

Inhalt

Vorwort	19
Danksagung	21

1 Einleitung 23

Teil I Betriebswirtschaftliche Konzeption

2 Einführung und Begriffsdefinition 31

2.1	Methodische Überlegungen	32
2.1.1	Ansätze für das betriebswirtschaftliche Berechtigungskonzept	33
2.1.2	Beteiligte am Berechtigungskonzept	35
2.2	Compliance ist Regelkonformität	36
2.3	Risiko	37
2.4	Corporate Governance	41
2.5	Technische versus betriebswirtschaftliche Bedeutung des Berechtigungskonzepts	43
2.6	Technische vs. betriebswirtschaftliche Rolle	45
2.7	Beschreibung von Berechtigungskonzepten	47
2.7.1	Role Based Access Control	47
2.7.2	Core RBAC und SAP ERP	50
2.7.3	Hierarchical RBAC und SAP ERP – limitierte Rollenhierarchien	55
2.7.4	Hierarchical RBAC und SAP – allgemeine Rollenhierarchien	56
2.7.5	Constrained RBAC	56
2.7.6	Constrained RBAC und SAP ERP	58
2.7.7	Restriktionen des RBAC-Standards	58
2.7.8	Beschreibung technischer Berechtigungskonzepte	59

3 Organisation und Berechtigungen 61

3.1	Organisatorische Differenzierung am Beispiel	63
3.2	Begriff der Organisation	65
3.3	Institutioneller Organisationsbegriff	66
3.4	Instrumenteller Organisationsbegriff	70

3.4.1	Aufbauorganisation	70
3.4.2	Aufgabenanalyse	79
3.5	Folgerungen aus der Organisationsbetrachtung	84
3.6	Sichten der Aufbauorganisation in SAP-Systemen	85
3.6.1	Organisationsmanagement	86
3.6.2	Organisationssicht des externen Rechnungswesens	87
3.6.3	Organisationssicht des Haushalts- managements	88
3.6.4	Organisationssicht der Kostenstellenstandardhierarchie	89
3.6.5	Organisationssicht der Profit-Center-Hierarchie	90
3.6.6	Unternehmensorganisation	91
3.6.7	Organisationssicht im Projektsystem	92
3.6.8	Logistische Organisationssicht	93
3.6.9	Integration der Organisationssichten im Berechtigungskonzept	93
3.7	Organisationsebenen und -strukturen in SAP ERP	94
3.7.1	Organisationsebene »Mandant«	95
3.7.2	Relevante Organisationsebenen des Rechnungswesens	96
3.7.3	Relevante Organisationsebenen in der Materialwirtschaft	99
3.7.4	Relevante Organisationsebenen im Vertrieb	100
3.7.5	Relevante Organisationsebenen in der Lagerverwaltung	101
3.7.6	Integration der Organisationsebenen im Berechtigungskonzept	101
3.8	Hinweise zur Methodik im Projekt	102
3.9	Fazit	105

4 Rechtlicher Rahmen – normativer Rahmen 107

4.1	Interne und externe Regelungsgrundlagen	108
4.2	Internes Kontrollsystem	112
4.3	Rechtsquellen des externen Rechnungswesens	113
4.3.1	Rechtsquellen und Auswirkungen für den privaten Sektor	115

4.3.2	Konkrete Anforderungen an das Berechtigungskonzept	118
4.4	Datenschutzrecht	118
4.4.1	Gesetzliche Definitionen in Bezug auf die Datenverarbeitung	121
4.4.2	Rechte des Betroffenen	122
4.4.3	Pflichten in Bezug auf das IKS	123
4.4.4	Konkrete Anforderungen an das Berechtigungskonzept	124
4.4.5	Regelkonformität versus Datenschutz	125
4.5	Allgemeine Anforderungen an ein Berechtigungskonzept	126
4.5.1	Identitätsprinzip	128
4.5.2	Minimalprinzip	128
4.5.3	Stellenprinzip	129
4.5.4	Belegprinzip der Buchhaltung	130
4.5.5	Belegprinzip der Berechtigungsverwaltung	130
4.5.6	Funktionstrennungsprinzip	131
4.5.7	Genehmigungsprinzip	131
4.5.8	Standardprinzip	131
4.5.9	Schriftformprinzip	132
4.5.10	Kontrollprinzip	132
4.6	Fazit	133

5 Berechtigungen in der Prozesssicht 135

5.1	Prozessübersicht	135
5.2	Der Verkaufsprozess	137
5.3	Der Beschaffungsprozess	143
5.4	Unterstützungsprozesse	147
5.5	Maßgaben für die Funktionstrennung	150
5.6	Fazit	152

Teil II Werkzeuge und Berechtigungspflege im SAP-System

6 Technische Grundlagen der Berechtigungspflege ... 155

6.1	Benutzer	156
6.2	Berechtigungen	164

6.2.1	Berechtigungsfelder und Berechtigungsobjekte	164
6.2.2	Berechtigungsprüfungen für ABAP-Programme	166
6.3	Rollen und Profile	169
6.3.1	Manuelle Profile und Berechtigungen	170
6.3.2	Rollenpflege	171
6.4	Transfer von Rollen	209
6.4.1	Rollentransport	209
6.4.2	Down-/Upload von Rollen	211
6.5	Benutzerabgleich	212
6.6	Vom Trace zur Rolle	214
6.7	Weitere Auswertungen von Berechtigungsprüfungen	221
6.7.1	Auswertung der Berechtigungsprüfung	221
6.7.2	Prüfung des Programms	223
6.8	Fazit	225

7 Systemeinstellungen und Customizing 227

7.1	Pflege und Nutzung der Vorschläge für den Profilgenerator	228
7.1.1	Grundzustand und Pflege der Berechtigungsvorschlagswerte	230
7.1.2	Nutzen der Berechtigungsvorschlagswerte	240
7.2	Traces	247
7.2.1	Vorgehen beim Berechtigungstrace	249
7.2.2	Vorgehen beim System-Trace	251
7.3	Upgrade von Berechtigungen	252
7.4	Parameter für Kennwortregeln	259
7.5	Menükonzept	262
7.6	Berechtigungsgruppen	268
7.6.1	Optionale Berechtigungsprüfungen auf Berechtigungsgruppen	270
7.6.2	Tabellenberechtigungen	276
7.6.3	Berechtigungsgruppen als Organisationsebenen	281
7.7	Parameter- und Query-Transaktionen	283

7.7.1	Parametertransaktion zur Pflege von Tabellen über definierte Views	285
7.7.2	Parametertransaktion zur Ansicht von Tabellen	288
7.7.3	Queries in Transaktionen umsetzen	289
7.8	Anhebung eines Berechtigungsfeldes zur Organisationsebene	291
7.8.1	Auswirkungsanalyse	292
7.8.2	Vorgehen zur Anhebung eines Feldes zur Organisationsebene	296
7.8.3	Anhebung des Verantwortungsbereichs zur Organisationsebene	297
7.9	Berechtigungsfelder und -objekte anlegen	300
7.9.1	Berechtigungsfelder anlegen	300
7.9.2	Berechtigungsobjekte anlegen	301
7.10	Weitere Transaktionen der Berechtigungsadministration	304
7.11	Rollen zwischen Systemen oder Mandanten bewegen	306
7.11.1	Down-/Upload von Rollen	306
7.11.2	Transport von Rollen	307
7.12	Benutzerstammabgleich	308
7.13	Fazit	308

8 Rollenzuordnung über das Organisationsmanagement 311

8.1	Grundkonzept des SAP ERP HCM- Organisationsmanagements	312
8.2	Fachliche Voraussetzungen	314
8.3	Technische Umsetzung	315
8.3.1	Voraussetzungen	315
8.3.2	Technische Grundlagen des SAP ERP HCM-Organisationsmanagements	315
8.3.3	Zuweisung von Rollen	316
8.3.4	Auswertungsweg	318
8.3.5	Benutzerstammabgleich	318
8.4	Konzeptionelle Besonderheit	319
8.5	Fazit	319

9 Zentrales Management von Benutzern und Berechtigungen 321

9.1	Grundlagen	322
9.1.1	Betriebswirtschaftlicher Hintergrund	322
9.1.2	User Lifecycle Management	325
9.1.3	SAP-Lösungen für die zentrale Verwaltung von Benutzern	328
9.2	Zentrale Benutzerverwaltung	328
9.2.1	Vorgehen zur Einrichtung einer ZBV	330
9.2.2	Integration mit dem Organisations- management von SAP ERP HCM	335
9.2.3	Integration mit SAP Access Control	336
9.3	SAP Access Control User Access Management	337
9.4	SAP NetWeaver Identity Management	345
9.4.1	Relevante technische Details	347
9.4.2	Funktionsweise	348
9.4.3	Technische Architektur	354
9.4.4	Integration mit SAP Access Control	359
9.5	Fazit	362

10 Berechtigungen: Standards und Analyse 363

10.1	Standards und ihre Analyse	364
10.1.1	Rolle anstelle von Profil	364
10.1.2	Definition der Rolle über das Menü	365
10.1.3	Vorschlagsnutzung	367
10.1.4	Tabellenberechtigungen	367
10.1.5	Programmausführungsberechtigungen	368
10.1.6	Ableitung	369
10.1.7	Programmierung – Programmierrichtlinie	370
10.2	Kritische Transaktionen und Objekte	372
10.3	Allgemeine Auswertungen technischer Standards	374
10.3.1	Benutzerinformationssystem	374
10.3.2	Tabellengestützte Analyse von Berechtigungen	377
10.4	AGS Security Services	381
10.4.1	Secure Operations Standard und Secure Operations Map	382

10.4.2	Berechtigungs-Checks im SAP EarlyWatch Alert und Security Optimization Service	384
10.4.3	Reporting über die Zuordnung kritischer Berechtigungen mithilfe der Configuration Validation	390
10.5	Fazit	392

11 SAP Access Control 393

11.1	Grundlagen	393
11.2	Access Risk Analysis	397
11.3	Business Role Management	403
11.4	User Access Management	405
11.5	Emergency Access Management	407
11.6	Risk Terminator	410
11.7	Fazit	411

12 User Management Engine 413

12.1	Überblick über die UME	414
12.1.1	UME-Funktionen	414
12.1.2	Architektur der UME	416
12.1.3	Oberfläche der UME	417
12.1.4	Konfiguration der UME	419
12.2	Berechtigungskonzept von SAP NetWeaver AS Java	422
12.2.1	UME-Rollen	422
12.2.2	UME-Aktionen	423
12.2.3	UME-Gruppe	425
12.2.4	Java-EE-Sicherheitsrollen	427
12.3	Benutzer- und Rollenadministration mit der UME ...	427
12.3.1	Voraussetzungen zur Benutzer- und Rollenadministration	428
12.3.2	Administration von Benutzern	428
12.3.3	Benutzertypen	430
12.3.4	Administration von UME-Rollen	431
12.3.5	Administration von UME-Gruppen	432
12.3.6	Tracing und Logging	432
12.4	Fazit	434

Teil III Berechtigungen in spezifischen SAP-Lösungen

13 Berechtigungen in SAP ERP HCM 437

13.1	Grundlagen	437
13.2	Besondere Anforderungen von SAP ERP HCM	438
13.3	Berechtigungen und Rollen	440
13.3.1	Berechtigungsrelevante Attribute in SAP ERP HCM	441
13.3.2	Beispiel »Personalmaßnahme«	442
13.4	Berechtigungshauptschalter	446
13.5	Organisationsmanagement und indirekte Rollenzuordnung	448
13.6	Strukturelle Berechtigungen	450
13.6.1	Strukturelles Berechtigungsprofil	451
13.6.2	Auswertungsweg	452
13.6.3	Strukturelle Berechtigungen und Performance	454
13.6.4	Anmerkung zu strukturellen Berechtigungen	454
13.7	Kontextsensitive Berechtigungen	455
13.8	Fazit	457

14 Berechtigungen in SAP CRM 459

14.1	Grundlagen	460
14.1.1	Die SAP CRM-Oberfläche: der CRM Web Client	460
14.1.2	Erstellen von Benutzerrollen für den CRM Web Client	468
14.2	Abhängigkeiten zwischen der Benutzerrolle und PFCG-Rollen	469
14.3	Erstellen von PFCG-Rollen abhängig von Benutzerrollen	471
14.3.1	Voraussetzungen für das Erstellen von PFCG-Rollen	471
14.3.2	Erstellen von PFCG-Rollen	477
14.4	Zuweisen von Benutzerrollen und PFCG-Rollen	482
14.5	Beispiele für Berechtigungen in SAP CRM	490

14.5.1	Berechtigten von Oberflächenkomponenten	490
14.5.2	Berechtigten von Transaktionsstarter-Links	500
14.5.3	Sonstige Berechtigungsmöglichkeiten für den CRM Web Client	502
14.5.4	Berechtigten von Stammdaten	504
14.5.5	Berechtigten von Geschäftsvorgängen	507
14.5.6	Berechtigten von Attributgruppen	518
14.5.7	Berechtigten von Marketingelementen	519
14.6	Fehlersuche im CRM Web Client	521
14.7	Access-Control-Engine	524
14.8	Fazit	539

15 Berechtigungen in SAP SRM 541

15.1	Grundlagen	541
15.2	Berechtigungsvergabe in SAP SRM	544
15.2.1	Berechtigten der Oberflächenmenüs	548
15.2.2	Berechtigten typischer Geschäftsvorgänge ...	550
15.3	Fazit	565

16 Berechtigungen in SAP NetWeaver BW 567

16.1	OLTP-Berechtigungen	568
16.2	Analyseberechtigungen	570
16.2.1	Grundlagen	571
16.2.2	Schrankenprinzip	573
16.2.3	Transaktion RSECADMIN	574
16.2.4	Berechtigungspflege	574
16.2.5	Massenpflege	577
16.2.6	Zuordnung zu Benutzern	578
16.2.7	Analyse und Berechtigungsprotokoll	582
16.2.8	Generierung	585
16.2.9	Berechtigungs migration	587
16.3	Modellierung von Berechtigungen in SAP NetWeaver BW	588
16.3.1	InfoProvider-basierte Modelle	589
16.3.2	Merkmalsbasierte Modelle	589
16.3.3	Gemischte Modelle	590

16.4	RBAC-Modell	590
16.5	Fazit	592

17 Berechtigungen in der SAP BusinessObjects Business Intelligence-Plattform 4.x 593

17.1	Berechtigungskonzept	593
17.1.1	Benutzer und Benutzergruppen	595
17.1.2	Objekte, Ordner, Kategorien	598
17.1.3	Zugriffsberechtigungen	599
17.2	Interaktion mit SAP NetWeaver BW	602
17.2.1	System für Endbenutzer anschließen	603
17.2.2	Beispiel einer Anwendung: Query in Web Intelligence einbinden	604
17.3	Fazit	606

18 Berechtigungen in SAP HANA 609

18.1	Architektur von SAP HANA	610
18.2	Anwendungsszenarien von SAP HANA	611
18.3	Objekte des Berechtigungswesens in SAP HANA	614
18.3.1	Benutzer	615
18.3.2	Privilegien	617
18.3.3	Rollen	620
18.3.4	Beispiel	621
18.4	Fazit	622

19 Prozesse in SAP ERP – spezifische Berechtigungen 625

19.1	Grundlagen	626
19.1.1	Stamm- und Bewegungsdaten	626
19.1.2	Organisationsebenen	627
19.2	Berechtigungen im Finanzwesen	628
19.2.1	Organisatorische Differenzierungs- kriterien	629
19.2.2	Stammdaten	631
19.2.3	Buchungen	643
19.2.4	Zahllauf	648
19.3	Berechtigungen im Controlling	650
19.3.1	Organisatorische Differenzierungs- kriterien	651

19.3.2	Stammdatenpflege	652
19.3.3	Buchungen	661
19.3.4	Altes und neues Berechtigungskonzept im Controlling	663
19.4	Berechtigungen in der Logistik (allgemein)	664
19.4.1	Organisatorische Differenzierungs- kriterien	664
19.4.2	Materialstamm/Materialart	666
19.5	Berechtigungen im Einkauf	669
19.5.1	Stammdatenpflege	670
19.5.2	Beschaffungsabwicklung	670
19.6	Berechtigungen im Vertrieb	676
19.6.1	Stammdatenpflege	676
19.6.2	Verkaufsabwicklung	678
19.7	Berechtigungen in technischen Prozessen	681
19.7.1	Funktionstrennung in der Berechtigungsverwaltung	681
19.7.2	Funktionstrennung im Transportwesen	684
19.7.3	RFC-Berechtigungen	686
19.7.4	Debugging-Berechtigungen	687
19.7.5	Mandantenänderung	688
19.7.6	Änderungsprotokollierung	689
19.7.7	Batchberechtigungen	690
19.8	Fazit	690

20 Konzepte und Vorgehen im Projekt 693

20.1	Berechtigungskonzept im Projekt	694
20.2	Vorgehensmodell	696
20.2.1	Logischer Ansatz	697
20.2.2	Implementierung	699
20.2.3	Redesign	700
20.2.4	Konkretes Vorgehen	701
20.3	SAP Best Practices-Template-Rollenkonzept	705
20.3.1	SAP Best Practices	705
20.3.2	SAP-Template-Rollen	706
20.3.3	Methodische Vorgehensweise des SAP Best Practices-Rollenkonzepts	708
20.3.4	Einsatz mit SAP Access Control	711
20.4	Inhalte eines Berechtigungskonzepts	712

20.4.1	Einleitung und normativer Rahmen des Konzepts	713
20.4.2	Technischer Rahmen	715
20.4.3	Risikobetrachtung	715
20.4.4	Person – Benutzer – Berechtigung	716
20.4.5	Berechtigungsverwaltung	717
20.4.6	Organisatorische Differenzierung	718
20.4.7	Prozessdokumentation	718
20.4.8	Rollendokumentation	718
20.5	Schritte zum Berechtigungskonzept	719
20.6	Fazit	721

Anhang 723

A	Abkürzungsverzeichnis	725
B	Glossar	729
C	Literaturverzeichnis	745
D	Die Autoren	751
Index		755