

Inhalt

Vorwort 11

1 Einführung 13

1.1 Hinweise zum Buch 13

1.1.1 Kapitelübersicht 14

1.1.2 Zielgruppe 15

1.1.3 Abgrenzung 16

1.2 SAP R/3-Umfeld 17

1.2.1 SAP R/3-Sicherheitsaspekte 18

1.2.2 IT-Infrastruktur 20

1.2.3 Integration der Sicherheitsaspekte und der Infrastruktur 21

1.2.4 Weiterentwicklung mit Webarchitektur (ITS) 24

1.2.5 mySAP Workplace/SAP Portal 25

1.3 Komplexe Systemlandschaften 27

1.4 Fazit 30

2 SAP R/3-Benutzer und Berechtigungen 31

2.1 Vorbemerkung – Sicherheit im SAP R/3-System 31

2.1.1 Risiken 31

2.1.2 Ziele 32

2.1.3 Aufwand 32

2.1.4 Nutzen 33

2.1.5 Umfeld 33

2.2 Benutzer – der SAP R/3-Anwender 34

2.2.1 Benutzerstammsatz 34

2.2.2 Benutzergruppen 39

2.2.3 Benutzertypen 39

2.2.4 Kennwort-Regelungen 40

2.2.5 SAP R/3-Standardbenutzer 43

2.2.6 Relevante SAP-Tabellen für Benutzerstammsätze 44

2.3 Das SAP R/3-Berechtigungskonzept 45

2.3.1 Profilgenerator 46

2.3.2 Transaktionen, Berechtigungsobjekte und Berechtigungen 47

2.3.3 Unternehmensstruktur und Organisationsebenen 51

2.3.4 Rollen 52

2.3.5 Berechtigungsprofile 55

2.3.6 Technische Vorgehensweise – SAP-Profilgenerator 56

2.3.7 Namenskonventionen 60

2.3.8 Relevante SAP-Tabellen für Berechtigungen und Rollen 61

2.3.9 Aufgabenteilung in der Administration 63

2.4	Systemvoreinstellungen	64
2.4.1	Instanzen und Profilparameter	66
2.4.2	Übernahme der SAP-Vorschläge in die Kundentabellen	67
2.5	Berechtigungsprüfungen in den SAP-Anwendungen	70
2.6	Schutz von Tabellen	78
2.7	Schutz von Reports	81
2.7.1	Einführung in ABAP/4-Programme – Vorbemerkungen	81
2.7.2	Nutzung eigenentwickelter Transaktionen	83
2.8	Basissicherheit	83
2.8.1	Vorbemerkung	84
2.8.2	Betroffene Basisberechtigungen	84
2.9	HR-Sicherheit	89
2.9.1	Berechtigungsobjekte – Berechtigungshauptschalter	90
2.9.2	Personalnummernprüfung	92
2.9.3	Zusätzliche Stammdatenprüfung	94
2.9.4	Strukturelle Berechtigungen	94
2.9.5	Weitere aktivierbare Berechtigungsprüfungen	98
2.9.6	Fazit	98
2.10	Neuerungen zum Release 4.6	99
2.11	Zentrale Benutzerverwaltung und Global User Manager	102
2.11.1	Zentrale Benutzerverwaltung	102
2.11.2	Global User Manager	103
2.12	Historie der SAP-Technologien im Berechtigungsumfeld	104
2.12.1	Hintergrund	104
2.12.2	Objektorientiertes Konzept	105
2.12.3	Objektorientiertes Konzept mit S_TCODE	105
2.12.4	Migration und Migrationstools	106
2.13	Zusammenfassung und Fazit	107
2.13.1	Systemzugriffsschutz	107
2.13.2	Benutzerverwaltung	108
2.13.3	Berechtigungskonzept	108
2.13.4	Dokumentation des Zugriffsschutzsystems	110
2.13.5	Aufbewahrungsfristen	111
2.14	Wichtige SAP-Hinweise im Berechtigungsumfeld	111
3	Einbettung in das interne Kontrollsystem	113
3.1	Notwendigkeit eines internen Kontrollsystems	114
3.1.1	Ermittlung des Risikoumfeldes	116
3.1.2	Identifikation der Risikoquelle (Prozesse, Bereiche etc.)	120
3.1.3	Risikoanalyse	120
3.2	Überführung in die Kontrollumgebung	123
3.2.1	Struktur der Kontrollumgebung	124

3.2.2	Anforderungen an eine Kontrollumgebung	125
3.2.3	Kontrolltypen	127
3.2.4	Kontrollansätze	129
3.3	Identifikation der Umsetzung	130
3.3.1	SAP R/3-Berechtigungskonzept	130
3.3.2	Realisierung – Einschränkungen	132
3.3.3	Kompensierende Kontrollen	133
3.3.4	Einordnung der Berechtigungskontrollen	133
3.3.5	Dokumentation der Kontrollen	134
3.4	Monitoring und Prüfung des IKS	134
3.4.1	Interne Revision	134
3.4.2	Externer Wirtschaftsprüfer	135
3.4.3	Unternehmensbewusstsein	135
4	Vorgehensmodell beim Design eines Berechtigungskonzeptes	137
4.1	Das IBM-Phasenmodell	137
4.1.1	Überblick	137
4.1.2	Projektvorbereitung und Rahmenbedingungen	138
4.1.3	Definition der Funktionen (Rollen) im Unternehmen	139
4.1.4	Design-Grobkonzept – Erstellung einer Aufgaben/Funktionen- Matrix	141
4.1.5	Design-Feinkonzept – Erstellung einer Organisations- und Wertematrix	145
4.1.6	Realisierung – Erstellung der Einzelrollen und -profile	146
4.1.7	Realisierung – Erstellung der Sammelrollen	147
4.1.8	Test, Dokumentation und Review	147
4.1.9	Einrichtung der Benutzerstammsätze	148
4.1.10	Erstellung eines Betreuungskonzeptes	148
4.1.11	Produktivvorbereitung – Know-how-Transfer und Schulung	148
4.1.12	Anlaufbetreuung und Go-Live-Support	148
4.1.13	Monitoring und Review	149
4.2	Beteiligte Partelen	149
4.2.1	Allgemeines	149
4.2.2	Steering Committee	151
4.2.3	Projektleitung	152
4.2.4	Revision	152
4.2.5	Modul- bzw. Prozessspezialisten	152
4.2.6	Ansprechpartner aus den Fachbereichen	153
4.2.7	Benutzer- und Berechtigungsverwaltung	153
4.3	Wesentliche Aspekte im Detail	154
4.3.1	Die elf Grundregeln	154
4.3.2	Rahmenbedingungen	156
4.3.3	Detaillierungsgrad eines SAP-Berechtigungskonzeptes	157
4.3.4	Dokumentation der Berechtigungsrollen	159

- 4.3.5 Template-Ansatz 162
- 4.3.6 Namenskonventionen 165
- 4.4 Definition der Arbeitsbereiche 172
- 4.4.1 Definition des verwendeten SAP-Funktionsumfangs 172
- 4.4.2 Vorgehen bei der Definition der Rollen im Unternehmen 172

5 Vorgehensmodell zur Realisierung eines Berechtigungskonzeptes 179

- 5.1 Übersicht 179
- 5.2 Realisierung 180
 - 5.2.1 Der Profilgenerator – Übersicht 180
 - 5.2.2 Initialisierung des Profilgenerators 185
 - 5.2.3 Von SAP zur Verfügung gestellte Rollen 187
 - 5.2.4 Benutzermenüs 188
 - 5.2.5 Generieren der Berechtigungen 189
 - 5.2.6 Kopieren von Rollen und Vererbung 193
 - 5.2.7 Sammelrollen 195
- 5.3 Test der implementierten Rollen 196
 - 5.3.1 Voraussetzungen 196
 - 5.3.2 Unit-Test 198
 - 5.3.3 Rollenintegrations-Test 198
 - 5.3.4 User-Acceptance-Test 199
 - 5.3.5 Abschließender Review 199
 - 5.3.6 Technische Durchführung der Rollentests 199
 - 5.3.7 Manuelle Pflege von Berechtigungsdaten 203
- 5.4 Einrichten der Benutzerstammsätze 206
- 5.5 Produktivstart 207
- 5.6 Laufender Betrieb 208
 - 5.6.1 Das Berechtigungskonzept im Produktivbetrieb 208
 - 5.6.2 Benutzer- und Rollenadministration 208
 - 5.6.3 Change-Request-Verfahren 210
- 5.7 Notfallkonzept 214
 - 5.7.1 Hintergrund 214
 - 5.7.2 Mehrstufiges Notfallkonzept 215
 - 5.7.3 Abläufe und Prozesse für Beantragung und Protokollierung 216
- 5.8 Technische Details 216
 - 5.8.1 Infosystem »Berechtigungen« 216
 - 5.8.2 Reduzieren des Umfangs von Berechtigungsprüfungen 217
 - 5.8.3 SAP_ALL und SAP_NEW 218

6	Prüfung von SAP R/3-Berechtigungskonzepten	219
6.1	Benutzerinformationssystem	220
6.1.1	Struktur	220
6.1.2	Fazit	223
6.2	Audit Information System	223
6.2.1	Historie	223
6.2.2	Ansatz	223
6.2.3	Struktur	224
6.2.4	System Audit	227
6.2.5	AIS-Teilbaum »Benutzerverwaltung«	230
6.2.6	Berechtigungen für das AIS	232
6.2.7	Rollenkonzept des AIS	232
6.2.8	Berechtigungen für die Prüfung von Berechtigungskonzepten	235
6.2.9	Datengewinnung und Auswerttechniken	237
6.2.10	Fazit	238
6.2.11	Weitere Informationen zum AIS	239
6.3	Direkter Tabellenzugriff	239
6.4	Ergänzende Prüfungsfelder	240
6.5	Weitere Prüfwerkzeuge	241
6.5.1	SAPAudit – CheckAud	241
6.5.2	ACE	243
6.5.3	APM	244
6.5.4	Weitere Tools	245
6.5.5	Fazit	246

7	SAP Enterprise Portal	247
7.1	Allgemeine Aspekte	247
7.2	Komponenten des Portals	249
7.2.1	Webserver	249
7.2.2	Applikationsserver	250
7.2.3	Laufzeit- und Entwicklungsumgebung	250
7.2.4	Verzeichnisdienst	250
7.2.5	Datenbank	250
7.2.6	Suchmaschinen	251
7.3	Zusammenspiel Portal und SAP R/3	251
7.3.1	Drag&Relate	253
7.4	Zugriffssteuerung und Verwaltung	254
7.4.1	Identifizierung und Authentisierung	255
7.4.2	Benutzerverwaltung	258
7.4.3	Rolle	260
7.4.4	Personalisierung	261
7.4.5	Synchronisierung	262
7.4.6	Single Sign-On	263

7.5	Weitere Sicherheitsmaßnahmen	267
7.5.1	Anforderungen	267
7.5.2	Risiken	267
7.5.3	Physische Sicherheit	269
7.5.4	Organisatorische Sicherheit	270
7.5.5	Einspielen von Aktualisierungen	271
7.5.6	Antivirus-Software	271
7.5.7	Sicherheitszone zum Internet	271
7.5.8	Intrusion Detection System	272
7.5.9	Verschlüsselung und Integritätssicherung	272
7.5.10	Sichere Konfiguration des Betriebssystems	273
7.5.11	Zusammenfassung	273

8 Zukünftige Entwicklungen und Wege 275

8.1	Vorbemerkungen	275
8.1.1	Zugriff auf Unternehmensverzeichnisse (LDAP)	276
8.1.2	Zentrale Benutzerverwaltung	277
8.1.3	Berechtigungs- und Rollenadministration (SAP Web AS)	279
8.1.4	Benutzerauthentifizierung	280
8.2	Weitere Themenpunkte	282
8.2.1	Auditing, Logging und Intrusion-Detection-Systeme	282
8.2.2	Weitere Transaktionen	283
8.2.3	Digitale Signaturen	283
8.3	Ausblick	284

Anhang

A	Berechtigungsobjekte	285
B	SAP-Hinweise	291
C	Literaturverzeichnis	295
D	Die Autoren	298
	Index	301