

Inhalt

Vorwort	21
Danksagung	23

1 Einleitung 27

TEIL I Betriebswirtschaftliche Konzeption

2 Einführung und Begriffsdefinition 35

2.1	Methodische Überlegungen	36
2.1.1	Ansätze für das betriebswirtschaftliche Berechtigungskonzept	37
2.1.2	Beteiligte am Berechtigungskonzept	39
2.2	Compliance ist Regelkonformität	40
2.3	Risiko	41
2.4	Corporate Governance	45
2.5	Technische vs. betriebswirtschaftliche Bedeutung des Berechtigungskonzepts	47
2.6	Technische vs. betriebswirtschaftliche Rolle	49
2.7	Beschreibung von Berechtigungskonzepten	51
2.7.1	Role Based Access Control	51
2.7.2	Core RBAC und SAP ERP	54
2.7.3	Hierarchical RBAC und SAP ERP – limitierte Rollenhierarchien	60
2.7.4	Hierarchical RBAC und SAP – allgemeine Rollenhierarchien	60
2.7.5	Constrained RBAC	61
2.7.6	Constrained RBAC und SAP ERP	63
2.7.7	Restriktionen des RBAC-Standards	64
2.7.8	Beschreibung technischer Berechtigungskonzepte	65

3 Organisation und Berechtigungen 67

3.1	Organisatorische Differenzierung am Beispiel	69
3.2	Begriff der Organisation	71
3.3	Institutioneller Organisationsbegriff	72

3.4	Instrumenteller Organisationsbegriff	76
3.4.1	Aufbauorganisation	77
3.4.2	Aufgabenanalyse	85
3.5	Folgerungen aus der Organisationsbetrachtung	90
3.6	Die Grenzen der Organisation und das Internet der Dinge	91
3.7	Sichten der Aufbauorganisation in SAP-Systemen	92
3.7.1	Organisationsmanagement	93
3.7.2	Organisationssicht des externen Rechnungswesens	95
3.7.3	Organisationssicht des Haushaltsmanagements	96
3.7.4	Organisationssicht der Kostenstellenstandardhierarchie	97
3.7.5	Organisationssicht der Profit-Center- Hierarchie	97
3.7.6	Unternehmensorganisation	98
3.7.7	Organisationssicht im Projektsystem	99
3.7.8	Logistische Organisationssicht	100
3.7.9	Integration der Organisationssichten im Berechtigungskonzept	100
3.8	Organisationsebenen und -strukturen in der SAP Business Suite	101
3.8.1	Organisationsebene »Mandant«	102
3.8.2	Relevante Organisationsebenen des Rechnungswesens	103
3.8.3	Relevante Organisationsebenen in der Materialwirtschaft	107
3.8.4	Relevante Organisationsebenen im Vertrieb	108
3.8.5	Relevante Organisationsebenen in der Lagerverwaltung	108
3.8.6	Integration der Organisationsebenen im Berechtigungskonzept	108
3.9	Hinweise zur Methodik im Projekt	110
3.10	Fazit	112

4 Rechtlicher Rahmen – normativer Rahmen 113

4.1	Interne und externe Regelungsgrundlagen	114
4.2	Internes Kontrollsystem	118

4.3	Rechtsquellen des externen Rechnungswesens	120
4.3.1	Rechtsquellen und Auswirkungen für den privaten Sektor	121
4.3.2	Konkrete Anforderungen an das Berechtigungskonzept	124
4.4	Datenschutzrecht	124
4.4.1	Gesetzliche Definitionen in Bezug auf die Datenverarbeitung	128
4.4.2	Rechte des Betroffenen	129
4.4.3	Pflichten in Bezug auf das IKS	130
4.4.4	Vereinfachtes Sperren und Löschen personenbezogener Daten – Auswirkungen auf das Berechtigungskonzept	131
4.4.5	Konkrete Anforderungen an das Berechtigungskonzept	133
4.4.6	Regelkonformität vs. Datenschutz	134
4.5	Allgemeine Anforderungen an ein Berechtigungskonzept	135
4.5.1	Identitätsprinzip	137
4.5.2	Minimalprinzip	137
4.5.3	Stellenprinzip	138
4.5.4	Belegprinzip der Buchhaltung	139
4.5.5	Belegprinzip der Berechtigungsverwaltung	139
4.5.6	Funktionstrennungsprinzip	139
4.5.7	Genehmigungsprinzip	140
4.5.8	Standardprinzip	140
4.5.9	Schriftformprinzip	141
4.5.10	Kontrollprinzip	141
4.6	Fazit	142

5 Berechtigungen in der Prozesssicht 143

5.1	Prozessübersicht	143
5.2	Der Verkaufsprozess	145
5.3	Der Beschaffungsprozess	151
5.4	Unterstützungsprozesse	155
5.5	Maßgaben für die Funktionstrennung	158
5.6	Fazit	160

TEIL II Werkzeuge und Berechtigungspflege im SAP-System

6 Technische Grundlagen der Berechtigungspflege ... 163

6.1	Benutzer	163
6.2	Berechtigungen	173
6.2.1	Berechtigungsfelder und Berechtigungsobjekte	173
6.2.2	Berechtigungsprüfungen für ABAP- Programme	174
6.3	Rollen und Profile	176
6.3.1	Manuelle Profile und Berechtigungen	177
6.3.2	Rollenpflege	178
6.3.3	Massenpflege von Rollen	218
6.4	Transfer von Rollen	222
6.4.1	Rollentransport	223
6.4.2	Down-/Upload von Rollen	225
6.5	Benutzerabgleich	225
6.6	Vom Trace zur Rolle	227
6.7	Weitere Auswertungen von Berechtigungsprüfungen	234
6.7.1	Auswertung der Berechtigungsprüfung	234
6.7.2	Prüfung des Programms	236
6.8	Fazit	239

7 Systemeinstellungen und Customizing 241

7.1	Pflege und Nutzung der Vorschläge für den Profilgenerator	242
7.1.1	Grundzustand und Pflege der Berechtigungsvorschlagswerte	244
7.1.2	Nutzen der Berechtigungs- vorschlagswerte	255
7.2	Traces	262
7.2.1	Vorgehen beim Berechtigungstrace	265
7.2.2	Vorgehen beim Systemtrace	269
7.2.3	Vorgehen beim Benutzertrace	270
7.3	Upgrade-Nacharbeiten von Berechtigungen	271
7.4	Parameter für Kennwortregeln	278
7.5	Menükonzept	284
7.6	Berechtigungsgruppen	290

7.6.1	Optionale Berechtigungsprüfungen auf Berechtigungsgruppen	292
7.6.2	Tabellenberechtigungen	297
7.6.3	Berechtigungsgruppen von Programmen ...	303
7.6.4	Berechtigungsgruppen als Organisationsebenen	304
7.7	Parameter- und Query-Transaktionen	305
7.7.1	Parametertransaktion zur Pflege von Tabellen über definierte Views	308
7.7.2	Parametertransaktion zur Ansicht von Tabellen	311
7.7.3	Querys in Transaktionen umsetzen	311
7.7.4	Zuordnung eines Programms zu einem Transaktionscode	314
7.8	Anhebung eines Berechtigungsfeldes zur Organisationsebene	315
7.8.1	Auswirkungsanalyse	315
7.8.2	Vorgehen zur Anhebung eines Feldes zur Organisationsebene	319
7.8.3	Anhebung des Verantwortungsbereichs zur Organisationsebene	321
7.9	Berechtigungsfelder und -objekte anlegen	323
7.9.1	Berechtigungsfelder anlegen	323
7.9.2	Berechtigungsobjekte anlegen	325
7.10	Weitere Transaktionen der Berechtigungsadministration	327
7.11	Fazit	329

8 Rollenzuordnung über das Organisations- management 331

8.1	Grundkonzept des SAP-ERP-HCM- Organisationsmanagements	332
8.2	Fachliche Voraussetzungen	335
8.3	Technische Umsetzung	335
8.3.1	Voraussetzungen	335
8.3.2	Technische Grundlagen des SAP-ERP- HCM-Organisationsmanagements	336
8.3.3	Zuweisung von Rollen	336
8.3.4	Auswertungsweg	338
8.3.5	Benutzerstammabgleich	339

8.4	Konzeptionelle Besonderheit	339
8.5	Fazit	340

9 Zentrales Management von Benutzern und Berechtigungen 341

9.1	Grundlagen	342
9.1.1	Betriebswirtschaftlicher Hintergrund	342
9.1.2	User Lifecycle Management	345
9.1.3	SAP-Lösungen für die zentrale Verwaltung von Benutzern	348
9.2	Zentrale Benutzerverwaltung	348
9.2.1	Vorgehen zur Einrichtung einer ZBV	350
9.2.2	Integration mit dem Organisationsmanagement von SAP ERP HCM	356
9.2.3	Integration mit SAP Access Control	357
9.3	SAP Access Control User Access Management	358
9.4	SAP Identity Management	366
9.4.1	Funktionen	367
9.4.2	Technische Architektur	369
9.4.3	Komponenten und Architektur in SAP Identity Management 8.0	373
9.4.4	Funktionsweise	374
9.4.5	Integration mit SAP Access Control	382
9.5	Compliant Identity Management	383
9.6	Fazit	385

10 Berechtigungen: Standards und Analyse 387

10.1	Standards und ihre Analyse	387
10.1.1	Rolle anstelle von Profil	388
10.1.2	Definition der Rolle über das Menü	389
10.1.3	Vorschlagsnutzung	391
10.1.4	Tabellenberechtigungen	391
10.1.5	Programmausführungsberechtigungen	392
10.1.6	Ableitung	393
10.1.7	Programmierung – Programmier-richtlinie	394
10.2	Kritische Transaktionen und Objekte	396
10.3	Allgemeine Auswertungen technischer Standards	398
10.3.1	Benutzerinformationssystem	398

10.3.2	Tabellengestützte Analyse von Berechtigungen	402
10.4	AGS Security Services	406
10.4.1	Secure Operations Standard und Secure Operations Map	408
10.4.2	Berechtigungs-Checks im SAP Early-Watch Alert und Security Optimization Service	409
10.4.3	Reporting über die Zuordnung kritischer Berechtigungen mithilfe der Configuration Validation	416
10.5	Fazit	418

11 SAP Access Control 419

11.1	Grundlagen	419
11.2	Access Risk Analysis	423
11.3	Business Role Management	429
11.4	User Access Management	431
11.5	Emergency Access Management	433
11.6	Fazit	436

12 User Management Engine 437

12.1	Überblick über die UME	438
12.1.1	UME-Funktionen	438
12.1.2	Architektur der UME	440
12.1.3	Oberfläche der UME	441
12.1.4	Konfiguration der UME	442
12.2	Berechtigungskonzept von SAP NetWeaver AS Java	446
12.2.1	UME-Rollen	446
12.2.2	UME-Aktionen	447
12.2.3	UME-Gruppe	448
12.2.4	Java-EE-Sicherheitsrollen	450
12.3	Benutzer- und Rollenadministration mit der UME ...	451
12.3.1	Voraussetzungen zur Benutzer- und Rollenadministration	451
12.3.2	Administration von Benutzern	452
12.3.3	Benutzertypen	453
12.3.4	Administration von UME-Rollen	454

12.3.5	Administration von UME-Gruppen	456
12.3.6	Tracing und Logging	456
12.4	Fazit	458

TEIL III Berechtigungen in spezifischen SAP-Lösungen

13 Berechtigungen in SAP ERP HCM 461

13.1	Grundlagen	461
13.2	Besondere Anforderungen von SAP ERP HCM	462
13.3	Berechtigungen und Rollen	464
13.3.1	Berechtigungsrelevante Attribute in SAP ERP HCM	464
13.3.2	Beispiel »Personalmaßnahme«	466
13.4	Berechtigungshauptschalter	470
13.5	Organisationsmanagement und indirekte Rollenzuordnung	472
13.6	Strukturelle Berechtigungen	474
13.6.1	Strukturelles Berechtigungsprofil	475
13.6.2	Auswertungsweg	476
13.6.3	Strukturelle Berechtigungen und Performance	478
13.6.4	Anmerkung zu strukturellen Berechtigungen	478
13.7	Kontextsensitive Berechtigungen	479
13.8	Zeitabhängiges Sperren personenbezogener Daten	481
13.8.1	Zeitabhängige Berechtigungsprüfung – Grundsätzliches	481
13.8.2	Ablauf der zeitabhängigen Berechtigungsprüfung	483
13.8.3	Einrichten der zeitabhängigen Berechtigungsprüfung	483
13.9	Fazit	486

14 Berechtigungen in SAP CRM 487

14.1	Grundlagen	488
14.1.1	Die SAP-CRM-Oberfläche: der CRM Web Client	488

14.1.2	Erstellen von Benutzerrollen für den CRM Web Client	496
14.2	Abhängigkeiten zwischen der Benutzerrolle und PFCG-Rollen	498
14.3	Erstellen von PFCG-Rollen abhängig von Benutzerrollen	500
14.3.1	Voraussetzungen für das Erstellen von PFCG-Rollen	500
14.3.2	Erstellen von PFCG-Rollen	503
14.4	Zuweisen von Benutzerrollen und PFCG-Rollen	508
14.5	Beispiele für Berechtigungen in SAP CRM	517
14.5.1	Berechtigen von Oberflächenkomponenten	517
14.5.2	Berechtigen von Transaktionsstarter-Links	526
14.5.3	Sonstige Berechtigungsmöglichkeiten für den CRM Web Client	528
14.5.4	Berechtigen von Stammdaten	530
14.5.5	Berechtigen von Geschäftsvorgängen	533
14.5.6	Berechtigen von Attributgruppen	543
14.5.7	Berechtigen von Marketingelementen	544
14.6	Fehlersuche im CRM Web Client	546
14.7	Access Control Engine	549
14.8	Fazit	563

15 Berechtigungen in SAP SRM 565

15.1	Grundlagen	565
15.2	Berechtigungsvergabe in SAP SRM	568
15.2.1	Berechtigen der Oberflächenmenüs	572
15.2.2	Berechtigen typischer Geschäftsvorgänge ..	574
15.3	Fazit	588

16 Berechtigungen in SAP BW 589

16.1	OLTP-Berechtigungen	590
16.2	Analyseberechtigungen	593
16.2.1	Grundlagen	593
16.2.2	Schrankenprinzip	595
16.2.3	Transaktion RSECADMIN	596
16.2.4	Berechtigungspflege	596

16.2.5	Massenpflege	600
16.2.6	Zuordnung zu Benutzern	600
16.2.7	Analyse und Berechtigungsprotokoll	604
16.2.8	Generierung	607
16.2.9	Berechtigungs migration	609
16.3	Modellierung von Berechtigungen in SAP BW	610
16.3.1	InfoProvider-basierte Modelle	611
16.3.2	Merkmalsbasierte Modelle	611
16.3.3	Gemischte Modelle	612
16.4	RBAC-Modell	612
16.5	Fazit	614

17 Berechtigungen in der SAP-BusinessObjects-Business-Intelligence-Plattform 4.x 615

17.1	Berechtigungskonzept	616
17.1.1	Benutzer und Benutzergruppen	617
17.1.2	Objekte, Ordner, Kategorien	620
17.1.3	Zugriffsberechtigungen	621
17.2	Interaktion mit SAP BW	624
17.2.1	System für Endbenutzer anschließen	625
17.2.2	Beispiel einer Anwendung: Query in Web Intelligence einbinden	626
17.3	Fazit	628

18 RFC-Sicherheit mittels Unified Connectivity 631

18.1	RFC-Sicherheit im Überblick	632
18.2	Das Konzept von Unified Connectivity	634
18.3	UCON einrichten und betreiben	637
18.4	Zusammenspiel von UCON und Berechtigungs- prüfungen auf Funktionsbausteine	641
18.5	Fazit	648

19 Berechtigungen in SAP HANA 649

19.1	Anwendungsszenarien von SAP HANA	650
19.2	Architektur von SAP HANA	651
19.2.1	Sicherheitsarchitektur in SAP HANA	654
19.2.2	Objekte des Berechtigungswesens in SAP HANA	656

19.3	Benutzerverwaltung in SAP HANA	657
19.4	Berechtigungen in SAP HANA	660
19.4.1	Privilegien in SAP HANA	660
19.4.2	Rollen in SAP HANA	664
19.4.3	Beispiel für Berechtigungen in SAP HANA	665
19.5	Fazit	667

20 Berechtigungen in SAP S/4HANA 669

20.1	Überblick	669
20.2	Fiori-Anwendungsrollen anlegen	670
20.3	Kontinuität im Benutzermanagement	677
20.4	Fazit	677

21 SAP Business Suite: Prozesse und Einstellungen ... 679

21.1	Grundlagen	680
21.1.1	Stamm- und Bewegungsdaten	680
21.1.2	Organisationsebenen	681
21.2	Berechtigungen im Finanzwesen	682
21.2.1	Organisatorische Differenzierungs- kriterien	683
21.2.2	Stammdaten	685
21.2.3	Buchungen	697
21.2.4	Zahllauf	702
21.3	Berechtigungen im Controlling	704
21.3.1	Organisatorische Differenzierungs- kriterien	705
21.3.2	Stammdatenpflege	706
21.3.3	Buchungen	715
21.3.4	Altes und neues Berechtigungskonzept im Controlling	718
21.4	Berechtigungen in der Logistik (allgemein)	718
21.4.1	Organisatorische Differenzierungs- kriterien	719
21.4.2	Materialstamm/Materialart	720
21.5	Berechtigungen im Einkauf	724
21.5.1	Stammdatenpflege	724
21.5.2	Beschaffungsabwicklung	724
21.6	Berechtigungen im Vertrieb	731

21.6.1	Stammdatenpflege	731
21.6.2	Verkaufsabwicklung	732
21.7	Berechtigungen in technischen Prozessen	735
21.7.1	Funktionstrennung in der Berechtigungsverwaltung	736
21.7.2	Funktionstrennung im Transportwesen	740
21.7.3	RFC-Berechtigungen	742
21.7.4	Debugging-Berechtigungen	743
21.7.5	Mandantenänderung	744
21.7.6	Änderungsprotokollierung	745
21.7.7	Batchberechtigungen	746
21.8	Vereinfachtes Sperren und Löschen personen- bezogener Daten in der SAP Business Suite	747
21.8.1	Konzept des vereinfachten Sperrens und Löschens personenbezogener Daten	748
21.8.2	Funktion in der SAP Business Suite	751
21.8.3	Berechtigungen für gesperrte Daten verwalten	754
21.9	Fazit	757

22 Konzepte und Vorgehen im Projekt 759

22.1	Berechtigungskonzept im Projekt	760
22.2	Vorgehensmodell	762
22.2.1	Logischer Ansatz	763
22.2.2	Implementierung	765
22.2.3	Redesign	766
22.2.4	Konkretes Vorgehen	767
22.3	SAP-Best-Practices-Template-Rollenkonzept	771
22.3.1	SAP Best Practices	771
22.3.2	SAP-Template-Rollen	772
22.3.3	Methodische Vorgehensweise des SAP- Best-Practices-Rollenkonzepts	774
22.3.4	Einsatz mit SAP Access Control	777
22.3.5	Template-Rollen für SAP HANA	778
22.4	Inhalte eines Berechtigungskonzepts	778
22.4.1	Einleitung und normativer Rahmen des Konzepts	779
22.4.2	Technischer Rahmen	781
22.4.3	Risikobetrachtung	781
22.4.4	Person – Benutzer – Berechtigung	782

22.4.5	Berechtigungsverwaltung	783
22.4.6	Organisatorische Differenzierung	784
22.4.7	Prozessdokumentation	784
22.4.8	Rollendokumentation	785
22.5	Schritte zum Berechtigungskonzept	785
22.5.1	Rahmenkonzept und Projektmitglieder	785
22.5.2	Rollenkonzept	786
22.5.3	Rollenimplementierung	791
22.5.4	Tests und Zuordnung zu Benutzern	791
22.6	Fazit	792
Anhang		793
A	Abkürzungsverzeichnis	795
B	Glossar	799
C	Literaturverzeichnis	815
D	Die Autoren	823
Index		827