

# SAP- Audit Guidelines R/3

**Release 3.0D**

**Current: February 20, 1997**

**Order no. 5001 4633      Fax no. 06227/7-41497**

**<http://www.sap.com/germany/contact/user.htm>**



SAP(R) AG- Neurtottstrasse 16- 69190 Walldorf, Germany  
Information in this document is subject to change without notice.

---

# SAP R/3 AUDIT GUIDELINES

<b>INTRODUCTION .....</b>	<b>8</b>
<b>1 SYSTEM OVERVIEW .....</b>	<b>11</b>
<b>1.1 Objective .....</b>	<b>11</b>
1.1.1 Technical and organizational overview of the system .....	11
1.1.2 Clarity of the system for the auditor/auditing task .....	12
1.1.3 Defining the scope of the audit .....	12
<b>1.2 Requirements .....</b>	<b>13</b>
<b>1.3 Risks .....</b>	<b>13</b>
<b>1.4 Audits .....</b>	<b>14</b>
1.4.1 Responsibilities .....	14
1.4.2 Systems in use (testing, ..., live) .....	14
1.4.3 Authorization and user menu for the auditor .....	14
1.4.4 Recording the business structure .....	16
1.4.5 Release versions .....	16
1.4.6 Components/functionality .....	16
1.4.7 Modifications .....	17
1.4.8 Update termination .....	19
1.4.9 Data flow plan .....	19
<b>1.5 Proposed auditor authorizations .....</b>	<b>20</b>
<b>1.6 Complete overview of customer name ranges .....</b>	<b>21</b>
<b>2 SECURITY AND ACCESS PROTECTION .....</b>	<b>23</b>
<b>2.1 Objective .....</b>	<b>23</b>
<b>2.2 Requirements .....</b>	<b>24</b>
<b>2.3 SAP facts .....</b>	<b>25</b>
2.3.1 Basics of the authorization model .....	25
2.3.2 Authorization structures .....	27
2.3.3 Separating maintenance and activation .....	27
2.3.4 User master .....	27
2.3.5 Password protection and logon .....	28
2.3.6 Customer-specific authorization checks .....	28
2.3.7 Upstream security systems .....	28
2.3.8 TABLE TSTC – "SAP Transaction Codes" .....	28
2.3.9 Customizing .....	28
<b>2.4 Risks .....</b>	<b>29</b>

<b>2.5</b>	<b>Audits</b> .....	<b>30</b>
2.5.1	User management .....	30
2.5.2	Security and access protection .....	32
2.5.3	Important individual authorizations .....	34
<b>3</b>	<b>WORKBENCH ORGANIZER AND TRANSPORT SYSTEM</b> .....	<b>38</b>
<b>3.1</b>	<b>Objective</b> .....	<b>38</b>
3.1.1	Functional Integrity .....	38
3.1.2	Traceability .....	38
<b>3.2</b>	<b>Requirements</b> .....	<b>39</b>
3.2.1	Job submission .....	39
3.2.2	Implementation of a change .....	39
3.2.3	Acceptance and production transfer .....	39
<b>3.3</b>	<b>SAP facts</b> .....	<b>40</b>
3.3.1	Purpose and structure .....	40
3.3.2	SAP systems .....	41
3.3.3	Correction and repair .....	42
3.3.4	WBOT settings .....	43
3.3.5	Conducting transports .....	44
<b>3.4</b>	<b>Risks</b> .....	<b>45</b>
3.4.1	Validity of ODEs .....	45
3.4.2	Incorrect CTS settings .....	45
3.4.3	Access to operating system level .....	45
3.4.4	Instability .....	46
3.4.5	Manipulation .....	46
<b>3.5</b>	<b>Audits</b> .....	<b>47</b>
3.5.1	Recording the existing procedure .....	47
3.5.2	Review of the model .....	47
3.5.3	Compliance with the model .....	47
3.5.4	Concrete auditing steps .....	47
<b>4</b>	<b>ACCESSING AND LOGGING TABLES</b> .....	<b>49</b>
<b>4.1</b>	<b>Objective</b> .....	<b>49</b>
<b>4.2</b>	<b>Requirements</b> .....	<b>50</b>
4.2.1	Logging .....	50
4.2.2	Customer-specific tables .....	50
4.2.3	Access protection .....	50
4.2.4	Work and organization instructions .....	51
4.2.5	Safeguarding the information flow .....	51
<b>4.3</b>	<b>SAP facts</b> .....	<b>52</b>
4.3.1	Purpose and structure of tables .....	52
4.3.2	Table access and logging .....	53
4.3.3	Validity range and customer tables .....	54
4.3.4	ABAP reports .....	54
4.3.5	Examples of important tables .....	55

---

4.4	Risks .....	56
4.5	Audits .....	57
<b>5</b>	<b>JOB REQUEST PROCEDURE/DOCUMENTATION AND SYSTEM LOGS .....</b>	<b>58</b>
5.1	Objective .....	58
5.1.1	Procedure for requesting jobs .....	58
5.1.2	Job documentation .....	58
5.1.3	Job logs .....	58
5.2	Requirements .....	59
5.2.1	Procedure for requesting jobs .....	59
5.2.2	Job documentation .....	59
5.2.3	System logs.....	59
5.3	SAP facts .....	60
5.4	Risks .....	61
5.5	Audits .....	62
5.5.1	Recording existing procedures .....	62
5.5.2	Checking procedural models .....	62
5.5.3	Checking adherence to procedure .....	62
5.6	Documenting SAP jobs (suggested format) .....	63
5.6.1	General items .....	63
5.6.2	Requirements for starting the job .....	63
5.6.3	Post-processing requirements after the job run .....	63
5.6.4	Measures for restarting a job .....	63
<b>6</b>	<b>BATCH INPUT INTERFACES .....</b>	<b>64</b>
6.1	Objective .....	64
6.2	Requirements .....	64
6.3	SAP facts .....	65
6.3.1	Introduction.....	65
6.3.2	Authorizations .....	65
6.3.3	Run modes.....	66
6.3.4	Session logs .....	66
6.3.5	Analyzing sessions .....	67
6.4	Risks .....	67
6.5	Audits .....	67
<b>7</b>	<b>MASTER DATA CHANGES .....</b>	<b>68</b>
7.1	Separation of functions .....	68
7.1.1	Objective .....	68
7.1.2	Requirements.....	68

7.1.3	SAP Facts .....	68
7.1.4	Risks .....	69
7.1.5	Audits .....	69
<b>7.2</b>	<b>Traceability .....</b>	<b>70</b>
7.2.1	Objective .....	70
7.2.2	Requirements .....	70
7.2.3	SAP facts .....	70
7.2.4	Risks .....	71
7.2.5	Audits .....	71
<b>8</b>	<b>RECONCILING POSTING DATA CLOSINGS .....</b>	<b>72</b>
<b>8.1</b>	<b>Objective .....</b>	<b>72</b>
<b>8.2</b>	<b>Requirements .....</b>	<b>73</b>
<b>8.3</b>	<b>SAP facts .....</b>	<b>74</b>
8.3.1	Reconciling posting data .....	74
8.3.2	Periodic closing .....	76
8.3.2.1	Day-end closing .....	77
8.3.2.2	Month-end closing .....	78
8.3.3	Year-end closing .....	79
<b>8.4</b>	<b>Risk .....</b>	<b>82</b>
<b>8.5</b>	<b>Audits .....</b>	<b>83</b>
8.5.1	Reconciliation .....	83
8.5.2	Periodic closing .....	84
8.5.3	Year-end closing .....	84
<b>9</b>	<b>INVOICE CHECKING AND PAYMENT RUN .....</b>	<b>85</b>
<b>9.1</b>	<b>Objective .....</b>	<b>85</b>
<b>9.2</b>	<b>Requirements .....</b>	<b>86</b>
<b>9.3</b>	<b>SAP facts .....</b>	<b>87</b>
9.3.1	Vendor master data .....	87
9.3.2	Special fields .....	87
9.3.3	Prerecording documents .....	89
9.3.4	Posting accounts using the net amount procedure .....	89
9.3.5	Amount limits and tolerances .....	90
9.3.6	Payment programs .....	91
9.3.7	Authorizations .....	92
9.3.8	Reports .....	95
<b>9.4</b>	<b>Risks .....</b>	<b>96</b>
9.4.1	Vendor master records .....	96
9.4.2	Invoice checking .....	96
9.4.3	Payment proposal, payment run .....	96
<b>9.5</b>	<b>Audits .....</b>	<b>97</b>

9.5.1	Functional separation.....	97
9.5.2	Suspense accounts .....	97
9.5.3	Payment proposal list and payment list .....	98
9.5.4	Double payments .....	98

## Summary of Changes and Updates

**First edition:      Release 2.2D              March 29, 1996**

**Second edition:    Release 3.0D              February 20, 1997**

## Introduction

This **Release 3.0** Audit Guidelines manual, designed for **SAP R/3** systems, is intended to provide external auditors, IT auditors, and members of internal auditing staffs of companies using SAP with useful tips on how to proceed in auditing SAP software systems. This guide applies primarily to the basis and important aspects of the FI (Financial Accounting) application.

The information in this manual is intended as a "suggestion," not as a "binding guideline" or "standard." Any and all responsibility for the type, scope and results of internal and external audits lies solely with the auditor.

To study this manual properly, you should have a fundamental knowledge of the SAP system, and you should also be familiar with sound accounting principles.

The authors are members of a work group from the SAP Auditing work team „REVISION.“ Their experiences are presented here for your benefit.

Copyright 1997 by the authors:

Herr Barthel	FORBIT e.V., Hamburg
Herr Bernd-Striebeck	KPMG Deutsche Treuhand-Gesellschaft, AG, Düsseldorf
Herr Göttmann	Philip Morris GmbH, Munich
Herr Grotebrune	Unilever Corporate Audit, Hamburg
Herr Hungerbühler	ATAG Ernst & Young, St. Gallen
Herr Jackisch	Price Waterhouse Wirtschaftsprüfungsgesellschaft GmbH, Düsseldorf
Dr. Koch	Osnabrück/Melle
Herr Lencses	SCHITAG Ernst & Young Deutsche Allgemeine Treuhand AG, Stuttgart
Dr. Peemöller	ORIGIN Information Technology GmbH, Hamburg
Ms. Salzmann	Fielmann AG, Hamburg
Herr Sengpiel	Beiersdorf AG, Hamburg
Herr Schiwek	SAP Aktiengesellschaft, Walldorf
Herr Stein	KPMG Deutsche Treuhand-Gesellschaft AG, Düsseldorf
Herr Storm	C&L Unternehmensberatung GmbH, Berlin.

The authors are responsible for the content. The manual was edited by Herr Schiwek, SAP AG, Walldorf.

---

**Note:** This document and all of its components are protected by copyright. Any unauthorized use of this work outside the limits of the copyright is prohibited and punishable by law. This applies particularly to duplicating, translating into other languages, microfilming, and storing and processing the document.

Information is available in further detail in the SAP R/3 online documentation manuals, particularly:

- The manual "BC System Administration"
- The user guides "Configuration and Organization"

The authors of this auditing guide welcome your critiques and requests for changes or enhancements to future editions of the manual. These might be suggestions on providing expanded detail in an existing chapter, giving examples from concrete auditing experiences, etc. In this context, the following questions are of particular interest to us:

- Which tables and/or Customizing settings should be viewed as critical from an audit perspective, and why?
- Which objects (i.e. authorization objects) should be viewed as critical from an audit perspective, and why?
- Which SAP facts (i.e., settings from the Correction and Transport System up to Release 3.0 are not logged) should be viewed as critical from an audit perspective, and why?
- Which examples of concrete auditing steps (positive and negative) are available and should be included in this audit guide?

**A reply form is provided on the following page for your convenience.**

Please send/fax the reply form(s) (sorted by chapter) to the address indicated at the top of the form. Please use a separate form for each suggestion.

Again, we would greatly appreciate your comments. Even single-page suggestions are welcome!

Address:

"SAP R/3 Audit Guidelines" Team  
Attention: Mr. Peter Schiwek  
c/o SAP Aktiengesellschaft  
Department DEV.FI  
Postfach 1461

**FAX: (49) 06227/75/6924**

D-69185 Walldorf  
GERMANY

Sender:

Name:

.....

Title:

.....

Department:

.....

Company:

.....

Address:

.....

Telephone: ..... Fax: .....

Re: Additional information on SAP R/3 Auditing Guidelines

I would like to provide the SAP Audit Team with information regarding the following subject area  
(check appropriate item):

- Critical tables/customizing settings
- Critical objects
- Critical SAP facts
- Concrete examples of auditing procedures

In reference to:

SAP R/3 Audit Guidelines, Chapter:  
SAP R/3 System, Release:

Here is my information:

.....  
.....  
.....  
.....

Attachments with further information are included (check appropriate response):

- Yes
- No

# 1 System Overview

This first chapter of the SAP audit guide provides a quick overview of the SAP system and its technical and organizational integration. The auditor needs this overview in order to obtain an adequate system orientation, to be able to assess the overall state of the system and to determine which audit steps will be required.

You can also set up your own **user menu** to be used in generating a system overview. Further details are provided in **section 1.4.3**.

## 1.1 Objective

The purposes outlined above may be broken down as follows:

### 1.1.1 Technical and organizational overview of the system

Because of the **technical** scope of the system and the changes that are constantly being made to it, only those who concern themselves exclusively with the R/3 System software are capable of obtaining a full overview of the R/3 System. Generally, auditors do not fall into this category; they are generally outsiders who must determine which technical functionality is employed by a particular user with only a few initial steps on the system. This entire technical overview should be obtained in the shortest possible time and without the need for complex additional technical efforts. Ideally, the system would be able to automatically-"at the press of a button," so to speak-provide pertinent self-diagnostic information, display the system status and, if applicable, identify any changes that might have been made to the system within a specified time. From an auditing point of view, the main aspects of the system status include:

- Transactions
- ABAP programs
- Tables
- Files
- Authorizations, authorization profiles and user master records
- Data carriers
- Other security measures (such as table types and separating different clients)

The SAP R/3 System's **organizational** integration and the changes made to it determine the effectiveness of technical measures aimed at ensuring efficient data processing. Please ensure that comprehensive documentation is accessible to explain the organizational system status. The overview is to be supplemented by random sampling at the user companies (for example, to examine user authorization transactions), the system documentation (for example, to check the program and table documentation) and the system environment (for instance, working with the

system in the event of an abnormal termination).

### **1.1.2 Clarity of the system for the auditor/auditing task**

In addition to the general objective of ease of use, the objective of clarity for the auditor specifically includes the ability to gain an understanding of the overall system within a reasonable time. This ability is subjectively possible and objectively present, and is prerequisite for making a competent, accurate evaluation of system events.

### **1.1.3 Defining the scope of the audit**

Finally, the system overview should enable the auditor to concentrate his auditing tasks on specifically defined auditing areas. Once they have obtained an overview, the functional scope of the audit should be defined for all concerned. In addition, it should be possible at this point to define both the functional and the chronological framework of the audit.

## 1.2 Requirements

The installation to be examined must meet auditability requirements. The assumption is that, in general, the auditability requirements of tax authorities are being fulfilled. In particular, a company's implementation of R/3 and all modifications to the installation must be made within the framework of SAP's own recommendations (see the chapter "Name Ranges and Naming Conventions" in the BC SAP Style Guide manual for R/3).

This specifically affects:

- The procedures for making changes and configuration adjustments to the standard software
- Documentation of changes to the system and the system environment
- Naming conventions when altering transactions, ABAP's, tables, files and other SAP objects (see the overview in section 1.6)

**Client 000** may **only** be used by the standard software supplied by SAP, because it serves as a reference for other clients and is partially overwritten by the subsequent release or put level change. Certain key information supplied by SAP resides in Client 000 and may only be maintained by the system administrator (where applicable in conjunction with SAP consultants). **DO NOT** work in Client 000!

**Client 000 should be used as an auditing object in conjunction with the productive system.**

**Note:** See section 2.5.3 for a summary of the system administrator's authorizations.

## 1.3 Risks

The following risks are essentially involved in auditing SAP business transactions:

- Failure to follow sound accounting principles
- Inconsistent data
- Faulty operation
- Lack of control
- Unreliability

## 1.4 Audits

### 1.4.1 Responsibilities

You must acquire an overview of the total system responsibilities and of responsibilities involving:

- Critical data and tables,
- Authorizations,
- Programs, and
- Interfaces,

as well as changes to these elements. The overview will be expanded and enhanced as the audit proceeds.

### 1.4.2 Systems in use (testing, ..., live)

Using transaction SE06 "Setting Up the Correction and Transport System," determine which systems are currently deployed and, of these, which are used for production, development and/or testing purposes, and which are used for acceptance and/or training purposes.

In the productive system (whose audit is the focus of the presentation below) use **Table T000 in Client 000** to identify which clients are active in this installation.

First determine which system in which client contains the:

- Production clients
- Test clients

For information on connections with other systems (i.e. SAP R/2), see Chapters 3, "Correction and Transport System" and 6 "Batch Input Interfaces."

### 1.4.3 Authorization and user menu for the auditor

The auditor should be granted direct access to the system, including all authorizations listed in section 1.5. In granting access to personal data, care should be taken to ensure compliance with data security requirements and any existing contractual or business agreements.

Restricting auditors' authorization to display only should be sufficient to guarantee that the auditor may not and cannot make any changes to data.

**User menu:**

Set up a personal **user menu** to get an overview of the system. To do this:

1. Begin menu maintenance by selecting System-->> User profile-->> Maintain user menu.
2. The system displays a dialog window in which you enter the name of your first (or only) work area (i.e. displaying system status). You can then enter additional work areas (such as changes to system state, settings in Customizing, etc.).

The maintenance screen for the user menu appears. Select New Entries to display a list containing the menu bar texts from the SAP standard menu. These text elements are the same ones you see when you log in to a standard R/3 system. You can also switch the display of the accompanying transaction descriptions by pressing the "New Entries via TCode" pushbutton on the symbol bar. Next select individual transaction codes one after another (see section 1.4.7).

3. To include other applications in your work area, repeat step 2. Navigate downward in the standard menus list by double-clicking on the menu names, or go back up the list by clicking "Back."

4. To save your work area together with its applications:

- When you are finished selecting the applications you need, click on "Back" as many times as necessary until the entire list of applications selected for your work area reappears. You can change the texts contained in the list.

- Save the menu by pressing F11=Save (or click on the appropriate symbol).

Once it is closed, you have access to the user menu in a separate window. If you want to make changes to your menu, proceed as necessary.

Beginning with Release 3.0D, the so-called Session Manager will be set up instead of the user menu—initially for Windows 95 and later for other clients. Your documentation provides additional information about customizing individual user menus in the Session Manager.

#### 1.4.4 Recording the business structure

In the first step, you enter and analyze the structure maintained by the SAP system within each productive client (see Table T000). Users can view the structure in a hierarchical grouping of data and access structures in the:

- Client,
- Company code,
- Business area,
- Plant, and
- Storage location.

**Table T001** displays the company codes within a client.

Other links are stored in Table T001B (posting periods), TGSB (business areas) and T001W (plants).

#### 1.4.5 Release versions

This guide is based on **Release 3.0D**. You can determine the Release version of the application to be audited by calling up the system status from the "System" menu. View any release-related changes or enhancements to the system by selecting the menu path Tools--> Find--> Info system--> Release information.

#### 1.4.6 Components/functionality

The system's active main functions as queried under section 1.4.5 refer to specific system functionalities supplied by SAP, namely:

- |                           |  |
|---------------------------|--|
| - ABAP/4 programs         | SE38                                     |
| - Menus                   | SE41                                     |
| - Dynpros                 | SE 51, SE 52                             |
| - Tables                  | Customizing transactions O*, SM31, ABAPs |
| - Data Dictionary objects | DI* transactions                         |

The functionalities on the left can be expanded and modified with the functions listed to their right.

You can most easily examine the correlation between the main user-activated functions and the respective functionalities supplied by SAP for those purpose by using the Business Navigator in the Component view (Transaction SB01, or Tools--> Business navigator--> Component view; transaction descriptions belonging to the displayed functions can be displayed at either the top left or the bottom right within the graphics via the menu Settings--> Attribute positions.)

### 1.4.7 Modifications

SAP recommends that user modifications be made in conformity with the naming conventions. Section 1.6 contains a complete list of name ranges reserved for customers' use. The auditor should display and examine all:

- Transactions from Table TSTCT that begin with a Y or a Z
- ABAPs that begin with Y or Z
- Tables beginning with T9, P9, Y or Z

In a second step, transactions, reports, and tables in the system and in files or online help files should be examined to determine whether they function properly and are sufficiently documented.

The auditor should test other, randomly sampled functions that may not outwardly appear to have been altered or modified. This can be done by systematically investigating which user (besides SAP) made which last change, and on what date the change was made. Details are provided in the table below:

---

System Doc.	System State	Changes
Tables	SE16 and DI01 (in DI02 via Edit menu>> select Table type, and show where applicable Pool, Cluster, and View Tables)	SE01, SE03 transport info system DI02, and/or RSTBPROT, RSPARAM rec/client = All or same as xxx, where xxx is the client to be examined; date and last changer in table info
Table fields	SE12	SE01, SE03 transport info system Doc state version = USR in selection screen
ABAP's	SA38, SE38, TADIR	SE01, SE03 transport info system in SE38, display attributes 'created by' (SAP only)
Program fields	SE12	SE01, SE03 transport info system, Doc. version = USR in select screen image from DIxy
Transactions	TSTCT, TADIR	SE01, SE03 transport info system: date and changer for last TSTCT change in Client 000
Dynpros	SE51, SE52, SE41, SE42	SE01, SE03 transport info system Date/Time dynpro was saved/generated and changer in SM51
Dynpro fields	SE12	SE01, SE03 transport info system Doc version = USR in selection screen
Authorizations	SU01 (users) SU02 (profiles) SU03 (authorizations) RSUSR002	Info>>Change documents Info>>Change documents Info>>Change documents
Price list components	TADIR, TRDIR, SB01	SE01, SE03 transport

---

		info system
Company org. structure	Systems in use TSYST Clients T000 Company codes T001 Posting periods T001B Business areas TGSB Plants T001W	Date and last changer in table log with RSTBPROT and RSTBSERV
Database tables	DI02	SE01, SE03 transport info system
Database table fields	DI02	SE01, SE03 transport info system

#### 1.4.8 Update termination

When an update termination occurs, completed database changes for the current update request are reversed.

The "err" indicator is inserted in the log record, which will not be deleted.

The user is informed of the update termination via R/3 mail. The termination itself is recorded in the SYSLOG.

Each user can analyze and post-process his own update records as needed. S\_ADMI\_FCD authorization under Basis Administration is required in order to process other users' records.

The RFVBER00 report provides a (daily) list of terminated updates.

#### 1.4.9 Data flow plan

Incoming data from non-SAP systems needs to be recorded; specifically, its format (as a data record description), content, origin and quantity should be registered.

Data flowing out of the SAP System must also be noted and recorded; the details required in this case are format (that is, data record description and information regarding the file format), content, origin, and quantity.

The details should be scrutinized by doing random checks on authorizations granted to process batch input sessions, and on download capabilities, if they exist.

## 1.5 Proposed auditor authorizations

An authorization profile for auditors should be strictly limited to display capabilities only, for all applications and basic functions. An auditor should also be able to display change documents in addition to active data.

SAP supplies standard profiles with display authorizations only.

**F\_ANZ** for the financial sector

**A\_ANZ** for the investment sector

**M\_ANZ** for the material sector

**S\_A.SHOW** for basic functions, etc. (plus activity 08!)

This is the most widely applicable recommendation; please bear in mind all legal regulations regarding data security, as well as any relevant business or contractual agreements that may exist.

## 1.6 Complete overview of customer name ranges

OBJECT:	NAME LENGTH:	CLIENT RESERVATIONS:
Change doc. object	10	X..., Z...
Authorization/Auth. profile	12	No underline in 2nd character
Authorization object	10	Y_..., Z_...
Data element	10	Y..., Z...
Data elem.supp.no.	4	9000-9999
Dialog module	30	Y..., Z...
Documentation modules:		
General text (TX)	28	Y..., Z...
Book chapter (CHAP)	20	Y..., Z...
Release information	20	Y..., Z...
Structure	12	Y..., Z...
Domains	10	Y..., Z...
Dynpro number	4	9000-9999
Development class	4	Y..., Z...
Form	16	Y..., Z...
Function modules	30	Y_..., Z_...
Function group	4	Y..., Z...
Device category	8	Y..., Z...
Logical database	2	Y..., Z...
Matchcode ID	1	0-9
Matchcode object	4	
Menu	8	MENUY..., MENUZ...
Module pool dynpro	8	SAPMY..., SAPMZ...
INCLUDES	8	MY..., MZ...
Module pool dialog	8	SAPDY..., SAPDZ...
INCLUDES	8	DY..., DZ...
Module pool subroutines	8	SAPFY..., SAPFZ...
INCLUDES	8	FY..., FZ...
Module pool updater	8	SAPUY..., SAPUZ...
INCLUDES	8	UY..., UZ...
Message ID	2	Y..., Z...
Message numbers	3	900-999
Number range doc. object	10	Y..., Z...
Pool/cluster name	10	Y..., Z...
Relation ID	2	Y..., Z...
Report	8	Y..., Z...
Report categories	4	Y..., Z...
SPA/GPA parameter	3	Y..., Z...
Lock object	10	Y..., Z...
Style	8	Y..., Z...
SYSLOG reports	2	Y..., Z...

<b>SAP Audit Guidelines R/3</b>	<b>Release 3.0D</b>	<b>Current 2/20/97</b>	<b>Author AK REV</b>	<b>Page 22</b>
Tables (Pool, cluster, transport)	10		Y..., Z..., T9..., P9...	
Transaction codes	4		Y..., Z...	
View	10		Y..., Z...	
Help view	10		H_Y..., H_Z...	

## 2 Security and Access Protection

### 2.1 Objective

An access protection system and the ability to grant individual authorizations serves four basic purposes:

- Protection of confidential data against unauthorized disclosure
- Protection of data against unauthorized (including unintentional) changes or deletion
- Assurance of procedure clarity by providing tracking of who has or has had which authorizations within the system, and when they had those authorizations
- Guarantee that applications are auditable

According to commercial law, these measures (i.e., preemptive controls in the internal control system) should prevent violations of any legal restrictions regarding the erasure of electronically stored data. They should also guarantee the legally required audit trail traceability and ensure that no violations of sound accounting principles occur. In other words, these measures ensure that no unauthorized, incomplete, or incorrect data, or no data posted to the wrong period of account is entered into the system.

## 2.2 Requirements

The access protection system must ensure that only authorized individuals have access to the system and to particular data. It must be possible to key in the corresponding codes (passwords) protected from the view of others.

The system should ensure that:

- Only passwords of a defined minimum length are accepted,
- Certain sequences of characters that could easily be guessed are not accepted,
- The password may be defined and altered by the user only,
- The system automatically demands the password to be changed at defined intervals,
- Passwords are protected against being divulged to anyone other than the user himself.

The authorization model must ensure that the user's rights of access are restricted to those activities within the system that are absolutely required for him to accomplish, based on his function/responsibility within the company (principle of minimal authorizations). In other words, the model must envisage the deepest hierarchical structuring possible with respect to:

- The nature of the data access (reading, creating, changing, deleting)
- Programs
- Data or files
- Functions (menus and menu lines)

in conjunction with as many different combinations of these levels as possible.

Since the effectiveness of the SAP authorization model is strongly influenced by the procedure for assigning authorizations, the procedure itself must be examined as a part of the auditing process. The procedure should be organizationally defined and allocated and should be traceable. There should also be controls ensuring that the procedure is followed.

Finally, bear in mind that user master records, authorizations and profiles are newly created, changed or deleted in the Quality Assurance (testing) System, and are then transported to the production environment via the Correction and Transport System.

## 2.3 SAP facts

By assigning **authorizations**, an organization defines proprietary data may be processed by employees within the company, as well as which processing functions are necessary to accomplish this.

With Release 5.0 in the R/2 environment, a new procedure was introduced for creating and maintaining user masters, profiles and authorizations, and for protecting access to the SAP System. The procedure remains essentially the same for R/3 systems. This authorization model allows organizations to precisely yet flexibly grant and control user access to the R/3 system. This allows different authorizations to be assigned to the same user for different company codes. For example, a user might be granted change authority in company code 01 and read-only authorization in 002. The authorization model also includes security measures to discourage unauthorized logons or access to user master records, profiles and authorizations.

The following facts apply to administration of user masters and authorizations in R/3 systems:

### 2.3.1 Basics of the authorization model

User master records and authorization components are client-dependent. Therefore, separate master records and authorization components must be maintained for each client in the R/3 system.

**Objects** (i.e., data, tables, etc.) are protected by **authorizations** or collective authorizations that are allocated to the protected objects like locks on a door. They contain **values** (for example, a concrete company code 0001) for **fields** that are defined for an associated authorization object. Authorization profiles are like keys for the user, and a collective authorization profile is comparable to a collection of keys on a key ring. These "keys" are entered in the user's master record. The system checks to see whether a user's authorization profile fits an authorization-like determining whether a key fits a lock-when an application is executed or when, in some cases, the keyword AUTHORITY CHECK appears in an ABAP (see section 2.3.6 and Chapter 3, "Correction and Transport System").

**Authorization checks are carried out only within the programs themselves.**

Authorization checks at transaction level are no longer commonly used, unless the check was explicitly defined during development of the transaction (for validation objects and/or validation rules). In any case, the checking of blocked transactions expires when the authorization check begins.

SAP requires that no direct changes are ever made to a productive system. SAP also recommends that change authorizations **not** be assigned to users in the following authorization objects:

- Authorization object S\_DEVELOP "ABAP/4 Development Workbench"
- Authorization object S\_PROGRAM "ABAP/4 Program Flow Validations"
- Authorization object D\_DDIC\_ALL "Authorization for Data Dictionary and Database Utility"
- Authorization object S\_TABU\_CLI "Table Maintenance for Client-independent Tables"

Access to the ABAP/4 programming language is validated using the following authorization objects:

- S\_PROGRAM: Starting ABAP/4 programs and maintaining variants, attributes and texts
- S\_ADMI\_FCD: ABAP/4 Administration

Further information is available in the following documentation manuals:

- BC "System Administration"
- XX "Configuration and Organization" for the respective SAP applications

(Note: XX stand for the respective SAP application.)

### 2.3.2 Authorization structures

/Refer to original page 31 for graphic/

Data protection / Data security  
Authorization Model

Customizing

Collective profiles  
Profiles--> User

Authorization--> Object

Value--> Field

You can build complex authorization structures from simpler ones by combining authorizations to create (individual) profiles and combining individual profiles to create collective profiles. With this technology, you can, for example, create a collective profile for Accounts Receivable clerks within company code 01. Each employee with that job description will then have this collective profile in his user master. If the profile needs to be changed, the change needs to be made only once (in the collective profile), and not in each user master.

For purposes of performance and system clarity, it is not advisable (although it is possible) to group collective profiles into other collective profiles.

### 2.3.3 Separating maintenance and activation

In the interest of security, the functions of maintaining and activating profiles and authorizations in the system are kept separate. Only the active version of a profile or authorization is valid in the system. An individual's maintenance authorization can be restricted to specific users, profiles and objects.

### 2.3.4 User master

The user master record contains a listing of the profiles and collective profiles authorized for that user. A reverse inheritance principle applies here, meaning that changes made at any level below the user master record level affect all higher levels above it, up to and including the user master record.

### 2.3.5 Password protection and logon

User-specific initial passwords are assigned to improve protection for passwords and system log-in. New passwords have to meet system-determined syntax requirements, and consequently undergo a variety of checks (see online documentation).

Moreover, customers can also add their own password validity checks to the SAP logon procedure as follows:

Any words/character sequences that are not allowable as passwords can be entered in Table USR40. The table can be maintained with transaction SM30.

Note: If the adjustable maximum number of user attempts is exceeded, the user will be blocked for a maximum of 24 hours, because the block is cancelled by the system when the date changes.

### 2.3.6 Customer-specific authorization checks

Customers can add their own authorization checks in an R/3 system by following one of these two procedures:

- Adding an authorization object to a **transaction in Table TSTC**; in this case programming is not required.
- Programming authorization checks in **ABAP/4 Programs** using the **AUTHORITY-CHECK** command

### 2.3.7 Upstream security systems

The following levels are significant for security checks:

- PC level
- Network level
- Operating system level
- Database level

Further validation is carried out at the SAP application level.

At this point, reference should also be made to the corresponding SAP Basis documentation and to the manufacturer's documentation.

### 2.3.8 TABLE TSTC – "SAP Transaction Codes"

Transaction SE93 is used to maintain transaction codes in Table TSTC of Client 000; use SM01 to lock and unlock it.

### 2.3.9 Customizing

Refer to Chapter 3, "Correction and Transport System," for information on security and access protection when customizing.

## 2.4 Risks

The high flexibility of the SAP authorization model and user administration model can lead to considerable security risks if they are used improperly. It is possible, for instance, for a user to influence work processes or posting tasks.

Examples:

- Recording of change documents (master data, documents and control tables) can be partially or completely deactivated.
- Authorization checks in programs (AUTHORITY-CHECK) can be removed.

SAP ships a wide array of "**standard**" profiles, each tailored to one of many different functions within a business. Many users adopt these profiles because of the complexity of the new authorization model. This might result in specific **risks**:

- Specific business requirements may not be sufficiently covered by the standard profiles.
- On the other hand, new risks might result from an attempt to adapt the standard profile to the company's business requirements (i.e., by expanding the authorizations assigned to a user).
- Auditability might be adversely affected if the SAP names for the profiles are kept after making changes to the profiles.

The profiles **S\_A.SYSTEM** and **S\_A.DEVELOP** both contain critical authorizations and therefore **should not be assigned in a productive system**.

Finally, a program for the test system that is "packaged" in another program could in some cases be transferred to the productive system and executed there, unless a mechanism within the company performs detailed checks of all transports to the productive system before releasing them.

These examples illustrate the fact that the security-as well as the proper and orderly functioning-of the entire system is directly dependent on the granted authorizations.

**Special attention should therefore be paid to the granting of authorizations.**

Before reviewing processing results, always check the relevant user authorizations to ensure that the processing results are based on authorized routines and entries.

## 2.5 Audits

### 2.5.1 User management

Familiarize yourself with the process for granting user authorizations (application and approval procedures and division of "create/maintain user," "create/maintain objects and authorizations," and "activate profile and authorizations" responsibilities) and also examine the internal procedures dealing with those subjects (ICS).

Find out whether written instructions exist for allocating and changing USERIDs. Obtain the relevant application forms and file them with the working papers.

Check whether official measures exist for ensuring that an employee's USERID is deleted as soon as he leaves the company.

Check whether the granting, changing and deleting of USERIDs must be authorized by a responsible member of staff.

Determine whether control procedures are carried out by responsible departments when a new user master is created or when a user's access levels are changed.

Check whether a mandatory procedure is required to change a user's access level when:

- The user's responsibilities within the organization change, necessitating changes to his user master record (danger of accumulated data access authority due to frequently changing responsibilities within the firm)
- Employees leave the company (resignation)

Check whether employees' authorization profiles correspond to their areas of responsibility.

Take random samples to compare approved authorizations with authorizations actually granted.

Check whether a mandatory procedure is required to change profiles and authorizations when an object is changed.

Check whether changes to the user authorization concept are being documented, and whether this documentation is being retained for at least 10 years.

**Special individual checks:**

Who is active in the system?

Menu path Tools--> Administration--> Monitor-->

System monitoring--> User overview

Alternative: Transaction code SM04

Statistical evaluation via user activities (per app. server only!)

Menu path Tools--> Administration--> Monitor--> Performance--> Workload-->

Statistics Record--> Choose Record pushbutton. Then look at SE38 (for example).

Alternative: Transaction code STAT

Changes made to user XXX

Menu path Tools--> Administration--> User maintenance--> Users--> Info-->

Change documents--> Users--> User name--> Changes since--> Chg.Auth.  
pushbutton.

Alternative: Transaction code: SU01

Which user has critical system authorizations?

Menu path Tools--> Administration--> User maintenance--> Profiles--> Info-->

Overview--> Users--> Select Object--> Basis Administration--> System  
authorizations. Values with \* = test all.

Alternative: Transaction code: SU01--> Info system

## 2.5.2 Security and access protection

Determine whether any special access protection software is installed.

Have someone explain and demonstrate the logon procedures. Obtain a copy of any written documentation that is available (manuals, organizational instructions, etc.).

Establish whether the system forces the user to regularly changes his password (system parameters and/or **external** security software).

Check Table USR40 to see which customer-specific passwords are not allowed. Find out whether changes can be made to this table online, and determine which people have access to the corresponding report authorization group.

Check whether passwords must be re-entered after the system has been left running unused for long periods of time (system parameters and/or **external** security software).

Make sure that all authorizations for user **SAP\*** have been revoked and have been transferred to a secret emergency user.

**Caution:** If the SAP\* user master is deleted, SAP\* is reset to the standard password "PASS" and reverts to the standard privileges of a superuser.

Also ensure that the standard password of user DDIC, which is generally required only for installation and maintenance activities, has been changed in Clients 000 and 001. In addition, the extensive authorizations in the DDIC should be only temporarily accessible.

Using the menu or transactions SU01-SU03, display user master records and authorization information. The following analyses are possible:

- User master records
- Profiles
- Authorizations
- Authorization objects
- Change documents

Use these analyses to determine if only appropriate, job-specific authorizations were issued. Pay special attention to authorizations for data processing employees; authorization to actually change data should be granted to DP employees only in exceptional cases. Also determine what records of assigned authorizations are available.

Using transaction **SE16**, you can look at Table **USR02** to determine which users have not been logged in to the system for an extensive period of time or at one time were not logged in for an extensive period of time. When requested, enter the user with a "\*" character and make an unmasked 8-character 0 entry in the "TRDAT" field.

Recommend to the company being audited that they delete these user master records, or at least block them.

Manipulation possibilities exist when these unused user master records are accessed without proper authorization. This can occur if the "owners" of these records have never logged into the system and therefore never changed the password from the standard initial password. In this case, it might be possible for an unauthorized user to manipulate data using other user names.

In this context, you should also check whether the system requires the standard password to be changed or after a certain number of days (also possible for all other passwords) or whether the user is blocked if this does not occur. This function is specified using the system profile parameter "login/password\_expiration\_time" (Report **RSPARAM**).

Using transaction **SM01**, find out which transactions are blocked (an X indicates that the transaction is blocked for all users).

When the **rec/client** switch in the operating system is set to "All" or "<md>," logs of table changes can be called up using the ABAP reports **RSTBPROT** (table log database evaluation) or **RSTBSERV** (analysis via display and comparison of table-like objects). This function is originally set up in Customizing (monitoring with report **RSPARAM**).

Change documents are generated if a table includes the technical parameter "logging" and if the "write change documents" function is active in the system.

Check whether an adequate table change and release procedure exists (see Chapter 4) and whether any mechanism exists to verify that all changes in Table **TSTC** are completely logged.

Determine whether each department follows procedures to ensure that data for which it is responsible cannot be changed without its authorization.

Ensure that no validation objects can be switched off or deleted (Table **TSTC**, Tables and Check Routines and, in this context, transactions **SM31** and **SE38**).

Check whether the installed access control procedures secure the function that logs changes, so that any improper changes or attempts to conceal them can be discovered.

### 2.5.3 Important individual authorizations

As a rule, SAP users in secured areas (especially Accounting and System Maintenance) should operate under the **dual control principle**. What this generally means for system and master transactions is that an EMERGENCY USER should be appointed to fulfill required measures **in conjunction with** a representative from the relevant department. A substitute for the emergency user should also be named in case the emergency user is absent.

Relevant standard profiles, authorization objects and transactions from the accounting and system maintenance areas are listed in the following section.

---

**Note:**

*Transactions with mandatory posting will not only/no longer be entered and generated by the Accounting department alone, due to the increased integration of various programs (modules). This will apply to both documents and master records from other SAP systems.*

**Posting authorizations**

SAP systems include various standard profiles, authorization objects and transactions for posting, changing and displaying documents, not only in the FI application, but in AM, CO, HR, MM, SD, etc. as well. In keeping with the principle of division functions, the authorization for posting and documenting change transactions should be restricted to employees who are responsible for those tasks.

**Audits:**

Determine whether the authorization objects for posting functions of the SAP systems, as well as the corresponding standard profiles for posting functions, are granted only to employees of the appropriate departments who are responsible for those tasks.

**Examples:**

- Accounting document: Authorization for document types
- Accounting document: Authorization for company codes
- Accounting document: Authorization for business areas
- Accounting document: Authorization for account types
- Accounting document: Account Authorization for customers
- Accounting document: Account Authorization for vendors
- Accounting document: Account Authorization for G/L account

**Master data maintenance (such as FDxx, FKxx, FSxx, etc.)**

**Note:** xx stands for 01, 02, 03, etc.

In an internal control system (ICS), care should be taken to guarantee separation of the "posting" and "master data maintenance" functions.

In smaller accounting departments, this can be done by having the customer and vendor master data maintained by different departments, but with the responsible accounting department retaining the functions of monitoring and posting.

Alternatively, the SAP system can monitor master data changes to the respective areas by using transaction FK04 for vendors, FS04 for G/L accounts, and FD04 for customers. It is also possible to perform regular analyses using the RFDABL00 (customers) and RFKABLOO (vendors) ABAP reports. These reports can print out and display all master data changes onscreen.

Use report RFKKAG00 to compare vendor master records existing in both the Financial Accounting and Purchasing areas.

**Note:** Other analysis reports are available for master records for: RFBABL00 (documents), RFSABL00 (G/L accounts), RFDKLIAB (credit management), and RFBKABL0 (banks).

All master data changes must be logged for as long as they maintain document status. As it is generally quite difficult to distinguish between changes with and changes without document status, all master data changes must be included under the logging requirement for security reasons. It must be impossible to change and/or delete change documents.

#### **Audits:**

Gain an overview of which authorizations from the individual authorization objects predefined by SAP are actually defined, and what values are contained in the fields of those objects.

Determine which employees can **maintain master records** (i.e., objects F\_KNAI\_XXX, F\_LFA1\_XXX, F\_SKA1\_XXX).

Check whether those employees can also post transactions.

Find out how master data changes are monitored.

Check compliance with mandatory document retention periods.

#### **System transactions**

Profiles containing system authorizations (S\_USER\_All, SAP\_ALL, SAP\_NEW) should be **restricted** to as few employees as possible. Find out, therefore, who has control of these system authorizations.

**Only the emergency user should perform the debugging replace function (authorization S\_DEVELOP) in a productive system, and that user must strictly observe the requirements of audit traceability.**

#### **Master transactions**

Master transactions (SExx, SMxx, SUxx), as well as standard profiles S\_A.SYSTEM, S\_A.ADMIN, S\_A.CUSTOMIZ, S\_TSKH\_ALL and the S\_ADMI\_FCD authorization object, should be assigned only to a few selected user (i.e., the EMERGENCY USER and his substitute).

**Audits:**

It is important to determine who has the **transaction authorizations**:

**SM01**            "**Block and unblock transactions**"  
**SM02**            "**Select blocking entries**"

and who maintains the corresponding functions in the **authorization objects**:

**S\_ADMI\_FCD**        **System authorizations, including "Blocking transactions"**  
**S\_ENQUE**           **Display/delete blocking entries**

If **Table TSTC** is valid for all clients, you must perform this audit in the delivery client, otherwise perform it in the productive client.

Determine who has authorization to set or change system parameters (using operating system techniques).

Determine who controls the **transaction STAT** "Daily system statistics."

Determine who controls the maintenance authorizations **SU01/SU02/SU03** and/or the **S\_USER\_GRP**, **S\_USER\_PRO** and **S\_USER\_AUT** objects, and check whether these employees should be able to create and/or maintain SAP system users.

Check the assignment of maintenance transactions **SUxx**, in order to ensure separation of functions:

- User administrator:	Create users	<b>(SU01)</b>
- Authorization administrator:	Authorization maintenance	<b>(SU02, SU03)</b>
- Activation administrator:	Activation	<b>(SU02, SU03)</b>

**Note:**

*An administrator should **not** have **both** maintenance and activation authorization for profiles **and** authorizations. A user with these authorizations could assign restricted privileges to authorizations, then activate and assign them. This means, for example, that the value 07 in the authorization objects **S\_USER\_PRO** and **S\_USER\_AUT** should be accessible only to the activation administrator.*

*The SAP manual "BC- System Administration" contains further information on required authorizations for system and authorization administrators, especially in Chapter 2, "User Master Records," and Chapter 3, "Authorizations."*

*Since administrators often have extensive system privileges, you should check from time to time whether the authorizations assigned to them are correct and still correspond to the organizational situation of the company.*

Check to see who has **S\_NUMBER** "Maintain number ranges" authorization.

Find out which users have client-dependent or cross-client authorization for the transaction authorizations **SM30 and SM31** and/or standard profiles like **S\_TABU\_DIS, S\_TABU\_CLI** "Maintain ATAB Tables." Then determine which authorization classes exist for tables in Table TBRG and/or TDDAT. Check whether table authorization for all users with SM31 authorization is restricted to individual classes. Each authorized user should be able to maintain only the tables belonging to his area of responsibility.

Find out who has authorization for the **SE38** transaction "ABAP/4 Programming," and who has authorization for transaction **SE51** "Screen painter/Dynpro changes."

**Due to traceability requirements required by law, transaction SE38 is not permitted within a productive system.**

However, a special user with that authorization should be created for emergencies (with the name EMRGNCY, for example). All entries made by this user must then be logged in an easily traceable manner. The principle of **dual control** should be strictly followed in this situation.

Determine who has transaction authorization for **SM13** "Handling update records."

Report **RFVBER00** creates a list of terminated updates that should have been posted using the "post document" function. It also includes postings that have entered FI from other applications.

## **3 Workbench Organizer and Transport System**

### **3.1 Objective**

The Workbench Organizer and Transport System (WBOT) has the functions listed below (as of Release 3.0, the CTS is located under WBOT):

- Registration and documentation of all changes to system objects (objects in the development environment, or ODEs). This includes Data Dictionary elements (such as tables), ABAP/4 programs, screen templates, and user-defined objects (UDOs) and customizing objects.
- Avoidance of concurrent changes to a system object made by different developers.
- Orderly transfer and release of ODEs between different SAP systems or various clients within a SAP system.

#### **3.1.1 Functional Integrity**

Changes made to tables and programs lead to functional changes in the system. It is therefore important to ensure that only authorized changes are implemented and that all functions retain their proper relationship to each other.

#### **3.1.2 Traceability**

A further aim is to completely document all changes to the system in order to make them traceable.

## 3.2 Requirements

All changes are to be made using the Workbench Organizer (and Transport System).

Sufficient and binding rules must be established for job submission (such as the creation of an ABAP) and implementation of changes, as well as for testing, acceptance, and transferring changes to the productive system (see also section 3.2.3).

### 3.2.1 Job submission

Every programming change must be described in detail in a change request and must be formally approved by the owner of the data. This applies to both authorization for changes to programs and to the transfer of datasets.

### 3.2.2 Implementation of a change

Since ODEs are often valid system-wide, the test and production systems must be maintained separately.

the WBOT uses a locking mechanism to avoid making concurrent changes to the same object by different developers.

When ODEs are changed using the Workbench Organizer, the system log maintains a history log. This means that it is possible to restore prior versions of existing programs.

Follow the SAP naming conventions (name range for customer objects) to avoid problems during later release or put level changes.

Self-defined ODEs must be adequately documented.

### 3.2.3 Acceptance and production transfer

The dual control principle must be observed during acceptance testing; and it should be performed independently of the programmer. As a rule, it should be performed by the employee (department) requesting the change.

If program changes have made, examine the source code to make sure that only that part of the program that was meant to be changed was actually modified.

The acceptance test should be performed in an SAP system that is completely separate from the productive system (pre-production), using the same customizing settings that exist in the productive system as well as a suitable dataset.

Organizational measures should guarantee that no subsequent changes can be made to the changes or new developments after the current change has been.

Acceptance and transfer to production must be documented in writing. Other accompanying documentation (such as order and release forms) should be archived according to appropriate legal requirements.

## 3.3 SAP facts

### 3.3.1 Purpose and structure

The Workbench Organizer and Transport System consists of the following components:

- Workbench Organizer
- Transport System

The **Workbench Organizer** guarantees that only a single original objects exists for each existing ODE in all (networked) SAP systems. Changes are normally made only to this original and are then transferred to other SAP systems via the transport system.

The Workbench Organizer saves all changes to Data Dictionary elements and ABAP/4 programs. Old versions can then be restored or compared against the current version. Customizing settings can also be recorded according to system setting (Table T000).

The Workbench Organizer is automatically activated as soon as a user tries to change an object. Users cannot create or change an object until they have first created a change request with jobs in the Workbench Organizer or unless they use an existing change request. To prevent concurrent alterations, all other developers are locked out of an object whenever a job is being entered. This lock is not removed until the request is released.

When jobs are released, they are forwarded to the Transport System. The Transport System is designed to ensure complete and traceable transport of ODE and Customizing settings. It is system-independent, meaning that ODEs can be transported between all operating systems supported by R/3. The system automatically carries out all required conversions.

The Workbench Organizer and Transport System are set up to work in concert with each other. At the beginning of the development process, a change request and one or more tasks for each employee concerned is created. The corresponding objects are then generated and changed, and they are registered in the job. At the end of development, individual employees release their task(s) so that the change request and all edited objects can be exported out of the source system via a release. Transport to the respective target system then occurs at operating system level. Several corrections can be combined into one transport order.

### 3.3.2 SAP systems

For CTS, a networked SAP system consists of one or more SAP R/3 systems of the same version that share a common database system. SAP employs the following nomenclature to distinguish among these systems:

- (Special) **Development system:**  
Separate development of critical components of a project in an isolated environment
- **Integration system:**  
For development work on non-critical applications and system tests
- **Consolidation system:**  
To ensure development status; distributing function for following delivery systems
- **Delivery systems:**  
Can automatically import software (ODEs from consolidation systems)

**Note:** The term "delivery system" stands for the totality of a system delivered to a customer.

The minimum environment recommended by SAP is a system configuration containing development and productive systems. For many clients, the development and integration systems are combined into one "test system," and the consolidation and delivery systems are combined into a single "productive system."

**If development work is done on ODEs, a system with multiple clients for development, test, and release is not sufficient, because ODEs are generally valid for all clients, which means that any changes could immediately affect production.**

A client's system types are apparent when viewing the current settings for the **TASYS** and **TSYST** control tables (see section 3.3.4).

### 3.3.3 Correction and repair

SAP distinguishes between

- original objects and
- copies of original objects

An ODE is an original in exactly one SAP system. All other (networked) systems only contain copies of the original. All ODEs are stored in Table TADIR along with their development class, original system, author responsible, and last correction or last transport. The table is updated using the appropriate maintenance transaction for the ODE.

All SAP ODEs (tables, ABAPs, etc.) are stored at SAP in their original form; only copies are shipped to customers.

If users are developing their own programs, those objects exist as originals. Originals will never be overwritten by a transport.

The term **correction** as used by SAP refers to changes made to an original object, while the term **repair** refers to changes made to a copy.

The principle of **unique changeability** applies here:

An object can be changed only by a correction in the system in which it was created.

**Repairs** (changes to copies) should be made only if the "normal" method, meaning a **correction of the original and transporting to another SAP system**, cannot be used. This may be the case if there are errors within the SAP objects themselves, which, as mentioned above, are only available at the customer's site as copies (so-called emergency repairs).

The status of an ODE (original, copy, repair, etc.) is administered in Table TADIR. This table should be protected against manual access.

A repaired object will not be overwritten by transports as long as no confirmation of a change to the original is entered. The status indicator for changes to originals is not verified by the system, which means that the system does not check whether the original object was also corrected and whether it matches the repaired copy.

### 3.3.4 **WBOT settings**

The WBOT is controlled by tables that can be displayed and edited using transaction **SE06** (System settings for Correction and Transport System):

- **Table TSYST:**

Contains the technical description of all available SAP systems (in the network), including name, operating system, database system, etc. The Transport System exclusively uses the name entered in the "System name" field when checking the availability of an SAP system. Specifications in the other fields in this table are operational, with the exception of the "Charset" attribute (the character set used in each system).

- **TABLE TASY:**

Contains information defining the target systems for transports from the consolidation system.

- **Table DEVL:**

Contains the definition of transport levels. A transport level specifies the transport path from the integration system to the consolidation system.

(If there are multiple delivery systems, table TWSYS is also used.)

- **Table TWSYS:**

Contains the consolidation paths for change requests

- **Table TDEVC:**

Contains a directory of all development classes. An integration and consolidation system is assigned to each class.

These tables can be maintained **only by user DDIC** and must have the same contents in all SAP systems linked to the WBOT.

Further, you can determine which system-wide changes are allowed. This setting can only be made under user DDIC or by a user who has all authorizations for the Workbench Organizer (transaction SE03 or Tools--> ABAP/4 Workbench--> Overview--> Workbench Organizer--> Jump-- Tools) (Transaction SE01--> Utilities--> Tools-- Set System Changeability).

The following options are available:

- Objects not changeable:  
This settings allows no changes whatsoever to objects. No new objects can be created.
- Only original objects (with Workbench Organizer)  
This setting allows only original objects of the system to be changed, subject to correction control.
- All customer objects (with Workbench Organizer):  
This setting includes the setting "Only original objects" and also includes the capability of repairing customer objects in non-original systems.
- All objects (with Workbench Organizer):  
In addition to "All customer objects," this setting also offers the capability of repairing SAP objects.

**Note:** According to SAP, changes to these system settings are not logged. In Release 3.0 the WBOT can be assigned to an authorization object, which provides special protection as part of the authorization model.

### 3.3.5 Conducting transports

When a transport request is generated, a help file with the appropriate transport contents is created at the operating system level. When imported to the target system, this file is evaluated by the "**tp**" **transport program**. The "r3trans" program used in earlier releases should no longer be used, according to SAP recommendations.

If the SAP systems have a common transport directory, a "test import" can be automatically conducted when the transport requests are exported from the source system to the target system.

The authors of the transport requests will be informed of the success/failure (of the export or test import). Transport logs can be displayed in the Info system.

## 3.4 Risks

### 3.4.1 Validity of ODEs

Since ODEs are valid throughout the system, changes made to an ABAP program, for example, affect all clients within the indicated SAP system. For this reason, authorizations to change an ODE must be heavily restricted in the productive system (for example, no programming authorizations).

### 3.4.2 Incorrect CTS settings

Some transports may fail if the WBOT is not customized properly (Tables TSYST, TASYs and DEVL). The entire Transport System can be circumvented if the system's changeability is improperly configured ("all objects changeable"); in such a case, the changes made would no longer be traceable.

**Note:** The "all objects changeable" setting is still available as of Release 3.0.

### 3.4.3 Access to operating system level

When the WBOT is used, all transportable change requests are stored in a file at the operating system level. The changed data and customizing settings are stored in the file System name<sid> KT90001. Subscripts and documentation are stored in file <sid>KX90001. The actual import into the target system is effected by calling up the "tp" program at operating system level. While the import of file <sid> KT90001 is imported by the operating system using the command "tp import <sid>KT90001," the second file <sid>KX90001 can also be imported from SAP (in the target system). Like other types of system data, all directors and files involved should be protected from access by unauthorized users.

Only Subscript file <sid>KX90001 can be imported directly from the R/3 environment.

#### **3.4.4 Instability**

The SAP system consists of various changeable components, each independent of the others. Because of this complexity, modifications can easily lead to security lapses and instability. For example:

- Errors cannot be recognized immediately.
- Data may erroneously remain unprocessed or be incompletely processed or processed multiple times.
- The needed availability of system functions is not always guaranteed.
- There may be delays during planned function execution (run security)
- Planned checks may not always be carried out, which renders them totally ineffective.
- The system is then no longer reliable.

It is obvious that these situations can produce a great deal of risk.

#### **3.4.5 Manipulation**

The complexity of an SAP system and the accompanying error risk if modifications are not monitored can lead to instabilities that might be abused.

If no appropriate monitoring mechanisms are established, the fundamental possibility of system manipulation exists.

## **3.5 Audits**

### **3.5.1 Recording the existing procedure**

The first requirement is to get an overview of all user-defined ODEs and all corrections/repairs to SAP objects. It is important that a clear description of their functions is made available.

The existing procedure and documentation of the system maintenance and release procedure (if required for the audit) should then be recorded.

### **3.5.2 Review of the model**

The aforementioned requirements should be the basis for evaluating the model described above. In addition, you should perform a general check of the system, bearing in mind the objectives and risks detailed above. During this general check, note whether an adequate separation of functions exists (development- release-transport).

### **3.5.3 Compliance with the model**

Conduct random tests of development requests with the associated testing and release logs. These should be both top-down (from the change request to the ODE in the production environment) and bottom-up.

### **3.5.4 Concrete auditing steps**

Required audits:

- Check the WBOT settings and system changeability.
- Determine what procedure is used for the customer's own development as well as correction and repair (as of Release 3.0, repairs to SAP objects are possible only after requesting a repair key from SAP).
- Identify which users may generate and release a transport request.
- Conduct random tests of the transport logs (Transactions SE06 and ABAP RDDIT070- RDDI077).
- Identify which users may perform imports to the productive system.

- Determine what company-wide regulations are in place for using the Correction and Transport System, and determine the ways in which compliance with those requirements is verified.
- Examine manual access to Table TADIR.

**Note:** Changes to settings in Customizing which were made in the test system or development system and transported into the production system using the WBOT may be logged only in the test system. To trace changes, consult the change logs in the test or development system. Changes that are sent to the production system by a transport request are not logged there.

## 4 Accessing and Logging Tables

### 4.1 Objective

The objectives of the procedure for changing tables are:

- To ensure proper table configuration
- To provide the ability to trace all changes

The term "changes" is understood in this context as:

- Changes to the content of tables containing system control data from the following delivery classes:
  - > C- Customizing table- maintained by customer only- no SAP support
  - > G- Customizing table- customer can only insert information
  - > E- System control table- SAP and customer possess individual keys
  - > S- System table- maintained solely by SAP change = modification
  - > W- Customer's system table
- Changes made to table structures are monitored by the Workbench Organizer and the Transport System.

## 4.2 Requirements

### 4.2.1 Logging

The system must log all (relevant) changes made to information contained in tables (data records). Structural changes, such as changes made by corrections and repairs to the Data Dictionary, must also be recorded.

The logs for "critical" tables, such as tables that control the flow of quantities and values (i.e. Account Determination or Valuation), should be checked regularly using, at minimum, a random sample.

#### **Records of table changes must be retained for 10 years (in Germany).**

Users must be able to read changes made to tables within a reasonable time period.

### 4.2.2 Customer-specific tables

The SAP naming convention must be followed to avoid creating conflicts with future release upgrades and to maintain system traceability.

Document carefully all tables that you define yourself and all objects that you develop yourself.

### 4.2.3 Access protection

An authorization model must exist that regulates which user IDs are assigned authorization for table maintenance (for example, authorization objects S\_TABU\_DIS, S\_TABU\_CLI). S\_TABU\_CLI controls authorization for maintaining cross-client tables.

SAP has created a series of authorization groups for the standard system and has allocated an authorization group to each table and view.

- Existing authorization groups are stored in table **TBRG**
- Assign tables to authorization groups via table **TDDAT**

In order to maintain tables, should it become necessary to do so, you need the following authorizations:

- Authorization for the table authorization group and for the "Table Maintenance" activity
- Global authorization for client-independent tables

The global authorization check is for all tables with delivery class C (customers), G (customer tables with SAP entries), and E (system tables the customer can change).

This additional authorization is required because changes made to a client-independent table might also affect other clients within the system.

Use program **RSCLASDU**, "Table Classification," to list all tables that require client-independent authorization.

#### 4.2.4 **Work and organization instructions**

In order to be more independent of the knowledge of individuals and to insure that tables are properly configured, critical tables should contain "work and organization instructions" that provide the following information:

- Naming conventions
- Causes of and reasons for changing a table
- Consequences of changing a table

Change requests for critical tables must also follow the release procedure and must be performed via the Correction and Transport System. It must be possible to document a change that has been made to a table.

#### 4.2.5 **Safeguarding the information flow**

Because of the high level of integration within the SAP System, a table change may result in unintentional side effects (to other modules, for example). For this reason, the system must include a mandatory procedure to ensure the flow of information to everyone affected by a change in a "critical" table.

## 4.3 SAP facts

### 4.3.1 Purpose and structure of tables

A table is a two dimensional matrix that describes a relationship within the database system. It contains a header that defines the fields (attributes) and a variable number of identically configured rows that contain data values (data records).

A data record is divided into a primary key area and a functional area. The primary key uniquely identifies the data records within a table, and can be made up of several attributes.

There are four main types of **tables**:

- Tables containing system control data
- Tables containing basic commercial data
- Tables containing data of an organizational structure
- Tables for application data

**Tables** containing system control data should allow companies to adapt the standard software to their needs without changing the program itself. Tables contain variable influencing factors for:

- Process flow controls (i.e. account determination)
- Logic checks (i.e. allows only specific values to be input)
- Calculation routines (i.e. value added tax calculation)
- Automatic processes (i.e. posting of cash discount receipts)
- Screen modifications (i.e. mandatory field input)

### 4.3.2 Table access and logging

Follow the **introductory guide** when installing a system, as this can ensure that all system set-up tasks are completed appropriately.

Access tables in order to enter information using:

- Introductory guide
- Customizing menus
- Direct table maintenance (transaction SM30-SM32)
- The Correction and Transport System
- ABAP

#### **Table T000 (modify client-dependent Customizing settings)**

Use this table to specify whether changes to client-specific Customizing settings should be automatically logged in Customizing requests (change request) within a client. Enter the basic setting for this option in the "Display scope" field.

Changes made to table contents must be logged. Fulfill this requirement by making two system settings:

- For relevant tables, activate the field "**Table Logging**" (technical setting) in the Data Dictionary
- Initialize the parameter "**rec/clinet**" for the client(s) you want to log in the SAP start-up profile.

Analyze start-up parameters using **RSPARAM**.

Analyze changes to tables using the following ABAP reports:

- **RSTBPROT** Analysis of Log Database
- **RSTBHIST** Table Analysis (with History Administration)

Changes resulting from corrections and repairs to table structures logged in the Data Dictionary are monitored by the Correction and Transport System (if activated). The system maintains a table history so that these types of changes can be traced with the help of the SAP Information System.

### 4.3.3 Validity range and customer tables

A table can apply to all clients in the SAP system (client-independent) or apply only to a single client (client-specific).

- Client-independent tables contain data of general relevance, such as SAP system control data, language indicators, or transaction codes
- Client-specific tables contain application data as well as basic commercial data (with certain exceptions)

A table attribute that determines whether a table is client-independent or client-specific is specified at the time the table is defined in the Data Dictionary. In client-specific tables, the client is always entered in the first key position.

To comply with the SAP naming convention, the names of **customer-specific tables** should begin with Y or Z. Character strings beginning with T9 or P9 are still permitted for naming tables, due to methods that were formerly used.

A table name can consist of a maximum of ten characters; however only the first seven are significant. In order to set up a table that can be maintained using the "Table maintenance" transaction (**SM30-SM32**), use a maximum of five characters to name the table.

### 4.3.4 ABAP reports

Important ABAP reports for table analyses include:

- RSCLASDU "Table List with Classification"
- RSPARAM "Analysis of Start-up Parameters"
- RSTBPROT "Analysis of Log Database"
- RSTBSERV "Table Analysis (with History Administration)"

### 4.3.5 Examples of important tables

In financial accounting:

T000	Clients
T001*	Company codes and company code control
T003*	Types of documents and texts
T004*	Account plans
T007*	Control key
T008*	Blocking reasons for automated payment
T012*	House banks
T030	Fixed content table
T033*	Account determination
T042*	Payment transactions
T044A	Methods of foreign currency valuation
T044Z	Changed reconciliation accounts
T074	Special general ledger accounts
T077*	Account groups
T169*	Tolerances for account audits
TBAER	Document change rules
TCUR*	Exchange rates
T9*	Customer tables

In the Basis system:

TSTC	Transaction code administration (including test object)
TBRG	Authorization groups for tables
TDDAT	Authorization groups to be analyzed by table
TACTZ	Valid activities for each authorization object
TADIR	Development objects and transport attributes
TSYST	Directory of available systems (CTS)
TASYS	Delivery table (CTS)
TDEVC	Development classes for Transport System (CTS)
T078*	Screen selection, transaction dependent
T079*	Screen selection, entry dependent

(\*) \* indicates that the table contains further subdivisions.

## 4.4 Risks

Since tables in the SAP System have a central control function, the following risks exist if the procedure for changing table contents is insufficient:

- Incorrect settings may be made.
- 
- Changes made to a table may produce unintentional side effects in another area.
- These changes may then damage the integrity of the dataset and system functionality. Authorizations might also be changed if they are defined within tables. There is a risk that system changes might be made that cannot be traced.
- Change documents can be deleted without archiving.

Particular risks:

- Failure to initialize the "rec/client" parameter (see 4.3.2)
- Erroneous entry in Table T000 (see 4.3.2)
- Failure to log important tables
- System settings of the previous system (i.e., the system upstream of the production system, from which objects are configured via the Transport System)
- Copy functions between clients that overwrite the settings of tables without history updates

## 4.5 Audits

The following auditing steps are mandatory:

- Determine the procedure for changing tables.
- Evaluate the procedure according to the requirements described in the previous section.
- Make random checks to determine whether requirements have been met.

Other audit operations include:

- Test and release procedures
- Responsibilities and the authorization system for table changes
- A random check of the customer's tables with regard to documentation requirements and adherence to SAP conventions
- Settings in the procedure for logging tables, especially the technical setting in the Data Dictionary and the "rec/client" parameter in the SAP start-up profile
- Settings made in Table T000 (Change documents for Table T000 indicate whether changes have been made to the display scope during the test period.)

*Note: The "Log data changes" switch for Table T000 is passive in SAP delivery systems.*

- Determination of archival functions (before deletion)
- Monitoring of the frequency of changes to important tables

## **5 Job Request Procedure/Documentation and System Logs**

### **5.1 Objective**

#### **5.1.1 Procedure for requesting jobs**

The primary objectives of this procedure are:

- Protect company data and personal data
- Integrate data and functions
- Protect resources

#### **5.1.2 Job documentation**

The objectives of documenting jobs are:

- Ensure error-free processing
- Establish independence from the detailed knowledge of individual users
- Enable third parties who understand business activities to check the technical functions of the DP system within a given time frame.

#### **5.1.3 Job logs**

Job logs are required in order to prove that functions have been carried out in compliance with sound accounting principles, specifically according to the job request procedure.

## 5.2 Requirements

### 5.2.1 Procedure for requesting jobs

The basic job request procedure must include clearly-defined processes and responsibilities for:

- Requesting a job
- Executing a job
- Post-processing a job and distributing output

Since many jobs in the R/3 System can be created and started by a department, it is generally sufficient to maintain documentation of the procedure in the user manual for the application within each respective department.

Special procedures must exist for jobs that (1) require an operating device and (2) are not executed exclusively with the departmental operations because of this device. These jobs in particular must not be executed without a request (by a service department such as the computer center, for example). The job is usually requested by the department.

### 5.2.2 Job documentation

The SAP System automatically documents jobs that it generates.

When a job is generated by a user ("native job generation," such as sessions), the user must also document the job. This documentation should be created according to a standardized format (see the suggested format in section 5.6).

**The retention period for job documentation is 10 years.**

### 5.2.3 System logs

Job logs must identify the job that was started, when it was started, and the parameters used to run the job. System-generated job logs must be specially protected.

Furthermore, exceptional reports must be generated in critical areas based on system logs.

## 5.3 SAP facts

Generally, the system automatically generates a job (dunning run, for example) based on a job-specific command by the user. You can limit access to commands for generating jobs as part of the general authorization model.

Generally, jobs are defined, job steps are created, and start dates are specified in transaction **SM36** or by selecting the menu path Tools--> Administration--> Jobs--> **Job definition**.

Some jobs, like preparation reports, can be defined in transaction **SA38** or by choosing the menu path System--> Services--> Reporting--> **Program**.

Use transaction **SM37** to display the job overview, or choose the menu path System--> Services--> Jobs--> **Job overview**. Tools--> Administration--> Jobs--> **Overview**.

A job can consist of several steps.

There are two types of jobs:

- One-time jobs that are executed immediately or according to a schedule
- Periodic jobs

The system will start a job when a defined event occurs (i.e. at a specified time or upon completion of a different job). This allows you to set up a job network.

A job always has one status (and one status only) from the following list:

- Scheduled
- Released
- Ready
- Active
- Finished
- Cancelled

The following logs relating to an SAP/R/3 System are available as system logs:

- Job logs
- System log
- Database log
- UNIX log
- Workload log

Logs are objects of the Correction and Transport System (see Chapter 3).

To date, there is no job library.

## 5.4 Risks

In addition to these general risks:

- Unauthorized (display) access to company data and personal data
- Data program changes that are unauthorized, uncontrolled and unobserved
- High resource consumption due to unconventional program combinations
- Faulty operation, especially in exceptional cases (error handling)
- Dependency on the knowledge of individuals

there are specific risks related to the UNIX operating system, such as:

- An SAP job may initialize UNIX programs that copy or destroy the SAP System
- System passwords may be stored in procedures that can be openly read
- Jobs may depend on events external to the SAP System

## **5.5 Audits**

### **5.5.1 Recording existing procedures**

Record and document (to the extent required by the audit) the organizational rules for:

- Requesting jobs
- Documenting jobs
- Generating and handling system logs

### **5.5.2 Checking procedural models**

Check the organizational rules recorded in the last step against the requirements and risks detailed in this chapter.

### **5.5.3 Checking adherence to procedure**

To determine whether the organizational rules have been followed:

- Review company documents
- Evaluate system logs and log files (transaction SM21)

## 5.6 Documenting SAP jobs (suggested format)

The following items are a suggested format for documenting SAP jobs; this list, however, contains only suggestions and does not claim to be complete.

### 5.6.1 General items

Person responsible for content:

Job ID:

Brief task description:

Event:

Date:

Estimated runtime:

Online processing advisable:

Programs within the job:

Special features of the job:

### 5.6.2 Requirements for starting the job

(Event: see above)

Required peripherals:

Required tables and parameters:

Other requirements for starting the job:

### 5.6.3 Post-processing requirements after the job run

Data medium and forms required for output:

Subsequent jobs:

### 5.6.4 Measures for restarting a job

Error must be corrected directly:

- Correct error
- Restart procedure

Error need not be corrected directly:

- Reload saved data
- Generate error log
- Inform person responsible for the operation

Job name for reversing data:

What jobs may not run after a termination:

## **6 Batch Input Interfaces**

### **6.1 Objective**

Commercial laws require businesses to record, store and process all data completely, correctly, and in a timely fashion in compliance with accounting principles, and they prohibit changed data from being falsified in any way. Businesses are also legally required to monitor batch input procedures.

### **6.2 Requirements**

Requirements for creating effective monitoring include:

- Organizing process flows
- Separating incompatible functions
- Establishing control measures and control operations

The effectiveness of the internal control system is greatly influenced by the type and extent of process flow organization. Mandatory process requirements must be observed. Failure to comply with requirements must interrupt the process flow in a way that is brought to the attention of the control organization.

In an effective internal control system, certain functions remain separated. There should be a distinction between planning, executing and supervisory functions.

## 6.3 SAP facts

### 6.3.1 Introduction

Batch input is typically used to transfer data from non-SAP systems to SAP systems or to transfer data between SAP systems. The output system uses a data transfer interface provided by the R/3 application in the receiving system to transfer data via batch input. The interface program in the application then initiates a batch input session.

A batch input session is a set of one or more transaction calls supplied by a program containing user data. The system normally executes the transactions non-interactively, allowing rapid entry of bulk data into an SAP System.

A session simulates online entry of transaction codes and data. It generally uses the same procedures as interactive operation.

The data entered into transaction screens by a session is subject to the same consistency checking as data entered in normal interactive operation.

You can access batch input processing by selecting the menu path System--> Services--> Batch input--> Edit, or by accessing transaction SM35.

In most systems, sessions are started **non-interactively** with a background job that periodically scans for and initiates any sessions that have not yet been run. To execute a batch input session automatically, call up the ABAP/4 program RSBDCSUB. This program schedules sessions for immediate execution in the background processing system.

Running sessions **interactively** is usually reserved for testing or correcting sessions.

### 6.3.2 Authorizations

The system carries out the usual checks on user authorizations when batch input sessions are processed.

If a session is run in **batch mode**, the system checks the authorizations of the user specified in the batch input session. The user must be defined as user type BDC.

If a session is processed **online**, the system validates the authorizations of the user who is processing the session.

### 6.3.3 Run modes

A session can be run in one of three modes:

- Background  
In this mode, a session is processed immediately.
- Process/foreground  
Transactions that contain errors can be corrected interactively and transactions that have not yet been executed can be stepped through one at a time.
- Display errors only  
This mode is like process/foreground, except that transactions that have not yet been run and that do not contain errors are run non-interactively.

A transaction contains an error if it issues a message of type E (error) or type A (abnormal termination). Other messages are ignored and do not affect the execution of a session.

### 6.3.4 Session logs

Every batch input session generates a log when it is processed. Display this log by selecting the menu path System--> Services--> Batch input--> Edit--> Log, or by accessing transaction SM35. It contains all error messages resulting from transactions in sessions. It also includes the batch input error messages resulting from problems in the transaction process, listing the transaction code and screen where the error occurred. Finally, the session log contains all statistics about the session processing.

The system creates a log for a batch input session only if the session is processed. That is, the session must be processed in one of the above run modes. When processing a session, the system posts all error-free transactions and marks them as having been processed in the session. Transactions that contain errors are not posted and are flagged as incorrect. A session that contains incorrect transactions can be re-processed. During re-processing, the system processes only those transactions previously marked as incorrect.

The system generates a session log for each processing transaction which overwrites any existing log. This log lists only those messages issued in the most recent process. The system logs error messages as well as transaction messages. At least one message will appear for each transaction processed.

Delete processed sessions, their logs and the logs for which a session no longer exists by using program **RSBDCREO**. This program also reorganizes the log file in the batch input system.

### 6.3.5 Analyzing sessions

It is possible to analyze batch input sessions both before and after processing. To do this, mark the session in the overview. Select the session in the map log screen by selecting the menu path Goto--> Analysis--> Session.

## 6.4 Risks

Non-SAP source systems may contain data validation checks that differ from those for SAP tables. This may affect master data and transaction data.

If session names cannot be validated, users with batch input authorizations may be able to run, correct or delete sessions from other departments (depending on their authorizations).

## 6.5 Audits

The auditor should ask the following questions based on these monitoring requirements:

Is there an overview of all batch input interfaces for the SAP System that covers specifications such as these? :

- Work area to be transferred
- Data content
- File name
- Period
- Session name
- Processing job
- Relevant tables
- Reconciliation group
- Responsibilities

Which users are allowed to generate, run, correct or delete which sessions?  
(Menu path: Tools--> Administration--> User maintenance--> Info)

Is there an overview that shows which session names are reserved for specific departments?

(Menu path: System--> Services--> Batch input--> Edit--> Overview or transaction SM35)

Who reconciles the posting data in the processed sessions?

Who checks to see whether the data from the source system has been completely and accurately transferred on a timely basis?

What internal controls are maintained between the source systems and the regular processing sessions?

## 7 Master Data Changes

### 7.1 Separation of functions

#### 7.1.1 Objective

To obtain adequate security and force the internal control system to conform to sound accounting principles, specific functions within an organization must be separated.

In small companies, this objective is often difficult to realize for organizational reasons. These companies therefore require special checking of changes to master data, audits which must be individually designed to achieve a sufficient standard of security. In large firms, there is no substitute for the complete separation of functions.

#### 7.1.2 Requirements

Companies must clearly define the responsibilities and authorizations related to master data management.

Companies must adequately separate the functions between the DP department and the functional departments, as well as between master data maintenance and all types of entry activity.

#### 7.1.3 SAP Facts

The design of the SAP System and the wide range of different authorizations generally allow reasonable separation of organizational functions.

Authorizations for **G/L account master data** can be assigned based on:

- F\_SKA1\_KTP Organizational unit chart of accounts
- F\_SKA1\_BUK Organizational unit company code
- F\_SKA1\_BES Grouping of accounts according to authorization groups (optional)

Authorizations for **customer and vendor master data** can be assigned based on:

- F\_....\_APP Application (Financial Accounting, Sales or Purchasing)
- F\_....\_BUK Organizational unit company code
- F\_....\_BE. Grouping of accounts according to authorization groups (optional)
- F\_....\_AEN Grouping of individual master record fields (optional)

Individual G/L closing accounts, for example, can be protected by a special four-character authorization group that can be freely defined (master record: field SKB1-BEGRU authorization group, authorization object: F\_SKA1\_BES account authorization).

The **activity** belonging to the individual authorization determines the possible processing function:

- Create (01)
- Change (02)
- Display (03)
- Block/unblock (05)
- Delete (06)
- Display change documents (08)
- All activities (\*)

The activity codes are specified by SAP; see documentation for the Activity field for further information.

#### 7.1.4 Risks

An insufficient internal control system to monitor master data changes may impair compliance with accounting principles and the data security of the organization. Inadequate security for payment transactions (master data maintenance), for example, could result in financial losses.

#### 7.1.5 Audits

Who has authorization to create (01) and change (02) customer, vendor and general ledger master data?

In larger departments, are authorizations for accessing specific customer, vendor or G/L groups further restricted by account authorizations or change authorizations for specific fields?

Who has simultaneous rights to both change master data and to post data?

Are there any special authorization procedures (external to the system) for making changes to sensitive master data, and have dual control procedures been implemented?

Have the amount limits defined for posting and the tolerance limits defined for payment differences been followed (OBA4/OB57)?

## 7.2 Traceability

### 7.2.1 Objective

The accounting process must be traceable in all instances. In compliance with sound accounting principles and commercial law (§§ 238 f. of the HGB), all data that is posted is final („posted is posted“) and may not be erased. These principles must be observed at all costs.

### 7.2.2 Requirements

All master data changes and deletions must be properly logged, documented and retained.

Background: Accounting data must be recorded in compliance with sound accounting principles over the entire legal retention period (HGB § 257).

In this context, **change documents** become of central importance. They record all of the changes made to master records, tables, documents, etc., and pursuant to §257 of the HGB (German accounting regulations) they must be retained for up to ten years.

In order for the system to log changes made to an object, it must be defined as a **change document object** within the system. When a field in a master record/document is changed, the standard system creates a change document.

This requirement can be restricted by explicitly specifying in the Data Dictionary that no change documents should be generated for a particular field.

### 7.2.3 SAP facts

The system fundamentally records all changes, ensuring the traceability of all changes.

The automatic system change log procedures can be circumvented by individual developments.

The authorization object **S\_SCDO** (Delete Basis- Central Functions, Change Documents) affects only change documents for data that are not relevant for accounting.

.See: Transaction SE84 (Repository Info System) --> Environment--> Authorizations--> Authorization objects--> Document use--> Program/Transaction//

#### 7.2.4 Risks

- Failure to completely record posting data
- Deviation from sound accounting principles

#### 7.2.5 Audits

Do **authorizations** exist which allow users to change a dataset without logging the change?

Are adequate checks and controls over master data **changes** maintained and implemented in a verifiable manner?

Check master data **change documents** using these **ABAP reports and transactions**:

- **RFDABL00** Documentation of Customer Master Data Changes
- **RFKABL00** Documentation of Vendor Master Data Changes
- **RM06ICD1** Purchasing Info Record Changes
- **RSSCD100** Display Change Documents
- **FS04** G/L Account Changes
- **MM04** Display Material Master Data Changes

**As of Release 3.0:**

- **RFBABL00** Change Documents for Master Data
- **RFBKABL0** Bank Master Data Changes
- **RFDKLIAB** Credit Management Master Data Changes
- **RFSABL00** G/L Account Master Data Changes

---

## 8 Reconciling Posting Data Closings

### 8.1 Objective

Business entities are legally obligated to keep books and comply with applicable accounting rules and regulations in doing so. If accounting tasks are performed by data processing systems, the business entity must ensure that those systems also comply with accounting rules and regulations.

Thus, the department or the person responsible for accounting information must monitor the processing results. The object of doing so is to ensure:

- Completeness
- Authenticity
- Timeliness
- Correct data valuation
- Precise account assignment
- Accurate summation
- Proper posting

Accounting is deemed to be efficient and in compliance with accounting principles if its design allows outside parties who have a reasonable knowledge of business to obtain an overview of the company's activities and position within a reasonable span of time. Users of the information must be able to trace the origin and settlement of business activities.

As a rule, the basic functions of an accounting system comprise the following ledgers and statements:

- Opening balance sheet
- Document collection
- Compact journal
- General ledger
- List of assets and liabilities in report form
- Balance sheet and profit and loss statement

## 8.2 Requirements

The formal structure of an accounting system will depend on the legal requirements of the respective country. Systems that automatically process and store accounting information must follow specific procedures for collecting and recording documents, journals and ledgers in compliance with commercial law. This data will be retained for six to ten years, depending on the laws of the respective country and on whether or not a hard copy of the posting document is created.

To fulfill the objective of completeness, it must be possible to reconcile posting data at any time, regardless of how integrated the SAP applications are. To that end, SAP provides the process controls and checks at various levels of the application. Controls that detect and prevent inconsistencies must be complementary.

To fulfill the basic requirements of sound accounting principles, companies must fully and accurately record all business activities that are subject to financial reporting in a consistent and timely fashion which can be easily audited at any time. In an integrated system, these requirements are not limited to posting-related transactions; data security and backup, as well as the tables that control such a system, are also subject to those requirements.

The procedure for year-end closing must include the controls and checks for day-end and month-end closings. Non-recurrent tasks must also be monitored. Responsibilities must be clearly regulated for these tasks in particular.

Posting data must be documented. This can be accomplished by either printing or microfilming the journals and accounts.

---

## 8.3 SAP facts

### 8.3.1 Reconciling posting data

Users can enter original documents in document sessions. The system assigns control totals, such as the number of documents, debit total/customers, etc., to each session. The FI system stores control totals per user (FB07) so that they can be compared against the existing control total.

The document storage capability guarantees that the balance of all postings remains zero. This can be verified at any time by using the programs for balance sheets and P/L statements.

Subsequently post totals using program RFBUSU00.

A unique document number is assigned to each document. When the system assigns numbers to documents (transaction FBN1/table INRDP), it numbers them consecutively. If documents are numbered externally, the system ensures that the same number is not assigned twice.

*When SAP Module MM is used, non-consecutive document numbers might be issued in some cases in Financial Accounting. Specify the quantity of numbers stored in the buffers by using transaction SNRO.*

*If entries are made successively from different application servers, each application server assigns the next available document number from its number range buffer. This means that the document numbers are not issued in the chronological order in which the documents were produced.*

*When entering numbers into the buffer, the last number in the buffer is used as the last issued number of the number range interval. If the SAP System is powered down, the document numbers that have been entered into the buffer but have not been used are lost. When the system is re-started, the next document numbers are entered into the buffer according to the last document number that was issued. This can cause gaps to occur in the document numbering system.*

All documents generated within a specific time period are recorded in the compact document journal **RFBELJ00**. The summary report RFBELJ00 provides the totals sheets for reconciliation. Manually transfer these reconciliation totals to a list where they can be aggregated and their balances carried forward.

To compare accounting figures, perform the "**accounting reconciliation**," which shows whether the monthly debits and credits are supported by appropriate documentation. For this purpose, use report *SAPF190, "Financial Accounting Reconciliation Analysis."*

### **Reconciling G/L account postings**

G/L accounts are reconciled using the audit trail. To do this, compare the lists from report **RFHABU00**, "General Ledger from the Document File," or from report **RFKLBU10**, "Account Details from Historical Accumulated Audit Trail" against the list of G/L account balances **RFSSLD00**.

### **Reconciling accounts on an open item basis**

Open item accounts are reconciled by comparing the lists of customer and vendor balances **RFDSL00** and **RFKSLD00** against the lists in the audit trail for open item accounts or against the historical balance.

- Open item account balance audit trail: **RFKKBU00** or **RFKKBU10**
- Historical balance audit trail: **RFHABU00** or **RFKLBU10**

Additional reconciliation programs can be found by selecting the path "System--> Services--> Reporting" and then entering RF\*. Program **RFBPET00**, "Document Line Item Extract," can be used for closing procedures at the document level.

### 8.3.2 Periodic closing

The main purpose of general ledger accounting is to fully represent external accounting and the accounts involved in it. Collecting and maintaining all business transactions (primary postings and settlements from internal accounting) in an integrated business software system guarantees that the accounting process is complete and reconciled at defined periods of time.

The FI general ledger system offers the following functions:

- Freely definable classification of accounts at the group or company level
- Automatic entry of all subsidiary ledger items to the general ledger (reconciliation accounts)
- Periodic updates of the general ledger and the values in cost accounting areas
- Timely evaluations of and reports on the current posting data in the form of account statements, financial statements with different balance sheet versions, and other analyses

Documentation of individual transactions in the following areas is available at all times in documents, line items and transaction figures at various levels:

- Accounting information
- The journal audit trail
- Summary and balance transaction figures
- Evaluations of the balance sheet and profit and loss statement.

During the current fiscal year, the general ledger is primarily used:

- For continuous, central collection, reconciliation, and documentation of all posting data
- As the basis for a reporting and analysis system structured according to requirements (such as transaction figures per account or individual document audit trail)
- For day-end and/or month-end closing procedures that can be called up when they are required.

### 8.3.2.1 Day-end closing

Daily closing procedures are not mandatory in the system.

To monitor data according to the ICS, you can regularly create and check the following analyses:

- Document journal **RFBELJ00**
- Posting Totals **RFBUSU00**
- Update Terminations **RFVBER00**
- List of Change Documents **RSSCD150**
- Correspondence **SAPF140**

These analyses of day-to-day operations are performed at the user's discretion.

### 8.3.2.2 **Month-end closing**

The activities for month-end closing will depend, among other things, on how the data structure (business areas, profit centers, etc.) has been configured. In general, proceed as follows:

- Block the old month
- Compare documents and transaction figures
- Create the necessary evaluations for documenting the posting data
- Create the advance return for the tax on sales and purchases
- Reconcile the accounts

The document journal, RFBELJ00, functions like the general ledger.

Reconcile the posting data as described in Chapter 8.

The accumulated balance audit trail must be established before the documents are archived.

The sequence in which the documents are archived will depend on the volume of documents and the amount of available storage space in your DP system.

#### **Posting periods**

Maintain posting periods for each company code depending on the fiscal year variant. The R/3 System recognizes 12 posting periods for regular posting of data and four additional posting periods for closing procedures.

Different periods can be defined for individual accounts or account groups.

### 8.3.3 Year-end closing

The year-end closing can be based on the month-end closing procedure, although this is not mandatory. A specific range of programs prepares the accounts and posted line items for year-end closing. Important steps in preparation for the closing include:

- Closing the posting periods
- Valuing the line items and G/L accounts in foreign currencies
- Identifying the vendors carrying debit balances and customers carrying credit balances
- Posting the revaluations, adjustments and accruals
- Reconciling the subledger accounting systems and the upstream systems

A number of real-time reports support the closing procedures, such as:

- Comparison of documents and transaction figures
- Aggregate postings
- Posting of open items
- Carrying forward balance sheet account balances with multiple balances carried forward after the start of the new fiscal year

All reports can be accessed at any time online.

### **Balance sheet and profit and loss statement**

The balance sheet and profit and loss statement can only be printed out by means of ABAP. Report **RFBILA00** is available as a standard feature.

The list contains the financial statements (balance sheet and profit and loss statement) of the reporting timeframe you choose within a fiscal year, including the absolute and relative results of a comparison period.

The structure of the financial statements depends on the chart of accounts you choose for the company code (see Table T0004/transaction OB13).

### **Balance carried forward**

A new fiscal year is opened with the first posting to the fiscal year. To do this, the appropriate posting period must be opened.

In the SAP System, the balance carried forward procedure is executed using the appropriate reports (SAPF010 for open item accounts and SAPF011 for general ledger accounts). The profit and loss account balances are carried forward to the retained earnings account or accounts, and the balance sheet account balances are carried forward to their own accounts. A special opening balance sheet is not required.

Postings made to the old fiscal year automatically adjust the balance carried forward. Therefore, it is not necessary to close the old fiscal year and make the closing entries in order to open the new fiscal year.

If a balance carried forward procedure is performed at the end of the fiscal year, postings made to the old fiscal year will not adjust the balance carried forward, since the system does not interpret postings to the old fiscal year as such.

## Reorganization/archiving

Archive data that is no longer needed in the online system by using the special standard functions (in Accounting, for example, under the menu path Financial accounting--> General ledger--> Periodic processing--> Archiving or using transaction F045). The system reorganizes any data that remain available online. In order to archive data, certain conditions that are partly predefined by the system must be met. The user can also define other conditions, such as the life span of accounts and documents (by selecting the menu path (Customizing--> Financial Accounting Configuration Menu--> Tools--> Archiving or by executing transaction OBR7 or OBR8).

The following objects can be archived:

- Accounting documents
- Transaction figures
- Checks
- Master data from customers, vendors and G/L accounts
- Master data on banks
- The document and archive index

Commercial regulations or internal operations may require you to retrieve data stored in archive files at a later time period. One way of accessing this data is to reload it.

The following objects can be reloaded:

- Accounting documents
- Transaction figures
- Checks
- G/L account master data
- Bank master data
- The document and archive index

There is no need to reload the master data from accounts receivable and payable.

## 8.4 Risk

If posting data is not reconciled on a timely basis—that is, monthly—there is a risk that errors may occur and remain undetected for an extended period of time. These errors may make it difficult to carry out the year-end closing procedures. Another obvious consequence of this is that management could make decisions based on unreliable information, which would then lead to serious, irreversible errors.

There is also a risk that you may not be able to identify why or where an error occurred in order to prevent it from recurring and from jeopardizing the system's compliance with sound accounting principles.

In addition to the risk of error resulting from reconciliation that does not occur on a timely basis, there are other risks in month-end closing that must be eliminated using system-wide controls and checks. For example, accounting periods that are not accurately defined may result in inconsistencies between the general ledger and subsidiary ledgers. Inconsistent data could then be used in subsequent evaluations for tax purposes or sales statistics. Inadequate data backup will make it difficult to restructure information for external purposes if errors do occur.

Risks related to the balance sheet and profit and loss statement may arise due to the type of accounts summarized in the individual year-end closing items. If allocations do not match the formal requirements, the year-end closing procedure may be rejected. Incomplete data increases the risk of erroneous information being used by management.

Non-compliance with classification requirements and retention time limits may result in legal consequences.

Improper handling of the balance carried forward may cause losses in the continuity of the balance sheet or may result in balance sheet manipulation.

Changes to the document number ranges may affect the archive in such a way that prevents objects from being reloaded into the system.

## 8.5 Audits

### 8.5.1 Reconciliation

Based on control and monitoring requirements, the following questions (among others) arise for the auditor:

How often are postings checked? Who checks them?

Is accounting reconciliation performed regularly?

Were any inconsistencies found? How were they handled?

When upgrading to a new release, do the closing balance lists of the old release match the beginning balance lists of the new release and have they been documented properly?

Is there any record of abnormal system termination?

*If other SAP modules are used, do buffers issue document numbers (Transaction SNR0, number range object MATBELEG)?*

Check the **selection criteria** for the ABAPs used in the accounting reconciliation. SAP recommends defining fixed selection criteria in variants for each client for the following reports:

- RFBELJ00
- RFDSL000
- RFKSLD00
- RFSSLD00

Within Financial Accounts, the reconciliation reports for the General Ledger area can be found in the path „Periodic processing--> Month end reports--> Reconciliation“ or in the Accounts Receivable or Payable areas in the path „Periodic processing--> Reporting--> Account balances.“

To run these reports, specify a standard CPU data as the selection criterion for the time period.

## 8.5.2 Periodic closing

The following questions are essential to assessing the system controls and checks:

Who is responsible for the month-end closing procedure?

Do the rules for executing the closing procedure satisfy the requirement of separating the functions between the functional department and the DP area?

What measures guarantee that standard process flows will be carried out in the proper order?

Are there any rules governing error management?

Are user profiles properly set up for separating functions (**transaction SU02**)?

Are all documents that must be archived being generated?

## 8.5.3 Year-end closing

In addition to questions in the auditing steps for month-end closing, the auditor must deal with problems related to year-end closing, which include presenting the balance sheet, documenting posting data and retaining documents subject to retention requirements.

Responsibility for year-end closing, for period-end accrual and deferral and for defining the G/L accounts must be obtained from the assigned user profiles (Tools--> Administration--> User maintenance).

Check the procedure for executing the balance carried forward, as well as the balances that have been carried forward.

Also check whether changes made to the document number ranges during the year will affect the archive (transaction FBN1).

## **9 Invoice Checking and Payment Run**

### **9.1 Objective**

This chapter discusses the invoice checking and payment run in relation to the Financial Accounting module. The requirements for vendor master data administration that are most important for that area are also covered. To guarantee compliance with sound accounting principles, reference is made to the master data change service described in Chapter 7.

This chapter does not cover logistic invoice checking in connection with SAP R/3 MM Material Management, which performs computerized checks by having the system compare orders, goods received, and invoicing.

Upstream and downstream organizational monitoring and appropriate functional separation in the areas of vendor master data administration, invoice checking and payment runs are required to guarantee that processes will flow smoothly and ensure that the internal control system is effective. The scope of the upstream and downstream monitoring depends on the size of the individual company and the complexity of business transaction processing. SAP grants authorizations based on a company-specific authorization model, and can provide effective support in that regard on several different levels.

## 9.2 Requirements

Correct processing and handling of transaction data as part of company functions (such as invoice checking and offsetting payments) depend on complete, consistent, and up-to-date vendor master data. When using the Material Management module, it is particularly important to avoid inconsistency and redundancy by clearly dividing each department's responsibility for creating and maintaining master data between Accounting and Purchasing.

Staff who have access to master data should not be able to access transaction data. Master data fields that are used for payment (such as information on bank affiliations) should be subject to the dual control principle or be monitored by additional compensatory checks. In this regard, the number of suspense accounts should be kept to a minimum and monitored separately.

Compliance with sound accounting principles requires complete, correct documentation of accounts payable and receivable. Therefore, incoming invoices must be promptly recorded. They must be checked to ensure that they match the order and the goods or services received. Only invoices that reflect the proper quantity of goods and services that were actually received under the stipulated conditions should be paid. Tolerances for differences are allowed and can be configured by the system.

SAP R/3 has the capability of prerecording documents (replaces the register of invoices received), if the invoices cannot be promptly posted because they have not yet been checked.

Payment should be made in a timely fashion and should meet any deadlines required for discounts. The outflow of funds is also subject to dual control, either by monitoring payment proposal lists or by an appropriate internal control system for master data administration and invoice release. The forwarding of transfer order datasets to banks should be documented and protected against manipulation.

## 9.3 SAP facts

### 9.3.1 Vendor master data

To ensure that invoices are posted in accordance with sound accounting principles, appropriate information is provided from the master file (name, address, bank affiliation, terms of payment, payment routes, and account control data).

For one-time vendors or those who invoice infrequently, the system has a master record for suspense accounts. It contains no customer-specific data, since the account is used for multiple vendors. The specific data must be entered when the invoice is posted.

### 9.3.2 Special fields

The following fields in the vendor master records have a special function:

- **Different payment recipient**

The payment program can make payments to a payee who is different from the vendor to whose account the invoice was posted. The payment is made to a different recipient. That recipient must be entered in the general or specific company code area of the master record. If there are entries in both areas, the entry in the company code has priority. The payment program will then call up the name and address of the different payment recipient when processing payments for the applicable vendor account.

It is also possible to enter the payment recipient for the first time in the document (requires marking of the payment recipient field in the document). When the document is recorded, a field will then be available for entry of a different payment recipient.

- **Affiliated companies**

Invoices submitted to an affiliated company require special treatment in a group consolidation. All sales and purchases resulting from transactions within a company group must be eliminated (elimination of internal transactions). This requires every affiliated company to have a uniform number in the Partner Company field that is consistent throughout the group. That number is then entered in the Partner Company field in the vendor master record. The consolidation system uses it to recognize internal transactions for consolidation.

- **Offsets between vendors and customers**

If a business partner is both a vendor and a customer, open items can be offset by the payment program and the dunning program.

However, offsetting is possible only if:

1. A customer master record has been created for a customer who is simultaneously recorded as a vendor.
2. The customer's account number has been entered in the customer field in the control area of the general data in the vendor master record, and the vendor's account number has similarly been entered in the vendor field of the customer master record.
3. The Offset with Customer or Offset with Vendor field has been marked in the company code data of the customer and vendor master record. Each company code can then separately decide whether it is advisable to offset the amounts for the customer and the vendor.

### 9.3.3 Prerecording documents

Prerecording documents allows invoices to be prerecorded and parked without the need to check entries in detail. A prerecorded document can be changed and completed in a series of steps. Many head and position fields can be changed. The system rules for changes to document recording are not used. Changes to prerecorded documents are logged and can be displayed before and after posting.

The document number of a prerecorded document that has been deleted cannot be reused.

A prerecorded document can be posted individually or by selecting from a list. The system generates a list that shows whether the documents were successfully posted. Documents that have not been posted can be revised from that list.

When a prerecorded document is posted, the data from that prerecorded document is deleted, a document is written to the document database and the corresponding data (transaction figures) is updated. The document number is imported into the posted document.

### 9.3.4 Posting accounts using the net amount procedure

In some cases, the net amount of vendor invoices must be posted; that is the case, for example, when acquiring fixed assets or raw materials. When using the net amount procedure to post an invoice, it is assumed that the discount was withheld. The invoice is not yet paid, and the system automatically subtracts the discount from the expenditure. This method is typically used to record the acquisition of property, plant, and equipment. The amount reduced by the discount (net amount) is then transferred to expense or balance sheet accounts.

A "net document type" must be used when invoices are posted using the net amount procedure. The accounts, rules, and posting keys must be set in the system configuration to automatic posting of the discount difference.

### 9.3.5 Amount limits and tolerances

In addition to assigning posting authorizations, amounts can be limited when posting documents and document line items and tolerance limits can be set for discounts and payment differences. Such specifications may also be the subject of agreements with business partners. Both specifications apply during posting. The more restrictive limits will apply.

Examples of amount limits for posting:

What is the maximum amount for a document that an employee can post?

What is the maximum amount of a document line item that he can record in a customer or vendor account?

What percentage discount can the employee grant in a document line item?

What is the maximum acceptable payment difference?

The specified tolerances and amounts are a function of the company code. This means that it is possible to specify different tolerances for specific company codes to the same group of employees. If no group is indicated, the defined tolerances apply to all employees who are not assigned to a group.

Examples of tolerances for payment differences:

Payment differences within specified tolerance limits are automatically posted. When that occurs, the system can post the difference by correcting the discount or by booking a separate expense or income account.

Tolerance limits are used to determine how the system should post the difference. For example, up to what amount or percentage does the system automatically post to a separate expense or income account, if it is not possible to correct the discount?

/words omitted in original/ difference does the system correct the discount? In that case, the difference is automatically added to or deducted from the discount.

### 9.3.6 Payment programs

The payment program is designed to handle both outgoing and incoming payments. Both functions are supported for vendors and customers. The program generates payment documents and provides the data for the payer program. It prints payment lists and payment forms (such as checks) or generates data carriers (diskettes or magnetic tapes).

The payment program determines the open line items and decides which line items must be paid. It always pays each item as late as possible without losing the discount. The exact time of payment is determined by the configuration of the payment program.

The base date and the terms of payment contained in the open line item determine when the entry is due for payment.

The payment program calculates discount deadlines and when net payment is due.

During configuration, tolerance days can be specified for the accounts payable of specific company codes. The tolerance days are added to the calculated payment deadlines. Payment can then be postponed.

A minimum discount percentage for outgoing payments can be specified for a specific company code. If the specified minimum percentage cannot be obtained, payment is made when the net amount is due. The minimum account percentage is used if the terms for net payment are more advantageous than the terms of a potential discount. If a minimum amount is not indicated, then the program pays when the highest possible discount is available.

In addition, special main ledger procedures, such as installment payment requests or payment requests, can be specified during configuration as procedures to be regulated.

The date of the next payment run must be indicated before each payment run. The program uses that information to decide whether a line item should be included in the current or next payment run.

When payment parameters are recorded, the authorization to change payment parameters can be limited to certain users.

### 9.3.7 Authorizations

The following authorizations are relevant for audits:

#### Customer and vendor master data

Authorizations for vendor master data can be assigned with regard to the application (Financial Accounting or Purchasing), the company code organizational unit, the individual master records and the individual master record fields. The authorized activities are contained in Table TACTZ.

Authorization objects in detail:

General maintenance authorization for customer or vendor master data (application authorization)

Customer master data:	F_KNA1_APP
Vendor master data:	F_LFA1_APP

Authorization object for customer or vendor master data in the company code

Customer master data:	F_KNA1_BUK
Vendor master data:	F_LFA1_BUK

Authorization object for customer or vendor master data as a function of master record (account authorization)

Customer master data:	F_KNA1_BED
Vendor master data:	F_LFA1_BEK

Authorization object to change specific fields

Customer master data:	F_KNA1_AEN
Vendor master data:	F_LFA1_AEN

Authorization object to change specific account groups (applies only to customers):

F\_KNA1\_KGD

Authorization object for account analysis (applies only to customers):

F\_KNB1\_ANA

An analysis function is available for customer accounts that provides an overview of the total amount of open line items, deductions and interest, the credit limit and the payment history. This function has its own authorization object: Authorization for account analysis. The authorization object is comprised only of the company code field.

---

**Banks**

An authorization object was defined for banks which can be used to protect the creation and processing of bank master data. A second authorization object is used to specify the company codes in which house banks can be defined and processed.

The individual authorization objects for the banks are:

Authorization object for bank master data (general maintenance authorization):  
F\_BNKA\_MAN

Authorization object for house banks (authorization for company codes):  
F\_BNKA\_BUK

**Financial calendar**

The financial calendar provides an overview of the periodic work planned in the system, such as dunning runs, payment runs and reports. All of the jobs that should be displayed simultaneously are combined in the schedule. The authorization object F\_T001E ("authorization for financial calendar) assigns authorizations to make changes and to display.

**Accounting document**

Authorization objects are defined for the accounting document which can be used to limit posting, displaying, and similar functions to company codes, business areas, document types, account types, or accounts.

Authorization object for company codes: F\_BKPF\_BUK

The object is also used to define the general authorization. An employee can call up the function for posting if he is authorized to post documents in one at least one company code.

Authorization object for business areas: F\_BKPF\_GES

Authorizations with the following objects can be assigned for posting and editing documents related to accounts and business transactions:

Authorizations for posting periods: F\_BKPF\_BUP  
Authorizations for account types: F\_BKPF\_KOA  
Authorizations for document types: F\_BKPF\_BLA

Authorization object account authorization for G/L, vendor, and customer accounts:

G/L accounts: F\_BKPF\_SAK  
Vendors: F\_BLPF\_BEK  
Customers: F\_BKPF\_BED

Authorization object change proposed values for document type and posting key:  
F\_BKPF\_VW

The system is supplied with proposed values for the document type and posting key. These values are suggested to the user when a function is called up. Change authorizations can be assigned so that the proposed values can be changed using the configuration guide for Accounting.

**Credit limit**

The credit limit to be granted to a vendor or customer can generally be established for a general customer or for an isolated customer based on credit control areas. The credit control area is an organizational unit that issues and controls credit limits. A control area can be responsible for one or several company codes.

Three authorization objects have been defined for credit limits: The first authorization object restricts the general maintenance authorization and the second restricts credit limit maintenance and display to the credit control area. The third authorization object can be used to protect specific fields on credit management in customer master data against changes.

In detail, the authorization objects for the credit limit are:

General maintenance authorization:	F_KNKA_MAN
Authorization for credit monitoring areas:	F_KNKA_MAN
Change authorization for specific fields:	F_KNKA_AEN

**Payment run**

To define authorizations, the system contains special activity keys that apply only to the payment program. They can be called up using the Environment menu item in the Request screen of the payment program.

To define the authorizations, enter the desired activities using the keys. To define the authorizations, you can combine the activities with company codes or account types.

The following authorizations can be assigned for the payment run:

Authorization object for the company code:	F_REGU_BUK
Authorization object for the account type:	F_REGU_KOA

**Dunning run**

The following authorizations can be assigned for the dunning run:

Authorization object for the company code:	F_MAHN_BUK
Authorization object for the account type:	F_MAHN_KOA

---

### 9.3.8 Reports

RFAUSZ00	Generate account statement
RFAVIS20	Reorganization of payment notices
RFBISA00	Import G/L data from a source system into the R/3 system
RFCHKR10	Correction if the wrong check number was entered when writing checks
RFDABL00	Changes in customer data masters for multiple accounts
RFDKLI10	Search for customers without credit limits
RFDKLI20	Restructure credit limits of selected credit monitoring areas
RFDKLI30	Brief overview of credit limit
RFDKLI40	Overview of credit limit (expanded)
RFDKLI41	Credit master sheet
RFDKLI50	Change in assets
RFDKLIAB	Display changes in credit management for multiple accounts
RFDKLIAB	Display changes for multiple accounts
RFEBCK00	Enter check reverse run
RFKABL00	List changes in vendor master records for multiple accounts
RFKORD00	Print payment notices directly with the print report
RFKORD10	Print account statement and open line items list
RFPKDB00	Evaluate liabilities from previously recorded documents and where applicable post as lump sum
RFSABL00	List changes in G/L account master records for multiple accounts
RFWEDI00	Submission list for the bank
RFZALI00	Reports on generation of the payment proposal list and /words omitted/
RFZALI10	Reports on generation of exception list
SAPF019	/word omitted/ master data in chart of accounts
SAPF140	Print all requested types of correspondence that has not yet been printed

### RCCLCUST

For Release 3.0D the report must be started so that the data in customizing of the class system, which SAP changed for this release, will also be imported in your system. This report transports new or changed table entries made by SAP in Client 000 into all clients of your productive system.

## **9.4 Risks**

If payment transactions are not sufficiently protected by system validations and automatic checks/reconciliations, and if effective manual checks are not performed by the organization both upstream and downstream, working errors and/or deliberate actions may cause economic losses for the company.

### **9.4.1 Vendor master records**

Incomplete or faulty maintenance of vendor master records can result in the need for extensive corrective efforts. Traceability will be more difficult or impossible (see Chapter 7). A failure to separate functions between access to (create and maintain) master data and transaction data increases the risk of manipulations to vendor master data (e.g., bank affiliation).

The use of suspense accounts for payment transactions also involves additional risks due to the open input capability for the payment route and payment recipient and the lack of clarity about evaluation capabilities (such as supplier statistics).

### **9.4.2 Invoice checking**

Without internal company rules on invoice checking (dual control principle, functional separation, release procedure) there is a risk of double payments (such as posting and payment of copies of invoices or payment reminders) and manipulations (such as invoices for which no service was provided).

### **9.4.3 Payment proposal, payment run**

Blocked invoices do not appear on the payment proposal list. Failure to check or reconcile payment proposals and payments could allow invoices to be released inadvertently after release of the proposal lists and to be included in the payment run.

## 9.5 Audits

Use interviews, job descriptions, and flow charts to collect information about the form of procedural organization that has been chosen by the company. Then use the documentation for the authorization model designed by the company to evaluate the extent to which the company's organizational structure harmonizes with its authorization model.

### 9.5.1 Functional separation

Check authorizations to determine whether there is an appropriate functional separation between invoice checking, invoice posting, and release for payment. Questions that should be asked are: Can any employees create or maintain vendor master data and also post invoices and/or release them for payment? Can employees with system authorizations set them up themselves (see Chapter 2 for authorization to do so)?

If these functional separations are missing-i.e., if several of the jobs involved in payment transactions are combined because organizational units are smaller-questions should be asked regarding appropriate internal control measures. Useful questions include: What checks are called for by the ICS? The dual control principle should be followed when creating and maintaining vendors; when posting and releasing for payment at one work station, there should be validity checks, verifying the services described in the invoice or the amount invoiced by each vendor, for example. Later checks of payments that have been made should also be recommended, perhaps by collecting an appropriate number of random samples.

### 9.5.2 Suspense accounts

When checking internal company rules on the creation and maintenance of vendors, the handling of suspense accounts should also be examined. What instructions exist with regard to the suspense accounts? Are the suspense accounts subject to special monitoring? What are the conditions for debiting suspense accounts?

### 9.5.3 Payment proposal list and payment list

Be sure to check the procedures followed when generating and monitoring the payment proposal lists and the payment run files. Are the payment proposal lists checked before payment? If yes, do any errors or changes detected on the proposal lists correspond to the payment lists? Are there rules on how to set and reset blocked identifiers?

Is there a reconciliation of the proposed balance sheet total and the payment run total? How are payment run files saved? Is it possible to access the files and spool systems?

To monitor the payment run, the payment log should be read and the payment list should be checked before the forms are printed. (To call up the payment log, select Edit--> Payment--> Display log. To display the payment run, select Edit--> Payment--> Display payment.)

This allows you to use functions like Search and Sort to obtain a quick overview of the payments. In addition, after the payment run (Edit--> Proposal--> Display), a history of the proposed changes can be traced, showing who made what changes and when.

### 9.5.4 Double payments

Determine the extent to which double payments can occur and what measures the company has taken to avoid them. Are there instructions on how to handle copies of invoices and payment reminders? Have validation checks been included in the system? Can the same vendor be created in the master more than once?