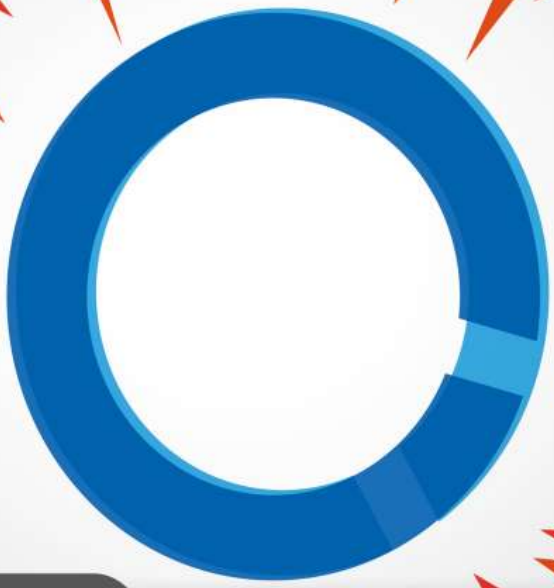
ESPRESSO TUTORIALS



Sebastian Mayer & Martin Metz

Schnelleinstieg in SAP® GRC – Access Control

- Analyse und Simulation von Berechtigungsrisiken
- privilegierte Berechtigungen und Notfallzugriffe
- Herzstück »Access Risk Analysis«: Regelwerke erstellen
- mindernde Kontrollen für unvermeidbare Risiken

Inhaltsverzeichnis

Vorwort **7**

Widmung 8

1 Risiken und rechtliche Grundlagen im Berechtigungsmanagement **11**

1.1 Aktuelle Vorkomnisse und resultierende Risiken 11

1.2 Rechtliche Grundlagen 13

2 Vorstellung der GRC-Suite von SAP **23**

2.1 Kurzvorstellung der SAP-Rollen- und Profilstruktur 23

2.2 Die SAP-GRC-Suite 26

2.3 SAP GRC im Unternehmenskontext des Berechtigungsmanagements 30

2.4 Die Module von SAP Access Control 40

3 ARA – das Herzstück des GRC **47**

3.1 Funktionsweise des Regelwerks 47

3.2 Anlage von Regelwerken 55

3.3 Die umfassenden Berichtsfunktionen in ARA 72

3.4 Anlage und Zuordnung mindernder Kontrollen 84

4 BRM – konfliktfreie Rollen als Voraussetzung für ein funktionierendes Berechtigungsmanagement **93**

4.1 Der Rollenmanagementprozess in BRM 93

4.2 Nützliche Werkzeuge des BRM 134

5 ARM – Benutzermanagementprozesse mit integierter Berechtigungsprüfung **153**

5.1 Die fachlichen Prozesse des Benutzermanagements 153

5.2 Erstellung von Anträgen und Prüfung der Risiken 156

5.3 Genehmigung von Anträgen und Nutzung mindernder Kontrollen 167

5.4 Suche und Analyse von Benutzeranträgen 174

6 EAM – Zugriff auf das System mit speziellen kritischen Rechten 181

6.1 Zugriffsszenarien mit SAP AC EAM 181
6.2 Bestellung und Zuweisung einer Firefighter-ID 188
6.3 Nutzung einer Firefighter-ID 198
6.4 Analyse der Zugriffsprotokolle 201

7 Verantwortlichkeiten im Umfeld von SAP Access Control 209

8 Fazit 214

A Anhang 215

Abkürzungsverzeichnis 215
Glossar 216
Literaturverzeichnis 219

B Die Autoren 222

C Index 225

D Disclaimer 230

2 Vorstellung der GRC-Suite von SAP

Nach einer Kurzvorstellung der SAP-Rollen- und Profilstruktur erhalten Sie in diesem Kapitel einen Einblick in die SAP-Suite Governance, Risikomanagement und Compliance (GRC) mit ihren diversen Modulen, gefolgt von einer Einordnung von SAP GRC im Unternehmenskontext des Berechtigungsmanagements. Abschließend geben wir Ihnen einen Überblick über die einzelnen Module der SAP-GRC-Lösung *Access Control*.

2.1 Kurzvorstellung der SAP-Rollen- und Profilstruktur

Programme, Services, Informationen und Tabellen werden in SAP mittels *Berechtigungen* vor unerlaubtem Zugriff geschützt. Endanwender benötigen daher in SAP für ihre tägliche Arbeit passende Befugnisse in Form von Transaktionen und adäquat ausgeprägten Berechtigungsobjekten. Im SAP-Berechtigungswesen wird zur Verwaltung von Berechtigungen grundsätzlich zwischen den folgenden Objekttypen unterschieden:

- Berechtigungsprofil (kurz: Profil),
- Einzelrolle,
- Sammelrolle,
- abgeleitete Rolle.

Berechtigungen werden in SAP mittels sogenannter *Berechtigungsprofile* gebündelt. Soll ein Endanwender Zugriff auf bestimmte Informationen oder Programme erhalten, ist es erforderlich, seinem *Benutzer(konto)* Berechtigungsprofile mit den notwendigen Berechtigungen zuzuweisen.

Unterscheidung zwischen Anwender und Benutzer

Ein (End-)Anwender ist eine Person bzw. ein Mitarbeiter Ihres Unternehmens, der ein IT-System nutzt. Ein Benutzer(konto) hingegen ist ein technischer Account auf dem IT-System, der es Mitarbeitern ermöglicht, auf ein gewünschtes IT-System zuzugreifen.

Zur einfachen Verwaltung von Berechtigungsprofilen wurde seitens der SAP der *Profilgenerator* eingeführt, den Sie mittels der Transaktion **PFCG** aufrufen können. Im Profilgenerator legen Sie sog. *Rollen* an, verwalten diese, definieren deren Attribute und ordnen ihnen Berechtigungen zu. Rollen ermöglichen die automatische Generierung eines Profils. Auch diese können Sie einem Benutzerkonto in SAP unmittelbar zuweisen. Damit einhergehend wird ihm jedoch immer automatisch auch das entsprechende, einer Rolle zugehörige Berechtigungsprofil zugeordnet.

Wie zuvor aufgelistet, gibt es drei unterschiedliche Arten von Rollen. In einer *Einzelrolle* sind, vereinfacht dargestellt, verschiedene Transaktionen und Berechtigungsobjekte enthalten, die Anwender für den Zugriff auf bspw. Programme oder Informationen benötigen. *Sammelrollen* wiederum ermöglichen Ihnen die Bündelung von Einzelrollen. Dies geschieht bspw. zur Verringerung des Pflegeaufwands bei der Benutzerverwaltung. Hätten Sie ausschließlich Einzelrollen im Einsatz, müssten Sie in SAP stets alle von einem Anwender benötigten Einzelrollen manuell zuordnen. In Sammelrollen fassen Sie fachlich verbundene Einzelrollen zusammen und ordnen dem Benutzer lediglich die übergeordnete Sammelrolle zu. *Abgeleitete Rollen* entstehen, indem Sie bestimmte, in einer Einzelrolle nicht näher definierte Organisationswerte wie bspw. Buchungskreise (in der SAP-Terminologie BUKRS) im Rahmen der Rollenableitung ausprägen. Einzelrollen, die in diesem Rahmen als Vorlage dienen, werden häufig auch als *Masterrollen* oder *Stammrollen* bezeichnet. Abgeleitete Rollen werden automatisch vom System inkl. der jeweiligen Organisationswerte erzeugt und gehören technisch gesehen ebenfalls zu den Einzelrollen. In Abbildung 2.1 veranschaulichen wir Ihnen nochmals die Funktionsweise der Rollenableitung.

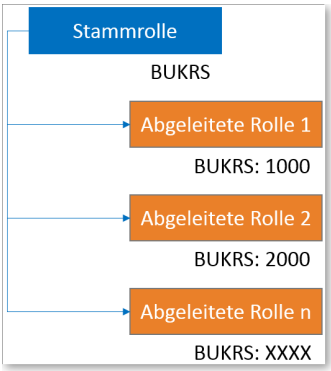


Abbildung 2.1: Rollenableitung in SAP

Neben der Nutzung der über die PFCG automatisch aus Rollen generierten Profile können Sie nach wie vor manuelle Profile mittels der Transaktion **SU02** anlegen und verwalten sowie diese Benutzerkonten zuordnen. Manuelle Profile werden mittlerweile jedoch nur noch selten eingesetzt, sodass wir diesen keine weitere Aufmerksamkeit schenken.

In Abbildung 2.2 stellen wir das Zusammenwirken von Rollen, Profilen und Berechtigungen zur Verdeutlichung grafisch dar.

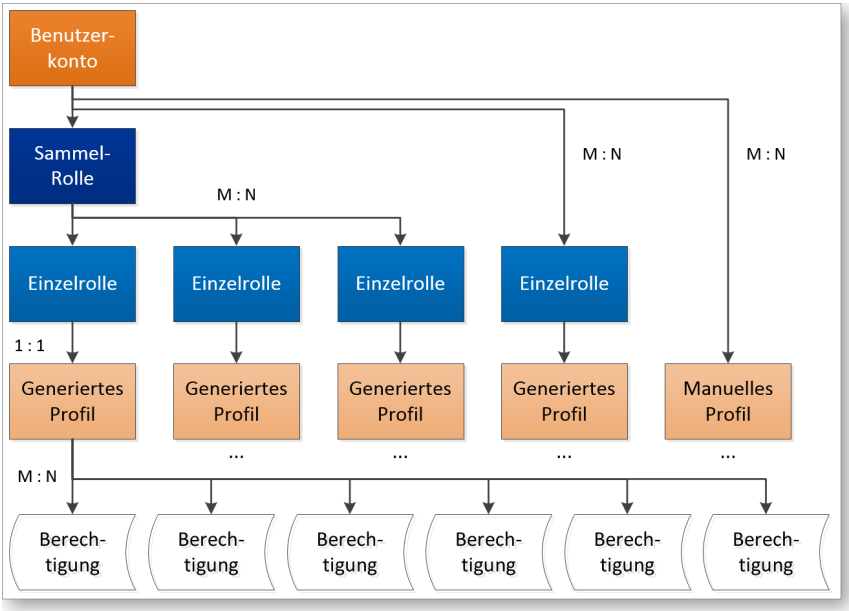


Abbildung 2.2: Zusammenwirken von Rollen, Profilen und Berechtigungen

2.2 Die SAP-GRC-Suite

SAP-Lösungen für Governance, Risikomanagement und Compliance (GRC) stellen eine eigenständige Produktpalette innerhalb des SAP-Portfolios dar. Zusammenfassend dient die GRC-Suite dazu, Unternehmen bei der Steuerung ihrer SAP-Landschaft zu unterstützen und die Wahrung gesetzlicher und regulatorischer Anforderungen sicherzustellen. Um dieses weitreichende Ziel zu erreichen, umfasst sie, wie Abbildung 2.3 darstellt, die Produkte Access Control, Process Control, Risk Management, Fraud Management und Audit Management.

Abbildung 2.3: Überblick über die SAP-GRC-Suite

Nachfolgend möchten wir Ihnen einen kurzen Überblick über die einzelnen Produkte der SAP-GRC-Suite geben.

Access Control

SAP Access Control unterstützt Unternehmen dahingehend, Kontrollen im Berechtigungswesen durchzuführen, diese zu überwachen und in bestimmten Prozessen sogar zu erzwingen. Access Control ist darüber hinaus die SAP-GRC-Lösung zur ganzheitlichen Unterstützung des Berechtigungswesens in SAP-Systemen. Hierfür beinhaltet es Werkzeuge zur Analyse von Benutzern, Rollen und Profilen hinsichtlich vorhandener Berechtigungsrisiken, zur Erstellung und Genehmigung von Rollen und Benutzern wie auch eine Lösung zur Unterstützung von Notfallbenutzern bzw. Notfallsystemzugriffen. Darüber hinaus können in Access Control *mindernde Kontrollen* dokumentiert und Risiken zugeordnet werden, für den Fall, dass diese nicht vermieden werden können. Unter mindernden Kontrollen sind manuelle, halb automatische oder automatische Prüfschritte zu verstehen, die detektiv, d. h. nachgelagert, durchgeführt werden, um dolose Handlungen in einem SAP-System zumindest zu einem späteren Zeitpunkt aufzudecken.

Process Control

SAP Process Control ist eine Lösung, die Unternehmen bzw. deren Management bei der Implementierung eines internen Kontrollsystems und einer diesbezüglichen Berichterstattung sowie der Durchführung und Dokumentation von Kontrollen unterstützt. SAP Prozess Control bietet darüber hinaus die Möglichkeit, Kontrollen in Bezug auf SAP-Systeme zu automatisieren.

Process Control kann zudem mit Access Control integriert betrieben werden, sodass beide Produkte auf derselben Plattform laufen und teilweise gleiche Stammdaten (wie bspw. Geschäftsprozesse) nutzen. Darüber hinaus können mindernde Kontrollen, die in Access Control Berechtigungsrisiken zugeordnet wurden, in Process Control aufgenommen werden. Dies erleichtert bspw. die Kontrolldurchführung sowie -dokumentation in Process Control.

C Index

A

Access Request Management (ARM) 41, 44, 153
Access Risk Analysis (ARA) 40, 41, 47
Access-Control-
  Verantwortliche 104, 177
  Rollenverantwortliche 104
  Workflow-Administrator 177
Anforderungsart 156
Anwendungsart 99
ARA-Regelwerk 41, 43, 44, 47, 48, 55, 56, 71
Ausführungsanalyse siehe *Ausführungsreport*
Ausführungsreport 72, 82
Authentifizierung 33
automatische Benutzerzuordnung 108
Autorisierung 35

B

BDSG siehe *Bundesdatenschutzgesetz*
benutzerdefinierte Daten 167
benutzerdefiniertes Feld 104
Benutzerdetails 163
Benutzergruppe 166
Benutzermanagement 36, 153
Benutzersperre 155
  automatische 155
  manuelle 155
Benutzersystemdetails 167
Benutzerzugriff 156
Berechtigung 23
Berechtigungsgruppe 51
Berechtigungskonflikt Siehe Zugriffsrisiko
Berechtigungskonzept 35
  funktionales 35
  organisatorisches 35
Berechtigungsmanagement 12, 23, 30
Berechtigungsprofil 23, 95
Berechtigungsrisiko
  Analyse 72, 73
  Simulation 72
Berechtigungswert 49
Berechtigungswesen siehe *Berechtigungsmanagement*
Bilanzrechtsmodernisierungsgesetz 15
BilMoG siehe *Bilanzrechtsmodernisierungsgesetz*
Bundesdatenschutzgesetz 16
Business Role Management (BRM) 40, 42, 93

C

Cross-System-Berechtigung 57
Cybersicherheitsgesetz 16

D

Dashboard 72, 80
DCGK siehe *Deutscher Corporate Governance Kodex*
Detailbeschreibung 106
Deutscher Corporate Governance Kodex 15
Drilldown 72, 80

E

Edward Snowden 11
Emergency Access Management (EAM) 41, 45, 181
  dezentral 45, 188
  zentral 45, 187
Empfindlichkeit 102
extended EAM 183, 184

F

Firefighter-ID 45, 186, 188, 198
Firefighter-Rolle 45
focussed EAM 183, 184
Funktion 49, 57
Funktionsbereich 103
Funktionstrennungskonflikt 35, 41, 47, 48, 49, 53, 63, 95
Funktionstrennungsrisiko siehe Funktionstrennungskonflikt

G

Geschäftsprozess 99
Gesetz zur Kontrolle und Transparenz im Unternehmensbereich 15
Grundsätze ordnungsgemäßer datenverarbeitungsgestützter Buchführungssysteme (GoBS) 18

H

Handelsgesetzbuch 15
HERAS-Modell 184, 188
HGB siehe *Handelsgesetzbuch*

I

ID-basiertes Firefighting 186
Identitätsmanagement 32, 38, 39
IDW-Stellungnahme zur Rechnungslegung
  Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1) 17
Information Security Management Systems 16, 19
Instanzstatus 175, 179

Internet Security Threat Report 2016 12
ISMS siehe *Information Security Management Systems*
ISO 27001 19
IT-Architektur 37
IT-Grundschutz-Kataloge 19
IT-Sicherheitsgesetz 16
IT-Sicherheitskonzept 12

J

Joiner-Prozess 154

K

Konnektorgruppe 99
KonTraG siehe *Gesetz zur Kontrolle und Transparenz im Unternehmensbereich*
Kritikalität 102
kritische Aktion siehe *kritische Transaktion*
kritische Berechtigung siehe *kritisches Berechtigungsobjekt*
kritische Transaktion 41, 47, 48, 52, 63, 95
kritisches Berechtigungsobjekt 41, 47, 48, 51, 63, 95

L

Landschaft 99
Leaver-Prozess 155

M

MaRisk siehe *Mindestanforderungen für Risikomanagement*
Mehrfaktoren-Authentifizierung 34
mindernde Kontrolle 42, 44, 84, 171
Mindestanforderungen für Risikomanagement 16
Mover-Prozess 154

N

Namenskonvention 61
Need-to-do 154
Need-to-know 154
Notfallzugriff 181
NSA-Affäre 11

O

Org. Value Map siehe *Organisationswertzuordnung*
Organisationswertzuordnung 125

P

Parameter 165
Privileged Account Management 182
privilegierte Berechtigung 181
Profil siehe *Berechtigungsprofil*
Profilgenerator 24, 71, 93, 113
Projektfreigabe 99

Prüfregel siehe *Zugriffsregel*
Prüfungsstandard (PS) 330
18

R

Regel siehe *Zugriffsregel*
Regelübersicht 51
Regelwerk siehe *ARA-Regelwerk*
Revisionsprotokoll 179
Rezertifizierung 38, 100, 155
Risiko 49, 50, 52, 61
Risikoanalyse 115, 160
Risikobeschreibung 62
Risikoüberschreitung 160
Rolle 24
abgeleitete Rolle 24, 42, 114, 120
Business-Rolle 43
Einzelrolle 24, 42
Masterrolle 24
Sammelrolle 24, 42
Stammrolle 24
Unternehmen zuordnen 103
Rollenaktualisierung 141
rollenbasiertes Firefighting 186
Rollenbestätigung 102
Rollengenerierung 128
Rollenimport 134
Rollenkonzept 35
Rollenmethodologie 43, 95
Rollenstatus 107
Rollensuche 150
Rollenvergleich 145
Rollenvoraussetzung 105
Rollenzuordnung 106
RSUSR_008_009_NEW 71

S

SAP Access Control 27, 30, 39, 40
SAP Access Control Plugin 39
SAP Audit Management 29
SAP Fraud Management 28
SAP NetWeaver Business Client 46
SAP Process Control 27
SAP Risk Management 28
Sarbanes-Oxley Act 17
Schadensanalyse 115, 160
Self-Services 36
Single Sign-on 34
SOX siehe *Sarbanes-Oxley Act*

T

Teilprozess 99
Token 34
Transportwesen 95

U

Ursachencode 199

V

Verwendungsrolle 110
Vodafone 11

W

Whitelist 91

Z

Zertifizierung siehe *Rezertifizierung*
Zugriffsmanagement 33
Zugriffsprotokoll 201
Zugriffsregel 50, 51, 52, 53, 65
Zugriffsregelübersicht 55
Zugriffsrisiko 39
  Simulation 76
Zusatzdetail 106