

Arbeitskreis Revision Prüfungsleitfaden FI für SAP - R/3

Release 3.0D

Stand 20. Februar 1997

Bestell-Nr. 5001 4633 Fax-Nr. 06227/7-41497

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



SAP® AG • Neurottstr. 16 • D-69190 Walldorf

Änderungen und Ergänzungen vorbehalten

Prüfungsleitfaden FI für SAP-R/3

PRÜFUNGSLEITFADEN FI FÜR SAP-R/3	2
0. EINLEITUNG	7
1. SYSTEMÜBERSICHT	11
1.1. ZIELSETZUNG	11
1.1.1. Technische und organisatorische Übersicht über das System	11
1.1.2. Transparenz des Systems für den Prüfer und seinen Auftrag	12
1.1.3. Prüfungsfelder abgrenzen	12
1.2. ANFORDERUNGEN	13
1.3. RISIKEN	13
1.4. PRÜFUNGEN	14
1.4.1. Verantwortlichkeiten	14
1.4.2. Systeme im Einsatz (Test, ..., Produktion)	14
1.4.3. Berechtigung und Benutzermenü für den Prüfer	14
1.4.4. Aufnahme der Business-Struktur	16
1.4.5. Releasestände	16
1.4.6. Komponenten/Funktionalitäten	16
1.4.7. Modifikationen	17
1.4.8. Verbuchungsabbruch	19
1.4.9. Datenflussplan	19
1.5. VORSCHLAG FÜR BERECHTIGUNGSSATZ EINES PRÜFERS	20
1.6. GESAMTÜBERBLICK ÜBER KUNDEN-NAMENSÄUME	21
2. SICHERHEIT UND ZUGRIFFSSCHUTZ	23
2.1. ZIELSETZUNG	23
2.2. ANFORDERUNGEN	24
2.3. SAP-FAKTEN	25
2.3.1. Grundsätzliches zum Berechtigungskonzept	25
2.3.2. Berechtigungsstrukturen	27
2.3.3. Trennung von Pflege und Aktivierung	27
2.3.4. Benutzerstammsatz	27
2.3.5. Passwortschutz und Anmeldung	28
2.3.6. Kundeneigene Berechtigungsprüfungen	28
2.3.7. Vorgelagerte Sicherheitssysteme	28
2.3.8. Tabelle TSTC 'SAP-Transaktionscodes'	28
2.3.9. Customizing	29
2.4. RISIKEN	30
2.5. PRÜFUNGEN	31
2.5.1. Benutzerverwaltung	31
2.5.2. Sicherheit und Zugriffsschutz	33
2.5.3. Wichtige Einzelberechtigungen	35
3. WORKBENCH ORGANIZER UND TRANSPORTSYSTEM	39
3.1. ZIELSETZUNG	39
3.1.1. Funktionale Integrität	39
3.1.2. Nachvollziehbarkeit	39
3.2. ANFORDERUNGEN	40
3.2.1. Auftragserteilung	40
3.2.2. Durchführung der Änderung	40
3.2.3. Abnahme und Produktionsübergabe	40
3.3. SAP-FAKTEN	41
3.3.1. Zweck und Aufbau	41

3.3.2.	<i>SAP-Systeme</i>	42
3.3.3.	<i>Korrektur und Reparatur</i>	43
3.3.4.	<i>Einstellungen des WBOT</i>	44
3.3.5.	<i>Durchführung von Transporten</i>	45
3.4.	RISIKEN	46
3.4.1.	<i>Gültigkeit von EUO</i>	46
3.4.2.	<i>Fehleinstellungen des KTW</i>	46
3.4.3.	<i>Zugriff auf Betriebssystemebene</i>	46
3.4.4.	<i>Instabilität</i>	46
3.4.5.	<i>Manipulation</i>	47
3.5.	PRÜFUNGEN	48
3.5.1.	<i>Ist-Aufnahme des Verfahrens</i>	48
3.5.2.	<i>Überprüfung des Konzeptes</i>	48
3.5.3.	<i>Einhaltung des Konzeptes</i>	48
3.5.4.	<i>Konkrete Prüfungshandlungen</i>	48
4.	TABELLENZUGRIFF UND PROTOKOLLIERUNG	50
4.1.	ZIELSETZUNG	50
4.2.	ANFORDERUNGEN	51
4.2.1.	<i>Protokollierung</i>	51
4.2.2.	<i>Kundeneigene Tabellen</i>	51
4.2.3.	<i>Zugriffsschutz</i>	51
4.2.4.	<i>Arbeits-/Organisationsanweisungen</i>	52
4.2.5.	<i>Sicherstellung des Informationsflusses</i>	52
4.3.	SAP-FAKTEN	53
4.3.1.	<i>Zweck und Aufbau</i>	53
4.3.2.	<i>Tabellenzugriff und Protokollierung</i>	54
4.3.3.	<i>Gültigkeitsbereich und Kundentabellen</i>	55
4.3.4.	<i>ABAP-Reports</i>	55
4.3.5.	<i>Beispiele für wichtige Tabellen</i>	56
4.4.	RISIKEN	57
4.5.	PRÜFUNGEN	58
5.	JOB-AUFTRAGSVERFAHREN UND -DOKUMENTATION SOWIE SYSTEM- PROTOKOLLE	59
5.1.	ZIELSETZUNG	59
5.1.1.	<i>Job-Auftragsverfahren</i>	59
5.1.2.	<i>Job-Dokumentation</i>	59
5.1.3.	<i>Job-Protokolle</i>	59
5.2.	ANFORDERUNGEN	60
5.2.1.	<i>Job-Auftragsverfahren</i>	60
5.2.2.	<i>Job-Dokumentation</i>	60
5.2.3.	<i>System-Protokolle</i>	60
5.3.	SAP-FAKTEN	61
5.4.	RISIKEN	62
5.5.	PRÜFUNGEN	63
5.5.1.	<i>IST-Aufnahme der Verfahren</i>	63
5.5.2.	<i>Prüfung der Verfahrenskonzepte</i>	63
5.5.3.	<i>Prüfung der Einhaltung der Verfahren</i>	63
5.6.	SAP-JOBDOKUMENTATION (MUSTERVORSCHLAG)	64
5.6.1.	<i>Allgemeines</i>	64
5.6.2.	<i>Voraussetzungen für den Jobstart</i>	64
5.6.3.	<i>Erforderliche Nachbearbeitungen nach Joblauf</i>	64
5.6.4.	<i>Maßnahmen für den Restartfall</i>	64
6.	BATCH-INPUT-SCHNITTSTELLEN	65
6.1.	ZIELSETZUNG	65
6.2.	ANFORDERUNGEN	65

6.3. SAP-FAKTEN.....	66
6.3.1. Einführung	66
6.3.2. Berechtigungen	66
6.3.3. Bearbeitungsarten	67
6.3.4. Protokolle.....	67
6.3.5. Mappenanalyse.....	67
6.4. RISIKEN.....	68
6.5. PRÜFUNGEN.....	68
7. STAMMDATENÄNDERUNGEN	69
7.1. FUNKTIONSTRENNUNG	69
7.1.1. Zielsetzung	69
7.1.2. Anforderungen.....	69
7.1.3. SAP-Fakten	69
7.1.4. Risiken	70
7.1.5. Prüfungen.....	70
7.2. NACHVOLLZIEHBARKEIT	71
7.2.1. Zielsetzung	71
7.2.2. Anforderungen.....	71
7.2.3. SAP-Fakten	71
7.2.4. Risiken	72
7.2.5. Prüfungen.....	72
8. ABSTIMMUNG BUCHUNGSSTOFF UND ABSCHLÜSSE	73
8.1. ZIELSETZUNG	73
8.2. ANFORDERUNGEN.....	74
8.3. SAP-FAKTEN.....	75
8.3.1. Abstimmung des Buchungsstoffes.....	75
8.3.2. Periodenabschluss.....	77
8.3.2.1. Tagesabschluss	78
8.3.2.2. Monatsabschluss.....	79
8.3.2.3. Jahresabschluss	80
8.4. RISIKEN.....	83
8.5. PRÜFUNGEN.....	84
8.5.1. Abstimmung.....	84
8.5.2. Periodenabschluss.....	85
8.5.3. Jahresabschluss.....	85
9. RECHNUNGSPRÜFUNG UND ZAHLUNGSLAUF	86
9.1. ZIELSETZUNG	86
9.2. ANFORDERUNGEN.....	87
9.3. SAP-FAKTEN.....	88
9.3.1. Kreditorenstammdaten.....	88
9.3.2. Besondere Felder	88
9.3.2.1. Abweichender Zahlungsempfänger	88
9.3.2.2. Verbundene Unternehmen	88
9.3.2.3. Verrechnung zwischen Kreditor und Debitor.....	89
9.3.3. Belegvorerfassung	90
9.3.4. Rechnungen im Nettoverfahren buchen.....	90
9.3.5. Betragsgrenzen und Toleranzen.....	91
9.3.6. Zahlungsprogramm.....	92
9.3.7. Berechtigungen	93
9.3.7.1. Debitoren- und Kreditorenstammdaten.....	93
9.3.7.2. Banken	93
9.3.7.3. Finanzkalender	94
9.3.7.4. Buchhaltungsbeleg.....	94
9.3.7.5. Kreditlimit	95
9.3.7.6. Zahllauf.....	95

9.3.7.7. Mahnlauf.....	95
9.3.8. Reports.....	96
9.4. RISIKEN.....	98
9.4.1. Kreditorenstammsätze	98
9.4.2. Rechnungsprüfung.....	98
9.4.3. Zahlungsvorschlag, Zahlungslauf.....	98
9.5. PRÜFUNGEN.....	99
9.5.1. Funktionstrennung.....	99
9.5.2. CpD-Konten	99
9.5.3. Zahlungsvorschlagsliste und Zahlungsliste	99
9.5.4. Doppelzahlungen.....	100

Zusammenfassung der Änderungen und Nachträge

Erste Auflage: Release 2.2D 29.03.1996

Zweite Auflage: Release 3.0D 20.02.1997

0 Einleitung

Der vorliegende Prüfleitfaden FI zum **Releasestand 3.0** im SAP-Systemumfeld **R/3** soll Wirtschaftsprüfern, EDV-Revisoren und Mitarbeitern der Internen Revisionsabteilungen der SAP-Anwender Anhaltspunkte für die Vorgehensweise bei Prüfungen von SAP-Software geben. Er gilt im wesentlichen für die Basis und wichtige Aspekte der Applikation FI.

Der Leitfaden ist als "Empfehlung" gedacht, nicht aber als "Verbindliche Richtlinie" oder "Norm". Jegliche Verantwortung für Art, Umfang und Ergebnis externer und interner Prüfungen verbleibt somit beim Prüfer selbst.

Für das Studium dieses Leitfadens werden Grundkenntnisse der SAP-Systeme sowie Kenntnisse der GoB "Grundsätze ordnungsmäßiger Buchführung" vorausgesetzt.

Die Autoren sind Mitglieder einer Arbeitsgruppe des SAP-Arbeitskreises REVISION und stellen hiermit ihre Erfahrungen zur Verfügung.
Copyright 1997 der Autoren:

Herr Barthel	FORBIT e.V., Hamburg
Herr Bernd-Striebeck	KPMG Deutsche Treuhand-Gesellschaft AG, Düsseldorf
Herr Göttmann	Philip Morris GmbH, München
Herr Grotebrune	Unilever Corporate Audit, Hamburg
Herr Hungerbühler	ATAG Ernst & Young, St.Gallen
Herr Jackisch	Price Waterhouse Wirtschaftsprüfungsgesellschaft GmbH, Düsseldorf
Herr Dr. Koch	Osnabrück/Melle
Herr Lencses	SCHITAG Ernst & Young Deutsche Allgemeine Treuhand AG, Stuttgart
Herr Dr. Peemöller	ORIGIN Information Technology GmbH, Hamburg
Frau 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.

Die Verantwortung für den Inhalt tragen die Autoren. Die redaktionelle Bearbeitung lag bei Herrn Schiwek, SAP AG, Walldorf.

Hinweis: Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechts ist ohne Zustimmung der Urheber unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Vertiefende Erläuterungen sind der SAP-Online-Dokumentation zu entnehmen.

Die Autoren des **Prüfungsleitfaden FI** sind für Kritik, Änderungs- und Ergänzungswünsche dankbar. Dies gilt sowohl für Vorschläge zur Vertiefung der einzelnen Kapitel als auch für die Nennung von Beispielen aus konkreten Prüfungserfahrungen.

Um dem Leser die Antwort zu erleichtern, ist auf der folgenden Seite ein Formular eingefügt.

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

Zur weiteren Erläuterung sind Anlagen beigefügt (bitte ankreuzen):

- Ja Nein

1 Systemübersicht

Dieses erste Kapitel des Leitfadens für SAP-Prüfungen unterstützt die schnelle Erstellung einer Übersicht über das System und seine systemtechnische und organisatorische Einbindung. Diese Übersicht braucht der Prüfer zur eigenen Orientierung am System, zur Beurteilung des allgemeinen Systemzustandes und zur Bestimmung der erforderlichen Prüfungshandlungen.

Zur Erstellung einer Systemübersicht können Sie sich ein **eigenes Benutzermenü** einrichten. Nähere Einzelheiten entnehmen Sie bitte dem **Kapitel 1.4.3**.

1.1. Zielsetzung

Die oben genannten Ziele beinhalten im einzelnen:

1.1.1. Technische und organisatorische Übersicht über das System

Der Umfang des **t e c h n i s c h e n** Systems und dessen ständige Veränderungen erlauben eine Gesamtsicht des R/3 Systems nur denjenigen, die sich ausschließlich mit der Software befassen. Dies gilt im allgemeinen nicht für den Prüfer, der nicht selten von außen kommend mit einigen ersten Schritten am System feststellen muß, welche technische Funktionalität bei einem bestimmten Anwender genutzt wird. Diese technische Übersicht sollte insgesamt in kürzestmöglicher Zeit und ohne aufwendige technische Zusatzleistungen erstellt werden. Wünschenswert wäre, wenn das System gewissermaßen "auf Knopfdruck" alle wichtigen Aussagen über sich selbst, seinen Systemzustand und ggf. dessen Veränderungen seit einem bestimmten Zeitpunkt trifft. Zu den unter Revisionsgesichtspunkten wichtigen Aspekten des Systemzustandes zählen:

- Transaktionen,
- ABAP Programme,
- Tabellen,
- Dateien,
- Berechtigungen, Berechtigungsprofile und Benutzerstammsätze,
- Datenträger und
- andere Sicherungsmaßnahmen (z.B. Tabellenklassen, Trennung verschiedener Mandanten).

Die **o r g a n i s a t o r i s c h e** Einbettung des SAP R/3 Systems und deren Veränderungen bestimmen die Wirksamkeit der technischen Maßnahmen zur Gewährleistung der ordnungsgemäßen Datenverarbeitung. In Bezug auf den organisatorischen Systemzustand ist das Vorhandensein einer aussagekräftigen Dokumentation zu überprüfen. Die Übersicht ist durch Stichproben bei den Anwendern (z.B. hinsichtlich der Handhabung von Benutzerberechtigungen), bei der Systemdokumentation (z.B. hinsichtlich der Programm- und Tabellendokumentation) und in der Systemumgebung (z.B. beim allgemeinen Umgang mit dem System bei Systemabbrüchen) zu ergänzen.

1.1.2. **Transparenz des Systems für den Prüfer und seinen Auftrag**

Neben dem allgemeinen Ziel der Übersichtlichkeit beinhaltet das Ziel der Transparenz für den Prüfer im speziellen, die subjektiv mögliche und objektiv vorhandene, in angemessener Zeit herstellbare Durchschaubarkeit des Gesamtsystems als Voraussetzung für eine kompetente und sachlich einwandfreie Beurteilung des Systemgeschehens zu erreichen.

1.1.3. **Prüfungsfelder abgrenzen**

Die Systemübersicht soll schließlich dem Prüfer ermöglichen, seinen Prüfungsauftrag auf abgrenzbare Prüfungsfelder zu beziehen. Nach der Erarbeitung der Übersicht muß für alle Betroffenen der sachliche Rahmen der Prüfung abgrenzbar sein. Es sollte darüber hinaus möglich werden, den funktionalen und den zeitlichen Rahmen der Prüfung zu beschreiben.

1.2. Anforderungen

Die zu untersuchende Systeminstallation muß den Anforderungen der Prüfbarkeit entsprechen. Dies setzt voraus, daß im allgemeinen die Anforderungen an die Prüfbarkeit im Sinne der Finanzbehörden erfüllt werden. Insbesondere haben die Anwendung des Systems und alle Modifikationen am System im Rahmen der Empfehlungen von SAP (z.B. im R/3-Dokumentationshandbuch BC-SAP Style Guide das Kapitel 'Namensräume und Namenskonventionen') zu erfolgen.

Dies betrifft vor allem die

- Verfahren der Änderung und Anpassung der Standardsoftware;
- Dokumentation von Veränderungen am System und seiner Umgebung;
- Einhaltung von Namenskonventionen bei der Veränderung von Transaktionen, ABAPs, Tabellen, Dateien und anderen SAP-Objekten (siehe Überblick unter Abschnitt 1.6).

Der **Mandant 000** darf **nur** von der von SAP ausgelieferten Software benutzt werden, denn er dient als Referenz für die übrigen Mandanten und wird beim nächsten Release- oder Putlevelwechsel teilweise überschrieben. Im Mandanten 000 verbleiben einige von SAP ausgelieferte Schlüsselinformationen, die allein vom Systemverwalter (ggf. unter Hinzuziehung von SAP-Spezialisten) gepflegt werden dürfen. Im übrigen darf im Mandanten 000 **nicht** gearbeitet werden!

Der Mandant 000 ist neben dem produktiven System als Prüfungsobjekt heranzuziehen!

Hinweis: zum Umfang der Rechte des Systemverwalters siehe Kapitel 2.5.3.

1.3. Risiken

Für die Prüfung von SAP-Geschäftsvorfällen werden im wesentlichen folgende Risiken gesehen:

- mangelnde Ordnungsmäßigkeit
- Dateninkonsistenz
- Fehlbedienung
- Unbeherrschbarkeit
- fehlende Zuverlässigkeit.

1.4. Prüfungen

1.4.1. Verantwortlichkeiten

Es ist ein Überblick über die Gesamtverantwortung für das System und über die Verantwortlichkeiten hinsichtlich der

- entscheidenden Daten und Tabellen,
- Berechtigungen,
- Programme und
- Schnittstellen

sowie deren Veränderung zu erheben, der in der laufenden Prüfung vertieft wird.

1.4.2. Systeme im Einsatz (Test,....,Produktion)

Mit der Transaktion SE06 'Einrichten System für Korrektur- und Transportwesen' ist festzustellen, welche Systeme im Einsatz sind und welche davon zu Produktions-, Entwicklungs- bzw. Testzwecken oder zur Abnahme bzw. zu Schulungszwecken genutzt werden.

Im Produktivsystem - auf dessen Prüfung sich die weitere Darstellung konzentriert - ist an Hand der **Tabelle T000 im Mandanten 000** zu überprüfen, welche Mandanten in dieser Installation aktiv sind.

Dabei sollte zunächst geklärt werden, welches System in welchem Mandanten den oder die

- Produktionsmandanten
- Testmandanten

enthält.

Hinsichtlich der Verbindung zu anderen Systemen (z.B. SAP-R/2) vergl. die Kapitel 3 'Korrektur- und Transportwesen' und 6 'Batch-Input-Schnittstellen'.

1.4.3. Berechtigung und Benutzermenü für den Prüfer

Dem Prüfer soll der direkte Systemzugang mit den in Abschnitt 1.5 aufgeführten Berechtigungen zur Verfügung gestellt werden. Hierbei sind beim Zugriff auf personenbezogene Daten unbedingt die Vorschriften des Datenschutzes und ggf. bestehende tarifliche oder betriebliche Vereinbarungen zu beachten.

Die Beschränkung der Berechtigungen auf die reine Anzeige soll dabei sicherstellen, daß der Prüfer keine Veränderungen an den Daten vornehmen darf bzw. kann.

Benutzermenü:

Zur Erstellung einer Systemübersicht richten Sie sich ein eigenes **Benutzermenü** ein. Hierzu gehen Sie folgendermaßen vor:

1. Starten Sie die Menüpflege. Wählen Sie dazu System -->> Benutzervorgaben -->> Benutzermenü pflegen.

2. Das System zeigt ein Dialogfenster an, in das Sie den Namen Ihres ersten (oder einzigen) Arbeitsbereichs eingeben (z.B. Anzeige des Systemzustands). Sie können anschließend weitere Arbeitsbereiche anlegen (z.B. Änderungen des Systemzustands, Einstellungen im Customizing etc.).

Es erscheint das Pflegebild für das Benutzermenü. Wählen Sie Neue Einträge, um sich eine Liste mit den Menüleistentexten der SAP-Standardmenüs anzeigen zu lassen. Diese Texte entsprechen den Menünamen, die Sie sehen, wenn Sie sich am R/3-Standardsystem anmelden. Schalten Sie außerdem die Anzeige der zugehörigen Transaktionsbezeichnungen durch Drücken der Drucktaste 'Neue Eintr. ü. TCode' in der Symbolleiste hinzu. Wählen Sie nun nacheinander die einzelnen Transaktionscodes aus (vergl. Kapitel 1.4.7).

3. Wenn Sie weitere Anwendungen in Ihren Arbeitsbereich aufnehmen möchten, wiederholen Sie den Schritt 2. In der Liste der Standardmenüs navigieren Sie nach unten über Doppelklick auf einen Menünamen und nach oben über Zurück.

4. Um Ihren Arbeitsbereich mit seinen Anwendungen zu sichern, verfahren Sie wie folgt:

- Wenn Sie die gewünschten Anwendungen ausgewählt haben, wählen Sie so oft Zurück, bis die Liste der ausgewählten Anwendungen Ihres Arbeitsbereichs wieder erscheint. Sie können die Texte in dieser Liste ändern.

- Sichern Sie das Menü mit F11=Sichern (oder wählen Sie das entsprechende Symbol).

Nach dem Schließen steht Ihnen dann das Benutzermenü in einem separaten Fenster zur Verfügung. Bei Änderungswünschen zu Ihrem Menü verfahren Sie entsprechend.

An Stelle des Benutzermenüs wird ab Release 3.0 D zunächst nur für Windows 95, später auch für andere Clients der sogenannte Session Manager eingerichtet. Näheres zur benutzereigenen Menügestaltung im Session Manager entnehmen Sie bitte Ihrer Dokumentation.

1.4.4. Aufnahme der Business-Struktur

Im ersten Schritt ist innerhalb jedes Produktionsmandanten (siehe Tabelle T000) die im SAP-System realisierte Aufbaustruktur zu erfassen und zu analysieren. SAP stellt zur Abbildung der Aufbaustruktur die hierarchische Gliederung der Daten- und Zugriffsstrukturen in

- Mandant
- Buchungskreis
- Geschäftsbereich
- Werk und
- Lagerort

dem Anwender zur Verfügung.

Die Buchungskreise eines Mandanten zeigt **Tabelle T001**.

Weitere Verknüpfungen sind in den Tabellen T001B (Buchungsperioden), TGSB (Geschäftsbereiche) und T001W (Werke) hinterlegt.

1.4.5. Releasestände

Dieser Prüfungsleitfaden bezieht sich auf den **Releasestand 3.0D**. Den Releasestand der zu prüfenden Anwendung ergibt ein Aufruf des System Status im Menü 'System'. Releasebezogene Änderungen bzw. Erweiterungen sind über den Menüpfad Werkzeuge --> Suchen --> Infosystem --> Release Infos einsehbar.

1.4.6. Komponenten/Funktionalitäten

Die unter 1.4.5 erfragten aktiven Hauptfunktionen des Systems verweisen auf bestimmte von SAP ausgelieferte Funktionalitäten des Systems, nämlich:

- ABAP/4 Programme, SE38,
- Menüs, SE41,
- Dynpros, SE51, SE52
- Tabellen, Customizing Transaktionen O*, SM31, ABAPs,
- Data Dictionary Objekte DI* Transaktionen.

Die links stehenden Funktionalitäten können mit den danebenstehenden Funktionen erweitert und modifiziert werden.

Der Zusammenhang zwischen den von einem Anwender aktivierten Hauptfunktionen und der von SAP dazu gelieferten Funktionalität lässt sich am anschaulichsten mit dem Business Navigator in der Komponentensicht nachvollziehen (Transaktion SB01, bzw. Werkzeuge --> Business Navigator --> Komponentensicht; zu den angezeigten Funktionen gehörende Transaktionsbezeichnungen lassen sich in den Graphiken jeweils über das Menue Einstellungen --> Attributpositionen links oben oder rechts unten dazuschalten).

1.4.7. Modifikationen

Modifikationen des Anwenders sollten - gemäß den SAP-Empfehlungen - nur im Rahmen der Namenskonventionen erfolgen. Eine Auflistung der für Kunden reservierten Namensräume finden Sie unter Abschnitt 1.6. Der Prüfer sollte zunächst diese untersuchen, indem er sich alle

- Transaktionen, die mit Z oder Y beginnen, aus der Tabelle TSTCT,
- ABAPs, die mit Y oder Z beginnen,
- Tabellen, die mit T9, P9, Y oder Z beginnen,

anzeigen lässt. In einem zweiten Schritt sind die Transaktionen, Reports und Tabellen im System und in den Akten bzw. Online-Hilfen auf deren Funktion und ordnungsgemäße Dokumentation zu überprüfen.

Der Prüfer sollte Stichproben bei weiteren Funktionen durchführen, die dem äußeren Anschein nach nicht verändert worden sind. Dies kann dadurch geschehen, daß systematisch untersucht wird, welcher Änderer (außer SAP) zu welchem Datum welche letzte Änderung vorgenommen hat. Einzelheiten sind der folgenden Aufstellung zu entnehmen:

System-Doku	System-Zustand	Änderungen
Tabellen	SE16 und DI02 (in DI02 über das Menue Bearbeiten>> Tabellentyp wählen ggf. Pool-, Cluster- und View-Tabellen dazuschalten)	SE01, SE03 Transport- infosystem DI02, bzw. RSTBPROT, RSPARAM rec/client = All oder gleich xxx, wobei xxx für den zu untersuchenden Mandanten steht; Datum und letzter Änderer in Tabellen-Info
Tabellenfelder	SE12	SE01, SE03 Transport- infosystem Dokustand= USR im Auswahlbild
ABAP's	SA38, SE38, TADIR,	SE01, SE03 Transport- infosystem in SE38 Attribute zeigen 'erstellt durch'(nur noch SAP)
Programmfelder	SE12	SE01, SE03 Transport- infosystem Dokustand=USR im Auswahlbild von DIxy
Transaktionen	TSTCT, TADIR	SE01, SE03 Transport- infosystem allgemein: Datum u. Änderer der letzten TSTCT-Änderung im Mandanten 000
Dynpros	SE51, SE52, SE41, SE42	SE01, SE03 Transport- infosystem Datum/Zeit d.Dynpro- sicherung/Generierung u.Änderer in SM51
Dynprofelder	SE12	SE01, SE03 Transport- infosystem Dokustand=USR im Auswahlbild
Berechtigungen	SU01 (Benutzer) SU02 (Profile) SU03 (Berechtigungen) RSUSR002	Infos>>Änderungsbelege, Infos>>Änderungsbelege, Infos>>Änderungsbelege,

System-Doku	System-Zustand	Änderungen
Preislisten- komponenten	TADIR, TRDIR, SB01	SE01, SE03 Transport- infosystem
Aufbau- organisation	Systeme im Einsatz TSYST Mandanten T000 Buchungskreise T001 Buchungsperioden T001B Geschäftsbereiche TGSB Werke T001W	Datum u.letzter Änderer im Tabellenprotokoll mit RSTBPROT und RSTBSERV
Datenbanktabellen	DI02	SE01, SE03 Transport- infosystem
Datenbank- tabellenfelder	DI02	SE01, SE03 Transport- infosystem

1.4.8. Verbuchungsabbruch

Bei einem Verbuchungsabbruch werden die bereits durchgeführten Datenbankveränderungen für diesen Verbuchungsauftrag zurückgenommen.

Der Protokollsatz erhält das Kennzeichen 'err' und wird nicht gelöscht.

Der Benutzer wird über R/3-Mail über den Verbuchungsabbruch informiert. Der Abbruch selbst wird in der SYSLOG festgehalten.

Jeder Benutzer kann seine Verbuchungssätze uneingeschränkt analysieren und nachbearbeiten, für die Bearbeitung fremder Verbuchungssätze ist die Berechtigung S_ADMI_FCD in der Basis-Administration erforderlich.

Der Report RFVBER00 liefert eine (Tages-)Liste über abgebrochene Verbuchungen.

1.4.9. Datenflussplan

Die eingehenden Daten aus Fremdsystemen sind hinsichtlich der Form (als Datensatzbeschreibung), ihres Inhaltes, ihrer Herkunft und der Menge zu erheben.

Die aus dem SAP-System abfließenden Daten sind ebenfalls hinsichtlich ihrer Form (d.h. als Datensatzbeschreibung und hinsichtlich des Dateiformates), ihres Inhaltes, ihrer Herkunft und der Menge zu erfragen und aufzuzeichnen.

Die Angaben sind stichprobenartig im Hinblick auf die Vergabe der Berechtigungen zum Abspielen von Batch Input-Mappen und auf ggf. vorhandene Download-Möglichkeiten zu überprüfen.

1.5. Vorschlag für Berechtigungssatz eines Prüfers

Ein Berechtigungssatz für Prüfer sollte auf die reine Anzeigefunktion für alle Applikationen und Basisfunktionen beschränkt sein. Neben der Anzeige der aktiven Daten soll auch die Anzeige der Änderungsbelege möglich sein.

SAP liefert Standardprofile mit reinen Anzeigeberechtigungen aus.

- **F_ANZ** für den Finanzbereich,
- **A_ANZ** für den Anlagenbereich,
- **M_ANZ** für den Materialbereich
- **S_A.SHOW** für Basisfunktionen, etc. (zuzüglich Aktivität 08 !)

Dies ist die weitestgehende Empfehlung; zu beachten sind aber insbesondere die Bestimmungen des Bundesdatenschutzgesetzes (BDSG) und sonstige betriebliche/tarifvertragliche Vereinbarungen.

1.6. Gesamtüberblick über Kunden-Namensräume

OBJEKT:	NAMENSLÄNGE:	KUNDENRESERVEN:
Änderungsbelegobjekt	10	Y..., Z...
Berechtigung/-sprofil	12	kein Unterstrich an 2. Stelle
Berechtigungsobjekt	10	Y_..., Z_...
Datenelement	10	Y..., Z...
Datenelementzusatznummer	4	9000 - 9999
Dialogbaustein	30	Y..., Z...
Dokumentationsbausteine:		
Allgemeiner Text (TX)	28	Y..., Z...
Buchkapitel (CHAP)	20	Y..., Z...
Release-Information	20	Y..., Z...
Struktur	12	Y..., Z...
Domäne	10	Y..., Z...
Dynpronummer	4	9000 - 9999
Entwicklungs-klasse	4	Y..., Z...
Formular	16	Y..., Z...
Funktionsbausteine	30	Y_..., Z_...
Funktionsgruppe	4	Y..., Z...
Gerätetyp	8	Y..., Z...
Logische Datenbank	2	Y..., Z...
Matchcode-ID	1	0 - 9
Matchcodeobjekt	4	Y..., Z...
Menü	8	MENUY..., MENUZ...
Modulpool Dynpro	8	SAPMY..., SAPMZ...
INCLUDES	8	MY..., MZ...
Modulpool Dialog	8	SAPDY..., SAPDZ...
INCLUDES	8	DY..., DZ...
Modulpool Unterroutine	8	SAPFY..., SAPFZ...
INCLUDES	8	FY..., FZ...
Modulpool Verbucher	8	SAPUY..., SAPUZ...
INCLUDES	8	UY..., UZ...
Nachrichten-ID	2	Y..., Z...
Nachrichten-Nummer	3	900 - 999
Nummernkreisbelegobjekt	10	Y..., Z...
Pool-/Clusternamen	10	Y..., Z...
Relation-ID	2	Y..., Z...
Report	8	Y..., Z...

Reportklassen	4	Y..., Z...
SPA-/GPA-Parameter	3	Y..., Z...
Sperrojekt	10	Y..., Z...
Stil	8	Y..., Z...
SYSLOG-Meldungen	2	Y..., Z...
Tabelle (Pool, Cluster, Transport)	10	Y..., Z..., T9..., P9...
Transaktionscode	4	Y..., Z...
View	10	Y..., Z...
Helpview	10	H_Y..., H_Z...

2 Sicherheit und Zugriffsschutz

2.1. Zielsetzung

Ein Zugriffsschutzsystem und die Möglichkeit zur Vergabe individueller Berechtigungen dient im wesentlichen vier Zielen:

- dem Schutz vertraulicher Daten vor unberechtigter Kenntnisnahme,
- dem Schutz der Daten vor unberechtigter, auch versehentlicher Veränderung oder Löschung,
- der Transparenz der Verfahren insoweit, als nachvollziehbar wird, wann welche Berechtigungen im System hatte und hat,
- der Sicherstellung der Prüfbarkeit von Anwendungen.

Handelsrechtlich sollen hierdurch (d.h. durch vorbeugende Kontrolle im Internen Kontrollsystem) Verstöße gegen das elektronische Radierverbot (§ 239, Abs.3 HGB) verhindert werden, die Nachvollziehbarkeit im Sinne der §§ 238 ff. HGB gewährleistet und Verstöße gegen die GoB vermieden werden - um sicherzustellen, daß keine unautorisierten, unvollständigen, unrichtigen und zeitlich oder sachlich falsch zugeordneten Daten in das System gelangen.

2.2. Anforderungen

Der Zugriffsschutz muß gewährleisten, daß nur autorisierte Personen in das System und an bestimmte Daten gelangen. Die entsprechenden Schlüssel (Passwörter) müssen verdeckt eingegeben werden können.

Das System sollte sicherstellen, daß

- nur Passwörter einer bestimmten Mindestlänge akzeptiert werden,
- bestimmte, leicht zu erratende Zeichenfolgen nicht akzeptiert werden,
- das Passwort nur vom Anwender selbst vergeben und verändert werden kann,
- eine Änderung des Passworts in definierbaren Abständen erzwungen wird,
- Passwörter vor Kenntnisnahme durch jeden außer dem Anwender selbst geschützt sind.

Das Berechtigungskonzept muß es ermöglichen, die Rechte des Anwenders auf die Tätigkeiten bzw. Zugriffe im System zu beschränken, die er aufgrund seiner Stellung und Verantwortlichkeit im Unternehmen unabdingbar braucht (Prinzip der minimalen Berechtigung), d.h. es muß eine möglichst tiefe Staffelung möglich sein im Hinblick auf

- die Art des Datenzugriffs (lesen, neu anlegen, ändern, löschen),
- Programme,
- Daten bzw. Dateien,
- Funktionen (Menüs, Menüzeilen)

bei möglichst beliebiger Kombination dieser Ebenen.

Da die Ordnungsmäßigkeit des SAP-Berechtigungskonzepts stark beeinflußt wird durch das Verfahren zur Vergabe von Berechtigungen, ist auch das Vergabeverfahren selbst Gegenstand der Prüfung. Es sollte organisatorisch definiert, geordnet und nachvollziehbar sein sowie ausreichend auf seine Einhaltung überwacht werden!

Schließlich sollte darauf geachtet werden, daß Benutzerstammsätze, Berechtigungen und Profile im Qualitätssicherungs(Test-)system neu angelegt, geändert oder gelöscht und anschließend mittels Korrektur- und Transportwesen in die Produktionsumgebung übernommen werden.

2.3. SAP-Fakten

Durch die Vergabe von **Berechtigungen** wird definiert, welche betriebswirtschaftlichen Objekte von den Mitarbeitern der Unternehmen bearbeitet werden dürfen und welche Bearbeitungsfunktionen dabei zugelassen sind.

Mit dem Release 5.0 im R/2-Umfeld war ein neues Verfahren eingeführt worden, Benutzerstammsätze, Profile und Berechtigungen anzulegen bzw. zu pflegen und Zugang zum SAP-System zu gewähren. Dieses Verfahren gilt im wesentlichen auch im R/3-Umfeld. Das Berechtigungskonzept ermöglicht es, Zugriffe der Benutzer auf das R/3-System präzise und flexibel zu erlauben und zu kontrollieren. So können einem Benutzer in verschiedenen Buchungskreisen unterschiedliche Berechtigungen gegeben werden; z.B. für das Ändern in Buchungskreis 01 und für das ausschließliche Lesen in Buchungskreis 02. Das Berechtigungskonzept enthält zudem Sicherungsmaßnahmen, die ein unberechtigtes Anmelden oder unerlaubtes Eingreifen in die Benutzerstammsätze, Profile und Berechtigungen einschränken.

Für die Verwaltung der Benutzerstammsätze und Berechtigungen ergeben sich im R/3 folgende Fakten:

2.3.1. Grundsätzliches zum Berechtigungskonzept

Benutzerstammsätze und Berechtigungskomponenten sind mandantenabhängig. Für jeden Mandanten im R/3-System sind also eigene Benutzerstammsätze und Berechtigungskomponenten zu pflegen.

Der Schutz von **Objekten** (z.B. Daten, Tabellen etc.) wird einerseits durch **Berechtigungen** oder Sammelberechtigungen beschrieben, die - Schlössern einer Tür vergleichbar - den zu schützenden Objekten zugeordnet sind. Sie enthalten **Werte** (z.B. einen konkreten Buchungskreis 0001) zu **Feldern**, die in einem zugehörigen Berechtigungsobjekt festgelegt sind. Den Benutzern selbst sind Berechtigungs**profile** - Schlüsseln vergleichbar - und/oder Sammelberechtigungsprofile - einem Schlüsselbund vergleichbar - an die Hand gegeben, d.h. in ihren Benutzerstammsatz eingetragen. Die Prüfung, ob ein Berechtigungsprofil eines konkreten Benutzers zu einer Berechtigung paßt, also ob ein Schlüssel zu einem Schloß paßt, wird zur Laufzeit im Dialog vorgenommen oder, wenn z.B. in einem ABAP das Schlüsselwort 'AUTHORITY CHECK' steht (vergleiche Abschnitt 2.3.6 und Kapitel 3 'KORREKTUR- und TRANSPORTWESEN').

Die Berechtigungsprüfungen finden grundsätzlich nur noch in den Programmen statt!

Eine Prüfung auf Transaktionsberechtigungen findet in der Regel nicht mehr statt - es sei denn, diese Prüfung wird bei der Entwicklung der Transaktion explizit vorgesehen (Prüfobjekt bzw. Prüfvorschrift). In jedem Falle läuft zu Beginn der Berechtigungsprüfungen die Prüfung der gesperrten Transaktionen ab.

SAP schreibt vor, an einem produktiven System niemals direkte Änderungen vorzunehmen und im Produktivsystem Änderungsberechtigungen in folgenden Berechtigungsobjekten **n i c h t** an die Benutzer zu vergeben:

- Berechtigungsobjekt S_DEVELOP 'ABAP/4 Development Workbench',
- Berechtigungsobjekt S_PROGRAM 'ABAP: Programmablaufprüfungen',
- Berechtigungsobjekt D_DDIC_ALL 'Berechtigung für Data Dictionary und Datenbank-Utility'),
- Berechtigungsobjekt S_TABU_CLI 'Tabellenpflege mandantenunabhängiger Tabellen',

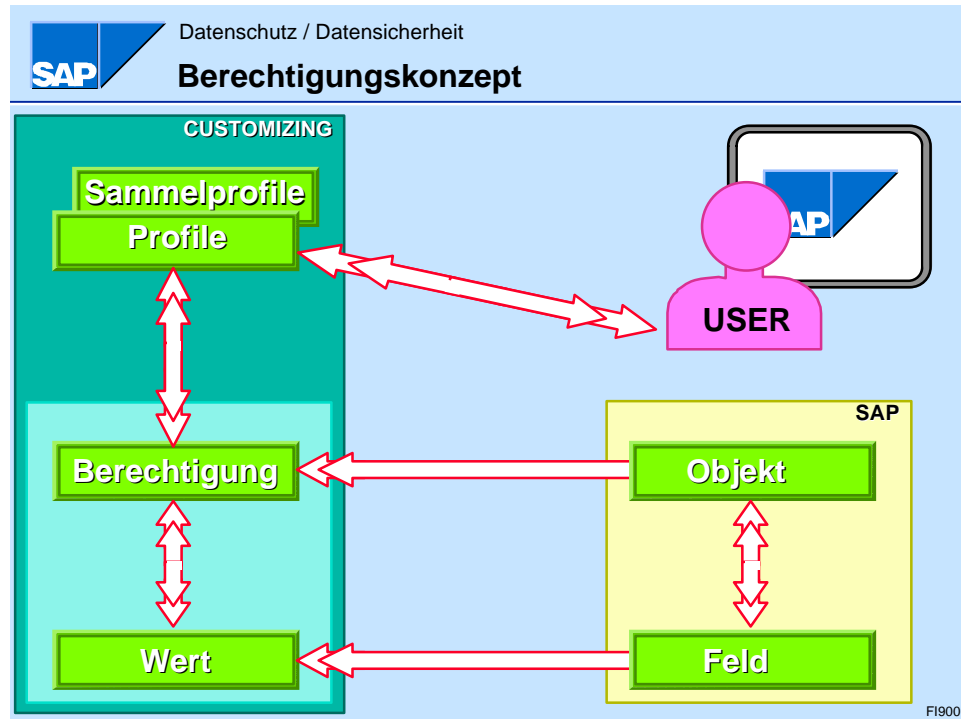
Zugriffe auf die Programmiersprache ABAP/4 werden mit folgenden Berechtigungsobjekten geprüft:

- S_PROGRAM: ABAP/4-Programme starten und Varianten, Attribute und Texte pflegen,
- S_ADMI_FCD: ABAP/4-Administration.

Weitere Hinweise finden Sie in den Dokumentationshandbüchern

- BC 'Systemverwaltung' und
- XX 'Konfiguration und Organisation' der jeweiligen SAP-Anwendungen.
(Anmerkung: XX steht für die jeweilige SAP-Anwendung).

2.3.2. Berechtigungsstrukturen



Mit der Zusammenfassung von Berechtigungen zu (Einzel-)Profilen und von Einzel- zu Sammelprofilen lassen sich jeweils aus einfacheren Strukturen komplexere bilden. Konkret kann mit dieser Technik z.B. ein Sammelprofil für Debitorenbuchhalter im Buchungskreis 01 angelegt werden. Dieses Sammelprofil erhält dann jeder Mitarbeiter, der die entsprechenden Tätigkeiten ausüben soll, in seinen Benutzerstammsatz eingetragen. Muß das Profil verändert werden, so braucht es nur einmal und nicht in jedem Benutzerstammsatz gepflegt zu werden.

Aus Performancegründen und aus Gründen der Übersichtlichkeit ist es nicht immer sinnvoll (obwohl zulässig), Sammelprofile in andere Sammelprofile einzubinden.

2.3.3. Trennung von Pflege und Aktivierung

Zur Erhöhung der Sicherheit sind Pflege und Aktivierung von Profilen bzw. Berechtigungen im System getrennt. Nur die Aktivversion eines Profils oder einer Berechtigung ist im System wirksam. Die Pflegeberechtigung einer Person kann auf bestimmte Benutzer, Profile und Objekte beschränkt werden.

2.3.4. Benutzerstammsatz

Im Benutzerstammsatz werden die für einen Benutzer zugelassenen Profile und/oder Sammelprofile aufgezählt. Dabei gilt ein umgekehrtes Vererbungsprinzip, d.h. Änderungen, die auf einer unter dem Benutzerstammsatz liegenden Ebene durchgeführt werden, wirken sich auf allen oberen Ebenen bis zum Benutzerstammsatz aus.

2.3.5. Passwortschutz und Anmeldung

Um den Schutz für Passwort und Anmeldung zu verbessern, müssen benutzerspezifische Initialpasswörter vergeben werden. Neue Passwörter müssen einer vom System vorgeschriebenen Syntax entsprechen und durchlaufen somit eine Vielzahl von Prüfungen(siehe Online-Dokumentation).

Darüber hinaus kann auch eine kundeneigene Paßwortprüfung dem SAP-Anmeldeverfahren hinzugefügt werden:

In der Tabelle USR40 können alle Wörter/Zeichenfolgen eingetragen werden, die als Kennwort nicht zugelassen sind. Die Tabelle kann mit der Transaktion SM 30 gepflegt werden.

Hinweis:Die einstellbare Maximalzahl von Anmeldeversuchen führt bei Überschreitung zu einer Sperrung des Users von maximal 24 Stunden, da nach Datumswechsel die Sperre systemintern zurückgenommen wird.

2.3.6. Kundeneigene Berechtigungsprüfungen

Kundeneigene Berechtigungsprüfungen können im R/3-System auf zwei Wegen hinzugefügt werden:

- einer **Transaktion** wird in **Tabelle TSTC** ein Berechtigungsobjekt hinzugefügt; in diesem Fall ist kein Programmieren erforderlich,
- in **ABAP/4-Programmen** sind die Berechtigungsprüfungen mit der Anweisung **AUTHORITY-CHECK** zu programmieren.

2.3.7. Vorgelagerte Sicherheitssysteme

Für die Sicherheitsprüfungen sind folgende Ebenen von Bedeutung:

- PC-Ebene
- Netzebene
- Betriebssystemebene
- Datenbankebene.

Die weitere Prüfung erfolgt auf der SAP-Applikationsebene.

An dieser Stelle muß auf die entsprechenden Dokumentationen der SAP-Basis und auf die Herstellerunterlagen verwiesen werden.

2.3.8. Tabelle TSTC 'SAP-Transaktionscodes'

Mit der Transaktion SE93 werden die Transaktionscodes im Mandanten 000 der Tabelle TSTC gepflegt; mit SM01 ge- bzw. entsperrt.

2.3.9. Customizing

Bezüglich Sicherheit und Zugriffsschutz beim Customizing wird auf das Kapitel 3 „Korrektur- und Transportwesen“ verwiesen.

2.4. Risiken

Die hohe Flexibilität des SAP-Berechtigungs- und Benutzerverwaltungskonzepts kann bei unsachgemäßer Anwendung zu erheblichen Sicherheitsrisiken führen. So ist es z.B. möglich, Workprozesse und/oder Buchungstasks zu beeinflussen.

Beispiele:

- Die Aufzeichnung von Änderungsbelegen (Stammdaten, Belege, Steuerungstabellen) kann ganz oder teilweise unterbunden werden,
- Die Berechtigungsprüfung in Programmen (AUTHORITY-CHECK) kann entfernt werden.

Von SAP werden in erheblichem Umfang sogenannte "**Standard**"-Profile ausgeliefert, die auf die verschiedensten betrieblichen Funktionen zugeschnitten sind. Wegen der Komplexität des neuen Berechtigungskonzepts werden diese von vielen Anwendern übernommen. Hieraus können sich bestimmte **Risiken** ergeben:

- die betrieblichen Erfordernisse werden durch die Standardprofile nicht hinreichend abgedeckt,
- durch eine eventuelle Anpassung der Standardprofile an die betrieblichen Erfordernisse können sich andererseits neue Risiken ergeben (z.B. durch Erweiterung der vergebenen Rechte),
- werden die SAP-Bezeichnungen der Profile beibehalten, obwohl an den Profilen Änderungen vorgenommen wurden, kann die Revisionsfähigkeit gefährdet sein.

Die Profile **S_A.SYSTEM** und **S_A.DEVELOP** enthalten ebenfalls kritische Berechtigungen und **sollten deshalb in einem produktiven System nicht vergeben werden!**

Schließlich kann gegebenenfalls ein Programm aus dem Testsystem - in ein anderes Programm "verpackt" - in das Produktivsystem übernommen und dort ausgeführt werden, es sei denn, es besteht eine innerbetriebliche Instanz, welche die Transporte in das Produktionssystem detailliert kontrolliert und freigibt.

Diese Beispiele machen deutlich, daß die Sicherheit - und letztlich auch die Ordnungsmäßigkeit - des gesamten Systems direkt von den vergebenen Berechtigungen abhängt.

Der Berechtigungsvergabe ist deshalb besondere Aufmerksamkeit zu widmen!

Vor einer Prüfung der Verarbeitungsergebnisse muß stets eine Prüfung der Benutzerberechtigungen vorgenommen werden, um sicherzustellen, daß die Verarbeitungsergebnisse auf autorisierten Routinen und Eingaben beruhen.

2.5. Prüfungen

2.5.1. Benutzerverwaltung

Informieren Sie sich über die Organisation der Vergabe von Benutzerberechtigungen (Antrags- und Genehmigungsverfahren, Trennung der Verantwortungsbereiche 'anlegen/pflegen Benutzer', 'anlegen/pflegen Objekte und Berechtigungen', 'aktivieren Profile und Berechtigungen') und die dafür vorhandenen innerbetrieblichen Anweisungen (IKS).

Klären Sie, ob schriftliche Anweisungen zur Vergabe und Änderungen von USERIDs existieren. Beschaffen Sie sich die entsprechenden Antragsformulare und nehmen Sie sie zu den Arbeitspapieren.

Prüfen Sie, ob bei Ausscheiden eines Mitarbeiters aus dem Unternehmen die Löschung seiner USERID durch organisatorische Maßnahmen sichergestellt ist.

Prüfen Sie, ob die Vergabe, Änderung und Löschung von USERIDs durch einen verantwortlichen Mitarbeiter genehmigt werden muß.

Untersuchen Sie, ob Kontrollverfahren von den dafür zuständigen Fachabteilungen angewandt werden, wenn ein neuer Benutzerstammsatz angelegt wird oder wenn die Zugriffsrechte eines Benutzers geändert werden.

Prüfen Sie, ob die Benutzerzugriffsrechte durch ein zwangsläufiges Verfahren geändert werden:

- wenn die Verantwortlichkeiten des jeweiligen Benutzers im Unternehmen wechseln und daher Änderungen seines Benutzerstammsatzes erforderlich sind (Gefahr kumulierter Zugriffsrechte bei häufig wechselnder Zuständigkeit im Unternehmen),
- wenn Mitarbeiter das Unternehmen verlassen (Ausscheiden).

Prüfen Sie, ob die Berechtigungsprofile der Mitarbeiter mit ihren Aufgabengebieten übereinstimmen.

Stimmen Sie in Stichproben die tatsächlich vergebenen mit den genehmigten Berechtigungen ab.

Prüfen Sie, ob Profile und Berechtigungen durch ein zwangsläufiges Verfahren geändert werden, wenn ein Objekt verändert wird.

Prüfen Sie, ob Änderungen innerhalb des Benutzerberechtigungskonzepts dokumentiert werden und die entsprechende Dokumentation mindestens 10 Jahre aufbewahrt wird.

Spezielle Einzelprüfungen:

- Wer ist im System aktiv?
Menüpfad Werkzeuge --> Administration --> Monitor -->
Systemüberwachung --> Benutzerübersicht
alternativ: Transaktionscode SM04
- Statistische Auswertung über User-Aktivitäten (nur pro Appl.-Server!)
Menüpfad Werkzeuge --> Administration --> Monitor --> Performance -
-> Workload --> Statistic Records --> Schaltfläche Choose Record.
Sodann Durchsicht auf z.B. SE38
alternativ: Transaktionscode STAT
- Vorgenommene Änderungen am User XXX
Menüpfad Werkzeuge --> Administration --> Benutzerpflege -->
Benutzer --> Info --> Änderungsbelege --> Benutzer --> Benutzername --
> Änderungen seit --> Schaltfläche Ber.änd.
alternativ: Transaktionscode SU01
- Welcher User hat kritische Systemberechtigungen?
Menüpfad Werkzeuge --> Administration --> Benutzerpflege --> Profile
--> Info --> Übersicht --> Benutzer --> Select Objekt --> Basis
Administration --> Systemberechtigungen. Werte mit * = alle Abfragen.
alternativ: Transaktionscode SU01 --> Infosystem

2.5.2. Sicherheit und Zugriffsschutz

Stellen Sie fest, ob spezielle Zugriffsschutztools installiert sind.

Lassen Sie sich das Anmeldeverfahren erklären und vorführen. Beschaffen Sie sich vorhandene schriftliche Unterlagen (Handbücher, Organisationsanweisungen etc.).

Klären Sie, ob systemseitig eine regelmäßige Passwortänderung erzwungen wird (Systemparameter bzw. **externe** Sicherheitssoftware).

Prüfen Sie in der Tabelle USR40, welche kundeneigenen Paßwörter nicht erlaubt sind. Stellen Sie fest, ob Online-Änderungen dieser Tabelle möglich sind, und ermitteln Sie den Personenkreis, der auf die entsprechende Reportberechtigungsgruppe zugriffsberechtigt ist.

Prüfen Sie, ob bei längerer Nichtbenutzung des Systems eine erneute Anmeldung erforderlich ist (Systemparameter bzw. **externe** Sicherheitssoftware).

Stellen Sie sicher, daß dem User **SAP*** alle Berechtigungen entzogen und auf einen geheimen Notfall-User übertragen wurden.

Achtung: Wenn der Benutzerstammsatz von SAP* gelöscht wird, wird SAP* auf das Standardpasswort "PASS" und die Standardprivilegien des Super-Users zurückgesetzt.

Stellen Sie ebenso sicher, daß das Standard-Paßwort des Benutzers DDIC, der i.d.R. nur für Installations- und Wartungstätigkeiten benötigt wird, in den Mandanten 000 und 001 geändert wurde. Außerdem sollten die weitgehenden Berechtigungen im DDIC nur temporär zur Verfügung gestellt werden.

Lassen Sie sich über das Menü oder mit den Transaktionen SU01-SU03 Benutzerstammsätze und Berechtigungsinformationen anzeigen. Folgende Auswertungen sind möglich:

- Benutzerstammsätze
- Profile
- Berechtigungen
- Berechtigungsobjekte
- Änderungsbelege.

Stellen Sie durch die Untersuchung dieser Auswertungen fest, ob nur aufgabenadäquate Berechtigungen vergeben wurden. Insbesondere die Berechtigungen der EDV-Mitarbeiter sind kritisch zu prüfen; ihnen sollten vor allem datenverändernde Zugriffsrechte nur im Ausnahmefall zugebilligt sein. Stellen Sie ferner fest, welche Kontrollen über die vergebenen Berechtigungen vorhanden sind.

Mit der Transaktion **SE16** kann in Tabelle **USR02** festgestellt werden, welche Benutzer über einen längeren Zeitraum hinweg nicht im System angemeldet sind oder waren. Bei der Abfrage ist der Benutzer mit '*' anzugeben und das Feld 'TRDAT' mit einem unmaskierten 8-stelligen 0-Eintrag zu versehen.

Dem zu prüfenden SAP-Anwender ist in diesen Fällen zu empfehlen, die entsprechenden Benutzerstammsätze aus dem System zu löschen, zumindest aber zu sperren.

Manipulationsmöglichkeiten bestehen ferner durch den unberechtigten Zugriff auf solche Benutzerstammsätze, deren Eigentümer sich noch nie in das System eingelogged haben und für die noch keine Standard-Passwortänderung erzwungen wurde. In diesem Fall können unter fremdem Namen Daten manipuliert werden.

Prüfen Sie in diesem Zusammenhang, ob im System festgelegt wurde, daß das Standard-Passwort (auch für alle anderen Passwörter möglich) nach einer bestimmten Anzahl von Tagen geändert bzw. der Benutzer gesperrt wird. Diese Funktion wird mit dem Systemprofilparameter 'login/password_expiration_time' festgelegt (Report **RSPARAM**).

Prüfen Sie mit der Transaktion **SM01**, welche Transaktionen gesperrt sind (ein X zeigt an, daß die Transaktion für sämtliche Benutzer gesperrt ist).

Tabellen-Änderungsprotokolle können mit den ABAP-Reports **RSTBPROT** (Auswertung der Tabellen-Protokolldatenbank) bzw. **RSTBHIST** (Auswertungen, d.h. Anzeige und Vergleich von tabellenartigen Objekten) aufgerufen werden, wenn im Betriebssystem der Schalter **rec/client** auf 'All' oder '<md>' sitzt. Die Einstellung der Protokollierung erfolgt im Customizing (Kontrolle mit Report **RSPARAM**).

Änderungsbelege werden geschrieben, wenn die Tabelle die technische Einstellung 'Protokollierung' besitzt und im System die Funktion 'Änderungsbelege schreiben' aktiv ist.

Prüfen Sie, ob ein adäquates Tabellenänderungs- und Freigabeverfahren besteht (vgl. Kapitel 4) und ob sichergestellt ist, daß sämtliche Veränderungen in der Tabelle **TSTC** lückenlos protokolliert werden.

Untersuchen Sie, ob sichergestellt ist, daß Kontrollen durch die Fachabteilungen vorgenommen werden, ob z.B. alle Daten, für welche die jeweilige Abteilung verantwortlich ist, nur mit ihrer Berechtigung geändert werden können.

Es ist zu prüfen, daß generell keine Prüfobjekte ausgeschaltet bzw. gelöscht werden können (z.B. Tabelle **TSTC**, Tabellen mit Prüfroutinen und in diesem Zusammenhang auch die Transaktionen **SM31** und **SE38**).

Prüfen Sie, ob die installierten Verfahren der Zugriffskontrollen die Protokollierung ihrer Veränderungen sicherstellen, so daß mißbräuchliche Veränderungen und jeder Vertuschungsversuch entdeckt werden können.

2.5.3. Wichtige Einzelberechtigungen

Grundsätzlich sollen SAP-Anwender in den sicherheitsrelevanten Bereichen (insbesondere Buchhaltung und Systembetreuung) nach dem **4-Augenprinzip** verfahren. Für System- und Mastertransaktionen bedeutet das im allgemeinen, daß ein 'NOTFALLUSER' zu bestellen ist, der **z u s a m m e n** mit einem Vertreter des jeweiligen Fachbereichs die erforderlichen Maßnahmen zu treffen hat. Für den Notfalluser sollte außerdem für Fälle der Abwesenheit ein Vertreter benannt sein.

Die relevanten Standardprofile, Berechtigungsobjekte und Transaktionen aus den Bereichen Buchhaltung und Systembetreuung werden im folgenden genannt.

Hinweis:

Buchungspflichtige Vorgänge werden, bedingt durch die verstärkte Integration der Programme (Module), nicht nur/nicht mehr allein in der Fachabteilung 'Buchhaltung' abgesetzt und generiert. Dies betrifft nicht nur Belege, sondern auch Stammdaten aus anderen SAP-Systemen.

Buchungsberechtigungen

In den SAP-Systemen gibt es verschiedene Standardprofile, Berechtigungsobjekte und Transaktionen zum Buchen, Ändern und Anzeigen von Belegen, und zwar nicht nur im FI, sondern auch in den Applikationen AM, CO, HR, MM, SD u.s.w.. Im Sinne der Funktionstrennung sollte in allen Systemen die Berechtigung für Buchungs- und Belegänderungstransaktionen auf die fachlich zuständigen und verantwortlichen Mitarbeiter beschränkt sein.

Prüfungen:

Prüfen Sie, ob die Berechtigungsobjekte für die Buchungsfunktionen der SAP-Systeme bzw. die entsprechenden Standardprofile für Buchungsfunktionen nur an die fachlich zuständigen und verantwortlichen Mitarbeiter der einzelnen Abteilungen vergeben sind.

Beispiele:

- Buchhaltungsbeleg: Berechtigung für Belegarten
- Buchhaltungsbeleg: Berechtigung für Buchungskreise
- Buchhaltungsbeleg: Berechtigung für Geschäftsbereiche
- Buchhaltungsbeleg: Berechtigung für Kontoarten
- Buchhaltungsbeleg: Kontenberechtigung für Debitoren
- Buchhaltungsbeleg: Kontenberechtigung für Kreditoren
- Buchhaltungsbeleg: Kontenberechtigung für Sachkonten

Stammdatenpflege (z.B. FDxx, FKxx, FSxx etc.)

Anmerkung: xx steht für 01, 02, 03 etc.

Im Rahmen eines Internen Kontrollsystems (IKS) ist darauf zu achten, daß eine Trennung der Funktionen 'Buchen' und 'Stammdatenpflege' vorgesehen ist.

Dies kann in kleineren Buchhaltungen dadurch erreicht werden, daß die Debitoren- und Kreditorenstammdaten jeweils von anderen Abteilungen gepflegt werden, die Kontrolle und die Buchungen jedoch in der sachlich zuständigen Buchhaltung erfolgen.

Alternativ kann im SAP-System eine Kontrolle mit den Transaktionen FK04 für Kreditoren-, FS04 für Sachkonten- und FD04 für Debitorenstammänderungen durchgeführt werden. Auch eine regelmäßige Auswertung mit den ABAP-Reports RFDABL00 (Debitoren) bzw. RFKABL00 (Kreditoren) ist möglich, bei der alle Stammdatenänderungen ausgedruckt und am Bildschirm angezeigt werden.

Für den Abgleich von Kreditorenstammdaten zwischen Finanzbuchhaltung und Einkauf steht der Report RFKKAG00 zur Verfügung.

Anmerkung: Weitere Auswertungsreports für Stammdaten existieren für: RFBABL00 (Belege), RFSABL00 (Sachkonten), RFDKLIAB (Kreditmanagement), RFBKABLO (Banken).

Alle Stammdatenänderungen sind zu protokollieren, soweit sie Belegcharakter haben. Da eine Abgrenzung von Änderungen mit und ohne Belegcharakter im allgemeinen sehr schwierig ist, sollten aus Sicherheitsgründen alle Änderungen in die Protokollierung einbezogen werden. Das Ändern und Löschen von Änderungsbelegen muß ausgeschlossen sein.

Prüfungen:

Verschaffen Sie sich einen Überblick, welche Berechtigungen zu den einzelnen von SAP vordefinierten Berechtigungsobjekten definiert sind und welche Werte die Felder der Objekte enthalten.

Stellen Sie fest, welche Mitarbeiter **Stammdaten pflegen** können (z.B. Objekte F_KNA1_xxx, F_LFA1_xxx, F_SKA1_xxx).

Prüfen Sie weiterhin, ob diese Mitarbeiter gleichzeitig auch buchen können.

Informieren Sie sich, wie Stammdatenänderungen kontrolliert werden.

Prüfen Sie, ob die gesetzlich vorgeschriebenen Aufbewahrungsfristen eingehalten werden.

Systemtransaktionen

Profile, die Systemberechtigungen enthalten (S_USER_ALL, SAP_ALL, SAP_NEW) sollten äußerst **restriktiv** vergeben werden. Prüfen Sie daher, wer über diese Systemberechtigungen verfügt.

Die Replacefunktion im Debugging (Berechtigung S_DEVELOP) darf in einem produktiven System nur vom Notfalluser unter Beachtung strenger Auflagen bezüglich der Nachvollziehbarkeit ausgeübt werden!

Mastertransaktionen

Die Mastertransaktionen (SExx, SMxx, SUxx) sowie die Standardprofile S_A.SYSTEM, S_A.ADMIN, S_A.CUSTOMIZ, S_TSKH_ALL und das Berechtigungsobjekt S_ADMI_FCD sollten nur an wenige ausgewählte Benutzer (z.B. NOTFALLUSER und/oder Vertreter) vergeben werden.

Prüfungen:

Prüfen Sie insbesondere, wer die **Transaktionsberechtigungen**

SM01 'Sperrern und Entsperrern Transaktionen'

SM12 'Sperrereinträge selektieren'

und in den folgenden Berechtigungsobjekten die entsprechenden Funktionen besitzt:

S_ADMI_FCD Systemberechtigungen, u.a. 'Sperrern von Transaktionen',

S_ENQUE Anzeigen/Löschen von Sperrereinträgen.

Wenn die **Tabelle TSTC** mandantenübergreifend ist, hat ihre Prüfung im Auslieferungsmandanten zu erfolgen, ansonsten im produktiven Mandanten.

Prüfen Sie, wer die Berechtigung hat, (mit Betriebssystemmitteln) System-Parameter zu setzen oder zu verändern.

Prüfen Sie, wer über die **Transaktion STAT** 'Tages-Systemstatistik' verfügt.

Stellen Sie fest, wer über die Pflegeberechtigungen **SU01/SU02/SU03** bzw. über die Objekte **S_USER_GRP**, **S_USER_PRO** und **S_USER_AUT** verfügt, und prüfen Sie, ob diese Mitarbeiter Benutzer im SAP-System anlegen bzw. pflegen sollen.

Prüfen Sie im Sinne der Funktionstrennung weiter die Zuteilung der Pflege-Transaktionen **SUxx**:

- Benutzeradministrator: Anlegen von Benutzern (**SU01**)
- Berechtigungsadministrator: Berechtigungspflege (**SU02, SU03**)
- Aktivierungsadministrator: Aktivierung (**SU02, SU03**).

Hinweis:

*Ein Administrator sollte **nicht gleichzeitig** zur Pflege und Aktivierung von Profilen **und** Berechtigungen befugt sein. Mit diesen Berechtigungen ist ein Benutzer in der Lage, unzulässige Privilegien an Berechtigungen zu definieren, zu aktivieren und zu vergeben. Das heißt z.B., daß der Wert 07 in den Berechtigungsobjekten **S_USER_PRO** und **S_USER_AUT** nur für den Aktivierungsadministrator zur Verfügung stehen sollte.*

Über die erforderlichen Berechtigungen der System- und Berechtigungsadministratoren informieren im übrigen insbesondere die Kapitel 2 'Benutzerstammsätze' und 3 'Berechtigungen' des SAP-Handbuchs 'BC-Systemverwaltung'.

Da die Administratoren häufig weitgehende Rechte besitzen, prüfen Sie von Zeit zu Zeit, ob die ihnen erteilten Berechtigungen korrekt sind und noch den organisatorischen Gegebenheiten entsprechen.

Prüfen Sie, wer das Berechtigungsobjekt **S_NUMBER** 'Pfleger Nummernkreise' besitzt.

Prüfen Sie, welche Benutzer über die Transaktionsberechtigungen **SM30** und **SM31** bzw. Berechtigungsobjekte wie **S_TABU_DIS**, **S_TABU_CLI** 'Pfleger ATAB-Tabellen' mandantenbezogen bzw. mandantenübergreifend verfügen. Stellen Sie fest, welche Berechtigungsklassen für Tabellen in der Tabelle TBRG bzw. TDDAT existieren. Prüfen Sie, ob alle Benutzer, die über SM31 verfügen, über die Tabellenberechtigung nur auf einzelne Klassen Zugriff erhalten. Jeder berechtigte Benutzer sollte nur die Tabellen pflegen können, die zu seinem Aufgabengebiet gehören.

Stellen Sie fest, wer die Transaktionsberechtigung **SE38** 'ABAP/4-Programmierung' und wer die Transaktionsberechtigung **SE51** 'Screenpainter/Dynproveränderung' besitzt.

Aufgrund der im Handelsgesetzbuch (HGB) geforderten "Nachvollziehbarkeit" ist die Transaktion SE38 in einem Produktionssystem nicht zulässig!

Für Notfälle sollte jedoch ein spezieller Benutzer (z.B. mit dem Namen 'NOTFALL') angelegt sein, der über diese Berechtigung verfügt. Alle Einsätze dieses Benutzers müssen dann in einer nachvollziehbaren Art und Weise protokolliert werden. Hierbei sollte das "**Vier-Augen-Prinzip**" eingehalten werden!

Prüfen Sie, wer über die Transaktionsberechtigung **SM13** 'Handling Verbuchungssätze' verfügt.

Der Report **RFVBER00** erzeugt eine Liste über abgebrochene Verbuchungen, die mittels 'Buchen Beleg' hätten gebucht werden sollen. Hierbei werden auch Buchungen berücksichtigt, die aus anderen Anwendungen in die Anwendung FI gelangt sind.

3 Workbench Organizer und Transportsystem

3.1. Zielsetzung

Das Workbench Organizer und Transportsystem (ab Release 3.0 ist das KTW unter dem Workbench Organizer und Transportsystem (WBOT) angesiedelt) dient zur:

- Registrierung und Dokumentation aller Änderungen an Systemobjekten (Objekte der Entwicklungsumgebung EUO); dazu gehören u.a. Elemente des Data Dictionary (z.B. Tabellen), ABAP/4-Programme, Bildschirmmasken, Oberflächen-Definitionen, Dokumentationsbausteine sowie anwendungsdefinierte Transportobjekte und Customizing-Objekte ;
- Vermeidung paralleler Änderungen an einem Systemobjekt durch unterschiedliche Entwickler;
- geordneten Übergabe und Freigabe von EUO zwischen unterschiedlichen SAP-Systemen oder unterschiedlichen Mandanten innerhalb eines SAP-Systems.

3.1.1. Funktionale Integrität

Durch die Änderung von Tabellen und Programmen erfolgt eine Funktionsänderung des Systems. Daher muß sichergestellt sein, daß ausschließlich genehmigte Änderungen wirksam werden und die Gesamtfunktionalität gewährleistet bleibt.

3.1.2. Nachvollziehbarkeit

Weitere Zielsetzung ist es, alle Änderungen am System lückenlos zu dokumentieren und somit nachvollziehbar zu machen.

3.2. Anforderungen

Grundsätzlich sollen alle Änderungen über den Workbench Organizer (und Transportsystem) erfolgen.

Es müssen ausreichende und verbindliche Regelungen für Auftragserteilung (z.B. Erstellung eines ABAP), Durchführung von Änderungen sowie für Test, Abnahme und Übernahme in die Produktion festgelegt sein (siehe auch Kapitel 3.2.3).

3.2.1. Auftragserteilung

Jede Änderung muß in einem Änderungsauftrag hinreichend genau beschrieben und formal vom Dateneigner genehmigt werden. Hierbei handelt es sich sowohl um die Genehmigung für die Änderung von Programmen als auch um die Übernahme von Datenbeständen.

3.2.2. Durchführung der Änderung

Da EUO in der Regel systemweite Gültigkeit besitzen, müssen Test- und Produktionssystem getrennt sein.

Zur Vermeidung paralleler Änderungen eines Objekts durch mehrere Entwickler nutzt das WBOT einen Sperrmechanismus.

Bei Einsatz des Workbench Organizer erfolgt bei Änderungen von EUO eine systemseitige Historienführung, d.h. es können beispielsweise alte Programmversionen wiederhergestellt werden.

Die SAP-Namenskonvention (Namensraum für Kundenobjekte) ist einzuhalten, um Probleme bei späteren Release- oder Putlevelwechseln zu vermeiden.

Selbstdefinierte EUO sind ausreichend zu dokumentieren.

3.2.3. Abnahme und Produktionsübergabe

Bei der Abnahme ist das Vier-Augenprinzip zu beachten, d.h. sie sollte unabhängig vom Programmierer in der Regel durch den Auftraggeber (Fachabteilung) durchgeführt werden.

Bei Programmänderungen sollte durch Vergleich der Quelltexte geprüft werden, ob tatsächlich nur der zu ändernde Programmteil modifiziert wurde.

Der Abnahmetest soll in einem von der Produktionsumgebung getrennten SAP-System (Preproduktion) mit einem dem Produktionssystem entsprechenden Customizing sowie einem geeigneten Datenbestand durchgeführt werden.

Es muß organisatorisch sichergestellt sein, daß nach Abnahme der Änderungen/Neuentwicklung keine nachträglichen Änderungen mehr durchgeführt werden können.

Abnahme sowie Übernahme in die Produktion müssen schriftlich dokumentiert werden. Entsprechende Nachweise (z.B. Auftrags- und Freigabeformular) sind gemäß den jeweiligen gesetzlichen Vorschriften zu archivieren.

3.3. SAP-Fakten

3.3.1. Zweck und Aufbau

Das Workbench Organizer und Transportsystem besteht aus den Komponenten

- Workbench Organizer
- Transportsystem.

Der Workbench Organizer garantiert, daß innerhalb (vernetzter) SAP-Systeme für jedes existierende EUO ein einziges Originalobjekt besteht. Änderungen werden normalerweise nur an diesem Original vorgenommen und mittels des Transportsystems in andere SAP-Systeme übernommen.

Der Workbench Organizer speichert sämtliche Änderungen an Data Dictionary Elementen und ABAP/4-Programmen. Alte Versionen können wiederhergestellt oder mit der derzeit aktuellen Version verglichen werden. Customizingeinstellung können je nach Systemeinstellung (Tabelle T000) auch aufgezeichnet werden.

Der Workbench Organizer wird automatisch aktiviert, sobald ein Benutzer ein Objekt zu ändern versucht. Benutzer können ein Objekt erst anlegen oder ändern, wenn sie vorher im Workbench Organizer einen Änderungsauftrag mit Aufgaben angelegt haben oder einen existierenden Änderungsauftrag benutzen. Zur Verhinderung von parallelen Änderungen werden die Objekte bei Erfassung einer Aufgabe für alle anderen Entwickler gesperrt. Diese Sperre wird erst bei Freigabe des Auftrages wieder aufgehoben.

Bei der Freigabe der Aufgaben werden diese an das Transportsystem übergeben. Das Transportsystem soll den sicheren und nachvollziehbaren Transport von EUO und Customizing-Einstellungen gewährleisten. Es ist systemunabhängig, d.h. die EUO können zwischen allen Betriebssystemen transportiert werden, die von R/3 unterstützt werden. Sämtliche erforderlichen Konvertierungen werden automatisch durchgeführt.

Der Workbench Organizer und das Transportsystem sind genau aufeinander abgestimmt. Zu Beginn einer Entwicklung wird ein Änderungsauftrag und für alle beteiligten Mitarbeiter eine/mehrere Aufgabe(n) angelegt. Danach werden die betroffenen Objekte erstellt oder geändert und dabei im Auftrag registriert. Zum Schluß der Entwicklung geben die einzelnen Mitarbeiter ihre Aufgabe(n) frei, um den Änderungsauftrag mit allen bearbeiteten Objekten via Freigabe aus dem Quellsystem zu exportieren. Auf Betriebssystemebene erfolgt dann der Transport in das jeweilige Zielsystem. Es besteht die Möglichkeit mehrere Änderungsaufträge zu einem Transportauftrag zusammenzufassen.

3.3.2. SAP-Systeme

Ein vernetztes SAP-System besteht für die Zwecke des KTW aus einem oder mehreren SAP R/3-Systemen der gleichen Version und desselben Datenbanksystems. Zur Unterscheidung dieser Systeme verwendet SAP folgende Nomenklatur:

- (Sonder-) **Entwicklungssystem:**

separate Entwicklung kritischer Bestandteile eines Projektes in einer isolierten Umgebung

- **Integrationssystem:**

für Entwicklungsarbeit nichtkritischer Anwendungen und Systemtests

- **Konsolidierungssystem:**

zur Sicherung von Entwicklungsständen; Verteiler für nachfolgende Belieferungssysteme

- **Belieferungssysteme:**

können automatisch Software (EUO) aus Konsolidierungssystemen übernehmen.

Anmerkung: Der Begriff 'Belieferungssystem' stellt die Gesamtheit des jeweils an den Kunden übertragenen Systemstandes dar.

SAP empfiehlt als Minimalumgebung eine Systemkonfiguration mit Entwicklungs- und Produktivsystem. Bei vielen Mandanten werden das Entwicklungs- und Integrationssystem zum 'Entwicklungs- und Testsystem', das Konsolidierungs- und Belieferungssystem zum 'Produktionssystem' zusammengefaßt.

Soweit Entwicklungsarbeiten an EUO stattfinden, ist ein System mit mehreren Mandanten für Entwicklung, Test und Freigabe nicht ausreichend, da EUO in der Regel mandantenübergreifend sind, und somit Änderungen sofort Auswirkungen auf den Produktionsbetrieb haben können.

Die bei einem Mandanten ausgeprägten Systemarten sind aus den aktuellen Einstellungen der Steuerungstabellen **TASYS** und **TSYST** ersichtlich (vergl. Abschnitt 3.3.4).

3.3.3. Korrektur und Reparatur

SAP unterscheidet zwischen

- Originalobjekten
- Kopien von Originalobjekten.

Ein EUO ist in genau einem SAP-System Original. Alle anderen (vernetzten) Systeme enthalten lediglich eine Kopie des Originals. Alle EUO mit Entwicklungsklasse, Originalsystem, verantwortlichem Autor, letzter Korrektur oder letztem Transport sind in der Tabelle TADIR hinterlegt. Die Tabelle wird jeweils bei der Pflegetransaktion des EUO aktualisiert.

Alle SAP-EUO (Tabellen, ABAPs,...) liegen als Original direkt bei SAP, an Kunden werden lediglich Kopien ausgeliefert.

Sofern der Anwender selbstdefinierte Eigenentwicklungen durchführt, liegen diese Objekte als Original vor. Originale werden durch einen Transport niemals überschrieben.

Mit dem Begriff **Korrektur** bezeichnet SAP die Änderung eines Originalobjekts, während eine **Reparatur** die Änderung einer Kopie bedeutet.

Es gilt das **Prinzip der eindeutigen Änderbarkeit:**

ein Objekt kann nur in demjenigen System mittels einer Korrektur geändert werden, in dem es erstellt wurde.

Reparaturen (Änderungen an Kopien) sollten lediglich dann vorgenommen werden, wenn der 'normale' Weg, d.h. **Korrektur des Originals und Transport in ein anderes SAP-System**, nicht eingehalten werden kann. Dies kann z.B. bei vorliegenden Fehlern innerhalb der SAP-Objekte, die nach dem oben Gesagten lediglich als Kopie beim Kunden vorliegen, zutreffen (sogenannte Notreparaturen).

Der Status eines EUO (Original, Kopie, Reparatur,...) wird in der Tabelle TADIR verwaltet. Diese Tabelle ist gegen manuelle Eingriffe zu schützen.

Ein repariertes Objekt wird nicht durch Transporte überschrieben, solange keine Bestätigung der Änderung des Originals eingegeben wird. Das Statuskennzeichen für die Änderung des Originals wird nicht systemseitig kontrolliert, d.h. das System prüft nicht, ob das Originalobjekt ebenfalls korrigiert wurde und mit der reparierten Kopie übereinstimmt.

3.3.4. Einstellungen des WBOT

Das WBOT wird über Tabellen gesteuert, welche mit der Transaktion **SE06** (Systemeinstellung für Korrektur und Transportwesen) angezeigt und bearbeitet werden können:

- **Tabelle TSYST:**

Enthält die technische Beschreibung aller (im Netz) verfügbaren SAP-Systeme (Name, Betriebs- und Datenbanksystem etc.). Das Transportsystem verwendet zur Überprüfung der Verfügbarkeit eines SAP-Systems ausschließlich den im Feld 'Systemname' eingegebenen Namen. Die Angaben in den übrigen Feldern der Tabelle mit Ausnahme des Attributs 'Charset' (dem vom jeweiligen System verwendeten Zeichensatz) sind optional.

- **Tabelle TASYS:**

Enthält Festlegungen, an welche Systeme die Transporte aus einem Konsolidierungssystem weitergeleitet werden sollen.

- **Tabelle DEVL:**

Enthält die Definition der Transportschichten. Eine Transportschicht legt den Transportpfad vom Integrationssystem zum Konsolidierungssystem fest.

(falls es mehrere Belieferungssysteme gibt, ist auch die Tabelle TWSYS von Bedeutung)

- **Tabelle TWSYS:**

Enthält die Konsolidierungswege für Änderungsaufträge

- **Tabelle TDEVC:**

Enthält ein Verzeichnis aller Entwicklungsklassen. Jeder Klasse ist ein Integrations- und ein Konsolidierungssystem zugewiesen.

Diese Tabellen sind **lediglich durch den Benutzer DDIC pflegbar** und müssen in allen SAP-Systemen, die mit dem WBOT verknüpft sind, gleichen Inhalt aufweisen.

Ferner läßt sich festlegen, welche systemweiten Änderungen zugelassen sind. Diese Einstellung kann lediglich der Benutzer DDIC oder ein Benutzer, der sämtliche Berechtigungen für den Workbench Organizer besitzt, vornehmen. (Transaktion SE03 oder Werkzeuge --> ABAP/4 Workbench --> Übersicht --> Workbench Organizer --> Springen --> Tools)(Transaktion SE01 --> Hilfsmittel --> Tools --> setze Systemänderbarkeit).

Es sind folgende Möglichkeiten vorhanden:

- Objekte sind nicht änderbar:
Mit dieser Einstellung sind keinerlei Änderungen an Objekten möglich. Es können auch keine neuen Objekte angelegt werden.
- nur Originalobjekte (mit Workbench Organizer):
Mit dieser Einstellung sind nur Originalobjekte des Systems unter Korrekturkontrolle änderbar
- alle Kundenobjekte (mit Workbench Organizer)
Diese Einstellung umfaßt die Einstellung „Nur Originalobjekte“ und bietet darüber hinaus die Möglichkeit, Kundenobjekte in Nicht-Originalsystemen zu reparieren.
- alle Objekte (mit Workbench Organizer):
Diese Einstellung bietet zusätzlich zu „Alle Kundenobjekte“ die Möglichkeit, auch Objekte der SAP zu reparieren.

Hinweis : Änderungen dieser Systemeinstellungen werden nach Angaben von SAP nicht protokolliert. Das WBOT kann in Rel. 3.0 einem Berechtigungsobjekt zugeordnet werden und damit im Rahmen des Berechtigungskonzeptes besonders geschützt werden.

3.3.5. Durchführung von Transporten

Durch Erstellung eines Transportauftrags wird auf Betriebssystemebene eine Hilfsdatei mit den jeweiligen Transportinhalten angelegt, welche beim Import in das Zielsystem durch das **Transportprogramm 'tp'** ausgewertet wird. Das in älteren Releaseständen eingesetzte Programm 'r3trans' soll nach der Empfehlung von SAP nicht mehr eingesetzt werden.

Besitzen die SAP-Systeme ein gemeinsames Transportverzeichnis, so wird beim Export der Transportaufträge vom Quellsystem in das Zielsystem automatisch ein 'Testimport' durchgeführt.

Die Autoren der Transportaufträge werden über deren Erfolg/Mißerfolg (des Exportes bzw. des Testimportes)benachrichtigt. Transportprotokolle sind über das Info-System anzeigbar.

3.4. Risiken

3.4.1. Gültigkeit von EUO

Da die EUO im allgemeinen systemweite Gültigkeit besitzen, wirkt sich z.B. die Änderung eines ABAP auf alle Mandanten des betroffenen SAP-Systems aus. Die Berechtigungen zum Ändern von EUO müssen demzufolge im Produktionssystem ausgesprochen restriktiv gehandhabt werden (z.B. keine Berechtigung zur Programmierung).

3.4.2. Fehleinstellungen des KTW

Durch falsches Customizing des WBOT (Tabellen TSYST, TASY, DEVL) können Transporte fehlschlagen. Das gesamte Transportwesen kann durch falsche Einstellung der Systemänderbarkeit ('alles änderbar') umgangen werden; Änderungen sind somit nicht mehr nachvollziehbar.

Hinweis: Die Einstellung „Alles änderbar“ ist auch in Rel. 3.0 noch vorhanden

3.4.3. Zugriff auf Betriebssystemebene

Bei Anwendung des WBOT werden alle transportierbaren Änderungsaufträge in einer Datei auf Betriebssystemebene abgelegt. In der Datei Sytemname<sid>KT90001 sind die geänderten Daten, Customizingeinstellungen gespeichert. In der Datei <sid>KX90001 sind Subscripte und Dokumentationen gespeichert. Der eigentliche Import in das Zielsystem erfolgt durch Aufruf des Programms 'tp' auf Betriebssystemebene. Während der Import der Datei <sid>KT90001 vom Betriebssystem über den Befehl 'tp import <sid>KT90001 erfolgt, kann die zweite Datei <sid>KX90001 auch aus SAP (im Zielsystem) heraus importiert werden. Wie die übrigen Systemdaten sollten die betroffenen Verzeichnisse und Dateien vor dem Zugriff unberechtigter Benutzer geschützt werden.

Nur Subscript-Datei<sid>KX90001 kann direkt aus der R/3 Umgebung importiert werden.

3.4.4. Instabilität

Das SAP-System besteht aus verschiedenen änderbaren Komponenten, die in ihrer Gesamtheit voneinander abhängig sind. Aufgrund dieser Komplexität können Änderungen leicht zu Unsicherheiten und Instabilitäten führen, z.B.:

- Fehler sind nicht sofort erkennbar,
- Daten werden nicht, unvollständig oder mehrfach verarbeitet,
- die erforderliche Verfügbarkeit der Systemfunktionen ist nicht immer sichergestellt,
- Verzögerung bei der Funktionsausführung (Ablaufsicherheit),
 - Kontrollen können möglicherweise nicht mehr durchgeführt werden und sind somit wirkungslos,
- das System ist somit nicht mehr verlässlich.

Es ist offensichtlich, daß hierdurch erhebliche Risiken gegeben sind.

3.4.5. Manipulation

Die Komplexität eines SAP-Systems und die damit verbundene Fehleranfälligkeit bei unkontrollierten Änderungen können zu Instabilitäten führen, die mißbraucht werden können.

Sofern keine angemessenen Kontrollmechanismen vorliegen, ist grundsätzlich die Möglichkeit der Manipulation gegeben.

3.5. Prüfungen

3.5.1. Ist-Aufnahme des Verfahrens

Zunächst ist Einsicht zu nehmen in die Gesamtübersicht aller durch den Anwender selbst definierten EUO und aller vorgenommenen Korrekturen/Reparaturen an SAP-Objekten. Dabei ist wichtig, daß für diese auch eine klare Beschreibung ihrer Funktion verfügbar ist.

Anschließend erfolgt die Ist-Aufnahme und (soweit für die Prüfung erforderlich) Dokumentation des Systempflege- und Freigabeverfahrens.

3.5.2. Überprüfung des Konzeptes

Basis der Überprüfung des zuvor aufgenommenen Konzeptes sind zunächst die oben aufgeführten Anforderungen. Darüber hinaus erfolgt eine allgemeine Prüfung im Hinblick auf die oben formulierten Ziele und Risiken. Hierbei ist insbesondere auf eine angemessene Funktionstrennung zu achten (Entwicklung - Freigabe - Transport).

3.5.3. Einhaltung des Konzeptes

Stichprobenartige Prüfung der Entwicklungsaufträge mit zugehörigen Test- und Freigabeprotokollen. Dies geschieht sowohl top-down, d.h. in Richtung vom Änderungsauftrag zum EUO in der Produktionsumgebung als auch umgekehrt.

3.5.4. Konkrete Prüfungshandlungen

Erforderliche Prüfungen:

- Überprüfung der Einstellungen zum WBOT sowie der Systemänderbarkeit
Ermittlung des angewandten Verfahrens bei Eigenentwicklungen sowie bei Korrekturen und Reparaturen (Reparaturen an SAP-Objekten sind ab Release 3.0 nur nach Beantragung eines Reperaturschlüssels bei SAP möglich)
Ermittlung derjenigen Benutzer, die einen Transportauftrag erstellen und freigeben dürfen
- Untersuchung einer Stichprobe der Transportprotokolle
(Transaktion SE06 und ABAP RDDIT070 - RDDIT077)
- Ermittlung derjenigen Benutzer, die Importe in das Produktionssystem durchführen können
- Feststellung der unternehmensweiten Regelungen zum Einsatz des Korrektur- und Transportwesens sowie Kontrolle der Einhaltung dieser Festlegungen
- Prüfung von manuellen Eingriffen in die Tabelle TADIR.

Hinweis

Änderungen von Customizing-Einstellungen, die im Testsystem bzw. Entwicklungssystem vorgenommen und mittels des WBOT in das Produktionssystem transportiert wurden, sind nur im Testsystem protokolliert. Will man also Änderungen nachvollziehen, so sind die Änderungsprotokolle im Test bzw. Entwicklungssystem anzusehen. Änderungen die durch einen Transportauftrag in das Produktionssystem eingehen, werden dort nicht protokolliert.

4 Tabellenzugriff und Protokollierung

4.1. Zielsetzung

Ziele des Verfahrens zur Tabellenänderung sind:

- die Sicherstellung der korrekten Tabelleneinstellung,
- die Nachvollziehbarkeit aller Änderungen.

Unter dem Begriff „Änderungen“ werden hierbei verstanden:

- Änderungen von Tabelleninhalten in Tabellen mit Systemsteuerdaten der Auslieferungsklassen
 - C - Customizingtabelle -Pflege nur durch Kunden - kein SAP.Import
 - G - Custimizingtabelle durch Kunden nur Insert erlaubt.
 - E - Systemsteuertabelle, SAP und Kunde haben eigene Keys
 - S - Systemtabelle, Pflege nur durch SAP Änderung = Modifikation
 - W - Systemtabelle des Kunden
- Änderungen von Tabellenstrukturen erfolgen unter Kontrolle des Workbench Organizer und des Transportsystems.

4.2. Anforderungen

4.2.1. Protokollierung

Alle (relevanten) Änderungen von Tabelleninhalten (Datensätzen) sind zu protokollieren. Ferner sind Strukturänderungen, d.h. Änderungen im Data Dictionary durch Korrekturen oder Reparaturen, fortzuschreiben.

Diese Protokolle sollten bei 'kritischen' Tabellen, z.B. Tabellen, die den Mengen- und Wertefluß steuern wie Kontenfindung und Bewertung, regelmäßig zumindest stichprobenweise überprüft werden.

Die Nachweispflicht für Tabellenänderungen beträgt (in Deutschland) 10 Jahre!

Tabellenänderungen müssen in angemessener Zeit lesbar gemacht werden können.

4.2.2. Kundeneigene Tabellen

Die SAP-Namenskonventionen müssen eingehalten werden, um Probleme bei späteren Releasewechseln zu vermeiden und das System nachvollziehbar zu halten.

Selbstdefinierte Tabellen sind wie alle eigenentwickelten Objekte ausreichend zu dokumentieren.

4.2.3. Zugriffsschutz

Es muß ein Berechtigungskonzept vorliegen, in dem u.a. zu regeln ist, welche Benutzerkennungen die Berechtigung zur Tabellenpflege besitzen (z.B. Berechtigungsobjekte S_TABU_DIS, S_TABU_CLI). S_TABU_CLI steuert die Berechtigung für mandantenübergreifende Tabellen.

SAP hat standardmäßig einen Bestand an Berechtigungsgruppen angelegt und Tabellen und Views jeweils Berechtigungsgruppen zugeordnet.

- Die eingerichteten Berechtigungsgruppen sind in der Tabelle **TBRG** hinterlegt,
- die Zuordnung von Tabellen zu Berechtigungsgruppen erfolgt über die Tabelle **TDDAT**.

Sofern Tabellen gepflegt werden sollen, sind folgende Berechtigungen erforderlich:

- Berechtigung für die Berechtigungsgruppe der Tabelle und die Aktion 'Tabellenpflege',
- globale Berechtigung für mandantenunabhängige Tabellen.

Die globale Berechtigungsprüfung gilt für alle Tabellen der Auslieferungsklasse C (Kunden), G (Kundentabellen mit SAP-Einträgen) und E (Systemtabellen, die der Kunde ändern kann).

Diese zusätzliche Berechtigung ist grundsätzlich erforderlich, weil Änderungen an einer mandantenunabhängigen Tabelle Auswirkungen auch auf andere im System eingetragene Mandanten haben können.

Mit dem Programm **RSCLASDU** 'Tabellenklassifikation...' kann eine Liste aller Tabellen erstellt werden, für die eine mandantenunabhängige Berechtigung erforderlich ist.

4.2.4. Arbeits-/Organisationsanweisungen

Um die Unabhängigkeit vom Wissen einzelner Personen und die Sicherheit für eine korrekte Tabelleneinstellung zu erhöhen, sollten für kritische Tabellen "Arbeits-/Organisationsanweisungen" vorliegen, in denen z.B. folgende Informationen niedergelegt sind:

- Namenskonventionen,
- Anlaß und Begründung einer Tabellenänderung,
- Konsequenzen einer Tabellenänderung.

Änderungsaufträge an kritischen Tabellen müssen auch dem Freigabeverfahren unterliegen und mit Hilfe des Korrektur- und Transportwesens durchgeführt werden. Der Nachweis der Durchführung einer Tabellenänderung muß erbracht werden können.

4.2.5. Sicherstellung des Informationsflusses

Durch die hohe Integration des SAP-Systems kann es bei einer Tabellenänderung zu unbeabsichtigten Nebenwirkungen (z.B. in anderen Modulen) kommen. Deshalb sollte ein verbindliches Verfahren vorliegen, das bei "kritischen" Tabellen den Informationsfluß zu den von einer Tabellenänderung Betroffenen sicherstellt.

4.3. SAP-Fakten

4.3.1. Zweck und Aufbau

Eine Tabelle ist eine zweidimensionale Matrix, die eine Relation im Datenbanksystem beschreibt. Sie besteht aus einer Kopfzeile, welche die Felder (Attribute) definiert, und einer variablen Anzahl gleichartig aufgebauter Zeilen, die Datenwerte enthalten (Datensätze).

Ein Datensatz ist unterteilt in einen Primärschlüssel- und einen Funktionsteil. Über den Primärschlüssel sind die Datensätze innerhalb einer Tabelle eindeutig identifiziert. Der Primärschlüssel kann aus mehreren Attributen zusammengesetzt sein.

Tabellen lassen sich unterscheiden in:

- Tabellen mit Systemsteuerdaten
- Tabellen mit betriebswirtschaftlichen Grunddaten
- Tabellen mit Daten zur Unternehmensstruktur
- Tabellen für Anwendungsdaten.

Tabellen mit Systemsteuerdaten sollen die unternehmensspezifische Anpassung der Standard-Software ohne Modifikation der Programme ermöglichen. Sie enthalten variable Einflußgrößen für:

- Ablaufsteuerungen (z.B. Kontenfindung),
- Logik-Prüfungen (z.B. nur Eingabe bestimmter Werte zulässig),
- Rechenroutinen (z.B. Berechnung der Mehrwertsteuer),
- Automatische Generierungen (z.B. Buchung von Skontoerträgen),
- Bildmodifikationen (z.B. Pflichteingabe eines Feldes).

4.3.2. Tabellenzugriff und Protokollierung

Bei Installation eines Systems sollte nach dem **Einführungsleitfaden** vorgegangen werden, da dadurch erreicht werden kann, daß alle Systemeinrichtungsarbeiten vollständig abgearbeitet werden.

Der Tabellenzugriff für Tabelleneinträge ist möglich mittels:

- Einführungsleitfaden
- Customizingmenüs
- direkter Tabellenpflege (Transaktion SM30-SM32)
- Korrektur- und Transportwesen
- ABAP

Tabelle T000 (Mandantenabhängige Customizing-Einstellungen ändern.)

Mit dieser Tabelle wird festgelegt, ob in einem Mandanten Änderungen an mandantenspezifischen Customizing-Einstellungen automatisch in Customizing-Aufträgen (Änderungsauftrag) aufgezeichnet werden. Die erforderliche Grundeinstellung erfolgt im Feld 'Aufzeichnungsgrad'.

Änderungen an Tabelleninhalten sind zu protokollieren. Technisch ist diese Anforderung durch zwei Systemeinstellungen umzusetzen:

- für relevante Tabellen ist im Data Dictionary das Feld '**Tabellenprotokollierung**' zu aktivieren (technische Einstellung),
- im SAP-Startprofile ist der Parameter '**rec/client**' auf den (die) zu protokollierenden Mandanten zu initialisieren.

Eine Auswertung der Startparameter kann mit dem ABAP **RSPARAM** erfolgen.

Die Auswertung der Tabellenänderungen ist mit folgenden ABAP-Reports möglich:

- **RSTBPROT** 'Auswertung der Protokolldatenbank'
- **RSTBHIST** 'Tabellenauswertung (inkl. Historienverwaltung)'

Änderungen von im Data Dictionary eingetragenen Tabellenstrukturen durch Korrekturen oder Reparaturen erfolgen unter Kontrolle des Korrektur- und Transportwesens (soweit aktiviert). Systemseitig wird eine Historie geführt, sodaß derartige Modifikationen mit Hilfe des SAP-Infosystems nachvollzogen werden können.

4.3.3. Gültigkeitsbereich und Kundentabellen

Eine Tabelle kann entweder für alle Mandanten im System gelten (mandantenunabhängig) oder auf nur einen bestimmten Mandanten beschränkt sein (mandantenabhängig):

- mandantenunabhängige Tabellen enthalten Daten, die von allgemeiner Gültigkeit sind, z.B. Systemsteuerdaten, Sprachkürzel oder Transaktionscodes,
- in mandantenabhängigen Tabellen werden die Anwendungsdaten sowie mit wenigen Ausnahmen die betriebswirtschaftlichen Grunddaten abgelegt.

Die Mandanten(un)abhängigkeit ist eine Tabelleneigenschaft, die im Data Dictionary bei der Definition der Tabelle festgelegt wird. Eine mandantenabhängige Tabelle hat stets den Mandanten an erster Schlüsselposition.

Kundenspezifische Tabellen sollen nach der von SAP festgelegten Namenskonvention mit Y oder Z beginnen. Aus historischen Gründen sind weiterhin für Tabellennamen Zeichenketten, beginnend mit T9 oder P9, zugelassen.

Der Tabellename kann aus maximal zehn Zeichen bestehen, wovon jedoch lediglich die ersten sieben Zeichen signifikant sind. Soll die Tabelle über die Transaktion 'Tabellenpflege' (SM30-SM32) pflegbar sein, darf der Tabellename höchstens fünfstellig sein.

4.3.4. ABAP-Reports

Wichtige ABAP-Reports für Tabellenauswertungen sind:

- RSCLASDU 'Tabellenliste mit Klassifizierung'
- RSPARAM 'Auswertung der Startparameter'
- RSTBPROT 'Auswertung der Protokolldatenbank'
- RSTBHIST 'Tabellenauswertung (inkl. Historienverwaltung)'

4.3.5. Beispiele für wichtige Tabellen

In der Finanzbuchhaltung:

T000	Mandanten
T001*	Buchungskreise und Buchungskreissteuerung
T003*	Belegarten und Texte
T004*	Kontenpläne
T007*	Steuerschlüssel
T008*	Sperrgründe für den maschinellen Zahlungsverkehr
T012*	Hausbanken
T030	Fixkontentabelle
T033*	Kontenfindung
T042*	Zahlungsverkehr
T044A	Methoden der Fremdwährungsbewertung
T044Z	geänderte Abstimmkonten
T074	Sonderhauptbuchkonten
T077*	Kontengruppen
T169*	Toleranzen Rechnungsprüfung
TBAER	Belegänderungsregeln
TCUR*	Währungskurse
T9*	Kudentabellen

Im Basissystem:

TSTC	Transaktionscodeverwaltung (inkl. Prüfobjekt)
TBRG	Berechtigungsgruppen für Tabellen
TDDAT	Berechtigungsgruppen nach Tabellen auswertbar
TACTZ	gültige Aktivitäten je Berechtigungsobjekt
TADIR	Entwicklungsobjekte und Transporteigenschaften
TSYST	Verzeichnis der verfügbaren Systeme (KTW)
TASYS	Auslieferungstabelle (KTW)
TDEVC	Entwicklungsklassen Transportwesen (KTW)
T078*	Bildauswahl transaktionsabhängig
T079*	Bildauswahl buchungskreisabhängig

(*) *Bei Angabe eines * ist die Tabelle weiter unterteilt.*

4.4. Risiken

Da den Tabellen im SAP-System eine zentrale Steuerungsfunktion zukommt, liegen die Risiken eines unzureichenden Verfahrens zur Änderung von Tabelleninhalten auf der Hand:

- Es besteht die Gefahr von Fehleinstellungen.
- Die Veränderung einer Tabelle kann ungewollte Nebenwirkungen an anderer Stelle haben.
- Hierdurch kann die Integrität des Datenbestandes und der Funktionalität verletzt werden. Außerdem können Berechtigungen verändert werden, soweit sie in Tabellen definiert sind. Es besteht die Gefahr nicht nachvollziehbarer Systemveränderungen.
- Änderungsbelege können ohne Archivierung gelöscht werden.

Besondere Risiken:

- Fehlende Initialisierung des Parameters 'rec/client' (siehe 4.3.2.)
- Fehlerhafte Eintragung in Tabelle T000 (siehe 4.3.2.)
- Fehlende Protokollierung von wichtigen Tabellen
- Systemeinstellungen des Vorsystems (= dem Produktionssystem vorgelagerten System, aus dem Objekte über das Transportwesen eingestellt werden)
- Kopierfunktionen zwischen Mandanten, die Einstellungen von Tabellen ohne Historienfortschreibung überschreiben

4.5. Prüfungen

Folgende Prüfungsschritte sind erforderlich:

- das Verfahren zur Änderung von Tabellen ist zu ermitteln,
- das Verfahren ist an Hand der im vorigen Abschnitt aufgeführten Anforderungen zu bewerten,
- die Einhaltung der Anforderungen ist stichprobenweise zu überprüfen.

Weitere Prüfungshandlungen sind:

- das Test- und Freigabeverfahren,
- Zuständigkeiten und das Berechtigungssystem für Tabellenänderungen,
- stichprobenweise Prüfung kundeneigener Tabellen hinsichtlich Dokumentation und Einhaltung der SAP-Konventionen,
- die Einstellungen des Verfahrens zur Tabellenprotokollierung, insbesondere die technische Einstellung im Data Dictionary und der Parameter 'rec/client' im SAP-Startprofile.
- Einstellungen in der Tabelle T000.(Aus den Änderungsbelegen der Tabelle T000 geht hervor, ob während des Prüfungszeitraums am Aufzeichnungsgrad Änderungen vorgenommen wurden.)

Hinweis: Im SAP-Auslieferungssystem ist der Schalter „Datenänderungen protokollieren“ für die Tabelle T000 passiv!

- Feststellung von Archivierungen (vor Löschung)
- Überwachung der Änderungshäufigkeit wichtiger Tabellen

5 Job-Auftragsverfahren und - Dokumentation sowie System-Protokolle

5.1. Zielsetzung

5.1.1. Job-Auftragsverfahren

Beim Job-Auftragsverfahren stehen folgende Ziele im Vordergrund:

- Schutz der Unternehmensdaten und der personenbezogenen Daten
- Integrität der Daten und Funktionen
- Schutz der Ressourcen.

5.1.2. Job-Dokumentation

Ziele der Job-Dokumentation sind:

- Sicherstellung eines reibungslosen Ablaufs
- Unabhängigkeit von Detailkenntnissen bestimmter Personen
- Überprüfbarkeit der EDV-technischen Abwicklung durch einen sachverständigen Dritten in angemessener Zeit.

5.1.3. Job-Protokolle

Job-Protokolle sind erforderlich für den Nachweis der ordnungsgemäßen Abwicklung, d.h. insbesondere der Einhaltung des Job-Auftragsverfahrens.

5.2. Anforderungen

5.2.1. Job-Auftragsverfahren

Das Job-Auftragsverfahren muß grundsätzlich klar definierte Abläufe und Verantwortlichkeiten enthalten für

- Auftragserteilung
- Durchführung
- Nachbearbeitung und Output-Verteilung.

Da im R/3 viele Jobs von der Fachabteilung generiert und gestartet werden können, ist in der Regel eine entsprechende Verfahrensdokumentation im Anwendungshandbuch der jeweiligen Fachabteilung ausreichend.

Jobs, die ein Device-Operating benötigen und deshalb nicht ausschließlich im Aktionsbereich der Fachabteilung durchgeführt werden, müssen besonders beachtet werden. Insbesondere bei diesen Jobs darf keine Ausführung (z.B. durch eine Service-Abteilung wie das RZ) ohne Auftrag erfolgen. Auftraggeber ist in der Regel die Fachabteilung.

5.2.2. Job-Dokumentation

Bei Jobs, die vom SAP-System generiert werden, wird die Dokumentation automatisch mit generiert.

Bei vom Anwender selbst generierten Jobs ("native Job-Generierung", z.B. Mappen) muß auch die Dokumentation durch den Anwender selbst erfolgen. Die Dokumentation sollte nach einem einheitlichen Schema erstellt werden (siehe Mustervorschlag in Kapitel 5.6).

Die Aufbewahrungsfrist der Job-Dokumentation beträgt 10 Jahre!

5.2.3. System-Protokolle

Job-Protokolle müssen nachweisen, wann welcher Job mit welchen Parametern gelaufen ist. Die im System generierten Job-Protokolle sind speziell zu schützen.

Außerdem muß ein exceptionelles Reporting in sensiblen Bereichen auf Basis der System-Protokolle erfolgen.

5.3. SAP-Fakten

Im allgemeinen wird ein spezieller Job (z.B. Mahnlauf) aufgrund eines job-spezifischen Befehls vom Anwender durch das System automatisch generiert. Der Zugriff auf einen Job-Generierungsbefehl kann im Rahmen des allgemeinen Berechtigungskonzepts geschützt werden.

Die Definition von Jobs, das Anlegen von Jobsteps und die Festlegung von Startterminen erfolgen in der Regel mit der Transaktion **SM36** oder über den **Menüpfad** Werkzeuge --> Administration --> Jobs --> **Jobdefinition**.

Einige Jobs, z.B. Vorlaufreports, können aber auch über die Transaktion SA38 oder über den Menüpfad System --> Dienste --> Reporting --> **Programm** definiert werden.

Die Job-Übersicht erhält man mit der Transaktion **SM37** oder über den **Menüpfad** System --> Dienste --> Jobs --> **Job-Übersicht**. Werkzeuge --> Administration --> Jobs --> **Übersicht**

Ein Job kann aus mehreren Steps bestehen.

Man kann zwei Arten von Jobs unterscheiden:

- Einmal-Jobs, die sofort oder gemäß Plan ausgeführt werden sollen,
- Periodische Jobs.

Ein Job wird vom System gestartet, wenn ein definiertes Ereignis eingetreten ist (z.B. ein Zeitpunkt, Ende eines anderen Jobs). Hierdurch ist es möglich, Jobnetze aufzubauen.

Ein Job ist genau in einem der folgenden Zustände:

- eingeplant
- freigegeben
- bereit
- aktiv
- beendet
- abgebrochen.

Im Zusammenhang mit einem SAP-R/3-System stehen folgende Protokolle als Systemprotokolle zur Verfügung:

- Jobprotokolle
- Systemlog
- DB-Log
- Unix-Log bzw. Win/NT-Log
- Workloadprotokoll.

Jobs sind Objekte des Korrektur- und Transportwesens (siehe Kapitel 3).

Eine Job-Bibliothek gibt es bisher nicht.

5.4. Risiken

Neben den allgemeinen Risiken, wie

- unberechtigter (lesender) Zugriff auf Unternehmensdaten und personenbezogene Daten,
- unberechtigte, unkontrollierte, unbemerkte Änderung von Daten und Programmen,
- hohe Ressourcenbelastung durch unsachgemäße Programmzusammenstellung,
- Fehlbedienung, insbesondere im Ausnahmefall (Fehlerbehandlung),
- Abhängigkeit vom Wissen einzelner Personen

gibt es spezielle, mit dem Betriebssystem UNIX zusammenhängende Risiken, wie z.B.

- aus einem SAP-Job heraus können Unix-Programme angestoßen werden, die das SAP-System kopieren oder das SAP-System zerstören,
- System-Passworte sind offen lesbar in Prozeduren hinterlegt,
- Jobs können von Ereignissen außerhalb des SAP-Systems abhängig sein.

5.5. Prüfungen

5.5.1. IST-Aufnahme der Verfahren

Es sind die bestehenden Soll-Vorschriften für

- Job-Auftragsverfahren
 - Job-Dokumentation
 - Erstellung und Behandlung von System-Protokollen
- aufzunehmen und (soweit für die Prüfung erforderlich) zu dokumentieren.

5.5.2. Prüfung der Verfahrenskonzepte

Die zuvor aufgenommenen Soll-Vorschriften sind anhand der oben genannten Anforderungen und Risiken zu prüfen.

5.5.3. Prüfung der Einhaltung der Verfahren

Die Prüfung der Einhaltung der Soll-Vorschriften geschieht durch

- Sichtung der Unterlagen
- Auswertung von Logfiles und Protokollen (Transaktion SM21).

5.6. SAP-Jobdokumentation (Mustervorschlag)

Dies ist ein Mustervorschlag für eine SAP-Jobdokumentation, der jedoch keinen Anspruch auf Vollständigkeit erhebt.

5.6.1. Allgemeines

Verantwortlich für den Inhalt:

Kennung des Jobs:

Kurze Aufgabenbeschreibung:

Ereignis:

Periode:

Geschätzte Laufzeit:

Verarbeitung zum Online-Betrieb sinnvoll:

Programme innerhalb des Jobs:

Besonderheiten des Jobs:

5.6.2. Voraussetzungen für den Jobstart

(Ereignis: siehe oben)

Benötigte Peripherie:

Welche Tabellen/Parameter werden benötigt:

Sonstige Voraussetzungen für den Jobstart:

5.6.3. Erforderliche Nachbearbeitungen nach Joblauf

Benötigte Datenträger/Formulare für den Output:

Folge-Jobs:

5.6.4. Maßnahmen für den Restartfall

Fehler ist direkt zu beheben:

- Fehler beheben
- Wiederanlaufmaßnahme

Fehler ist nicht direkt zu beheben:

- Zurückladen der gesicherten Daten
- Fehlerprotokoll erzeugen
- Benachrichtigung der fachlich Verantwortlichen

Jobname für die Datenrücksetzung:

Welche Jobs dürfen nach Abbruch nicht mehr laufen:

6 Batch-Input-Schnittstellen

6.1. Zielsetzung

Die Anforderungen der §§ 239, Abs.2 HGB und 146, Abs.1 AO, wonach Daten vollständig, richtig, zeitgerecht und geordnet erfaßt, gespeichert und verarbeitet werden müssen und bei Änderungen nicht verfälscht werden dürfen (Anforderungen der §§ 239, Abs.3 HGB und 146, Abs.4 AO), verlangen nach Kontrollen auch im Batch-Input-Verfahren.

6.2. Anforderungen

Voraussetzungen für die Schaffung wirksamer Kontrollen sind:

- Organisation der Arbeitsabläufe,
- Trennung unvereinbarer Funktionen,
- Kontrollmaßnahmen und -instanzen.

Art und Umfang der Organisation der Arbeitsabläufe beeinflussen wesentlich die Wirksamkeit des Internen Kontrollsystems. Dabei muß eine Zwangsläufigkeit in den Abläufen erreicht werden, bei der jedes Verlassen notwendigerweise zu einer Störung führt, die einer Kontrollinstanz auffallen muß.

Ein wirksames Internes Kontrollsystem beinhaltet die Trennung bestimmter Funktionen, wobei zwischen dispositiver, ausführender und überwachender Funktion unterschieden werden sollte.

6.3. SAP-Fakten

6.3.1. Einführung

Batch-Input wird in der Regel eingesetzt, um Daten aus externen Systemen in SAP-Systeme zu übernehmen oder Daten zwischen SAP-Systemen zu übertragen. Für die Datenübertragung verwendet das Ausgangssystem eine Übertragungsschnittstelle, die von einem R/3-Anwendungsprogramm im Zielsystem zur Verfügung gestellt wird. Das Schnittstellenprogramm der Anwendung erzeugt dann eine Batch-Input-Mappe.

Eine Batch-Input-Mappe besteht aus mehreren Transaktionsaufrufen, die durch ein Programm mit Anwenderdaten versehen wurden. Üblicherweise läßt man das System die Transaktionen in einer Mappe ohne weiteren User-Eingriff ausführen. Dadurch kann eine große Datenmenge in kürzester Zeit in das SAP-System eingespielt werden.

Eine Mappe simuliert die Online-Eingabe von Transaktionscodes und Daten. Dabei werden allgemein dieselben Verfahren wie im Dialogbetrieb angewandt.

Die über eine Mappe in die Bildschirmfelder eingegebenen Daten sind denselben Konsistenzprüfungen wie im Dialogbetrieb unterworfen.

Die Batch-Input-Bearbeitung wird über den Menüpfad System --> Dienste --> Batch-Input --> Bearbeiten oder über die Transaktion SM35 erreicht.

Meistens werden BI-Mappen **nichtinteraktiv** gestartet, wobei ein Hintergrund-Job in regelmäßigen Abständen noch nicht abgespielte Mappen startet. Um Batch-Input-Mappen automatisch zu starten, ist das ABAP/4-Programm RSBDCSUB aufzurufen. Das Programm plant Mappen zur sofortigen Hintergrundverarbeitung ein.

Das **interaktive** Abspielen von Mappen beschränkt sich üblicherweise auf das Testen und Korrigieren von Mappen.

6.3.2. Berechtigungen

Grundsätzlich werden Batch-Input-Mappen den üblichen Benutzerberechtigungsprüfungen durch das System unterzogen.

Wenn eine Mappe im **Batch-Modus** abgespielt wird, gelten die Berechtigungen des in der Batch-Input-Mappe angegebenen Benutzers. Der Benutzer muß vom Benutzertyp BDC sein.

Beim **Online-Abspielen** einer Mappe gelten die Berechtigungen des abspielenden Benutzers.

6.3.3. Bearbeitungsarten

Es besteht die Wahl zwischen drei Bearbeitungsarten:

- Unsichtbar
Bei dieser Bearbeitungsart wird eine Mappe sofort verarbeitet.
- Sichtbar abspielen
Fehlerhafte Transaktionen können interaktiv korrigiert und noch nicht ausgeführte Transaktionen stufenweise durchgearbeitet werden.
- Nur Fehler anzeigen
Diese Bearbeitungsart gleicht der Bearbeitungsart "Sichtbar abspielen", außer daß Transaktionen, die noch nicht ausgeführt wurden und keine Fehler enthalten, nichtinteraktiv ablaufen.

Eine Mappe enthält einen Fehler, wenn sie eine Fehlermeldung vom Typ E (Error) oder A (Abbruch) verursacht. Andere Meldungen werden ignoriert und haben keinen Einfluß auf die Verarbeitung einer Mappe.

6.3.4. Protokolle

Zu jeder Batch-Input-Mappe existiert ein Protokoll, das über den Menüpfad System --> Dienste --> Batch-Input --> Bearbeiten --> Protokoll oder mit der Transaktion SM35 angezeigt werden kann. Es enthält alle Fehlermeldungen zu Transaktionen in Mappen. Ein solches Protokoll enthält auch Batch-Input-Fehlermeldungen zu Problemen beim Ablauf von Transaktionen mit dem zugehörigen Transaktionscode und dem Bild, auf dem der Fehler auftrat. Außerdem enthält das Protokoll eine Gesamtstatistik der Mappenverarbeitung.

Ein Protokoll zu einer Batch-Input-Mappe existiert erst, wenn diese Mappe abgespielt, d.h. nach einer der drei vorstehend genannten Bearbeitungsarten bearbeitet wurde. Beim Abspielen einer Mappe werden die fehlerfreien Vorgänge verbucht und die jeweilige Transaktion wird in der Mappe als verarbeitet gekennzeichnet. Vorgänge, die Fehler enthalten, werden nicht verbucht und als fehlerhaft vermerkt. Enthält eine Mappe fehlerhafte Transaktionen, so kann sie wiederholt abgespielt werden, wobei dann nur die als fehlerhaft vermerkten Vorgänge erneut verarbeitet werden.

Zu jedem Abspielvorgang erzeugt das R/3-System ein Protokoll zur Mappe, welches ein bereits existierendes Protokoll überschreibt. Im Protokoll sind nur die Meldungen enthalten, die beim letzten Abspielen aufgetreten sind. Es werden nicht nur Fehlermeldungen protokolliert, sondern auch Verbuchungsmeldungen. Pro verarbeiteter Transaktion erscheint mindestens eine Meldung.

Mit dem Programm **RSBDCREO** können abgespielte Mappen und deren Protokolle sowie Protokolle, zu denen es keine Mappen mehr gibt, gelöscht werden; ferner wird mit dem Report die Protokolldatei des Batch-Input-Systems reorganisiert.

6.3.5. Mappenanalyse

Die Analyse von Batch-Input-Mappen ist vor und nach dem Abspielen möglich. Die Mappe ist in der Mappenübersicht zu markieren. Über den Menüpfad Springen --> Analyse --> Mappe wird die Mappe im Mappenprotokollbild ausgewählt.

6.4. Risiken

Bei von SAP unabhängigen Vorsystemen besteht die Gefahr, daß Plausibilitäten abweichend von den SAP-Tabellen gehandhabt werden. Davon können Stamm- und Bewegungsdaten betroffen sein.

Falls Mappen-Namen nicht plausibilisiert werden, können möglicherweise Batch Input-Berechtigte Mappen anderer (Abteilungen) starten, korrigieren oder löschen (je nach erteilten Berechtigungen).

6.5. Prüfungen

Auf der Basis dieser Kontrollanforderungen sollte der Prüfer folgende Fragen stellen:

Gibt es eine Übersicht über alle Batch-Input-Schnittstellen zu SAP unter Angabe der Spezifikationen, wie

- abgebendes Arbeitsgebiet
- Dateninhalt
- Dateiname
- Periode
- Mappenname
- Verarbeitungsjob
- relevante Tabellen
- Abstimmkreis
- Verantwortlichkeit?

Welche Anwender dürfen welche Mappen erstellen, starten, korrigieren oder löschen? (Menüpfad: Werkzeuge --> Administration --> Benutzerpflege --> Info)

Gibt es eine Übersicht, welche Mappen-Namen für welche Abteilung reserviert sind? (Menüpfad: System --> Dienste --> Batch-Input --> Bearbeiten --> Übersicht oder Transaktion SM35)

Wer stimmt den Buchungsstoff der verarbeiteten Mappen ab?

Wer kontrolliert, daß die Daten aus Vorsystemen vollständig, richtig und zeitgerecht übernommen werden?

Sind die Internen Kontrollen zwischen Vorsystemen und laufendem Abspielen gewahrt?

7 Stammdatenänderungen

7.1. Funktionstrennung

7.1.1. Zielsetzung

Zur Erreichung einer ausreichenden Sicherheit, auch im Sinne eines Internen Kontrollsystems zur Erfüllung der Erfordernisse der GoB, sind bestimmte Funktionstrennungen erforderlich.

Bei kleinen Unternehmen ist dies jedoch organisatorisch oft nicht realisierbar. Deshalb sind hier zur Erreichung eines ausreichenden Sicherheitsstandards besondere - individuell konzipierte - Überprüfungen der Stammdatenänderungen erforderlich. Bei größeren Unternehmen können diese Prüfungen jedoch nicht die durchgehende Funktionstrennung ersetzen.

7.1.2. Anforderungen

Eindeutig festgelegte Zuständigkeiten/Berechtigungen hinsichtlich der Stammdatenverwaltung.

Funktionstrennung in angemessener Form zwischen EDV und Fachabteilung einerseits sowie zwischen Stammdatenpflege und Buchungstätigkeit jeder Art andererseits.

7.1.3. SAP-Fakten

Das SAP-System ermöglicht durch Systemdesign und ein umfangreiches und differenziertes Berechtigungsspektrum die Realisierung angemessener Funktionstrennungen.

Für die **Sachkontenstammdaten** sind Berechtigungen zu vergeben aus der Sicht

- F_SKA1_KTP der Organisationseinheit Kontenplan,
- F_SKA1_BUK der Organisationseinheit Buchungskreis,
- F_SKA1_BES der Gruppierung der Konten nach Berechtigungsgruppen (optional).

Für die **Debitoren- und Kreditorenstammdaten** sind Berechtigungen zu vergeben aus der Sicht

- F_ _APP der Anwendung (Finanzbuchhaltung, Vertrieb oder Einkauf),
- F_ _BUK der Organisationseinheit Buchungskreis,
- F_ _BE . der Gruppierung der Konten nach Berechtigungsgruppen (optional),
- F_ _AEN der Gruppierung einzelner Stammsatzfelder (optional).

Sollen z.B. einzelne Sach-Abschlußkonten speziell geschützt werden, so kann dies durch Vergabe einer 4-stelligen Berechtigungsgruppe, die frei definierbar ist, geschehen (Stammsatz: Feld SKB1-BEGRU Berechtigungsgruppe, Berechtigungsobjekt: F_SKA1_BES Kontenberechtigung).

Über die zur jeweiligen Berechtigung gehörende **Aktivität** wird die mögliche Bearbeitungsfunktion bestimmt:

- Anlegen (01)
- Ändern (02)
- Anzeigen (03)
- Sperren/Entsperren (05)
- Löschen und (06)
- Anzeige von Änderungsbelegen (08)
- Alle Aktivitäten (*)

Die Verschlüsselung der Aktivitäten ist von SAP festgelegt und kann über die Dokumentation des Feldes Aktivität nachgelesen werden.

7.1.4. Risiken

Durch ein unzureichendes Internes Kontrollsystem für die Überwachung von Stammdatenänderungen können sowohl die Ordnungsmäßigkeit als auch die Datensicherheit beeinträchtigt werden. So können z.B. bei mangelnder Sicherheit des Zahlungsverkehrs (Stammdatenpflege) auch Vermögensschäden auftreten.

7.1.5. Prüfungen

Wer hat die Berechtigung zum Anlegen (01) und Ändern (02) von Debitoren-, Kreditoren- und Sachkontenstammdaten?

Sind bei größeren Abteilungen die Berechtigungen für den Zugriff auf die jeweiligen Debitoren-, Kreditoren- oder Sachkonten durch die Kontenberechtigung oder Änderungsberechtigung für bestimmte Felder weiter eingegrenzt?

Wer darf Stammdaten ändern und gleichzeitig buchen?

Bestehen außerhalb des Systems für die Änderung sensibler Stammdaten besondere Genehmigungsverfahren und wird das Vieraugenprinzip gewahrt?

Werden die festgelegten Betragsgrenzen für das Buchen bzw. die festgelegten Toleranzgrenzen für Zahlungsdifferenzen eingehalten (OBA4 / OB57) ?

7.2. Nachvollziehbarkeit

7.2.1. Zielsetzung

Die Nachvollziehbarkeit der Buchhaltung muß in jedem Falle gegeben sein. Die Prinzipien "gebucht ist gebucht" bzw. die Einhaltung des "Radierverbots" sind gemäß den Grundsätzen ordnungsmäßiger Buchführung (GoB) bzw. gemäß §§ 238 f.HGB unbedingt zu gewährleisten.

7.2.2. Anforderungen

Ausreichende Protokollierung, Dokumentation und Aufbewahrung von Stammdatenänderungen und -löschungen.

Hintergrund: Aufzeichnung des Buchungstoffes gemäß GoB über den gesamten Zeitraum der gesetzlichen Aufbewahrungspflicht (§ 257HGB).

In diesem Zusammenhang kommt den **Änderungsbelegen** zentrale Bedeutung zu. Sie dokumentieren Änderungen an Stammsätzen, Belegen, Tabellen, etc. und sind gemäß § 257 HGB aufbewahrungspflichtig und bis zu 10 Jahren zu archivieren.

Um Änderungen zu einem Objekt protokollieren zu können, muß dieses Objekt als **Änderungsbelegobjekt** im System definiert sein. Im Standardsystem wird ein Änderungsbeleg erstellt, sobald ein Feld eines Stammsatzes/Beleges geändert wird.

Diese Vorgabe kann eingeschränkt werden, indem explizit im Data Dictionary festgelegt wird, daß für ein Feld keine Änderungsbelege erstellt werden sollen.

7.2.3. SAP-Fakten

Eine vollständige Aufzeichnung und damit Nachvollziehbarkeit von Änderungen ist grundsätzlich gegeben.

Die Änderungsprotokollierung kann bei Eigenentwicklungen unterlaufen werden.

⇒ Das Berechtigungsobjekt **S_SCD0**
(Basis - Zentrale Funktionen, Änderungsbelege löschen) wirkt
nur für Änderungsbelege nicht buchhalterisch relevanter Daten.

Siehe hierzu: Transaktion SE84 (Repository-Infosystem)

--> Umfeld --> Berechtigungen --> Berechtigungsobjekte

--> Verwendungsnachweis --> Programm/Transaktion

7.2.4. Risiken

- Beeinträchtigung der vollständigen Aufzeichnung des Buchungsstoffes,
- Beeinträchtigung der Ordnungsmäßigkeit.

7.2.5. Prüfungen

Gibt es **Berechtigungen**, die Änderungen im Datenbestand ohne Protokollierung ermöglichen?

Sind für die **Änderungen** von Stammdaten ausreichende Kontrollen vorgesehen und nachvollziehbar durchgeführt?

Die Prüfung der **Änderungsdokumentation** von Stammdaten ist z.B. anhand folgender **ABAP-Reports bzw. Transaktionen möglich**:

- **RFDABL00** Dokumentation der Stammdatenänderungen Debitoren
- **RFKABL00** Dokumentation der Stammdatenänderungen Kreditoren
- **RM06ICD1** Änderungen Einkaufs-Infosatzdaten
- **RSSCD100** Anzeige von Änderungsbelegen
- **FS04** Änderung von Sachkonten
- **MM04** Anzeige von Änderungen Materialstammdaten

Ab Release 3.0:

- **RFBABL00** Stammdaten-Änderungsbelege
- **RFBKABL0** Stammdatenänderungen Banken
- **RFDKLIAB** Stammdatenänderungen Kreditmanagement
- **RFSABL00** Stammdatenänderungen Sachkonten

8 Abstimmung Buchungsstoff und Abschlüsse

8.1. Zielsetzung

Der Kaufmann ist nach §§ 238, Abs. 1 HGB und 140 AO verpflichtet, Bücher zu führen und die dafür geltenden Vorschriften einzuhalten. Werden Buchführungsaufgaben auf die Datenverarbeitung übertragen, so hat der Kaufmann dafür zu sorgen, daß die Datenverarbeitung die Vorschriften in gleicher Weise einhält.

Die Fachabteilung oder der für den Buchungsstoff Verantwortliche hat also die Verarbeitungsergebnisse zu überwachen. Die Kontrollziele sind dabei die Eigenschaften

- vollständig
- echt
- richtig bewertet
- periodenrichtig
- richtig kontiert
- korrekt summiert
- korrekt gebucht.

Eine Buchführung gilt als ordnungsgemäß, wenn ein sachverständiger Dritter sich in angemessener Zeit einen Überblick über die Geschäftsvorfälle und die Lage des Unternehmens verschaffen kann. Die Geschäftsvorfälle müssen sich dabei in ihrer Entstehung und Abwicklung verfolgen lassen.

Die Grundfunktionen einer Buchführung umfassen in der Regel folgende Bücher und Nachweise:

- Eröffnungsbilanz
- Belegsammlung
- Grundbuch
- Hauptbuch
- Inventar
- Bilanz mit Gewinn- und Verlustrechnung.

8.2. Anforderungen

Die formellen Anforderungen zum Aufbau der Buchführung ergeben sich u.a. aus §§ 238 bis 241 HGB, §§ 257-261 HGB und §§ 140 bis 147 AO. Als Bedingung für die Ordnungsmäßigkeit ist dabei festgelegt, daß auch die automatisch verarbeitete bzw. gespeicherte Buchführung die Funktionen Belegsammlung, Grundbuch und Hauptbuch beachten muß, und diese Daten Aufbewahrungsfristen von in Deutschland sechs bzw. zehn Jahren unterliegen - unabhängig davon, ob der Buchungsnachweis ausgedruckt wird oder nicht.

Unabhängig vom Integrationsgrad der SAP-Anwendungen muß unter dem Aspekt der Vollständigkeit jederzeit die Möglichkeit bestehen, den verarbeiteten Buchungsstoff abzustimmen. SAP bietet hierzu Verarbeitungskontrollen, die auf verschiedenen Ebenen der Anwendung installiert sind. Präventive und detektive Kontrollen müssen sich dabei ergänzen.

Um die Grundforderung der GoB erfüllen zu können, müssen die aufzeichnungspflichtigen Geschäftsvorfälle vollständig, richtig, zeitgerecht und geordnet sowie nachvollziehbar und prüfbar festgehalten werden. In einem integrierten System beschränken sich diese Forderungen nicht allein auf die buchungsrelevanten Vorgänge. Die Tabellen, die steuernd in ein solches System eingreifen, sowie die Datensicherheit und die Datensicherung sind in diese Anforderungen mit einzubeziehen.

Die Kontrollen des Tages- bzw. des Monatsabschlusses müssen in der Prozedur für den Jahresabschluß enthalten sein. Darüber hinaus sind noch Kontrollen für die sogenannten Einmalarbeiten erforderlich. Insbesondere für diese Arbeiten müssen die Zuständigkeiten und Verantwortlichkeiten klar geregelt sein.

Der Buchungsstoff muß dokumentiert werden. Dies kann durch Ausdruck oder Verfilmung des Journals und der Konten geschehen.

8.3. SAP-Fakten

8.3.1. Abstimmung des Buchungsstoffes

Die Erfassung von Originalbelegen kann in Belegmappen erfolgen. Jede Mappe ist mit Kontrollsummen versehen, z.B. Anzahl Belege, Summe Soll/Debitoren etc. Das System FI führt einen Kontrollsummen-Speicher je Benutzer (FB07), so daß ein Vergleich mit der vorgegebenen Kontrollsumme möglich ist.

Die Belegspeicherung garantiert, daß der Saldo aller Buchungen Null bleibt. Dies ist durch die Bilanz- und GuV-Programme jederzeit nachprüfbar.

Die Auswertung der Buchungssummen kann nachträglich über den Report RFBUSU00 erfolgen.

Die Belegnummer ist eindeutig einem Beleg zugeordnet. Bei der Belegnummernvergabe durch das System (Transaktion FBN1/Tabelle INRDP) wird eine lückenlose Numerierung vorgenommen, bei extern vergebenen Belegnummern wird auf Doppelbelegung geprüft.

In Verbindung mit dem Einsatz des SAP-Moduls MM kann es in der Finanzbuchhaltung u. U. zu einer lückenhaften Vergabe von Belegnummern kommen. Über die Transaktion SNR0 ist die Anzahl der gepufferten Belegnummern einstellbar.

Werden abwechselnd von unterschiedlichen Applikationsservern aus Belege gebucht, vergibt jeder Applikationsserver die nächste freie Belegnummer aus seinem Nummernkreispufer. Dadurch werden die Belegnummern nicht in der Reihenfolge des Entstehens der Belege vergeben.

Beim Puffern wird die letzte gepufferte Nummer als letzte vergebene Nummer des Nummernkreisintervalls hochgezählt. Wird das SAP-System heruntergefahren, gehen so die gepufferten, aber noch nicht vergebenen Belegnummern verloren. Bei nächsten Hochfahren des Systems werden nämlich entsprechend der letzten vergebenen Belegnummer des Nummernkreisintervalls die nächsten Belegnummern gepuffert. Dadurch können Lücken in der Belegnummernvergabe entstehen.

Die Dokumentation aller Belege eines ausgewählten Zeitraums erfolgt im Belegkompakt-Journal **RFBELJ00**. Der Summenbericht des RFBELJ00 weist die Abstim-Summenblätter aus. Diese Abstimmsummen müssen manuell in eine Liste übertragen und dort mit den Zahlen der Vorträge kumuliert werden.

Zur Abstimmung der Buchhaltung ist die "**Große Umsatzprobe**" vorzunehmen. Sie dokumentiert, daß alle Verkehrszahlen durch entsprechende Belege erklärt werden. Hierfür steht der Report *SAPF190 'Abstimmanalyse Finanzbuchhaltung'* zur Verfügung.

Abstimmung der Sachkontenbuchungen

Die Abstimmung der Sachkonten erfolgt an Hand der Kontenschreibung. Hierzu sind die Listen der Berichte **RFHABU00** 'Hauptbuch aus der Belegdatei' oder **RFKLBU10** 'Niederschrift aus kumulierter klassischer Kontenschreibung' mit der Sachkonten-Saldenliste **RFSSLD00** abzugleichen.

Abstimmung des Kontokorrents

Die Abstimmung des Kontokorrents erfolgt durch Abgleich der Debitoren- und Kreditoren-Saldenlisten **RFDSL00** bzw. **RFKSLD00** mit den Listen aus der Kontokorrent- oder der klassischen Kontenschreibung.

- Kontokorrent-Kontenschreibung: **RFKKBU00** oder **RFKKBU10**
- Klassische Kontenschreibung: **RFHABU00** oder **RFKLBU9**.

Weitere Abstimmungs-Reports sind über den Pfad "System --> Dienste --> Reporting" mit der Eingabe RF* erhältlich. Insbesondere der Report **RFBPET00** 'Belegpositionen-Extrakt' bietet sich für Abstimmarbeiten auf Belegebene an.

8.3.2. Periodenabschluss

Die zentrale Aufgabe der Hauptbuchhaltung ist die Gesamtdarstellung des externen Rechnungswesens und damit der Konten. Die Aufnahme und Sammlung aller Geschäftsvorfälle (Primärbuchungen, Abrechnungen aus dem internen Rechnungswesen) in einem betriebswirtschaftlich integrierten Softwaresystem garantiert, daß die Kontenführung zu definierten Zeitpunkten vollständig und abgestimmt ist.

Das Hauptbuch des Systems FI bietet folgende Funktionen:

- die freie Wahl der Kontengliederung auf Konzern- oder Firmenebene,
- das automatische Mitbuchen aller Posten der Nebenbücher in der Hauptbuchhaltung (Abstimmkonten),
- das periodengleiche Fortschreiben des Hauptbuchs und der Werte der Kostenrechnungsbereiche,
- das zeitnahe Auswerten und Berichten des aktuellen Buchungsstoffes in Form von Kontendarstellungen, Ergebnisrechnungen mit unterschiedlichen Bilanzversionen und Zusatzanalysen.

Die Nachweise der einzelnen Vorgänge sind über Belege, Einzelposten und Verkehrszahlen auf unterschiedlichen Ebenen, wie

- der Kontenführung,
- der Journalschreibung,
- der Summen-/Saldenverkehrszahlen,
- der Bilanz-/GuV-Auswertungen
online zu jedem Zeitpunkt verfügbar.

Schwerpunktmäßig dient das Hauptbuch vor allem während des laufenden Geschäftsjahres

- als kontinuierliche und zentrale Sammel-, Abstimm- und Dokumentationsfunktion des gesamten Buchungsstoffes,
- als Basis einer beliebig strukturierbaren bzw. fallweisen Berichts- und Analysesystems (z.B. Verkehrszahlen je Konto, Einzelbelegnachweis) und
- als ein jederzeit abrufbares Abschlußsystem in Form von Tages- und/oder Monatsabschlüssen.

8.3.2.1. **Tagesabschluß**

Systemseitig bestehen keinerlei Zwänge für tagesbezogene Abschlußarbeiten.

IKS-konforme Kontrollen können durch das regelmäßige Erstellen und Prüfen der folgenden Auswertungen erreicht werden:

- | | |
|--------------------------------|----------|
| - Belegjournal | RFBELJ00 |
| - Buchungssummen | RFBUSU00 |
| - Abgebrochene Verbuchungen | RFVBER00 |
| - Anzeige von Änderungsbelegen | RSSCD150 |
| - Korrespondenz | SAPF140 |

Die tagesbezogenen Auswertungen liegen somit im Ermessen des Anwenders.

8.3.2.2. Monatsabschluß

Die Arbeiten im Rahmen des Monatsabschlusses sind unter anderem abhängig von der Ausprägung der Datenstruktur (Geschäftsbereiche, Profitcenter...). Grundsätzlich sollte wie folgt vorgegangen werden:

- Sperren des alten Monats,
- Abstimmung Belege/Verkehrszahlen,
- Erstellung der erforderlichen Auswertungen zur Dokumentation des Buchungsstoffes,
- Erstellung der Umsatzsteuer-Voranmeldung,
- Abstimmung der Buchhaltung.

Das Belegjournal RFBELJ00 hat die Funktion des Grundbuches.

Die Abstimmung des Buchungsstoffes kann wie im Kap. 8 beschrieben erfolgen.

Die kumulierte Kontenschreibung muß vor der Belegarchivierung erfolgen.

Die Sequenz, in der die Belegarchivierung durchgeführt werden muß, ist abhängig von der verfügbaren Speicherkapazität der EDV-Anlagen und vom Belegvolumen.

Buchungsperioden

Die Buchungsperioden sind in Abhängigkeit von der Geschäftsjahres-Variante je Buchungskreis zu pflegen. R/3 kennt 12 Buchungsperioden für den laufenden Buchungsstoff sowie 4 zusätzliche Buchungsperioden im Zusammenhang mit Abschlußarbeiten.

Über den Buchungskreis hinaus können für einzelne Konten bzw. Kontengruppen abweichende Perioden definiert werden.

8.3.2.3. **Jahresabschluß**

Der Jahresabschluß kann auf einem Montasabschluß aufbauen, dies ist allerdings nicht zwingende Voraussetzung. Eine Reihe abschlußspezifischer Programme bereitet die gebuchten Einzelposten und Konten für den Jahresabschluß auf. Wichtige Schritte bei der Abschlußvorbereitung sind:

- das Abschließen der Buchungsperiode,
- die Bewertung von Einzelposten und Hauptbuchkonten in Fremdwährungen,
- die Ermittlung debitorischer Kreditoren bzw. kreditorischer Debitoren,
- das Buchen von Umbewertungen, Korrekturen und Abgrenzungen,
- die Abstimmung der Nebenbuchhaltungen und Vorsysteme.

Die Abschlußarbeiten werden durch eine Reihe von realtimegestützten Reports unterstützt, wie:

- Abstimmung der Belege mit den Verkehrszahlen,
- Buchungssummen,
- Kontokorrentschreibung,
- Vortragen der Bestandskontensalden mit mehrfachem Übertrag auch nach Beginn des neuen Geschäftsjahres.

Alle Berichte sind jederzeit aktuell im Dialog abrufbar.

8.3.2.3.1. Bilanz und Gewinn- und Verlustrechnung

Das Ausdrucken der Bilanz und der GuV erfolgt ausschließlich über ABAP. Standardmäßig steht der Bericht **RFBILA00** zur Verfügung.

Die Liste beinhaltet Ergebnisrechnungen (Bilanz und GuV) für einen beliebigen Berichtszeitraum innerhalb eines Geschäftsjahres mit absoluten und relativen Vergleichen zu einer Vergleichsperiode.

Der Aufbau der Ergebnisrechnungen ist abhängig von dem für den Buchungskreis gewählten Kontenplan (Tabelle T004/Transaktion OB13).

8.3.2.3.2. Saldovortrag

Ein neues Geschäftsjahr wird mit der ersten Buchung in das Geschäftsjahr eröffnet. Dazu muß die entsprechende Buchungsperiode geöffnet sein.

Der Saldovortrag wird im SAP-System mit Hilfe von Reports (SAPF010 für das Kontokorrent, SAPF011 für das Hauptbuch) vorgenommen. Dabei werden die GuV-Konten auf das Ergebnisvortragskonto bzw. auf die Ergebnisvortragskonten, die Bestandskonten auf sich selbst vorgetragen. Eine spezielle Eröffnungsbilanz ist nicht erforderlich.

Buchungen in das alte Geschäftsjahr führen automatisch zur Korrektur des Saldovortrags. Damit muß das alte Geschäftsjahr nicht geschlossen werden und die Abschlußbuchungen müssen noch nicht durchgeführt worden sein, um das neue Geschäftsjahr zu eröffnen.

Wird der Saldovortrag am Ende eines Geschäftsjahres vorgenommen, führen Buchungen in das alte Geschäftsjahr nicht zur Korrektur des Saldovortrags, da Buchungen in das alte Geschäftsjahr nicht als solche interpretiert werden.

8.3.2.3.3. Reorganisation/Archivierung

Daten, die im Online-System nicht mehr benötigt werden, können mit speziellen Standardfunktionen archiviert werden (z.B. im Finanzbereich über den Menüpfad Finanzwesen --> Hauptbuch --> Period.Arbeiten --> Archivierung oder über die Transaktion F045). Die im Online verbleibenden Daten werden dabei reorganisiert. Für das Archivieren der Daten müssen Bedingungen erfüllt sein, die z.T. vom System vorgegeben sind. Der Anwender kann darüber hinaus weitere Bedingungen definieren, z.B. die Laufzeit für Konten und Belege (über den Menüpfad Customizing --> Einstellungsmenü Buchhaltung --> Werkzeuge --> Archivierung oder mit den Transaktionen OBR7 bzw. OBR8).

Das Archivieren ist für folgende Objekte möglich:

- Buchhaltungsbelege,
- Verkehrszahlen,
- Schecks,
- Stammdaten von Debitoren-, Kreditoren- und Sachkonten,
- Bankenstammdaten,
- Index Beleg/Archiv.

Aus gesetzlichen und betriebsinternen Gründen ist es erforderlich, die in den Archivdateien ausgelagerten Daten unter bestimmten Umständen zu einem späteren Zeitpunkt wieder verfügbar machen zu können. Dies kann u.a. durch Rückladen der Daten erreicht werden.

Das Rückladen ist für folgende Objekte möglich:

- Buchhaltungsbelege,
- Verkehrszahlen,
- Schecks,
- Sachkontenstammdaten,
- Bankenstammdaten,
- Index Beleg/Archiv.

Für Debitoren und Kreditoren wird keine Notwendigkeit gesehen, die Stammdaten rückzuladen.

8.4. Risiken

Wird der Buchungsstoff nicht zeitnah, d.h. monatlich, abgestimmt, besteht das Risiko, daß Fehler auftreten und für längere Zeit unerkannt bleiben. Dies bedeutet insbesondere für die Jahresabschlußarbeiten unter Umständen eine bedeutende Erschwernis. Die Folge kann ferner sein, daß dem Management eine fehlerhafte Entscheidungsbasis zur Verfügung gestellt wird, die zu irreparablen Fehlentscheidungen führen kann.

Weiterhin besteht das Risiko, daß die Fehlerursache nicht erkannt oder der Fehlerursprung nicht lokalisiert wird, sodaß Wiederholungsfehler nicht ausgeschlossen werden und damit die Ordnungsmäßigkeit der Buchhaltung gefährdet ist.

Neben dem Fehlerrisiko, das mit einer nicht zeitnahen Abstimmung verbunden ist, treten beim Monatsabschluß weitere Risiken hinzu, die durch systemübergreifende Kontrollen ausgeschaltet werden müssen. So kann es bei nicht exakter Periodenabgrenzung zu Unstimmigkeiten zwischen Hauptbuch und Nebenbuchhaltungen kommen. Nachfolgende Auswertungen für steuerliche Zwecke oder Vertriebsstatistiken greifen auf eine unstimmige Datenbasis zu. Bei ungenügender Sicherungsorganisation wird im Fehlerfall die Rekonstruktion der Ausgangsdaten erschwert.

Risiken im Zusammenhang mit Bilanz und GuV können sich vor allem durch die Art der in den einzelnen Jahresabschlußposten zusammengefaßten Konten ergeben. Entsprechen die Zuordnungen nicht den formellen Anforderungen, kann der Abschluß verworfen werden. Unvollständige Daten bergen die Gefahr der Fehlinformation für das Management.

Nichtbeachten der Gliederungsvorschriften und der Aufbewahrungsfristen kann zu gerichtlichen Konsequenzen führen (§§ 331-335 HGB).

Bei falscher Handhabung des Saldovortrags kann die Bilanzkontinuität verlorengehen; es besteht außerdem die Gefahr der Bilanzmanipulation.

Bei Änderung der Belegnummernkreise kann das Archiv in der Form betroffen sein, daß ein Rückladen von Objekten nicht mehr möglich ist.

8.5. Prüfungen

8.5.1. Abstimmung

Auf der Basis dieser Kontrollanforderungen ergeben sich für den Prüfer u.a. folgende Fragen:

In welchen Abständen und durch wen werden die Buchungen kontrolliert?

Wird die "Große Umsatzprobe" regelmäßig durchgeführt?

Gab es dabei Unstimmigkeiten, wie wurden sie behandelt?

Ist sichergestellt, daß bei Releasewechseln die Endsaldenlisten des alten Releasestandes mit den Anfangssaldenlisten des neuen Releasestandes übereinstimmen und entsprechend dokumentiert werden?

Liegen Kenntnisse über Systemabbrüche vor?

Wird in Verbindung mit anderen SAP-Modulen bei der Vergabe von Belegnummern mit Pufferung gearbeitet (Transaktion SNR0, Nummernkreisobjekt MATBELEG)?

Prüfen Sie die **Selektionskriterien** für die **ABAPs** der Großen Umsatzprobe. Es ist zu empfehlen, in mandanteneigenen Varianten fixe Selektionskriterien der Reports

- RFBELJ00
- RFDSL00
- RFKSLD00
- RFSSL00

zu hinterlegen.

Die Abstimmreports sind jeweils innerhalb des Rechnungswesens für den Bereich Hauptbuch im Pfad "Period. Arbeiten --> Monatsabschluß --> Abstimmung", für die Bereiche Debitoren und Kreditoren im Pfad "Period. Arbeiten --> Reporting --> Saldenliste" hinterlegt.

Hierbei ist zu beachten, daß als zeitliches Abgrenzungskriterium ein einheitliches CPU-Datum gewählt wird.

8.5.2. **Periodenabschluß**

Folgende Fragen sind u.a. zur Beurteilung der Kontrollen von Wichtigkeit:

Wer ist für die Durchführung des Monatsabschlusses verantwortlich?

Wie erfolgten die Regelungen für die Durchführung des Abschlusses unter dem Aspekt der Funktionstrennung zwischen Fachbereich und Informatikbereich?

Durch welche Maßnahmen wird eine Zwangsläufigkeit in den Abläufen garantiert?

Gibt es Regelungen für ein Fehlermanagement?

Sind die Benutzerprofile unter dem Aspekt der Funktionstrennung entsprechend eingerichtet (**Transaktion SU02**)?

Werden alle aufbewahrungspflichtigen Unterlagen erstellt?

8.5.3. **Jahresabschluß**

Für den Prüfer ergeben sich dieselben Fragestellungen wie zum Monatsabschluß; sie müssen jedoch um die spezifischen Probleme des Jahresabschlusses ergänzt werden, die sich mit dem Bilanzausweis, der Dokumentation des Buchungsstoffes und den aufbewahrungspflichtigen Unterlagen befassen.

Aus den vergebenen Benutzerprofilen (Werkzeuge --> Administration --> Benutzerpflege) muß sich die Verantwortlichkeit für den Jahresabschluß, die Periodenabgrenzung und für die Sachkontendefinition ableiten lassen.

Das Verfahren der Durchführung des Saldovortrags sowie die Saldovorträge selbst sind zu prüfen.

Ferner ist zu prüfen, ob während des Jahres Änderungen an den Belegnummernkreisen vorgenommen wurden, die sich auf das Archiv auswirken (Transaktion FBN1).

9 Rechnungsprüfung und Zahlungslauf

9.1. Zielsetzung

In diesem Kapitel wird die Rechnungsprüfung und der Zahlungslauf aus Sicht des Moduls Finanzbuchhaltung behandelt. Die für diesen Bereich wichtigen Anforderungen an die Kreditorenstammdatenverwaltung werden in der Betrachtung berücksichtigt, wobei für die Gewährleistung der Ordnungsmäßigkeitsanforderungen auf den im Kapitel 7 beschriebenen Stammdatenänderungsdienst verwiesen wird.

Nicht eingegangen wird auf die Logistik-Rechnungsprüfung im Rahmen der SAP R/3-MM-Materialwirtschaft, die eine maschinelle Prüfung durch den systemseitigen Abgleich von Bestellung, Wareneingang und Rechnung ermöglicht.

Zur Gewährleistung einer ausreichenden Ablaufsicherheit und zur Sicherstellung eines wirksamen internen Kontrollsystems sind organisatorisch vor- und nachgelagerte Überwachungskontrollen und eine angemessene Funktionstrennung in den Bereichen Kreditorenstammdatenverwaltung, Rechnungsprüfung und Zahlungslauf erforderlich. Der Umfang dieser vor- und nachgelagerten Kontrollen ist von der individuellen Unternehmensgröße und der Komplexität der Verarbeitung der Geschäftsvorfälle abhängig. Die SAP-seitige Berechtigungsvergabe, deren Basis ein unternehmensspezifisches Berechtigungskonzept ist, kann dort auf mehreren Ebenen wirksame Unterstützung bieten.

9.2. Anforderungen

Voraussetzung für die richtige Be- und Verarbeitung von Bewegungsdaten innerhalb der betrieblichen Funktionen (z.B. Rechnungsprüfung, Zahlungsausgleich) sind vollständige, konsistente und aktuelle Kreditorenstammdaten. Insbesondere bei Einsatz des Moduls Materialwirtschaft sollte die abteilungsspezifische Zuständigkeit für das Anlegen und die Pflege der Stammsätze zwischen Buchhaltung und Einkauf eindeutig geregelt sein, um Inkonsistenz und Redundanz zu vermeiden.

Der Zugriff auf Stammdaten sollte personell von dem auf Bewegungsdaten getrennt sein. Zahlungsrelevante Stammdatenfelder (wie Angabe der Bankverbindung) sollten nach dem Vier-Augen-Prinzip oder durch weitere nachgelagerte kompensierende Kontrollen überwacht werden. In diesem Zusammenhang sollte die Anzahl der CpD-Konten auf ein Minimum reduziert und gesondert überwacht werden.

Aus Ordnungsmäßigkeitsgründen ist der vollständige und richtige Ausweis der Forderungen und Verbindlichkeiten vorgeschrieben. Eingehende Rechnungen müssen daher zeitgerecht erfaßt werden. Sie sind zu prüfen, ob sie sich mit Bestellung und Wareneingang oder Dienstleistung in Übereinstimmung befinden. Es dürfen nur Rechnungen bezahlt werden, die bestellte und gelieferte Waren oder Dienstleistungen in der richtigen Menge zu den vereinbarten Konditionen ausweisen. Toleranzen für Abweichungen sind zulässig und systemseitig einstellbar.

SAP R/3 bietet die Möglichkeit der Belegvorerfassung an (Ersatz für ein Rechnungseingangsbuch), sofern die Rechnungen aufgrund noch nicht erfolgter Prüfungen nicht zeitnah gebucht werden sollen.

Die Bezahlung soll zeitgerecht und unter Wahrung von Skontofristen erfolgen. Für Geldabflüsse ist das Vier-Augen-Prinzip einzuhalten. Dies kann entweder durch die Kontrolle von Zahlungsvorschlagslisten oder durch ein angemessenes internes Kontrollsystem bei der Stammdatenverwaltung und Rechnungsfreigabe realisiert werden. Der Transfer der Überweisungsdatenbestände zu den Banken ist vor Manipulationen zu schützen und zu dokumentieren.

9.3. SAP-Fakten

9.3.1. Kreditorenstammdaten

Für die ordnungsgemäße Buchung der Rechnungen werden aus der Stammdatei entsprechende Vorgaben bereitgestellt (Name, Adresse, Bankverbindung, Zahlungsbedingungen, Zahlwege sowie Kontosteuerungsdaten).

Für Kreditoren mit einmaliger oder seltener Rechnungsstellung kennt das System den Stammsatz für CpD-Konten. Dort werden keine kundenspezifischen Daten gespeichert, da das Konto für mehrere Kreditoren genutzt wird. Die spezifischen Daten müssen bei der Rechnungserfassung eingegeben werden.

9.3.2. Besondere Felder

Die folgenden Felder in den Kreditorenstammsätzen haben eine spezielle Funktion:

9.3.2.1. Abweichender Zahlungsempfänger

Das Zahlungsprogramm kann Zahlungen an einen Kreditor leisten, der nicht mit dem Kreditor übereinstimmt, auf dessen Konto die Rechnung gebucht wurde. Die Zahlung wird an einen abweichenden Zahlungsempfänger geleistet. Dieser Empfänger muß im allgemeinen oder im buchungskreisspezifischen Bereich des Stammsatzes eingegeben sein. Sind in beiden Bereichen Eingaben vorhanden, hat der Eintrag im Buchungskreis Vorrang. Das Zahlungsprogramm ruft dann den Namen und die Anschrift des abweichenden Zahlungsempfängers bei der Verarbeitung von Zahlungen für das betreffende Kreditorenkonto ab.

Zudem ist es möglich, den Zahlungsempfänger erst in den Beleg (Voraussetzung: Markieren des Feldes *Zahlempfg.in Beleg*) einzugeben. Beim Erfassen eines Belegs steht dann ein Feld für die Eingabe eines abweichenden Zahlungsempfängers zur Verfügung.

9.3.2.2. Verbundene Unternehmen

Werden Rechnungen an ein verbundenes Unternehmen gestellt, so müssen diese bei einer Konzernkonsolidierung berücksichtigt werden. Das heißt, alle Umsätze, die durch Geschäftsvorfälle innerhalb des Konzerns gemacht wurden, müssen eliminiert werden (Binnenumsatzeliminierung). Voraussetzung für ihre Vornahme ist, daß in das Feld **Part. Gesell** im Kreditorenstammsatz jedes verbundenen Unternehmens eine konzernweit einheitliche Unternehmensnummer eingegeben ist. Anhand dieser Nummer kann das Konsolidierungssystem die Binnenumsätze für die Konsolidierung erkennen.

9.3.2.3. **Verrechnung zwischen Kreditor und Debitor**

Wenn ein Geschäftspartner als Kreditor und Debitor geführt wird, können die offenen Posten durch das Zahlungs- und das Mahnprogramm miteinander verrechnet werden.

Eine Verrechnung ist aber nur möglich, wenn:

1. Ein Debitorenstammsatz für den Debitor angelegt ist, der gleichzeitig auch als Kreditor geführt wird.
2. Im Steuerungsbereich der allgemeinen Daten des Kreditorenstammsatzes die Kontonummer des Debtors im Feld Debitor und analog im Debitorenstammsatz die Kontonummer des Kreditors im Feld Kreditor eingegeben ist
3. In den Buchungskreisdaten im Debitoren- und im Kreditorenstammsatz das Feld *Verr.mit Debi* bzw. *Verr.mit Kred.* markiert wird. Jeder Buchungskreis kann somit separat entscheiden, ob für den Debitor eine Verrechnung mit dem Kreditor gewünscht ist.

9.3.3. Belegvorerfassung

Mit der Belegvorerfassung können Rechnungen ohne umfangreiche Eingabeprüfungen vorerfaßt und geparkt werden. Ein vorerfaßter Beleg kann geändert und schrittweise vervollständigt werden. Dabei sind viele Kopf- und Positionsfelder änderbar. Die systeminternen Änderungsregeln der Belegerfassung werden nicht verwendet. Änderungen an vorerfaßten Belegen werden protokolliert und können vor und nach dem Buchen angezeigt werden.

Die Belegnummer eines gelöschten vorerfaßten Belegs kann nicht wiederverwendet werden.

Ein vorerfaßter Beleg kann einzeln oder über eine Listenauswahl gebucht werden. Das System gibt eine Liste aus, die anzeigt, ob die Belege erfolgreich gebucht wurden. Nicht gebuchte Belege können aus dieser Liste nachbearbeitet werden.

Wird ein vorerfaßter Beleg gebucht, so werden die Daten dieses vorerfaßten Beleges gelöscht, ein Beleg wird auf die Belegdatenbank geschrieben und die entsprechenden Daten (Verkehrszahlen) fortgeschrieben. Die Belegnummer wird in den gebuchten Beleg übernommen.

9.3.4. Rechnungen im Nettoverfahren buchen

Einige Kreditorenrechnungen müssen netto buchbar sein; das ist z.B. beim Erwerb von Anlagevermögen oder beim Kauf von Rohstoffen der Fall. D.h. bei einer Rechnungsbuchung im Nettoverfahren geht man davon aus, daß Skonto einbehalten wird. Die Rechnung ist dann noch nicht bezahlt, und das System subtrahiert den Skonto automatisch vom Aufwand. Diese Vorgehensweise ist für die Erfassung des Erwerbs von Eigentum, Anlagen und Ausrüstungsgegenständen typisch: Auf Aufwands- oder Bestandskonten wird jeweils der um den Skonto verminderte Betrag (Nettobetrag) ausgewiesen.

Wenn Rechnungen im Nettoverfahren gebucht werden, muß eine 'Netto-Belegart' verwendet werden. In den Systemeinstellungen müssen die Konten, Regeln und Buchungsschlüssel für die automatische Buchung der Skontodifferenz eingestellt sein.

9.3.5. Betragsgrenzen und Toleranzen

Zusätzlich zu den Buchungsberechtigungen können Betragsgrenzen für das Buchen von Belegen und Belegpositionen und Toleranzgrenzen für Skonti und Zahlungsdifferenzen festgelegt werden. Diese Festlegungen können auch abhängig von den Geschäftspartnern getroffen werden. Beim Buchen wirken sich beide Festlegungen aus. Die jeweils engeren Grenzen sind gültig.

Beispiele zu Betragsgrenzen für das Buchen

- bis zu welchem Betrag darf der Mitarbeiter einen Beleg buchen?
- bis zu welchem Betrag darf er eine Belegposition auf einem Debitoren- oder Kreditorenkonto erfassen?
- wieviel Prozent Skonto darf der Mitarbeiter in einer Belegposition gewähren?
- bis zu welcher Höhe werden Zahlungsdifferenzen akzeptiert?

Die Toleranz- und Betragsangaben sind buchungskreisabhängig. Dadurch ist es möglich, für gleiche Mitarbeitergruppen unterschiedliche buchungskreispezifische Toleranzen festzulegen. Wird keine Gruppe angegeben, gelten die dazu definierten Toleranzen für alle Mitarbeiter, die keiner Gruppe zugeordnet sind.

Beispiele zu Toleranzen für Zahlungsdifferenzen:

Zahlungsdifferenzen innerhalb bestimmter Toleranzgrenzen werden automatisch gebucht. Dazu kann das System die Differenz über eine Korrektur des Skontos oder auf ein separates Aufwands- oder Ertragskonto buchen.

Über Toleranzgrenzen wird festgelegt, wie das System die Differenzen buchen soll. Z.B, bis zu welchen Beträgen oder Prozentsätzen bucht das System automatisch auf ein separates Aufwands- oder Ertragskonto, wenn eine Korrektur des Skontos nicht möglich ist?

Differenzbeträgen korrigiert das System den Skonto? Der Skonto wird in diesem Fall automatisch um die Differenz erhöht oder vermindert.

9.3.6. Zahlungsprogramm

Das Zahlungsprogramm ist so ausgelegt, daß sowohl Ausgangs- als auch Eingangszahlungen abgewickelt werden können. Diese Funktionen sind gleichermaßen für Kreditoren und Debitoren unterstützt. Das Programm erzeugt Zahlungsbelege und stellt die Daten für die Zahlungsträgerprogramme bereit. Es druckt Zahlungslisten, Zahlungsformulare (z.B. Schecks) oder erstellt Datenträger (Disketten, Magnetbänder).

Das Zahlungsprogramm ermittelt die offenen Posten und wählt aus, welche Posten gezahlt werden müssen. Grundsätzlich zahlt es Posten so spät wie möglich, ohne Skontoverlust. Der genaue Zeitpunkt der Zahlung wird durch die Konfiguration des Zahlungsprogramms bestimmt.

Die Fälligkeit der Posten wird grundsätzlich bestimmt durch das Basisdatum und die Zahlungsbedingungen, die in den offenen Posten stehen.

Das Zahlungsprogramm ermittelt die Skontofristen und die Nettofälligkeit.

Bei der Konfiguration können buchungskreisspezifisch Toleranztage bei Verbindlichkeiten festgelegt werden. Die Toleranztage werden auf die ermittelten Zahlungsfristen addiert. Die Zahlung kann dadurch später erfolgen.

Es kann buchungskreisspezifisch ein Mindestskontoprozentsatz für Ausgangszahlungen festgelegt werden. Kann der angegebene Mindestprozentsatz nicht erreicht werden, wird zur Nettofälligkeit gezahlt. Der Mindestskontoprozentsatz wird verwendet, wenn die Nettobedingung vorteilhafter ist als eine mögliche Skontobedingung. Ist kein Mindestsatz angegeben, zahlt das Programm mit dem jeweils höchstmöglichen Skonto.

Außerdem können im Rahmen der Konfigurierung bestimmte Sonderhauptbuchvorgänge, z.B. Anzahlungsanforderungen oder Zahlungsanforderungen als zu regulierende Vorgänge angegeben sein.

Vor jedem Zahllauf ist das Datum des nächsten Zahllaufs anzugeben. Anhand dieser Angabe entscheidet das Programm, ob ein Posten im aktuellen oder im nächsten Zahllauf berücksichtigt werden muß.

Bei der Erfassung der Zahlungsparameter kann die Berechtigung zur Änderung der Zahlungsparameter auf bestimmte Benutzer eingeschränkt werden.

9.3.7. Berechtigungen

Relevante Berechtigungen für die Prüfungen sind:

9.3.7.1. Debitoren- und Kreditorenstammdaten

Für die Kreditorenstammdaten können Berechtigungen vergeben werden aus der Sicht der Anwendung (Finanzbuchhaltung oder Einkauf), der Organisationseinheit Buchungskreis, der einzelnen Stammsätze und der einzelnen Stammsatzfelder. Die zugelassenen Aktivitäten sind aus der Tabelle TACTZ zu entnehmen.

Berechtigungsobjekte im einzelnen:

Generelle Pflegeberechtigung für Debitoren- oder Kreditorenstammdaten (Anwendungsberechtigung)

Debitorenstammdaten: F_KNA1_APP

Kreditorenstammdaten: F_LFA1_APP

Berechtigungsobjekt für Debitoren- oder Kreditorenstammdaten im Buchungskreis

Debitorenstammdaten: F_KNA1_BUK

Kreditorenstammdaten: F_LFA1_BUK

Berechtigungsobjekt für Debitoren- oder Kreditorenstammdaten abhängig vom Stammsatz (Kontenberechtigung)

Debitorenstammdaten: F_KNA1_BED

Kreditorenstammdaten: F_LFA1_BEK

Berechtigungsobjekt für die Änderung bestimmter Felder

Debitorenstammdaten: F_KNA1_AEN

Kreditorenstammdaten: F_LFA1_AEN

Berechtigungsobjekt für die Änderung bestimmter Kontengruppen (gilt nur für Debitoren): F_KNA1_KGD

Berechtigungsobjekt für die Kontoanalyse (gilt nur für Debitoren): F_KNB1_ANA

Für die Debitorenkonten steht eine Analysefunktion zur Verfügung für einen Überblick über die Gesamtsumme der offenen Posten, die Abzüge und Zinsen, das Kreditlimit und das Zahlungsverhalten. Für diese Funktion gibt es ein eigenes Berechtigungsobjekt: Berechtigung für Kontoanalyse. Das Berechtigungsobjekt besteht nur aus dem Feld Buchungskreis.

9.3.7.2. Banken

Für die Banken wurde ein Berechtigungsobjekt definiert, mit dem das Anlegen und Bearbeiten von Bankenstammdaten geschützt werden kann. Mit einem zweiten Berechtigungsobjekt legt man fest, in welchen Buchungskreisen Hausbanken definiert und bearbeitet werden können.

Die Berechtigungsobjekte für die Banken sind im einzelnen:

Berechtigungsobjekt für Bankenstammdaten (generelle Pflegeberechtigung):
F_BNKA_MAN.

Berechtigungsobjekt für Hausbanken (Berechtigung für Buchungskreise):
F_BNKA_BUK

9.3.7.3. **Finanzkalender**

Der Finanzkalender erlaubt eine Übersicht über im System eingeplante periodische Arbeiten wie Mahnläufe, Zahlläufe und Reports. Alle Aufgaben, die gleichzeitig angezeigt werden sollen, werden im Terminplan zusammengefaßt.

Für den Terminplan können mit dem Berechtigungsobjekt
("Berechtigung für Finanzkalender") F_T001E

Berechtigungen für das Ändern und Anzeigen vergeben werden.

9.3.7.4. **Buchhaltungsbeleg**

Für den Buchhaltungsbeleg wurden Berechtigungsobjekte definiert, mit denen das Buchen, Anzeigen usw. auf Buchungskreise, Geschäftsbereiche, Belegarten, Kontoarten oder Konten eingeschränkt werden kann.

Berechtigungsobjekt für Buchungskreise: F_BKPF_BUK

Das Objekt wird auch zur Definition der generellen Berechtigung verwendet. Ein Mitarbeiter kann die Funktion zum Buchen aufrufen, wenn er mindestens in einem Buchungskreis die Berechtigung zum Buchen von Belegen hat.

Berechtigungsobjekt für Geschäftsbereiche: F_BKPF_GES

Für das Buchen und Bearbeiten von Belegen können aus der Sicht der Konten und der Geschäftsvorfälle Berechtigungen mit folgenden Objekten vergeben werden:

Berechtigung für Buchungsperioden: F_BKPF_BUP

Berechtigungsobjekt für Kontoarten: F_BKPF_KOA

Berechtigungsobjekt für Belegarten: F_BKPF_BLA

Berechtigungsobjekt Kontenberechtigung für Sach-, Kreditoren- und Debitorenkonten:

Sachkonten: F_BKPF_SAK

Kreditoren: F_BKPF_BEK

Debitoren: F_BKPF_BED

Berechtigungsobjekt Vorschlagswerte für Belegart und Buchungsschlüssel ändern: F_BKPF_VW

Das System wird mit Vorschlagswerten für Belegart und Buchungsschlüssel ausgeliefert. Diese Werte werden dem Anwender beim Aufruf einer Funktion vorgeschlagen. Für die Änderung der Vorschlagswerte über den Einstellungsleitfaden der Buchhaltung können Änderungsberechtigungen vergeben werden.

9.3.7.5. **Kreditlimit**

Das Kreditlimit, das ein Debitor oder Kreditor erhalten soll, kann allgemein für einen Debitor oder für einen Debitor getrennt nach Kreditkontrollbereichen eingerichtet werden. Der Kreditkontrollbereich ist eine organisatorische Einheit, die Kreditlimits vorgibt und kontrolliert. Ein Kontrollbereich kann für einen oder mehrere Buchungskreise zuständig sein.

Für die Kreditlimits wurden drei Berechtigungsobjekte definiert: Mit dem ersten Berechtigungsobjekt wird die generelle Pflegeberechtigung, mit dem zweiten die Kreditlimitpflege und -anzeige auf Kreditkontrollbereiche eingeschränkt. Über das dritte Berechtigungsobjekt können bestimmte Felder der Debitorenstammdaten zum Kreditmanagement vor Änderungen geschützt werden.

Die Berechtigungsobjekte für das Kreditlimit sind im einzelnen:

Generelle Pflegeberechtigung:	F_KNKA_MAN
Berechtigung für Kreditkontrollbereiche:	F_KNKA_KKB
Änderungsberechtigung für bestimmte Felder:	F_KNKA_AEN

9.3.7.6. **Zahllauf**

Für die Definition von Berechtigungen gibt es im System spezielle Aktivitätsschlüssel, die nur für das Zahlungsprogramm gelten. Sie können über den Menüpunkt Umfeld im Anforderungsbild des Zahlungsprogramms abgefragt werden.

Wenn Sie die Berechtigungen definieren, geben Sie die gewünschten Aktivitäten mit den Schlüsseln an. Für die Definition der Berechtigungen können Sie die Aktivitäten mit Buchungskreisen bzw. Kontoarten kombinieren.

Für den Zahllauf können folgenden Berechtigungen vergeben werden:

Berechtigungsobjekt für den Buchungskreis:	F_REGU_BUK
Berechtigungsobjekt für die Kontoart:	F_REGU_KOA

9.3.7.7. **Mahnlauf**

Für den Mahnlauf können Sie folgende Berechtigungen vergeben:

Berechtigungsobjekt für den Buchungskreis:	F_MAHN_BUK
Berechtigungsobjekt für die Kontoart:	F_MAHN_KOA

9.3.8. Reports

RFAUSZ00	Kontoauszug erstellen
RFAVIS20	Reorganisation von Zahlungsvisen
RFBISA00	Sachkontendaten aus einem Vorsystem in das System R/3 übernehmen.
RFCHKR10	Korrektur, wenn bei Schecks die falsche Schecknummer eingegeben wurde
RFDABL00	Änderungen in Debitorenstammsätzen kontenübergreifend auflisten
RFDKLI10	Suche nach Debitoren ohne Kreditlimits
RFDKLI20	Neuaufbau der Kreditlimits ausgewählter Kreditkontrollbereiche
RFDKLI30	Kurzübersicht Kreditlimit
RFDKLI40	Übersicht Kreditlimit (erweitert)
RFDKLI41	Kreditstammblatt
RFDKLI50	Massenänderung
RFDKLIAB	Änderungen im Kreditmanagement kontenübergreifend anzeigen
RFDKLIAB	Änderungsanzeige, kontenübergreifend
RFEBCK00	Scheckrücklauf einspielen
RFKABL00	Änderungen in Kreditorenstammsätzen kontenübergreifend auflisten lassen
RFKORD00	Zahlungsmittelungen direkt mit dem Druckreport drucken:
RFKORD10	Kontoauszug und Offene-Posten-Liste drucken
RFPKDB00	Verbindlichkeiten aus vorerfaßten Belegen auswerten und ggf. pauschal buchen
RFSABL00	Änderungen in Sachkontenstammsätzen kontenübergreifend auflisten
RFWEDI00	Einreichungsliste für die Bank
RFZALI00	Reports zur Erstellung der Zahlungsvorschlagsliste und der
RFZALI10	Reports zur Erstellung der Ausnahmeliste
SAPF019	Stammdaten im Kontenplan und/oder im Buchungskreis wieder löschen.
SAPF140	Druck aller angeforderten und noch nicht gedruckten Korrespondenzarten.

RCCLCUST

Zu Release 3.0D ist es notwendig, den Report zu starten, damit die Daten im Customizing des Klassensystems, die von SAP zu diesem Release geändert wurden, auch in Ihrem System übernommen werden. Über diesen Report werden neue oder geänderte Tabelleneinträge, die von SAP im Mandant 000 vorgenommen wurden, in alle Mandanten Ihres Produktivsystems transportiert.

9.4. Risiken

Ohne ausreichenden Schutz des Zahlungsverkehrs durch systemseitige Plausibilitäten und maschinelle Kontrollen/Abstimmungen und ohne wirksame organisatorisch vor- und/oder nachgelagerte manuelle Kontrollen können dem Unternehmen Vermögensschäden durch Arbeitsfehler und/oder dolose Handlungen entstehen.

9.4.1. Kreditorenstammsätze

Die unvollständige oder fehlerhafte Pflege von Kreditorenstammsätzen kann aufwendige Nacharbeiten zur Folge haben. Die Nachvollziehbarkeit ist erschwert bzw. nicht gegeben (siehe auch Kapitel 7). Fehlende Funktionstrennung zwischen dem Zugriff (Neuanlage, Pflege) auf Stammdaten und Bewegungsdaten erhöht das Risiko von Manipulationen an Kreditorenstammdaten (z. B. Bankverbindung).

Die Nutzung von CpD-Konten im Zahlungsverkehr beinhaltet zusätzliche Risiken aufgrund der offenen Eingabemöglichkeiten beim Zahlungsweg, Zahlungsempfänger und der fehlenden Transparenz über Auswertungsmöglichkeiten (z.B. Lieferantenstatistik).

9.4.2. Rechnungsprüfung

Ohne unternehmensinterne Regelungen zur Rechnungsprüfung (Vier-Augen-Prinzip, Funktionstrennung, Freigabeverfahren) besteht das Risiko zu Doppelzahlungen (z.B. Buchung und Zahlung von Rechnungskopien oder Mahnungen) und zu Manipulationen (z.B. Rechnung ohne Leistung).

9.4.3. Zahlungsvorschlag, Zahlungslauf

Gesperrte Rechnungen erscheinen nicht auf den Zahlungsvorschlagslisten. Bei fehlenden Kontrollen oder fehlendem Abgleich zwischen Zahlungsvorschlag und Zahlung können Rechnungen unbemerkt nach Freigabe der Vorschlagslisten freigegeben werden und in den Zahlungslauf gelangen.

9.5. Prüfungen

Anhand von Interviews, Stellenbeschreibungen und Organigrammen sollten zunächst Informationen darüber gesammelt werden, welche Form der Ablauforganisation durch das Unternehmen gewählt wurde. Mittels der Dokumentation des durch das Unternehmen konzipierten Berechtigungskonzeptes sollte dann beurteilt werden, inwieweit die organisatorische Struktur des Unternehmens mit dem Berechtigungskonzept übereinstimmt.

9.5.1. Funktionstrennung

Durch eine Prüfung der Berechtigungen sollte festgestellt werden, ob im Unternehmen eine sinnvolle Funktionstrennung zwischen Rechnungsprüfung / Buchung / Freigabe zur Zahlung besteht. Fragestellungen lauten: Gibt es Mitarbeiter, die sowohl die Kreditoren-Stammdaten anlegen/pflegen als auch Rechnungen buchen und/oder zur Zahlung freigeben können ? Können Mitarbeiter mit Systemberechtigungen sich diese selbst einrichten ? (Berechtigungen dazu siehe Kapitel 2)

Fehlen diese Funktionstrennungen, weil beispielsweise aufgrund kleinerer Organisationseinheiten mehrere Arbeitsinhalte im Ablauf des Zahlungsverkehrs zusammengefaßt sind, ist nach entsprechenden Maßnahmen des internen Kontrollsystems zu fragen. Sinnvolle Fragestellungen lauten: Welche Prüfungen sieht das IKS vor ? Vier-Augen-Prinzip bei der Anlage und Pflege von Kreditoren, bei Buchung und Zahlungsfreigabe an einem Arbeitsplatz, Plausibilitätsprüfungen z.B. hinsichtlich der in Rechnung gestellten Leistungen oder der Rechnungshöhe je Kreditor. Auch sind nachgelagerte Prüfungen von durchgeführten Zahlungen z.B. mittels qualifizierter Stichproben zu empfehlen.

9.5.2. CpD-Konten

Bei der Prüfung der unternehmensinternen Regelungen zur Anlage und Pflege von Kreditoren ist auch nach dem Umgang mit den CpD-Konten zu fragen. Welche Anweisungen gibt es zu den CpD-Konten ? Werden die CpD-Konten besonders kontrolliert ? Unter welchen Bedingungen wird zu Lasten CpD-Konten gebucht ?

9.5.3. Zahlungsvorschlagsliste und Zahlungsliste

Es sollten die Abläufe bei der Erstellung und Kontrolle der Zahlungsvorschlagslisten und der Zahlungslaufdateien geprüft werden. Werden die Zahlungsvorschlagslisten vor Zahlung geprüft ? Wenn ja, stimmen festgestellte Fehler oder Änderungen auf den Vorschlagslisten mit den Zahlungslisten überein ? Existieren Regeln zum Setzen und Rücksetzen von Sperrkennzeichen ?

Gibt es eine Abstimmung zwischen der Vorschlagsbestandssumme und der Zahlungslaufsumme ? Wie werden die Zahlungslaufdateien gesichert ? Sind Eingriffe in die Dateien und Spoolsysteme möglich ?

Zur Kontrolle des Zahlungslaufs sollte vor dem Drucken der Formulare das Zahlungsprotokoll gelesen und die Zahlungsliste überprüft werden. (Um das Zahlungsprotokoll aufzurufen, wählen Sie Bearbeiten . Zahlung . Protokoll anzeigen. Um den Zahlungslauf anzuzeigen, wählen Sie Bearbeiten . Zahlung. Anzeigen).

Dadurch ist es möglich, sich mit Hilfe von Funktionen wie Suchen und Sortieren einen schnellen Überblick über die Zahlungen zu verschaffen. Außerdem kann hier auch nach dem Zahlungslauf (Bearbeiten . Vorschlag . Anzeige) über eine Historie der Vorschlagsänderungen verfolgt werden wer welche Änderungen wann durchführte.

9.5.4. Doppelzahlungen

Es sollte geprüft werden, inwieweit Doppelzahlungen vorkommen können und welche Maßnahmen das Unternehmen zur Vermeidung vorgesehen hat. Gibt es Anweisungen für den Umgang mit Rechnungskopien und Mahnungen ? Sind systemseitig Plausibilitätsprüfungen eingerichtet ? Können Kreditoren mehrfach im Stamm angelegt sein ?