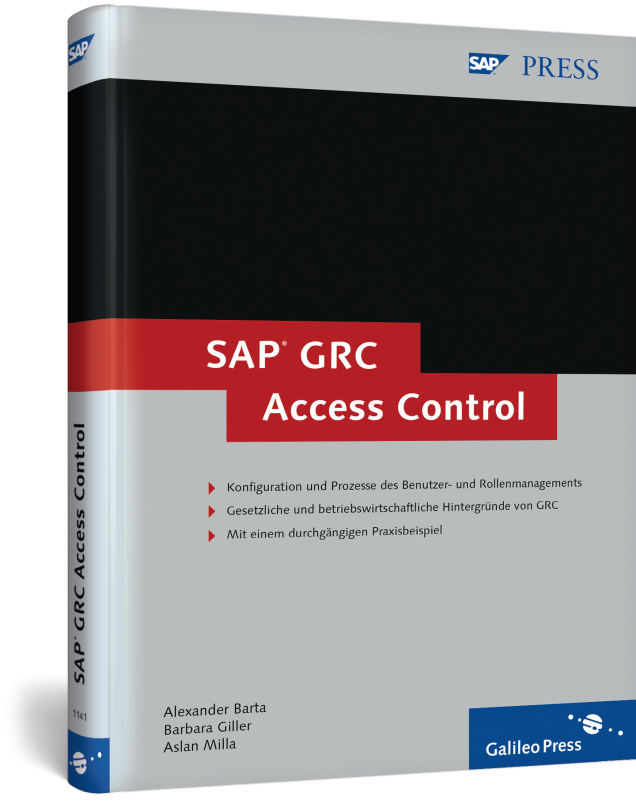
Alexander Barta, Barbara Giller, Aslan Milla

SAP® GRC Access Control



Galileo Press

Bonn • Boston

Auf einen Blick

Inhalt

Anhang

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 Kontrollsystem 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 Kontrollsystem 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-

rechtigungskonzept 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

Was ist GRC?

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-

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

An wen richtet sich dieses Buch?

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

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 Benutzeradministrationsprozess 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.

Die SAP-Lösungen für GRC

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.

Das SAP-Berechtigungskonzept

Im Laufe von Kapitel 5, »SAP-Berechtigungskonzept und Funktionstrennung«, 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.

Analyse des Ist-Zustands

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.

Aufsetzen des Rollen- und Benutzermanagements

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.

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« miterlebt 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.

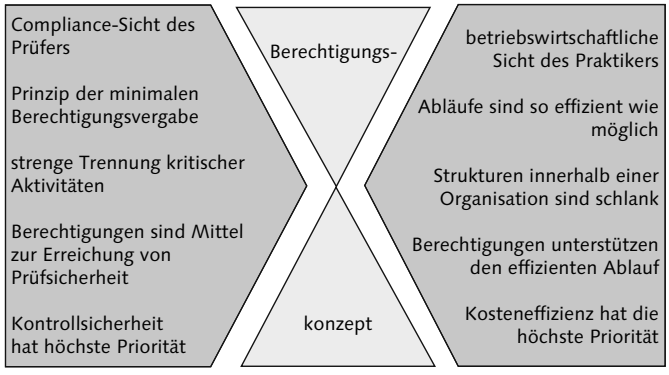


Abbildung 6.1 Das Berechtigungskonzept zwischen den Fronten

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.

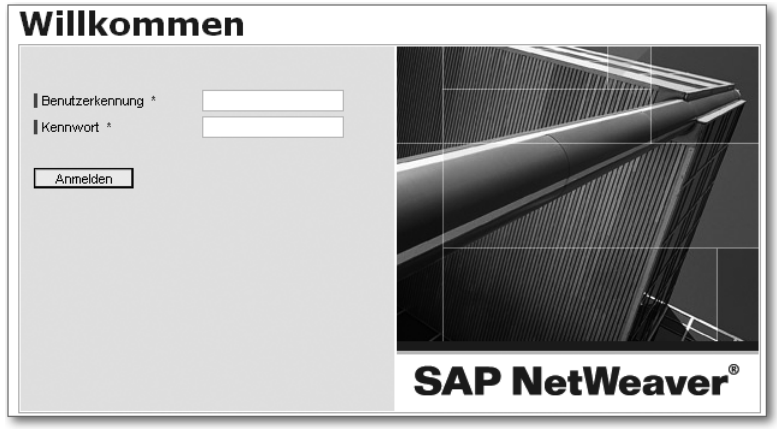


Abbildung 6.2 Direkter Einstieg in RAR

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.

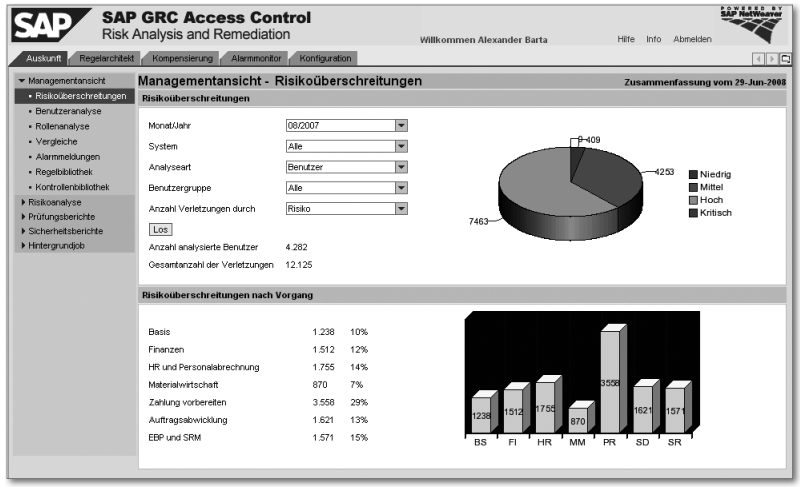


Abbildung 6.3 Startansicht der RAR-Anwendung

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.

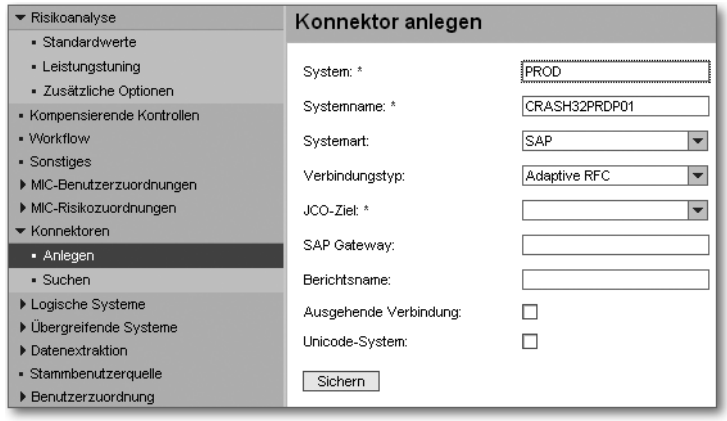


Abbildung 6.4 Konnektoren für zu prüfende Systeme anlegen

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.

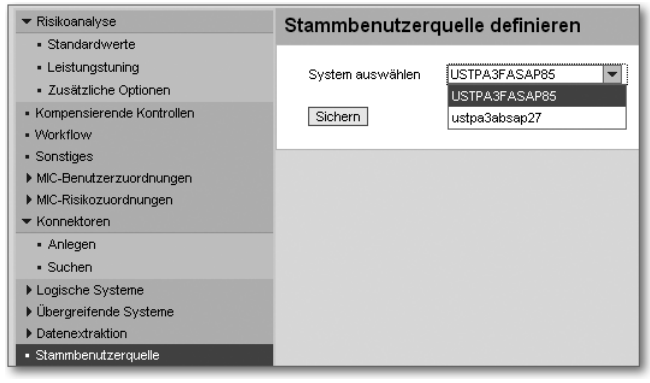


Abbildung 6.5 Definition des Referenzsystems für Benutzerstammsätze

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 Hintergrundjobs 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.

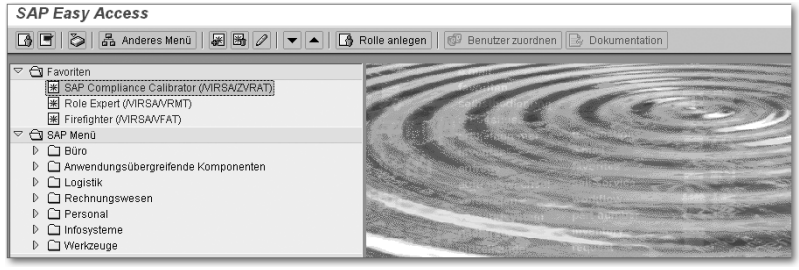


Abbildung 6.6 Einstieg in den Compliance Calibrator über das SAP-Menü

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.

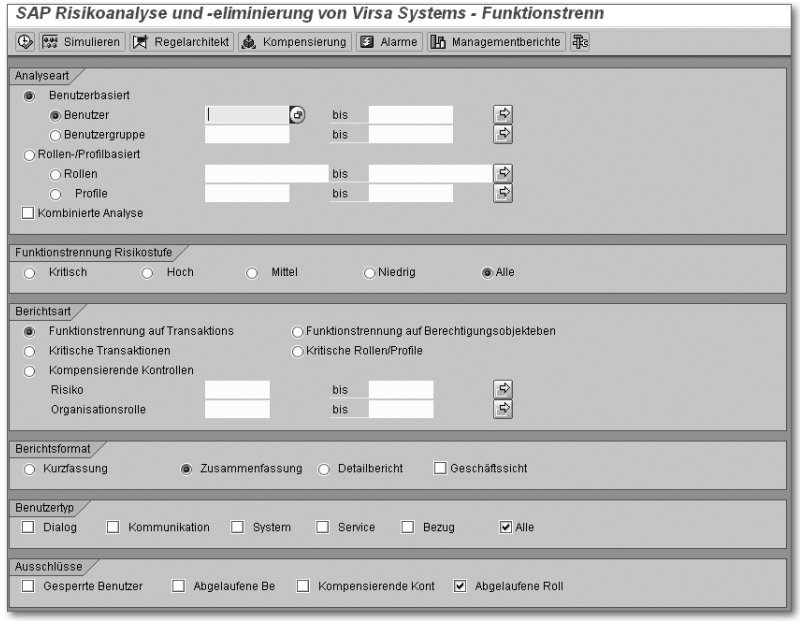


Abbildung 6.7 Zentrales Menü des Compliance Calibrators 4.0

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 »Treffern« ein User nur einmal pro verletzter Funktionstrennung gezählt wird. Bei Verwendung von BERECHTIGUNG als Basis wird bei »Treffern« 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.

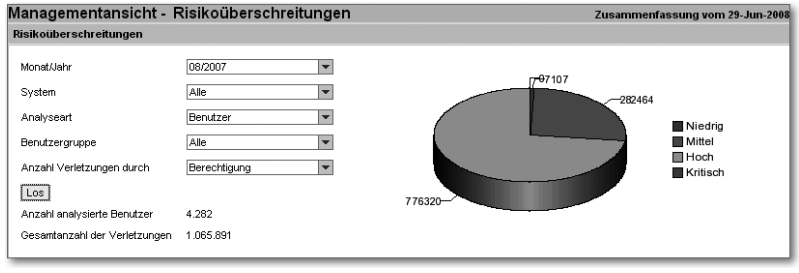


Abbildung 6.8 Anzahl der Verletzungen mit Basis-Berechtigung

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.

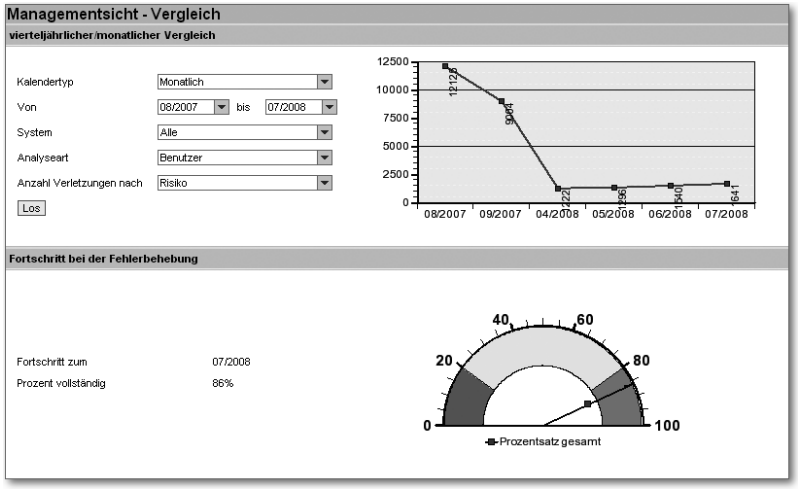


Abbildung 6.9 Vergleichende Managementberichte

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.

Risikoanalyse auf verschiedenen Ebenen

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.

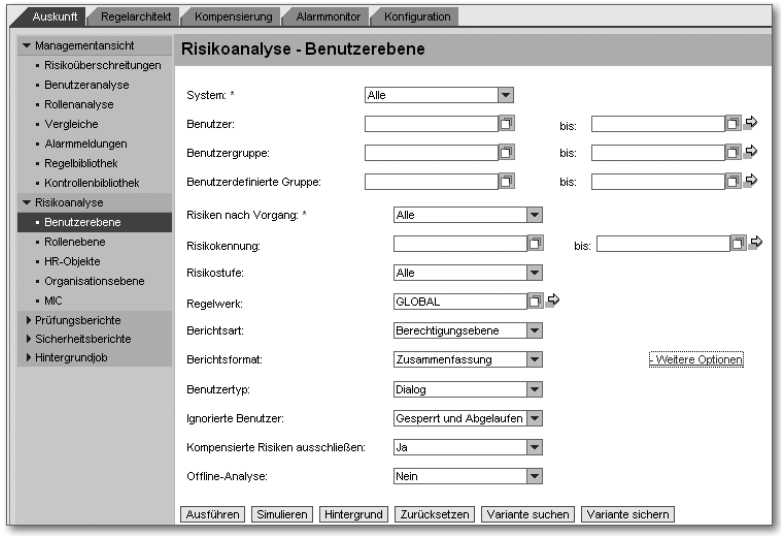


Abbildung 6.10 Einstieg in die Risikoanalyse in der SAP NetWeaver Application Server-Variante

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.

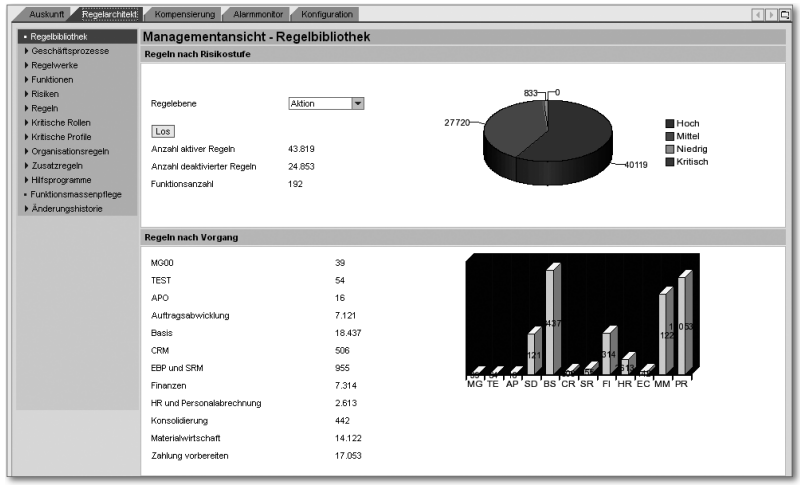


Abbildung 6.11 Menüpunkte im Regelarchitekten

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.

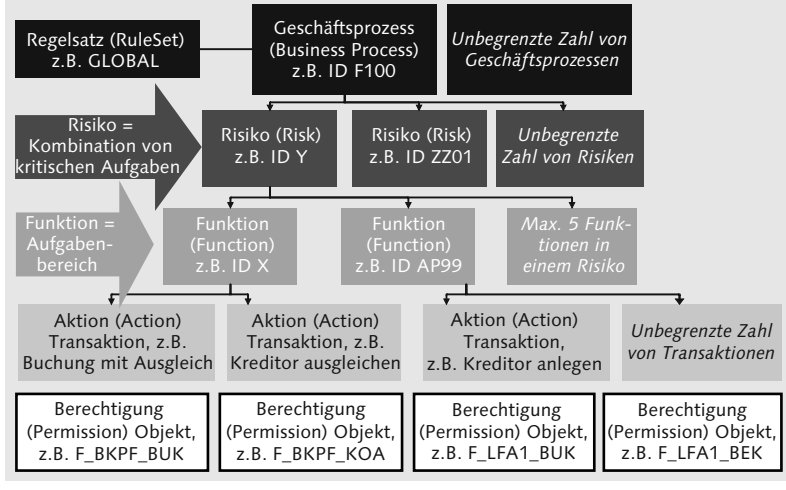


Abbildung 6.12 Begriffe und Zusammenhänge in RAR

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 gekannten 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.

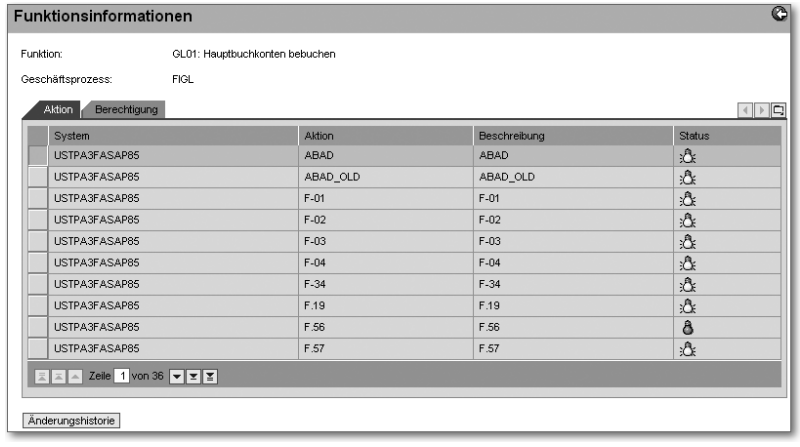


Abbildung 6.13 Aufbau einer Funktion auf der Ebene »Aktion«

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

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X

Z