

# Inhaltsverzeichnis

<b>Vorwort</b>	<b>9</b>
<b>1 Grundlagen für SAP-Anwender</b>	<b>13</b>
1.1 Überblick für Einsteiger	14
1.1.1 Was bedeutet SAP ERP?	14
1.1.2 Was sind Geschäftsprozesse?	17
1.1.3 Die Module von SAP ERP	21
1.1.4 Wie sieht eine Systemlandschaft aus?	23
1.1.5 Welche Bedeutung hat der Mandant?	27
1.1.6 Programme, Dynpros, Transaktionen und Jobs	29
1.2 Berechtigungsprobleme aus Prozesssicht	33
1.3 Typische Fragen und Lesehinweise	36
<b>2 Authentifizierung und SAP-Benutzerstammsatz</b>	<b>39</b>
2.1 Authentifizierung	39
2.1.1 Was bedeutet Authentifizierung?	39
2.1.2 Welche Authentifizierungsmerkmale gibt es?	41
2.1.3 Welche Authentifizierungstechniken gibt es im SAP-Umfeld?	46
2.1.4 Was kann ein Anwender zur Sicherheit des SAP-Systems beitragen?	49
2.2 Benutzerstammsatz	52
2.3 Rollen und Profile	57
2.3.1 Was ist eine Rolle in SAP?	57
2.3.2 Die verschiedenen Rollentypen in SAP	62
2.3.3 Was ist ein Profil?	64
<b>3 Berechtigungsvergabe in SAP</b>	<b>67</b>
3.1 Grundlegende Begriffe des SAP-Berechtigungswesens	67
3.1.1 Was ist ein Berechtigungsfeld?	68
3.1.2 Was ist ein Berechtigungswert?	76
3.1.3 Was sind Berechtigungsobjekte?	80
3.1.4 Was genau ist eine Berechtigung in SAP?	83

3.2	Berechtigungen in Rollen und Profilen	87
3.2.1	Der Rollen- bzw. Profilgenerator	88
3.2.2	Bedeutung des Rollenmenüs	92
3.2.3	Wie kommen konkrete Berechtigungen in Rollen und Profilen?	96
3.2.4	Was sind Orgebenen in einer Rolle?	103
3.3	Berechtigungen von SAP-Benutzern	105
3.3.1	Was ist der Benutzerpuffer?	105
3.3.2	Auswirkungen von Änderungen an Rollen und Profilen auf Anwender	109
<b>4</b>	<b>Berechtigungsprüfungen im SAP-System</b>	<b>113</b>
4.1	Arten von Berechtigungsprüfungen	113
4.1.1	Was ist eine Transaktionsberechtigung?	114
4.1.2	Alternative Startberechtigungsprüfungen	116
4.1.3	Welche Berechtigungen werden nach dem Start einer Transaktion noch geprüft?	119
4.1.4	Was ist ein AUTHORITY CHECK?	121
4.2	Modulspezifische Berechtigungen	125
4.2.1	Rechnungswesen	126
4.2.2	Personalwesen	137
4.2.3	Logistik	141
4.3	Spezielle Berechtigungsprüfungen	143
4.3.1	Ausführen von ABAP-Programmen	143
4.3.2	Zugriffe auf Dateien, Uploads und Downloads	149
4.3.3	Zugriff auf Tabellen und Views	152
4.3.4	Varianten und Layouts	156
4.3.5	Berechtigungsgruppen	160
4.3.6	LSMW- und Batch-Input-Berechtigungen	163
4.4	Kontrolle fehlgeschlagener Berechtigungsprüfungen	167
4.4.1	Wie sieht eine fehlgeschlagene Berechtigungsprüfung aus?	167
4.4.2	Transaktion SU53	170
4.4.3	Wie setzt man die SU53 sinnvoll ein?	175
4.4.4	Was ist ein Berechtigungstrace?	180
4.4.5	Warum werden Benutzer geklont?	185

4.5	Fehlende Berechtigungsprüfungen	188
4.5.1	Wie erkennt man eine fehlende Berechtigungsprüfung?	188
4.5.2	Wie werden berechtigungsbezogene Programmfehler korrigiert?	190
4.5.3	Welche Alternativen zur Berechtigungsprüfung gibt es?	191
<b>5</b>	<b>Rahmenbedingungen für das SAP-Berechtigungswesen</b>	<b>195</b>
5.1	Akteure im SAP-Umfeld	195
5.1.1	Anwender	196
5.1.2	Key-User	198
5.1.3	Anwendungsbetreuer	199
5.1.4	Benutzerverwalter	200
5.1.5	Systemadministrator	200
5.1.6	Sonstige Akteure	201
5.2	Das Vier-Augen-Prinzip	202
5.3	Sicherheitsanforderungen und Konzepte für die IT-Sicherheit	205
5.3.1	Gesetzliche Rahmenbedingungen für den SAP-Einsatz	206
5.3.2	Betriebskonzept für den SAP-Einsatz	208
5.3.3	Berechtigungskonzept	210
5.3.4	Entwicklungsrichtlinien	211
5.4	Rollen- und Namenskonventionen	213
5.5	Kritische und unkritische Berechtigungen	217
5.5.1	Kritische Transaktionsberechtigungen	217
5.5.2	Kritische Berechtigungsobjekte	221
5.5.3	Auswertung kritischer Berechtigungen	224
5.5.4	Unkritische Berechtigungen	227
<b>6</b>	<b>Fazit</b>	<b>229</b>
<b>7</b>	<b>Weiterführende Informationen</b>	<b>231</b>
7.1	Literatur	231
7.2	SAP Onlinehilfe	233
7.3	SAP Support Portal	235

<b>A Der Autor</b>	<b>240</b>
<b>B Index</b>	<b>241</b>
<b>C Disclaimer</b>	<b>248</b>
<b>Weitere Bücher von Espresso Tutorials</b>	<b>249</b>