to ensure automatic supplementary updates of not yet executed update requests, in cases where an update server needs to be re-started, the parameter "RDISP/VBSTART" should be set to "1".

- No deactivation of the update function

The parameter "RDISP/VB\_STOP\_ACTIVE" can deactivate the update activities. That makes no sense in a production system. The parameter should be set to "0" and not be deactivated.

- Stopping update activities if technical database errors occurs

Database errors can result in accounting data inconsistencies. It is useful to set the parameter "RDISP/AUTO\_VB\_STOP" to "1" in order to ensure an automatic update lock if technical database errors occur.

- Evenly distributed update processes

The SAP™ system offers the option to distribute the system load due to update processes evenly. The parameter "RDISP/VB\_DISPATCHING" has to be set to "1" (recommended).

- Saving unprocessed (erroneous) update requests

The issues connected to update terminations were already discussed in detail. As explained, update requests, which were not transferred to the database remain in the collective file "VBLOG" and are automatically deleted after 50 days, if the system parameter "RDISP/VBDELETE" is set to "50", which is the default setting in the delivered system. The data can not be checked after this period, neither by users in business departments nor by the auditors. The recommended parameter setting "0" deactivates the deleting procedure.

VBLOG is additionally re-organized if an update server is re-started and the parameter "RDISP/VBREORG" is set to "1". In order to deactivate this – unwanted – re-organization, the setting "0" is recommended.

### 5.7.3 **Comprehending transports**

- Ruling out program changes during transports

If changed objects are transferred to a productions system by utilizing the change and transport system, at the same time as programs are being changed, erroneous recordings and inconsistent program statuses can not be ruled out. By setting the parameter "TRANSPORT/DURING\_UPGRADE" to the recommended value "OFF" these situations can be ruled out.

- Activating the logging

The logging of transport activities is controlled by the parameter "TRANSPORT/TP\_LOGGING", which should be set to "ON" in order to ensure compliance with documentation requirements in commercial and tax laws.

### 5.7.4 **Other logs**

- Table changes

The effects of changing table data – in particular if controlling information is changed – and that table data changes should be handled as program changes has already been discussed. The setting of the parameter "REC/CLIENT" must ensure, that such table changes are logged. To do so, the parameter must be set to "000" as well as an entry for the production client.

- Logging critical system activities

By activating the security audit logs critical activities can be tracked in the system. Several parameters have to be set for this purpose:

- RSAU/ENABLE = „1“  
the security audit log is activated.
- RSAU/SELECTION\_SLOTS = „2“  
Recommended value for the number of selection units, which are checked during processing.
- RSAU/MAX\_DISKSPACE/LOCAL = „1.000.000“  
Recommended maximum space for security audit file.
- RSAU/MAX\_DISKSPACE/PER\_DAY = „0“  
Recommended value for the maximum size of all security audit files per day.
- RSAU/MAX\_DISKSPACE/PER\_FILE = „0“  
Recommended value, if only one audit file per day is created

- Documenting remote function calls  
The external activation of SAP™ activities via RFC access is logged if the parameter "STAT/VERSION" is set to the (recommended) value "2".
- Recording daily activities  
Daily activities can be recorded by user and transaction in the so called daily statistics, and be tracked over an extended period of time. This enables the auditor to monitor the utilization of critical transactions, such as SCC4 (client modifiability) continuously. In order to do so, the parameter "STAT/LEVEL" has to be set to the (recommended) value "1".

### 5.7.5 Locking invalid logins

- Invalid login attempts  
With the recommended setting "6" of the parameter "LOGIN/FAILS\_TO\_USER\_LOCK", a user will automatically be locked by the system after six invalid login attempts.
- Automatic release of locked users  
If the parameter "LOGIN/FAILED\_USER\_AUTO\_UNLOCK" is set to "1", the system does not consider users locked due to incorrect login in the previous days. It is recommended not to change the default setting, as nasty user may lock colleagues and administrators on purpose by invalid logins. The report "RSUSR006" should be run on a regular basis though, in order to determine which user IDs were used for failed intrusion attempts.
- Terminating an SAP™ session  
AN SAP™ session is automatically terminated, if the parameter "LOGIN/FAILS\_TO\_SESSION\_END" is set to "3". This default setting should not be changed.
- Dates until password must be changed  
The regular sequence for changing passwords is defined with the parameter "LOGIN/PASSWORD\_EXPIRATION\_TIME". The setting should be set to e.g. "90" days, which should be in accordance with the security policy of the company.
- Controlling the special status of "SAP\*"  
The special status of the standard user "SAP\*", which enables access to the system with extensive authorizations using the password "PASS" after the user ID SAP\* has been deleted, can be deactivated. The parameter "LOGIN/NO\_AUTOMATIC\_USER\_SAPSTAR" is set to "1" (recommended).
- Preventing multiple sessions  
The parameter "LOGIN/DISABLE\_MULTI\_GUI\_LOGIN" disables R/3™ users to log on to multiple sessions in one client, using the same password. The parameter is set to "1".
- Minimum password length  
The minimum password length can be defined with parameter "LOGIN/MIN\_PASSWORD\_LNG". The entry should not be less than "6".

### 5.7.6 Controlling the authorization check

- Storing authorizations in user buffer

The buffering of authorizations in UST\* tables is standardized if the parameter "AUTH/NEW\_BUFFERING" is set to the recommended value "3".

- Number of authorizations in the user buffer

As already explained, the user authorizations are loaded to a user buffer at login. If the user buffer is too small, the system is not able to compare required user authorizations for starting a transaction. The parameter "AUTH/AUTH\_NUMBER\_IN\_USERBUFFER" should have a value of at least "1000", to enable a sufficient number of authorizations to be loaded in the user buffer.

- Switching off authorization checks by transaction

Authorization checks in transaction codes can not be switched off, if the parameter "AUTH/NO\_CHECK\_IN\_SOME\_CASES" is set to the (recommended) value "N".

- General deactivation of authorization objects

The general deactivation of authorization objects can be prohibited, if the parameter "AUTH/OBJECT\_DISABLING\_ACTIVE" is set to the recommended value "N".

- Updating table USOBX

In the already described table USOBX authorization objects and their related values are assigned to specific transactions, which are checked when a transaction is called. The table update, and the resulting performance problems, is not necessary, as the table is delivered by SAP. The default setting "N" of the parameter "AUTH/AUTHORIZATION\_TRACE" should be kept.

- Disabling authorization checks for SU53 and SU56

The transactions SU53 and SU56 for analyzing faulty authorization checks can disable the authorization check with the object "S\_TCODE". In a production environment, there should be no entry for the profile parameter "AUTH/TCODES\_NOT\_CHECKED" (authorization check is not deactivated).

- Including ABAP/4 language elements in the authorization check

The SAP<sup>TM</sup> system enables the deactivation of authorization checks for certain ABAP/4 language elements. This makes no sense from an auditor's point of view, and the parameter "AUTH/SYSTEM\_ACCESS\_CHECK\_OFF" should be set to "0" (active authorization check).

- Extensive authorization checks of remote-function-calls

An extensive authorization check of remote-function call system access for all users, including the functional group "SRFC", requires the parameter "AUTH/RFC\_AUTHORITY\_CHECK" – as opposed to the default value – to be set to "9".

### 5.7.7 Tools for auditing parameter settings

Purpose	Transaction/function	Tables and programs
Checking parameter settings	SA38	RSPARAM

### Notes:

[illegible]

### Exercises on checking parameter settings

- 1 Determine the minimum password length for the system to be audited.

---

---

---

- 2 Determine if the user "SAP\*" has a special status in the system.

---

---

---

- 3 Check the number of authorities in the user buffer.

---

---

---

- 4 Determine how many days the log records resulting from update terminations remain in the VBLOG.

---

---

---

- 5 Determine if technical database errors result in an automatic update lock.

---

---

---

- 6 Check if transports are properly logged.

---

---

---



**Checklist for system audits**  
**(parameter setting in the SAP™ start-up profile)**

Parameter	Recommended value	Default value	Checked value
auth/auth_number_in_userbuffer	1000	2000	
auth/authorization_trace	N	N	
auth/check/calltransaction	2	2	
auth/new_buffering	3	3	
auth/no_check_in_some_cases	N	Y	
auth/object_disabling_active	N	Y	
auth/rfc_authority_check	9	1	
auth/system_access_check_off	0	0	
auth/tcodes_not_checked	No entry	No entry	
auth/test_mode	N	N	
login/disable_multi_gui_login	1	0	
login/failed_user_auto_unlock	1	1	
login/fails_to_session_end	3	3	
login/fails_to_user_lock	7	12	
login/min_password_lng	6	3	
login/no_automatic_user_sapstar	1	0	
login/password_expiration_time	90	0	
rdisp/auto_vb_stop	1	1	
rdisp/vb_stop_active	0	1	
rdisp/vbdelete	0	50	
rdisp/vbmail	1	1	
rdisp/vbreorg	0	1	
rdisp/vbstart	1	1	
rec/client	000, (and prod client)	OFF	
rsau/enable	1	0	
rsau/max_diskspace/local	1000000	1000000	
rsau/max_diskspace/per_day	0	0	
rsau/max_diskspace/per_file	0	0	
rsau/selection_slots	2	2	
stat/level	1	1	
stat/version	2	2	
transport/during_upgrade	OFF	OFF	
Transport/tp_logging	ON	ON	

## **5.8      *Selected audit activities related to program development and maintenance***

### **5.8.1    *Introduction***

Compliance, protection and security in the SAP R/3™ system is only ensured, if it is also ensured that no development work is carried out in the production environment and that the duties in this activity area are strictly segregated. Work for development and test purposes have to be carried out in a provided development and test environment. Otherwise, there is a continuous risk of

- System manipulation
- Data integrity being affected by test procedures
- Changing procedures not being documented and recorded in a change history, as legally required

This applies to standard programs delivered by SAP as well as in-house developments, created by utilizing the SAP™ programming language, even if the programs are only generating information for reporting purposes.

There are several mechanisms in the SAP™ system in order to ensure that the security requirements are met. Changing SAP™ standard programs requires a so called “development key”, and a specified program release by SAP™. A differentiated assignment of authorizations by the authorization administration ensures, that changes and developments in the system and organization programming can only be carried out in the development environment, where they are tested in order to be transferred to the production environment in a pre-defined manner. The presented appropriate system parameter settings are additional measures for protecting the production client from changes.

Changes and in-house developments should only be requested in accordance with a defined written procedure, stating at least:

- Comprehensible description of the requested change
- Purpose and effect of the change
- Time frame (temporary or permanent) of the change
- Listing of affected departments and SAP™ processes
- Approval by the business department responsible for the data
- Estimated costs

Changes and in-house developments should additionally only be carried out based on a pre-defined binding programming guideline in writing and in accordance with the rules stated in the SAP<sup>TM</sup> standard manual, including defined naming conventions. The completed changes can be transported to the production environment by a responsible person, independent from the programming, after successful tests and with required documentation. The complete procedure has to be comprehensible. The changes and in-house developments require sufficient documentation and the outdated configurations have to be saved.

During the basic SAP R/3<sup>TM</sup> system audit, the auditor is responsible for ensuring that the company has established presented procedures for changes and in-house developments and complies with these.

### 5.8.2 *Change and transport system*

The SAP R/3<sup>TM</sup> system supports the described segregation of duties and the related saving of outdated configurations with an automated procedure, the so-called change and transport system.

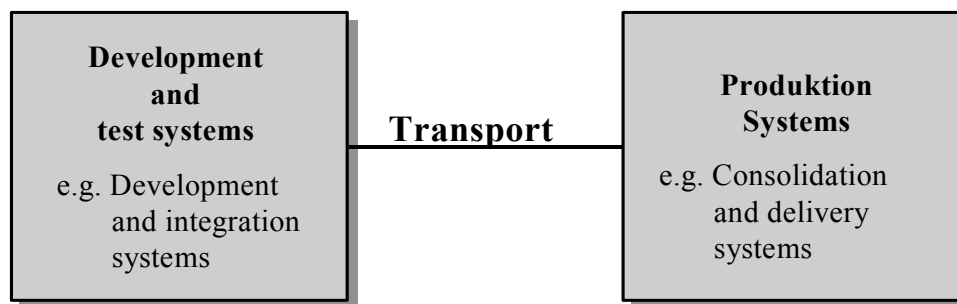


Figure 231: Two connected SAP<sup>TM</sup> systems with different purposes

The change and transport system includes the workbench organizer (WBO) and provides an uniform development environment (workbench). All objects related to a program changes, such as executable programs, tables, screens and developers with segregated duties, can be gathered in one development class. The class is then processed by the responsible program author.

An extensive change includes several object classes, which are put together as a task. The task is the smallest organizational unit in the change and transport system. Staff assigned to a task can process all related object classes. Objects to be changed, authorized staff and transport routes from the development to the production environment are defined within the organizational units object class and task. Completed changes are requested to be transported, as soon as the change has been completed, tested and released for utilization in the production system. The transport system transports the request to the production system in a defined and comprehensible manner and logs the completed object changes. The objects can be reviewed, compared to outdated configurations and re-created any time. Without going into further details of the rather complex change and transport system, the six major tables for ensuring proper functions should be mentioned

- TSYST list of and transports to available R/3™ systems
- TASYM defining system to be changed
- TWSYS defining (specific) transport routes for changes from the development system to the system to be changed
- DEVL defining general transport routes from the test environment to the production environment
- TDEVC creating development classes
- TADIR list of all objects with information on name, class, date of change etc

Unauthorized tampering with these tables may have severe consequences for compliance procedures. During the authorization audit, the auditor has to make sure that the listed tables have been assigned to privileged table classes and can be maintained only by the responsible administrative staff.

The utilization of the change and transport system is protected by the protective authorization objects "S\_TRNSPRT" and "S\_CTS\_ADMI". The objects have the following standard authorizations:

S_CTS_ALL	✓	All Auths: Request Administration and Corr./Transport
S_CTS_DEVELO	✓	Developers, only tasks can be edited (CTS)
S_CTS_PDORDER	✓	Authorization for developers in P systems (request level)
S_CTS_PDTASK	✓	Authorization for developers in P systems (task level)
S_CTS_PIECLS	✓	Edit Object Lists (Change and Transport System)
S_CTS_PPORDER	✓	Authorization for persons resp. for P systems (request level)
S_CTS_PPTASK	✓	Authorization for persons resp. for P systems (task level)
S_CTS_PQORDER	✓	Authorization for Q team members in P systems (req. level)
S_CTS_PQTASK	✓	Authorization for Q team members in P systems (task level)
S_CTS_PROJEC	✓	Project Leader (Change & Transport System)
S_CTS_SHOW	✓	Display authorization in Change and Transport System
S_CTS_TR_ALL	✓	All authorizations for requests and tasks (CTS)

Figure 232: Standard authorizations for authorization object "S\_TRNSPRT"

The extensive authorization "S\_CTS\_ALL" should be assigned only to an emergency user in a production system. The authorization "S\_CTS\_TR\_ALL" should also be assigned restrictively. Developer and project managers usually do not require these authorizations. Finally, the auditor should determine if changes can be made directly in the production environment. This should be checked in client "000". If the setting for system modifiability (transaction SE06) is "modifiable", the change and transport system can not fulfill its purpose as required by the auditor.

### 5.8.3 ABAP/4™ programming authorization

The risks related to ABAP/4™ programming authorizations in the production environment have already been discussed. Such programs can be ruled out in the production environment by assigning authorizations. Development work and the necessary tools are basically protected by the following authorization objects.

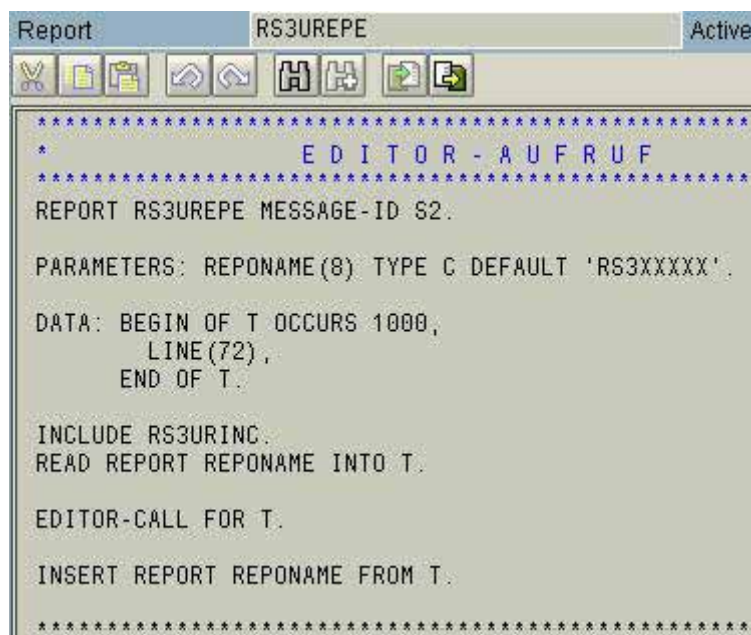
- S\_PROGRAM starting ABAP/4™ programs (SUBMIT) and maintaining related program attributes
- S\_DEVELOP calling and utilizing the development environment

Critical situations occur when developers have change authorization for the authorization object S\_DEVELOP in the production environment and at the same time can start changed programs (authorization "SUBMIT" for the authorization object S\_PROGRAM).

An entry "DEBUG" in the field object type and "02" in the field activity for the authorization object S\_DEVELOP brings a risk of changes to the main storage, which are not documented. SAP™ recommends only system administrators and the EARLYWATCH user to have authorization for the authorization object S\_DEVELOP in the production system. For the EARLYWATCH user the object type "SYST" and activity "03" have to be entered.

### 5.8.4 Backdoor o programming authorization

The standard program "RS3UREPE" for migration purposes is implemented in every SAP™ system, and can be utilized for opening reports in the R/3™ editor in order to process them.



```

Report      RS3UREPE      Active
*****
*                               EDITOR - AUFRUF
*****
REPORT RS3UREPE MESSAGE-ID S2.

PARAMETERS: REPONAME(8) TYPE C DEFAULT 'RS3XXXXX'.

DATA: BEGIN OF T OCCURS 1000,
       LINE(72),
     END OF T.

INCLUDE RS3URING.
READ REPORT REPONAME INTO T.

EDITOR-CALL FOR T.

INSERT REPORT REPONAME FROM T.
*****

```

Figure 233: Source code of report "RS3UREPE"

The program can be executed only by "authorized" users. The authorization check is done in another report "RS3URINC", managed as INCLUDE. The reports lists the names of the authorized users in a readable format.

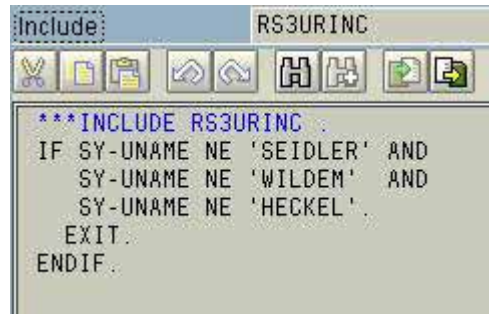


Figure 234: "Neutralized" source code for RS3URINC

If somebody is able to login with a listed user ID, or create one, he will obtain extensive development authorizations in the production environment.

The auditor should determine if changes were carried out with the readable names in the report "RS3URINC" in the past. If so, he should inquire about the reasons.

#### 5.8.5 Tools for auditing program development

Purpose	Transaction/function	Tables	Programs
Mapping available systems	AIS + Transport management system  SE16 and tables  STMS	TSYST TASYS TWSYS  DEVL TDEVL TADIR	
System modifiability	AIS + Transport management system  SE06		
Tables and authorization objects	AIS + table recordings  SE16 and tables	TBRG TDDAT	
Checking selected authorizations	AIS + Information system users and authorizations (user, by complex search criteria)  SA38 and program		RSUSR050
Check utilization of readable names in report RSURINC for changes	SE16 and table (selecting readable names)	TRDIR	

### Exercises on auditing program maintenance

1. Check if there is a separate program development environment in the SAP<sup>TM</sup> group

---

---

---

2. Are the tables TSYST and DEVL assigned to specified authorization groups?

---

---

---

3. Who can change the two tables?

---

---

---

4. Do users in the production environment have the SAP<sup>TM</sup> standard profiles "S\_CTS\_XXX"?

---

---

---

5. Can users in the production system change the main storage (without audit trail)?

---

---

---

6. Check if transports are properly logged.

---

---

---



**Checklist for system audits  
(auditing program developments)**

- ☐ Mapping the environment
  - Separate development and test environments?
  - Development and test guidelines in place?
  - Job descriptions for developers in place?
  - Request procedure for in-house developments in place?
  
- ☐ Assessing the listed documentation
  - Level of detail and timeliness
  - Binding character
  - Completeness and clarity
  
- ☐ Protection of important tables
  - TSYST, TASYs, TWSYS, DEVL, TDEVc, TADIR
  - Utilizing authorization groups
  - Logging ensured
  - Who has change authorizations?
  
- ☐ Protecting the change and transport system from unauthorized access
  - Who has authorization for the objects "S\_TRNSPRT" and "S\_CTS\_ADMI"?
  - Who has the SAP™ standard authorization "S\_CTS\_XXX"?
  
- ☐ Who has development authorization in the production system
  - Authorization for the objects "S\_PROGRAM" and "S\_DEVELOP"
  - Who can change the main storage (DEBUG with activity "02" in S\_DEVELOP)?
  
- ☐ Is the program "RS3UREPE" available?
  - How is it protected?
  - Which readable names are listed in "RS3URINC"?
  - Were changes carried out with these readable names?

## **5.8 Tracking critical master record changes**

### **5.9.1 Creating and logging master records**

The SAP R/3™ system is processing master record information in posting documents during automated accounting procedures on a regular basis. The major part of the master records and in particular their changes regard information, which has to be archived according to commercial and tax laws.

The creation and changes of important master records can be restricted to certain transactions and company codes. The commonly used restrictions by transaction for specific work areas are summarizing these in field groups such as

- maintaining vendor / accounts payable master data by purchasing
- maintaining vendor / accounts payable master data by financial accounting

which users can select when calling the transaction. Transaction oriented field groups is one element of purposeful segregation of duties. Maintaining and changing the field groups is a customizing task, resulting in entries in the following tables

- T078D Screen selection - customers
- T078K Screen selection - vendors
- T078S Screen selection - general ledger
- T078W Screen selection - plant master records

The related tables for field groups assigned to company codes have the same systematic names in the area "T079\*".

The entries in the tables above decide which master records changes are based on transactions and table access should be assigned with great restriction in the production system. Therefore - as already explained in this manual - the auditor should determine if

- the tables have been assigned to privileged table classes
- only few users have access to the privileged table classes
- table changes for the tables above are logged

Table "TBAER" (rules for changing documents) is based on fields and just as important, defining which changes can be made (and under what circumstances) to already processed documents in the SAP R/3™ system. Here too, compliance aspects are affected, which requires an audit of the table protection in a production system.

### 5.9.2 Auditing table protection

The presented checks can be carried out utilizing the AIS menu. They include the following steps:

- ❑ Determine the authorization group for presented tables

In the AIS menu

system audit

repository/tables

table authorization

assignment of authorization groups to tables/views

(transaction SE16 and table "TDDAT") an overview of tables and the assigned authorization groups can be created.

Table	Authorization group	
<input type="checkbox"/> T078D	FB02	FI: Basis tables
<input type="checkbox"/> T078K	FB02	FI: Basis tables
<input type="checkbox"/> T078S	FB02	FI: Basis tables
<input type="checkbox"/> T078W	WC	ML: User control
<input type="checkbox"/> T079D	FB02	FI: Basis tables
<input type="checkbox"/> T079K	FB02	FI: Basis tables
<input type="checkbox"/> T079M	FB02	FI: Basis tables
<input type="checkbox"/> T079V	FS	FI: SAP control

Figure 235: Display of tables and assigned authorizations

In the screen display above, specified tables can be selected in the menu

Selection criteria

by contents

by marking "table name". The next selection screen

Conn.	Field description	Co	Field contents
<input type="checkbox"/>	Table name	=>	T078*

Buttons: Confirm, Choose, Append, [Help], [Delete], [Print]

Figure 236: Specified selection of tables for checking assigned authorization groups

enables the direct display of the selected table and the assigned authorization groups. The overview should be printed.

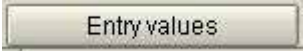
❑ Determine users with authorizations for presented table authorization groups

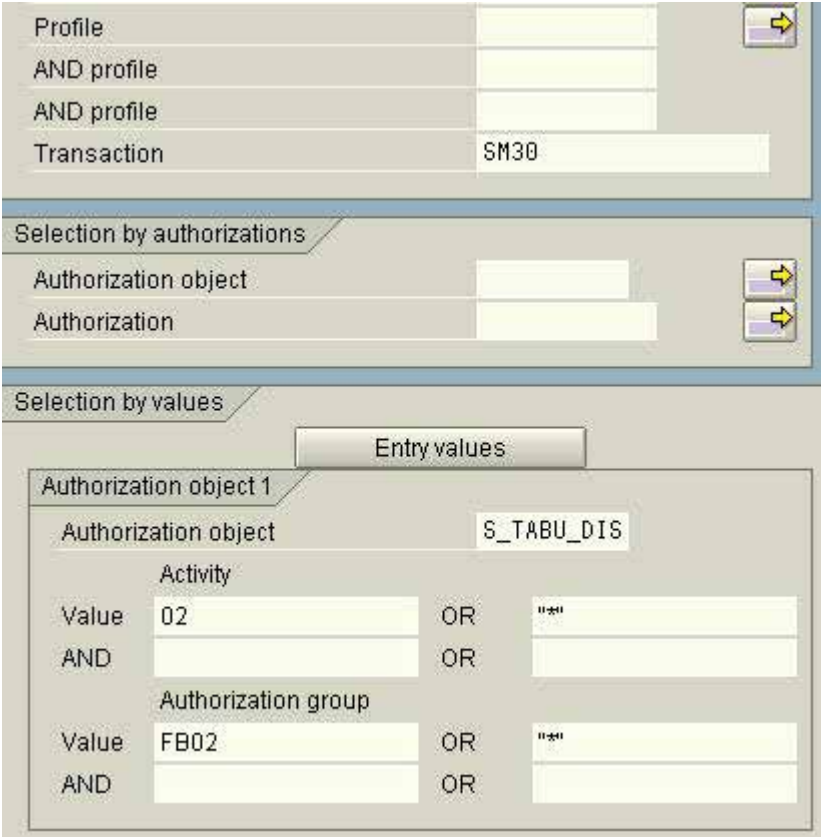
Determining users with maintenance authorization for the presented tables is a part of the authorization audit which has been discussed in detail. The tables can be maintained by users with

- authorization for transaction SM30 and
- authorization with changing activity of the authorization object "S\_TABU\_DIS"

for the stated authorization groups. The menu for the authorization audit is

system audit  
user administration  
information systems users and authorizations  
user  
by complex search criteria

"SM30" has to be entered in the field "transaction". In the section "selection by values" the authorization object "S\_TABU\_DIS" is entered. The entry screen is expanded for the related object with the button "entry values"  The values in the figure below are entered.



Profile			
AND profile			
AND profile			
Transaction	SM30		

**Selection by authorizations**

Authorization object			
Authorization			

**Selection by values**

**Entry values**

**Authorization object 1**

Authorization object				S_TABU_DIS	
Activity					
Value	02	OR			
AND		OR			
Authorization group					
Value	FB02	OR			
AND		OR			

Figure 237: Entering activities and authorization groups for the object "S\_TABU\_DIS"

In a final step the report is started. As a result all users with authorization to change the presented table will be displayed.

**5.9.3    Logging table changes**

Table changes have to be logged and filed with other documentation with archiving requirements. SAP supports the automatic logging if

- it is has been set up in the start-up profiles
- the log filed has been activated in specific tables

Both is to be checked for the presented tables. The procedure and the available tools were discussed in detail in section 5.3.5.3.2 "logging data changes", to which we refer.

**5.9.4    Reports on master record change logs**

In order to audit master record changes the auditor can call the reports

- RFSABL00    display changes to general ledger accounts
- RFBABL00    display of changed documents
- RFDKLIABdisplay changes to credit management
- RFBKABL0    display of bank changes
- RFDABL00    display changes to customers
- RFKABL00    display changes to vendors

with the menu

system  
services  
reporting

Time	Vendor	Changed by	Field name	CoCd	PuOr	New value	Old value
Other keys							

**Figure 238: Display of changes to vendor master records**

The AIS system offers several additional possibilities within the "business audit" for analyzing master records changes related to the balance sheet.



### Exercises on auditing master record changes

1. Which authorization groups have tables "T078\*" been assigned to?

---

---

---

---

2. Determine which users have change authorization for the tables.

---

---

---

---

3. Have the tables been set to be logged?

---

---

---

---

4. Check if company code specific data, such as vendor bank information, was changed during the last year.

---

---

---

---



### **Checklist for system audits (master record changes)**

- ☐ Mapping the environment
  - Procedures for changing master records
  - Responsibilities
  - Rules for accessing critical tables
  - Procedure for tracking critical changes of master records in the company
  
- ☐ Controlling tables for field group selection and for document change rules
  - Assignment to authorization groups
  - Logging specific tables
  - Logging parameter "rec/client"
  - Change authorization for listed tables
  
- ☐ Logging critical changes of master records
  - Changing company code data for
    - customers
    - vendors
  - Changing general ledger master records
  - Changing bank master records
  - Changes by authorized staff?

## **5.10 Setting up and processing automated program flows (jobs)**

### **5.10.1 Introduction**

There are several areas for utilizing automated flows (jobs) within the SAP R/3™ environment. These include

- allocating data processing (such as dunning or payments) to times of low system load (no dialogs)
- automated processing of data, transferred to the SAP™ system from other or sub systems
- processing created work queues
- running periodic reconciliation and control procedures
- automated processes for monitoring the complete SAP R/3™ system, etc

The set up of jobs used to be an area reserved for IT administrators, which in large parts was transferred to the user departments as SAP R/3™ was implemented. Proficient users with the required authorizations are now able to set up, schedule and start jobs, i.e. running several - possibly not related – programs, independent of administrators.

Audit aspects demand absolute adherence to the requirements for company data protection and compliance. This means in particular

- smooth job processing
- ensuring smooth job processing with tested mechanisms even if errors occur
- comprehensible procedures for detailed job control
- archiving of required job logs according to laws and regulations

Possible sources of errors, possibly affecting the stated requirements, usually result from lack of user knowledge. Jobs which have been set up or put together improperly result in an increased system load and are not processed correctly or are incomplete. The scheduled time frames are not sufficient for processing the job properly, which means other users can not access the required operative data. Erroneously finished jobs are not handled properly by the users, which has negative effects on the subsequent processing of business transactions and programs. The auditor should obtain information about the quality of job processing.

### **5.10.2 Auditing the job processing**

#### **5.10.2.1 Defined job concept in writing**

Just as a written concept is required for program development it is also required for putting together, scheduling and setting up jobs in the operation processes.

The following should be defined in the concept:

❑ **Procedure for job requests**

It should be defined who can request complex jobs. With whom and according to which criteria are jobs to be co-ordinated with the administrators. It should also be defined which training users should have in order to set up jobs.

❑ **Job monitoring**

It should be defined who is responsible for releasing generated jobs and who deals with the continuous monitoring of jobs running without errors. The procedure for erroneous jobs should also be defined, e.g. cancellation of jobs which are critical to the company. Further is to define which logs (and in which format) have to be archived in order to comply with the requirements of commercial and tax laws.

❑ **Documentation requirements**

A competent third party must be able to comprehend the basics of every job run within an acceptable time frame. Additionally, it is important for the user department and for the administration to obtain a detailed overview of the job contents and structure, of the conditions for proper processing, required information prior to the run and how to handle errors. This requires detailed documentation of each job, stating at least the following:

- who is responsible for the job
- description of business purpose and contents
- involved programs
- required parameters prior to the run
- timely and hierarchic processing of other involved programs
- handling of errors

A sample of the listed written documents should be reviewed regarding level of detail, completeness and timeliness.

#### **5.10.2.2 Auditing in the SAP R/3™ system**

A comprehensive overview of the scheduled and finished jobs can be created in the AIS menu

system audit

background processing

job overview

(transaction SM37).

- 244 -

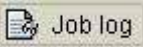
Figure 239: Selection screen for creating a job overview

After entering the selection criteria, the auditor obtains an overview of scheduled and finished jobs and all status information.

JobName	Ln	Job CreatedBy	Status	Start date	Start time	Duration(sec.)
AUTO_SESSION_MANAGER		BRAUN	Released			0
COLLECTOR_FOR_PERFORMANCEMONITOR		DDIC	Released			0
COLLECTOR_FOR_PERFORMANCEMONITOR		DDIC	Finished	10.12.2002	00:49:03	3
COLLECTOR_FOR_PERFORMANCEMONITOR		DDIC	Finished	10.12.2002	01:49:03	2
COLLECTOR_FOR_PERFORMANCEMONITOR		DDIC	Finished	10.12.2002	02:49:03	1
COLLECTOR_FOR_PERFORMANCEMONITOR		DDIC	Finished	10.12.2002	03:49:03	305
COLLECTOR_FOR_PERFORMANCEMONITOR		DDIC	Finished	10.12.2002	04:49:03	2
COLLECTOR_FOR_PERFORMANCEMONITOR		DDIC	Finished	10.12.2002	05:49:03	0
COLLECTOR_FOR_PERFORMANCEMONITOR		DDIC	Finished	10.12.2002	06:49:03	212
COLLECTOR_FOR_PERFORMANCEMONITOR		DDIC	Finished	10.12.2002	07:49:03	203

Figure 240: Calling a summarized job overview


The auditor should note who created the job and if there are jobs with the status "canceled".

The log file can be displayed with the button "job-log" .

Job log overview for job: COLLECTOR\_FOR\_PERFORMANCEMONITOR

Date	Time	Message content
10.12.2002	00:49:03	Job started
10.12.2002	00:49:03	Step 001 started (program RSCOLL00, variant , user name DDIC)
10.12.2002	00:49:06	Job finished

Figure 241: Selected job-log

Details on a conspicuous job, like which programs and job steps were summarized in the job or which conditions have to be fulfilled for starting the job, can be displayed with the button "display and compare jobs" .

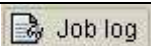

Display Job Tree

Selected jobs
COLLECTOR_FOR_PERFORMANCEMONIT
General job information
Job class:A
Status:Finished
Tgt server:CMDHP3_146_33
WP no. /PID: 9/0000000441
Job steps
0001 -ABAP program:RSCOLL00
Job start conditions
Date/Time--20021210/004854

Figure 242: Display of job details

The listed information should be printed for the work papers. Then the auditor can inquire how specific situations were handled.

### 5.10.3 Tools for job control

Purpose	Transaction/function	Tables	Programs
Checking job procedures	Written documentation		
Overview of scheduled and finished jobs	AIS + background processing SM37		
Details on jobs and job logs	Buttons  		

### Exercises on job control

- 1 Create an overview of finished and canceled jobs

---

---

---

---

- 2 Determine who started the jobs

---

---

---

---

- 3 Analyze the sources of error for canceled jobs based on the job logs

---

---

---

---

### Checklist for system audits (job control)

- ☐ **Review the written procedures**
  - Procedure for job requests
  - Procedure for monitoring and controlling jobs
  - Procedure for job documentation
  - Contents and level of detail
  - Comprehensiveness and timeliness
- ☐ **Check a sample of the procedures**
  - Who starts jobs?
  - Handling of errors
- ☐ **Archiving the job logs**
  - According to laws and regulations
  - Archiving procedure

## **5.11 Checking the batch input procedure**

### **5.11.1 Introduction to the batch input procedure**

The data from sub systems to the SAP<sup>TM</sup> financial accounting is transferred via so called batch input interfaces. The sub system transfers the data to an SAP<sup>TM</sup> interface program, which automatically transforms the data into a transaction format in sessions. The data is automatically transferred in the system, analogous to a dialog process. The program also carries out the same plausibility and authorization checks, which would have been carried out in a dialog transaction operation. Incorrect data records are rejected and remain in so called incorrect sessions until they are further processed by the user.

In order to ensure data security and integrity as well as proper operation, including complete and timely data processing, the following should be considered

- only authorized staff can initiate the batch input process and change the sessions
- incorrect sessions are processed on a timely basis
- the quantity and value of data transferred via interface is reconciled to the sub systems

### **5.11.2 Auditing established procedures**

There are several sources of errors in cases where batch input procedures are utilized improperly. A clear written procedure is required for the user department and the auditor in order to ensure transparency and avoid such errors.

This includes:

#### **❑ Mapping batch input interfaces**

The origin of the data must be recognizable in all cases. The sub system must be described as well as the data to be transferred via this interface. Possible data formats resulting from the interface processing must be presented. The required information for identifying the processed batch is also to be stated, such as

- file name
- session name
- transfer frequency and timing
- processing program

#### **❑ Reconciling procedures**

The procedures for reconciling accounting data and control totals have to be described for each interface and the related batch input sessions.



❑ Responsibilities and authorizations

The responsibilities for the complete data transfer process and specific related tasks should be defined.

The level of detail, clarity and timeliness of the written procedures should be reviewed. After that, the realization of the procedure can be checked in a sample in the system.

5.11.3 Auditing the batch input procedure in the SAP R/3™ system

The audit can be carried out in the AIS™ system menu

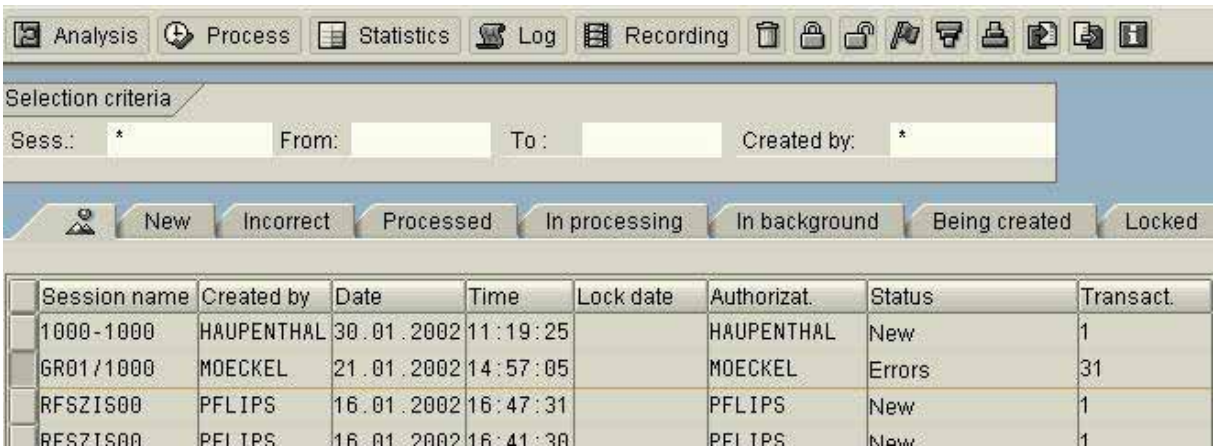
system audit

background processing

batch input logs

(transaction SM35)

The generated overview displays all transferred sessions via a specified interface during a selected period.



The screenshot shows the SAP SM35 transaction interface. At the top, there is a menu bar with icons for Analysis, Process, Statistics, Log, Recording, and other functions. Below the menu bar is a 'Selection criteria' section with fields for 'Sess.: \*', 'From:', 'To:', and 'Created by: \*'. Below this is a tabbed interface with tabs for 'New', 'Incorrect', 'Processed', 'In processing', 'In background', 'Being created', and 'Locked'. The 'New' tab is selected, and a table of sessions is displayed below it.

Session name	Created by	Date	Time	Lock date	Authorizat.	Status	Transact.
1000-1000	HAUPENTHAL	30.01.2002	11:19:25		HAUPENTHAL	New	1
GR01/1000	MOECKEL	21.01.2002	14:57:05		MOECKEL	Errors	31
RFSZIS00	PFLIPS	16.01.2002	16:47:31		PFLIPS	New	1
RFSZIS00	PFLIPS	16.01.2002	16:41:30		PFLIPS	New	1

Figure 243: Overview of processing of batch input sessions

Checking compliance with the established procedure should include how incorrect sessions are handled. These can be called with the flag "incorrect".



The screenshot shows the SAP SM35 transaction interface, similar to Figure 243, but with the 'Incorrect' tab selected. The table below the tabs shows sessions that are marked as 'Incorrect'.

Session name	Created by	Date	Time	Lock date	Authorizat.	Transact.	Screens	D.	Queue
/1000-1000	HAUPENTHAL	30.01.2002	11:19:26		HAUPENTHAL	1	3	X	02013
GR01/1000	MOECKEL	21.01.2002	14:57:05		MOECKEL	31	62	X	02012

Figure 244: Remaining incorrect sessions in the system

Detailed information can be obtained by marking a session and clicking the button "analysis"

 Analysis This enables for example an overview of incorrect transactions in the session.

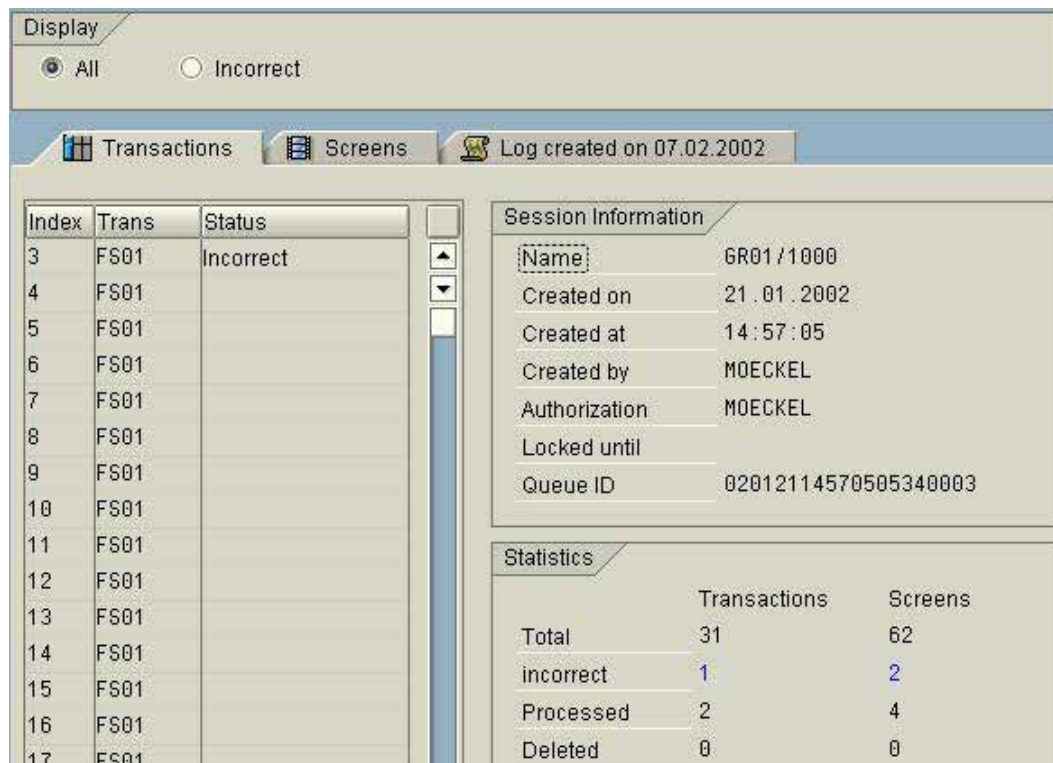


Figure 245: Overview of incorrect transactions in an incorrect session

The flag "log created on...." in the upper screen enables further details analysis of the incorrect transactions.

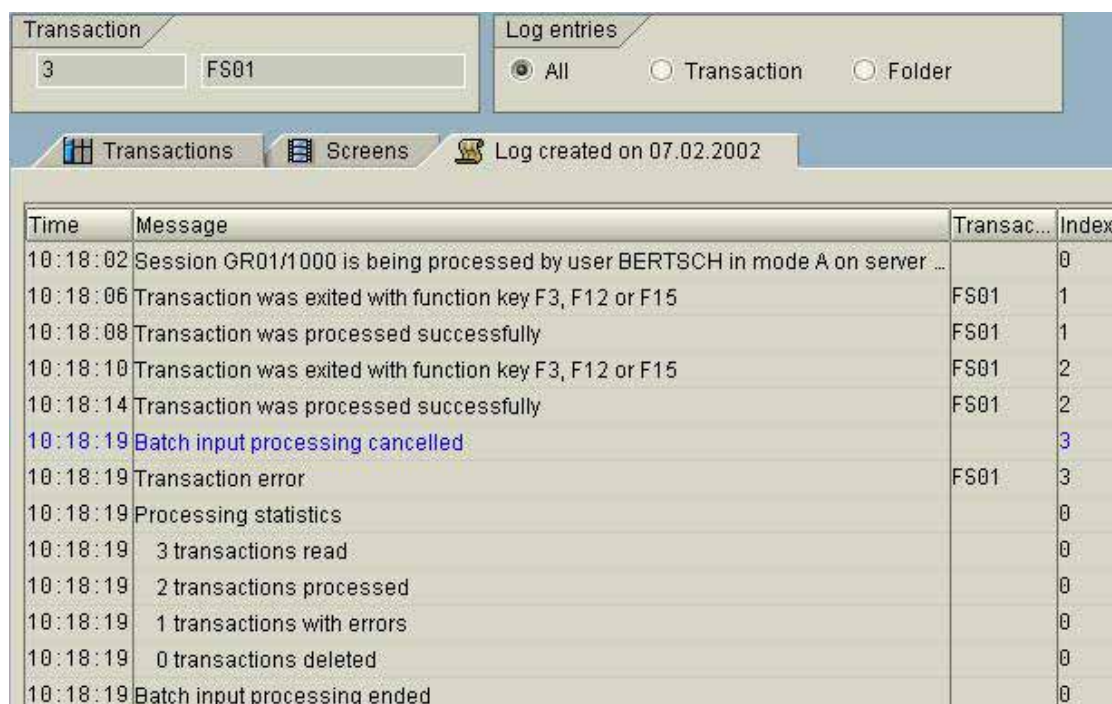


Figure 246: Detailed error analysis in an incorrect session

Based on a sample of incorrect sessions, the auditor can determine if the responsible person is able to correct errors. Additionally, it should be determined if the incorrect sessions are checked on a timely basis and if subsequent processes are based on completely processed accounting data in all cases.

#### 5.11.4 Checking sufficient segregation of duties for processing sessions


The general user access for business department staff to batch input sessions is controlled by the authorization object S\_BDC\_MONI. The related activities include

- Process sessions in dialog mode AONL
- Pass on sessions to background processing ABTC
- Analyze sessions and logs ANAL
- delete sessions DELE
- lock and release sessions LOCK
- release sessions FREE
- reorganize session and logs REOG

The activities can be limited to specified sessions by user specific naming of the sessions.

During the authorization audit, the auditor should utilize presented tools in order to make sure that no user in the system has access to all sessions with every activity.

#### 5.11.5 Tools for auditing the batch input procedure

Purpose	Transaction/function	Tables	Programs
Describing the batch input procedure	Written company documentation		
Overview of saved sessions	AIS + background processing SM35		
Analyzing incorrect sessions	Flag "incorrect"  Analysis Button flag "log created on ...."		
Checking session authorizations	AIS + Information system users and authorizations (complex search criteria) for object S_BDC_MONI SA38 and program		RSUSR050

### Exercises on batch input procedures

- 1 List the minimum requirements on the contents of an interface description.

---

---

---

---

- 2 Create an overview of incorrectly processed sessions.

---

---

---

---

- 3 Determine the number of incorrect and properly transferred transactions in an incorrect session. Which transactions were incorrect and what was the purpose of these transactions.

---

---

---

---

- 4 Determine the authorization object for the session processing.

---

---

---

---

- 5 Which users have extensive authorizations for processing all session activities?

---

---

---

---

### **Checklist for system audits (Batch input procedure)**

#### ☐ **Mapping the procedure**

- interface overview
- detailed interface description
- overview of reconciliation procedures
- description of specific sessions
- overview of responsibilities
- description of error handling

#### ☐ **Overview of processed folders**

- list of incorrect sessions
- detailed analysis in a sample
  - which sessions
  - responsibility
  - nature of error
  - error handling
  - timely processing

#### ☐ **Authorizations for responsible users**

- restricted to specified sessions?
- user with extensive session authorizations
- proper segregation of duties?

## 5.12 Data protection of personnel related data

### 5.12.1 Introduction

The legal requirements on data protection of personnel related data and on logging the utilization and transfer of such data are very strict. This concerns almost all employee data, processed for employee administration and payroll in the HR-module. Customer and vendor data is also regarded as personnel related data, if natural persons are concerned. User IDs in the SAP<sup>TM</sup> system are personnel related data as well, and have to be treated according to legal requirements on data protection.

The AIS<sup>TM</sup> system provides a separate section for audits to be carried out for data protection purposes,

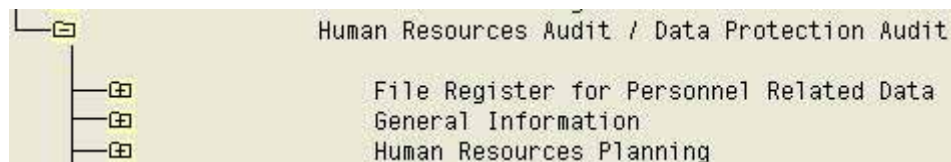


Figure 247: Reporting functions for data protection audits

which provides all necessary functions for carrying out such audits. However, these functions are useful for IT audit purposes as well and should be reviewed during the basic system audit.

### 5.12.2 File register for personnel related data

According to data protection laws, the company has an obligation to keep a register with files and tables for saved personnel related data. With the functions below

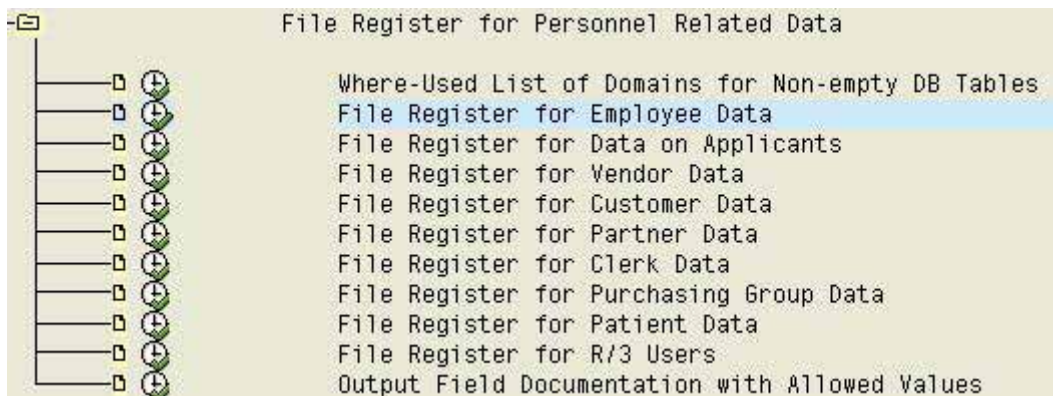


Figure 248: Overview of file register for personnel related data

the auditor can obtain a table overview by topic.



System	I46	Client	800	Created by	RV_BENU4	Date	10.12.2002
Domains							
I EQ PERSNO							
Personnel number							
Only tables that are not empty							
<div><div>Table</div><div>Short text</div><div>Field name</div><div>Key</div><div>Short text</div></div>							
<div><div>PA0000</div><div>HR Master Record: Infotype 0000 (Actions)</div></div>							
<div><div>PA0001</div><div>HR Master Record: Infotype 0001 (Org. Assignment)</div></div>							
<div><div>PA0002</div><div>HR Master Record: Infotype 0002 (Personal Data)</div></div>							
<div><div>PA0003</div><div>HR Master Record: Infotype 0003 (Payroll Status)</div></div>							
<div><div>PA0004</div><div>HR Master Record: Infotype 0004 (Challenge)</div></div>							
<div><div>PA0005</div><div>HR Master Record: Infotype 0005 (Leave Entitlement)</div></div>							
<div><div>PA0006</div><div>HR Master Record: Infotype 0006 (Addresses)</div></div>							

Figure 249: Overview of tables with personnel related data

Based on this overview, the auditor can check the access protection for these tables in a sample, by determining their assignment to protection classes and comparing the access authorizations for the protection classes.

A rather interesting function is revealed by clicking the button "output field documentation with allowed values", which provides documentation on input options for every field in a selected table.

System	I46	Client	800	Created by	RV_BENU4	Date	10.12.2002
Domains							
I EQ PERSNO							
Personnel number							
Only tables that are not empty							
<div><div>Table</div><div>Short text</div><div>Field name</div><div>Key</div><div>Short text</div></div>							
<div><div>PA0000</div><div>HR Master Record: Infotype 0000 (Actions)</div></div>							
MANDT	X	Client		MANDT		MANDT	C
PERNR	X	Personnel number		PERSNO		PERSNO	N
SUBTY	X	Subtype		SUBTY		SUBTY	C
OBJPS	X	Object identification		OBJPS		OBJPS	C
SPRPS	X	Lock indicator for HR master record		SPRPS		SPRPS	C
ENDDA	X	End Date		ENDDA		DATUM	D
BEGDA	X	Start date		BEGDA		DATUM	D

Figure 250: Field documentation for table T047T



### 5.12.3 Human resources planning

As far as the HR-module is utilized for organizational management, task related functions can be created in a pre-defined role structure and authorizations can be assigned accordingly. An overview and information on personnel related data is displayed in related functions, and can be called by specific users.

### 5.12.4 Personnel administration

Table fields with personnel related data are grouped in info types and sub types. This enables very differentiated authorization checks down to field level and only authorizations specifically defined for their tasks can be assigned to the staff in human resources.

By clicking the button "info types" a log with an overview of the separate info types and related descriptions can be created.

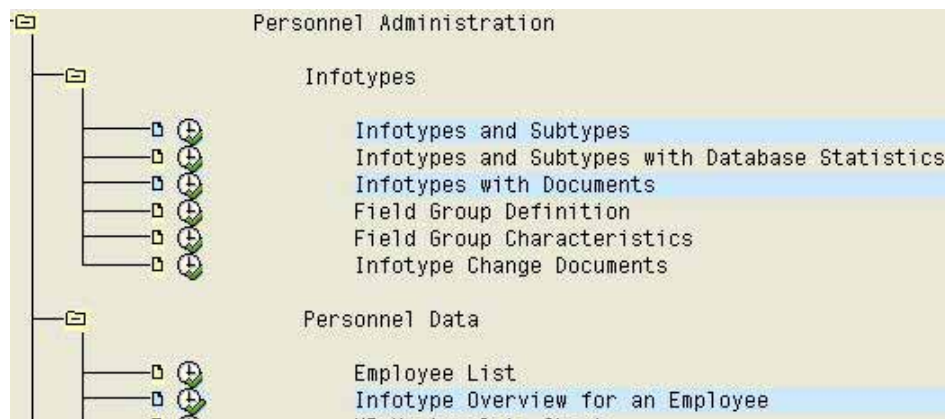


Figure 251: Overview of info types

The auditor can audit selected access authorizations in the HR area based on the created overview.

By clicking the function "info types and sub types with database statistics" he can determine which fields in an employee master record were accessed (and how often).

The button "info type overview for an employee" in the menu "personnel data" creates an overview of related info types by topic for the selected personnel number.

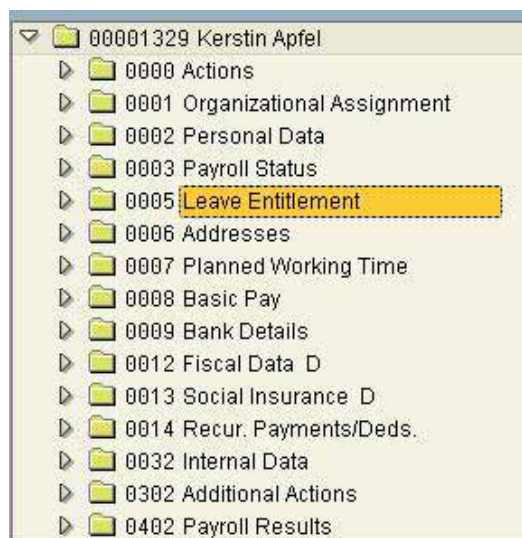


Figure 252: Info type overview for an employee

A form with detailed information is displayed after selecting specified items.

The screenshot shows the 'Leave entitlement' form in SAP. At the top, it displays employee details: Personnel no. 1329, Name Kerstin Apfel, EE group 1 (Active employee), Pers. area 1300 (Frankfurt), EE subgroup DN, Monthly wage ear..., Cost center 4279 (External Services), From 01.01.2000, To 31.12.2000, and Chg. 02.02.1999 (BONIN). Below this, the 'Leave entitlement' section shows 'Leave year 2000 / 01' and 'Remaining leave on 01.01.2000 30,00000'. A table follows with columns: Leave type, Entitlement, Requested, Compensated, Remaining, and Taken up to 31.12.2000. The first row shows '01 Standard le...' with an entitlement of 30,00000, requested 0,00000, compensated 0,00000, and remaining 30,00000. The bottom of the form shows summary totals of 30,00000.

Figure 253: Leave overview for an employee

Reports on administered employees, certain employee codes or single employees can be created utilizing the function "flexible data".

The screenshot shows the 'Flexible Employee Data' report. It has a title 'Flexible Employee Data' and a 'Key date: 10.12.2002'. Below is a table with columns: Total basic pay, Last name, and Date of birth. The data rows are:

Total basic pay	Last name	Date of birth
6.400,00	Müller	04.01.1960
3.900,00	Maier	05.06.1960
9.000,00	Zaucker	05.09.1960
3.860,00	Pfändili	09.06.1960

Figure 254: Report example with payroll information an photo of an employee group

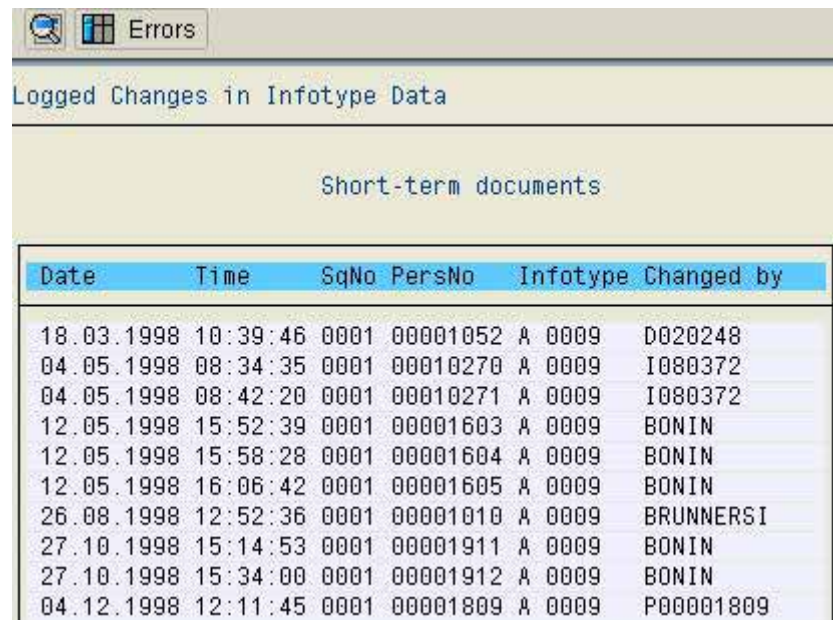
A document is created when personnel related data, which has been assigned to info types, is changed. The function "info type change documents" enables a specified control of such changes in a comprehensive selection screen.

The screenshot shows the 'Selection' screen for 'info type change documents'. It has a title 'Read documents from database' and two checkboxes: 'Long-term documents' (checked) and 'Short-term documents'. Below is the 'Selection' section with radio buttons for 'Transaction class' (Master data, Appl. data, All). The 'Master data' option is selected. There are input fields for 'Personnel number', 'Infotype', 'Changed on', and 'Changed by', each with a 'to' field and a search icon. Below is the 'Output options' section with checkboxes for 'Direct output of docs' and 'Output program selections', and a checkbox for 'New page per doc.'. There are also radio buttons for 'Sort order' (Time, Personnel no., Infotype, User) and a 'Default currency' field.

Figure 255: Selection screen for requesting info type change documents

- 257 -

In addition to the overview, containing date of change, relevant personnel number and who the data was changed by,



Date	Time	SqNo	PersNo	Infotype	Changed by
18.03.1998	10:39:46	0001	00001052	A 0009	D020248
04.05.1998	08:34:35	0001	00010270	A 0009	I080372
04.05.1998	08:42:20	0001	00010271	A 0009	I080372
12.05.1998	15:52:39	0001	00001603	A 0009	BONIN
12.05.1998	15:58:28	0001	00001604	A 0009	BONIN
12.05.1998	16:06:42	0001	00001605	A 0009	BONIN
26.08.1998	12:52:36	0001	00001010	A 0009	BRUNNERSI
27.10.1998	15:14:53	0001	00001911	A 0009	BONIN
27.10.1998	15:34:00	0001	00001912	A 0009	BONIN
04.12.1998	12:11:45	0001	00001809	A 0009	P00001809

Figure 256: Overview of info type change documents

detailed information on relevant fields with old and new field contents can be displayed on the screen

PersNo	00010270	Henry Miller	
Infotype	A 0009	Bank Details	
Changed by	I080372		
Date	04.05.1998	Time	08:34:35
		Seq. no.	0001

Subty	Obj	Lck	From	To	No	Old record	changed	Action
Field name			Old field			New field		
0			01.01.1997	31.12.9999	000			I
*Bank key						123123123		
*Bank acct						12566365		
*Bank ctry						US		
*Ctrl key						01		
Payee								
*Pay.method						T		

Figure 257: Detailed change log

In a final step the function "display logs of report starts (HR)" offers the described possibility to track programs which deal with reporting of HR data and should be logged.

### **5.13 Summary of the SAP<sup>TM</sup> basic system audit**

The presented audit activities merely summarize a slice of possible audit activities in the SAP<sup>TM</sup> system. They focus on major compliance aspects and are meant to give the auditor a truthful impression of the quality of business transaction processing and system administration within an acceptable time frame.

Based on the presented audit approach, there are manifold possibilities to deal with the SAP<sup>TM</sup> system. The module related audits should be mentioned, such as the necessary HR module audit. Additionally, certain process sequences with high risks should be reviewed completely, such as the steps in the purchasing cycle, beginning with a purchase request, purchase order, goods received, receipt and check of the invoice and ending with the posting in the financial accounting. The same applies for the often underestimated sales cycle, where the source code is adapted in many cases due to the close customer relations. The realization of complex rebate and discount structures usually result in problematic reconciliation procedures of accounting relevant data.

The extended audit activities are not a part of this manual. We refer to the additional ODENTHAL documentation "Process oriented audits in the SAP R/3<sup>TM</sup> system" (in German) and to commonly known documentation published by the SAP audit forums.

## **6 Utilizing the SAP R/3™ AIS system for business audits**

### **6.1 Introduction**

The business audit aspects in this manual include only the functions provided for the auditor's work place, in the AISTM menu "business audit". The AISTM system is based on the statutory audit requirements for auditing the financial statements at year end. The specific functions are therefore structured analogous to balance sheet items. The reports are of interest for internal auditors as well, as far as their work concern business and efficiency aspects.

The concept of a properly set and customized AIS™ system business audit is to generate adequate audit results in a particular audit field, such as company code or financial year, with a mouse click. Certain preparatory customizing procedures are required, which have to be co-ordinated with the statutory auditors, staff from the business departments and the system administrators. Additionally, the AIS™ system offers the option to configure the auditor's work place for specified audit purposes. These topics will be discussed in the next sections.

In following sections the basic menu structure, which applies to most balance sheets items, in the AIS™ system "business audit" will be explained. This allows the auditor to find any report on the proper spot. Selected reports on typical topics will also be shown.

The last section will describe how to transfer AISTM system data to common audit software directly via interface, in order to analyze specified single items in more detail or select a sample.

### **6.2 Setting up the AIS™ system**

#### **6.2.1 Customizing the user interface for the auditor's work**

##### **6.2.1.1 Customizing the user menu**

When calling the AIS™ system, it is possible to create different menus for different audit areas, such as

- IT audit
- data protection audit
- statutory audit

by calling the menu

Audit Information System

create / change view

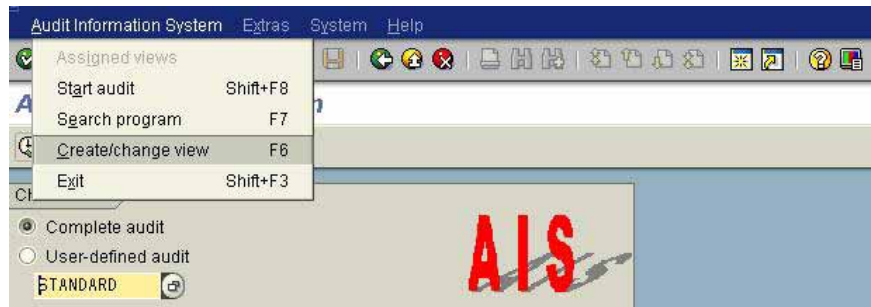


Figure 258: AIS function for creating and changing menus

After selecting the preferred structure, e.g. AUDIT\_FI for business audits, the name of the "view" to be developed has to be entered. Customer specific views have to begin with "Z" or "Y".

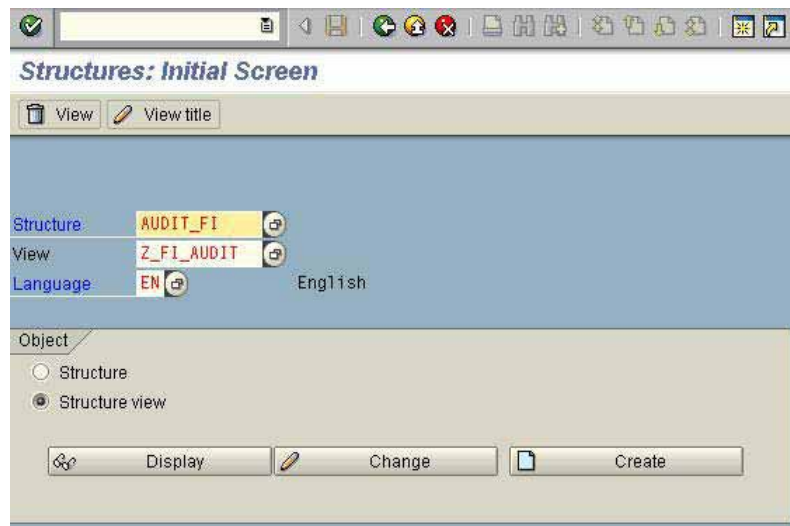


Figure 259: Creating a new menu in the AIS system

A meaningful description is given to the new view. New views are preferably created based on the delivered original structure. Specific menu items are selected by clicking "manual selection".

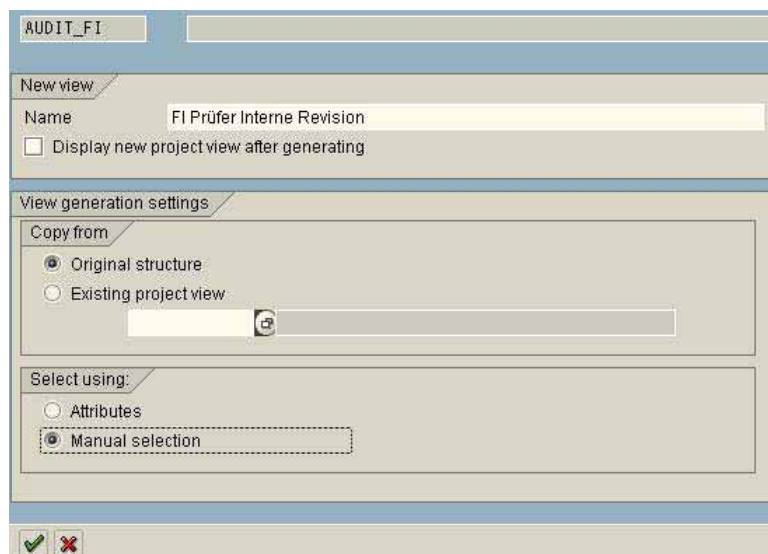


Figure 260: Entry of new menu attributes



Now specific program functions for the different menus as required by the users can be selected and the menu layout can be generated.

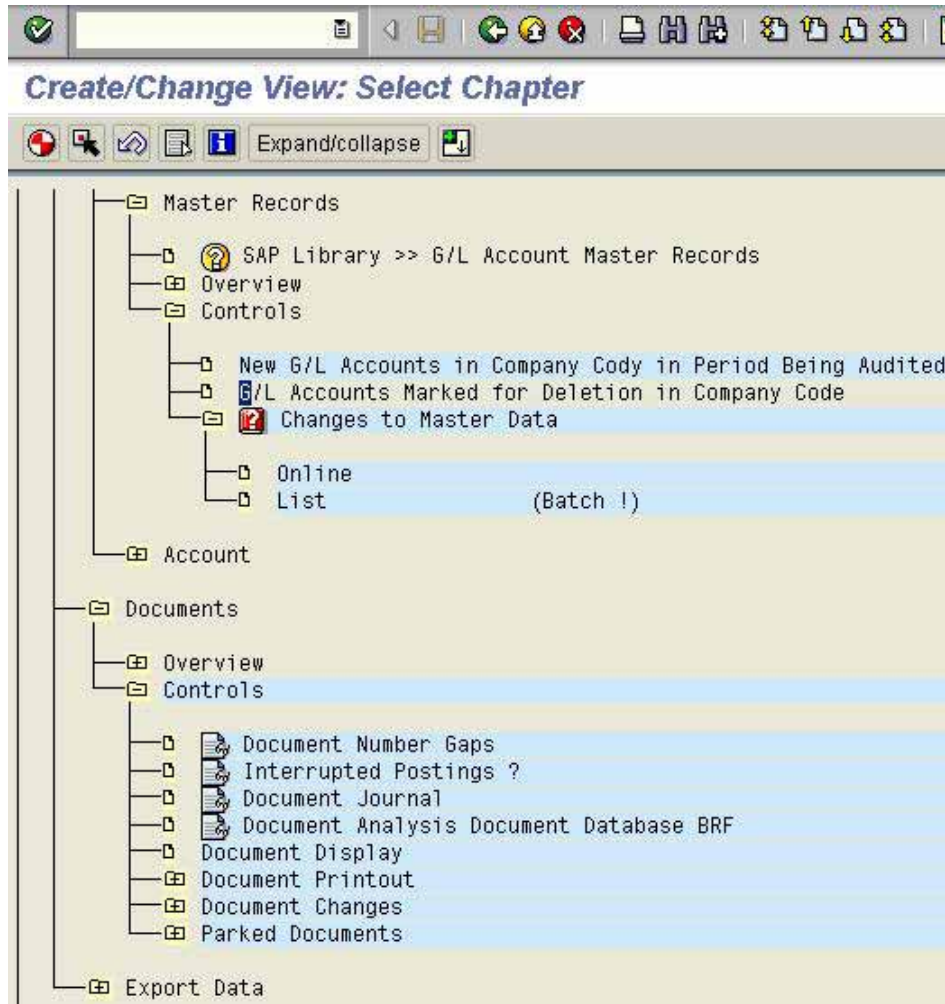


Figure 261: Selecting program functions and generating a new AIS menu

After creating the new menus, the auditor can select the menu of his choice when calling the AIS system with the option

choose view

user defined audit

(preferred menu)


which will be displayed on the screen.



Figure 262: Selecting a user defined AIS menu



The commands "position" and "set focus" offer other possibilities to size down the rather complex AIS™ structure to the specific audit requirements.

In a widely expanded AIS™ menu, where the functions to be selected only appear in the lower screen, it is useful to mark the beginning of the relevant work area and click the button "position" . The work area is moved to the upper screen and makes the navigation easier for the auditor.

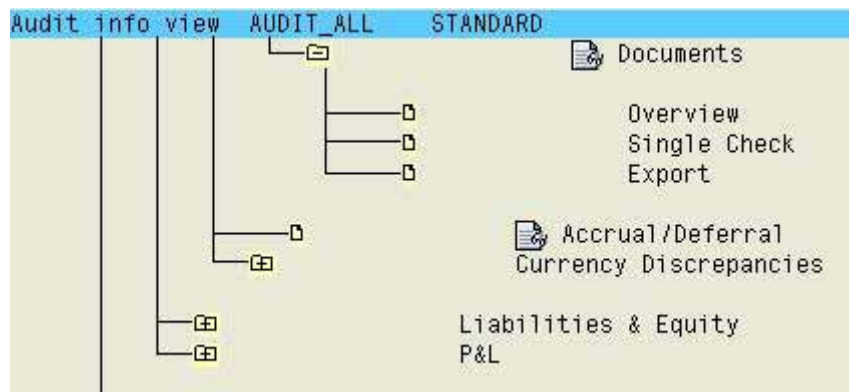



Figure 263: Positioning a low menu level in the upper screen

By clicking the button "set focus"  only the marked menu area will be displayed on the screen.

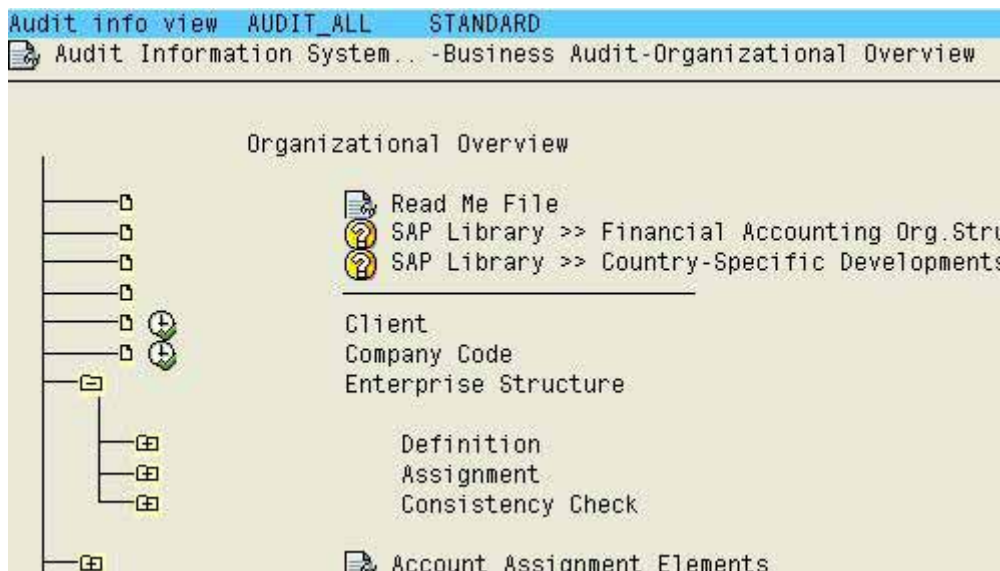


Figure 264: Setting an certain focus in the AIS menu

This function also makes the navigation between the manifold functions easier for the auditor.

### 6.2.1.2 User specific notes and support

The auditor can not only generated his own menu, but also create notes for each menu item, such as user manuals, reporting suggestions and checklists. The AIS™ menu, either the standard version or the specified menu, has to be activated in the first step. In a second step, the text editor can be called with the menu

edit

edit note

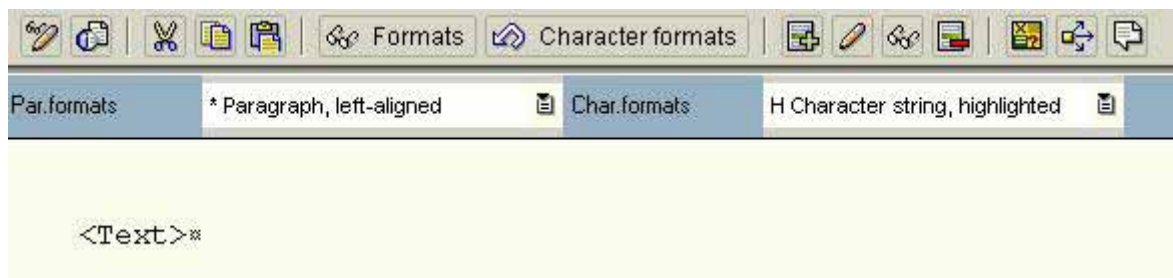


Figure 265: Entering supporting notes for functions in the AIS system

Notes can be entered manually, or existing checklists and audit procedures in a word format can be added. This is done with the function

text

upload

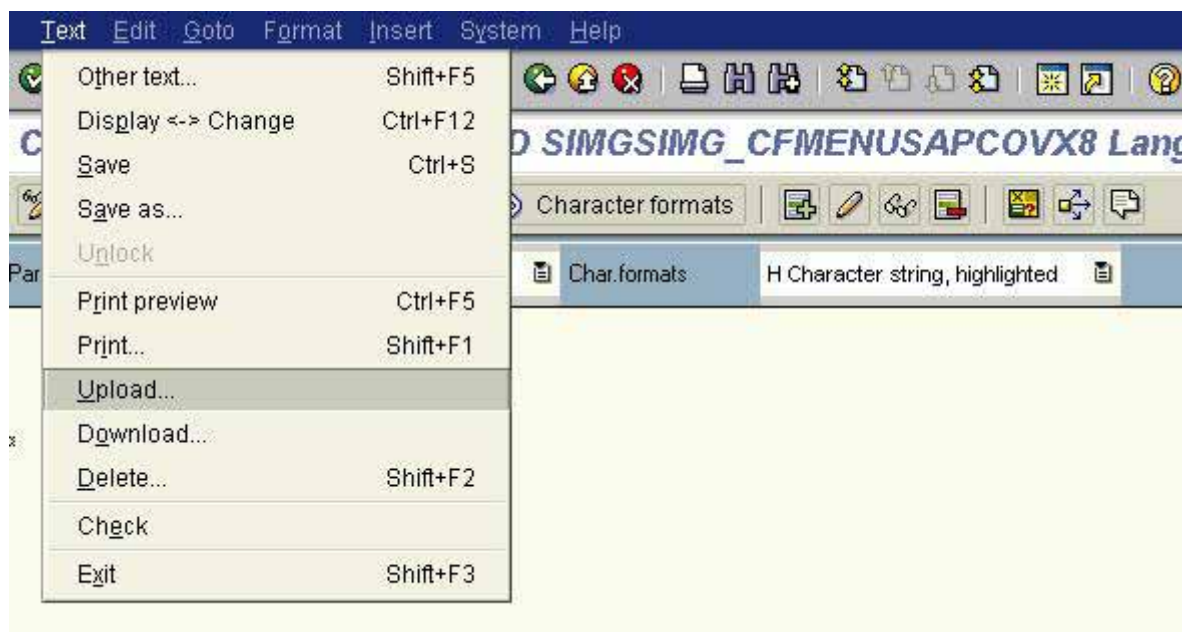


Figure 266: Upload function for adding existing texts and checklists

Existing texts can be added in ASCII or RTF formats.

There is a button in the AIS menu for the notes and saved texts, which have been added and edited in the text editor next to the relevant function.



Figure 267: Button for notes in the AIS menu

### 6.2.1.3 Layout of menu display options

In a final step, the auditor can layout the display options in the AIS menu flexibly. In the standard menu only the title of the functions to be called are displayed. The auditor can activate the additional display of related transactions, programs and their documentation and notes (in the open AIS menu) by calling the menu

Utilities

Additional information

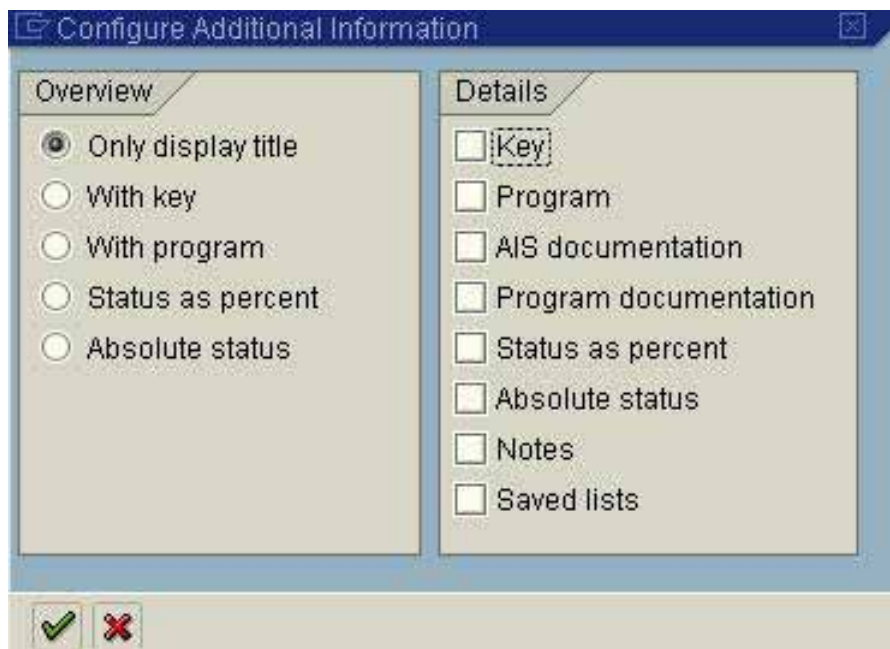


Figure 268: Display options in the AIS™ menu

In accordance with the selected option the AIS™ menu will be displayed with details.

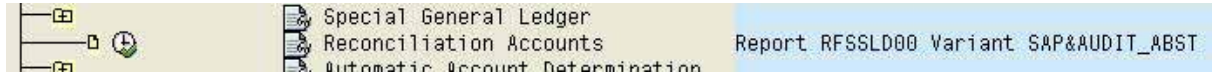


Figure 269: AIS™ menu with additional information on related reports

With “utilities” the switch layout in the menu and the explanation of symbols and icons can be called also.

## 6.2.2. Customizing the AIS™ system to company specific requirements

### 6.2.2.1 Introduction

SAP™ is providing several pre-defined analyses in prepared report variants. These reports have to be customized to company specific requirements, which have been recorded as preprocessing information. This applies in particular to information relevant for business audits. The required variants are listed in table TVARV. Please note, that TVARV is a cross client table and the settings in this table will be valid for every AIS™ user.

Customizing requirements have to be met regarding general ledger account analyses, key figures for special analysis in the BAETGE system and different integrated information systems.

Detailed information can be obtained from the documentation integrated to the AIS™ system by calling the menu

Audit information system  
     Introduction  
         Preparatory work (business audit)  
             AIS customizing or  
             Customize financial information system

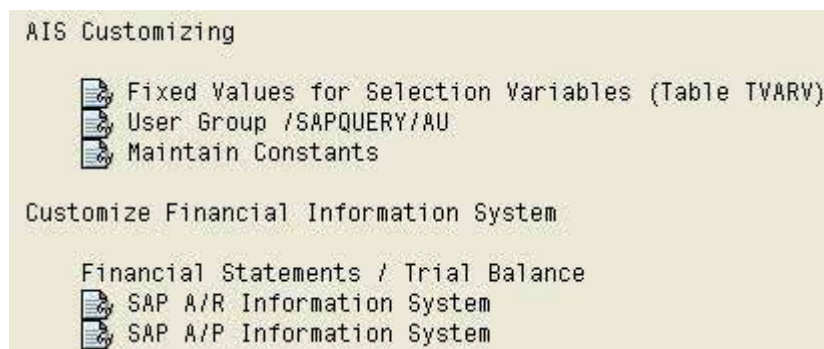


Figure 270: Calling documentation on AIS™ Customizing

### 6.2.2.2 Table TVARV – maintaining report system variants

This is a cross client table and requires a proper maintenance authorization. If the auditor does not have such an authorization, he must ask the administrators to enter the necessary values.

A maintenance transaction is implemented in the AIS system. It can be called in the menu

Audit info view

Introduction

Preparatory work (business audit)

AIS customizing

Fixed values for selection variables (table TVARV)

Maintenance is also possible in transaction SM31.

The names of variables in the table with preprocessing information and selection parameters begin with “AUDI”. Values which were pre-defined at installation have to be customized, usually in preparation of every financial statement audit.

These include:

Variable name	... parameter	Selection- criterion	Description
AUDI_WERKE		+	Plants
AUDI_BA-AUSGANGSRECHNUNG	+		Outgoing invoices document type
AUDI_BERICHTSJAH	+	+	Reporting year
AUDI_BILANZSTRUKTUR		+	Financial statement version
AUDI_BN_AUSGANGSRECHNUNGEN	+		Outgoing invoice doc. number interval
AUDI_BN_AUSZAHLUNGEN	+		Outgoing payment doc. number interval
AUDI_BN_EINGANGSRECHNUNGEN		+	Incoming invoice doc. number interval
AUDI_BN_EINZAHLUNGEN		+	Incoming payment doc. number interval
AUDI_BN_KASSENBUCH		+	Cash journal document number interval
AUDI_BUCHUNGSKREIS	+	+	Company code
AUDI_CUT_OFF_VON/BIS		+	Cut off period
AUDI_FORDERUNGEN_GRÖßER_N		+	Receivables larger than
AUDI_FREMDWÄHRUNG		+	Foreign currency
AUDI_HAUSWÄHRUNG	+		Local currency
AUDI_KONTENPLAN	+	+	Chart of accounts
AUDI_KREDITKONTROLLBEREICH		+	Credit control area
AUDI_L_AUSLAND		+	International
AUDI_L_INLAND		+	Domestic
AUDI_PRÜFUNGSDATUM		+	Check date
AUDI_STICHTAG	+		Balance sheet key date
AUDI_STICHTAG-VON/BIS		+	From/to key date
AUDI_STICHTAG_BIS		+	Key date to
AUDI_TITLE	+		Additional heading
AUDI_VERBINDLICHK_GRÖßER_N		+	Payable larger than
AUDI_VERGLEICHSJAH	+		Comparison year



Figure 271: Maintaining the parameter for the additional title in table TVARV

### 6.2.2.3 Customizing the general ledger information system

The general ledger information system has to be customized to the organizational structure, the relevant company information, company codes and business areas, balance sheet structure to be utilized etc.

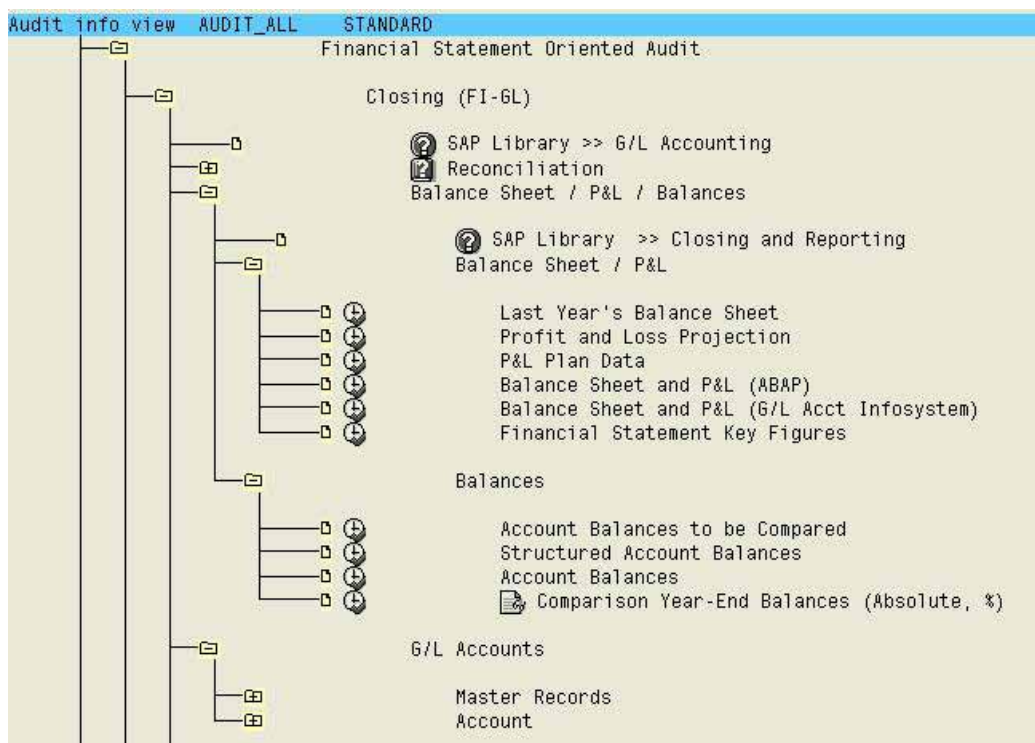


Figure 272: Parameters for the general ledger information system



#### 6.2.2.4 The analysis system "BAETGE"

##### 6.2.2.4.1 Introduction

The company Baetge & Partner developed an early warning system for major risks with a number of key figures, based on scientific research of financial statements from German blue chip enterprises. There is a direct interface for this tool in the AIS™ system.

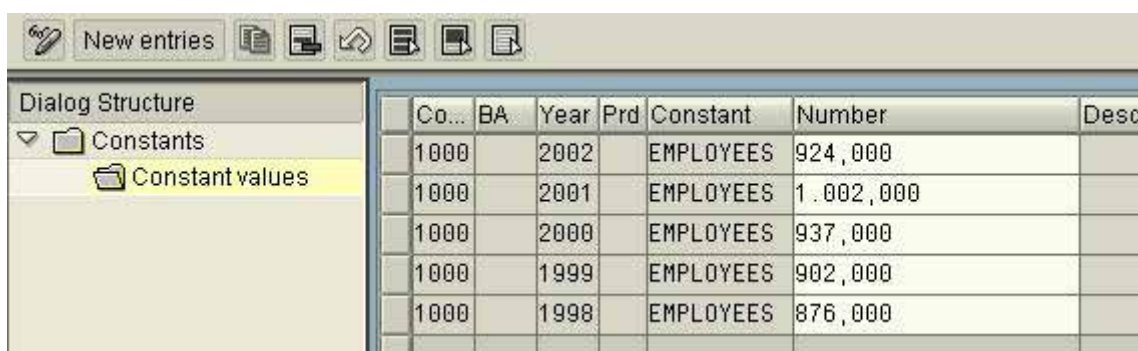
In order to utilize this tool as intended, the provided form has to be customized, not only to the BAETGE but also to the company specific requirements. This will be discussed in detail.

##### 6.2.2.4.2 Number of employees

For comparisons to previous years and resulting key figures, the BAETGE system requires the average number of employees for a number of years, which can be entered in the menu

- Audit info view
  - Introduction
    - Preparatory work (business audit)
      - AIS customizing
        - Maintain constants

The relevant constant is EMPLOYEE.



Co...	BA	Year	Prd	Constant	Number	Desc
1000		2002		EMPLOYEES	924,000	
1000		2001		EMPLOYEES	1.002,000	
1000		2000		EMPLOYEES	937,000	
1000		1999		EMPLOYEES	902,000	
1000		1998		EMPLOYEES	876,000	

Figure 273: Maintaining the EMPLOYEE constant

The constant first has to be created and then filled in with the average number of employees for the last five years.



#### 6.2.2.4.3 Customizing the BAETGE analysis form

The key figures in the BAETGE system require the balance sheet structure, including the chart of accounts and the balance sheet items to be customized to the actual business circumstances in the company. The settings can be done in the menu

- Audit info view
  - Introduction
    - Preparatory work (business audit)
      - Customize financial information system
        - Financial statements / trial balance
          - Financial statement key figures
            - Export financial statement data (Baetge)

The related transaction is FSI5.

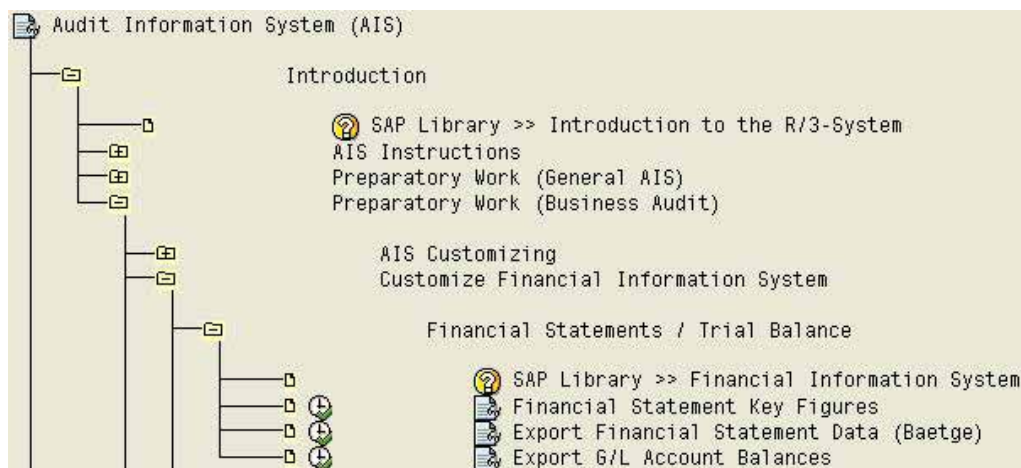


Figure 274: Customizing the BAETGE system information

The procedure is explained in detail in the attached text documents.

Form	Text	Changed by	Changed on
0CZ-ACTIV-01	ASSETS Czech	SAP	25.09.1998
0CZ-CASHF-01	Cashflow Czech	SAP	25.09.1998
0CZ-PASSI-01	Liabilities Czech	SAP	25.09.1998
0CZ-RESUL-01	Profit + Loss: Czech Republic	SAP	28.07.1999
0JP-BAJP-1M	Japan BSPL + product cost attachment	SAP	25.09.1998
0PT-ACTIV-01	Assets: Portugal	SAP	23.02.1998
0PT-PASSI-01	Liabilities: Portugal	SAP	23.02.1998
0PT-RESUL-01	Demonstração de Resultados - Portugal	SAP	23.02.1998
0SAPAUDIT-01	Balance sheet key figures	SAP	28.07.1999
0SAPAUDIT-20	Export to Baetge	SAP	28.07.1999
0SAPRATIO-01	Cons.Statem.Cash Fl.	SAP	19.01.2000
0SAPRATIO-03	Cash flow (indirect)	SAP	19.01.2000
0SAPRATIO-04	Cash flow (direct)	SAP	19.01.2000
0SAPRATIO-50	Cash flow (China)	SAP	23.02.1998
AUDIT-BAETGE	Interface test	SAP	23.02.1998
AUDIT-TEST	Audit test	SAP	23.02.1998

Figure 275: Customizing forms for the BAETGE system

6.2.2.5 Customizing the interface “general ledger account balances” for further systems

It is possible to set the interfaces in the AIS system to enable an export of general ledger account balances to further programs, such as the common statutory audit software AUDITAgent supplied by AUDICON. This will only be required in rare cases, as general ledger account balances are accessed directly.

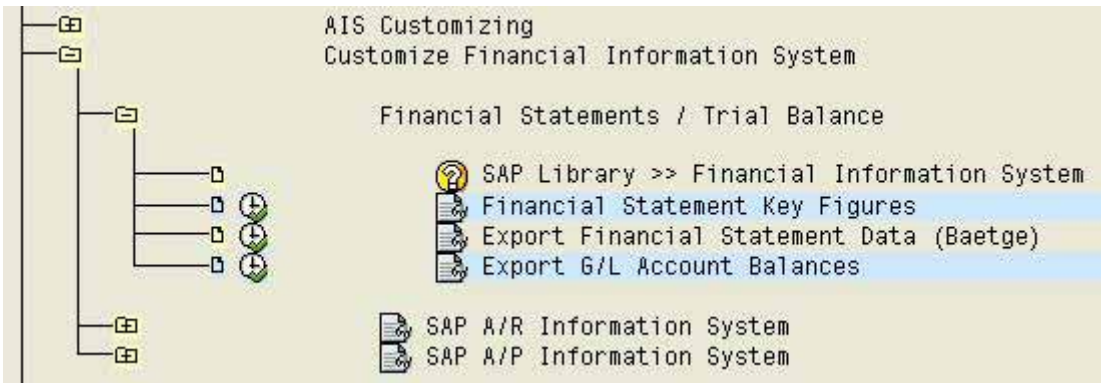


Figure 276: Customizing interfaces for export of general ledger account balances

The data export via customized interfaces is realized in the AIS menu “closing” at the latest.

Form 0SAPAUDIT-40 Export audit agent		
Ratio		
per 01 &1FY	XXX.XXX.XXX	
per 02 &1FY	XXX.XXX.XXX	
per 03 &1FY	XXX.XXX.XXX	
per 04 &1FY	XXX.XXX.XXX	
per 05 &1FY	XXX.XXX.XXX	
per 06 &1FY	XXX.XXX.XXX	
per 07 &1FY	XXX.XXX.XXX	
per 08 &1FY	XXX.XXX.XXX	
per 09 &1FY	XXX.XXX.XXX	
per 10 &1FY	XXX.XXX.XXX	
per 11 &1FY	XXX.XXX.XXX	
per 12 &1FY	XXX.XXX.XXX	
FY &1FY	XXX.XXX.XXX	
FY-1 &1FY	XXX.XXX.XXX	
FY-2 &1FY	XXX.XXX.XXX	
FY-3 &1FY	XXX.XXX.XXX	
FY-4 &1FY	XXX.XXX.XXX	

Figure 277: Form structure "general ledger account balances"

## 6.2.2.6 Setting up the customer and vendor information systems

### 6.2.2.6.1 Introduction

The report variant technique was introduced in SAP R/3™ release 3.0 and enables the auditor to conduct a business audit with a mouse click by utilizing the AIS system and its output of pre-prepared analyses. All selection criteria, which are interesting for standard analyses can be gathered in a report. Additional information is picked up in the described table TVARV (see section 2), and yet other is added by specific transactions.

In the following section the procedure for creating and utilizing report variants based on SAP™ standard reports is described.

### 6.2.2.6.2 Creating specified report variants

The standard reports (views) for the customer and vendor information systems are implemented during the SAP™ installation in order to support the user departments in their regular work.

The standard reports are also useful for statutory and internal auditing purposes. Since auditors have a primary interest in specific inquiries, such as cut-off issues, it is useful to create specified audit variants. Preferably, the SAP™ standard reports are copied to an audit view. The required functions are provided by the SAP™ system in the menu

Audit information system  
     introduction  
         Business audit  
             Preparatory work (business audit)  
                 Customize financial information system  
                     SAP A/R information system  
                     SAP A/P information system

The attached documentation contains special notes on the set-up and customizing, and should be printed in advance.

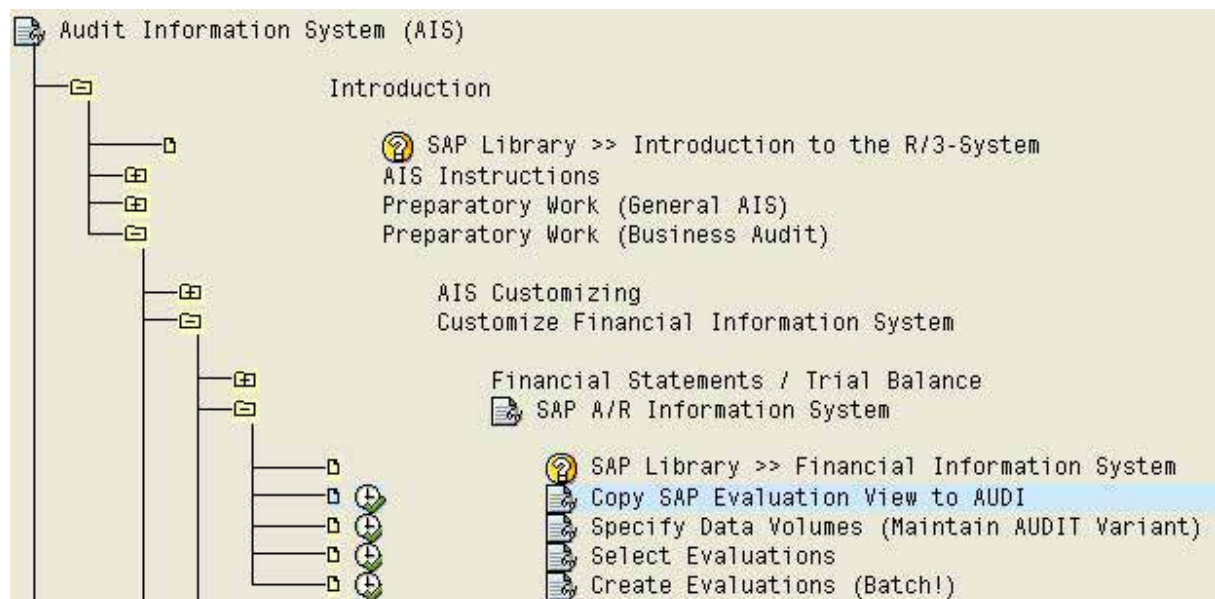


Figure 278: Functions for customizing information system

After calling the function “copy SAP evaluation view to AUDI” the system displays the available standard evaluations for customizing.

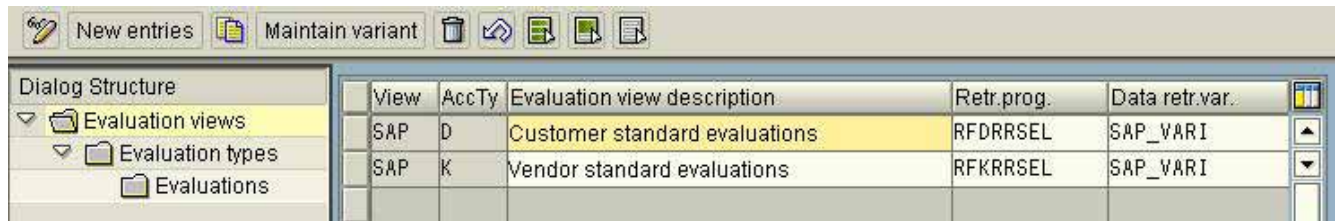


Figure 279: Customer and vendor standard evaluations

The selected standard evaluation is marked and a new variant can be created with “maintain variant”.



Figure 280: Creating a new variant for customer evaluation

In a second step, the new audit variant – if utilized – is assigned to already created selection variables in table TVARV. To do so, the button “create” is clicked and in the appearing selection the button “attributes”.



**Maintain Variant: Report RFDRRSEL, Variant SAP\_VARI1**

Attributes

Customer selection

Customer account  to

Company code  to

Selection using search help

Search help ID

Search string

Complex search help

Reporting period

Fiscal year  to

Line item selection

Open items at key date

Figure 281: Function maintenance and assignment of selection variables

A meaningful description is entered for the variant to be created. The fields “company code” and “key date” are marked as selection variables.

Variant name

Description

Created for selection screens

Only for background processing ☐

Protect variant ☐

Only display in catalog ☐

System variant (automatic transport) ☐

Field attributes

Required field ☐

Switch SPA/GPA off ☐

Save field without values ☐

Selection variable ☐

Hide field 'BIS' ☐

Hide field ☐

Protect field ☐

Field name	Type	P	I	N	L	P	L	O
Company code	S	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Customer search help	P	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alternative local currency	P	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Translation date	P	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fiscal year	S	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Open items at key date	P	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 282: Maintaining the variable attributes (description and selection variables)

With the button “selection variables” the variables in table TVARV can be assigned to the variant.

Selection criterion	T	D	B
Variable name			
Company code	Selected	Not supported	Not selected
Open items at key date	Selected	Not selected	Not supported

Figure 283: Assigning table variables to the report variant

In a final step, the selected items from the variables, the variant attributes and the created variant are saved.

After a new variant for audit purposes has been created with the described procedure, the other settings for SAP™ standard reports are to be copied to the new view and be linked to the created variant. For this purpose, the “copy SAP evaluation view to AUDI” in the AIS™ opening screen is activated. The standard evaluation view is marked and a new entry is possible in the menu

Edit

Copy as...

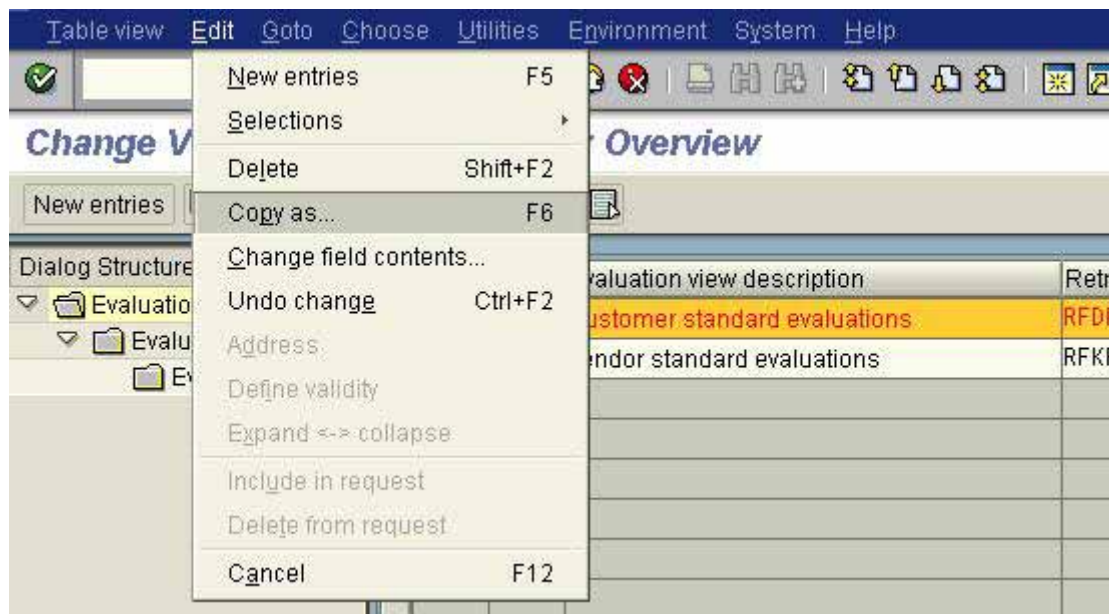


Figure 284: Copying a standard evaluation to an audit specific variant

The new created view is named AUDI. Additionally, a description should be input. In the field “database variant” the created variant is assigned by entering AUDIT. An additional menu can be activated with the right mouse button to click the item “copy”.

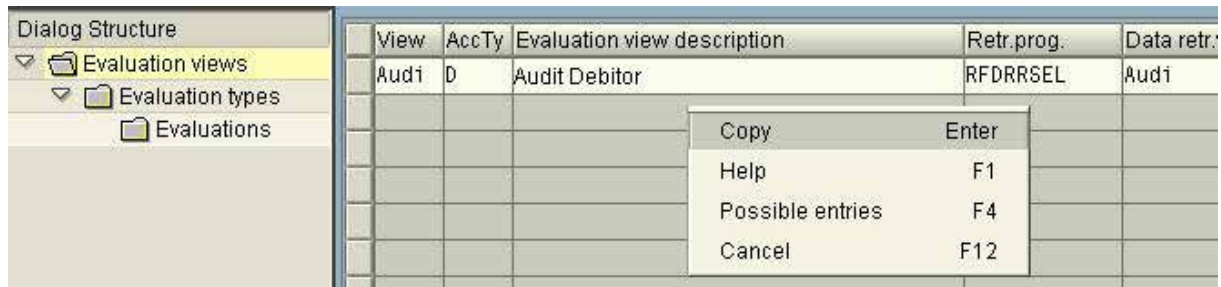


Figure 285: Creating a new evaluation view for the created variant

All relevant settings in the SAP™ standard evaluation should be transferred to the new view with the appearing menu.

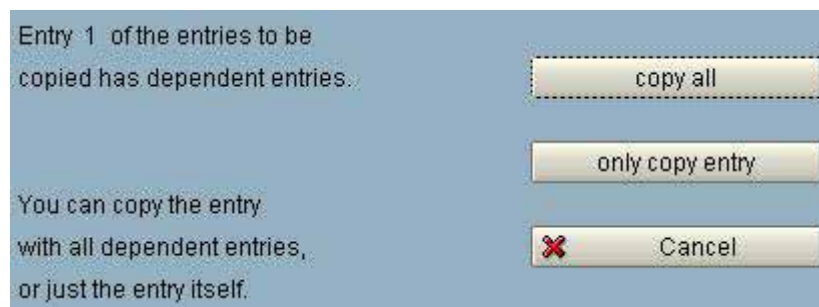


Figure 286: Copying SAP™ standard settings

The button “copy all” is clicked to do so, resulting in a new view provided for the AIS™ system,

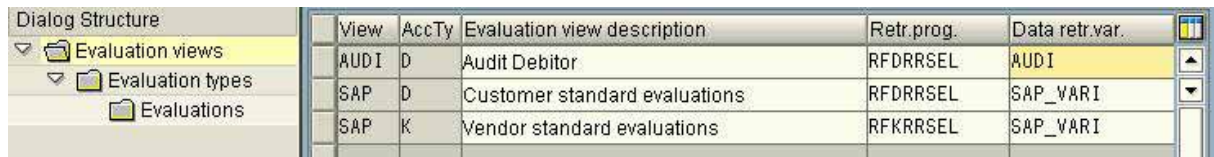


Figure 287: Newly configured selection view for the AIS system

which has to be saved by utilizing a customizing request.



Figure 288: Saving the created view with a new request



The same described procedure can be repeated for vendor evaluations.

The data volume required for generating different reports can be affected at all times, if the auditor is adjusting the variants and evaluation selections according to the current audit needs, with the function "specify data volume (maintain AUDIT variant" in the AIS system. Additionally, the function "specify data volume" is necessary for generating specified reports, and the SAP<sup>TM</sup> standard reports should be deactivated.

Once the variants have been finalized, up to 40 evaluations can be selected for customer and vendor information, by calling the menu

Introduction

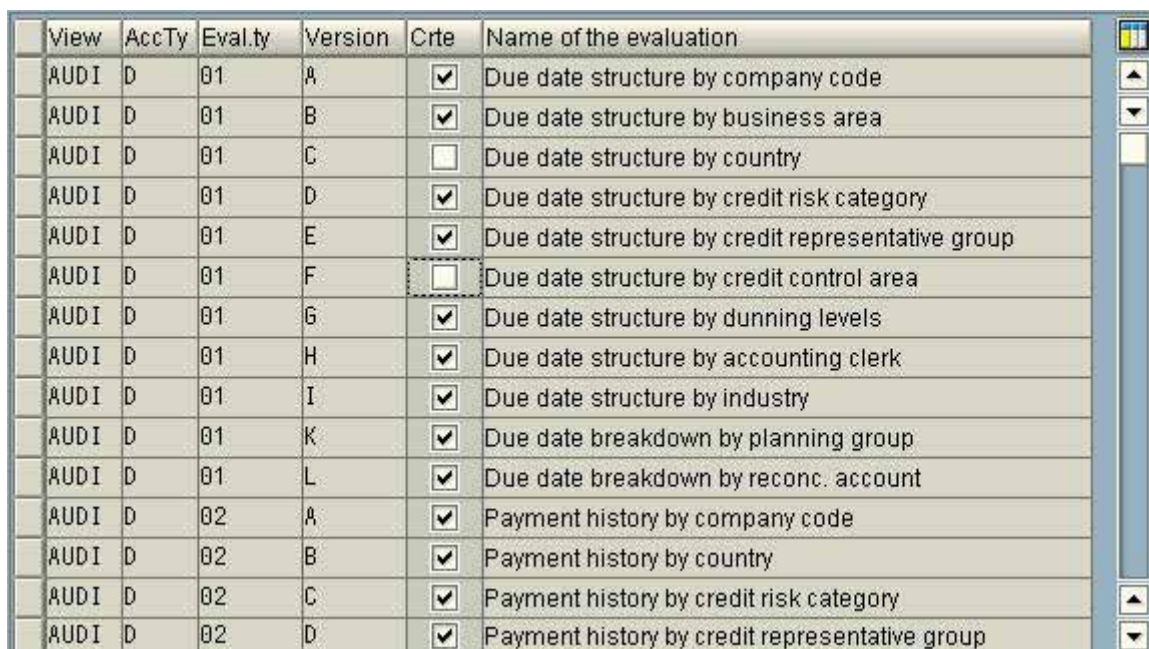
Preparatory work (business audit)

Customize financial information system

SAP A/R information system

SAP A/P information system

Select evaluations



View	AccTy	Eval.ty	Version	Crte	Name of the evaluation
AUDI	D	01	A	<input checked="" type="checkbox"/>	Due date structure by company code
AUDI	D	01	B	<input checked="" type="checkbox"/>	Due date structure by business area
AUDI	D	01	C	<input type="checkbox"/>	Due date structure by country
AUDI	D	01	D	<input checked="" type="checkbox"/>	Due date structure by credit risk category
AUDI	D	01	E	<input checked="" type="checkbox"/>	Due date structure by credit representative group
AUDI	D	01	F	<input checked="" type="checkbox"/>	Due date structure by credit control area
AUDI	D	01	G	<input checked="" type="checkbox"/>	Due date structure by dunning levels
AUDI	D	01	H	<input checked="" type="checkbox"/>	Due date structure by accounting clerk
AUDI	D	01	I	<input checked="" type="checkbox"/>	Due date structure by industry
AUDI	D	01	K	<input checked="" type="checkbox"/>	Due date breakdown by planning group
AUDI	D	01	L	<input checked="" type="checkbox"/>	Due date breakdown by reconc. account
AUDI	D	02	A	<input checked="" type="checkbox"/>	Payment history by company code
AUDI	D	02	B	<input checked="" type="checkbox"/>	Payment history by country
AUDI	D	02	C	<input checked="" type="checkbox"/>	Payment history by credit risk category
AUDI	D	02	D	<input checked="" type="checkbox"/>	Payment history by credit representative group

Figure 289: Selecting specific customer and vendor evaluations

The selected evaluations can be generated in one batch run with a mouse click prior to the audit, in order to be provided as hardcopies to the auditor.

### 6.2.2.3 Tools for setting up the AIS™ system

Purpose	Transaction/functions	Tables	Programs
Customizing the menu	AIS – opening screen and audit information system / create/change view		
Additional information to the AIS functions	AIS – menu and utilities / additional information		
Maintaining report parameter and selections	SM31 and table	TVARV	
Settings in the general ledger information system	AIS – menu Preparatory work AIS customizing Maintain constants		
Maintaining BAETGE form for balance sheet key figures	FSI5		
Setting up interface general ledger account balances	AIS – menu Preparatory work Customizing financial information system Export general ledger account balances		
Setting up customer and vendor information systems	AIS – menu Preparatory work Customizing financial information system SAP A/R / A/P information system		

**Checklist for business audits  
(setting up the AIS™ system)**

- ☐ Check AIS™ function
  - Single evaluation function
  - Sufficient authorization
- ☐ Customize user menu
- ☐ Upload company specific checklists in the AIS™ system
- ☐ Set up menu display options
  - Transactions and programs
  - Program documentation
  - AIS™ documentation
- ☐ Set up table TVARV
  - Cross client table
  - Support by administrators required
- ☐ Customize general ledger information system
- ☐ Set up analysis system “BAETGE”
  - If required and utilized
  - Constant “EMPLOYEES”
  - Transfer form / interface
- ☐ Set up interface “general ledger account balances” (SUSALI)
- ☐ Customize customer / vendor information system

### **6.3 Utilizing the AIS™ in business audits**

The AIS system provides manifold functions for supporting the business audit and the audit of financial statements. They can be categorized as follows:

#### **❑ Preparatory work**

Customizing and settings in the AIS™ system for specific audits. The major objective is to customize all reports to contain only relevant accounting information for the current audit (financial year, organizational units). These preparations were described in detail in section II and will not be discussed at this point.

#### **❑ Organizational overview**

This menu contains all required functions for obtaining a general overview of the statutory and management accounting systems. Additionally, the automatic account control is described in detail. The auditor also obtains an overview of the quantity structure (general ledger accounts, customers, vendors, documents...) of his audit fields, which enables him to plan the audit and consider sampling methods.

#### **❑ Closing (FI-GL)**

In this menu, information and functions relevant for every audit of financial statements, balance sheets and profit & loss accounts, as well as specific accounts and documents, can be found, including reconciliation and control procedures required for the SAP™ system. There are also functions for exporting account balances and document data to personal computers, to software supporting statutory audits or to specified audit software.

#### **❑ Assets**

All audit activities of the assets in the balance sheet are supported by the functions in this menu and the attached specified reports. There are also functions for exporting data such as receivables, inventories and current funds to software on personal computers, in order to carry out further analyses.

#### **❑ Liabilities and equity**

All audit activities of the liabilities and equity are supported by the functions in this menu. There are also functions for exporting data to software on personal computers.

The complete business audit menu contains very useful audit relevant documentation, which can be recommended to every user. The documentation is based on the needs for financial statements audits with audit activities and work papers.

Users can utilize several functions by intuition, and for clarity purposes only distinctive features will be discussed in this manual.

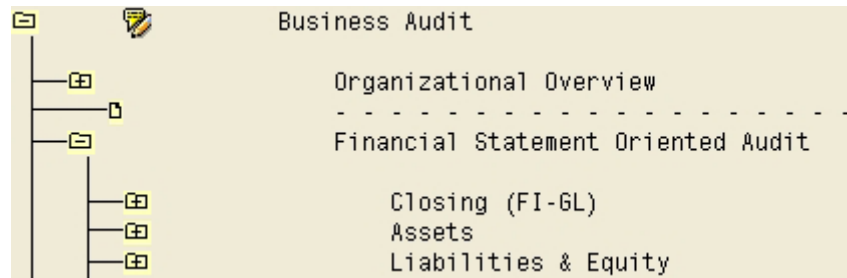


Figure 290: AIS functions for business audits

## 6.4 Mapping the business / organizational parameters

### 6.4.1 Business structure

In order to carry out audits in the SAP R/3™ system and generate information which meet audit requirements, the auditor needs to have an overview of the business structure and related links in the system. The business structure is controlling the process flows, the data model and the reporting structures of financial data.

Several elements are available for structuring the system, such as the client on the corporate group level and company codes on the level of legal entities within the group. Depending on the company needs, controlling areas can be defined. Business areas can be utilized as sub units of company codes or consolidate business segments in business areas across company codes. Storage locations are created for physical inventories. The inventory valuation is done on plant or company code level. Customer and vendor relations are maintained in purchasing or sales organizations.

The AIS™ functions such as client, company code and enterprise structure provide an overview of the structural elements.

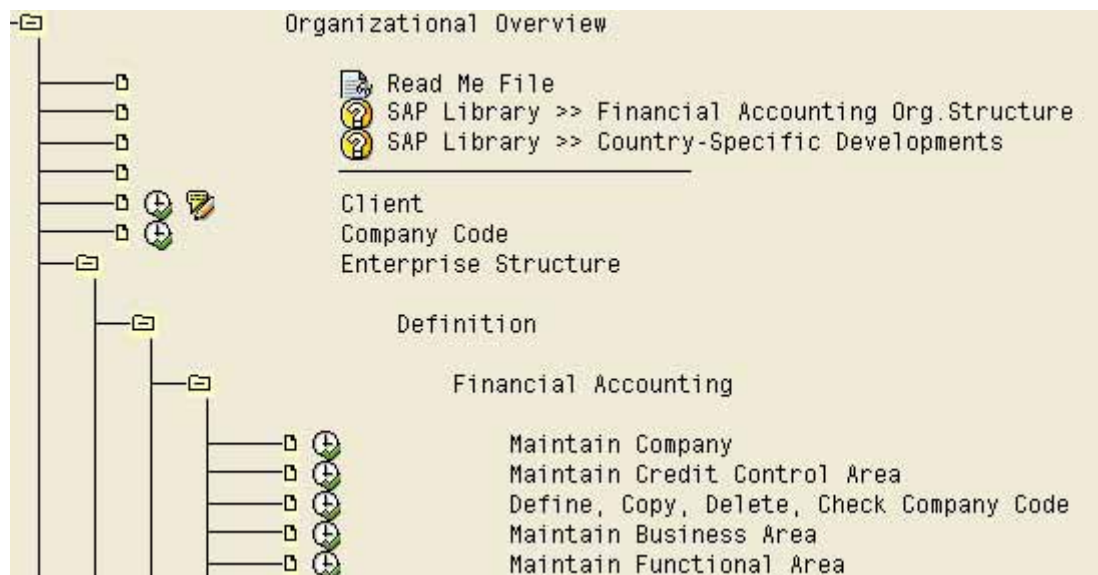


Figure 291: Functions for displaying the business structure in the finance area

The presented functions are parts of the customizing. The auditor should make sure, that his authorizations are restricted only to display and generation of work papers and that structural changes can not be carried out, as this could cause severe damage to the system functionality.

There is a distinct feature in the menu

Organizational overview

Enterprise structure

Consistency check

Check enterprise structure for sales and distribution

Since inconsistencies often occur in the complex area of sales and distribution organization (SD module), resulting in reconciliation difficulties for the sales and distribution information systems and the financial accounting, the provided consistency check shows structural deficiencies

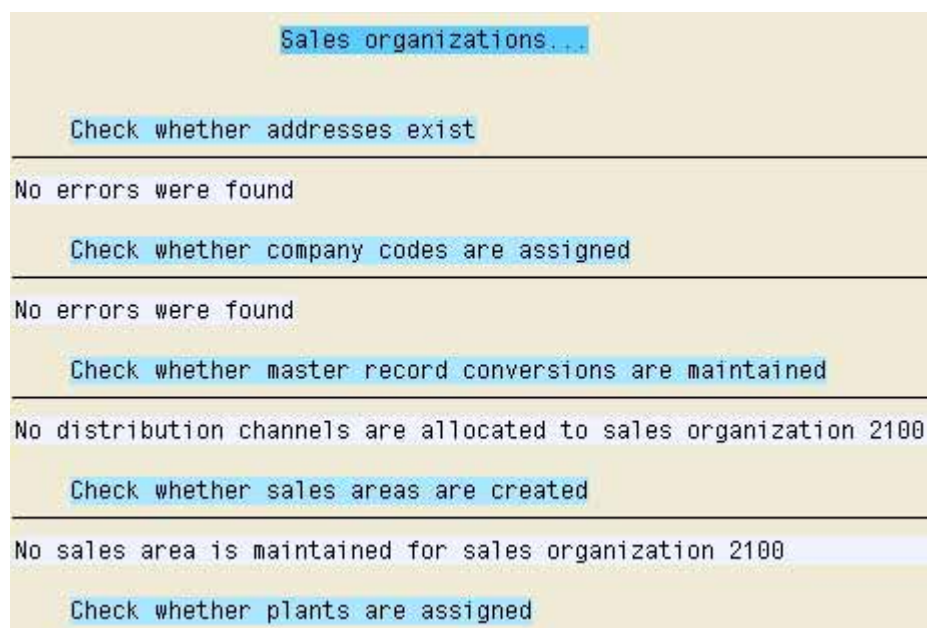


Figure 292: Log of customizing display in the sales and distribution area

which should be analyzed and corrected immediately.

## 6.4.2 Information on account assignment elements

### 6.4.2.1 Introduction

The data flow in the SAP<sup>TM</sup> system is controlled by documents, where the major part of all postings are largely automatically generated by utilizing controlling elements.

The specific account assignment elements, such as document and account types, posting keys, assigned document numbers and the VAT or sales tax calculation procedures, control how the business transaction is processed in the system.

Erroneous settings of controlling elements and their improper impact on the operations in the production system are affecting the compliance of the financial accounting on a permanent basis, and result in a system, which can not be reconciled.

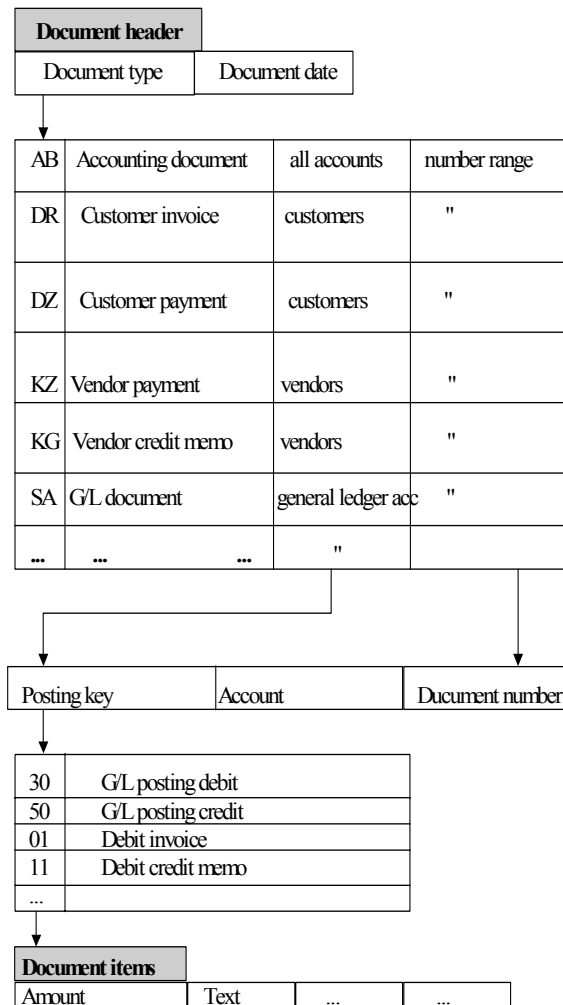


Figure 293: Account assignment elements and document in the SAP™ system

The automated control usually references a posting transaction to a particular business transaction. A particular document type is assigned to a defined business transaction. There are several standardized document types, which can be supplemented according to company specific requirements. The document type - e.g. KR "vendor invoice" – is linked to a specific group of accounts and is posted within a defined range of document numbers. Both assignments are defined during the customizing procedure. Every document type has different posting keys, which e.g. define if the document is posted as a debit or credit entry. Depending on the selected document type and posting key, an input template is displayed to the user, where individual posting features can be entered. Which entries in which fields and if the entry is required or optional, depending on the assigned field groups, is again defined in the customizing.

Further account assignment elements are the tax codes linked to accounts. The tax codes control the tax calculations and the automatic entries to reconciling accounts, ensuring that the business transactions are posted to the proper general ledger accounts.



The following functions give the auditor an overview of account assignment elements.

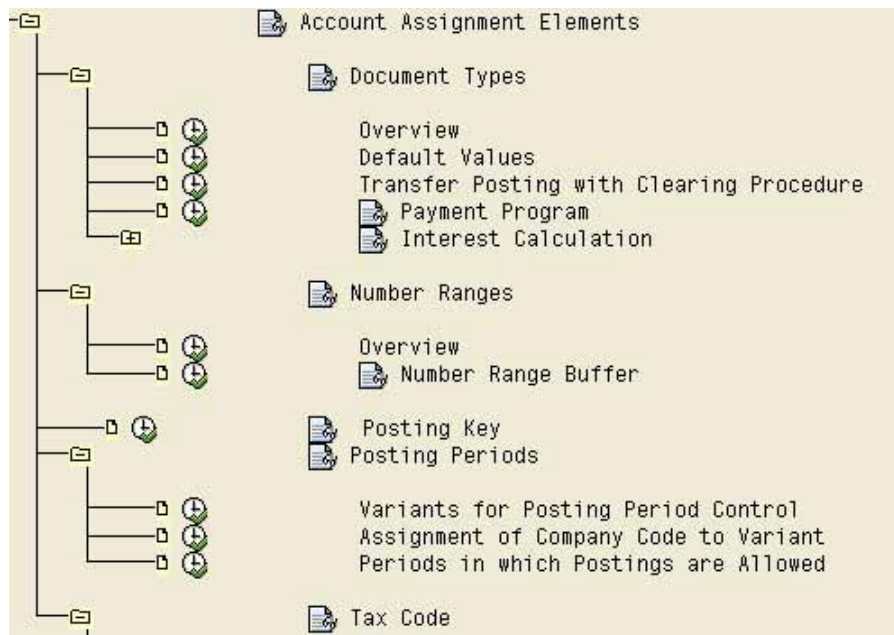


Figure 294: Functions for auditing and obtaining an overview of account assignment elements

## 6.4.2.2 Details on account assignment elements

### 6.4.2.2.1 Document types

In the AIS menu

Document types

Overview

an overview of created document types (business transactions) can be obtained.

Type	Description
AA	Asset posting
AB	Accounting document
AF	Dep. postings
AN	Net asset posting
C1	Closing GR/IR accts
CI	Customer invoice
CP	Customer payment
DA	Customer document
DB	Cust.recurring entry
DG	Customer credit memo
DR	Customer invoice
DZ	Customer payment
EU	Conversion diff.Euro
EX	External number
GF	Subsequent adjustmnt

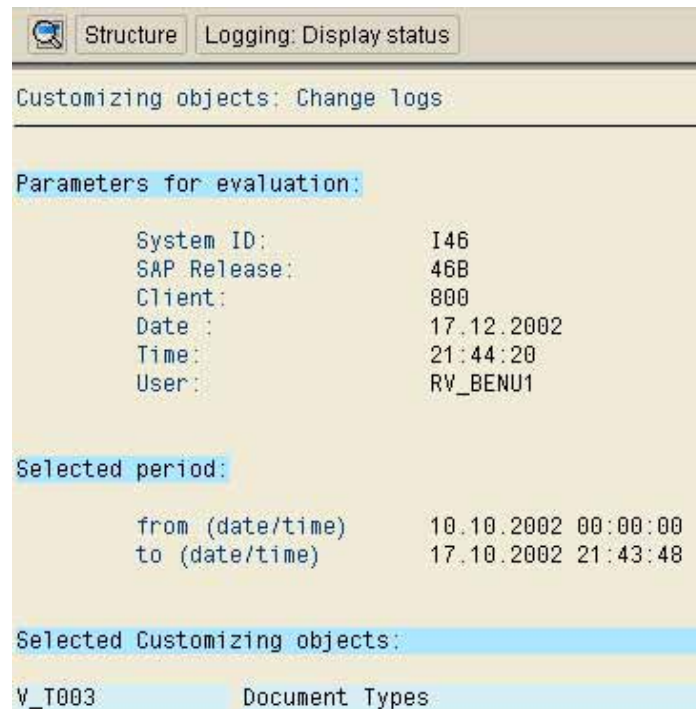
Figure 295: Document types in the SAP R/3™ system

In the menu

Utilities

Change log

the change logs of specific document types are displayed.



Structure Logging: Display status

Customizing objects: Change logs

Parameters for evaluation:

System ID:	I46
SAP Release:	46B
Client:	800
Date :	17.12.2002
Time:	21:44:20
User:	RV_BENU1


Selected period:

from (date/time)	10.10.2002 00:00:00
to (date/time)	17.10.2002 21:43:48

Selected Customizing objects:

V_T003	Document Types
--------	----------------

Figure 296: Document type change log

Details on the connections between document type (business transactions), allowed account types, assigned ranges of document numbers and other controlling elements can be obtained by clicking the magnifying glass .



Document type AB Accounting document

Properties

Number range	01	Number range information
Reverse doc. type	AB	
Authorization groups		

Account types allowed

- ☒ Assets
- ☒ Customer
- ☒ Vendor
- ☒ Material
- ☒ G/L account

Special usage

- ☐ Btch input only
- ☐ Rollup
- ☐ Planning
- ☐ Act.allocation
- ☐ Plan.allocation

Figure 297: Detailed information on a document type

The system guides the user through system transactions by suggesting certain document types, linked to certain posting keys. The suggestions are displayed as default values when the user calls the transactions. The default values for transactions can be displayed on the screen by calling the menu

Organizational overview

Account assignment elements

Document types

Default values

Transaction		Doc.type	Posting key
F-41	Enter Vendor Credit Memo	KG	21
F-42	Enter Transfer Posting	AB	
F-43	Enter Vendor Invoice	KR	31
F-46	Reverse Refinancing Acceptance	KA	
F-47	Down Payment Request	KA	
F-48	Post Vendor Down Payment	KZ	
F-49	Customer Noted Item	DA	09
F-51	Post with Clearing	AB	
F-52	Post Incoming Payments	KZ	
F-53	Post Outgoing Payments	KZ	
F-54	Clear Vendor Down Payment	KA	

Figure 298: Overview of transaction default values for a document

#### 6.4.2.2.2 Number ranges

As already explained, every business transaction is assigned to a document number range. An overview of created number ranges for posting documents can be obtained in the AIS menu

Number ranges

Overview

Number range obj.		Accounting document			
Company code		1000			
Ranges					
No	Year	From number	To number	Current number	Ext
01	1992	0100000000	0199999999	0	<input type="checkbox"/>
01	1993	0100000000	0199999999	0	<input type="checkbox"/>
01	1999	0100000000	0199999999	100013157	<input type="checkbox"/>
01	2000	0100000000	0199999999	100000194	<input type="checkbox"/>
01	2004	0100000000	0199999999	100000379	<input type="checkbox"/>
02	1992	0200000000	0299999999		<input checked="" type="checkbox"/>
02	1993	0200000000	0299999999		<input checked="" type="checkbox"/>
02	1999	0200000000	0299999999		<input checked="" type="checkbox"/>
02	2000	0200000000	0299999999		<input checked="" type="checkbox"/>
02	2004	0200000000	0299999999		<input checked="" type="checkbox"/>

Figure 299: Created document number ranges

Each document type has to be assigned to a defined number range and number interval. The assignment of number intervals to the number ranges enables a differentiated assignment of intervals to company codes.

The number range buffer is another distinct feature of the SAP™ system. It is possible to buffer each document number object, such as accounting documents, locally. Defined number intervals are assigned to specific application servers or linked entities, and the intervals are available to users who log on to these servers in order to carry out posting activities.

Since not used document numbers are not transferred back to the central number table, but expire without being assigned to a document, the number range buffering results in gaps in the document number sequence. Additionally it is not ensured, that the document numbers are assigned in a timely sequence.

If and which document numbers are to be buffered can be determined in the menu item “number range buffer”. The displayed log shows all number range objects in the SAP™ system. The object RF\_BELEG is assigned to number ranges for accounting documents. The auditor should determine, if the buffer flag has been set for this number range object.

Change documents	
Object	RF_BELEG No. range object has intervals
Short text	Accounting document
Long text	Number Ranges For Accounting Documents
Interval characteristics	
Subobject data element	BUKRS
To-year flag	<input checked="" type="checkbox"/>
Number length domain	CHAR10
No interval rolling	<input type="checkbox"/>
Customizing specifications	
Number range transaction	FBN1
Warning %	10,0
Number ranges not buffered	

Figure 300: Checking the buffer flag for the number range object RF\_BELEG

The number range buffer and its consequences are in compliance, if the gaps in the document number sequence can be explained. This can be checked via the menu

Number ranges  
Overview

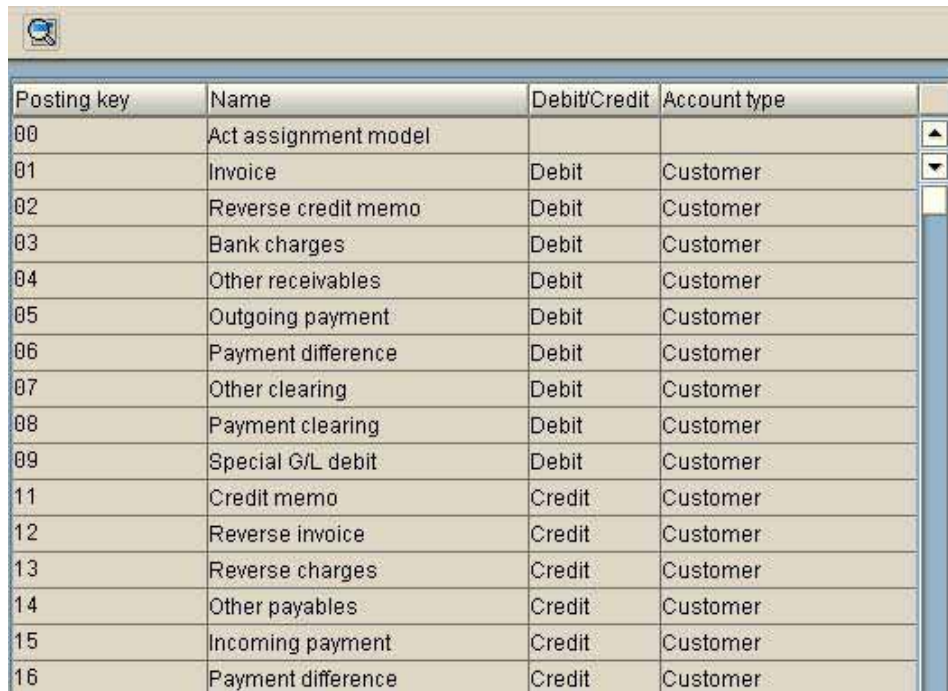
after selecting a company code and display assigned intervals, in the menu “interval / not assigned numbers”.

It has to be noted, that gaps in the document number sequence can occur due to update terminations. For documenting these gaps, there is a defined procedure with manual archiving of deleted posting documents<sup>3</sup>.

<sup>3</sup> See the discussion in section 5.4 on data flow


#### 6.4.2.2.3 Posting key

An overview of the created posting keys in the system can be obtained in the AIS function “posting key”.



Posting key	Name	Debit/Credit	Account type
00	Act assignment model		
01	Invoice	Debit	Customer
02	Reverse credit memo	Debit	Customer
03	Bank charges	Debit	Customer
04	Other receivables	Debit	Customer
05	Outgoing payment	Debit	Customer
06	Payment difference	Debit	Customer
07	Other clearing	Debit	Customer
08	Payment clearing	Debit	Customer
09	Special G/L debit	Debit	Customer
11	Credit memo	Credit	Customer
12	Reverse invoice	Credit	Customer
13	Reverse charges	Credit	Customer
14	Other payables	Credit	Customer
15	Incoming payment	Credit	Customer
16	Payment difference	Credit	Customer

Figure 301: Created posting keys

After marking a posting key detailed information on debit / credit indicator, account type and other properties can be displayed with “choose” . In the next screen, the button “field status” is of interest, displaying field groups (document fields) assigned to this posting key.



Subgroup list

Posting keys 11 Credit memo

Select group

- General data
- Additional account assignments
- Materials management
- Payment transactions
- Asset accounting
- Taxes
- Foreign payments
- Consolidation
- Real estate management
- Financial assets management

Figure 302: Field groups assigned to posting key 11 - credit memo



By selecting a field group, details on fields assigned to this field group can be displayed. This shows if the fields are available for input to the users and if the entries are required or optional.

	Suppress	Req. entry	Opt. entry
Assignment number	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Text	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Invoice reference	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Hedging	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Collective invoice	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Reference specification 1/2	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Reference specification 3	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Inflation revaluation	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Figure 303: Field attributes of the field group

6.4.2.2.4 Tax codes and tax keys

Account assignment elements of major importance for tax relevant business transactions are the tax codes. Output and input VAT or sales tax is calculated according to a defined procedure and posted to the relevant general ledger accounts. In the AIS menu

Tax code

Analysis program

the calculation procedure is displayed in detail.

MWSKZ	KSCHL	TXJCD	STGRP	STAZF	STNSK	STBKZ	KVSL1	KNUMH
A0	MWAS		OUTP VAT			SEP POSTING	MWS	0000000006
A1	MWAS		OUTP VAT			SEP POSTING	MWS	0000000002
A2	MWAS		OUTP VAT			SEP POSTING	MWS	0000000003
A3	MWAS		OUTP VAT			SEP POSTING	MWS	0000001528
A4	MWAS		OUTP VAT			SEP POSTING	MWS	0000006437

Figure 304: Created tax calculations

- 289 -

Calc.procedure TAXD						
Tax code A0 0% domestic output tax						
Tax type A						
Error message for incorrect tax amount X						
Target tax code (for deferred tax)						
Country for tax return						
EU identifier						
G/L account (debit) 175000						
G/L account (credit) 175000						
Log from PRICING call						
Calculation procedure for tax on s/s/purch. code A0						
Cond.type	Description	Percent	Level	From	Acct key	Tax account
BASB	Base Amount		100	000		
MWAS	Output Tax	0,00	110	100	MWS	175000
MWVS	Input Tax		120	100	VST	154000
ZAST	Interest markdown		125	100	ZAS	
MWRK	Travel Expenses (%)		130	100	VST	154000
MWVN	Non-deduct. Input Tax		140	100	NAV	465000
MWVZ	Non-deduct. Input Tax		150	100	NVV	
NLXA	Acqu. Tax Outgoing		200	100	ESA	175000
NLXV	Acquisition Tax Deb.		210	200	ESE	154000

Figure 305: Details on tax calculation procedure "AO"

It is also possible for the auditor to check the clerical accuracy in the calculation procedure at this point. After calling the menu

Account assignment elements

Tax code

Analysis program

the selection screen below is displayed.

<b>Tax customizing</b>	
Company code	0001
Tax code	A1
Jurisdiction code	
<b>Tax calculation</b>	
Amount	7.583,23
Currency	EUR
<input type="checkbox"/> Net	
Date	28.08.1998
Cash discount amount	

Figure 306: Selection screen for the tax analysis program

The company code, the tax code (here A1 = output VAT 15% for calculation procedure TAXD), the amount and display of net or gross value is entered.



Beside further information, the relevant condition type for the tax key (here MWAS) is displayed.

TSP code - dependent data							
MWSKZ	KSCHL	TXJCD	STGRP	STAZF	STNSK	STBKZ	KVSL1
A1	MWAS		OUTP VAT			SEP POSTING	MWS

Figure 307: Condition type for tax code A1

Details on the calculation procedure is displayed by double clicking the condition type. The tax calculation for the amount to be checked is in the lower screen.

Tax calculation			
Gross amount		7.583,23	
Taxes FWSTE	+	989,12	
Taxes NAV	+	0,00	
Taxes NVV	+	0,00	
No.	Tax amount in PC	Tax rate	Acct key
1	989,12	15,000	MWS

Figure 308: Tax calculation for an entered amount and a selected calculation procedure

### 6.4.3 Special general ledger

A major part of the business transactions are only posted in the sub ledgers in the SAP™ system. At the same time, there is a posting in the linked account in the general ledger, in order to update the transaction data. This is done by automatic entries to the reconciliation accounts.

In cases where the generally accepted accounting principles do not allow netting on the linked general ledger accounts, which applies for e.g. receivables and down payments, the reconciliation accounts in the special general ledger are updated. The business transaction (posting code) is assigned to a special general ledger account. The relevant settings are done in the system customizing.

In the menu

Special general ledger

Overview

the special general ledger processes for each company code and account type, including assigned accounts and tax codes can be printed.

Errors, such as not created accounts in a company code, are also displayed.

Chart of accounts	INT	Chart of accounts - international
Company code	0001	SAP A.G.
Acct type D Customer		
Sp.6/L ind A Down payment		
Reconciliation acct	140000	Trade Receivables - domestic
6/L account	170000	Advanced Customer Payments
Acct determinatn tax	A	
Planning level		
Reconciliation acct	140010	Trade Receivables - domestic one-time
6/L account	170000	Advanced Customer Payments
Acct determinatn tax	A	
Planning level		
Reconciliation acct	141000	Trade Receivables - foreign
6/L account	170000	Advanced Customer Payments
Acct determinatn tax	A	
Planning level		
Reconciliation acct	141010	Trade Receivables - foreign one-time
6/L account	170000	Advanced Customer Payments
Acct determinatn tax	A	
Planning level		

Figure 309: Overview of special general ledger processes

Other special general ledger processes with details are grouped by topic and can be called in the AIS menu.

#### 6.4.4 Reconciliation accounts

The reconciliation accounts are general ledger accounts which are automatically updated by entries from the sub ledgers, and can not process direct postings. The general ledger can be reconciled to the sub ledgers at any time.

IDES AG		G/L Account Balances		
Frankfurt		*** REVIDATA-AUDIT-LETTER ***		
Company code	1000	Local currency	DEM	
Previous periods	00-00 1999	Reporting periods	01-16 1999	
Acct no.	Name			
	Curr. BusAr.	C/fwd balance	Previous months	Debit amount
196000	Payment requests - customers			
DEM ****		0,00	0,00	0,00
196100	Guarantees - customers			
DEM ****		0,00	0,00	0,00
196200	Contingent claim for bills of exchange (customers)			
DEM ****		0,00	0,00	0,00
196800	Contingent liabilities - bills/exch. (Italy/Spain)			
DEM ****		0,00	0,00	0,00
196900	IS-RE Advance payment receivable - operating costs			
DEM ****		340,00	0,00	118.523,25
196910	IS-RE Advance payment - operating costs			
DEM ****		57.585,75-	0,00	61.389,75

Figure 310: Reconciliation log for general ledger balances

A log for general ledger balances can be created with the corresponding AIS™ function.

#### 6.4.5 Automatic account determination

This menu supports the audit of automatic account controls. Postings and business transactions with automatic account controls can be displayed by calling the menu

Transaction

G/L accounts

In the menu

G/L account

transaction

a log is generated, which displays utilized tables for the automatic account assignment for specific general ledger accounts.

Evaluation of G/L Account Master Records with Branch to Acct.Determin.

Number	Description	A	PT	ACGR	CUR	LCB	TXCA	PWT	RAC	DIM	OI	SRT	FSTG	IPO
34000	EDV-Software	X		AS	DEM		-	X	A		X		6007	
34010	WB EDV-Software	X		AS	DEM				A				6001	
35000	Konzessionen	X		AS	DEM		-	X	A				6007	
35010	WB Konzessionen	X		AS	DEM				A				6001	
36000	Gewerb. Schutzrechte	X		AS	DEM		-	X	A				6007	
36010	WB gewerb. Schutzre.	X		AS	DEM				A				6001	
37000	Lizenzen	X		AS	DEM		-	X	A				6007	
37001	Lizenzen	X		AS	Account not created 1000 in company code									
37010	WB Lizenzen	X		AS	DEM				A				6001	
38000	Geschäfts/Firmenwert	X		AS	DEM		-	X	A				6007	
38010	WB Gesch/Firmenwert	X		AS	DEM				A				6001	
38020	Mietrechte	X		AS	Account not created 1000 in company code									
39000	Gel. Anzahl. imm.Anl	X		GL	DEM		-B	X	A		X	018	6039	
39010	VST Verr. immat. Anl	X		GL	DEM	X							6001	
39100	Aktiv. Anzahl. imm.A	X		GL	DEM				A		X	018	6007	

Figure 311: Log of automatic account determination

Errors, such as not created accounts, are also displayed in the log. Directly from this log, the user can drill down to the master records of listed general ledger accounts and to the tables for the automatic account determination.

#### **6.4.6    *Quantity structure (database)***

An overview of the administered data in the SAP<sup>TM</sup> system, such as number of accounts, customers, vendors and documents, is required for the audit planning, for determining materiality and for statistical evaluations. Preparatory functions for such purposes are provided in the AIS<sup>TM</sup> menu. These can be set to determine e.g. the number of documents of a specified document type for a certain company (company code) during a defined financial year, by entries in the selection screens and by utilizing dynamic selections.

By determining the number of vendors and customers the auditor will also know if e.g. there is transactions data in the databases, which is not linked to a created customer or vendor master record. This would possibly imply an erroneous automatic recording from sub systems directly in the databases.

The function "data browser (number of entries), transaction SE16" additionally enables the display of the contents and number of entries of any database table on the screen.

#### **6.4.7    *Summary on the organizational overview***

Not all presented functions will be utilized in detail during a financial statement audit or a regular business audit in order to obtain an overview of the organization and structure of the system. However, it should be noted that the information on the business structure and e.g. the document types is absolutely necessary for assessing such things as segregation of duties based on an authorization audit. Additionally, reconciliation problems can be identified with acceptable effort.

#### 6.4.8 Tools for creating an organizational overview

Purpose	Transaction/functions	Tables	Programs
Overview of created document types and related number ranges	AIS + business audit Account assignment elements Document types / magnifier OBA7		
Overview of transactions and assigned document types / posting keys	AIS + business audit Account assignment elements Document types Default values OBU1		
Document type change logs	AIS + business audit Account assignment elements Document type Utilities Change logs		
Number range overview	AIS + business audit Number ranges Overview FBN1		
Check document number buffer	AIS + business audit Number ranges Number range buffer SA38 and program		RSNR0DSP
Overview of created posting keys	AIS + business audit Account assignment elements Posting key OB41		
Overview of posting key details	As above, and magnifier		
Tax code overview	AIS + business audit Account assignment elements Tax code Customizing view FTXP		
Validating of tax code calculation	AIS + business audit Account assignment elements Tax code Analysis program SA38 and program		RFCOR99

Overview and validation of special general ledger processes	AIS + business audit Organizational overview Special general ledger Overview list SA38 and program		SAPUFKB2
Overview of reconciliation account balances	AIS + business audit Organizational overview Reconciliation accounts SA38 and program		RFSSLD00
Error analysis of automatic account determination	AIS + business audit Organizational overview Automatic account determination SA38 and program		RFAUDI30
Determine quantity structure of master records	AIS + business audit Organizational overview Quantity structure SE16 and tables	Miscellaneous	

Notes:

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and extend across the width of the page. There are no margins, text, or other markings on the paper.

**Exercises on organizational overview**

- 1 Determine the document type for posting customer invoices and which number range has been assigned.

---

---

---

---

- 2 Determine the transaction for posting an asset retirement, which results in a customer invoice.

---

---

---

---

- 3 Are there default values for the document type and the posting key for the transaction above?

---

---

---

---

- 4 Determine if customer invoices were posted with the transaction for asset retirement in 1999.

---

---

---

---

- 5 Determine which posting key is being used for posting payment differences; which account type has been assigned and which debit / credit indicator is used.

---

---

---

---



6 Create an overview of the tax codes for Germany.

---

---

---

---

7 Obtain more details on the tax code A1 (company code 1000). Which condition key and which account key is valid?

---

---

---

---

8 Check the tax calculation for a gross vendor invoice amount of EUR 5.832,76.

---

---

---

---

9 Determine the balance of the reconciliation account 175000 for the financial year 1999.

---

---

---

---

10 Check if VAT relevant postings are processed correctly in the “automatic account determination” (chart of accounts INT in company code 1000).

---

---

---

---

---

- 11 Determine (for chart of accounts INT in company code 1000) which accounts are being used for FI account assignments in the “automatic account determination”.

---

---

---

---

- 12 Display details on the settings for account 175000 from the overview above.

---

---

---

---

- 13 Determine the number of canceled outgoing invoices for company code 1000 in 1998.

---

---

---

---

Notes:

---

---

---

---

---

---

---

---

---

---

**Checklist for business audits  
(organizational environment)**

- ☐ Mapping clients and company codes
  - Purpose of the utilized organizational units
  - Client modifiability
  - Utilization in the production system
  - Other settings
  
- ☐ Mapping and auditing the account assignment elements
  - Document types / change logs
  - Number ranges / buffer / status
  - Posting key
  - Tax code / validation
  
- ☐ Special general ledger and reconciliation accounts
  - Overview
  - Validation / errors
  - Reconciliation amounts
  
- ☐ Automatic account determination
  - Overview
  - Validation a sample of specific procedures
  
- ☐ Quantity structure
  - Overview
  - sampling

## 6.5 Functions for auditing balance sheet items

### 6.5.1 Introduction

The functions for business audits in the AIS™ system have been designed to meet the requirements for information and analyses within the scope of financial statement audits. The structure is similar to a balance sheet and covers the following areas:

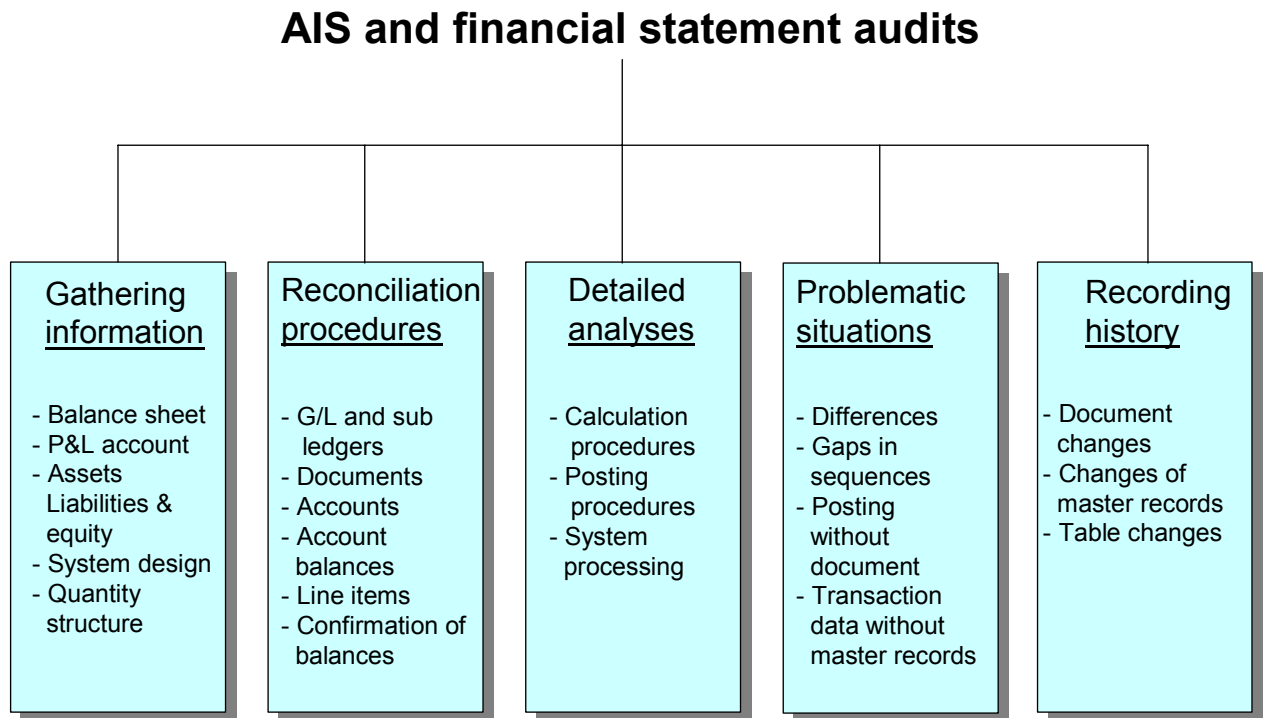


Figure 312: Supporting functions in the AIS™ system for the financial statement audit

The complete financial accounting can be comprehended any time in the complex integrated SAP™ system, where timely recording of business transactions in a journal, the assignment to accounts, the business overviews of the balance sheet and the profit and loss account can be analyzed.

The AIS system supports the mapping of information regarding specific balance sheet items and assigned accounts. Valuation effects on balance sheet items can be analyzed in detail. By utilizing implemented control programs, it can be determined if the posting records are complete, correct, timely, orderly and comprehensible - as far as the SAP™ system is involved.

The required reconciliation programs are also implemented in the AIS system. And the AIS functions offer the possibility to transfer document data and master records to audit software in a pre-defined format via a standardized interface, in order to enable additional plausibility checks.

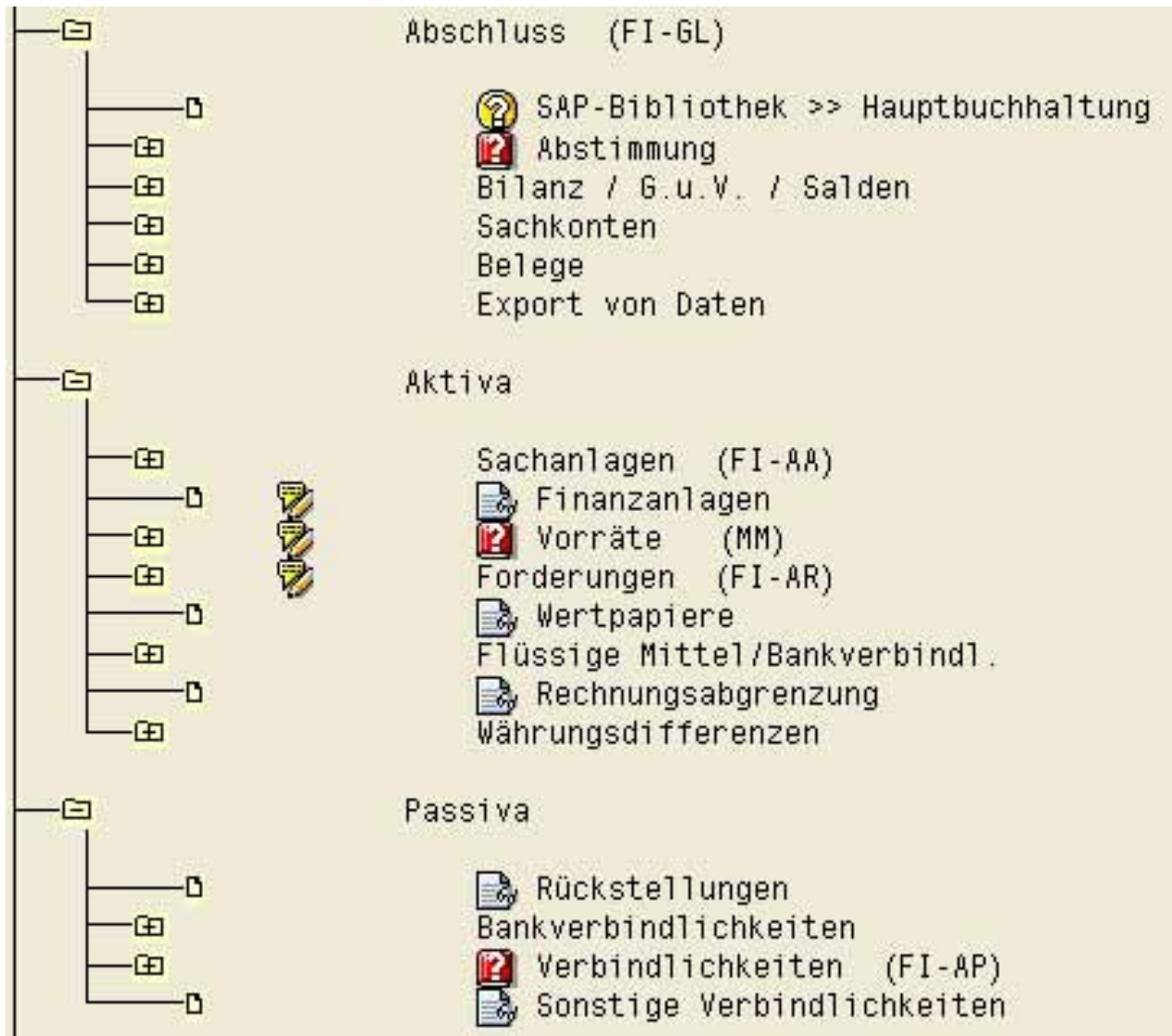


Figure 313: AIS functions supporting financial statements audits

The major part of the supporting functions for financial statement audits does not need to be explained. There is sufficient documentation for the reports, which generate relevant information for the year end closing. The AIS system provides wide ranging additional documentation too. At this point, merely special control programs and procedures will be discussed, which describe or enable further analyses of specific problematic situations in the SAP<sup>TM</sup> system.

## 6.5.2 Functions in the menu closing (FI-GL)

### 6.5.2.1 Reconciling accounts and documents

The global accounting reconciliation procedure for agreeing the transactions data on customer, vendor and general ledger accounts to the debit and credit totals in posted documents can be found in the menu "accounting reconciliation". There are several plausibility checks during running operations in the production system in order to ensure that such inconsistencies do not occur. Nevertheless, specific and in particular technical problems or a poorly secured direct recording of accounting data in the databases may result in differences, which should be revealed in the global accounting reconciliation procedure.

The provided report enables the reconciliation of transaction data on the accounts to the so-called user-indices, which are controlling the assignment of specific line items to the accounts.

The account and document totals are displayed for specific periods. If differences between the accounts and the documents or between accounts and user-indices occur, these will be displayed with information on amounts and accounts.

Display Totals				
Documents/transaction figures				
CoCd Year Periods				
AT Curr.	Debit items	Debit master	Credit	
1000 1998 01 - 16				
D DEM	12.684.191,84	12.684.191,84	16.052.0	
K DEM	0,00	0,00	3.865.5	
S DEM	44.169.163,64	44.169.163,64	44.169.1	
Indexes/transaction figures				
CoCd Year Periods				
AT Curr.	Debit indexes	Debit master	Credit i	
1000 1998 01 - 16				
D DEM	12.684.191,84	12.684.191,84	16.052.0	
K DEM	0,00	0,00	3.865.5	
S DEM	25.517.542,46	25.517.542,46	16.536.3	

Figure 314: Reconciliation log for the global accounting reconciliation procedure

Depending on the volume of postings and other selection parameters, it may take some hours to run the reconciliation report. It should be run during periods without dialogs and with low system load. Audit periods to be reconciled should be closed prior to running the program in order to avoid program terminations.

Berechtigungen usw. Ettlingen	Indexes/transaction figures master comparison Accounts with differences
A CoCd Acct no. T	
No differences have appeared.	

Figure 315: Result of the global accounting reconciliation procedure

SAP™ recommends the reconciliation report to be run during the financial year by the accounting department, in order to reveal inconsistencies on a timely basis and enable them to be solved. In the menu “accounting reconciliation / comparative analysis -> historical display” it can be determined, when the reconciliation report was run and if errors were detected.

Totals		Accounts	
11.11.1999	15:02:47	OLBERT	OK
25.05.1999	08:56:11	SCHUNTER	Errors
19.05.1999	12:35:09	SCHUNTER	OK
28.12.1998	13:37:11	SCHUNTER	OK
24.11.1998	15:35:33	SCHUNTER	OK
24.11.1998	14:58:36	SCHUNTER	OK
28.10.1998	09:19:48	SCHUNTER	OK
28.10.1998	09:18:45	SCHUNTER	OK
21.08.1998	11:02:14	UHRIGA	Errors
21.08.1998	11:01:59	UHRIGA	Errors
21.08.1998	11:00:27	UHRIGA	Errors

Figure 316: Historical display of the global accounting reconciliation procedure

Documents/transaction figures
CoCd Year Periods
AT Acct no.
1000 1999 01 - 16
D 1001
S 113109
S 140000
S 175000
S 881000
Indexes/transaction figures
CoCd Year Periods
AT Acct no.
1000 1999 01 - 16
D 1300
S 113109

Figure 317: Error log in the global accounting reconciliation procedure





The inquiries on balance sheet items can be drilled down to account level. On every level it is possible to display relevant documents by calling the menu

Goto

Line items

St	Assignment	Doc.no.	BA	Type	Doc. date	PK	Amount in local cur.	LCurr	Tx	Clrng
<input type="checkbox"/>	<input checked="" type="checkbox"/>	100000645	1000	AB	13.06.1995	70	470.000,00	DEM	V0	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	100005800	1000	SA	31.12.1995	75	4.220.000,00-	DEM	V0	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	100007293	1000	AA	31.12.1995	75	1.100.000,00-	DEM	V0	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	100007293	1000	AA	31.12.1995	70	4.222.000,00	DEM	V0	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	100007295	1000	AA	31.12.1995	75	4.222.000,00-	DEM	V0	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	100007323	1000	AA	31.12.1996	70	1.100.000,00	DEM	V0	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	100000012	1000	AA	01.06.1994	70	3.500.000,00	DEM	V0	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1000000001000000	1000	AA	02.02.1994	70	500.000,00	DEM	V0	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1000000001006000	1000	AA	05.12.1994	70	750.000,00	DEM	V0	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1000000001107000	1000	AA	01.01.1994	70	1.000.000,00	DEM	V0	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1000000001108000	1000	AB	01.01.1994	75	1.000.000,00-	DEM	V0	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1000000001108000	1000	AA	01.01.1994	70	470.000,00	DEM	V0	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1000000001108000	1000	AA	01.01.1997	75	470.000,00-	DEM	V0	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1000000001113000	1000	AA	15.01.1996	70	13.000.000,00	DEM	V0	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1000000001113000	1000	AA	30.06.1996	75	1.000.000,00-	DEM	V0	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1000000001120000	1000	AA	01.01.1997	70	16.000.000,00	DEM	V0	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1000000001129000	1000	AA	01.01.1997	70	3.000.000,00	DEM	V0	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1000000003024000	1000	AA	01.01.1995	70	100.000,00	DEM	V0	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1000000003024000	1000	AA	18.01.1996	70	200.000,00	DEM	V0	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	100005779	1000	AA	18.12.1996	75	1.300.000,00-	DEM	V0	
*	<input checked="" type="checkbox"/>						31.000.000,00	DEM		
**		Account 1000					31.000.000,00	DEM		

Figure 320: Display of line items for a selected balance sheet item

As the list is interactive, the relevant document can be displayed by double clicking the line item.

G/L account: 1000 Real estate and similar rights	
Asset: 1107	0 Vertriebsbüro Region Süd
Company code: 1000	Doc. no.: 100000081
IDES AG	
Line Item 1 / Debit asset / 70 External asset acqui / 100	
Amount: 750.000,00	DEM
Tax code: V0	W/o cash disc.
Additional details	
Asset val. date: 05.12.1994	
Quantity: 0,000	
Business area: 1000	Trdg part.BA:
	Order:
	Asset: 1107 0
WBS element:	

Figure 321: Display of selected document items

In the section “reporting” in this manual, several features of interactive reports, such as filtering certain items, graphical layout of value fields and the direct download to Excel etc, were described. These options also apply for the reports described in this section.

### 6.5.2.3 Balances

This AIS<sup>TM</sup> menu offers the financial statement auditor any account balances he might need. Beginning with the basic overview of general ledger account balances

IDES AG Frankfurt		G/L Account Balances *** REVIDATAT-PRÜFLISTE ***			Time 11.51.03	Date 18.12.2002
Company code 1000		Local currency DEM		RFSSLD00/RV-TEST4		Page 1
Previous periods 00-00 2001		Reporting periods 01-16 2001				
Acct no.	Name					
	Curr. BusAr.	C/fwd balance	Previous months	Debit amount	Credit amount	Total debit bal Total credit bal
001000	Real estate and similar rights					
DEM ****		0,00	0,00	0,00	0,00	0,00
001010	Accum. depn - real estate and similar rights					
DEM ****		0,00	0,00	0,00	0,00	0,00
002000	Buildings					
DEM ****		0,00	0,00	0,00	0,00	0,00
002010	Accumulated depreciation-buildings					
DEM ****		0,00	0,00	0,00	0,00	0,00
000000****	DEM ****	0,00	0,00	0,00	0,00	0,00
011000	Machinery and equipment					
DEM ****		0,00	0,00	0,00	0,00	0,00

Figure 322: Basic general ledger account balances

and ranging to detailed comparisons to previous years and key figure oriented reports on opening and year-end items, the auditor can generate any report he can think of.

## 6.5.3 General ledger account information

### 6.5.3.1 Overview

Comprehensive information on general ledger accounts within a company code to be audited, such as current chart of accounts, detailed account index of all general ledger accounts accessible for postings, detailed account information and their changes can be obtained in the AIS<sup>TM</sup> menu

G/L accounts

Master records

Overview

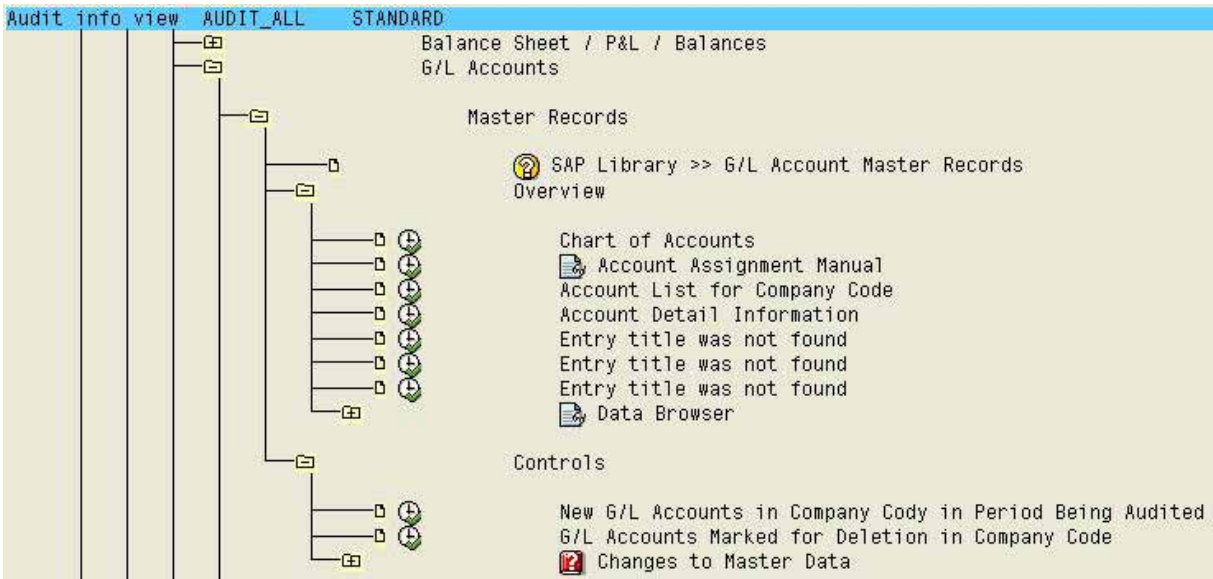


Figure 323: Menu for calling information on general ledger accounts

Experience show, that lack of knowledge among the users about the purpose of specific accounts result in quality problems with accounting data. An account assignment manual should be prepared in order to explain the account assignment procedures for at least critical accounts and business transactions. This is a task of the system operators, and the auditor should determine if such a manual is in place and also the level of detail.

6.5.3.2 *Creating and changing general ledger accounts*

Creation and changes of general ledger accounts can be audited in the menu

- G/L accounts
- Master records
- Controls

Berechtigungen usw. Ettlingen		G/L Account List *** REVIDATAT-PRÜFLISTE ***		T R
G/L accountChartofaccts: INT = Chart of accounts - international				
CoCd Sort: G/Laccount, Companycode				
100010	Petty cash (with cash journal)	Account group		CASH
Creation data for chart of accts				
Created by OLBERT		Created on		04.08.99
1000 IDES AG				
Creation data for company code				
Created by OLBERT		Created on		04.08.99

Figure 324: Log of new general ledger accounts



### 6.5.3.3 Analyzing general ledger accounts

In the general ledger accounts menu

G/L accounts

Account

specific accounts can be analyzed in detail. The offsetting account analysis displays the frequency of debit and credit entries for selected accounts in an interactive report. The overview also contains the cumulated posting value and the medium value for each posting of the posted total amount.

\*\*\* **Audit letter** \*\*\* **Offsetting account analysis for G/L account**

Document header for company code 1000 Doc. number 100005800 not found  
Document header for company code 1000 Doc. number 100005801 not found

36 Archived documents were selected

18.12.2002 12:26:39 Offsetting account freq. Page 2					
A	Offsetting	D	Amount in LC UNI	Total Number	Medium Value
A	1010	H	2.686.062,31-	72	37.306,42-
A	11000	H	87.600,00-	8	10.950,00-
A	11010	H	1.432.821,00-	84	17.057,39-
A	21000	S	1.665.680,00	27	61.691,85
A	21000	H	6.132,00-	41	149,56-
A	21010	H	547.500,00-	108	5.069,44-
A	32000	H	17.799.568,96-	12	1.483.297,41-
D	1000	S	1.000,00	1	1.000,00
D	1001	S	8.666.951,60	21	412.711,98
D	1001	H	10.129.986,20-	19	533.157,17-
D	1002	S	5.016.206,00	22	228.019,45

Figure 325: Detailed analysis of offsetting account frequency

For accounts considered to be critical, the auditor can drill down to specific documents from the interactive list.

### 6.5.4 Document information

#### 6.5.4.1 Overview

The auditor can obtain detailed overviews of documents in the journal in the menu

Documents

Overview

- 309 -

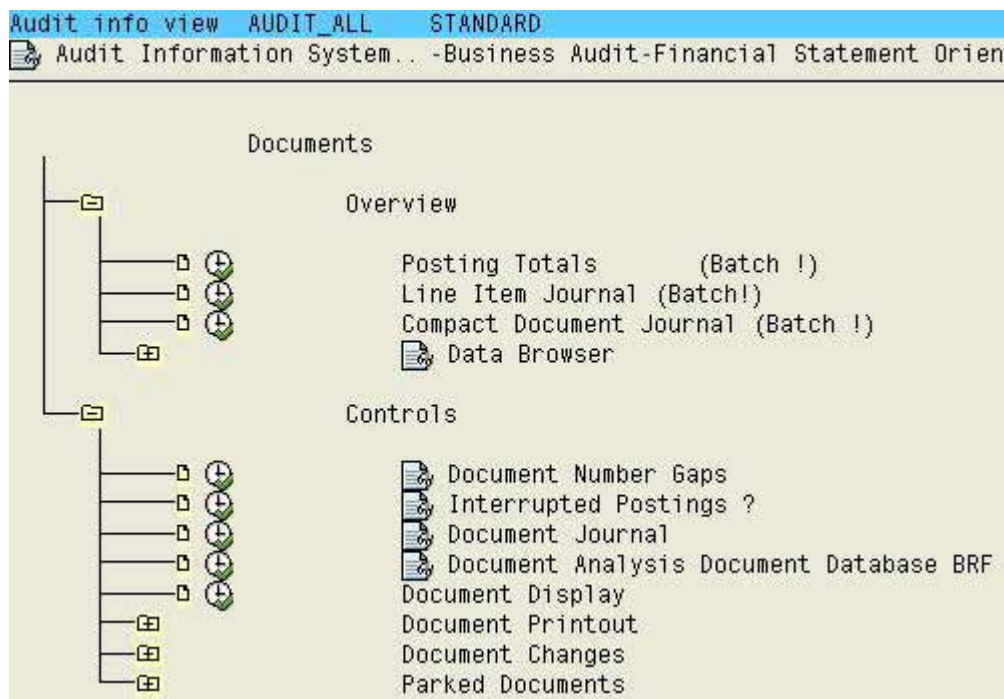


Figure 326: Functions for analyzing documents

With the line item journal the auditor can display any useful information for a selected company code on the screen.

IDES AG Frankfurt							Line Item Journal *** Audit-Letter ***			
Pstg	CPU	Document	Lin Doc.	Bus.	Po G S	Account	User	Curr.	D/C amount	
date	date	number	itm date	ar	ky L C	number	name	key		
Company code		1000	Account type S	Document type	DR	Sales type	Posting period	1399		
311299	130300	1800000255	001	311299	9100	40	0000140099	OLBERT	DEM 48,00	
311299	130300	1800000255	002	311299	9100	50	0000163000	OLBERT	DEM 48,00-	
311299	130300	1800000256	001	311299	9900	40	0000140099	OLBERT	DEM 180,00	
311299	130300	1800000256	002	311299	9900	50	0000163000	OLBERT	DEM 180,00-	
1000 S DR		1399	* DEM						0,00	

IDES AG Frankfurt							Line Item Journal *** Audit-Letter ***			
Pstg	CPU	Document	Lin Doc.	Bus.	Po G S	Account	User	Curr.	D/C amount	
date	date	number	itm date	ar	ky L C	number	name	key		
Company code		1000	Account type S	Document type	KR	Sales type	Posting period	1299		
041299	050100	1900004848	002	041299	9100	40	0000470400	EISENMANN	DEM 19.088,79	
041299	050100	1900004848	003	041299		40	0000154000	EISENMANN	DEM 3.054,21	

Figure 327: Calling the line item journal for a selected company code

If further information regarding the quantity of document or line items is required for the purpose of stochastic audit activities or for selecting a sample, the function “data browser” in the AIS menu can be utilized. After selecting the parameters, such as company code, financial year and document number interval, the button **Number of entries** is clicked to display the quantity.

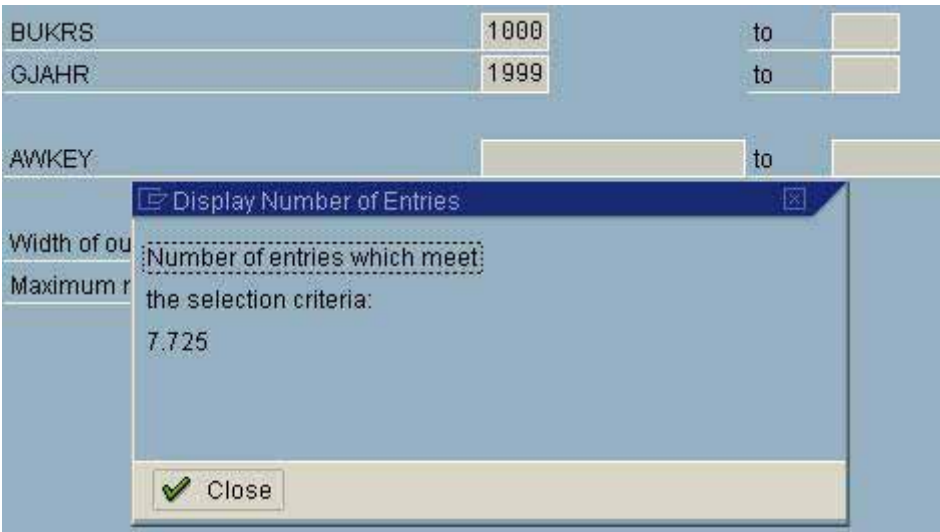


Figure 328: Determining the number of documents for selected parameters

6.5.4.2 *Checking document completeness and single items*

Gaps in a document number range can – as explained earlier - occur due to document number buffering or update terminations, which can not be corrected. If the gaps can be explained, they do not affect the system compliance. Defined procedures and documentation have to be in place <sup>4</sup>. Document number gaps and update terminations (menu “interrupted postings”) can be called in the menu “documents” and the sub menu “controls”.

Number range 01 of 1994 to year 1999		
Interval of	0100000000	To 0199999999 Number 0100013154
Fehlende Belegnummern		Mehrfach vergebene Belegnummern
100000041	... 100000044	
100000285	... 100000287	
100000295	... 100000296	
100000300	... 100000302	
100000307	... 100000309	
100000314	... 100000315	
100000321	... 100000328	
100000335		
100000349	... 100000350	
100000352	... 100000368	
100000370	... 100000379	
100000381		
100000383	... 100000392	

Figure 329: Log on gaps in document number assignment

<sup>4</sup> For detailed discussion, see the section on „data flow“ in this manual



The auditor should generate such a log of gaps and a list of update terminations.

Demonandant		FI-Beleg: Liste abgebrochener Verbuchun			
<hr/>					
<b>Belegkopf</b>					
Benutzername	BECKERU	Transaktion	MB01		
Erfaßt am	25.07.00	Erfaßt un	10:49:26		
Buchungskreis	1000	Belegnummer	5000000136	Geschäft:	
Buchungsdatum	25.07.00	Belegdatum	25.07.00	Belegart:	
Währung	DEM	Unrechnei			
<hr/>					
<b>Belegpositionen</b>					
Konto	BS SHB	HW-Betrag	FW-Betrag	Steuerken	
410000	81	1.240,00	1.240,00		
191100	96	1.240,00-	1.240,00-		
<hr/>					
command ag Demonandant		FI-Beleg: Liste abgebrochener Verbuchun			
Ettlingen					
<hr/>					
<b>Belegkopf</b>					
Benutzername	BERTSCH	Transaktion	MB10		
Erfaßt am	12.07.00	Erfaßt un	15:03:26		
Buchungskreis	1000	Belegnummer	4900000153	Geschäft:	
Buchungsdatum	12.07.00	Belegdatum	12.07.00	Belegart:	

Figure 330: List of update terminations

Based on this information, the auditor can determine if the gaps are documented and can be explained.

#### 6.5.4.3 Detailed document analyses

Selected document data can be analyzed in detail in the menu “documents / control” by utilizing the function “document analysis document database BRF”.

*** Audit letter *** Export/analysis from document database											
Document no.	Fiscal ye...	Entry date	Changed	Last updt	T code	User na...	S	Rev. with	Fiscal year	Document ty...	Curren
100009801	1999	15.01.1999	00.00.0000	00.00.0000	K088	HAMED				SA	DEM
100009801	1999	15.01.1999	00.00.0000	00.00.0000	K088	HAMED				SA	DEM
100009802	1999	15.01.1999	00.00.0000	00.00.0000	K088	HAMED				SA	DEM
100009802	1999	15.01.1999	00.00.0000	00.00.0000	K088	HAMED				SA	DEM
100009803	1999	15.01.1999	00.00.0000	00.00.0000	K088	HAMED				SA	DEM
100009803	1999	15.01.1999	00.00.0000	00.00.0000	K088	HAMED				SA	DEM
100009804	1999	15.01.1999	00.00.0000	00.00.0000	K088	HAMED				SA	DEM
100009804	1999	15.01.1999	00.00.0000	00.00.0000	K088	HAMED				SA	DEM
100009805	1999	15.01.1999	00.00.0000	00.00.0000	K088	HAMED				SA	DEM
100009805	1999	15.01.1999	00.00.0000	00.00.0000	K088	HAMED				SA	DEM

Figure 331: Detailed analysis of document data

It can e.g. be determined, if documents in a specific document number range were posted in the pre-defined posting month and in the proper period.

The report is displayed in an interactive format, which enables further analyses, such as filtering the selected data, display sums or specific line items etc.

6.5.4.4 Document changes

The SAP™ allows certain document elements to be changed after the posting and the changes are documented.

IDES-ALE: Central FI Syst Frankfurt - Deutschland				Change display: documents Sort by document number	
Date	Time	Changed by	Itm	Field nme	New value
Technical field name					
Company code	1000	Document no.	5100005034	Fiscal year	1999
05.01.1999	16:44	GRAUENHORST	001	F1	
				BSEGM-FDLEV	
			001	BSEGM-ZLSPR	
05.01.1999	16:44	GRAUENHORST	001	X	
				BSEGM-SPGRT	
Company code	1000	Document no.	5100005123	Fiscal year	1999
22.04.1999	16:39	GRAUENHORST	001	F1	
				BSEGM-FDLEV	
			001	BSEGM-ZLSPR	
22.04.1999	16:39	GRAUENHORST	008	X	

Figure 332: Log of changed documents

The changes can be tracked to the field level in the menu “document changes”.

6.5.4.5 Exporting data to the auditor’s software

In many cases, the financial audits are supported by external software, such as Audit-Agent, special analyses in Baetge-programs or specified audit software. SAP™ has created direct interfaces for such programs, which enable data and related data record descriptions to be exported directly to the external programs.

The requirements for the data export to external programs will not be discussed at this point, but in the following section.

Notes:

---

---

---

---

---

---

---

---

## 6.6 Other functions for auditing assets and liabilities & equity

The options for analyses in the menu “closing” as presented in the previous section basically apply to all other menu items for auditing assets, liabilities and equity

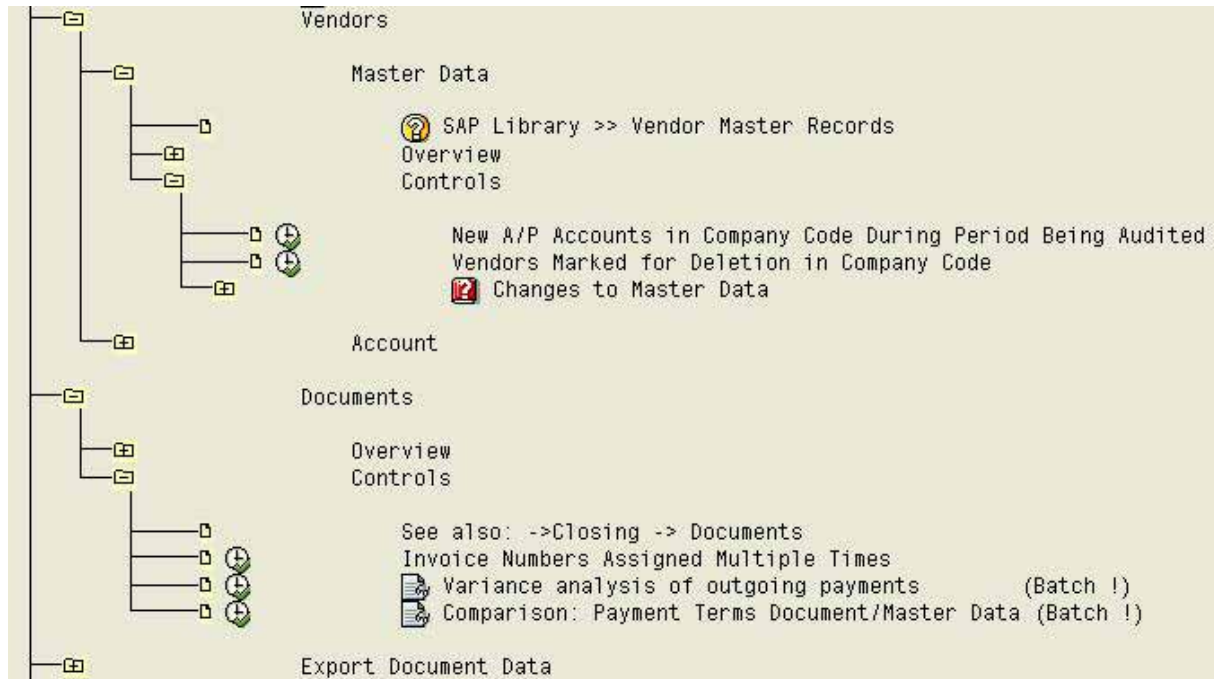


Figure 333: AIS™ functions for auditing vendors in the menu liabilities & equity

The menus include in particular

- Reconciliation between general and sub ledgers
- Master record overviews for fixed assets, customers, vendors and banks
- Plausibility checks, such as duplicate document numbers
- Detailed line item analyses of transaction data on accounts and offsetting accounts
- Plausibility checks on outgoing and incoming payments and the related conditions
- Exporting master records and document data

In order to avoid repeating the topics discussed in previous sections, we recommend the reader to study the previous sections on reports, setting options and requirements in detail <sup>5</sup>.

<sup>5</sup> Further notes on auditing a complete SAP business process based on a case study with vendor and payment processing can be found in the manual „Process oriented audits in the SAP R/3™ system“ by the same author.

## 7 Exporting AIS™ data to audit software

### 7.1 Requirements for the export

#### 7.1.1 Setting up a private folder

For the auditor to export document data from SAP R/3™ to a folder of his choice, the system administrators must set up a specified "USER-EXIT" (SQUE0001) and activate a linked "INCLUDE" after the AIS system has been installed. The system administrators will find the relevant documentation – after activating the help function as described in section 1 – in the menu

Business audit

Closing

Export data

Export document data

From document database BRF

Specific, 2<sup>nd</sup> phase, batch/dialog, w/field description

#### Audit Information System: Display

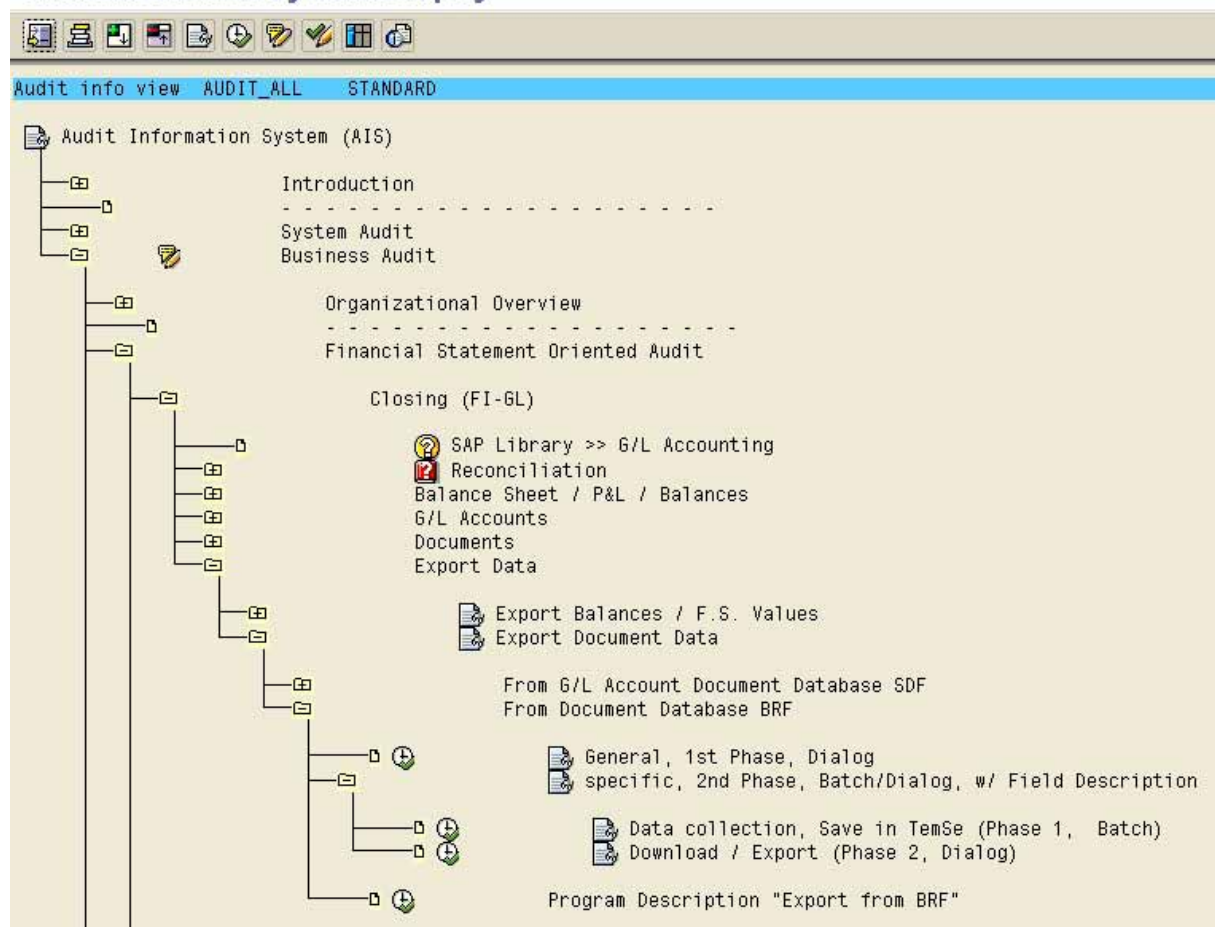


Figure 334: Calling the menu for context sensitive help

The set-up is described in detail in section III.6

By double clicking this menu item further information about “USER-EXIT” will be displayed on the screen.

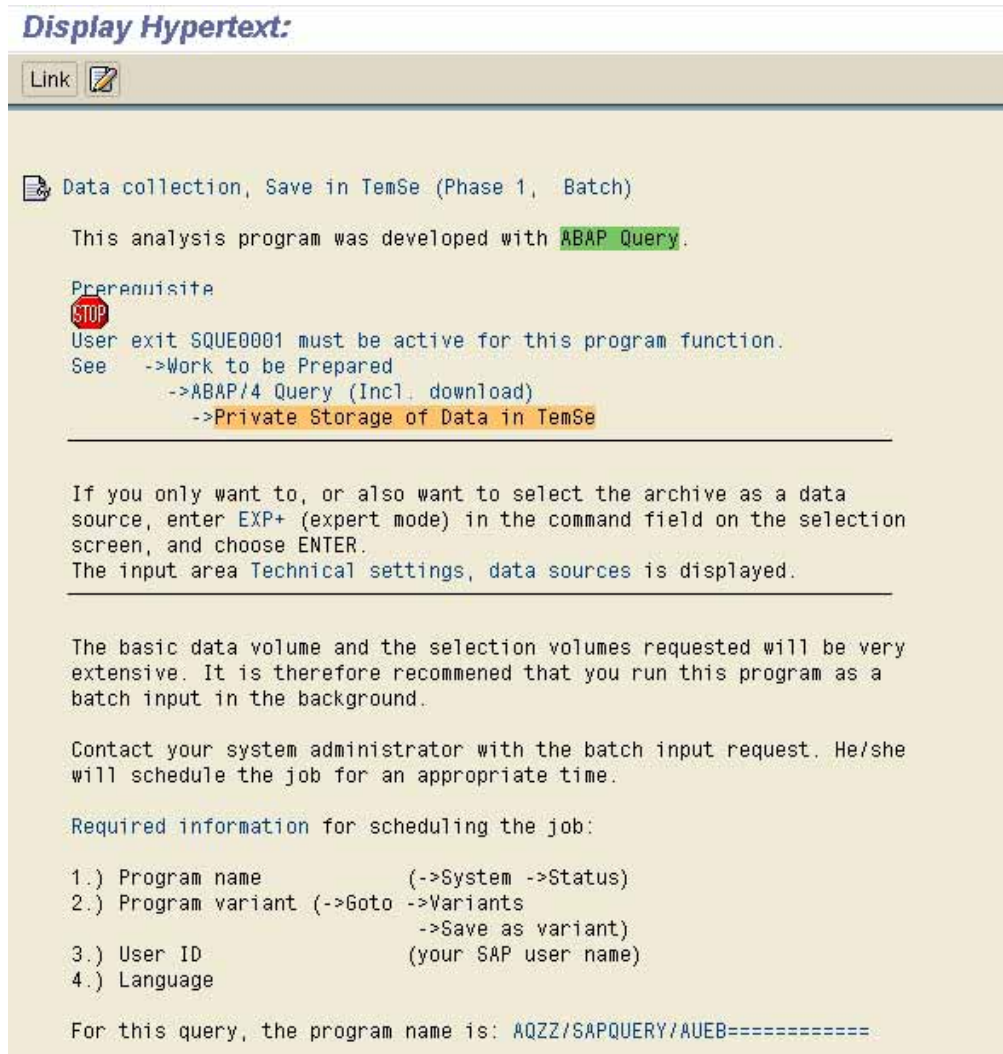


Figure 335: Documentation on USER-EXIT

The effort for setting up the Audit Information System and the subsequent set up of the USER-EXIT is acceptable, and it usually does not take more than a few hours.

### 7.1.2 Requirements for exporting data from SAP™ Query and Quick View

The utilization of the list generator SAP™ Query is based on the philosophy, that users generate reports and lists of their own interest independently. To avoid asking too much of the users regarding the vast amount of table fields, tables and related links, and still ensure proper system operations, the user access is restricted to pre-defined data areas, so called functional areas.

In a second step user groups are created, for example for the auditors, and these groups are assigned to the functional areas, which are grouped by topics such as materials, human resources or customer data, in order to provide a task related access to specific functional areas.



Since the system developers are utilizing the list generator for satisfying report requests from users, there are usually several pre-defined functional areas in the system <sup>6</sup>. Additional interesting functional areas are created in the SAP<sup>TM</sup> production system when the AIS<sup>TM</sup> system is installed.



Figure 336: Functional area STORAGE LOCATION with pre-defined lists

It is necessary for the auditors to discuss and co-ordinate the creation of an audit user group with the administrators, and assign appropriate functional areas with data of audit interest to this user group. If the administrators object, the auditors can argue that only those with SAP<sup>TM</sup> experience and training for SAP<sup>TM</sup> Query will be included in the user group. The auditors will be able to develop their own data reports and export these to audit software.

Even if there is no possibility for developing their own reports with SAP<sup>TM</sup> Query, it is still useful to create an audit user group.

The user group enables the system developers to create so called queries within the selected data sphere upon the auditor's request, which are available for direct export to audit software.

The final step of the preparations, is to assign the proper authorizations to the internal auditors for creating and calling the created queries.

### 7.1.3 Requirements for the audit software

The direct export of document data to audit software requires certain program versions.

ACL (Audit Command Language) has to be installed in version 6 or higher. The version 6.5 with an integrated import assistant was introduced recently, and enables an easy import of SAP<sup>TM</sup> data.

Document data can be imported to the audit software WinIDEA version 3.0 and higher. This and newer versions also have a menu supported import assistant, which makes the import of SAP<sup>TM</sup> data rather easy.

<sup>6</sup> Details for setting up functional areas can be found in section IV.3.4 in this manual

- 317 -

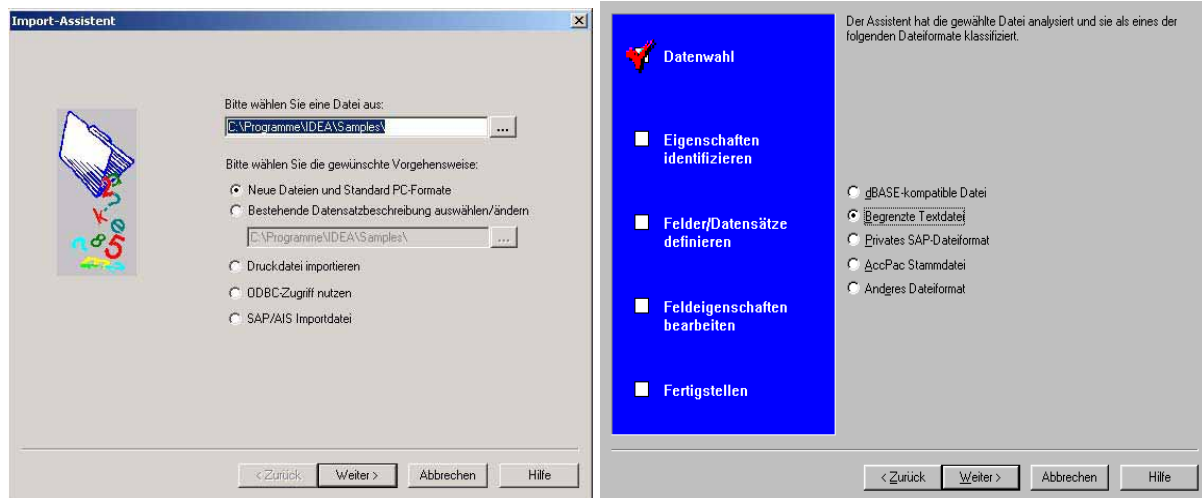


Figure 337: Menu supported import assistants in WinIDEA and ACL

## 7.2 Data export and import

### 7.2.1 Data export from the AIS™ system

For exporting FI document data, the AIS™ system is called with transaction SECR. The selection screen for the document data is called in the menu

Business audit

Closing

Export data

Export document data

From document database BRF

Specific, 2<sup>nd</sup> phase, batch/dialog, w/field description

Data collection, save in TemSe

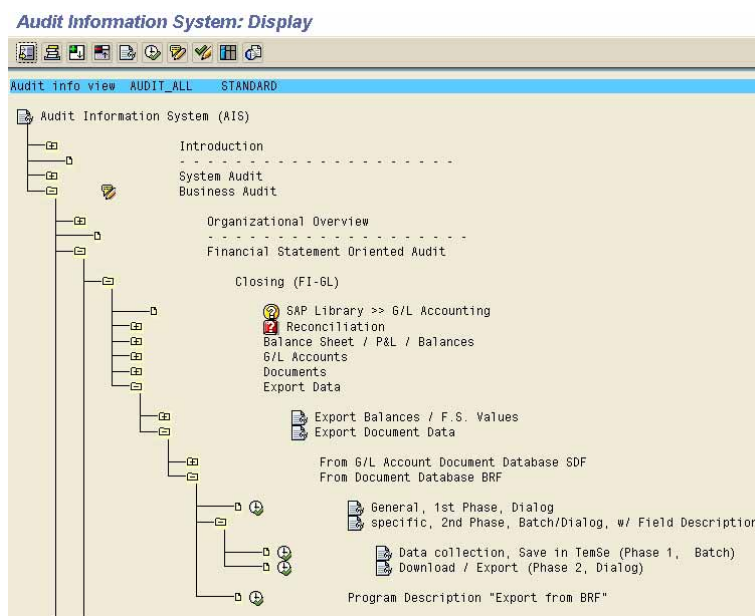


Figure 338: Calling the download function



The program requires entries for company code, document number interval or a fiscal year.

\*\*\* Audit letter \*\*\* Export/analysis from document database

Company code 1000 to [ ]

Document number 1800000000 to 1900000000

Fiscal year 1999 to [ ]

General selections

Posting date 01.01.1999 to 31.12.1999

Program selections

☒ Decimal comma instead of decim

Further processing options

☒ Private file

Figure 339: Entries in the selection screen

After entering the required data, the auditor should activate the option “decimal comma instead of decim” The option “private file” is marked in the default setting. The auditor confirms his entries and is requested to enter a menu path for the data transfer to a local file.

Transfer to a Local File

File name C:\Temp\Behnert.dat

Transfer [X]

Figure 340: Entering a menu path and a chosen file name

The transfer can be started. After the successful data transfer, a message about the administration of the temporary TemSe file is displayed.



Figure 341: Message on the successful data transfer

In this screen, the button “delete” can be clicked.

The described procedure is creating a file, which contains the names of the original SAP™ data fields and their descriptions and contents.

BKPF-BUKRS	BKPF-BELNR	BKPF-GJAHR	BKPF-CPUDT	BKPF-AEDAT	BKPF-UPDI
Buchungskreis	Belegnummer eines Buchhaltungsbeleges	Geschäftsjahr	Tag der Erfassung de		
1000	1700000086	1998	10.06.1998	FB08	MUELLERJ
1000	1700000086	1998	10.06.1998	FB08	MUELLERJ
1000	1700000086	1998	10.06.1998	FB08	MUELLERJ
1000	1700000087	1998	10.06.1998	FB08	MUELLERJ
1000	1700000087	1998	10.06.1998	FB08	MUELLERJ
1000	1700000087	1998	10.06.1998	FB08	MUELLERJ
1000	1700000088	1998	10.06.1998	FB08	MUELLERJ
1000	1700000088	1998	10.06.1998	FB08	MUELLERJ
1000	1700000089	1998	10.06.1998	FB08	MUELLERJ
1000	1700000089	1998	10.06.1998	FB08	MUELLERJ
1000	1700000089	1998	10.06.1998	FB08	MUELLERJ
1000	1700000090	1998	10.06.1998	FB08	MUELLERJ
1000	1700000090	1998	10.06.1998	FB08	MUELLERJ

Figure 342: Display of transferred file (extract)

Based on this information, the audit software can read the file directly, without further data record descriptions.

7.2.2 Data export from SAP™ Query and Quick View

The data export from functional areas of the auditor's choice and in pre-defined lists is initiated in the transaction SU00 or by calling the menu

System  
Services  
Quick viewer



Figure 343: Calling the QUERY function in SAP R/3™

The audit user group possibly has to be selected in the menu edit / other user group. After the AIS™ system has been installed, the user group AU (audit) is available, with interesting functional areas and reports.

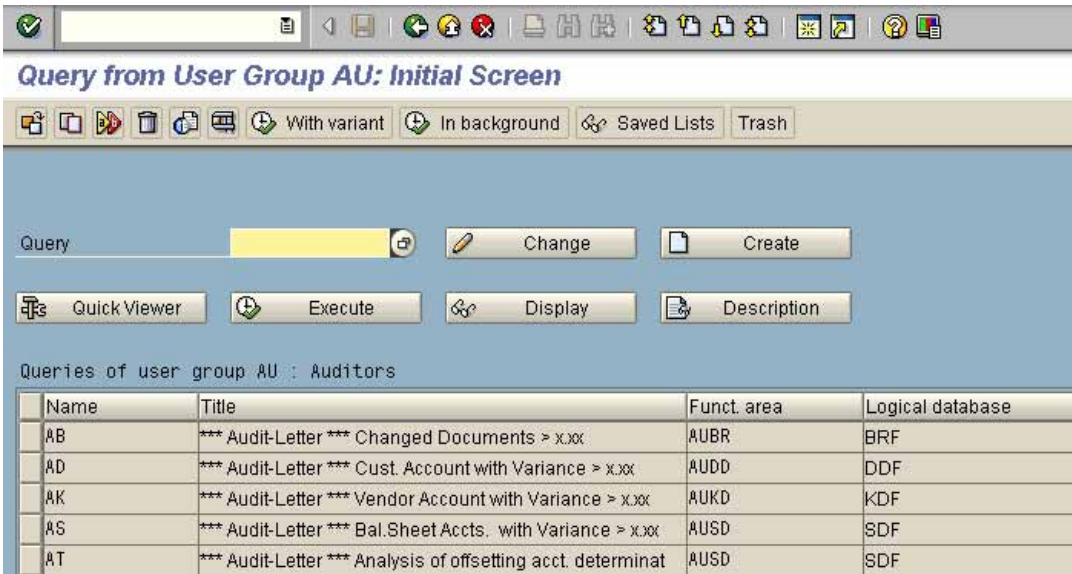


Figure 344: User group AUDIT and the pre-defined reports

In a second step, a report (list) with appropriate fields is selected for the export to the audit software and the button “execute” is clicked.

The displayed selection screen contains the menu “further processing options” in the lower screen. If no private file has been set up with a USER-EXIT (7.1.1) which can be utilized, the item “file store” is marked. The list can be started.

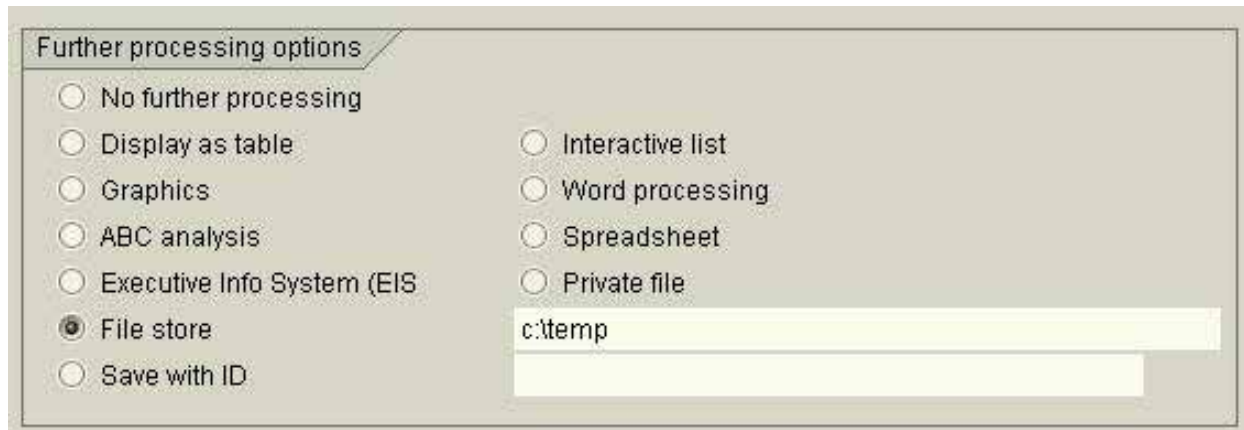


Figure 345: Selecting the FILE STORE for the data transfer

The user has the option to transfer the selected list to a local file on his personal computer. The default file name should be changed to the auditor’s drive, an appropriate folder and a file name of his choice in this case. The default file format DAT should not be changed though. The option for column headers has to be marked as well. The data can now be exported to the personal computer by clicking the button “transfer”.



Figure 346: Exporting a list via the file store

### 7.3 Importing SAP™ AIS data to audit software

#### 7.3.1 Import to ACL audit software

In the final step, the data exported from AIS is imported to the ACL audit software.

Up to ACL version 6.0, the automatic data import of exported data from the SAP™ AIS system was done in a separate program, the ACL service program.

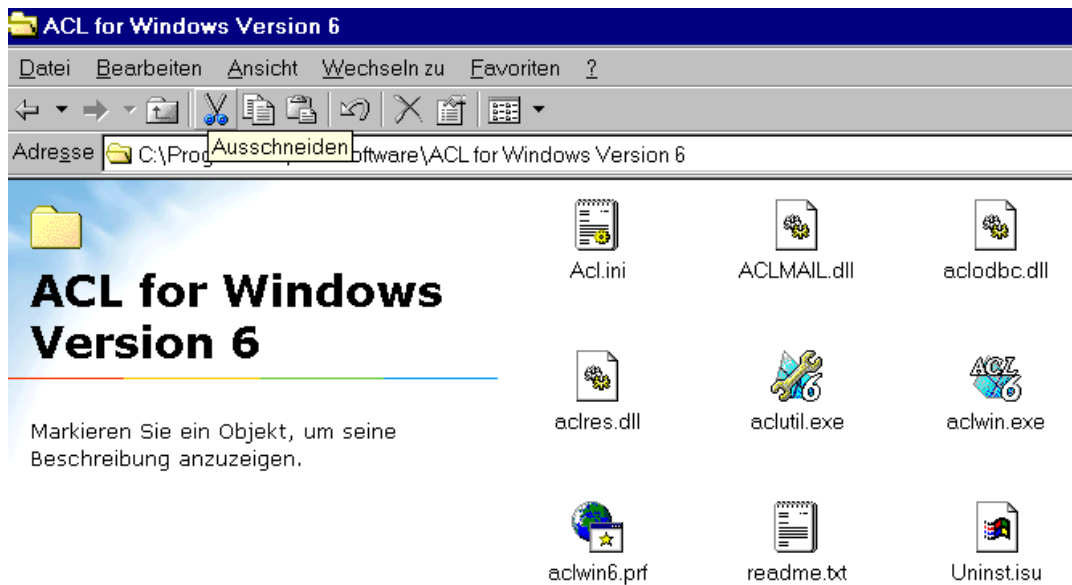


Figure 347: Calling the ACL service program

The menu “SAP – AIS to windows” is utilized for the data conversion.

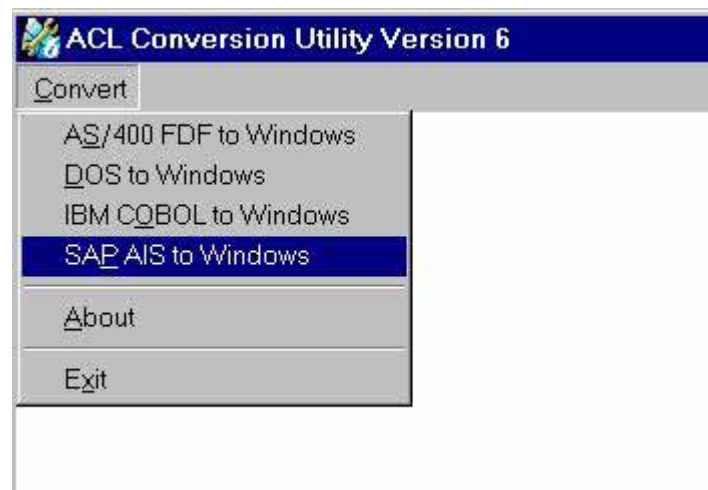


Figure 348: Menu selection for the data conversion

In the next input screen the complete file path of the exported file from the AIS™ system is entered in the field “convert”.

In the field “save as...” the ACL file name is entered, where the document data file is to be saved. Usually the file is named after the relevant client.

The last field “file definition” enables the auditor to give the document file from SAP™ an ACL name, which is valid for further processing.

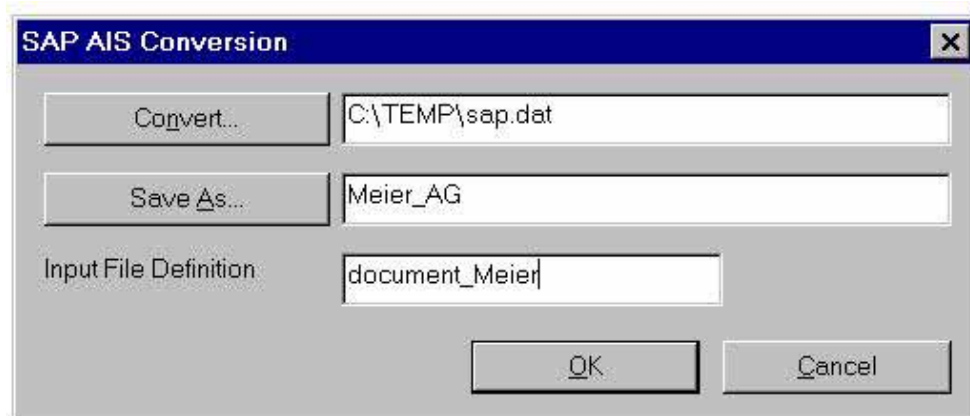


Figure 349: SAP-AIS™ data conversion in ACL up to version 6.0

After confirming the data conversion with the button “OK”, all required information for the audit software is automatically created.

In the ACL version 7.0 and higher, there is an import assistant which can be called in the menu

Data

Selection

New

After selecting the file to be imported, the menu item “private SAP™ file format” is marked by the user.

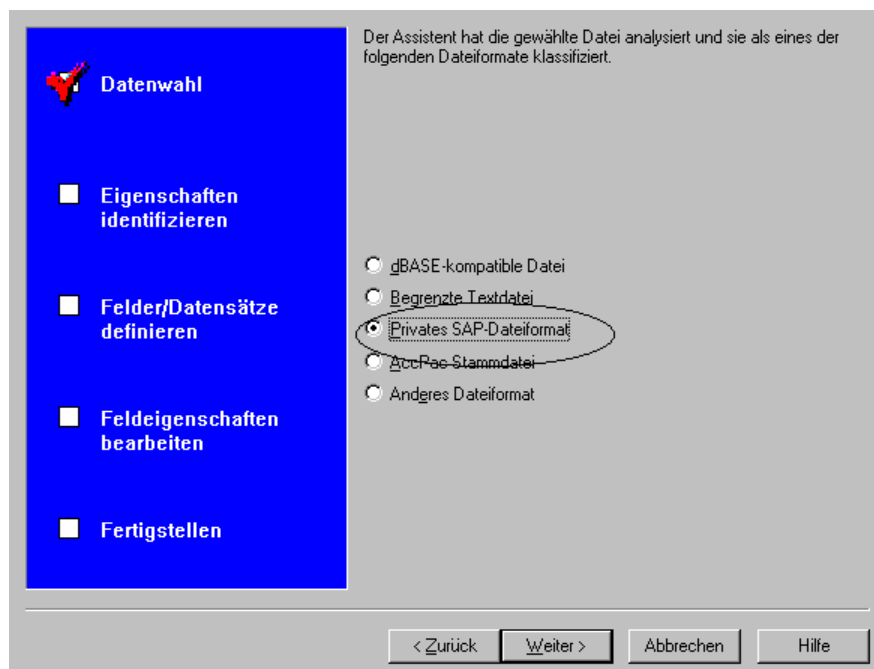


Figure 350: SAP-AIS™ data conversion in ACL in version 7.0 and higher

In the next step the user can define, if the cryptic SAP field names or the descriptive names are to be used in ACL. Up to version 6.0 the auditor has to start the audit software and open the file with the document data file. In version 6.5 and higher, the document file is saved in the open ACL file without this additional step.



ACL for Windows 6 - [View: Default_View [Data File: ap_trans.FIL]]									
File Edit Data Analyze Sampling Tools Window Help									
Document: Workbook.acf 102 Records Input File: ap_trans									
	Vendor Number	Invoice Number	Invoice Date	Invoice Amount	Product Number	Quantity	Unit Cost		
1	11663	5981807	11/17/96	618.30	070104397	90	6.87		
2	13808	2275301	11/17/96	6705.12	070104677	976	6.87		
3	12433	6585673	11/17/96	7955.46	070104657	1158	6.87		
4	11663	5983947	11/17/96	4870.83	070104327	709	6.87		
5	12130	589134	11/17/96	10531.71	070104377	1533	6.87		
6	13411	49545947	10/30/96	5734.00	030414313	122	47.00		
7	12433	6585951	10/30/96	2196.00	030414283	122	18.00		
8	10721	123196	10/30/96	265.19	030412553	23	11.53		
9	12433	6585880	10/30/96	225.00	030412753	18	12.50		
10	13411	49540141	10/30/96	14.88	030412903	6	2.48		
11	10787	591533	05/31/97	1217.16	030321683	828	1.47		
12	10534	58720114	05/31/97	158.60	030322303	130	1.22		
13	14913	8457230	05/31/97	2230.41	030324803	559	3.99		
14	10534	58724783	05/31/97	4324.00	030324883	460	9.40		
15	12433	6588155	06/29/97	1050.00	030030323	210	5.00		
16	11435	54328931	06/29/97	532.86	030934423	107	4.98		
17	12636	69465082	09/29/96	1173.90	030303413	301	3.90		
18	14438	296877	09/29/96	721.00	030303403	175	4.12		
19	10134	71073	09/29/96	883.00	030303343	100	8.83		
20	12130	581119	11/12/97	2583.96	130305603	183	14.12		
21	11837	2214405	11/12/97	7762.04	030309373	767	10.12		
22	12701	232556	11/12/97	2064.48	030302903	204	10.12		
23	10134	74841	11/12/97	18883.34	030302303	458	41.23		
24	10101	4517604	10/30/96	154.00	093788411	110	1.40		
25	10787	594272	10/30/96	522.00	090501541	174	3.00		
26	11663	5986811	10/30/96	1145.58	090501551	626	1.83		
27	11922	987320	10/30/96	983.28	090501051	204	4.82		
28	11475	8753871	10/30/96	368.53	090504061	269	1.37		
29	11663	5983621	10/30/96	31.68	090507841	11	2.88		
30	12701	232162	11/02/96	46.08	090507851	9	5.12		
31	13411	49548491	11/02/96	1357.44	090507811	168	8.08		
32	11475	8753935	11/02/96	2628.42	090504761	426	6.17		
33	14438	290254	10/21/96	50.53	090508191	31	1.63		
34	12433	6586825	10/21/96	3066.88	090509981	599	5.12		
35	12701	237541	10/21/96	2750.64	090509931	471	5.84		
36	11475	8752512	10/21/96	7125.80	090584072	41	173.80		

**Figure 351: Imported file in ACL**

Notes:

[illegible]

### 7.3.2 Import to WinIDEA audit software

An additional function in the menu “file / import assistant” for importing SAP™ AIS data was added to the available import assistant in WinIDEA.

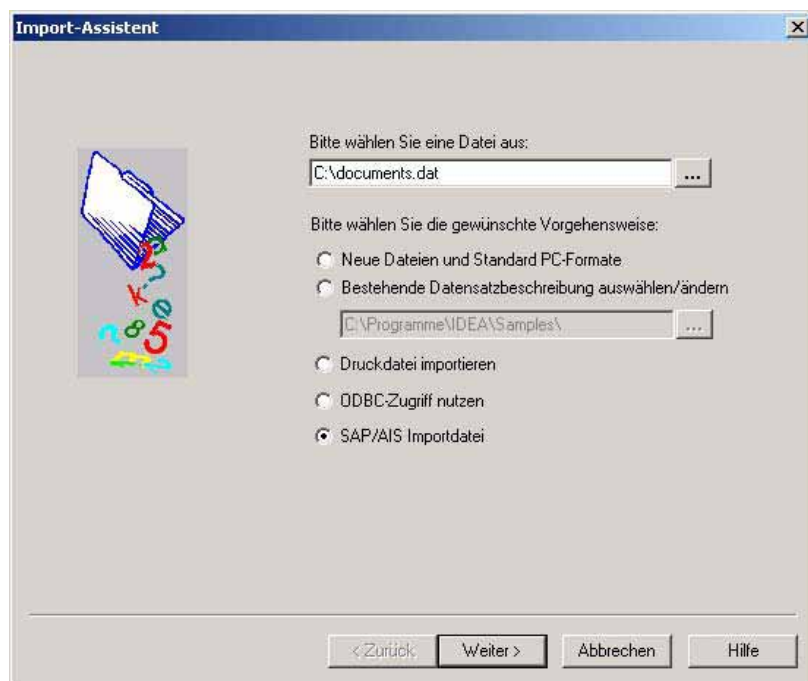


Figure 352: Calling the WinIDEA import assistant

The import assistant analyzes the imported file automatically and enables further editing on field level.

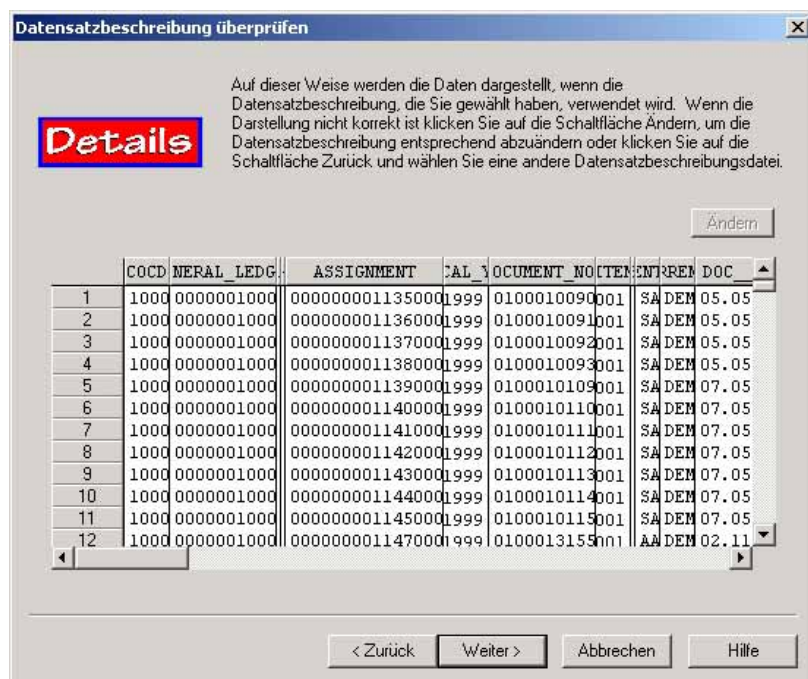


Figure 353: Automatic analysis of the SAP R/™ document file

An input field allows the auditor to save a specified data record description for the imported file.

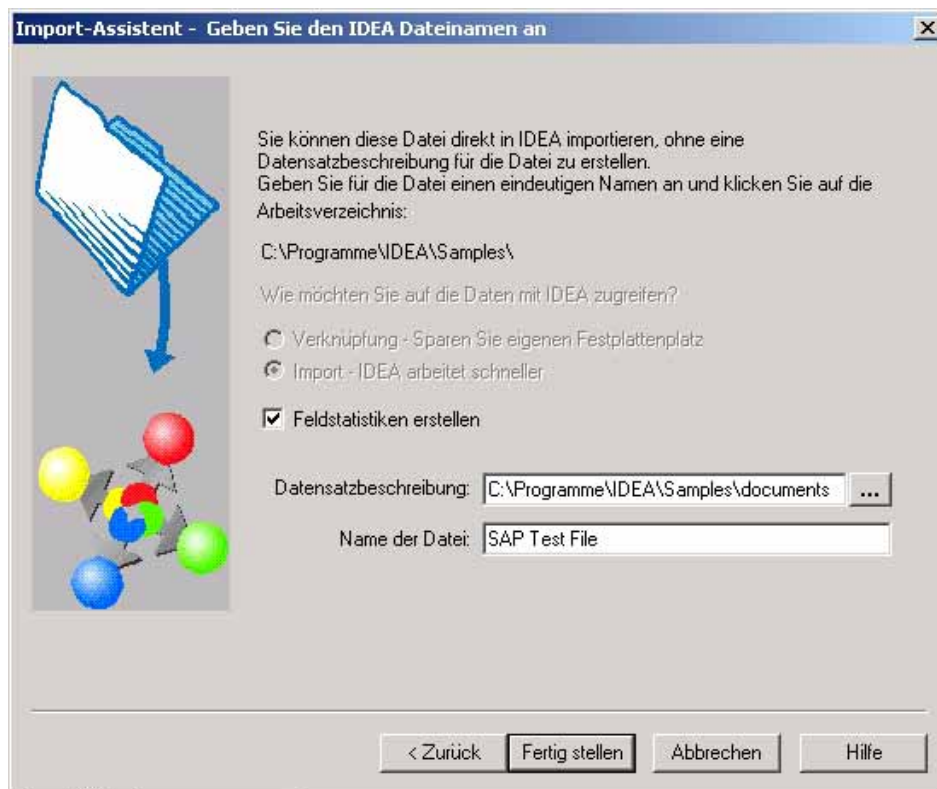


Figure 354: Generating a data record description for WinIDEA

When all entries in the import assistant for importing the file have been confirmed, the document file will be displayed for further processing in WinIDEA.

	COCD	GENERAL_LEDGER	CLEARING	ASSIGNMENT	FISCAL_YEAR	DOCUMENT_NO.	ITEM	S	DOCUMENT_TYPE	CURRENCY	DOC_DATE
1	1000	0000001000	0000/00/00	0000000001134000	1999	0100010094	1	SA	DEM		1999/05/05
2	1000	0000001000	0000/00/00	0000000001135000	1999	0100010090	1	SA	DEM		1999/05/05
3	1000	0000001000	0000/00/00	0000000001136000	1999	0100010091	1	SA	DEM		1999/05/05
4	1000	0000001000	0000/00/00	0000000001137000	1999	0100010092	1	SA	DEM		1999/05/05
5	1000	0000001000	0000/00/00	0000000001138000	1999	0100010093	1	SA	DEM		1999/05/05
6	1000	0000001000	0000/00/00	0000000001139000	1999	0100010109	1	SA	DEM		1999/05/07
7	1000	0000001000	0000/00/00	0000000001140000	1999	0100010110	1	SA	DEM		1999/05/07
8	1000	0000001000	0000/00/00	0000000001141000	1999	0100010111	1	SA	DEM		1999/05/07
9	1000	0000001000	0000/00/00	0000000001142000	1999	0100010112	1	SA	DEM		1999/05/07
10	1000	0000001000	0000/00/00	0000000001143000	1999	0100010113	1	SA	DEM		1999/05/07
11	1000	0000001000	0000/00/00	0000000001144000	1999	0100010114	1	SA	DEM		1999/05/07
12	1000	0000001000	0000/00/00	0000000001145000	1999	0100010115	1	SA	DEM		1999/05/07
13	1000	0000001000	0000/00/00	0000000001147000	1999	0100013155	1	AA	DEM		1999/11/02
14	1000	0000001000	0000/00/00	0000000001147000	1999	1900004854	2	KR	DEM		1999/11/02
15	1000	0000032000	0000/00/00	0000000004143000	1999	0100010102	2	SA	DEM		1999/05/06
16	1000	0000032000	0000/00/00	0000000004143000	1999	0100010109	2	SA	DEM		1999/05/07
17	1000	0000032000	0000/00/00	0000000004144000	1999	0100010103	2	SA	DEM		1999/05/06
18	1000	0000032000	0000/00/00	0000000004144000	1999	0100010110	2	SA	DEM		1999/05/07
19	1000	0000032000	0000/00/00	0000000004145000	1999	0100010104	2	SA	DEM		1999/05/06
20	1000	0000032000	0000/00/00	0000000004145000	1999	0100010111	2	SA	DEM		1999/05/07
21	1000	0000032000	0000/00/00	0000000004146000	1999	0100010105	2	SA	DEM		1999/05/06
22	1000	0000032000	0000/00/00	0000000004146000	1999	0100010112	2	SA	DEM		1999/05/07
23	1000	0000032000	0000/00/00	0000000004147000	1999	0100010106	2	SA	DEM		1999/05/06
24	1000	0000032000	0000/00/00	0000000004147000	1999	0100010113	2	SA	DEM		1999/05/07
25	1000	0000032000	0000/00/00	0000000004148000	1999	0100010107	2	SA	DEM		1999/05/06
26	1000	0000032000	0000/00/00	0000000004148000	1999	0100010114	2	SA	DEM		1999/05/07
27	1000	0000032000	0000/00/00	0000000004149000	1999	0100010108	2	SA	DEM		1999/05/06
28	1000	0000032000	0000/00/00	0000000004149000	1999	0100010115	2	SA	DEM		1999/05/07
29	1000	0000032000	0000/00/00	0000000004150000	1999	0100010085	2	SA	DEM		1999/05/05
30	1000	0000032000	0000/00/00	0000000004150000	1999	0100010090	2	SA	DEM		1999/05/05
31	1000	0000032000	0000/00/00	0000000004151000	1999	0100010086	2	SA	DEM		1999/05/05
32	1000	0000032000	0000/00/00	0000000004151000	1999	0100010091	2	SA	DEM		1999/05/05
33	1000	0000032000	0000/00/00	0000000004152000	1999	0100010087	2	SA	DEM		1999/05/05
34	1000	0000032000	0000/00/00	0000000004152000	1999	0100010092	2	SA	DEM		1999/05/05

Figure 355: Display of the WinIDEA file

## 7.4 Importing SAP™ data to audit software via file store

### 7.4.1 Introduction

If a private file and a related USER-EXIT has been created (see 1.13) in the SAP™ system, and the generated data was transferred via the private file, the data can be imported by utilizing the SAP™ – AIS option in the import assistant, as described in the previous section.

Only if the private file in the SAP™ system was not configured properly and the menu item file store was selected for transferring SAP™ data, the following procedure has to be used for importing data to the audit software.

### 7.4.2 Import to ACL audit software

After calling the import assistant and selecting the file to be imported, the file format “delimited text file” is selected in the menu

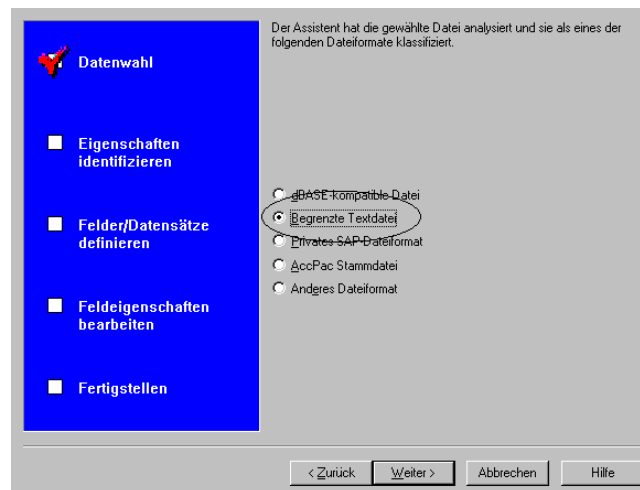


Figure 356: Selecting the file format in ACL

Field separators in the next menu is the tabulator “TAB”. The first line in the file contains the field names.

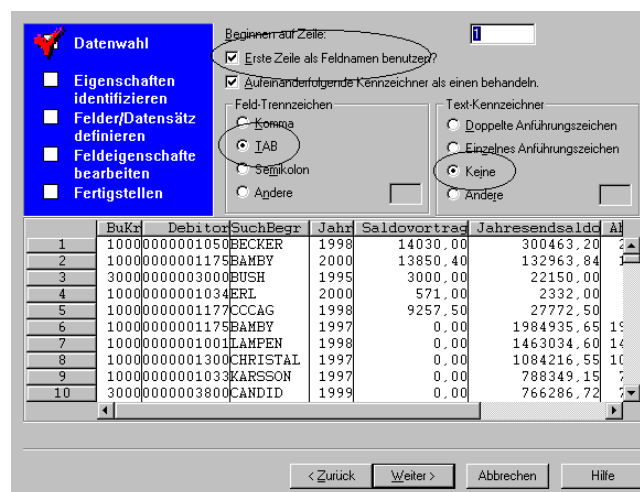


Figure 357: Entering import parameters in ACL



- 328 -

The field types of the specific data fields should be checked and edited, in cases where date formats or positions after decimal points are not recognized.

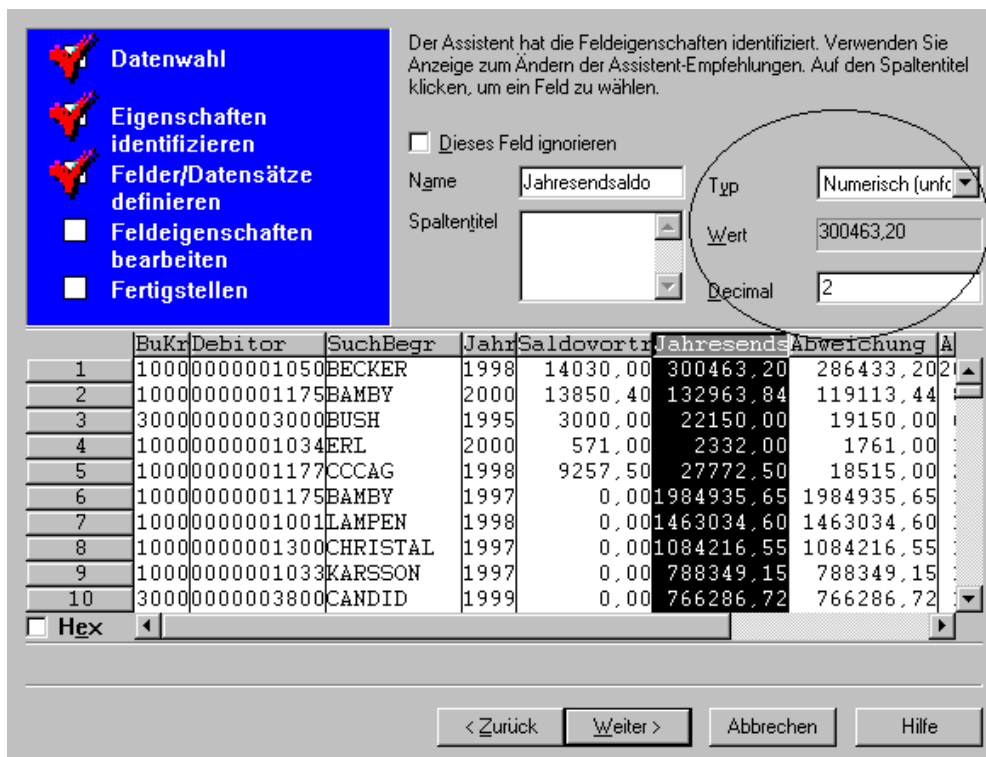


Figure 358: Checking the filed formats in ACL

The data is now ready for further processing in ACL.

Document: Workbook.acl    64 Records    Inp

View: Default\_View [Data File: CUSTOMER.FIL]

	Cust No	Name	Street Address	City	State	Zip Code	Credit Limit
1	35189	VERSA TIRES	51001 BORNEO RD	PITTSBURGH	TX	75686	32000
2	444413	EQUITABLE CORPORATION	6300 METZEROTT RD	LOUISVILLE	CO	80027	22000
3	463451	BLUE ATLANTA	301 E 2ND ST	ST LOUIS	MO	63131	53000
4	269267	UNIVERSITY NATIONAL	9600 MARKET ST	SCARSDALE	NY	10583	22000
5	359310	SECOND BONNET COMMERCIAL	20500 AMERICAN RD	RICHMOND	VA	23219	60000
6	519311	QUORUM JOY	650 BROADWAY	LA JOLLA	CA	92037	59000
7	564291	MICHIGAN OILFIELD INC.	8335 GRANDVIEW AVE	WILLOUGHBY	OH	44094	8000
8	815062	BANCO INC.	4441 N 12TH ST	BRONX	NY	10467	66000
9	277097	OFFICE COMPUTER LTD.	101 LOCUST AVE	LOWELL	MA	01851	60000
10	820025	UNITED CITY	920 4TH STREET	BRIDGEWATER	NJ	08807	46000
11	231494	EMPLOYMENT MEDIA LTD.	57 W 66TH ST	ELK GROVE VILLA	IL	60007	63000
12	795401	METROPOLITAN PHARMACEUTIC	693 DELAWARE AVE	CORNING	NY	14830	51000
13	081559	KIDDER ENTERPRISES	2900 HOLDREGE ST	STAMFORD	CT	06902	49000
14	878035	BLUE SERVICES GROUP	7600 WAKE FOREST RD	MALVERN	PA	19355	79000
15	258024	FARMERS LOTTERY	1260 LIEWIT PLAZA	LAWRENCE	KS	66045	81000
16	620304	BELAMINA NATIONAL INC.	9451 WALNUT ST	BURLINGTON	NC	27215	94000
17	284354	ASIA/AMERICA COOP	4310 WEST DESERT RD	CARSON CITY	NV	89701	92000
18	504356	UNION NATIONAL	51557 TELEGRAPH RD	HAZELWOOD	MO	63042	45000
19	065003	UNIVERSITY ELECTRONICS	7000 S WABASH AVE	BURLINGTON	NC	27215	10000
20	287397	ACCEL ENTERPRISES	1000 STRAYER DR	BROOKLYN	MA	02167	72000

Figure 359: ACL file after file import

### 7.4.3 Import to WinIDEA audit software

For importing data to WinIDEA the import assistant is called in the menu file / import assistant. In the next screen the item "new files and standard PC formats" is marked and then "ACII delimited file".

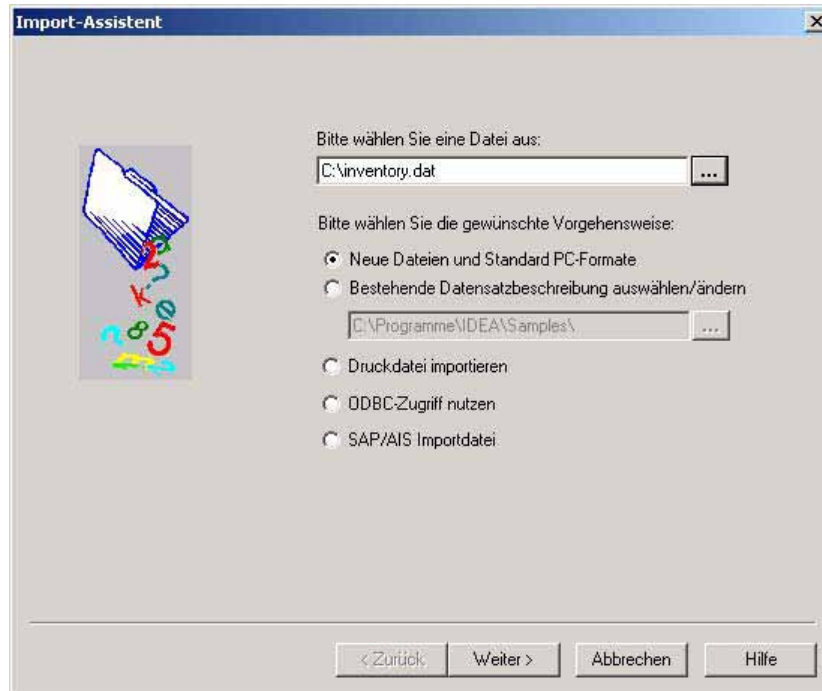


Figure 360: Selecting the WinIDEA file format

The tabulator "TAB" is defined as filed separator. The option to get the headers from the first file line is activated.

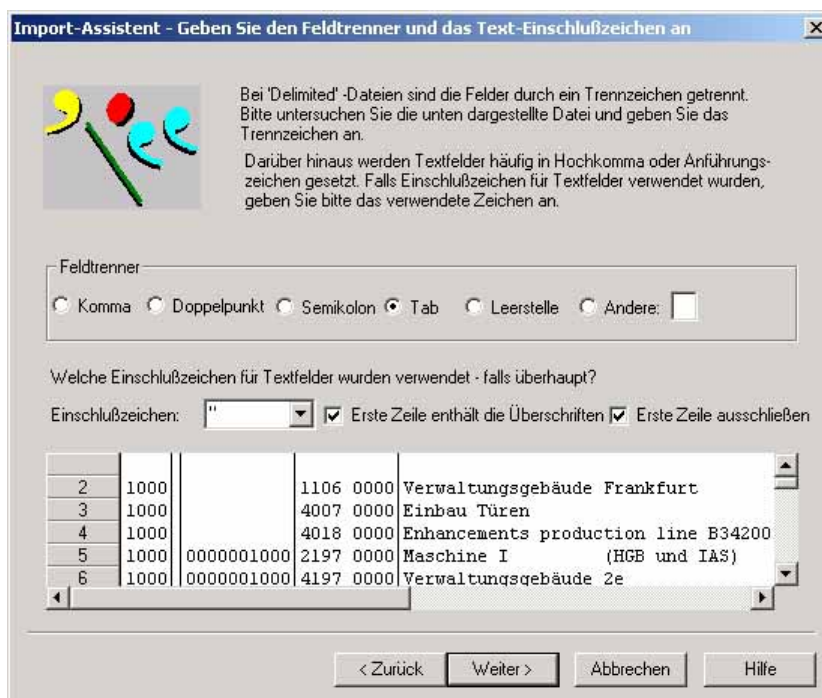


Figure 361: Entering import parameters in WinIDEA



- 330 -

The specific fields and their formats, such as positions after the decimal and date formats, should be checked.

**Import-Assistent - Felddetails**

Sie können das Feld genauer spezifizieren. Klicken Sie auf die Spaltenüberschrift zur Auswahl eines Feldes und ändern Sie die Felddetails.

**Details**

Feldname:  Typ:

Beschreibung:

☐ Bitte markieren falls die Dezimalstellen eingeschlossen sind.

☐ Dieses Feld nicht importieren

Anzahl der Dezimalkommastellen:

Konvertiertes Beispiel:

	ASSET_DESCRIPTION	ACQUISITION_VALUE	JANTIT	YEAR
1	Verwaltungsgebäude Frankfurt	19500000,00	0,000	1993
2	Einbau Türen	6000,00	0,000	1995
3	Enhancements production line B342	21739,13	0,000	1996
4	Maschine I (HGB und IAS)	1000,00	0,000	2001
5	Verwaltungsgebäude 2e	30689,65	0,000	2002

< Zurück Weiter > Abbrechen Hilfe

Figure 362: Checking the field formats in WinIDEA

Once the preparation in the import assistant are finished, the SAP<sup>TM</sup> data can be analyzed in WinIDEA.

	COCODE	PLANT	COST_CENTER	INVENTORY_NUMBER	ASSET_DESCRIPTION	ACQUISITION_VALUE	QUANTITY	YEAR
1	1000			1106 0000	Verwaltungsgebäude Frankfurt	1.950.000.000,00	0	1993
2	1000			4007 0000	Einbau Türen	600.000,00	0	1995
3	1000			4018 0000	Enhancements production line B34200	2.173.913,00	0	1996
4	1000		0000001000	2197 0000	Maschine I (HGB und IAS)	100.000,00	0	2001
5	1000		0000001000	4197 0000	Verwaltungsgebäude 2e	3.068.965,00	0	2002
6	1000		0000001000	4198 0000	Verwaltungsgebäude	2.000.000,00	0	2002
7	1000		0000004100	2205 0000	Fräsmaschine	8.565.217,00	0	2001
8	1000		0000020210	4711-0815	BMW 320d	0,00	0	2002
9	1000	1000	0000001200	2015 0000	Geschirrabrühranlage	2.468.933,00	0	1995
10	1000	1000	0000001200	2016 0000	Geschirrspülanlage	3.368.501,00	0	1995
11	1000	1000	0000001200	2047 0000	Geschirrspülautomat	2.099.800,00	0	1995
12	1000	1000	0000001230	2105 0000	Transformator GNT 56	24.956.522,00	0	1994
13	1000	1000	0000003100	3224 0000	Faxgerät UTAX LF30	150.000,00	0	1997
14	1000	1000	0000003100	3232 0000	TCI CPD-1791	650.000,00	0	1997
15	1000	1000	0000003100	3235 0000	TCI 80486DX-66	996.000,00	0	1997
16	1000	1000	0000003100	3236 0000	Compaq Personal Computer	370.000,00	0	1997
17	1000	1000	0000003110	3005 0000	Möbeleinrichtungen	2.824.000,00	0	1995
18	1000	1000	0000003110	3006 0000	Schreibtisch Schmidt & Schmidt	250.000,00	0	1995
19	1000	1000	0000003110	3007 0000	Kopierer KODAK EKTA COPY 2000	1.998.500,00	0	1995
20	1000	1000	0000003110	3008 0000	Faxgerät SHARP 99 FTX	674.500,00	0	1995
21	1000	1000	0000003110	3015 0000	Büroeinrichtung Vertriebsbüro	3.500.000,00	0	1995
22	1000	1000	0000003110	3016 0000	Büroeinrichtung Vertrieb	2.500.000,00	0	1995
23	1000	1000	0000003110	3214 0000	TCI 80486DX-66	996.000,00	0	1995
24	1000	1000	0000003110	3237 0000	Compaq Laptop	298.000,00	0	1997
25	1000	1000	0000004110	2103 0000	Bodenreinigungsmaschine Dreher 234/73	1.321.739,00	0	1994
26	1000	1000	0000004110	2104 0000	Fehlerdiagnosegerät Bosch 759	539.130,00	0	1994
27	1000	1000	0000004130	2018 0000	Gabelstapler	19.750.000,00	0	1995
28	1000	1000	0000004130	2019 0000	Gabelstapler (AV)	3.054.600,00	0	1995
29	1000	1000	0000004200	2133 0000	Fraesmaschine Maho 2313	24.782.609,00	0	1997
30	1000	1000	0000004200	2136 0000	CNC Drehmaschine Gildemeister HN	28.700.000,00	0	1997
31	1000	1000	0000004200	2137 0000	Mischanlage x.25	3.700.000,00	0	1997
32	1000	1000	0000004200	2145 0000	Bohrmaschine WEBO 56-HT	2.234.000,00	0	1997
33	1000	1000	0000004200	2146 0000	Elektro-Pumpe 636/78 Vereinte Mechanische Werke AG	3.600.000,00	0	1997
34	1000	1000	0000004200	2148 0000	Elektro Pumpe 636 / 79	3.540.000,00	0	1997
35	1000	1000	0000004200	2150 0000	Elektro-Pumpe 636/82	2.400.000,00	0	1997

Figure 363: Display of the imported WinIDEA file

## 7.5 Overview of transferred document fields

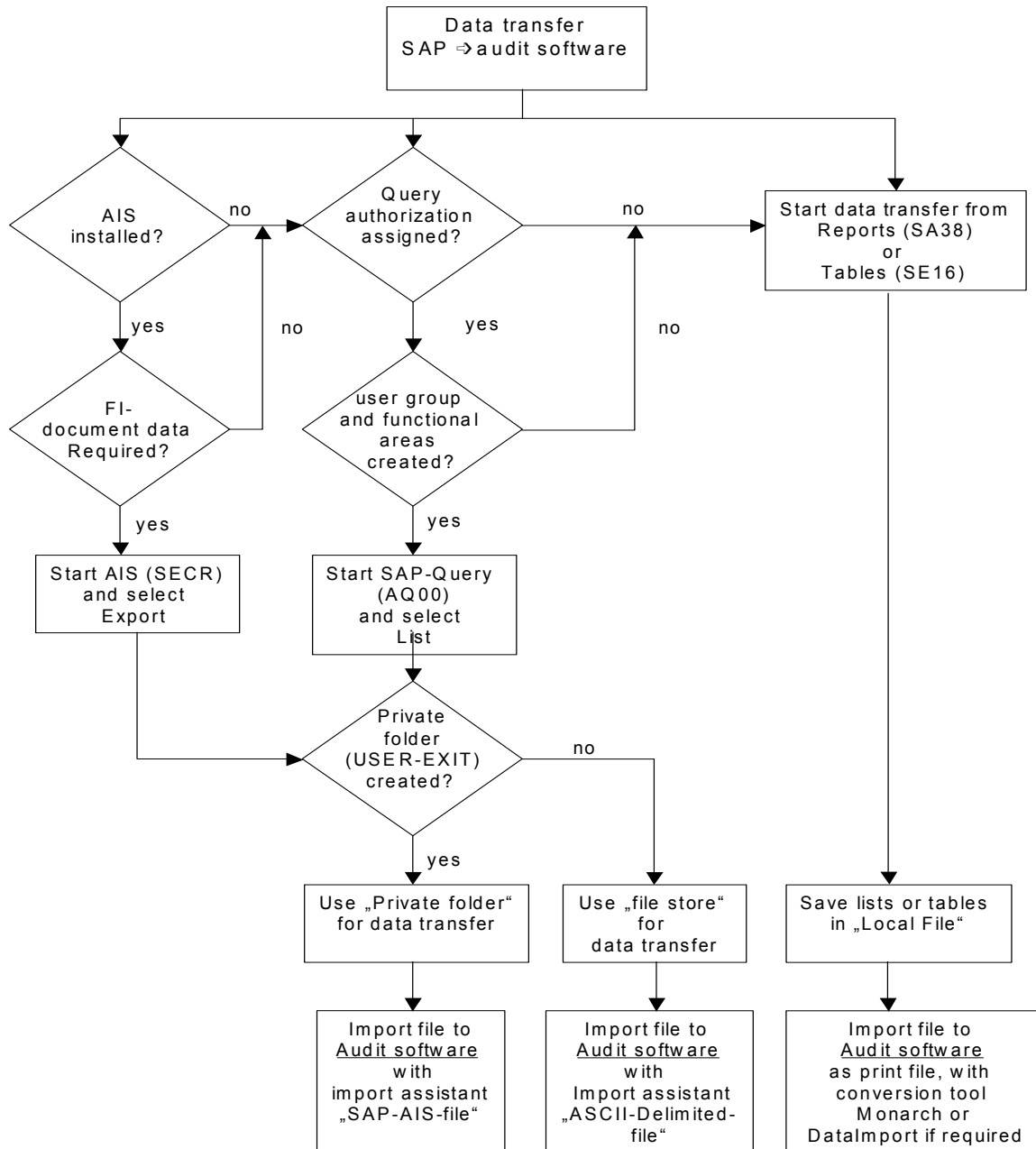
The overview below of transferred document data is meant to support audit activities in the audit software. It should be noted, that not all transferred fields contain useful information, depending on the selected document type.

<i>BKPF-BUKRS</i>	<i>Company code</i>
<i>BKPF-BELNR</i>	<i>Accounting document number</i>
<i>BKPF-GJAHR</i>	<i>Fiscal year</i>
<i>BKPF-CPUDT</i>	<i>Accounting document entry date</i>
<i>BKPF-AEDAT</i>	<i>Date of the last document change by transaction</i>
<i>BKPF-UPDDT</i>	<i>Date of the last document update</i>
<i>BKPF-TCODE</i>	<i>Transaction code</i>
<i>BKPF-USNAM</i>	<i>User name</i>
<i>BKPF-BSTAT</i>	<i>Document status</i>
<i>BKPF-STBLG</i>	<i>Reverse document number</i>
<i>BKPF-STJAH</i>	<i>Reverse document fiscal year</i>
<i>BKPF-BLART</i>	<i>Document type</i>
<i>BKPF-WAERS</i>	<i>Currency key</i>
<i>BKPF-BLDAT</i>	<i>Document date in document</i>
<i>BKPF-BUDAT</i>	<i>Posting date in the document</i>
<i>BKPF-MONAT</i>	<i>Fiscal period</i>
<i>BKPF-XBLNR</i>	<i>Reference document number</i>
<i>BKPF-BKTX</i>	<i>Document header text</i>
<i>BSEG-BUZEI</i>	<i>Line item number within the accounting document</i>
<i>BSEG-BSCHL</i>	<i>Posting keys</i>
<i>BSEG-KOART</i>	<i>Account type</i>
<i>BSEG-SAKNR</i>	<i>G/L account number</i>
<i>BSEG-HKONT</i>	<i>General ledger account</i>
<i>BSEG-KUNNR</i>	<i>Customer number</i>
<i>BSEG-LIFNR</i>	<i>Account number of supplier/vendor</i>
<i>BSEG-XCPDD</i>	<i>Indicator: Address and bank data set individually</i>
<i>BSEG-XAUTO</i>	<i>Indicator: Line item automatically created</i>
<i>BSEG-UMSKZ</i>	<i>Special G/L indicator</i>
<i>BSEG-UMSKS</i>	<i>Special G/L transaction type</i>
<i>BSEG-ZUMSK</i>	<i>Target special G/L indicator</i>
<i>BSEG-SHKZG</i>	<i>Debit/credit indicator</i>
<i>BSEGDMSHB</i>	<i>BSEG amount in LC with +/- sign</i>
<i>T001_WAERS</i>	<i>Currency key</i>
<i>BSEGWRSHB</i>	<i>BSEG amount in FC with +/- sign</i>
<i>BKPF_WAERS2</i>	<i>Currency key</i>
<i>BSEG-MWSKZ</i>	<i>Tax on sales/purchases code</i>
<i>BSEGMDSHB</i>	<i>BSEG tax on sales/purchases amount in LC with +/- sign</i>
<i>T001_WAERS2</i>	<i>Currency key</i>
<i>BSEGMWSHB</i>	<i>BSEG tax on sales/purchases amount in FC with +/- sign</i>
<i>BKPF_WAERS3</i>	<i>Currency key</i>
<i>BSEG-ZTERM</i>	<i>Terms of payment key</i>
<i>BSEG-ZFBDT</i>	<i>Baseline date for due date calculation</i>
<i>BSEG-ZBD1T</i>	<i>Days for first cash discount</i>

<i>BSEG-ZBD1P</i>	<i>Percentage for first cash discount</i>
<i>BSEG-ZBD2T</i>	<i>Days for second cash discount</i>
<i>BSEG-ZBD2P</i>	<i>Percentage for second cash discount</i>
<i>BSEG-ZBD3T</i>	<i>Net payment terms period</i>
<i>BSEGNETDT</i>	<i>BSEG Due date for net payment</i>
<i>BSEG_SKFBT</i>	<i>BSEG Amount eligible for cash discount</i>
<i>BKPF_WAERS4</i>	<i>Currency key</i>
<i>BSEG_SKNT0</i>	<i>BSEG Cash disc.amt in LC (+/-)</i>
<i>T001_WAERS3</i>	<i>Currency key</i>
<i>BSEG_WSKTO</i>	<i>BSEG Cash discount amount in document currency (+/+)</i>
<i>BSEG-AUGBL</i>	<i>Document number of the clearing document</i>
<i>BSEG-AUGDT</i>	<i>Clearing date</i>
<i>BSEG-GSBER</i>	<i>Business area</i>
<i>BSEG-KOSTL</i>	<i>Cost center</i>
<i>BSEG-AUFNR</i>	<i>Order number</i>
<i>BSEG-KSTRG</i>	<i>Cost object</i>
<i>BSEG-MENGE</i>	<i>Quantity</i>
<i>BSEG-MEINS</i>	<i>Base unit of measure</i>
<i>BSEG-WERKS</i>	<i>Plant</i>
<i>BSEG-VALUT</i>	<i>Value date</i>
<i>BSEG-ZUONR</i>	<i>Assignment number</i>
<i>BSEG-SGTXT</i>	<i>Item text</i>
<i>BSEG-MSCHL</i>	<i>Dunning key</i>
<i>BSEG-MABER</i>	<i>Dunning area</i>
<i>BSEG-MADAT</i>	<i>Date of last dunning notice</i>
<i>BSEG-MANST</i>	<i>Dunning level</i>
<i>BSEG-MANSP</i>	<i>Dunning block</i>
<i>BSEG-XZAH1</i>	<i>Indicator: Is this for a payment transaction?</i>
<i>BSEG-ZLSCH</i>	<i>Payment method</i>
<i>BSEG-ZLSPR</i>	<i>Payment block key</i>
<i>BSEG-ZBFIX</i>	<i>Fixed payment terms</i>
<i>BSEG-HBKID</i>	<i>House bank ID</i>

## 7.6 Summary

The presented options are displayed below:



Once the Audit Information System has been set up and customized, the direct data transfer to common audit software, such as ACL or WinIDEa is possible without further effort. The same applies if AIS™ is not available, but SAP™ Query is utilized. The financial statement auditor is able to analyze selected document data in various and complex ways, which is not possible in the SAP™ system itself. Typical areas for utilization include mathematical-statistical sampling methods, structural analyses of the auditor's choice, comparisons with data from external sources, determination of duplicate payments and forensic investigations.

## **VI Final remark**

The AIS system in the current release version proves to be a powerful tool for system administrators, for staff in the financial accounting department, internal auditors and financial statement auditors. These user categories should take an active part in the set up and the utilization of the tool in order to benefit from it during their daily work.

The tool is continuously being developed, and the involvement in the specific SAP<sup>TM</sup> audit forums, which are pleased to receive suggestions for further improvements, can be recommended.

Enclosure 1

Tables for the user administration

Table name	Short text
USGRP	User Groups
USGRP_USER	Assignment of Users to User Groups
USGRPT	Text table for USGRP (User groups)
USH02	Change history for logon data
USH04	Change history for authorizations
USH10	Change history for authorization profiles
USH12	Change history for authorization values
USKRI	Critical combination of authorizations
USKRIA	Entry of Critical Auths for Report RSUSR009
USKRIAT	Text table for USKRIA
USOBT	Relation transaction > authorization Object
USOBT_C	Relation Transaction > Auth. Object
USOBT_CD	Change History for Field Values
USOBT_DUP	Modification log for table USOBT. For SAP
USOBX	Check table for table USOBT
USOBX_C	Check Table for Table USOBT_C
USOBX_CD	Change History for Check Indicator
USOBX_DUP	Modification log for table USOBX. Only for SAP
USOBX_MOD	Check table for table USOBT
USOGR	Object groups for TCode < > Auth. Object
USOGT	Texts for object groups
USORG	Org. levels for profile generator
USOTT	Relation transaction > authorization Object
USPPT	Common User Table for Sequencing and Planning
USR_FLAGS	Various Flags for Authorization Programs
USR_FLGNT	Personal User Settings / Without Transport
USR01	User master record (runtime data)
USR02	Logon data
USR03	User address data
USR04	User master authorizations
USR05	User Master Parameter ID
USR06	Additional data per user
USR07	Object/values of last authorization
USR08	Table for user menu entries
USR09	Entries for user menus (work areas)
USR10	User master authorization profiles
USR11	User Master Texts for Profiles (USR10)
USR12	User master authorization values
USR13	Short Texts for Authorizations
USR14	Surchargeable language versions per user
USR15	External User Name
USR16	Values for Variables for User Authorizations
USR20	Date of last user master reorganization
USR22	Logon data without kernel access
USR30	Additional Information for User Menu
USR40	Table for illegal passwords
UST04	User masters



Enclosure 2

Controlling tables for the financial accounting

Table name	Short text
T001	Company Codes
T001B	Permitted Posting Periods
T001D	Validation of Accounting Documents
T001E	Company Code-Dependent Address Data
T001F	Company code-dependent form selection
T001G	Company Code-Dependent Standard Text
T001I	Company Code - Parameter Types
T001J	Company Code - Parameter Type Names
T001K	Valuation area
T001N	Company Code - EC Tax Numbers / Notification to auth.
T001O	Cross-System Company Codes
T001P	Personnel Area/Subarea
T001Q	Substitution in Accounting Documents
T001R	Rounding Rules for Company Code and Currency
T001S	Accounting Clerks
T001T	Company code-dependent texts
T001U	Clearing Between Company Codes
T001X	Configuration of External Receiving Company Codes
T001Z	Additional Specifications for Company Codes
T003	Document Types
T003A	Document Types for Posting with Clearance
T003B	Object Types for Early Entry in Financial Accounting
T003O	Order Types
T003P	Order Type Descriptions
T003R	Number Ranges RE_BELEG (Logistics Invoice check)
T003T	Document Type Texts
T004	Directory of Charts of Accounts
T004F	Field status definition groups
T004G	Field Status Definition Group Texts
T004M	Rules for Sample Accounts
T004R	Rules index for sample accounts
T004S	Texts for sample account rules
T004T	Chart of Account Names
T004V	Field Status Variant
T004W	Text Table for T004V
T007A	Tax Keys
T007B	Tax Processing in Accounting
T007C	Groupings for tax codes
T007F	Taxes on Sales/Purchases Groups
T007S	Tax Code Names
T007V	Tax Codes to be Transported
T008	Blocking Reasons for Automatic Payment
T008T	Blocking Reason Names in Automatic Payments
T030	Standard Accounts Table
T030A	Transaction Keys and Assignment to Groups
T030B	Standard Posting Keys
T030C	Global Standard Account Table

**Enclosure 3**

**Important tables for the financial accounting**

<b>Table name</b>	<b>Short text</b>
T001B	Permitted Posting Periods
T004	Directory of Charts of Accounts
T004F	Field status definition groups
T004G	Field Status Definition Group Texts
T004M	Rules for Sample Accounts
T004R	Rules index for sample accounts
T004S	Texts for sample account rules
T004T	Chart of Account Names
T004V	Field Status Variant
T004W	Text Table for T004V
T009	Fiscal year variants
T009B	Fiscal year variant periods
T009T	Fiscal year variant names
T011	Financial Statement Versions
T011T	Financial statement version names
T044A	Foreign Currency Valuation Methods
T044B	Valuation method names
T044Z	Customer/Vendor Accounts with Changed Reconciliation Accounts
T852P	Consolidation periods
T854	Financial statement items for consolidation
T854S	Selected FS items
T858	Consolidation versions
T864	Reclassifications
T865	Intercompany Elimination
T866	Elimination of IC profit/loss: FS items
T869	Consolidation methods
T876	Consolidation document types
T884	Currency translation
T884C	Control Balance Carried Forward

**Enclosure 4**

**Reports on user administration and authorization checks**

<b>Name</b>	<b>Title</b>
RSUSR001	Infosystem authorizations
RSUSR002	Lists of users according to complex selection criteria
RSUSR002_ADDRESS	User according to address data
RSUSR003	Check the Passwords of Users SAP* and DDIC in All Clients
RSUSR004	Restrict User Values to the Following Simple Profiles and Auth. Objs.
RSUSR005	List of Users With Critical Authorizations
RSUSR006	List of User Master Records Locked Due to Incorrect Logon
RSUSR007	List Users Whose Address Data is Incomplete
RSUSR008	Critical Combinations of Authorizations at Transaction Start
RSUSR009	List of Users With Critical Authorizations
RSUSR010	Transaction Lists According to Selection With User, Profile or Object
RSUSR012	Search authorizations, profiles and users with specified object values
RSUSR020	List Profiles by Complex Selection Criteria
RSUSR030	List Authorizations According to Complex Selection Criteria
RSUSR040	List Authorization Objects by Complex Selection Criteria
RSUSR050	Comparisons
RSUSR060	Where-used lists
RSUSR061	Enter Authorization Fields
RSUSR070	List of Activity Groups According to Complex Selection Criteria
RSUSR100	For user
RSUSR101	For profiles
RSUSR102	For authorizations
RSUSR200	List of Users According to Logon Date and Password Change
RSUSR300	Set external security names to all users
RSUSR998	Call Reporting Tree Info System

**Enclosure 5/Site 1**

**Company and staff**

- ☐ **Roger Odenthal services**
- ☐ **Papers, publications and manuals (in German)**
- ☐ **Contact persons**

**Enclosure 5/Site 2**

**Our services**

In addition to our IT supported audit services, our company is consulting clients on business issues and conduct IT system audits. We will be pleased to send you more information about our services, which are described in the following brochures. Upon request you will obtain the English version.

- ☐ IT system audit services
- ☐ Our services in your SAP R/3™ environment
- ☐ Audit support during the SAP R/3™ implementation
- ☐ Software application certification
- ☐ Methods and techniques for IT risk assessment
- ☐ Migrating data to new IT systems
- ☐ Efficient and compliant data archiving
- ☐ Preparation and support for outsourcing projects
- ☐ IT agreements and relevant audit aspects

### Papers, publications and manuals (in German)

We will be pleased to provide the following papers, publications and manuals, written by our staff.

- ☐ **Organisatorische Aspekte des Datenzugriffs der Finanzverwaltung auf Unternehmensdaten**  
**Zeitschrift Finanz Wirtschaft, Ausgabe 10, Oktober 2002**
- ☐ **Revision und Zahlenanalyse,**  
WIK, Zeitschrift für Sicherheit der Wirtschaft, Ausgabe 3, Juni 2001
- ☐ **EDV-Beweissicherung** bei Computerkriminalität,  
KES, Zeitschrift für Kommunikations- und EDV-Sicherheit, NR. 3, Juli 2001
- ☐ Mit **Digitaler Ziffernanalyse** gegen **Unterschlagungen**: Ein Beitrag zu IT-gestützten Möglichkeiten zur Enttarnung von Mitarbeitern,  
WIK, Zeitschrift für die Sicherheit der Wirtschaft, Nr. 3, Juni 2001
- ☐ **Beweissicherung** bei Computerkriminalität,  
**KES, Zeitschrift für Kommunikations- und EDV-Sicherheit, Ausgabe 3, Juli 2001**
- ☐ **EDV-Revision im Bereich des Rechnungswesens** bei Einsatz von EDI und EDIFACT,  
Die Wirtschaftsprüfung, Nr. 15, 1995
- ☐ **KonTraG und (EDV-)Verfahrensprüfung**, ZIR,  
Zeitschrift Interne Revision, Ausgabe 6/2000
- ☐ Vorgehensmodell zur **Prüfung des Berechtigungswesens** in einer SAP R/3™ Umgebung,  
ZIR, Zeitschrift Interne Revision, Juni 2000, Ausgabe 3/2000
- ☐ Verfahren und Instrumente zur **Aufdeckung wirtschaftskrimineller Handlungen**, Teil 1 – 2,  
RWZ, Zeitschrift für Recht und Rechnungswesen, 10/1999
- ☐ Notfallstrategie für den Umgang mit **Mitarbeiterkriminalität**,  
Audit Journal, Heft 4, Dezember 1999
- ☐ **Digitale Ziffernanalyse**: Ein Beitrag zur computergestützten Deliktrevision,  
WPg, Die Wirtschaftsprüfung, Der Berater der Wirtschaft, Heft 16, August 1999
- ☐ **Grundschutzhandbuch**: Ein Werkzeug für die wirkungsvolle EDV-Revision?  
KES, Zeitschrift für Kommunikations- und EDV-Sicherheit, Ausgabe 2, Mai 1999
- ☐ Ein ganzheitlicher **Archivierungsansatz im SAP R/3™-Umfeld**,  
Vortrag Management Circle, April 1999
- ☐ **Prüfung von IT-Verträgen**, Vortrag Management Circle, Frankfurt 1999
- ☐ **Prüfsoftware** im Alltag,  
KES, Zeitschrift für Kommunikations- und EDV-Sicherheit, Ausgabe 2, Mai 1998
- ☐ Alternativen, Techniken und Probleme (mit Lösungshinweisen) bei der **Übernahme von Großrechnerdaten** in PC-Prüfsoftware.  
Aktualisierter Aufsatz aus dem Leitfaden zur Einführung in die computergestützte Datenprüfung
- ☐ Wege und Verfahren zur **Prüfung doloser Handlungen**  
Zeitschrift Interne Revision, Hefte 5 und 6, Oktober und Dezember 1997
- ☐ **Verfahren** für die EDV-Revision  
KES, Zeitschrift für Kommunikations- und EDV-Sicherheit, Ausgabe 6, Dezember 1997
- ☐ **Mit Software gegen Unterschlagungen**, WIK, Zeitschrift für Wirtschaft, Kriminalität und Sicherheit, Nr. 4, August 1997, Zeitschrift „Sicherheit Forum“, Zürich, Nr. 6, November 1997
- ☐ In Eigenregie auswerten: **SAP™-Standardlisten**  
KES, Zeitschrift für Kommunikations- und EDV-Sicherheit, Ausgabe 5, Oktober 1996
- ☐ **EDV-Revision** in einer PC-Netzwerkumgebung  
Zeitschrift Datensicherheits-Report, Ausgabe 7, Juli 1996
- ☐ File interrogation in a **SAP™-Host** environment  
Zeitschrift audit, Issue 34, London, Mai 1996
- ☐ **Unterschlagungsprüfung** und –prophylaxe mit Hilfe von EDV-Unterstützung  
Zeitschrift „Deutsche Steuerrecht“, Nr. 12, März 1996
- ☐ Prüfsoftware im **Vergleich** (Ein Überblick)  
Zeitschrift Interne Revision, Ausgabe 1, Februar 1996
- ☐ Unterschlagung, **Detektivarbeit** am Bildschirm  
KES, Zeitschrift für Kommunikations- und EDV-Sicherheit, Ausgabe 1, Februar 1996



- ❑ Alles außer Haus – **EDV-Outsourcing** bei SAP R/3™-Anwendungen,  
Zeitschrift „it-Management“, Dezember, 1995
- ❑ Automatisierte Revision von **SAP™-Großrechnerdaten**.  
Vortrag Konferenz „Interne Revision“, Wiesbaden, Mai 1995,  
Aufsatz, Zeitschrift Interne Revision, Heft 3, Juni 1995
- ❑ Die Unterstützung von **Saldenbestätigungsaktionen**  
durch den Einsatz einer Revisionssoftware.  
Vortrag und Aufsatz IDEA Anwendertreffen, 1994
- ❑ **Voraussetzungen** für den erfolgr. Einsatz einer Prüfsoftware im Revisionsbereich.  
Zeitschrift „Die Wirtschaftsprüfung“, Nr. 9, Mai 1994  
Zeitschrift "Audit Journal", Wien, Nr. 2 und 3, Oktober 1994
- ❑ Der Einsatz **automatisierter Prüfroutinen** zur Unterst. der in- und externen Revisoren  
Aufsatz, September 1994
- ❑ Computergestützte Datenprüfung mit dem Personalcomputer - **Mittel und Verfahren** -  
Vortrag Konferenz „Computergestützte Revision und Abschlußprüfung“,  
Frankfurt, September 1994
- ❑ Die Prüfung von **Netzwerken** mit Hilfe einer Revisionssoftware.  
Zeitschrift „ECO-Management“, Ausgabe 1, Januar 1994
- ❑ **Computergestützte Analyse von Großrechnerdaten,**  
**Zeitschrift Interne Revision, Ausgabe 5, Oktober 1993**
- ❑ Analyse und Aufbereitung von Daten aus **Warenwirtschaftssystemen**.  
Vortrag, Konferenz „Die Warenwirtschaft im Einzelhandel..“, Köln, September 1993
- ❑ **Wirtschaftlichkeitskriterien** beim Einsatz einer Prüfsoftware,  
Vortrag Konferenz GEDICON, Düsseldorf, 1990
- ❑ **Buch: R. Odenthal**  
**Revision und Abschlußprüfung mit dem Personalcomputer**  
Hamburg 1994, ISBN 3-930291-01-0, EUR 50,00  
Mit WINDOWS-Leitfäden zur Unterschlagungsprüfung und SAP-Prüfung auf Disketten
- ❑ **Buch: Dr. G. Wähner**  
**Datensicherheit und Datenschutz, Methoden und Instrumentarien für Computernutzer,**  
Düsseldorf 1993, ISBN 3-18-401297-2, EUR 50,00.
- ❑ **Buch: Dr. G. Wähner**  
**DV-Revision, Handbuch für die Unternehmenspraxis,**  
Ludwigshafen 2002, ISBN 3-470-53911-1, EUR 60,00

**Manuals for Windows**

- ☐ **(EDV-)Revision und personenbezogener Datenschutz**
- ☐ **Der Einsatz des SAP R/3™-AIS-Systems im Bereich der EDV-Systemprüfung sowie der kaufmännischen Revision**
- ☐ **EDV-Checkliste zur Ermittlung unterschlagungsgefährdeter Bereiche im Unternehmen**
- ☐ **Prüfung von Netzwerksystemen**
- ☐ **SAP™-R/2 Basisprüfung**
- ☐ **Unterschlagungsprüfung und PC-Prüfsoftware**
- ☐ **EDV-Übersicht, Software für die Revision**
- ☐ **Grundlagen und Arbeitstechniken der internen Revision**
- ☐ **Betriebsprozesse in SAP-R/3™ und deren Prüfung**
- ☐ **Die Überleitung von SAP R/3™-Daten an PC-Prüfsoftware WinIDEA und ACL**

Your contact person

Roger Odenthal

Roger Odenthal Unternehmensberatung

Windmühlenstraße 159-161

D-51063 Köln

Phone                   +49-(0)221-4921403

Fax                     +49-(0)221-4921404

e-mail                 [info@roger-odenthal.de](mailto:info@roger-odenthal.de)

homepage             [www.roger-odenthal.de](http://www.roger-odenthal.de)