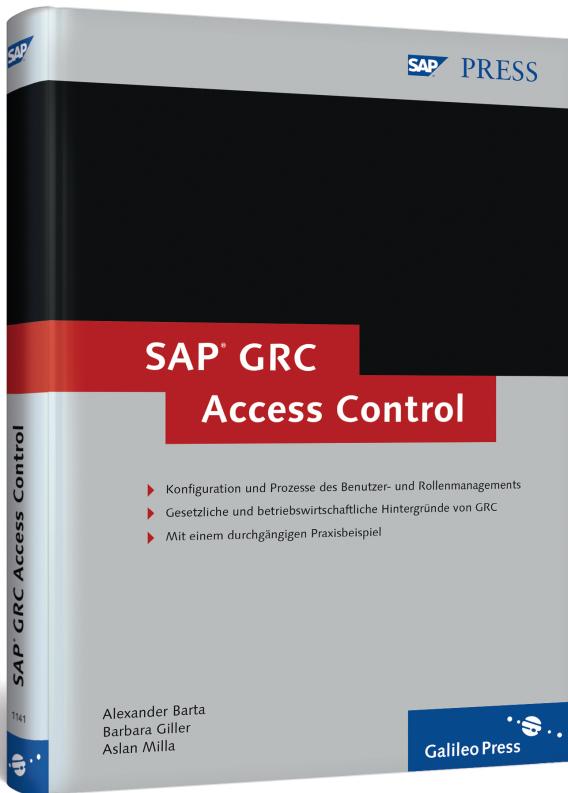


Alexander Barta, Barbara Giller, Aslan Milla

## SAP® GRC Access Control



- ▶ Konfiguration und Prozesse des Benutzer- und Rollenmanagements
- ▶ Gesetzliche und betriebswirtschaftliche Hintergründe von GRC
- ▶ Mit einem durchgängigen Praxisbeispiel

Galileo Press

Bonn • Boston

# Auf einen Blick

<b>1</b>	<b>Einleitung .....</b>	<b>17</b>
<b>2</b>	<b>Marktentwicklungen und gesetzliche Rahmenbedingungen .....</b>	<b>23</b>
<b>3</b>	<b>Einführung in Governance, Risikomanagement und Compliance .....</b>	<b>69</b>
<b>4</b>	<b>Integration von GRC-Initiativen durch SAP-Lösungen für GRC .....</b>	<b>125</b>
<b>5</b>	<b>SAP-Berechtigungskonzept und Funktionstrennung .....</b>	<b>143</b>
<b>6</b>	<b>Risikoanalyse und Re-Design mit SAP GRC Access Control .....</b>	<b>211</b>
<b>7</b>	<b>Benutzer- und Rollenmanagement mit SAP GRC Access Control .....</b>	<b>303</b>
<b>8</b>	<b>Abschluss der Fallstudie .....</b>	<b>383</b>
<b>9</b>	<b>Ausblick .....</b>	<b>387</b>
<b>A</b>	<b>Periodische Hintergrundjobs .....</b>	<b>391</b>
<b>B</b>	<b>Übersicht über deutsch-englische Begriffe .....</b>	<b>395</b>
<b>C</b>	<b>Literaturverzeichnis .....</b>	<b>399</b>
<b>D</b>	<b>Die Autoren .....</b>	<b>403</b>

# Inhalt

Vorwort .....	13
<b>1 Einleitung .....</b>	<b>17</b>
1.1 Inhaltliche Abgrenzung .....	17
1.2 Zielgruppen .....	19
1.3 Arbeiten mit diesem Buch .....	20
1.4 Danksagung .....	22
<b>2 Marktentwicklungen und gesetzliche Rahmenbedingungen .....</b>	<b>23</b>
2.1 Begriffsdefinition und -abgrenzung .....	24
2.1.1 Corporate Governance, Risikomanagement und Compliance (GRC) .....	24
2.1.2 Isolierte vs. integrierte Betrachtung von GRC .....	28
2.2 Steigender Handlungsbedarf für Unternehmen .....	33
2.2.1 Bilanz- und Wirtschaftsskandale in den USA und Europa .....	33
2.2.2 Wirtschaftskriminalitätsstudie von PwC – verdrängen Firmen das Risiko? .....	38
2.3 Die Fallstudie .....	46
2.4 Compliance-Vorschriften und ihre Auswirkungen .....	50
2.4.1 Der angloamerikanische Zugang – Sarbanes-Oxley 2002 .....	50
2.4.2 Entwicklungen in Europa: Die 8. EU-Richtlinie .....	55
2.4.3 Weitere gesetzliche Vorschriften in Deutschland, Österreich und der Schweiz .....	58
2.4.4 Implementierungsaufwand und laufende Kosten .....	63
2.4.5 Resultierende Konsequenzen für Unternehmen – Fallbeispiel .....	65
2.5 Nutzen und Nachhaltigkeit eines ganzheitlichen GRC-Managements .....	66

<b>3 Einführung in Governance, Risikomanagement und Compliance .....</b>	<b>69</b>
3.1 Governance als Basis .....	69
3.1.1 Was man über Corporate Governance wissen muss .....	70
3.1.2 Europäische Corporate-Governance-Kodizes .....	76
3.1.3 IT Governance .....	81
3.1.4 COSO I als Rahmenwerk für Governance .....	88
3.1.5 Fortführung der Fallstudie .....	91
3.2 Risikomanagement für das Erreichen der Ziele .....	93
3.2.1 Ein praxisorientierter Zugang zum Risikomanagement .....	94
3.2.2 COSO II – das Enterprise-Risk-Management-Modell (ERM) .....	97
3.2.3 Darstellung des Risikomanagementprozesses in der Fallstudie .....	100
3.2.4 Beispiele für Risiken und Kontrollen beim Berechtigungskonzept .....	106
3.3 Compliance – Umgang mit Regeln und Standards .....	109
3.3.1 Compliance – mehr als nur Regeleinhaltung! .....	109
3.3.2 Governance und Risikomanagement als Basis für Compliance-Ziele .....	111
3.3.3 Fortführung der Fallstudie .....	113
3.4 Vorstellung und Anwendung des Self-Assessment-Fragebogens .....	114
3.5 Integration von GRC .....	117
3.5.1 Arten der Integration .....	118
3.5.2 Beschreibung des integrierten GRC in der Fallstudie .....	119
<b>4 Integration von GRC-Initiativen durch SAP-Lösungen für GRC .....</b>	<b>125</b>
4.1 Übersicht über die SAP-Lösungen für GRC .....	125
4.1.1 GRC Foundation .....	128
4.1.2 SAP GRC Risk Management .....	128
4.1.3 SAP GRC Process Control .....	129
4.1.4 SAP GRC Global Trade Services (GTS) .....	130

4.1.5	SAP Environment, Health & Safety .....	131
4.1.6	Fallstudie zu den SAP-Lösungen für GRC .....	131
4.2	Übersicht über SAP GRC Access Control .....	132
4.3	Das SAP GRC Access Control-Implementierungs- projekt .....	137
4.4	Technische Installation von SAP GRC Access Control .....	141

## 5 SAP-Berechtigungskonzept und Funktions- trennung ..... 143

5.1	Berechtigungen und ihre Bedeutung für das Interne Kontrollsysteem .....	143
5.1.1	Relevanz und Auswirkungen eines funktionierenden Berechtigungskonzepts .....	144
5.1.2	Analyse von Ist-Status und Information Processing Objectives .....	147
5.1.3	Best-Practice-Prozess der Berechtigungs- pflege .....	150
5.2	Aufbau und Funktionsweise des SAP-Berechtigungskonzepts .....	157
5.2.1	Aufbau von Userprofilen und Rollen .....	157
5.2.2	Rollen, Benutzerstamm und Profilgenerator ...	171
5.2.3	Superuser und andere kritische Profile .....	175
5.2.4	Relevante SAP Reports und Tabellen, Prüfungsmethoden und Prüftools .....	180
5.3	Die Funktionstrennung aus Prüfersicht .....	189
5.3.1	Warum benötigt ein Unternehmen effektive Funktionstrennung? .....	190
5.3.2	SoD-Regeln aus IT-Sicht .....	191
5.3.3	SoD-Regeln aus Geschäftsbereichssicht .....	198
5.3.4	Praxisbeispiele .....	207

## 6 Risikoanalyse und Re-Design mit SAP GRC Access Control ..... 211

6.1	Anforderungen an SAP GRC Access Control .....	211
6.2	Risk Analysis and Remediation .....	213
6.2.1	Initiale Konfiguration von Risk Analysis and Remediation .....	215
6.2.2	Funktionsumfang von Risk Analysis and Remediation .....	218

6.2.3	Aufbau der Prüfregeln in Risk Analysis and Remediation .....	222
6.2.4	Anpassen und Erweitern der Abfragen .....	229
6.2.5	Durchführung und Beurteilung der Risikoanalysen .....	265
6.2.6	Kompensierende Kontrollen und automatische Alarmmeldungen .....	278
6.2.7	Risk Terminator .....	289
6.3	Superuser Privilege Management .....	290
6.3.1	Funktionsweise und Setup von Superuser Privilege Management .....	291
6.3.2	Fortführung der Fallstudie .....	297

## **7 Benutzer- und Rollenmanagement mit SAP GRC Access Control ..... 303**

7.1	Häufige Schwächen im Benutzer- und Rollen- management .....	304
7.2	Unterstützung durch SAP GRC Access Control .....	306
7.3	Compliant User Provisioning .....	307
7.3.1	Post-Installationsmaßnahmen für CUP .....	309
7.3.2	Funktionsumfang von Compliant User Provisioning .....	312
7.3.3	Konfigurationsschritte von CUP .....	338
7.4	Enterprise Role Management .....	350
7.4.1	Post-Installationsmaßnahmen für ERM .....	352
7.4.2	Funktionsumfang von Enterprise Role Management .....	352
7.4.3	Konfiguration des Rollenerstellungsprozesses in ERM .....	367

## **8 Abschluss der Fallstudie ..... 383**

8.1	Was der Crashkurs-Konzern gelernt hat .....	383
8.2	Wie es jetzt weitergeht .....	386

## **9 Ausblick ..... 387**

9.1	Rechtliche Entwicklungen .....	387
9.2	Entwicklung der SAP GRC-Lösungen .....	388
9.2.1	Ausblick für SAP GRC Access Control .....	389
9.2.2	Ausblick für das GRC-Produktportfolio .....	389

**Anhang**

A Periodische Hintergrundjobs .....	391
B Übersicht über deutsch-englische Begriffe .....	395
C Literaturverzeichnis .....	399
D Die Autoren .....	403
Index .....	405

# Vorwort

Nach der boomenden Wirtschaft in den 90ern kam mit den Bilanzskandalen um die Jahrtausendwende das große Erwachen. Auf einmal entstanden zahlreiche neue Gesetze und Vorschriften zur Vermeidung von Bilanzfälschung und zum Schutz der Investoren. Einige dieser Anforderungen führten vor allem am amerikanischen Markt zu einem kaum abschätzbaren Kostenvolumen und formalistischen Prüfmethoden für die Unternehmen.

In Europa wurde ein nachhaltigerer Ansatz als Reaktion auf die internationalen und europäischen Bilanzskandale angestrebt: So wurden 2006 zwei bedeutende Richtlinien – die Änderungsrichtlinie und die Abschlussprüferrichtlinie – in Kraft gesetzt. Die EU-Mitgliedsländer müssen diese Bestimmungen bereits Mitte 2008 in nationales Recht umgesetzt haben. In Österreich wurden diese Anforderungen mit dem Unternehmensrechts-Änderungsgesetz *URÄG 2008* eingeführt, in Deutschland soll das Bilanzrechtsmodernisierungsgesetz *BilMoG* die EU-Vorgaben in deutsches Recht transferieren.

Die zwei EU-Richtlinien fokussieren unter anderem auf Themen wie Corporate Governance, Risikomanagement, Internes Kontrollsyste und Compliance. Ziele sind eine verbesserte Unternehmensberichterstattung und eine konsequente Überwachung der Organisationsabläufe.

Einen wesentlichen Aspekt wird dabei ein funktionierendes Berechtigungskonzept in Ihrem ERP-System einnehmen. Denn ohne entsprechend eingerichtete und verwaltete Zugriffsrechte auf Unternehmensdaten bzw. die Einhaltung von Funktionstrennung können die Zuverlässigkeit der betrieblichen Abläufe und die Richtigkeit und Vollständigkeit der internen und externen Berichterstattung nicht sichergestellt werden.

Diese Richtlinien werden folglich nicht nur Vorstandsmitglieder, Geschäftsführer, Aufsichtsräte und Wirtschaftsprüfer wesentlich beeinflussen, sondern auch interne Revisoren und IT-Mitarbeiter beschäftigen.

Im Unterschied zu US-amerikanischen Gesetzesvorschriften versucht der europäische Ansatz, weniger sanktionsorientiert die Unternehmen und ihre Führungs- und Aufsichtsorgane zunächst zu überzeugen, vor allem ihren Rechnungslegungsprozess und andere interne Abläufe transparent zu machen. Das Umdenken muss unternehmensintern erfolgen – der Nutzen eines intakten Risikomanagements oder einer funktionsfähigen Corporate Governance kann nicht durch externe Prüfer oder Berater allein vermittelt werden.

Der Umgang mit diesen Anforderungen seitens der Unternehmen ist sehr unterschiedlich: Denken Sie an einen Vorstand, der sich halbherzig diesen Vorgaben widmet – wieder einmal ein Gesetz oder eine Richtlinie, die es einzuhalten gilt. Die unternehmensinterne Umsetzung der Anforderungen wird erst einmal eine Hierarchiestufe hinunterdelegiert. Meist wird versucht, im Rahmen eines befristeten Projekts die Vorgaben zu erfüllen – ein Jahr später ist der tiefere Blick für Corporate Governance und Co. auch schon wieder verschwunden.

In einem anderen Unternehmen hingegen entschließt sich die Geschäftsleitung, die Vorgaben an ein funktionierendes Risikomanagement und Internes Kontrollsysteem als potenziellen Nutzen für die Organisation zu sehen. Sie lässt wesentliche Geschäftsabläufe, z. B. im IT-Bereich, erheben und die Mitarbeiter kritische Prozessaktivitäten und Kontrollhandlungen optimieren. Auf diese Weise werden viele Redundanzen, ineffiziente Strukturen und Abläufe im Unternehmen offengelegt und können anschließend verbessert werden.

Hier geht es um nachhaltige Optimierung – denn auch wenn Vorschriften im Bereich Governance, Risikomanagement und Compliance selten ohne umfangreichen Arbeitsaufwand auskommen, ist es wichtig, diese Vorgaben als Chance für das eigene Unternehmen zu erkennen.

Das Berechtigungskonzept eines Unternehmens nimmt auch hier eine ganz besondere Rolle ein: Geschickt eingeführt und auf die wichtigsten Aspekte fokussiert, liefert ein solches Konzept seinen Beitrag zu einer nachhaltigen Verbesserung der Abläufe und Prozesse.

Es liegt an Ihnen, diese neuen Vorschriften als Chance und nicht als notwendiges Übel zu sehen. Es liegt an Ihnen, Ihr firmeneigenes Be-

rechigungskonzept selbstkritisch zu hinterfragen und auf die neuen Anforderungen auszurichten. Und es liegt an Ihnen, diese Aufgabe jetzt anzugehen!

Wir hoffen, dass dieses Buch Sie bei Ihrem ehrgeizigen Vorhaben unterstützen wird und Ihnen einen tieferen Einblick in aktuelle Herausforderungen, Best-Practice-Methoden und SAP GRC Access Control liefert.

**Dr. Aslan Milla**

PricewaterhouseCoopers Österreich  
Präsident des Instituts Österreichischer Wirtschaftsprüfer

*Welche Bedeutung haben Governance, Risk und Compliance heutzutage für Unternehmen und insbesondere ihre IT-Systeme? Welche Anforderungen werden in diesem Zusammenhang an ein Berechtigungskonzept gestellt, und wie lässt sich dies mithilfe von SAP GRC Access Control umsetzen? Dies sind die Fragen, die in diesem Buch beantwortet werden. In der Einleitung lesen Sie, an wen sich dieses Buch richtet und wie es strukturiert ist.*

# 1 Einleitung

Wir haben uns in der Vorbereitungsphase zu diesem Buch lange überlegt, wie wir das Thema *Access Control mit SAP* möglichst übersichtlich darstellen, aber dennoch die technischen Grundlagen und das rechtliche Hintergrundwissen dazu einbinden können. Das war schwieriger, als zuerst gedacht, und wir haben lange über die inhaltliche Abgrenzung und die Gewichtung der verschiedenen Themen diskutiert. Schließlich werden hier viele verschiedene und komplexe Themen angesprochen. Warum dieses Buch letztlich genau so zustande gekommen ist, wie es Ihnen nun vorliegt, und wie Sie damit arbeiten können, möchten wir in diesem Kapitel erläutern.

## 1.1 Inhaltliche Abgrenzung

Der Themenkomplex *Governance, Risk und Compliance* (GRC) ist äußerst kompliziert und vielschichtig. Er setzt sich aus einem Wirrwarr von Richtlinien, Gesetzen, Gesetzesinterpretationen und Prüfungsstandards zusammen, die in verschiedenen Ländern und von diversen Organisationen erstellt und weiterentwickelt wurden. Diese Regelungen sind oftmals in einer selbst für Eingeweihte schwer verständlichen Sprache verfasst. Letztlich stellt sich auch die Frage, welche Regelungen für welche Zielgruppen gültig und verpflichtend sind. Wir haben versucht, dieses Begriffsknäuel zu entwirren und die wichtigsten Grundprinzipien des Themenkreises GRC möglichst ver-

Was ist GRC?

ständlich und mit Beispielen unterlegt aufzuzeigen. Ziel dieses Buches ist es jedoch nicht, einen vollständigen Überblick dazu zu geben. Damit hätten wir die geplante Seitenzahl des Buches gesprengt. Im Literaturverzeichnis finden Sie jedoch weiterführende Literatur zu diesem Thema.

**SAP-Berechtigungskonzept** Ein aus den GRC-Initiativen abgeleitetes Thema ist die Prüfung und Optimierung von SAP-Berechtigungskonzepten. Auch dieses Thema wäre für sich bereits buchfüllend. Da ein gutes Verständnis eine wesentliche Voraussetzung für die erfolgreiche Nutzung von SAP Access Control ist, haben wir auch hier eine Übersicht über die wesentlichen Prinzipien in das Buch aufgenommen. Da ein Buch auch ein Ende haben sollte, mussten wir uns auch hier auf wesentliche Punkte beschränken.

**SAP GRC Access Control** Wie sich GRC-Initiativen in das SAP-Berechtigungskonzept überleiten und wie mit *SAP GRC Access Control* die daraus resultierenden Anforderungen und Best-Practice-Prozesse an das Rollen- und Benutzermanagement erfüllt werden können, ist der dritte Schwerpunkt unseres Buches. Hier haben wir versucht, den verbleibenden Platz für eine fundierte Beschreibung der wesentlichen Zusammenhänge und Wirkungsweisen der Access-Control-Anwendungen zu verwenden. Wir haben die wichtigsten Aspekte und Schritte für die Implementierung der Anwendungen vorgestellt und auch häufige Stolpersteine aufgezeigt.

Wir haben unsere Ausführungen mit der Darstellung von Zusammenhängen, wichtigen Konzepten sowie Prozessen und Abläufen unterlegt. Darüber hinaus haben wir Abbildungen aus SAP ERP-Systemen und den Access-Control-Anwendungen verwendet, um das »Look and Feel« und die wesentlichen Customizing-Einstellungen zu zeigen.

Dieses Buch basiert auf dem aktuellen Releasestand SAP GRC Access Control 5.3, der sich zurzeit im Ramp-Up befindet. Deshalb sind kleinere Änderungen an der Programmoberfläche möglich.

**Die Fallstudie** Um die vorgestellten Konzepte zu verdeutlichen, haben wir diese mit Beispielen untermauert, die sich in der Summe zu einer umfassenden Fallstudie ergänzen, die die dargestellten Inhalte illustrieren soll. Das Beispielunternehmen – der Crashkurs-Konzern – begleitet uns im Verlauf des gesamten Buches.

Wir haben versucht, unsere Ausführungen branchen- und länderneutral zu halten, um sie für einen möglichst großen Kreis von Interessenten anwendbar zu machen.

## 1.2 Zielgruppen

Folgende Zielgruppen sollten mit diesem Buch wertvolle Hinweise zum Thema Access Control mit SAP GRC erhalten:

An wen richtet sich dieses Buch?

Leiter und Mitarbeiter von *Compliance-Abteilungen*, *IT-Governance-Abteilungen* und *internen Revisionen* erhalten einen fundierten Überblick über den Aufbau der SAP-Berechtigungsstrukturen. Darüber hinaus wird dargestellt, wie die Funktionsweise der Access-Control-Anwendungen geplante GRC-Initiativen unterstützen kann.

SAP-Manager und Mitarbeiter aus *SAP-Abteilungen* bekommen eine umfassende Übersicht über die wesentlichen rechtlichen GRC-Grundsätze, darüber, wie sich diese im Prüfungsansatz bei Berechtigungsprüfungen niederschlagen, sowie über daraus abgeleitete Best-Practice-Prozesse. Weiterhin werden die Funktionalitäten der Access-Control-Anwendungen dargestellt und die mögliche Unterstützungsleistung, die Access Control für den Rollen- und Benutzer-administrationsprozess liefern kann.

Projektleiter, Teammitglieder und Berater von *GRC-Implementierungsprojekten* erhalten hilfreiche Hinweise zur Projektplanung sowie zu wesentlichen Customizing-Schritten von Access Control.

*IT-Prüfer* bekommen wertvolle Hinweise über die Funktionalität von Access Control und können daraus wiederum Rückschlüsse für ihre Prüfungshandlungen ziehen.

*Studenten und andere Interessierte* bekommen einen fundierten Überblick über den Zusammenhang zwischen GRC-Initiativen und SAP-Berechtigungskonzepten sowie über wesentliche Aspekte, Zusammenhänge und die Wirkungsweise von SAP GRC Access Control.

## 1.3 Arbeiten mit diesem Buch

Wir haben das Buch so aufgebaut, dass kein Vorwissen im Bereich GRC, SAP-Berechtigungen oder Access Control notwendig ist. Wir führen Sie Stück für Stück in diese Bereiche ein.

Sie können die einzelnen Kapitel des Buches in beliebiger Reihenfolge durcharbeiten. Da sich jedoch insbesondere unsere Fallstudie von Kapitel zu Kapitel fortsetzt und dadurch das Verständnis verbessert werden soll, würden wir empfehlen, das Buch in der Reihenfolge der Kapitelanordnung zu lesen.

### Struktur des Buches

Wir haben die Kapitel und unsere Ausführungen so angeordnet, wie wir grundsätzlich bei Implementierungen von SAP GRC Access Control vorgehen. Die Vertiefungen in die GRC-Grundlagen und SAP-Berechtigungsprinzipien werden im Rahmen des Projekts oftmals in Form von Grundlagentrainings und Coaching-Unterstützungen weitergeben. Dadurch hoffen wir, dass Sie auch einen guten Überblick über die Struktur, Ausmaße und Dauer entsprechender Implementierungen und Spin-Off-Projekte erhalten.

### Gesetzliche Rahmenbedingungen

In Kapitel 2, »Marktentwicklungen und gesetzliche Rahmenbedingungen«, erläutern wir die wesentlichen Marktentwicklungen, gesetzlichen Rahmenbedingungen sowie Bedeutung und Grundlagen von GRC. Dabei diskutieren wir einige der wichtigsten Bilanzskandale der letzten Jahre und deren Auswirkungen, stellen aktuelle Ergebnisse von Studien vor und versuchen, Begriffe wie *Corporate Governance*, *Internes Kontrollsystem*, *Sarbanes-Oxley Act* und die *8. EU-Richtlinie* näher zu erläutern.

### Grundlagen von GRC

In Kapitel 3, »Einführung in Governance, Risikomanagement und Compliance«, werden wir Ihnen Rahmenwerke und Konzepte vorstellen, die die Durchführung von GRC-Projekten unterstützen. Dabei erklären wir allgemeine Abläufe Schritt für Schritt und geben Ihnen auch die Möglichkeit, den Status Ihres eigenen Unternehmens selbst zu analysieren. Wir zeigen Ihnen die grundlegenden Strukturen einer effektiven Governance auf, stellen die Corporate-Governance-Kodizes für Österreich, Deutschland und die Schweiz vor, zeigen die wesentlichen Aspekte von IT-Best-Practice-Rahmenwerken wie *CobiT* und *ITIL* und ebenso Rahmenwerke für Interne Kontrollsysteme und Risikomanagementsysteme, *COSO I* bzw. *COSO II*, auf.

In Kapitel 4, »Integration von GRC-Initiativen durch SAP-Lösungen für GRC«, beschäftigen wir uns mit den wichtigsten Bestandteilen der SAP GRC-Lösungen und stellen sie in Verbindung mit den allgemeinen GRC-Initiativen. Wir zeigen auf, dass die Prüfung von Systemberechtigungen über Bordmittel zumeist nicht zielführend ist, und geben erste Einblicke in den Aufbau von SAP GRC Access Control und über den Ablauf von Implementierungsprojekten.

Die SAP-Lösungen für GRC

Im Laufe von Kapitel 5, »SAP-Berechtigungskonzept und Funktions trennung«, führen wir Sie in die wesentlichen Prinzipien des SAP-Berechtigungskonzepts und von *kritischen Funktionstrennungen* und *kritischen Berechtigungen* ein. Wir zeigen die Verbindung zu den GRC-Initiativen auf und sprechen Prüfungsthemen wie *Superuserberechtigungen*, *Data-Owner-Konzept* und typische Schwächen im Benutzer- und Rollenmanagement an.

Das SAP-Berechtigungskonzept

In Kapitel 6, »Risikoanalyse und Re-Design mit SAP GRC Access Control«, stellen wir die SAP GRC Access Control-Anwendungen *Risk Analysis and Remediation* (RAR) und *Superuser Privilege Management* (SPM) im Detail vor. Wir zeigen dabei unter anderem auf, wie Sie mit RAR Berechtigungen auf der Ebene von Benutzern oder Rollen auf kritische Funktionstrennungsverletzungen oder kritische Berechtigungen prüfen können, wie die festgestellten Risiken beseitigt werden können und wie Sie mit SPM eine Lösung für die Superuser-Problematik erhalten.

Analyse des Ist-Zustands

In Kapitel 7, »Benutzer- und Rollenmanagement mit SAP GRC Access Control«, werden dann die verbleibenden zwei SAP GRC Access Control-Anwendungen – *Compliant User Provisioning* (CUP) und *Enterprise Role Management* (ERM) – vorgestellt. Hier werden wir darstellen, wie Sie effiziente Rollen- und Benutzermanagementprozesse durch die Verwendung von CUP und ERM langfristig sicherstellen können.

Aufsetzen des Rollen- und Benutzer-managements

In diesem Buch finden Sie mehrere Orientierungshilfen, die Sie beim Zugriff auf die Informationen unterstützen. Die folgenden Symbole helfen Ihnen, sich schneller zu orientieren:

- ▶ *Hinweis:* Dieses Symbol steht an Stellen, die spezielle Empfehlungen enthalten, die Ihnen die Arbeit erleichtern können oder auf Fallstricke hinweisen.

[[<]]

- [\*] ► *Definition:* Dieses Symbol kennzeichnet zentrale Begriffe und Fakten, die Sie sich merken sollten.
- [zB] ► *Beispiel:* Unter diesem Symbol finden Sie Szenarien und Beispiele aus der Praxis.

## 1.4 Danksagung

Bei der Erstellung dieses Buches waren wir nicht gänzlich auf uns allein gestellt. Wir möchten uns an dieser Stelle bei allen Kollegen recht herzlich bedanken. Folgende Personen haben uns mit ihrem Fachwissen in verschiedenen Diskussionen zur Seite gestanden:

Carsten Trebuth, Johannes Liffers und Siegfried Filla von PricewaterhouseCoopers Deutschland, Antoine Wüthrich, Bastian Maylaender und Bernd Schnabl von PricewaterhouseCoopers Schweiz, Matthew Bennett und Scott Enerson von PricewaterhouseCoopers USA sowie Markus Ramoser und Raoul Vogel von PricewaterhouseCoopers Österreich. Danke für kritisches Feedback und laufende Motivation!

Bei der Recherche und der Erstellung der Abbildungen waren uns folgende Kollegen von PricewaterhouseCoopers Österreich behilflich: Michael Franz, Tatjana Heiszenberger und Martin Jandl.

Zudem danken wir Alexander Redlein von der Technischen Universität Wien, der uns vor allem bei den Praxisbeispielen mit kritischen Anmerkungen unterstützte.

Darüber hinaus möchten wir uns noch herzlich bei Gerald Zeiner von SAP Österreich für seine Unterstützung und bei unserem Lektoratsteam bei SAP PRESS, allen voran Frau Eva Tripp, für die gute Betreuung bedanken.

Zuletzt wollen wir auch unsere Familien und Freunde nicht vergessen, die die Entwicklung des Buchprojektes »hautnah und live« mit erlebt haben. Danke für eure Geduld und Unterstützung!

**Alexander Barta**

**Barbara Giller**

**Dr. Aslan Milla**

*Bevor Sie Ihr Berechtigungswesen reorganisieren, gilt es zunächst, den Ist-Zustand der SAP-Berechtigungen festzustellen. Wie SAP GRC Access Control dazu eingesetzt wird, lesen Sie in diesem Kapitel. Wie mit den Risiken zu verfahren ist, die Sie bei dieser Bestandsaufnahme aufdecken, ist außerdem Thema dieses Kapitels.*

## **6 Risikoanalyse und Re-Design mit SAP GRC Access Control**

In den vorangegangenen Kapiteln haben wir Sie in das Themengebiet Governance, Risikomanagement und Compliance (GRC) eingeführt und dabei insbesondere die Relevanz der Benutzerberechtigungen und des Benutzer- und Rollenmanagements aufgezeigt.

In diesem und dem nachfolgenden Kapitel wollen wir Ihnen zeigen, wie Sie die Benutzer- und Rollenmanagementanforderungen durch den Einsatz von SAP GRC Access Control erreichen.

In diesem Zusammenhang wird auch unsere Fallstudie fortgeführt: Unser Beispielkonzern hat sich zur langfristigen Sicherstellung der Ziele seiner GRC-Initiativen dafür entschieden, SAP GRC Access Control einzusetzen. In diesem Kapitel wird die Software im Unternehmen implementiert.

### **6.1 Anforderungen an SAP GRC Access Control**

Wir werden nun nochmals die wichtigsten Schlussfolgerungen aus unseren bisherigen Ausführungen zusammenfassen und aufzeigen, wie diese in einem Implementierungsprojekt aufgearbeitet werden.

Die folgenden wesentlichen Best-Practice-Standards für den Bereich der Systemberechtigungen sind auch für den Crashkurs-Konzern relevant:

**Best Practice für Berechtigungen**

1. Änderungen in den Benutzerstammsätzen von unternehmenskritischen Systemen (Neuanlage/Änderung bestehender User) müssen freigegeben und dokumentiert werden.
2. Der Freigabe von Änderungen an Benutzerstammsätzen, Rollen und Profilen sollte ein sauber definiertes *Data-Ownership-Konzept* zugrunde liegen.
3. Der Aufbau von Rollen und Profilen sowie deren Vergabe an Benutzer sollten die *Prinzipien der minimalen Vergabe von Berechtigungen* wie auch das *Prinzip der Trennung kritischer Funktionen* berücksichtigen.
4. Der Zustand der bestehenden Berechtigungen in den Systemen sollte regelmäßig auf bestehende Risiken geprüft, die Ergebnisse darüber sollten berichtet und entsprechende Konsequenzen abgeleitet werden.

Erinnern Sie sich an eine unserer wesentlichen Botschaften zu Systemberechtigungen:

[»]

**Bedeutung des Berechtigungskonzepts**

Ein aus Compliance-Sicht sauberes Berechtigungskonzept wirkt präventiv Risiken entgegen und unterstützt nachhaltig die Wirksamkeit interner Kontrollkonzepte.

In der Diskussion rund um das Erreichen all dieser Anforderungen treffen zwangsläufig zwei zum Teil sehr konträre Sichtweisen aufeinander. Wie auch Abbildung 6.1 verdeutlicht, handelt es sich dabei um die Compliance-Sicht des Prüfers und die betriebswirtschaftlich geprägte Sicht des Praktikers in den Fachabteilungen.

**Compliance-Sicht gegen Praktiker-Sicht**

Für den Prüfer wie die Leiterin der internen Revision für den Crashkurs-Konzern, Paula Prüfer, sind Berechtigungen ein wichtiges Mittel zur Erreichung von Kontrollsicherheit über systemgestützte Geschäftsprozesse, der Praktiker, wie es der IT-Governance-Verantwortliche Claus Cobit noch immer ist, sieht Berechtigungen jedoch eher aus dem Blickwinkel eines möglichst effizienten Arbeitsablaufs. Das Berechtigungskonzept steht somit im Spannungsfeld dieser zwei Sichtweisen. Aus unserer Erfahrung können sich dabei scheinbar unüberbrückbare Differenzen bei der Diskussion von Prüfungsfeststellungen im Bereich der Berechtigungen ergeben. Übliche – fast immer widerlegbare – Einwände in diesen Diskussionen haben wir für Sie

zusammengestellt. Diese Einwände werden für fast jedes denkbare Risiko und jede kritische Berechtigung verwendet:

- ▶ Das Risiko wird doch durch das SAP-Customizing abgedeckt, da kann nichts passieren ...
- ▶ Mit dieser Transaktion kommt man gar nicht zu der kritischen Funktion ...
- ▶ Wo ist bei dieser Funktion das Risiko? Das ist ja gar nicht kritisch ...
- ▶ Meine Mitarbeiter verwenden das ganz sicher nicht ...
- ▶ Wir kontrollieren so viel, da kann nichts durchrutschen ...

Auch wenn man viele Einwände durch Diskussion und genaue Erklärungen der jeweiligen Risiken ausräumen kann: Es besteht die Gefahr, in eine ineffiziente Pattstellung zu gelangen.

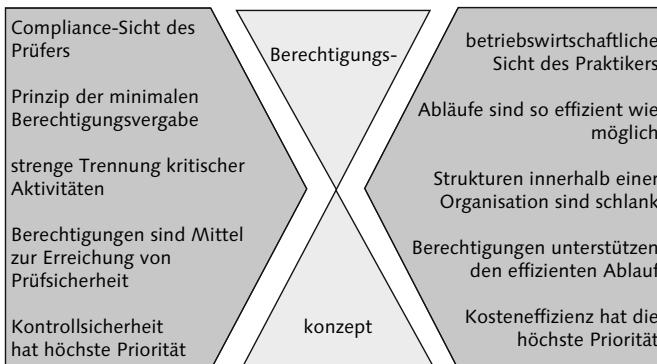


Abbildung 6.1 Das Berechtigungskonzept zwischen den Fronten

Die Anwendungen *Risk Analysis and Remediation* (RAR) und *Superuser Privilege Management* (SPM) versuchen, das oben beschriebene Spannungsfeld durch einen sowohl für Praktiker als auch Prüfer verständlichen, effizienten und tragbaren Prüfungsansatz weitgehend aufzulösen. Wie das funktioniert, wollen wir nun näher beleuchten.

## 6.2 Risk Analysis and Remediation

*Risk Analysis and Remediation* (RAR) ist das zentrale Modul von SAP GRC Access Control. Hier werden die Prüfungsregeln erzeugt, und es wird verwaltet, wie andere Module von Access Control im Rahmen der Risikoanalyse auf RAR zugreifen.

In diesem Buch beziehen wir uns, wenn nicht anders angegeben, auf RAR-Release 5.3, das auf dem *SAP NetWeaver Application Server* basiert. Vor allem was den Aufbau von Prüfregeln betrifft, sind die Inhalte aber auch auf die ABAP-Variante anwendbar.

#### Einstieg in RAR

Der Einstieg in RAR erfolgt mittels der *User Management Engine* (UME) des Benutzers entweder über das *Launch Pad* oder über den direkten Link `<anwendungsserver>:<portnummer>/webdynpro/dispatcher/sap.com/grc~ccappcomp/Compliance Calibrator`. Die Einstiegsmaske über den direkten Link sehen Sie in Abbildung 6.2. Im RAR-Modul können leider über diesen Einstieg – im Gegensatz zu *Compliant User Provisioning* (CUP) und *Enterprise Role Management* (ERM) – keine Spracheinstellungen geändert werden. Für RAR müssen Sie dazu die Spracheinstellungen über UME ändern.



Abbildung 6.2 Direkter Einstieg in RAR

#### Fünf Bereiche von RAR

Abbildung 6.3 zeigt die Bildschirmmaske von RAR, die direkt nach dem Einloggen erscheint. Wie Sie sehen, ist RAR über Registerkarten in fünf Bereiche aufgeteilt, in die, abhängig von den Berechtigungen des UME-Benutzers, navigiert werden kann:

- ▶ AUSKUNFT – aus diesem Register können Management- und Prüfungsberichte gestartet werden.
- ▶ REGELARCHITEKT – in diesem Register erfolgt die Konfiguration der Prüfregeln.
- ▶ KOMPENSIERUNG – in diesem Menü wird die Funktionalität der kompensierenden Kontrollen gepflegt.

- ▶ ALARMMONITOR – über dieses Menü werden automatisch generierte Warnmeldungen konfiguriert.
- ▶ KONFIGURATION – in diesem Register finden sich allgemeine Konfigurationseinstellungen abseits der Prüfregeln wieder.

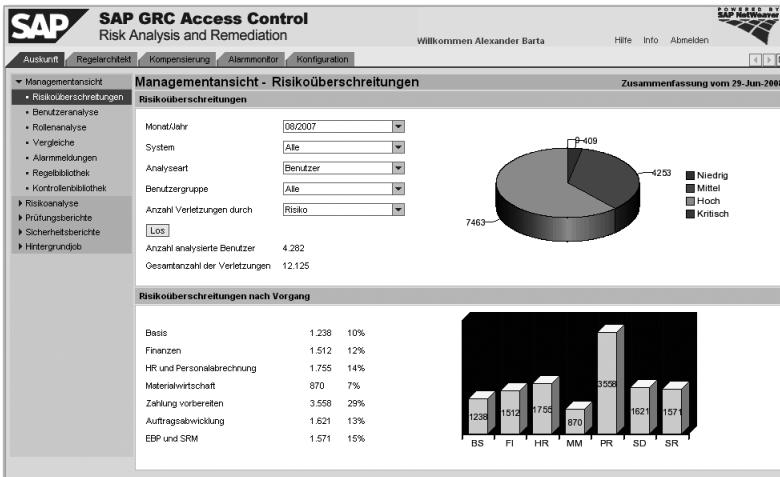


Abbildung 6.3 Startansicht der RAR-Anwendung

Über die im Startmenü angezeigte Managementansicht können grafische Übersichten über verschiedene Aspekte der in RAR vorgenommenen Prüfungen ausgewertet werden, durch das Klicken auf die Grafiken ist ein weiterer Drilldown möglich. Auf die Managementansicht kommen wir nochmals in Abschnitt 6.2.2, »Funktionsumfang von Risk Analysis and Remediation«, zurück.

### 6.2.1 Initiale Konfiguration von Risk Analysis and Remediation

Nach der Installation der verschiedenen Access-Control-Komponenten müssen einige initiale Konfigurationsmaßnahmen in RAR durchgeführt werden. Diese dienen dazu, RAR mit wichtigen Informationen und Details für die weitere Arbeit zu versorgen. Wie auch die Installation der Access-Control-Komponenten sind sie in *Guides* genau beschrieben, wir möchten daher an dieser Stelle nur einen Überblick geben.

Führen Sie folgende initialen Konfigurationsmaßnahmen durch:

1. Verbinden Sie RAR mit den zu prüfenden Systemen über Anlage der Systemkonnektoren im Konfigurationsmenü von RAR, siehe auch Abbildung 6.4. Der Verbindungstyp bei SAP-Systemen ist dabei zumeist ADAPTIVE RFC. Sie können nur Systeme auswählen, die Sie zuvor im Rahmen der technischen Installation über Java Connectors angebunden haben.

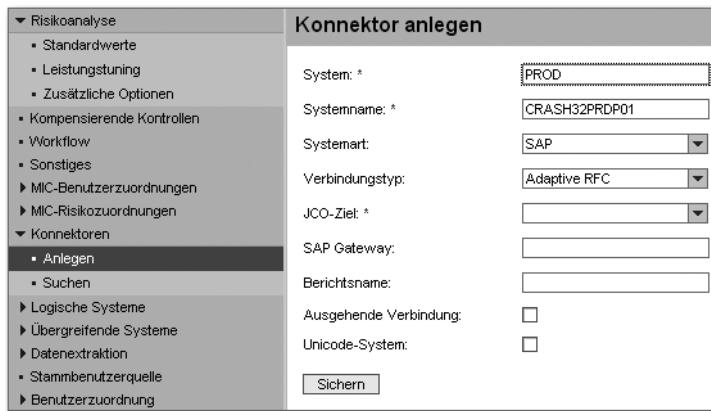


Abbildung 6.4 Konnektoren für zu prüfende Systeme anlegen

2. Geben Sie im Konfigurationsmenü von RAR im Unterpunkt STAMMBENUTZERQUELLE Ihr Referenzsystem für Benutzerstammdaten an (siehe Abbildung 6.5). Der etwas sperrige Begriff STAMMBENUTZERQUELLE ist in der englischen Originalbezeichnung vielleicht leichter verständlich – dort heißt er MASTER USER SOURCE.

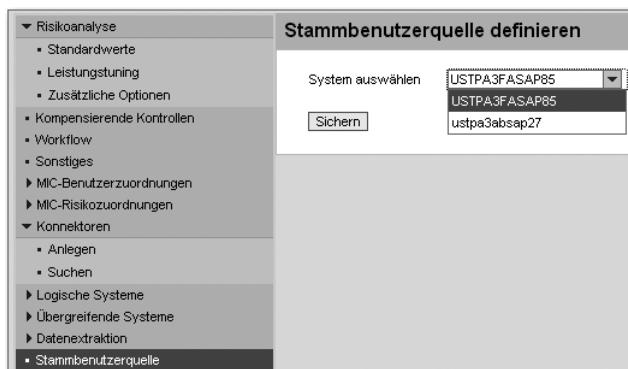


Abbildung 6.5 Definition des Referenzsystems für Benutzerstammsätze

3. Laden Sie statische Texte (im Wesentlichen die Bezeichnungen für SAP-Transaktionen) aus jedem der zu prüfenden SAP ERP-Systeme in RAR ein. Für den Extrakt wird ein entsprechendes ABAP-Programm zur Verfügung gestellt. Der Upload nach RAR wird über das Konfigurationsmenü unter dem Menüpunkt **OBJEKTE HOCHladen**, Untermenüpunkt **TEXTOBJEKTE**, durchgeführt.
4. Laden Sie den Stand der in Ihren SAP ERP-Systemen gepflegten SAP-Berechtigungsobjekte (siehe Transaktion SU24) in RAR für jedes zu prüfende SAP-System ein. Auch dazu wird ein entsprechendes ABAP-Programm zur Verfügung gestellt. Der Upload erfolgt dabei ebenfalls unter dem Menüpunkt **OBJEKTE HOCHladen**, aber im Untermenüpunkt **BERECHTIGUNGEN**.
5. Laden Sie die mit ausgelieferten Standardprüfregeln über das Konfigurationsmenü in RAR.
6. Planen Sie erste und regelmäßige und inkrementelle Hintergrund-jobs für die Synchronisation der Benutzer, Rollen und Profile, der Risikoanalysen und der Managementberichte ein.

Wir empfehlen Ihnen, die Schritte 5 und 6 erst nach erfolgter Anpassung der Standardprüfregeln durchzuführen. Beachten Sie dazu auch unsere Ausführungen in den nächsten Abschnitten.

#### Hinweis zu den initialen Konfigurationsmaßnahmen

[«]

Diese Maßnahmen sollten Sie zusammen mit Mitarbeitern Ihrer SAP-Basis-Administration durchführen. Achten Sie auf jeden Fall darauf, die angegebene Schrittabfolge einzuhalten.

### Pre- und Post-Installations-Check beim Crashkurs-Konzern

Nach erfolgtem Projekt-Kick-Off und der Coaching- und Voranalysephase mit Paula Prüfer und Claus Cobit erfolgt der Pre-Installations-Check durch die Berater und die SAP-Basis-Administration. Dabei wird anhand der *Installation Guides* und neuester *OSS-Meldungen* der SAP geprüft, ob die notwendigen technischen Voraussetzungen in der für Access Control vorgesehenen SAP NetWeaver Application Server-Plattform gegeben sind.

Danach werden die technische Implementierung und der initiale Setup der Komponenten der Access-Control-Anwendung durch die Mitarbeiter der SAP-Basis-Administration mit Unterstützung der Berater durchgeführt. Dabei werden wie geplant eine Testumgebung

mit Anschluss an das SAP ERP-Testsystem und eine Produktivumgebung mit Anschluss an das SAP ERP-Produktivsystem eingerichtet.

### 6.2.2 Funktionsumfang von Risk Analysis and Remediation

Es werden derzeit zwei Varianten von RAR und den anderen Access-Control-Anwendungen verwendet, eine ABAP-basierte und eine SAP NetWeaver Application Server-basierte Variante. Da beide Varianten zurzeit noch immer eingesetzt werden, dies zum Teil sogar parallel, wollen wir Ihnen kurz die Gemeinsamkeiten und Unterschiede der beiden Varianten, soweit es das RAR-Modul betrifft, vorstellen.

#### ABAP-basierte Variante

##### RAR in der ABAP-Variante

Die ABAP-basierte Version, besser bekannt unter *Compliance Calibrator 4.0*, läuft direkt auf dem zu prüfenden SAP ERP-System und ist, wie Abbildung 6.6 zeigt, über das SAP-Menü oder die Transaktion /VIRSA/ZVRAT aufrufbar. Historisch gesehen, ist die ABAP-Version die ältere Variante.



Abbildung 6.6 Einstieg in den Compliance Calibrator über das SAP-Menü

##### Fünf Bereiche von RAR in der ABAP-Variante

Grundsätzlich unterteilen sich der Compliance Calibrator 4.0 wie auch die neuere SAP NetWeaver Application Server-Variante in fünf gleiche Funktionsbereiche, die über das zentrale Menü erreicht werden können, siehe dazu auch Abbildung 6.7. Sie finden eine Reporting-Funktion, die High-Level-Berichte für das Management bietet (siehe Button **MANAGEMENTBERICHTE**), die *Risikoanalyse*, die direkt aus dem zentralen Menü heraus gestartet werden kann, und den *Regelarchitekten* (siehe Button **REGELARCHITEKT**), mit dem die zu prüfenden Abfragen verwaltet werden, vor.

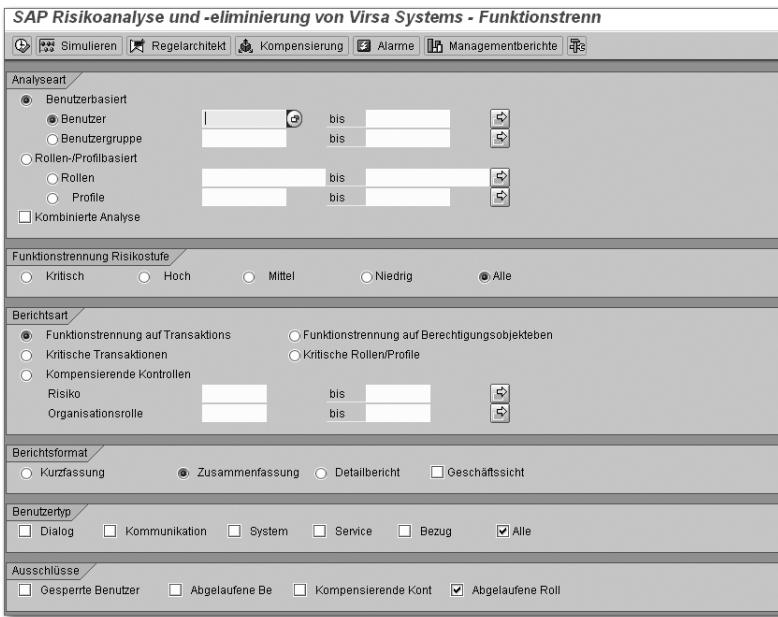


Abbildung 6.7 Zentrales Menü des Compliance Calibrators 4.0

Darüber hinaus gibt es auch hier Verzweigungen zur Anlage von *kompensierenden Kontrollen* (Button KOMPENSIERUNG) sowie zur Einrichtung von *automatischen Alarmmeldungen* (Button ALARME).

### Kompensierende Kontrolle

[\*]

Der Begriff *kompensierende Kontrolle* stammt aus dem Umfeld des Sarbanes-Oxley Acts. Im Englischen *Mitigating Control* genannt, wird er in der deutschen Literatur teilweise auch als *mitigierende Kontrolle* bezeichnet. Damit sind Kontrollen in den Unternehmen gemeint, die bekannte Kontrollschwächen zwar nicht gänzlich abstellen, aber das dadurch entstehende Risiko zumindest minimieren sollen.

Ein Beispiel dafür ist die stichprobenartige Kontrolle von durchgeführten Stammdatenänderungen, die durch einen Vorgesetzten auf Basis eines SAP-Standardberichts nachträglich durchgeführt wird, da sehr viele Mitarbeiter sowohl buchen als auch Stammdaten ändern können. Das Risiko unbefugter Änderungen der Stammdaten besteht weiterhin, es wird jedoch über die bestehende Kontrolle bis zu einem gewissen Grad minimiert.

Weitere Informationen zum Aufbau der Prüfregeln und der Verwaltung von kompensierenden Kontrollen und Alarmmeldungen erhalten Sie in den nachfolgenden Abschnitten.

### SAP NetWeaver Application Server-basierte Variante

RAR in der  
SAP NetWeaver  
Application Server-  
Variante

RAR in der SAP NetWeaver Application Server-Variante stellt die Weiterentwicklung der ABAP-Version dar. In den Grundfunktionalitäten, insbesondere der Art und Weise des Aufbaus der Prüfregeln, gibt es zur ABAP-Variante keine großen Unterschiede. Die fünf wesentlichen Funktionsbereiche haben wir bereits vorgestellt, siehe auch Abbildung 6.3.

Aktueller Status  
der vorhandenen  
Risiken

Die *Reporting-Funktionalität* für High-Level-Berichte an das Management findet sich im Register AUSKUNFT, Menüpunkt MANAGEMENTANSICHT. Ein Beispiel für das Management-Reporting auf der Ebene der Risikoverletzungen sehen Sie in Abbildung 6.3. Informationen über den aktuellen Stand der Analysen können dabei für verschiedene Zeitpunkte und über verschiedene Systeme auf der Basis von Risiko, Benutzer und Rollen durchgeführt und grafisch aufgearbeitet werden. Diese Berichte sollen dem groben Überblick dienen.

Unter dem Auswahlfeld GESAMTANZAHL DER VERLETZUNGEN ist die Summe der festgestellten Verstöße gegen die aufgestellten Prüfregeln je gewählter Basis zu verstehen. Diese kann auf Basis verschiedener Ansätze ermittelt werden.

[»]

#### Hinweis zur Managementansicht

Die Anzahl der Verletzungen sollte auf Basis des Risikos analysiert werden. Dies führt dazu, dass bei »Treffer« ein User nur einmal pro verletzter Funktionstrennung gezählt wird. Bei Verwendung von BERECHTIGUNG als Basis wird bei »Treffer« jedoch nicht einmal pro User und Risiko, sondern pro Kombination von kritischen Transaktionen und Objekten gezählt. Hat ein User also verschiedene kritische Kombinationen von Berechtigungen, werden diese entsprechend mehrfach gezählt. Abbildung 6.8 zeigt sehr deutlich, dass nur durch Änderung der Basis für unser Beispiel plötzlich die Zahl der »Treffer« im Vergleich zu Abbildung 6.3 stark erhöht wurde.

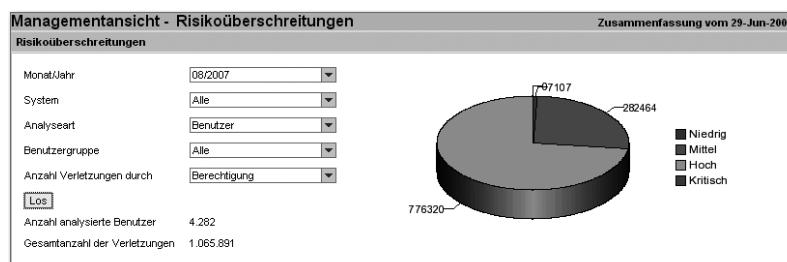


Abbildung 6.8 Anzahl der Verletzungen mit Basis-Berechtigung

Eine andere interessante High-Level-Berichtsmöglichkeit ist in Abbildung 6.9 dargestellt – über das Untermenü VERGLEICHE können Sie die Entwicklung auf den Ebenen Benutzer, Rollen und Profile für ein spezifisches oder alle geprüfte Systeme über einen zu wählenden Zeitverlauf darstellen. Verwenden Sie auch hier bei GESAMTANZAHL DER VERLETZUNGEN als Basis das RISIKO.

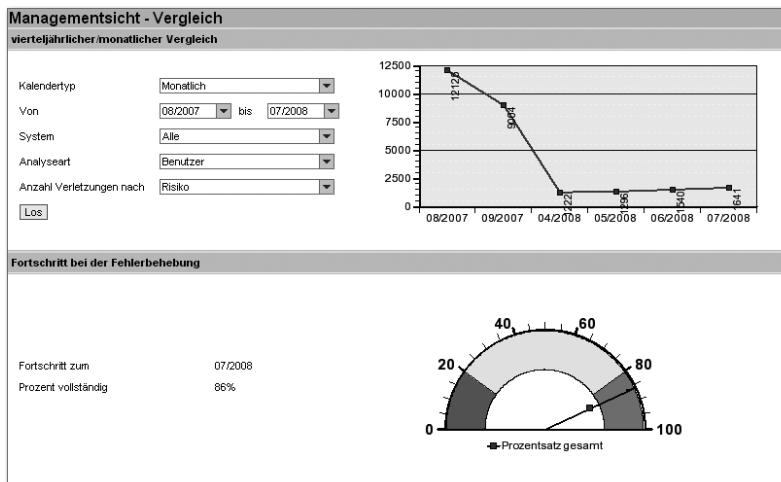


Abbildung 6.9 Vergleichende Managementberichte

Ebenfalls im Register AUSKUNFT findet sich unter einem eigenen Menüpunkt die RISIKOANALYSE, wie Abbildung 6.10 zeigt. Wie auch in der ABAP-Variante kann die Analyse auf Ebene von Benutzern, Rollen oder HR-Objekten für einen oder mehrere Prozesse und Risiken durchgeführt werden.

Üblicherweise wird (insbesondere im Rahmen von internen Revisionen oder IT-Revisionen) auf Ebene der Benutzer geprüft, um die vorhandenen Risiken aufzuzeigen, die ein Benutzer durch Anhäufung von Berechtigungen über die Vergabe einer oder einer Kombination vieler verschiedener Rollen erhalten hat. Die Analysen werden dabei oftmals getrennt pro Risiko ausgewertet, um einerseits die Reports übersichtlich zu halten und andererseits die Verteilung an entsprechende Stellen im Unternehmen zu erleichtern. Im Rahmen des Re-Designs des Berechtigungskonzepts wird auch die Analyse auf Ebene der Rollen zweckdienlich sein. Die Berichte der Risikoanalyse werden wir etwas später ausführlich besprechen.

Risikoanalyse auf verschiedenen Ebenen



**Abbildung 6.10** Einstieg in die Risikoanalyse in der SAP NetWeaver Application Server-Variante

### Einsatz von RAR auf Basis des SAP NetWeaver Application Servers ist die empfohlene Variante

Vorteil bei  
verteilten  
SAP-Landschaften

Üblicherweise wird RAR gemeinsam und integriert mit den anderen Teilmodulen von Access Control in der SAP NetWeaver Application Server-Variante eingesetzt. Dies hat insbesondere bei verteilten SAP-Landschaften den Vorteil, dass von einer zentralen Stelle übersichtlich auf die Abfragen aller angedockten Systeme zugegriffen und in einer gemeinsamen Datenbank verwaltet werden kann. Es kann jedoch zweckmäßig sein, die ABAP-Variante zusätzlich auf den zu prüfenden SAP-Systemen einzusetzen.

Die Komponenten der RAR-ABAP-Variante stehen nach der technischen Implementierung der *Real Time Agents* auf den SAP ERP-Systemen automatisch zur Verfügung.

Auch unser Crashkurs-Konzern wird die SAP NetWeaver Application Server-Variante der Access-Control-Anwendungen nutzen.

### 6.2.3 Aufbau der Prüfregeln in Risk Analysis and Remediation

Wie bereits erwähnt, werden die der Risikoanalyse zugrunde liegenden Prüfregeln im Register REGELARCHITEKT erstellt, mit Access Con-

trol ausgelieferte Standardregeln werden hochgeladen, gegebenenfalls modifiziert und die Regeln insgesamt verwaltet. Dies erfolgt dabei über die in Abbildung 6.11 dargestellten Menüpunkte.

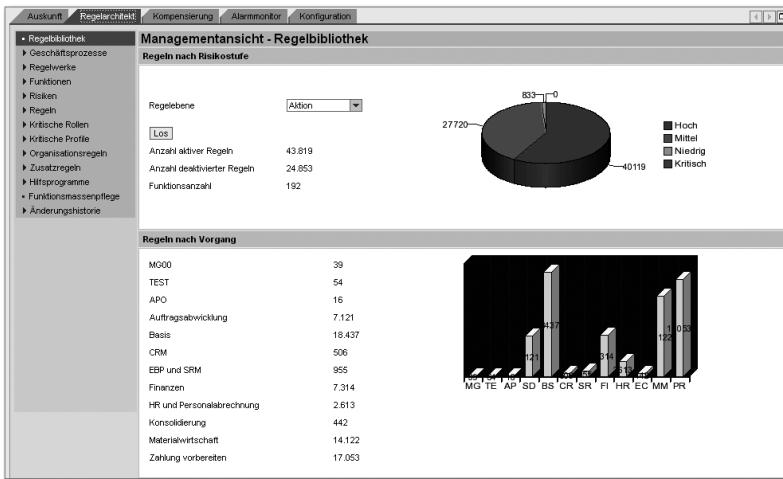


Abbildung 6.11 Menüpunkte im Regelarchitekten

In der Abbildung erkennen Sie dabei Begriffe wie *Geschäftsprozess*, *Regelsatz*, *Risiko* oder *Funktion*. Hans Huber, Paula Prüfer und Claus Cobit sehen uns als Berater etwas verwirrt an. Wie passen diese Begriffe zusammen? Das und die Bedeutung weiterer zentraler Begriffe wollen wir nun, ausgehend von Abbildung 6.12, erläutern.

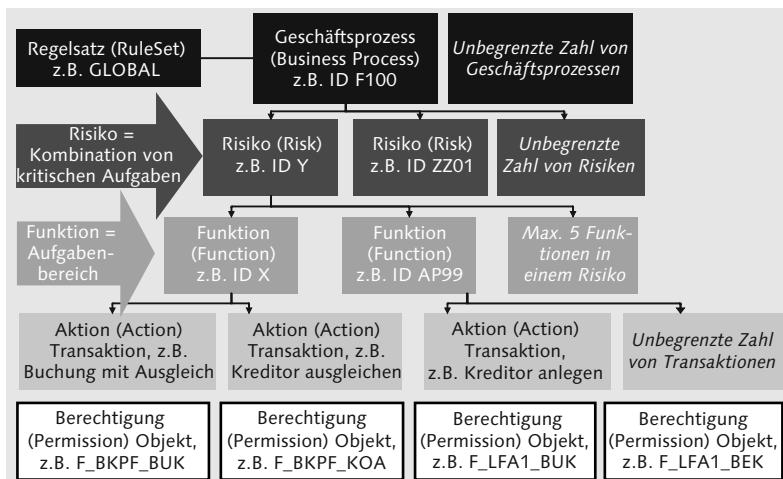


Abbildung 6.12 Begriffe und Zusammenhänge in RAR

## Regelsatz und Geschäftsprozess

### Ordnungskriterium für Regeln

Sowohl *Regelsatz* (*Rule Set*) als auch *Geschäftsprozess* (*Business Process*) dienen in RAR als Ordnungskriterium für die Vielzahl der bereits im Standard vorhandenen sowie für selbst entwickelte Prüfregeln. Seit Release Access Control 5.3 wird auch der Begriff *Regelwerk* an Stelle von Regelsatz verwendet. Wir werden für unsere weiteren Ausführungen beim bereits bekannten Begriff *Regelsatz* bleiben, in einigen Abbildungen wird jedoch der neue Begriff verwendet. *Funktionen* und *Risiken* werden darunter gruppiert und erhöhen somit die Übersichtlichkeit und erleichtern auch die Suche nach bestimmten Regeln und Risiken.

Es wird üblicherweise nur ein Standardregelsatz verwendet (»GLOBAL«), über die mit der Software ausgelieferten Standardregelsätze werden auch entsprechend vordefinierte Geschäftsprozesse bereitgestellt. Sie können zusätzlich beliebig viele Regelsätze und Geschäftsprozesse definieren, achten Sie jedoch darauf, dass diese den Abläufen Ihres Unternehmens auch entsprechen.



### Hinweis zu Regelsatz und Geschäftsprozess

Unsere Erfahrung zeigt, dass man mit den bereits angelegten Geschäftsprozessen und dem Standardregelsatz sehr gut auskommt. Es sollte nur in Ausnahmefällen notwendig sein, neue Regelsätze oder Geschäftsprozesse anzulegen.

Sie können Geschäftsprozesse und Regelsätze nur löschen, wenn diese nicht mit Funktionen oder Risiken verbunden sind. Das sollte jedoch nur selten notwendig sein.

Unser Crashkurs-Konzern wird zunächst nur den globalen Regelsatz verwenden.

## Funktion, Aktion und Berechtigung

### Funktion als Sammlung von Berechtigungen

Unter einer Funktion (*Function*) versteht man in RAR eine Sammlung verschiedener Systemberechtigungen, die man für die Ausübung eines zusammenhängenden Aufgabenbereiches in einem oder mehreren Systemen benötigt. Diese Systemberechtigungen sind dabei in *Aktionen* (*Action*) und *Berechtigungen* (*Permission*) unterteilt.

In einer SAP-Systemumgebung sind dabei unter *Aktion* eine SAP-Transaktion und unter *Berechtigung* die entsprechenden Berechti-

gungsobjekte und Feldwerte zu verstehen. Da in RAR jedoch auch Berechtigungen anderer Anwendungen (wie z. B. Oracle eBusiness Suite) geprüft werden können, hat man sich dazu entschlossen, neutrale Begriffe zu verwenden.

Nehmen wir zur Verdeutlichung ein Beispiel wie die Funktion GL01 – Hauptbuchkonten bebuchen – für ein SAP-System, siehe auch Abbildung 6.13. Sie ist bereits im Standardregelsatz für SAP-Systeme vorhanden und enthält auf der Registerkarte AKTION eine Sammlung von SAP-Transaktionen, die grundsätzlich für das Bebuchen von Hauptbuchkonten im SAP-System herangezogen werden können. Dabei müssen Sie jeweils auch das zu prüfende System (SAP-/Nicht-SAP-System) angeben.

Funktionsinformationen			
Funktion:	GL01: Hauptbuchkonten bebuchen		
Geschäftsprozess:	FIGL		
Aktion	Berechtigung	Beschreibung	Status
USTPA3FASAP85	ABAD	ABAD	aktiv
USTPA3FASAP85	ABAD_OLD	ABAD_OLD	aktiv
USTPA3FASAP85	F-01	F-01	aktiv
USTPA3FASAP85	F-02	F-02	aktiv
USTPA3FASAP85	F-03	F-03	aktiv
USTPA3FASAP85	F-04	F-04	aktiv
USTPA3FASAP85	F-34	F-34	aktiv
USTPA3FASAP85	F.19	F.19	aktiv
USTPA3FASAP85	F.56	F.56	aktiv
USTPA3FASAP85	F.57	F.57	aktiv

Abbildung 6.13 Aufbau einer Funktion auf der Ebene »Aktion«

Sie können einzelne Transaktionen dabei auch deaktivieren, diese werden dann nicht durch RAR geprüft. Ist eine Transaktion deaktiviert worden, erscheint eine ausgegraute Glühbirne im Feld STATUS. In unserem Beispiel sind alle im View sichtbaren Transaktionen aktiv.

Abbildung 6.14 zeigt für unser Beispiel die unter den Transaktionen zugeordneten entsprechenden SAP-Berechtigungsobjekte und Feldausprägungen auf der Registerkarte BERECHTIGUNG. Auch auf dieser Ebene können die vordefinierten Feldinhalte geändert oder Teile der Abfragen deaktiviert werden.

# Index

8. EU-Richtlinie 20, 55

## A

---

ABAP 218

Abfallbegleitschein 131

Abfallschlüssel 131

Abfragen

*anpassen* 229

*erweitern* 229

Ablaufdatum 348

*für Kontrollen* 279

Ablaufzeitermittlung 280

abteilungsfremde Rollen 305

Abteilungswechsel 304

Access Control Launch Pad 134, 307,  
350

Access Enforcer → Compliant User  
Provisioning (CUR)

Adaptive RFC 216

Aktion

*angeben* 247

*anpassen* 241

*definieren* 374

*Suchfunktion* 247

*zusätzliche anlegen* 250

Aktivierungsadministrator 192

Alarmbenachrichtigung 289

Alarmgenerierung

*Hintergrundjob* 288

Alarmmeldung 289

Alarmmonitor 215

Alarmüberwachung

*Einstieg* 287

Alert generieren 287

Analyseart 380

Analysephase 120

Analyseumfang 245

Änderungshistorie 365

Anlagenklasse 206

Anlagevermögen 204, 205

Ansprechpartner für Anwendungen 346

Ansprechpartner für Funktionsbereiche  
346

Antragsart 316

Antragsbearbeitung 307

Antragsformular 318, 344

Antragshistorie 334

Anzahl der Verletzungen 220

Anzeigeberechtigung 306

Application Approver → Ansprech-  
partner für Anwendungen

applikationsübergreifende Anwendun-  
gen 232

Arbeitsbelastung 131

ATLAS → Automatisiertes Tarif- und  
Lokales Zoll-Abwicklungssystem

Attribut deaktivieren 345

Attributgruppe 373

*definieren* 373

Audit Committee 56

Aushilfen 304

Auskunft 214, 351

Auswertung USOBX\_C 202

automatische Alarmmeldung anlegen  
286

automatische Berechtigungsprüfung 164

automatische Kontrolle 102, 129

automatischer Provisionierungstyp 342

Automatisiertes Tarif- und Lokales Zoll-  
Abwicklungssystem (ATLAS) 130

## B

---

Batchrisikoanalyse 266

Belegzugriff 161

Bentzerfestwert 349

Benutzeradministration 192

Benutzeränderungsprozess 304

Benutzerantrag verwalten 331

Benutzerberechtigungen anlegen 307

Benutzerdatenquelle definieren 310,  
311

benutzerdefinierte Attribute 357

benutzerdefiniertes Feld 345, 372

Benutzerdetails auslesen 311

Benutzerfestwert 349

Benutzergruppe SUPER 178

Benutzerkonto

*ändern* 316

- Benutzerkonto (Forts.)  
*einrichten* 316  
*löschen* 317  
*sperren/entsperren* 317
- Benutzermanagement 18, 58, 211, 303, 304
- Benutzerstamm 171
- Benutzerstammsatz 159, 174, 175, 216
- Benutzersynchronisation 266
- Berater 304
- Berechtigung 164  
*aktivieren* 243  
*ändern* 169  
*Änderungen* 154  
*anpassen* 241  
*Best Practices* 211  
*definieren* 357  
*erstmalige Berechtigungsvergabe* 151  
*Ist-Zustand* 211  
*Lösung* 155  
*manuelle Definition* 251  
*Sammlung* 224
- Berechtigungsadministrator 192, 272
- Berechtigungsdaten 357
- Berechtigungsfelder 164
- Berechtigungsgruppe 284
- Berechtigungskonzept 18, 134, 144, 190  
*Aufgaben* 144  
*Bedeutung* 212  
*Spezialfälle* 156
- Berechtigungsobjekt 132, 158, 159, 243, 358, 359  
*F\_BKPF\_BED* 161  
*F\_BKPF\_BEK* 161  
*F\_BKPF\_BES* 161  
*F\_BKPF\_BLA* 161  
*F\_BKPF\_BUK* 161, 170, 243  
*F\_BKPF\_BUP* 161  
*F\_BKPF\_GSB* 161, 244  
*F\_BKPF\_KOA* 161, 243  
*S\_TABU\_DIS* 166, 167
- Berechtigungspflege 192
- Berechtigungsprüfung 132
- Berichte  
*AGR\_AGRS* 174  
*AGR\_DEFINE* 174  
*AGR\_USERS* 174
- Berichte (Forts.)  
*RSSCD100\_PFCG* 174  
*RSUSR002* 133, 171, 193  
*RSUSR050* 174  
*RSUSR070* 174
- Berichtsarten 267
- Berichtsformate 269
- Bestandsaufnahme 211
- Bestätigungsdatum 348
- Bestellfreigabe 202
- Betriebssystem 310
- Bilanzrechtsmodernisierungsgesetz 58
- Boykottlisten → Sanktionslisten
- Buchung 198
- Business Application Programming Interface (BAPI) 343
- Business Process 224
- 
- C**
- Central User Administration (CUA) 343
- Change Management 303
- Change-Log-Auswertung 295
- CobiT 20, 83
- Compliance 28, 109
- Compliance Calibrator 4.0 218
- Compliance Calibrator → Risk Analysis and Remediation (RAR)
- Compliant User Provisioning (CUP) 21, 135, 137, 306, 307  
*Administrator* 308  
*Aufgaben* 308  
*Berichte* 308  
*Funktionsumfang* 312  
*Konfiguration* 309, 338  
*Standalone-Lösung* 310
- Compliant User Provisioning (CUR) 136
- Condition Group → Attributgruppe
- Configuration Guide 362
- Corporate Governance 20, 24, 25, 69
- Corporate Governance Kodex 76
- COSO I 20, 88
- COSO II 20
- Cross System 245
- Customer Approver Determinator (CAD) 340

**D**

Data Owner 21, 106, 151, 208, 272, 304, 305, 307, 313, 350  
*zuordnen* 296  
 Daten für die Rollenberechtigung sichern 375  
 Dateneigner-Konzept → Data Owner  
 Datensicherheitskonzept 305  
 Debitorenanlage 204  
 Default-Wert → Benutzerfestwert  
 Designphase 121  
 Detail 271  
 Determinator  
*benutzerdefiniert* 340  
 Detour Workflow → Umleitungs-workflow  
 Deutscher Corporate Governance Kodex 77

**E**

Eigenentwicklungen 255  
 Einkauf 201  
*Transaktionen* 202  
 Einkaufsprozess 190  
 Einzelsystem 245  
 elektronisches Ambulanzbuch 131  
 E-Mail-Erinnerung 340, 342  
 Embargoprüfung 130  
 Enron 34  
 Enterprise Role Management (ERM) 21, 135, 136, 137, 214, 306, 307, 347, 350, 364  
*Administrator-Rolle* 352  
*Funktionen* 352  
 Enterprise-Risk-Management-Modell 97  
 Entwicklung 356  
 Entzug von Berechtigungen 304  
 Environment, Health & Safety 127  
 Eskalation  
*Konfiguration* 323  
 Executive Summary 270  
 externe Benutzer 304  
 externe Prüfer 156

**F**

Fallstudie 46, 65  
 Feldausprägung 358  
 FI/CO  
*Transaktionen* 206  
 Finanzen 232  
 FireFighter 136, 291  
 FireFighter-Benutzer 300  
 Format  
*Detailbericht* 271  
*Kurzfassung* 270  
*Managementzusammenfassung* 270  
*Zusammenfassung* 271  
 Formularunterstützung  
*fehlende* 304  
 Freigabeverfahren 304, 312  
 Funktion  
*ändern* 247  
*anlegen* 244  
*anpassen* 241  
*GL01* 242  
*suchen* 248  
 Funktionsbereich 356, 372  
 Funktionstest  
*dokumentieren* 363  
*durchführen* 363  
 Funktionstrennung 133, 189, 190, 226, 304  
*Geschäftsbereichssicht* 198  
*IT-Sicht* 191, 197  
*Profilgenerators* 197  
*Risiko* 234

**G**

Gefahrgutklassifikation 131  
 Gefahrstoff 131  
 gegabelter Workflow 328  
 Genehmiger 378  
*ändern* 378  
*zuordnen* 341  
 Genehmigungsantrag 315, 316, 320, 332  
*anlegen* 332  
*Konfiguration* 346  
*suchen* 333  
 Genehmigungsprozess 312  
 Genehmigungsvertretung 334

Genehmigungsworkflow 141, 309, 353  
Geschäftsbereich  
    ändern 281  
    anlegen 281  
Geschäftsprozess 129, 224, 371  
    anlegen 233  
    anpassen 231  
Gestaltungsphase 122  
Governance, Risk und Compliance (GRC)  
    17, 30  
GRC Foundation 127  
GRC-Elemente  
    Arten der Integration 118  
GTS → SAP GRC Global Trade Services  
    (GTS)  
Güterklassifizierung 130

## H

---

Hauptbuch 206  
Hintergrundjob 265, 324  
HR Trigger 349  
Human Resources (HR) 232

## I

---

Implementierung 137  
    Durchführung der Risikoanalyse 139  
    Freigabestrategie 139  
    Konzeptionierung Workflow 139  
    Phase Bleibe sauber 139  
    Phase Werde sauber 137  
    Re-Design 139  
    Voranalyse- und Trainingsphase 137  
    Ziellandschaft 139  
    Zwei-System-Landschaft 139  
inaktive User 182  
Information Processing Objectives 147, 149  
Initiator 315, 320, 338  
    Konfiguration 321  
Installation Guides 141  
Instandhaltung 232  
interne Revision 156, 212  
Internes Kontrollsyste (IKS) 20, 37, 191, 304  
ISO/IEC 27002  
    2005 85  
IT Governance 81

IT Infrastructure Library (ITIL) 20, 86  
IT-Support 157

## J

---

Java Connector 216  
Java-Stack 142  
JD Edwards 310

## K

---

Karenzierung 156  
Kassa 207  
Kennwort-Self-Service 317  
Key Risk Indicators (KRI) 128  
kompensierende Kontrolle 135, 219, 278, 325, 339  
    anlegen 278, 281  
Kompensierung 214  
komplexen Selektionskriterien 166  
Konfiguration 351  
konforme Benutzererstellung →  
    Compliant User Provisioning (CUP)  
Konnektor  
    anlegen 368  
    definieren 310  
    zuordnen 369  
Kontenpflege 207  
Konto löschen 313  
KonTraG 59  
Kontrollmanagement 129  
Kreditor  
    Transaktionen 199  
Kreditoren-Stammdatenpflege 198  
Kriterium ändern 378  
kritische Berechtigung 21  
kritische Funktionstrennung 21  
kritische Profile 256, 265  
    ändern 258  
    anlegen 258  
kritische Rolle 256, 265  
    anlegen 256  
    auswählen 257  
    suchen 257  
kritische Standardprofile 169  
kritische Transaktionen 285  
Kundenstammdaten 203  
Kurzbezeichnung 372

**L**

- 
- laufende Genehmigung 331
  - Launch Pad → Access Control Launch Pad
  - LDAP-Zuordnung 349
  - Lehrlinge 304
  - Logfiles analysieren 287
  - logische Systeme 246

**M**

- 
- Management of Internal Controls (MIC) 267
  - Management Summary 270
  - Managementansicht 220
  - Managementbericht 266
  - Managementkontrollen 102
  - manuelle Kontrollen 102
  - Massenpflege 264
    - in ERM* 364
  - Maßnahmenkatalog 129
  - Materialwirtschaft 232
  - Methodik
    - Konfiguration* 374
  - Mitarbeiter des Sicherheitsteams 346
  - Mitarbeiterfunktionen anlegen 280
  - Mitigating Control 219, 278

**N**

- 
- nachträgliches Clearing 287
  - Namenskonvention 160, 165, 245
    - definieren* 378
  - NCTS → New Computerized Transit System (NCTS)
  - NetWeaver Visual Administrator 289
  - New Computerized Transit System (NCTS) 130
  - Notfalleinsatz 299

**O**

- 
- Objektdetails 252
  - Objektklasse 160, 359
  - obligatorische Risikoanalyse 314, 325
  - Oracle 310
  - Order to Cash 232
  - Organisationsebene 359

- Organisationsregel 258, 260, 265
  - ändern* 261
  - anlegen* 262
  - suchen* 261
- organisatorische Wertzuordnung 380
- Organizational Value Mapping → organisatorische Wertzuordnung
- OSS-Hinweis 141
- Österreichischer Arbeitskreis für Corporate Governance 79
- Österreichischer Corporate Governance Kodex 79

**P**

- 
- paralleler Workflow 328
  - Parmalat 35
  - Passwörter für FireFighter-Benutzer 296
  - PeopleSoft 310
  - Personalabrechnung 232
  - Personalabteilung 314
  - Pfad 315, 326, 328, 338
    - verwalten* 326
  - Phase »werde sauber« 137
  - Point of Contact → Ansprechpartner für Funktionsbereiche
  - Post-Installations-Check 217
  - Post-Konfigurationsmaßnahmen 309
  - Power-User 290
  - Präferenzabwicklung 130
    - Ausfuhrerstattung* 130
    - Zollpräferenz* 130
  - Pre- und Post-Implementierungsaktivität 141
  - Pre-Installations-Check 217
  - Procure to Pay 232
  - Produktion 356
  - Profil 159, 167
    - A\_ALL* 169
    - Einzelprofil* 168
    - generiertes Profil* 168
    - S\_A.DEVELOP* 179
    - S\_A.SYSTEM* 179
    - Sammelprofil* 168
    - Standardprofile* 169
  - Profiladministrator 197
  - Profilgenerator 169, 171, 172, 197, 290, 353, 359, 382
  - Profilname 356

- Profilsynchronisation 266  
Projekte/Releases 372  
Provisionierung 338  
Prozess definieren 376  
Prozess der Berechtigungspflege 150  
Prüfergebnis 259  
Prüfregel 134  
    *anpassen* 256  
    *aufbauen* 222  
Prüftool 180  
Prüfungsmethode 180
- 
- R**
- Rahmenbedingungen für Betrug 42  
RAR → Risk Analysis and Remediation (RAR)  
Reaffirm Period → Ablaufdatum  
Real Time Agent (RTA) 136, 141, 222  
Real Time Agents (RTA) 136  
rechtliche Rahmenbedingung 23  
Re-Design-Maßnahmen 276  
Regel 226  
    *aktualisieren* 228, 254  
    *generieren* 230  
    *Textfiles hochladen* 229  
Regelarchitekt 214, 218, 222, 264, 289  
Regelgenerierung  
    *Hintergrundjob* 254  
Regelkriterium 129  
Regelsatz 224  
    *angeben* 238  
Regelverletzung 220  
Regelwerk → Regelsatz  
Remote Function Call (RFC) 291, 294  
Report 180  
Request Type → Antragsart  
Risiken und Benutzer zuweisen 283  
Risiken und Kontrollen beim Berech-  
tigungskonzept 106  
Risiko 211, 226  
    *ändern* 239  
    *anlegen* 236  
    *anpassen* 231  
    *Bewertung* 234  
    *Risikoanalyse* 95  
    *Risikoidentifikation* 95  
    *Risikosteuerung* 95  
    *Risikoüberwachung* 96
- Risiko (Forts.)  
    *suchen* 239  
Risikoanalyse 218, 221, 332, 339, 361  
    *Benutzerebene* 267, 268  
    *beurteilen* 265  
    *durchführen* 265  
    *Ebene der Organisationsregel* 274  
    *Ergebnis* 362  
    *HR-Objekte* 267  
    *MIC* 267  
    *Organisationsebene* 267, 273  
    *Rollenebene* 267, 273  
Risikoanalyse und -eliminierung 135  
Risikograd 277  
Risikogruppen 128  
Risikomanagement 26, 128  
Risikomanagementsystem 20  
Risikoniveau 236  
Risikotyp 237  
Risikoverantwortlicher 289  
Risk Analysis and Remediation (RAR) 21,  
    135, 137, 213, 339  
    *Funktionen* 218  
    *Konfiguration* 215  
Risk Terminator 136, 140, 289, 360  
Role Expert → Enterprise Role Manage-  
ment (ERM)  
Role Management 350  
Role Relationship to Users and Groups  
    365  
Rolle 157, 165, 171, 319  
    *AEADMIN* 309  
    *ändern* 363  
    *Änderungshistorie* 366  
    *anlegen* 353, 355  
    *anzeigen* 173  
    *Beschreibung* 356  
    *genehmigen* 362, 374  
    *generieren* 362, 374  
    *kopieren* 364  
    *READMIN* 352  
    *Risikoanalyse* 361, 370  
    *suchen* 363  
    *Transaktion definieren* 357  
    *Verwaltung* 347  
    *Vorlage* 320  
Rollenableitung sichern 375  
Rollenanalyse initiieren 374  
Rollenänderungsprozess 304

- Rollenattribut  
*anlegen* 372  
*definieren* 371
- Rollenauswahl 319  
*Einschränkungen* 348
- Rollendefinition sichern 375
- Rollendetails anlegen 347
- Rolleneigner 314
- Rollenerstellungsprozess 377
- Rollengenerierung 370
- Rollengenerierung mit Verletzungen 380
- Rollengestalter 381
- Rollenmanagement 18, 58, 211, 303
- Rollenname 356, 379
- Rollenstatus 356
- Rollensuche 364
- Rollensynchronisation 266
- Rollentyp 356
- Rollenvergleich 366
- Rollenzuordnung 342, 349
- RTA → Real Time Agents (RTA)
- Rule Architect → Regelarchitekt
- Rule Set 224
- 
- S**
- Sammelrolle 171
- Sanktionslisten 130
- SAP Adapter 290
- SAP Advanced Planner and Optimizer (APO) 232
- SAP Compliance Management 130
- SAP Customer Relationship Management (CRM) 130, 232
- SAP Customs Management 130
- SAP EC-CS 232
- SAP Enterprise Buyer 232
- SAP ERP MM 130
- SAP ERP SD 130
- SAP GRC Global Trade Services 127
- SAP GRC Global Trade Services (GTS) 127
- SAP GRC Process Control 127
- SAP GRC → SAP-Lösungen für Governance, Risk und Compliance
- SAP GRC Risk Management 127
- SAP Internet Graphic Server 142
- SAP NetWeaver 126
- SAP NetWeaver Application Server 142, 217, 220, 291, 309, 339, 352
- SAP NetWeaver BI 128, 364
- SAP Service Marketplace 141
- SAP Supplier Relationship Management (SRM) 130, 232
- SAP System Landscape Directory 142
- SAP Test- und Entwicklungsumgebungen 314
- SAP\_ALL 153, 169, 209, 256, 283, 290, 297, 301
- SAP\_NEW 169, 256
- SAP-Basis 232
- SAP-Basisadministration 304, 309
- SAP-Benutzer zuordnen 296
- SAP-Berechtigungskonzept 157
- SAP-Branchenlösungen 232
- SAP-Lösungen für Governance, Risk und Compliance 125
- Sapstar 178
- Sarbanes-Oxley Act 20, 50, 125, 279
- Schadensdatenbank 129
- Schritt  
*definieren* 375  
*zuordnen* 375
- Security Lead → Mitarbeiter des Segregation of Duties (SoD) → Funktions-trennung
- Self-Assessment-Fragebogen 114
- sensible Felder (Debitoren) 284
- sensible Felder (Kreditoren) 286
- Service Level 336, 350  
*Diagrammansicht* 337
- Sicherheitsdatenblatt 131
- Sicherheitsteams 346
- Single System 245
- SMTP-Server 323
- Spezifikationsdatenbank 131
- SPM → Superuser Privilege Management (SPM)
- Spracheinstellung 214
- Stammbenutzerquelle 216
- Standard Workflow 309
- Standard-Determinator 322, 340  
*No Stage* 323
- Standardinitiator 320
- Standard-Konfiguration importieren 352
- Standard-Konfiguration von CUP impor-tieren 310

- Standardprüfregel anpassen 264  
Standardrisiko Excel 234  
Standardrollen 349  
Standard-Rollenprovisionierungstyp  
    342  
Stoffdossier 131  
Stoffmengenverwaltung 131  
Stufe 315, 321, 326, 338  
Stufendetails, Konfiguration 322  
SUIM 133  
Summary 271  
Superuser 64, 169, 175, 181  
    *Entwickleruser* 179  
    *SAP\** 177  
    *SAP\_ALL* 176  
    *SAP\_NEW* 178  
Superuser Privilege Management (SPM)  
    21, 135, 137, 213, 290  
    *benutzerbasiert* 292  
    *rollenbasiert* 293  
Superuserberechtigung 21  
Superuser-Berechtigungsverwaltung 135  
Supportkontakt hinterlegen 350  
Swiss Code of Best Practices 80  
SWX-Richtlinie 61  
Synchronisation 368  
    *Aktivitätswert* 369  
    *Feld* 369  
    *Objekt* 369  
    *Organisationswert* 369  
    *stufenweise* 267  
    *Transaktion* 369  
    *vollständige* 266  
Systemkonnektor 216  
Systemlandschaft 356  
    *anlegen* 369  
    *Konfiguration* 367  
systemübergreifendes System 245
- 
- T**
- Tabelle  
    *BKPF* 187  
    *BSEG* 187  
    *USOBT* 183  
    *USOBX* 183, 184  
    *USOBX\_C* 200  
    *UST10S* 167  
Tabellenpflege 185
- technische Installation 141  
Teilvorgang 356  
Testresultat sichern 375  
Tone at the top 72  
Trainees 304  
Transaction Usage 365  
Transaktion 132, 158  
    */n/virsa/zrtcnfg* 290  
    */VIRSA/ZVRAT* 218  
    *F110* 200  
    *PFCG* 289, 353, 359  
    *SA38* 133  
    *SPRO* 284  
    *SU01* 289, 293  
    *SU03* 165, 194  
    *SU10* 289  
Transaktionsberechtigung 158  
Transaktionszugriff 194
- 
- U**
- Überwacher 289  
Überwachung 105  
UME → User Management Engine (UME)  
UME-Benutzer 307, 350  
Umleitungsworkflow 327  
Umsetzung und Kontinuität 122  
Umsetzung von Governance 71  
unternehmenskritische Daten 305  
Unternehmensrollenverwaltung → Enterprise Role Management (ERM)  
URÄG 60  
User Data Source → Benutzerdatenquelle  
User Management Engine (UME) 142, 309, 352  
Userprofil 157
- 
- V**
- Verkaufsorganisation 255  
Verlinkung ERM/CUP 381  
Verlinkung ERM/RAR 381  
Vertrieb 203  
    *Transaktionen* 203  
Vier-Augen-Prinzip 284  
    *pflegen* 285  
Virsa Access Enforcer → Compliant User Provisioning (CUP)  
Vorlagebenutzer 319

Vorratsprozess 204  
*Transaktionen* 205

## W

---

Wirtschaftskriminalitätsstudie 38  
Wirtschaftsskandale 33  
Workflow  
    *erstellen* 329  
    *gegabelt* 328  
    *parallel* 329  
Workflow-spezifische Konfiguration 338  
Workflow-Typ 326, 362  
Workflow-Verkürzung 328

## X

---

XML-Datei 309, 352

## Z

---

Zentrales Benutzerverwaltungssystem  
(ZBV) 343  
Zugriffsrecht 207  
Zusatzregel 262  
    *anlegen* 263  
    *verwenden* 263