

Inhaltsverzeichnis

1	Einführung	25
1.1	Zur Nutzung dieses Buches	25
1.2	Transaktionen	27
1.2.1	Funktionsweise	27
1.2.2	Häufig benötigte Transaktionen	29
1.3	Reports.	30
1.3.1	Namenskonventionen.	30
1.3.2	Aufruf von Reports	31
1.3.3	Suchen von Reports.	34
1.3.4	Exportieren von Reports	36
1.3.5	Festlegung des Standardpfades zum Speichern	40
1.3.6	Speichern der Selektionsangaben (Varianten)	41
1.3.7	Dokumentationen zu Reports	42
1.4	Tabellen	44
1.4.1	Anzeigen von Tabellen	44
1.4.1.1	Transaktionen zur Tabellenanzeige	44
1.4.1.2	Die Transaktion SE16.	45
1.4.1.3	Die Transaktion SE16N (nur in SAP ERP)	49
1.4.2	Suchen von Tabellen	49
1.4.3	Exportieren von Tabellen.	54
1.4.4	Speichern der Selektionsangaben – Varianten.	54
1.5	Speichern von Listen als PDF-Datei	56
1.6	Die SAP-Hilfe	58
2	Die Systemsicherheit	61
2.1	Zu diesem Kapitel	61
2.2	SAP® NetWeaver® und SAP-Komponenten	62
2.2.1	SAP® NetWeaver®.	62
2.2.2	Die SAP™-Komponenten	64
2.3	Der technische Aufbau eines SAP-Systems	65
2.3.1	Applikations- und Datenbankservers	65
2.3.2	Instanzen	66
2.3.3	Die SAP-Prozesse und -Dienste	67
2.3.3.1	Abkürzungen: DVEBMGS	67
2.3.3.2	Der Dialogprozess	69
2.3.3.3	Der Verbuchungsprozess	69
2.3.3.4	Der Enqueue-Prozess	69
2.3.3.5	Der Batch-Prozess	70

2.3.3.6	Der Message-Server-Dienst	70
2.3.3.7	Der Gateway-Dienst	70
2.3.3.8	Der Spool-Prozess	70
2.3.4	Entwicklungs-, Konsolidierungs- und Produktivsystem	71
2.3.5	SAP-Systeme im Netzwerk	71
2.3.6	Checkliste zum Aufbau eines SAP-Systems	72
2.3.7	Praktische Prüfung zum Aufbau eines SAP-Systems	73
2.4	Grundlagen für die Prüfung der Systemsicherheit	74
2.4.1	Der Releasestand des SAP-Systems	74
2.4.2	Support Packages	75
2.4.3	Die Systemparameter	76
2.4.3.1	Das Prinzip der Systemparameter	76
2.4.3.2	Prüfen der Parameter mit dem Report RSPARAM (aktuelle Parameter prüfen)	79
2.4.3.3	Prüfen der Parameter mit Report/Transaktion RSPFPAR (aktuelle Parameter prüfen mit Selektionsmöglichkeit)	80
2.4.3.4	Dokumentation zu den einzelnen Parametern	81
2.4.3.5	Prüfen der Werte in den Profildateien über Transaktion AL11	82
2.4.3.6	Prüfen der Original-Profildateien (Parameter in den Profildateien prüfen)	84
2.4.3.7	Prüfen der Änderungen von Parameterwerten	84
2.4.3.8	Instanzübergreifende Prüfung der Parameterwerte	86
2.4.4	Protokolle im SAP-System	87
2.4.5	Zugriffsrechte	88
2.4.5.1	Prüfen im SAP-System	88
2.4.5.2	Prüfen mit CheckAud® for SAP® Systems	89
2.4.6	Checkliste zu den Grundlagen der Systemprüfung	90
2.4.7	Praktische Prüfung zu den Grundlagen der Systemprüfung	91
2.5	Mandanten	92
2.5.1	Die Mandanten des Systems	92
2.5.2	Mandantenkopien	94
2.5.3	Zugriffsrechte	99
2.5.3.1	Prüfen im SAP-System	99
2.5.3.2	Prüfen mit CheckAud® for SAP® Systems	102
2.5.4	Checkliste zu Mandanten	102
2.5.5	Praktische Prüfung zu Mandanten	104
2.6	Die SAP-Anmeldesicherheit	105
2.6.1	Die Kennwortkonventionen	105
2.6.2	Anforderungen zur Anmeldesicherheit	106
2.6.3	Unzulässige Kennwörter – Tabelle USR40	107

2.6.4	Protokolle von Mehrfachanmeldungen	108
2.6.5	Die Anmeldeparameter	109
2.6.6	Sicherheitsrichtlinien in Benutzerstammsätzen	117
2.6.7	Eigene Erweiterungen zur Anmeldesicherheit.	121
2.6.8	Zugriffsrechte	121
2.6.8.1	Prüfen im SAP-System	121
2.6.8.2	Prüfen mit CheckAud® for SAP® Systems	123
2.6.9	Checkliste zur Anmeldesicherheit	123
2.6.10	Praktische Prüfung zur Anmeldesicherheit	124
2.7	Das Notfallbenutzer-Konzept	127
2.7.1	Checkliste zum Notfallbenutzer-Konzept	128
2.7.2	Praktische Prüfung zum Notfallbenutzer-Konzept	129
2.8	Das Security AuditLog	130
2.8.1	Das Konzept des Security AuditLog	130
2.8.2	Konfiguration des Auditing	131
2.8.3	Konfiguration des statischen AuditLogs	134
2.8.4	AuditLog-Parameter.	137
2.8.5	Auswertung des AuditLog	138
2.8.6	Löschen alter AuditLogs	144
2.8.7	Mögliche Einstellungen für das AuditLog	145
2.8.8	Zugriffsrechte	147
2.8.8.1	Prüfen im SAP-System	147
2.8.8.2	Prüfen mit CheckAud® for SAP® Systems	148
2.8.9	Checkliste zum Auditing.	148
2.8.10	Praktische Prüfung zum Auditing.	149
2.9	Die Systemprotokollierung	150
2.9.1	Das Konzept der Systemprotokollierung	150
2.9.2	Zentrale und lokale Protokollierung	151
2.9.3	Anzeige des SysLog.	151
2.9.4	Inhaltliche Auswertung des SysLog	153
2.9.5	Zugriffsrechte	156
2.9.5.1	Prüfen im SAP-System	156
2.9.5.2	Prüfen mit CheckAud® for SAP® Systems	156
2.9.6	Checkliste zur Systemprotokollierung	157
2.9.7	Praktische Prüfung zur Systemprotokollierung	157
2.10	Sperren von Transaktionscodes.	158
2.10.1	Funktionsweise	158
2.10.2	Zugriffsrechte	159
2.10.2.1	Prüfen im SAP-System	159
2.10.2.2	Prüfen mit CheckAud® for SAP® Systems	160
2.10.3	Checkliste zum Sperren von Transaktionscodes	161
2.10.4	Praktische Prüfung zum Sperren von Transaktions- codes	161

Inhaltsverzeichnis

2.11	Logische Betriebssystemkommandos	161
2.11.1	Funktionsweise	161
2.11.2	Der Report RSBDCOS0	166
2.11.3	Nutzen der logischen Betriebssystemkommandos für Prüfer	167
2.11.4	Zugriffsrechte	169
2.11.4.1	Prüfen im SAP-System	169
2.11.4.2	Prüfen mit CheckAud® for SAP® Systems	170
2.11.5	Checkliste zu logischen Betriebssystemkommandos	171
2.11.6	Praktische Prüfung zu logischen Betriebssystemkommandos	171
2.12	Drucken und Speichern	172
2.12.1	Der Druckvorgang in SAP-Systemen	172
2.12.2	Schutz von Druckaufträgen.	175
2.12.3	Speichern von Daten in Dateien.	177
2.12.4	Zugriffsrechte	177
2.12.4.1	Prüfen im SAP-System	177
2.12.4.2	Prüfen mit CheckAud® for SAP® Systems	179
2.12.5	Checkliste zum Drucken und Speichern	179
2.12.6	Praktische Prüfung zum Drucken und Speichern	181
2.13	Batch-Input	183
2.13.1	Funktionsweise des Batch-Input-Verfahrens	183
2.13.2	Analyse des Batch-Input-Verfahrens	184
2.13.3	Zugriffsrechte	187
2.13.3.1	Prüfen im SAP-System	187
2.13.3.2	Prüfen mit CheckAud® for SAP® Systems	188
2.13.4	Checkliste zum Batch-Input-Verfahren	188
2.13.5	Praktische Prüfung zum Batch-Input-Verfahren	190
2.14	Integration des Business Warehouse in SAP® NetWeaver 7.x	191
2.14.1	Funktionalität	191
2.14.2	Datenextraktion	191
2.14.3	Der Extraktorchecker	192
2.14.4	Berechtigungen für die Extraktion einschränken	195
2.14.5	Zugriffsrechte	196
2.14.5.1	Prüfen im SAP-System	196
2.14.5.2	Prüfen mit CheckAud® for SAP® Systems	197
2.14.6	Checkliste zur BW-Integration	198
2.14.7	Praktische Prüfung zur BW-Integration	198
2.15	RFC-Verbindungen	200
2.15.1	Funktionsweise	200
2.15.2	Hinterlegte Kennwörter	202
2.15.2.1	Funktionalität	202
2.15.2.2	Kennwortspeicherung bis SAP NetWeaver 6.40	204
2.15.2.3	Kennwortspeicherung ab SAP NetWeaver 7.0	204

2.15.3	Systemübergreifender Zugriff über Transaktion SE37	206
2.15.4	Protokollierung von RFC-Anmeldungen	208
2.15.5	Berechtigungen für Schnittstellenbenutzer	211
2.15.6	Zugriffsrechte	211
2.15.6.1	Prüfen im SAP-System	211
2.15.6.2	Prüfen mit CheckAud® for SAP® Systems	213
2.15.7	Checkliste zu RFC-Verbindungen	214
2.15.8	Praktische Prüfung zu RFC-Verbindungen	215
2.16	Trusted-RFC-Verbindungen	218
2.16.1	Einsatzmöglichkeiten einer Trusted-Verbindung	218
2.16.2	Funktionsweise einer Trusted-Verbindung.	219
2.16.2.1	Definition einer Vertrauensbeziehung	219
2.16.2.2	Definition einer Trusted RFC-Verbindung	219
2.16.2.3	Erforderliche Berechtigungen im Trusting-(Ziel-)System	223
2.16.3	Betrachtung der Anmeldesicherheit	224
2.16.4	Zugriffsrechte	225
2.16.4.1	Prüfen im SAP-System	225
2.16.4.2	Prüfen mit CheckAud® for SAP® Systems	226
2.16.5	Checkliste zu Trusted RFC-Verbindungen	226
2.16.6	Praktische Prüfung zu Trusted RFC-Verbindungen	227
2.17	Zugriff von externen Programmen auf SAP-Systeme über RFC	230
2.17.1	Funktionsweise	230
2.17.2	Zugriff auf SAP am Beispiel von MS Excel	233
2.17.3	ABAP-Quelltexte über RFC ausführen	235
2.17.4	Zugriffsrechte	237
2.17.4.1	Prüfen im SAP-System	237
2.17.4.2	Prüfen mit CheckAud® for SAP® Systems	238
2.17.5	Checkliste zu externen Zugriffen	238
2.17.6	Praktische Prüfung zu externen Zugriffen	239
2.18	Das SAP Gateway im RFC-Umfeld	240
2.18.1	Checkliste zum Gateway	242
2.18.2	Praktische Prüfung zum Gateway	242
2.19	Nutzung der Zugriffsstatistik für Prüfungen	242
2.19.1	Funktionsweise	242
2.19.2	Analyse von aufgerufenen Transaktionen	245
2.19.2.1	Auswertung der Transaktions- und Reportaufrufe einzelner Benutzer	245
2.19.2.2	Auswertung der aufrufenden Benutzer einzelner Transaktionen und Reports	246
2.19.2.3	Auswertung aller Transaktions- und Reportaufrufe in einem Zeitraum	246
2.19.3	Analyse von RFC-Aufrufen	248
2.19.3.1	Auswertung der RFC-Aufrufe einzelner Benutzer	248

- 2.19.3.2 Auswertung aller RFC-Aufrufe in einem Zeitraum . . . 249
- 2.20 Die Lesezugriffsprotokollierung. 250
 - 2.20.1 Funktionsweise 250
 - 2.20.2 Protokollierung des Zugriffs auf sensible Felder 251
 - 2.20.3 Protokollierung des Aufrufes von Funktionsbausteinen 254
 - 2.20.4 Konfigurationseinstellungen 256
 - 2.20.5 Das Verwaltungsprotokoll 256
 - 2.20.6 Zugriffsrechte 257
 - 2.20.6.1 Prüfen im SAP-System 257
 - 2.20.6.2 Prüfen mit CheckAud® for SAP® Systems 259
 - 2.20.7 Checkliste zur Lesezugriffsprotokollierung. 259
 - 2.20.8 Praktische Prüfung zur Lesezugriffsprotokollierung 260
- 2.21 Kritische Basisberechtigungen 261
- 2.22 Gesetzeskritische Berechtigungen. 265
- 2.23 Wichtige Systemparameter. 269
 - 2.23.1 Globale Parameter 269
 - 2.23.2 Instanzparameter 270
 - 2.23.3 Verbuchungsparameter 270
 - 2.23.4 Anmeldeparameter 272
 - 2.23.5 Verzeichnis-Parameter 279
 - 2.23.6 SysLog-Parameter 280
 - 2.23.7 Security AuditLog-Parameter 280
 - 2.23.8 Parameter der Berechtigungsprüfung 281
- 2.24 Reports, Tabellen und Transaktionen zur Systemsicherheit 282
- 2.25 QuickWins 285
- 3 Der Verbuchungsvorgang 289**
 - 3.1 Zu diesem Kapitel 289
 - 3.2 Das Prinzip des Verbuchens. 289
 - 3.2.1 Die synchrone Verbuchung. 289
 - 3.2.2 Die asynchrone Verbuchung 289
 - 3.2.3 Die Verbuchungskomponenten 291
 - 3.2.4 Die Auswertung der Verbuchung über Transaktion SM13/SM14 293
 - 3.2.5 Meldungen im SysLog 296
 - 3.2.6 Die Steuerung der Verbuchung über Systemparameter 296
 - 3.2.7 Zugriffsrechte 298
 - 3.2.7.1 Prüfen im SAP-System 298
 - 3.2.7.2 Prüfen mit CheckAud® for SAP® Systems 299
 - 3.2.8 Checkliste zur Verbuchung. 299
 - 3.2.9 Praktische Prüfung zur Verbuchung. 300

3.3	Abgebrochene Buchungen	301
3.3.1	Weiterverarbeitung von abgebrochenen Buchungen	301
3.3.2	Prüfung von abgebrochenen Verbuchungssätzen	302
3.3.3	Die Abstimmanalyse der Finanzbuchhaltung	304
3.3.4	Checkliste zu abgebrochenen Buchungen	307
3.3.5	Praktische Prüfung zu abgebrochenen Buchungen	308
3.4	Die Belegnummernvergabe	310
3.4.1	Interne und externe Belegnummernvergabe	310
3.4.2	Nummernkreisobjekte und Nummernkreisintervalle	310
3.4.3	Die Pufferung von Belegnummern	311
3.4.4	Suchen nach Lücken in Belegnummern	315
3.4.5	Zugriffsrechte	316
3.4.5.1	Prüfen im SAP-System	316
3.4.5.2	Prüfen mit CheckAud® for SAP® Systems	317
3.4.6	Checkliste zur Belegnummernvergabe	317
3.4.7	Praktische Prüfung zur Belegnummernvergabe	318
3.5	Pufferung durch die Tabelle NRIV_LOKAL	319
3.6	Nummernkreisintervalle – Belegarten	320
3.7	Reports, Tabellen und Transaktionen der Verbuchung.	321
3.8	QuickWins.	322
4	Benutzerauswertungen	325
4.1	Zu diesem Kapitel	325
4.2	Organisatorische Regelungen	325
4.2.1	Allgemeine Anforderungen	325
4.2.2	Checkliste zu organisatorischen Regelungen	327
4.2.3	Praktische Prüfung zu organisatorischen Regelungen	328
4.3	Die SAP-Standardbenutzer	328
4.3.1	Überblick.	328
4.3.2	Der Benutzer SAP*	329
4.3.3	Der Benutzer DDIC	330
4.3.4	Der Benutzer SAPCPIC	330
4.3.5	Der Benutzer TMSADM	331
4.3.6	Der Benutzer EARLYWATCH	331
4.3.7	Prüfen der Standardbenutzer mit dem Report RSUSR003	332
4.3.8	Weitere Standardbenutzer	334
4.3.9	Zugriffsrechte	334
4.3.9.1	Prüfen im SAP-System	334
4.3.9.2	Prüfen mit CheckAud® for SAP® Systems	336
4.3.10	Checkliste zu den SAP-Standardbenutzern	337
4.3.11	Praktische Prüfung zu den SAP-Standardbenutzern	338

4.4	Der Benutzerstammsatz	339
4.4.1	Die Eigenschaften eines Benutzers	339
4.4.2	Die Tabellen des Benutzerstammsatzes	342
4.4.3	Die Nutzung der Tabellen des Benutzerstammsatzes	349
4.4.4	Einzelauswertung der Benutzerstammsätze	354
4.4.5	Benutzerauswertungen mit Standardreports	355
4.4.6	Berechtigungsprüfungen zur Benutzerverwaltung.	358
4.4.7	Zugriffsrechte	364
4.4.7.1	Prüfen im SAP-System	364
4.4.7.2	Prüfen mit CheckAud® for SAP® Systems	368
4.4.8	Checkliste zum Benutzerstammsatz.	368
4.4.9	Praktische Prüfung zum Benutzerstammsatz.	371
4.5	Referenzbenutzer	374
4.5.1	Zugriffsrechte	377
4.5.2	Checkliste zu Referenzbenutzern	377
4.5.3	Praktische Prüfung zu Referenzbenutzern	378
4.6	Benutzergruppen	379
4.6.1	Funktionalität der Benutzergruppen	379
4.6.2	Zugriffsrechte	381
4.6.2.1	Prüfen im SAP-System	381
4.6.2.2	Prüfen mit CheckAud® for SAP® Systems	382
4.6.3	Checkliste zu Benutzergruppen	383
4.6.4	Praktische Prüfung zu Benutzergruppen	383
4.7	Sammelbenutzer	384
4.7.1	Das Problem der Sammelbenutzer.	384
4.7.2	Checkliste zu Sammelbenutzern.	385
4.7.3	Praktische Prüfung zu Sammelbenutzern.	386
4.8	Die Benutzervermessungsdaten	387
4.8.1	Die Systemvermessung	387
4.8.2	Zugriffsrechte	393
4.8.2.1	Prüfen im SAP-System	393
4.8.2.2	Prüfen mit CheckAud® for SAP® Systems	394
4.8.3	Checkliste zu den Benutzervermessungsdaten.	395
4.8.4	Praktische Prüfung zu den Benutzervermessungs- daten	395
4.9	Benutzer mit Initialkennwort	396
4.9.1	Funktionsweise	396
4.9.2	Verfahren zur Vergabe von Initialkennwörtern	398
4.9.3	Zugriffsrechte	400
4.9.3.1	Prüfen im SAP-System	400
4.9.3.2	Prüfen mit CheckAud® for SAP® Systems	401
4.9.4	Checkliste zu Benutzern mit Initialkennwort	401
4.9.5	Praktische Prüfung zu Benutzern mit Initialkennwort	402

4.10	Die Kennwortverschlüsselung	402
4.10.1	Die Verschlüsselung bis NetWeaver 6.40	402
4.10.2	Die Verschlüsselung ab NetWeaver 7.0	403
4.10.3	Hacken von SAP-Kennwörtern	405
4.10.4	Verschlüsselung der Kennwörter bei der Übertragung im Netz	406
4.10.5	Checkliste zur Kennwortverschlüsselung	406
4.10.6	Praktische Prüfung zur Kennwortverschlüsselung	407
4.11	Die angemeldeten Benutzer	408
4.11.1	Auswertung der angemeldeten Benutzer	408
4.11.2	Zugriffsrechte	411
4.11.2.1	Prüfen im SAP-System	411
4.11.2.2	Prüfen mit CheckAud® for SAP® Systems	412
4.11.3	Checkliste zu den angemeldeten Benutzern	412
4.11.4	Praktische Prüfung zu den angemeldeten Benutzern	413
4.12	Die Änderungshistorie der Benutzer	413
4.12.1	Zugriffsrechte	415
4.12.1.1	Prüfen im SAP-System	415
4.12.1.2	Prüfen mit CheckAud® for SAP® Systems	416
4.12.2	Checkliste zur Änderungshistorie der Benutzer	416
4.12.3	Praktische Prüfung zur Änderungshistorie der Benutzer	417
4.13	SAP-Marketplace-Benutzer	420
4.13.1	Das Konzept der SAP-Marketplace-Benutzer	420
4.13.2	Checkliste zu SAP-Marketplace-Benutzern	421
4.13.3	Praktische Prüfung zu SAP-Marketplace-Benutzern	422
4.14	Das Benutzerinfosystem	422
4.14.1	Aufruf des Benutzerinfosystems	422
4.14.2	Konfiguration des Benutzerinfosystems	423
4.14.3	Die Reports des Benutzerinfosystems	425
4.15	Reports, Tabellen und Transaktionen zu Benutzer- auswertungen	426
4.16	QuickWins.	428
5	Die Tabellenpflege	431
5.1	Zu diesem Kapitel	431
5.2	Das Data Dictionary	431
5.2.1	Aufbau des Data Dictionary	431
5.2.2	Domänen	433
5.2.2.1	Der Aufbau einer Domäne	433
5.2.2.2	Dokumentation zu Domänen	437
5.2.2.3	Prüfansätze zu Domänen	437
5.2.3	Datenelemente	441

5.2.3.1	Aufbau eines Datenelementes	441
5.2.3.2	Dokumentation zu Datenelementen	444
5.2.4	Das Infosystem für das Data Dictionary.	445
5.2.5	Zugriffsrechte	446
5.2.5.1	Prüfen im SAP-System	446
5.2.5.2	Prüfen mit CheckAud® for SAP® Systems	447
5.2.6	Checkliste zum Data Dictionary	447
5.2.7	Praktische Prüfung zum Data Dictionary.	448
5.3	Das Konzept der Tabellensteuerung	449
5.3.1	Die Eigenschaften der Tabellen	449
5.3.2	Mandantenabhängige Tabellen.	452
5.3.3	Mandantenunabhängige Tabellen	453
5.3.4	Transparente, Pool- und Cluster-Tabellen	453
5.3.4.1	Transparente Tabellen.	454
5.3.4.2	Pool-Tabellen.	455
5.3.4.3	Cluster-Tabellen	458
5.3.5	Dokumentation zu Tabellen	461
5.3.6	Unternehmenseigene Tabellen und Views	465
5.3.7	Die Tabellenpufferung	465
5.3.7.1	Was ist die Tabellenpufferung?	465
5.3.7.2	Tabellenpufferungsarten	466
5.3.7.3	Welche Tabellen werden gepuffert?	469
5.3.7.4	Puffersynchronisation.	470
5.3.8	Zugriffsrechte	472
5.3.8.1	Prüfen im SAP-System	472
5.3.8.2	Prüfen mit CheckAud® for SAP® Systems	473
5.3.9	Checkliste zur Tabellensteuerung	473
5.3.10	Praktische Prüfung zur Tabellensteuerung	474
5.4	Views	475
5.4.1	Der Aufbau einer View	475
5.4.2	Suchen der Views zu einer Tabelle	479
5.4.3	View-Aufrufe über Transaktionen	481
5.4.4	Zugriffsrechte	483
5.4.4.1	Prüfen im SAP-System	483
5.4.4.2	Prüfen mit CheckAud® for SAP® Systems	483
5.4.5	Checkliste zu Views	484
5.4.6	Praktische Prüfung zu Views.	484
5.5	Die Protokollierung der Tabellenänderungen	485
5.5.1	Funktionsweise	485
5.5.2	Die Aktivierung der Protokollierung	486
5.5.3	Protokollierung bei Transporten	488
5.5.4	Die Protokollierung der einzelnen Tabellen	490
5.5.5	Protokollierung unternehmenseigener Tabellen	496
5.5.5.1	Die Problematik	496

5.5.5.2	Definition unternehmenseigener Tabellen	496
5.5.5.3	Beurteilungskriterien für die Rechnungslegungs- relevanz unternehmenseigener Tabellen	497
5.5.5.4	Vorgehensweise zur Bewertung der Protokollierungs- pflicht	498
5.5.6	Die Auswertung der Tabellenänderungen	498
5.5.7	Löschen von Tabellenänderungsprotokollen.	502
5.5.8	Nutzung der Protokollierung zur Systemsicherheit.	504
5.5.9	Zugriffsrechte	504
5.5.9.1	Prüfen im SAP-System	504
5.5.9.2	Prüfen mit CheckAud® for SAP® Systems	506
5.5.10	Checkliste zur Protokollierung	506
5.5.11	Praktische Prüfung zur Protokollierung	508
5.6	Die Protokollierung über die Änderungsbelege.	511
5.6.1	Funktionsweise	511
5.6.2	Suchen von über Änderungsbelege protokollierten Tabellen	513
5.6.3	Auswertung der Änderungsbelege	514
5.6.3.1	Auswertung über die Tabellen (mandantenbezogen)	514
5.6.3.2	Auswertung über Reports/Transaktionen (mandantenbezogen)	515
5.6.3.3	Mandantenübergreifende Auswertung von Änderungsbelegen	515
5.6.4	Löschen von Änderungsbelegen.	515
5.6.5	Ändern von Änderungsbelegobjekten	516
5.6.6	Zugriffsrechte	517
5.6.6.1	Prüfen im SAP-System	517
5.6.6.2	Prüfen mit CheckAud® for SAP® Systems	518
5.6.7	Checkliste zu Änderungsbelegen	518
5.6.8	Praktische Prüfung zu Änderungsbelegen	519
5.7	Anzeigen und Pflegen von Tabellen	520
5.7.1	Anzeige von Tabelleninhalten in der Datenbank	520
5.7.2	Ändern der Tabellen im SAP-System.	522
5.7.2.1	Direktes Ändern der Tabellen	522
5.7.2.2	Ändern von Tabellen über Views	523
5.7.2.3	Laufende Einstellungen	524
5.7.3	Ändern der Tabellen über die Datenbank	526
5.7.4	Zugriffsrechte	527
5.7.4.1	Prüfen im SAP-System	527
5.7.4.2	Prüfen mit CheckAud® for SAP® Systems	528
5.7.5	Checkliste zum Anzeigen und Pflegen von Tabellen	529
5.7.6	Praktische Prüfung zum Anzeigen und Pflegen von Tabellen	530

5.8	Berechtigungen auf Tabellen und Views	531
5.8.1	Berechtigungsgruppen	531
5.8.2	Berechtigungen auf Berechtigungsgruppen (Objekt S_TABU_DIS)	534
5.8.3	Berechtigungen auf Tabellen (Objekt S_TABU_NAM)	536
5.8.4	Berechtigungen auf mandantenunabhängige Tabellen (Objekt S_TABU_CLI)	537
5.8.5	Zeilenweise Berechtigungen (Objekt S_TABU_LIN).	538
5.8.5.1	Funktionsweise	538
5.8.5.2	Customizing	539
5.8.5.3	Berechtigung	540
5.8.6	Schutz von Tabellen ohne Berechtigungsgruppe	542
5.8.7	Prüfen der Zugriffsberechtigungen auf einzelne Tabellen/Views	542
5.8.8	Zugriffsrechte	546
5.8.8.1	Prüfen im SAP-System	546
5.8.8.2	Prüfen mit CheckAud® for SAP® Systems	547
5.8.9	Checkliste zu Tabellenberechtigungen	548
5.8.10	Praktische Prüfung zu Tabellenberechtigungen	549
5.9	Vergleich und Abgleich von Tabelleninhalten	551
5.9.1	Der Vergleich	551
5.9.2	Der Abgleich	553
5.9.3	Zugriffsrechte	555
5.9.3.1	Prüfen im SAP-System	555
5.9.3.2	Prüfen mit CheckAud® for SAP® Systems	556
5.9.4	Checkliste zum Vergleich und Abgleich von Tabelleninhalten	557
5.9.5	Praktische Prüfung zum Vergleich und Abgleich von Tabelleninhalten	557
5.10	Der SQL-Trace	558
5.10.1	Aktivierung des SQL-Trace.	558
5.10.2	Auswertung des Trace.	560
5.10.3	Zugriffsrechte	563
5.10.3.1	Prüfen im SAP-System	563
5.10.3.2	Prüfen mit CheckAud® for SAP® Systems	563
5.11	Tabelleninhalte auswerten mit dem QuickViewer	564
5.11.1	Funktionalität	564
5.11.2	Erstellen einer QuickView auf einer einzelnen Tabelle	565
5.11.3	Erstellen einer QuickView mit einem Tabellen-Join	569
5.11.4	Erstellen einer QuickView mit einer logischen Datenbank	572
5.11.5	Zugriffsrechte	574

5.11.5.1	Prüfen im SAP-System	574
5.11.5.2	Prüfen mit CheckAud® for SAP® Systems	575
5.12	Reports, Tabellen und Transaktionen zur Tabellenpflege	576
5.13	QuickWins.	579
6	Entwicklungen in SAP-Systemen	583
6.1	Zu diesem Kapitel	583
6.2	Organisation der Anwendungsentwicklung.	584
6.2.1	Systemlandschaften.	584
6.2.2	Entwicklerrichtlinien	587
6.2.3	Checkliste zur Organisation der Anwendungs- entwicklung	589
6.2.4	Praktische Prüfung zur Organisation der Anwendungsentwicklung	590
6.3	Entwickler- und Objektschlüssel	591
6.3.1	Entwicklerschlüssel.	591
6.3.1.1	Prüfung	591
6.3.1.2	Löschen von Entwicklerschlüsseln über eine Pflege- View	593
6.3.2	Objektschlüssel	593
6.3.3	Umgehung der Abfrage auf Entwickler- und Objekt- schlüssel	594
6.3.4	Checkliste zu Entwickler- und Objektschlüsseln	597
6.3.5	Praktische Prüfung zu Entwickler- und Objekt- schlüsseln	598
6.4	Die System- und Mandantenänderbarkeit	600
6.4.1	Schutz der SAP-Systeme vor Änderungen	600
6.4.2	Die Systemänderbarkeit	600
6.4.2.1	Funktionalität	600
6.4.2.2	Die Protokollierung der Systemänderbarkeit	603
6.4.3	Die Mandantenänderbarkeit	604
6.4.3.1	Funktionalität	604
6.4.3.2	Die Protokollierung der Mandantenänderbarkeit	607
6.4.4	Zugriffsrechte	609
6.4.4.1	Prüfen im SAP-System	609
6.4.4.2	Prüfen mit CheckAud® for SAP® Systems	610
6.4.5	Checkliste zur System- und Mandantenänderbarkeit.	610
6.4.6	Praktische Prüfung zur System- und Mandanten- änderbarkeit	612
6.5	Das Transportsystem	615
6.5.1	Der Change and Transport Organizer	615
6.5.1.1	Pakete/Entwicklungsklassen	615
6.5.1.2	Aufgaben und Aufträge.	615

6.5.1.3	Reparaturen	621
6.5.1.4	Der Objektkatalog: Tabelle TADIR	622
6.5.1.5	Das Organizer-Infosystem.	623
6.5.1.6	Zugriffsrechte	624
	6.5.1.6.1 Prüfen im SAP-System	624
	6.5.1.6.2 Prüfen mit CheckAud® for SAP® Systems	626
6.5.2	Das Transport Management System	626
6.5.2.1	Konfiguration.	626
6.5.2.2	Transportwege	627
6.5.2.3	Das Transportverzeichnis.	628
6.5.2.4	Transportprotokolle	630
6.5.2.5	Das Quality-Assurance-Genehmigungsverfahren	630
6.5.2.6	Prüfen der TMS-Konfiguration.	633
6.5.2.7	Zugriffsrechte	635
	6.5.2.7.1 Prüfen im SAP-System	635
	6.5.2.7.2 Prüfen mit CheckAud® for SAP® Systems	637
6.5.3	Der Ablauf eines Transports	637
6.5.3.1	Das Anlegen eines Auftrages	637
6.5.3.2	Durchführung des Customizing/der Programmierung	638
6.5.3.3	Die Freigabe der Aufgabe und des Auftrages.	638
6.5.3.4	Der Import ins Produktivsystem.	639
6.5.3.5	Zeitnähe der Importe	641
6.5.4	Funktionstrennungen im Transportsystem	641
6.5.4.1	Anwendungsentwicklung/Customizing.	642
6.5.4.2	Transporte	644
6.5.4.3	Berechtigungsverwaltung.	645
6.5.4.4	Notfälle	645
6.5.5	Checkliste zum Transportsystem	647
6.5.6	Praktische Prüfung zum Transportsystem	649
6.6	Das Customizing des SAP-Systems	653
6.6.1	Der Einführungsleitfaden	653
6.6.2	Auswerten der Protokolle des Customizing	657
6.6.3	Zugriffsrechte	657
6.6.3.1	Prüfen im SAP-System	657
6.6.3.2	Prüfen mit CheckAud® for SAP® Systems	659
6.6.4	Checkliste zum Customizing.	660
6.6.5	Praktische Prüfung zum Customizing.	660
6.7	Eigenentwicklungen in ABAP.	662
6.7.1	Was ist ABAP?	662
6.7.2	Die Programmiersprache ABAP	663
6.7.2.1	Der Aufbau eines ABAP-Programmes.	663
6.7.2.2	Die ABAP-Datentypen	665
6.7.2.3	Systemfelder	666
6.7.2.4	Ausgewählte ABAP-Befehle	667

6.7.2.5	ABAP-Namensräume	669
6.7.3	Gefahrenpunkte in der ABAP-Programmentwicklung .	669
6.7.3.1	„Allmacht“ der Entwickler.	670
6.7.3.2	Direkte Zugriffe auf die Datenbank mit dem Befehl EXEC SQL	670
6.7.3.3	Umgehung des Mandantenkonzeptes.	673
6.7.3.4	Enqueue- und Dequeue-Bausteine	673
6.7.3.5	Transaktionen aufrufen mit CALL TRANSACTION . .	675
6.7.3.6	Debuggen mit Hauptspeicheränderungen (Radieren). .	677
6.7.3.7	Berechtigungsprüfungen in ABAP-Programmen	679
	6.7.3.7.1 Berechtigungsprüfung mittels AUTHORITY-CHECK	679
	6.7.3.7.2 Berechtigungsprüfung durch schaltbare Berechtigungen	683
6.7.3.8	Generierung von ABAP-Programmen zur Laufzeit . . .	687
	6.7.3.8.1 Generierung von flexiblem Code	687
	6.7.3.8.2 Generierung von „verstecktem“ Code	689
6.7.4	Inhaltliches Prüfen von ABAP-Programmen.	693
6.7.5	Prüfen der Eigenschaften von ABAP-Programmen . . .	693
6.7.6	Programmübergreifende Suche in Quelltexten	695
6.7.7	Der ABAP Code Inspector	701
6.7.8	Code Vulnerability Analyzer (CVA).	705
6.7.9	Die Versionshistorie.	708
6.7.10	Dumps – ABAP-Programmabbrüche	715
6.7.11	Zugriffsrechte	719
6.7.11.1	Prüfen im SAP-System	719
6.7.11.2	Prüfen mit CheckAud® for SAP® Systems	720
6.7.12	Checkliste zur Programmiersprache ABAP	720
6.7.13	Praktische Prüfung zur Programmiersprache ABAP . .	722
6.8	Transaktionen	726
6.8.1	Funktionalität	726
6.8.2	Schutz über Berechtigungsobjekte	730
6.8.3	Zugriffsrechte	730
6.8.3.1	Prüfen im SAP-System	730
6.8.3.2	Prüfen mit CheckAud® for SAP® Systems	731
6.8.4	Checkliste zu Transaktionen.	732
6.8.5	Praktische Prüfung zu Transaktionen.	732
6.9	Berechtigungen zur Anwendungsentwicklung	735
6.9.1	Das Berechtigungsobjekt S_DEVELOP	735
6.9.2	Schutz von ABAP-Programmen durch Berechtigungsgruppen (S_PROGRAM)	738
6.9.3	Schutz von ABAP-Programmen nach Namen (S_PROGNAM)	742
6.9.4	Schutz von Funktionsbausteinen	743

6.9.5	Zugriffsrechte	746
6.9.5.1	Prüfen im SAP-System	746
6.9.5.2	Prüfen mit CheckAud® for SAP® Systems	751
6.10	Reports, Tabellen und Transaktionen.	751
6.11	QuickWins	754
7	Das Berechtigungskonzept	759
7.1	Zu diesem Kapitel	759
7.2	Die Funktionsweise des Berechtigungskonzeptes.	760
7.2.1	Allgemeine Beschreibung.	760
7.2.2	Berechtigungsobjekte	761
7.2.2.1	Beschreibung.	761
7.2.2.2	Felder der Objekte.	762
7.2.2.3	Transaktionsberechtigungen	764
7.2.2.4	Anwendungsberechtigungen	765
7.2.2.5	Kernel-Berechtigungsprüfungen	765
7.2.2.6	Unternehmenseigene Berechtigungsobjekte	765
7.2.3	Rollen	766
7.2.3.1	Die Rollenpflege	766
7.2.3.2	Sammelrollen	769
7.2.3.3	Tabellen und Reports zu Rollen	771
7.2.3.4	Änderungsbelege zu Rollenänderungen	772
7.2.4	Profile	773
7.2.5	Berechtigungen	776
7.2.6	Berechtigungsprüfungen in ABAP-Programmen.	778
7.2.7	Ablauf einer Berechtigungsprüfung im SAP-System	778
7.2.8	Zugriffsrechte	779
7.2.9	Checkliste zur Funktionsweise des Berechtigungs- konzeptes	779
7.2.10	Praktische Prüfung zur Funktionsweise des Berechtigungskonzeptes	780
7.3	Konzepte zum SAP-Berechtigungswesen	781
7.3.1	Übersicht über die Konzepte.	781
7.3.2	Das Dateneigentümerkonzept	782
7.3.3	Das Antrags-, Test- und Freigabeverfahren für Berechtigungen	783
7.3.3.1	Das Antragsverfahren für Benutzer	783
7.3.3.2	Das Antragsverfahren für Rollen.	786
7.3.4	Der Ablauf der Benutzerverwaltung.	787
7.3.5	Konzept für übergreifende Berechtigungen.	788
7.3.6	Das interne Kontrollsystem für SAP-Berechtigungen	789
7.3.7	Namenskonventionen für Rollen	790
7.3.8	Konventionen für die technische Rollenausprägung	791

7.3.9	Rollenkonzepte	792
7.3.10	Modul- und systemspezifische Teilkonzepte	793
7.3.11	Berechtigungen in Eigenentwicklungen	794
7.3.12	Sicherheitskonzept zum Berechtigungskonzept	794
7.3.13	Checkliste zu den Konzepten	796
7.3.14	Praktische Prüfung zu den Konzepten	798
7.4	Customizing zum Berechtigungswesen	798
7.4.1	Systemparameter	798
7.4.2	Benutzermenüs	800
7.4.3	Customizing-Schalter in Tabelle PRGN_CUST	803
7.4.4	Deaktivierte Berechtigungsobjekte	804
7.4.5	Deaktivierung von einzelnen Berechtigungs- prüfungen	806
7.4.6	Transaktionsaufrufe durch CALL TRANSACTION	808
7.4.7	Zugriffsrechte	810
7.4.7.1	Prüfen im SAP-System	810
7.4.7.2	Prüfen mit CheckAud® for SAP® Systems	812
7.4.8	Checkliste zum Customizing des Berechtigungs- konzeptes	812
7.4.9	Praktische Prüfung zum Customizing des Berechtigungskonzeptes	814
7.5	Praktische Prüfung von Zugriffsrechten	816
7.5.1	Referenzbenutzer	816
7.5.2	Kritische Standardprofile.	818
7.5.2.1	Übersicht	818
7.5.2.2	SAP_ALL	818
7.5.2.3	SAP_NEW	820
7.5.2.4	Kritische Profile der Basis	820
7.5.2.5	Kritische Profile zu den Modulen.	821
7.5.3	Zugriffsrechte für Benutzer auswerten (Report RSUSR002)	822
7.5.4	Zugriffsrechte für Rollen auswerten (Report RSUSR070)	825
7.5.5	Nutzung von Tabellen für Berechtigungsprüfungen	827
7.5.5.1	Erforderliche Berechtigungen	827
7.5.5.2	Die Tabellen der Benutzer und Profile	827
7.5.5.3	Tabellen der Rollenverwaltung	829
7.5.6	Fehlersuche in Berechtigungen	831
7.5.6.1	Die Transaktion SU53.	831
7.5.6.2	Der Berechtigungs-Trace	832
7.5.7	Berechtigungen für Prüfer	834
7.6	Zugriffsrechte im Bereich der Berechtigungsverwaltung	836
7.6.1	Zugriffsrechte zur Benutzerverwaltung.	836

Inhaltsverzeichnis

- 7.6.2 Zugriffsrechte zur Rollenverwaltung 841
- 7.6.3 Zugriffsrechte zu Profilen. 841
- 7.7 Reports, Tabellen und Transaktionen. 842
- 7.8 QuickWins. 845

- 8 Anhang 847**
- 8.1 Checklisten zur Systemprüfung. 847
 - 8.1.1 Die Systemsicherheit 847
 - 8.1.2 Der Verbuchungsvorgang 863
 - 8.1.3 Benutzerauswertungen 867
 - 8.1.4 Die Tabellenpflege. 878
 - 8.1.5 Entwicklungen in SAP-Systemen 884
 - 8.1.6 Das Berechtigungskonzept 896
- 8.2 Reports zur Systemprüfung 901
- 8.3 Tabellen zur Systemprüfung. 904
- 8.4 Transaktionen zur Systemprüfung 908
- 8.5 Leitfäden zur SAP-Systemsicherheit 912
 - 8.5.1 Der DSAG-Prüfleitfaden SAP ERP 6.0. 912
 - 8.5.2 Der DSAG-Datenschutzleitfaden SAP ERP 6.0. 914
 - 8.5.3 Die SAP-Sicherheitsleitfäden 915
 - 8.5.4 Das BSI IT-Grundschutzhandbuch –
Baustein SAP-System 916
- 8.6 Literaturhinweise 917

- 9 Glossar 919**

- Stichwortverzeichnis 931**