Best-Practice-Leitfaden zur Einführung der SAP BusinessObjects GRC-Lösungen

Deutschsprachige SAP® Anwendergruppe

DSAG-ARBEITSGRUPPE GOVERNANCE, RISK MANAGEMENT UND COMPLIANCE

STAND 17. MAI 2010

SAP® BusinessObjects Access Control

BEST-PRACTICE-LEITFADEN ZUR EINFÜHRUNG DER SAP BUSINESSOBJECTS GRC-LÖSUNGEN

VERSION 0.7, STAND 17. MAI 2010

DSAG e. V.
Deutschsprachige SAP-Anwendergruppe

Deutschsprachige
SAP® Anwendergruppe

Inhaltsverzeichnis

Deutschsprachige
SAP® Anwendergruppe

Abbildungsverzeichnis

1 Einleitung

Der vorliegende Leitfaden verfolgt das Ziel, Best-Practice-Empfehlungen zu folgenden Applikationen und Release-Ständen der SAP BusinessObjects GRC-Lösungen vorzustellen:

- SAP BusinessObjects Access Control 5.3 mit folgenden Modulen:
  - Risk Analysis and Remediation (vormals: GRC-SCC/Virsa Compliance Calibrator)
  - Compliant User Provisioning (vormals: GRC-SAE/Virsa Access Enforcer)
  - Enterprise Role Management (vormals GRC-SRE/Virsa Role Expert)
  - Superuser Privilege Management (vormals GRC-SFF/Virsa FireFighter for SAP)
- GRC Process Control 3.0
- GRC Risk Management 3.0

Mit der nun vorliegenden ersten Ausgabe des Leitfadens stellt das Autorenteam Best-Practice-Empfehlungen zu SAP BusinessObjects Access Control 5.3 vor. Weitere Ausgaben zu SAP BusinessObjects Process Control 3.0 und Risk Management 3.0 werden folgen.

Die Best-Practice-Empfehlungen erheben keinen Anspruch auf Vollständigkeit, sondern geben die Projekt- und Praxiserfahrung der Autoren wieder. Insofern ist das Autorenteam auch dankbar für jede Art von Anregungen und Hinweisen zur weiteren Vervollständigung und Verbesserung des Leitfadens.

Dieser Leitfaden soll insbesondere den Unternehmen eine Hilfestellung bieten, die sich mit verschiedensten Anforderungen gesetzlicher, fachlicher und organisatorischer Art bei der Gestaltung der Zugriffskontrollen auf ihre Programme und Daten konfrontiert sehen. Hinzuweisen ist hier insbesondere auf die Anforderungen des Bilanzrechtsmodernisierungsgesetzes (BilMoG) mit der Gestaltung und Überwachung von internen Kontroll- und Risikomanagementsystemen sowie generell auf Anforderungen eines modernen Compliance Managements bei der Sicherstellung von wirksamen Funktionstrennungsprinzipien innerhalb der Unternehmensorganisation.

Die Autoren sind Mitglieder der AG Governance, Risk Management und Compliance (GRC) des DSAG-Arbeitskreises „Revision und Risikomanagement". Die Verantwortung für den Inhalt tragen die Autoren. Die redaktionelle Bearbeitung und das Layout liegen bei der DSAG.

1 Einleitung

DIE AUTOREN:

Herr Siegfried Filla	PricewaterhouseCoopers AG WPG
Herr Rolf-Udo Gilbert	dobis GmbH & Co. KG
Herr Christian Hofmann	arvato systems Technologies GmbH
Herr Dirk Jakob	T-Systems International GmbH
Herr Oliver Messmann	arvato systems Technologies GmbH
Herr Dr. Frank Off	Secude Global Consulting
Herr Christoph Reckers	IBSolution GmbH

DEUTSCHSPRACHIGE SAP® ANWENDERGRUPPE E.V.
Altrottstraße 34 a
69190 Walldorf
Deutschland

Fon: +49 (0) 62 27 – 358 09 58
Fax: +49 (0) 62 27 – 358 09 59
E-Mail: info@dsag.de
Internet: www.dsag.de

Die Autoren des vorliegenden Best-Practice-Leitfadens sind für Verbesserungs- sowie Änderungs- und Ergänzungswünsche dankbar. Dies gilt sowohl für Vorschläge zur Vertiefung der einzelnen Kapitel als auch für die Nennung von Beispielen aus konkreten Projekt- oder Prüfungserfahrungen.

Nutzen Sie hierzu bitte das entsprechende Forum der Arbeitsgruppe GRC im DSAG*Net* unter:

INFO / SERVICE → Foren → AG Governance, Risk Management, Compliance.

Nicht-Mitglieder der DSAG können sich gerne per E-Mail an info@dsag.de wenden.

2 Überblick

SAP hat die Standardsoftwarelösungen für den Themenbereich Governance, Risk Management und Compliance (GRC) im SAP BusinessObjects-Portfolio gebündelt (siehe Abb. 1).

2.1 SAP BUSINESSOBJECTS GRC-LÖSUNGEN

Das SAP BusinessObjects-Portfolio enthält Lösungen, um mehr Transparenz in Geschäftsabläufen zu erreichen, um die Performance innerhalb von Geschäftsprozessen zu managen und um die Risiken und die Compliance von Unternehmen zu überwachen und zu steuern. Im Einzelnen sind dies Business-Intelligence- und Information-Management-Lösungen, Anwendungen für Governance, Risikomanagement und Compliance sowie Lösungen zum Management der Unternehmensperformance.

GRC umfasst dabei die Applikationen für Access Control, Process Control, Risk Management, Global Trade Services und Environment, Health and Safety.

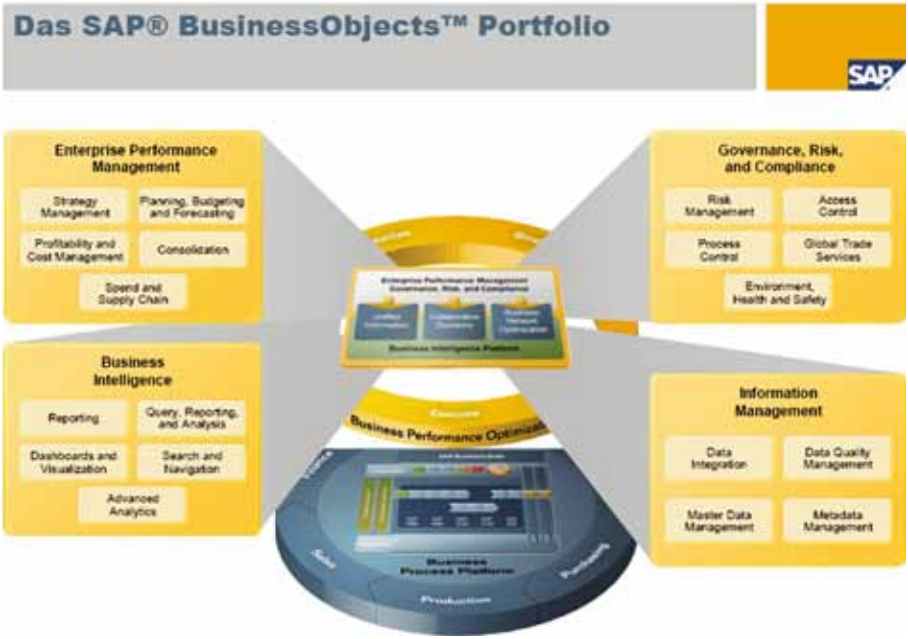

Abb. 1: Das SAP BusinessObjects-Portfolio

2 Überblick

Die SAP BusinessObjects GRC-Lösungen basieren auf der Technologieplattform SAP NetWeaver und den entsprechenden sog. „content shipments". Sie sollen Unternehmen dabei helfen, ihre strategische und operative Effektivität durch die Verdichtung und Steuerung von Aktivitäten bezüglich signifikanter Risiken (key risks) sowie durch die Automatisierung von Kontrollen über alle Geschäftsprozesse hinweg und die Überwachung von Risiken und Kontrollen über verschiedenste Systeme hinweg zu maximieren.

Im Überblick stellt sich die SAP-Release- und -Wartungsstrategie für GRC wie folgt dar (Stand: Januar 2009):

SAP BUSINESSOBJECTS GRC SOLUTIONS					
SAP® Release and Maintenance Strategy					
Release		Based on	Availability (Release to Customer)	End of Mainstream Maintenance	End of Extended Maintenance
Name	Version				
Access Control					
SAP GRC Access Control	5.3	SAP NetWeaver® 7.0	March 2008	March 2013	March 2016
Process Control					
SAP GRC Process Control	2.5	SAP NetWeaver® 7.0	March 2008	September 2010	n/a
SAP BusinessObjects Process Control	3.0	SAP enhancement package 1 for SAP NetWeaver® 7.0	May 2009	October 2011	n/a
Risk Management					
SAP BusinessObjects Risk Management	3.0	SAP NetWeaver® 7.0	May 2009	October 2011	n/a
Global Trade Services					
SAP BusinessObjects Global Trade Services	8.0	SAP NetWeaver® 7.0	March 2009	March 2013	n/a
SAP Electronic Invoicing for Brazil[11]	1.0	SAP NetWeaver® 7.0	April 2008	May 2010	n/a

Abb. 2: Release- und Wartungsstrategie SAP BusinessObjects GRC-Lösungen

SAP® BUSINESSOBJECTS ACCESS CONTROL

Access Control ermöglicht eine präventive Zugriffskontrolle zur Sicherstellung der Funktionstrennung in SAP-, Oracle- und PeopleSoft-Anwendungen. Kritische Berechtigungen können rasch entdeckt und eingeschränkt bzw. kontrolliert werden. Darüber hinaus wird ein standardisiertes und transparentes Berechtigungsmanagement unterstützt. Mit dieser Anwendung kann somit eine ordnungsmäßige und sichere Zugriffskontrolle organisiert werden, wobei folgende Module zunehmend integriert eingesetzt werden:

Risk Analysis and Remediation (RAR; vormals Compliance Calibrator)

Diese Software unterstützt eine sog. „Real-Time Compliance" mit dem Ziel, Sicherheits- und Kontrollverletzungen zu verhindern, bevor sie auftreten. Grundlage ist eine Bibliothek mit Funktionstrennungsregeln (segregation of duties) für SAP, Oracle und PeopleSoft.

Superuser Privilege Management (SPM; vormals Firefighter)

Mit diesem Modul können Notfallaktionen durch einen Superuser mit vollem Berechtigungsumfang durchgeführt werden. Diese Aktionen werden aufgezeichnet und sind damit auch nachprüfbar.

Enterprise Role Management (ERM; vormals Role Expert)

Ermöglicht ein standardisiertes, unternehmensweites Rollenmanagement. Geschäftsprozess-Owner können funktionale Rollen vorgeben, die dann von der IT-Benutzeradministration technisch umgesetzt werden können. Der gesamte Änderungsdienst wird aufgezeichnet und ist prüfbar.

Compliant User Provisioning (CUP; vormals Access Enforcer)

Ermöglicht eine ordnungsmäßige Benutzeradministration mit automatisierten Antrags- und Genehmigungsprozessen innerhalb einer Real-Time-Risikoüberwachung.

SAP BUSINESSOBJECTS PROCESS CONTROL

Mit Process Control können die Kontrollen sämtlicher Unternehmensprozesse im Sinne eines systematisierten internen Kontrollsystems dargestellt und überwacht werden. Durch automatische und manuelle Tests werden die Kontrollen auf ihre Wirksamkeit überprüft. Über eine „Global Heatmap" können jene Bereiche im Unternehmen identifiziert und priorisiert werden, in denen die Wirksamkeit von Kontrollen fraglich ist und Korrekturmaßnahmen ergriffen werden müssen.

SAP BUSINESSOBJECTS RISK MANAGEMENT

Mit der operativen Risikomanagementlösung „Risk Management" kann ein umfassendes Risikoprofil des Unternehmens entwickelt werden sowie Risikobereitschaft und Reaktionsstrategien bei Verlustereignissen festgelegt werden. Durch erhöhte Transparenz von Risikoabhängigkeiten wird eine wichtige Grundlage für strategische Entscheidungen geschaffen.

2 Überblick

SAP BUSINESSOBJECTS GLOBAL TRADE SERVICES

Global Trade Services ermöglichen ein wirksames Zoll- und Außenhandelsmanagement internationaler Handelsgeschäfte. Die Außenhandelsprozesse können dabei einheitlich und unternehmensweit standardisiert werden, was die Einhaltung diverser gesetzlicher und regulatorischer Anforderungen vereinfacht.

SAP ENVIRONMENT, HEALTH & SAFETY

Mit SAP Environment, Health & Safety (SAP EH&S) können Anforderungen aus internationalen Richtlinien und Bestimmungen zur Produktsicherheit, für Gefahrstoffe und Gefahrgüter oder für die Abfallentsorgung abgedeckt werden. Darüber hinaus können Aufgabenstellungen rund um die Arbeitshygiene oder Arbeitsmedizin geregelt werden.

2.2 REGULATORISCHE ANFORDERUNGEN

In Deutschland haben sich Gesetzgeber, das Institut der Wirtschaftsprüfer in Deutschland (IDW) sowie das Deutsche Rechnungslegungs Standards Committee e.V. (DRSC) schon seit vielen Jahren mit den Themen Governance, Risk Management und Compliance beschäftigt. Hervorzuheben sind dabei die Regelungen zum Deutschen Corporate Governance Kodex[1], zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG[2]), zum internen Kontrollsystem von Unternehmen[3] und aktuell zum Bilanzrechtsmodernisierungsgesetz (BilMoG[4]).

Den Maßstab für die Umsetzung regulatorischer Anforderungen in deutschen Unternehmen bilden im Rahmen der Prüfung der Finanzberichterstattung durch Wirtschaftsprüfer im Wesentlichen folgende gesetzliche Regelungen und Prüfungsstandards des Instituts der Wirtschaftsprüfer (IDW):

- die handels- und steuerrechtlichen Vorschriften zur Ordnungsmäßigkeit der Buchführung (§§ 238 f. und 257 HGB sowie §§ 145 bis 147 AO),
- die IDW-Stellungnahme zur Rechnungslegung „Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie“ (IDW RS FAIT 1, Stand: 24. September 2002),
- die IDW-Stellungnahme zur Rechnungslegung „Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Electronic Commerce (IDW RS FAIT 2, Stand: 29. September 2003),
- der IDW-Prüfungsstandard „Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken“ (IDW PS 261, Stand 6. September 2006),
- der IDW-Prüfungsstandard zur „Abschlussprüfung bei Einsatz von Informationstechnologie“ (IDW PS 330, Stand: 24. September 2002) sowie
- die von der Arbeitsgemeinschaft für Wirtschaftliche Verwaltung e.V. erarbeiteten „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)“ sowie das dazu ergangene Schreiben des Bundesministers der Finanzen vom 7. November 1995.

Die vorgenannten gesetzlichen Vorschriften und fachlichen Stellungnahmen sind generell zu beachtende Anforderungen und beziehen sich überwiegend auf rechnungslegungsrelevante Sachverhalte. Gleichwohl sind sie aufgrund gleicher Kontrollziele geeignet, auch Aussagen zur Ordnungsmäßigkeit bei Fragestellungen außerhalb der Buchführung zu treffen.

Darüber hinaus können im Einzelfall weitere Prüfungsstandards anzuwenden sein, z. B. für Dienstleistungsunternehmen oder Shared Service Center, die administrative Aufgaben u. a. im Bereich der Benutzeradministration und des Zugriffsschutzes übernommen haben (z. B. der IDW-Prüfungsstandard zur „Prüfung des

1 Deutscher Corporate Governance Kodex (DCGK Juni 2009)
2 Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) 1. Mai 1998
3 IDW-Prüfungsstandard „Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken“ (IDW PS 261, Stand 6. September 2006).
4 Bilanzrechtsmodernisierungsgesetz (BilMoG) vom 25. Mai 2009 (BGBl. I S. 1102)

internen Kontrollsystems bei Dienstleistungsunternehmen für auf das Dienstleistungsunternehmen ausgelagerte Funktionen" (IDW PS 951, Stand: 19. September 2007)).

Dieser GRC-Best-Practice-Leitfaden möchte lediglich in Kurzform auf wesentliche, zu beachtende regulatorische Anforderungen insbesondere in jüngerer Zeit eingehen und erhebt deshalb auch keinen Anspruch auf Vollständigkeit der hier vorgestellten Regelungen. Wer sich intensiver mit diesem Thema beschäftigen möchte, kann dies u. a. in folgenden Büchern nachlesen:

- SAP®-Berechtigungswesen, 2010, ISBN 978-3-8362-1349-3
- SAP® Access Control, 2008, ISBN 978-3-8362-1141-3
- Governance, Risk und Compliance mit SAP, 2008, ISBN 978-3-8362-1140-6
- SOX Compliance with SAP Treasury and Risk Management, 2008, ISBN 978-1-59229-2004
- CobiT und der Sarbanes-Oxley Act, 2007, ISBN 978-3-8362-1013-3
- Sicherheit und Berechtigungen in SAP-Systemen, 2005, ISBN 978-3-89842-670-1

Als ergänzende Lektüre empfehlen wir den DSAG Datenschutzleitfaden SAP ERP 6.0 sowie den Prüfleitfaden SAP ERP 6.0 (beide im DSAG*Net* veröffentlicht).

2.2.1 DEUTSCHER CORPORATE GOVERNANCE KODEX

Die Themen Risikomanagement und Compliance sind im DCGK in folgenden Abschnitten: „Zusammenwirken von Vorstand und Aufsichtsrat" wie folgt angesprochen:

Abschnitt 3 „Zusammenwirken von Vorstand und Aufsichtsrat"
Der Vorstand informiert den Aufsichtsrat regelmäßig, zeitnah und umfassend über alle für das Unternehmen relevanten Fragen der Planung, der Geschäftsentwicklung, der Risikolage, des Risikomanagements und der Compliance.

Abschnitt 4 „Aufgaben und Zuständigkeiten des Vorstands"
Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin (Compliance).

Der Vorstand sorgt für ein angemessenes Risikomanagement und Risikocontrolling im Unternehmen.

Abschnitt 5 „Aufgaben und Befugnisse des Aufsichtsratsvorsitzenden"
Der Aufsichtsratsvorsitzende soll mit dem Vorstand, insbesondere mit dem Vorsitzenden bzw. Sprecher des Vorstands, regelmäßig Kontakt halten und mit ihm die Strategie, die Geschäftsentwicklung und das Risikomanagement des Unternehmens beraten.

Abschnitt 5.3 „Bildung von Ausschüssen"
Der Aufsichtsrat soll einen Prüfungsausschuss (Audit Committee) einrichten, der sich insbesondere mit Fragen der Rechnungslegung, des Risikomanagements und der Compliance … befasst.

2.2.2 GESETZ ZUR KONTROLLE UND TRANSPARENZ IM UNTERNEHMENSBEREICH (KONTRAG)

Kern des KonTraG ist eine Vorschrift, die Unternehmensleitungen dazu zwingt, ein unternehmensweites Früherkennungssystem für Risiken (Risikofrüherkennungssystem) einzuführen und zu betreiben sowie Aussagen zu Risiken und zur Risikostruktur des Unternehmens im Lagebericht des Jahresabschlusses der Gesellschaft zu veröffentlichen.

Die Einrichtung eines Risikomanagementsystems (RMS) ist unmittelbar nur für Aktiengesellschaften gesetzlich vorgeschrieben. Das RMS muss demnach gewährleisten, dass die das Unternehmen möglichen drohenden Risiken vollständig erfasst (KonTraG – Erfassung der Risiken), beherrscht und gesteuert werden. Dies heißt konkret, dass das RMS Maßnahmen festlegen muss, die eine effiziente Identifikation, Analyse und Bewertung der Risiken ermöglichen (Risikostrategie).

Schließlich lässt sich hieraus die weitere inhaltliche Anforderung ableiten, dass es einer unterstützenden zielorientierten Koordination von Risikostrategie, Informationsversorgung, Überwachung und Steuerung durch ein Controlling oder spezieller ein sog. „Risikocontrolling" bedarf, denn dies bildet eine unabdingbare Voraussetzung für die Errichtung und Erhaltung der Reaktionsfähigkeit und Koordinationsfähigkeit des Unternehmens und ist daher als Element eines Risikomanagementsystems und eines Überwachungssystems unverzichtbar.

2.2.3 IDW RS FAIT 1[5]

RS FAIT 1 definiert u. a. Sicherheitsanforderungen an rechnungslegungsrelevante Daten. Im Einzelnen werden gefordert:

IT-Systeme haben daher die folgenden Sicherheitsanforderungen zu erfüllen:

- Vertraulichkeit verlangt, dass von Dritten erlangte Daten nicht unberechtigt weitergegeben oder veröffentlicht werden. Organisatorische und technische Maßnahmen – wie etwa Verschlüsselungstechniken – umfassen u. a. Anweisungen zur Beschränkung der Übermittlung personenbezogener Daten an Dritte, die verschlüsselte Übermittlung von Daten an berechtigte Dritte, die eindeutige Identifizierung und Verifizierung des Empfängers von Daten oder die Einhaltung von Löschfristen gespeicherter personenbezogener Daten.

- Integrität von IT-Systemen ist gegeben, wenn die Daten und die IT-Infrastruktur sowie die IT-Anwendungen vollständig und richtig zur Verfügung stehen und vor Manipulation und ungewollten oder fehlerhaften Änderungen geschützt sind. Organisatorische Maßnahmen sind geeignete Test- und Freigabeverfahren. Technische Maßnahmen sind z. B. Firewalls und Virenscanner. Die Ordnungsmäßigkeit der IT-gestützten Rechnungslegung setzt voraus, dass neben den Daten und IT-Anwendungen auch die IT-Infrastruktur nur in einem festgelegten Zustand eingesetzt wird und nur autorisierte Änderungen zugelassen werden.

- Verfügbarkeit verlangt zum einen, dass das Unternehmen zur Aufrechterhaltung des Geschäftsbetriebs die ständige Verfügbarkeit der IT-Infrastruktur, der IT-Anwendungen sowie der Daten gewährleistet. Zum anderen müssen die IT-Infrastruktur, die IT-Anwendungen und Daten sowie die erforderliche IT-Organisation in angemessener Zeit funktionsfähig bereitstehen. Daher sind z. B. geeignete Back-up-Verfahren zur Notfallvorsorge einzurichten. Maßnahmen zur Sicherung der Verfügbarkeit sind erforderlich, um den Anforderungen nach Lesbarmachung der Buchführung gerecht zu werden.

5 IDW Stellungnahme zur Rechnungslegung „Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie" (IDW RS FAIT 1, Stand: 24. September 2002).

> Autorisierung bedeutet, dass nur im Voraus festgelegte Personen auf Daten zugreifen können (autorisierte Personen) und dass nur sie die für das System definierten Rechte wahrnehmen können. Diese Rechte betreffen das Lesen, Anlegen, Ändern und Löschen von Daten oder die Administration eines IT-Systems. Dadurch soll ausschließlich die genehmigte Abbildung von Geschäftsvorfällen im System gewährleistet werden. Geeignete Verfahren hierfür sind physische und logische Zugriffsschutzmaßnahmen (z. B. Passwortschutz). Organisatorische Regelungen und technische Systeme zum Zugriffsschutz sind die Voraussetzung zur Umsetzung der erforderlichen Funktionstrennungen. Neben Identitätskarten werden zukünftig biometrische Zugriffsgenehmigungsverfahren an Bedeutung gewinnen.

> Authentizität ist gegeben, wenn ein Geschäftsvorfall einem Verursacher eindeutig zuzuordnen ist. Dies kann etwa über Berechtigungsverfahren geschehen. Beim elektronischen Datenaustausch bieten sich für eine Identifizierung des Partners beispielsweise digitale Signatur- oder passwortgestützte Identifikationsverfahren an.

> Unter Verbindlichkeit wird die Eigenschaft von IT-gestützten Verfahren verstanden, gewollte Rechtsfolgen bindend herbeizuführen. Transaktionen dürfen durch den Veranlasser nicht abstreitbar sein, weil beispielsweise der Geschäftsvorfall nicht gewollt ist.

2.2.4 IDW RS FAIT 2[6]

Risiken können sich innerhalb des E-Commerce insbesondere aus der fehlenden Kontrolle über den Datentransfer im Internet ergeben:

> Unzureichender Schutz vor Verfälschung (Verlust der Integrität)
> Unsichere Datenverschlüsselung (Verlust der Vertraulichkeit)
> Gefährdung der Verfügbarkeit (Verlust der Verfügbarkeit)
> Unwirksame Authentisierungsmechanismen (Verlust der Authentizität)
> Unauthorisierte Zugriffe mit Hilfsprogrammen (Verlust der Autorisierung)
> Unzureichende Protokollierung der Transaktionsdaten (Verlust der Verbindlichkeit)

Mangelnde Authentizität und Autorisierung bewirken beispielsweise, dass Geschäftsvorfälle inhaltlich unzutreffend abgebildet werden (Verletzung des Grundsatzes der Richtigkeit). Die Autorisierung soll insbesondere sicherstellen, dass keine unberechtigten bzw. keine fiktiven Geschäftsvorfälle in das System eingehen. Es ist festzulegen, wann, wie und durch wen die Autorisierung erfolgt.

Autorisierungsverfahren sind Teil der Verfahrensdokumentation und für zehn Geschäftsjahre aufbewahrungspflichtig.

Im Rahmen des durch den Anwender zu erstellenden Sicherheitskonzeptes sind auch für E-Commerce-Anwendungen Sicherungsmaßnahmen abzuleiten, die physische Sicherungsmaßnahmen und logische Zugriffskontrollen sowie Datensicherungs- und Auslagerungsverfahren umfassen.

6 IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Electronic Commerce (IDW RS FAIT 2)

2.2.5 IDW RS FAIT 3[7]

Diese IDW Stellungnahme zur Rechnungslegung konkretisiert die aus § 257 HGB resultierenden Anforderungen an die Archivierung aufbewahrungspflichtiger Unterlagen und veranschaulicht die in der IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung beim Einsatz von Informationstechnologie (IDW RS FAIT 1, Tz. 60 ff.) 2 dargestellten Aufbewahrungspflichten beim Einsatz von elektronischen Archivierungssystemen.

Technische und organisatorische Risiken aus dem Einsatz von Archivierungsverfahren können die Sicherheit und Ordnungsmäßigkeit der Rechnungslegung beeinträchtigen:

- Unzureichende organisatorische Festlegungen und Verfahrensanweisungen können die Nachvollziehbarkeit und Anwendbarkeit der Archivierungsverfahren gefährden.
- Mangelhafte Zugriffskontrollen innerhalb des Archivierungssystems ermöglichen die missbräuchliche oder unauthorisierte Einsichtnahme der archivierten Dokumente und Daten.
- Durch Veränderungen, Manipulationen oder Löschung der archivierten Daten und Dokumente wird deren Integrität, Authentizität oder Verfügbarkeit verletzt.

2.2.6 IDW PRÜFUNGSSTANDARD PS 261 (U. A. INTERNES KONTROLLSYSTEM)

Gem. IDW PS 261 werden unter einem internen Kontrollsystem die vom „Management im Unternehmen eingeführten Grundsätze, Verfahren und Maßnahmen (Regelungen) verstanden, die gerichtet sind auf die organisatorische Umsetzung der Entscheidungen des Managements

- zur Sicherung der Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit (hierzu gehört auch der Schutz des Vermögens, einschließlich der Verhinderung und Aufdeckung von Vermögensschädigungen),
- zur Ordnungsmäßigkeit und Verlässlichkeit der internen und externen Rechnungslegung sowie
- zur Einhaltung der für das Unternehmen maßgeblichen rechtlichen Vorschriften."[8]

Als organisatorische Sicherungsmaßnahmen sind z. B. definiert „laufende, automatische Einrichtungen ...". Sie umfassen fehlerverhindernde Maßnahmen, die sowohl in die Aufbau- als auch die Ablauforganisation eines Unternehmens integriert sind und ein vorgegebenes Sicherheitsniveau gewährleisten sollen (z. B. Funktionstrennung, Zugriffsbeschränkungen im IT-Bereich).[9]

Damit sind u. a. alle im Rahmen von Zugriffsberechtigungen getroffenen Maßnahmen Teil des internen Kontrollsystems und damit auch wesentlicher Bestandteil der Umsetzung der Compliance-Anforderungen durch das Management eines Unternehmens.

Die Regelungsbereiche des internen Kontrollsystems werden lt. IDW PS 261 wie folgt definiert:

7 IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren (IDW RS FAIT 3)
8 IDW PS 261, Tz. 19
9 IDW PS 261, Tz. 20

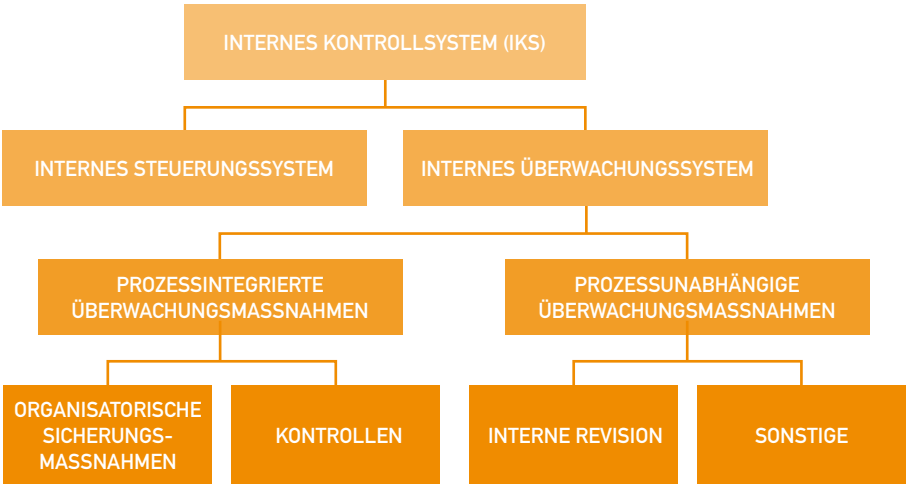

Abb. 3: Elemente des internen Kontrollsystems

Neben den o. g. organisatorischen Sicherungsmaßnahmen sind auch Kontrollen prozessintegrierte Überwachungsmaßnahmen, wie z. B. die Überprüfung der Vollständigkeit und Richtigkeit verarbeiteter Daten (u. a. Änderungen von Berechtigungen und Benutzerprofilen).

2.2.7 IDW PS 330[10]

Dieser Prüfungsstandard beschäftigt sich im Wesentlichen mit den Anforderungen an ordnungsmäßige und sichere Rechnungslegungssysteme und der Sicherstellung der Vollständigkeit, Richtigkeit, der in diesen Systemen erfassten, verarbeiteten und ausgegebenen Daten.

In diesem Zusammenhang werden u. a. folgende Risiken des IT-Einsatzes hervorgehoben:

- IT-Anwendungsrisiken (fehlende oder nicht aktuelle Verfahrensregelungen und -beschreibungen, unzureichende Zugriffsberechtigungskonzepte und Zugriffskontrollsysteme)
- IT-Geschäftsprozessrisiken (u. a. unzureichende Transparenz der Datenflüsse, unzureichende Integration der Systeme oder mangelhafte Abstimm- und Kontrollverfahren in Schnittstellen zwischen Teilprozessen mit der Gefahr, dass IT-Kontrollen wie Zugriffsrechte, Datensicherungsmaßnahmen, nur hinsichtlich der Teilprozesse, jedoch nicht hinsichtlich der Gesamtprozesse wirksam werden.)

Wesentliches Beurteilungsobjekt sind im Hinblick auf SAP Business Objects Access Control die logischen Zugriffskontrollen.

10 IDW-Prüfungsstandard zur „Abschlussprüfung bei Einsatz von Informationstechnologie" (IDW PS 330, Stand: 24. September 2002)

2 Überblick

Logische Zugriffskontrollen sind wesentliche Elemente der Datensicherheit und des Datenschutzes und Voraussetzung zur Gewährleistung der Vertraulichkeit. Die Sicherheitsanforderungen Autorisierung und Authentizität bedingen zwingend logische Zugriffskontrollen:

- Implementierung eines organisatorischen Verfahrens zu Beantragung, Genehmigung und Einrichtung von Benutzerberechtigungen in IT-Systemen
  - Berechtigungen auf Betriebssystemebene (Anmeldung gegenüber Rechnern in einem Netzwerk)
  - Rechte zur Ausführung von Transaktionen in einer IT-Anwendung.

Zugriffskontrollen sind als angemessen zu beurteilen, wenn sie geeignet sind sicherzustellen, dass die Berechtigungsverwaltung und die eingerichteten Systemrechte den Festlegungen im Sicherheitskonzept entsprechen und damit unberechtigte Zugriffe auf Daten sowie Programmabläufe zur Veränderung von Daten ausgeschlossen sind. Zudem müssen Zugriffskontrollen so ausgestaltet sein, dass sie die Identität des Benutzers eindeutig feststellen und nicht autorisierte Zugriffsversuche abgewiesen werden.

2.2.8 BUNDESDATENSCHUTZGESETZ (BDSG)

Gemäß § 9 BDSG sind zur Sicherstellung des Datenschutzes bei personenbezogenen Daten technische und organisatorische Maßnahmen erforderlich. Hinsichtlich der Zugriffskontrollen wird gefordert, dass die „die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle).

Ferner ist „zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle).

Gem. Ziff. 5 der Anlage zu § 9 BDSG ist „zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle).

Weiterhin ist lt. Ziff. 7 zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle).

Einzelheiten zum Datenschutz im SAP-Umfeld können Sie im DSAG-Datenschutzleitfaden nachlesen.[11]

11 Leitfaden Datenschutz SAP ERP 6.0 (Stand 20. September 2009), Download über DSAG*Net*

2.2.9 BILANZRECHTSMODERNISIERUNGSGESETZ (BILMOG)

Die neuen Bilanzierungsregelungen sind verpflichtend für Geschäftsjahre ab dem 01.01.2010 anzuwenden. Sie sind anzuwenden durch kapitalmarktorientierte (Konzern-)Unternehmen im Sinne des § 264d HGB n.F.

Sie können freiwillig bereits für den Abschluss 2009 angewendet werden, jedoch nur als Gesamtheit.

Neben einer Vielzahl neuer HGB-Regelungen zur Bilanzierung und Bewertung innerhalb der Rechnungslegung eines Unternehmens werden mit dem BilMoG auch wesentliche Vorgaben aus EU-Recht (8. EU-Richtlinie) umgesetzt.

Auch das interne Kontrollsystem und das Risikomanagementsystem rücken durch BilMoG stärker in den Blickpunkt von Vorständen und Aufsichtsräten und insofern stehen in den Unternehmen die entsprechenden aufbau- und ablauforganisatorischen Fragestellungen (auch zu Themen wie Funktionstrennung und sichere Berechtigungskonzepte und -systeme) im Fokus.

2.2.9.1 LAGEBERICHT (§§ 289, 315 HGB N.F.)

Im Lagebericht sind die wesentlichen Merkmale des rechnungslegungsbezogenen internen (IKS) Kontroll- und Risikomanagementsystems (RMS) zu beschreiben.

2.2.9.2 PFLICHTEN DES AUFSICHTSRATES

Der Aufsichtsrat hat die Verpflichtung zur Überwachung folgender Bereiche:

- Rechnungslegungsprozess
- internes Kontrollsystem (IKS)
- Risikomanagementsystem (RMS)
- internes Revisionssystem (Interne Revision)

Diese Überwachungspflichten werden dazu führen, dass sich Aufsichtsräte entsprechende Berichtswege mit wirksamen Überwachungsstrukturen einrichten und dies auch Auswirkungen auf effiziente und effektive Kontrollen insbesondere in solchen Unternehmensbereichen haben wird, die Daten zur Finanzberichterstattung beisteuern (insbesondere Rechnungs- und Finanzwesen, Personalwesen, Materialwirtschaft, Produktion, Vertrieb).

2.2.9.3 HANDLUNGSFELDER FÜR DEN VORSTAND

Der Vorstand trägt die Verantwortung für Einrichtung, angemessene Ausgestaltung und den Nachweis der Wirksamkeit u. a. des IKS und des RMS. Dies erfordert eine Bestandsaufnahme der vorhandenen Instrumente zum IKS/RMS:

- Systematische Aufnahme vorhandener wesentlicher Instrumente (u. a. Softwareunterstützung) und deren Verzahnung
- Analyse der Angemessenheit, insbesondere der „Nachweisfähigkeit"
- Maßnahmen zur Verbesserung des IKS/RMS

Darüber hinaus ist ein Nachweis der Wirksamkeit von IKS/RMS zu führen:

- Externe Zertifizierung der internen Revision (IR)
- Etablierung eines Regelprozesses zum Monitoring der Wirksamkeit (Self Assessment, Prüfungsplanung der IR, Prüfung durch Externe, Konsolidierung der Überwachungsergebnisse)
- Initiierung von Verbesserungsmaßnahmen bei festgestellten Schwächen
- Berichterstattung an den Aufsichtsrat

Durch eine möglichst integrierte Steuerung und Überwachung der Risiken und Kontrollen innerhalb für das Unternehmen besonders kritischer Geschäftsabläufe mit Hilfe von Access Control, Process Control und Risk Management kann ein effektives und effizientes Management der Risiken und Kontrollen erreicht werden. Dies ist eine wesentliche Voraussetzung für die praktische Umsetzung der BilMoG-Anforderungen an Vorstand und Aufsichtsrat im Rahmen der Überwachung des internen Kontrollsystems und internen Risikomanagementsystems.

Eine der wesentlichen Maßnahmen zur Verbesserung des internen Kontrollsystems ist die Beseitigung von Risiken aufgrund von fehlender oder unzureichender Funktionstrennung beim Daten- und Programmzugriff (Stichwort: Segregation of Duties) und damit dem unkontrollierten, umfassenden Zugriff auf wesentliche IT-Systeme zur Abwicklung wesentlicher finanzkritischer Geschäftsprozesse. Eine unter IKS-Gesichtspunkten wirksame Funktionstrennung in der Ablauforganisation eines Unternehmens lässt sich durch ein entsprechendes Benutzerkonzept mit auf den Arbeitsplatz zugeschnittenen Benutzerberechtigungen erreichen. Access Control ist das hierfür genutzte Instrument innerhalb der SAP- und Non-SAP-Welt.

Der geschilderte Handlungsbedarf gilt übrigens nicht nur für große börsennotierte Unternehmen, sondern ist auch für kapitalmarktorientierte Mittelstandsunternehmen verpflichtend, die ein funktionierendes internes Kontrollsystem sicherstellen wollen.

2.2.10 BASEL II

Unter dem Begriff Basel II werden die Eigenkapitalvorschriften für Kreditinstitute zusammengefasst, die vom Baseler Ausschuss für Bankenaufsicht in den letzten Jahren vorgeschlagen wurden. Auf der Grundlage der EU-Richtlinien 2006/48/EG und 2006/49/EG erfolgte in Deutschland die Umsetzung mit Wirkung ab 1. Januar 2007 durch das Kreditwesengesetz, die Solvabilitätsverordnung und die MaRisk (Mindestanforderungen an das Risikomanagement).

Die Rahmenvereinbarung von Basel II basiert auf den drei „Säulen“

- Mindestkapitalvorschriften (Berechnung einer angemessenen Eigenkapitalausstattung)
- aufsichtsrechtliche Überprüfungsverfahren
- Marktdisziplin (höheres Maß an Transparenz bei der Offenlegung von Informationen der Bank. Sie verlangt die Offenlegung quantitativer und qualitativer Aspekte der von der Bank verwendeten Methoden für das Management ihrer Eigenkapitalanforderungen).

Kreditinstitute müssen zu jedem einzelnen Risikobereich (z. B. Kredit-, Markt-, operationelles Risiko, Zinsänderungsrisiko des Anlagebuchs und Beteiligungspositionen) die internen Ziele und Grundsätze des Risikomanagements beschreiben. Dazu gehören:

> Strategien und Prozesse
> Struktur und Organisation der relevanten Risikomanagement-Funktion
> Art und Umfang der Risikomeldungen und/oder -messsysteme
> Grundsätze der Absicherung und/oder Minderung von Risiken sowie Strategien und Prozesse zur Überwachung der fortgesetzten Effektivität dieser Absicherungen/Risikominderungen

Innerhalb der Mindestanforderungen an das Risikomanagement (MaRisk) ist hinsichtlich der internen Kontrollverfahren festgelegt, dass Adressausfallrisiken, Marktpreisrisiken, Zinsänderungsrisiken, Liquiditätsrisiken und operationelle Risiken anhand wirksamer Risikosteuerungs- und Controllingprozesse zu überwachen sind und darüber zu berichten ist.

2.2.11 SARBANES-OXLEY ACT (SOX)

SOX ist ein Oberbegriff für gesetzliche Anforderungen an interne Kontrollen der Finanzberichterstattung und betrifft alle an US-Börsen gelisteten Unternehmen. Insofern fallen auch deutsche Unternehmen unter dieses US-Gesetz von 2002, sofern ihre Wertpapiere an einer US-Börse gelistet sind. Unternehmen müssen gem. SOX nachweisen, dass wirksame interne Kontrollen (unternehmensweite Kontrollen und Geschäftsprozesskontrollen) zur Sicherstellung einer zutreffenden und vertrauenswürdigen Finanzberichterstattung eingerichtet sind. Dieser Nachweis ist durch das Management gegenüber der amerikanischen Börsenaufsicht (SEC) zu erbringen und durch einen Wirtschaftsprüfer zu bestätigen. Die mit der Überwachung der Einhaltung von SOX befasste amerikanische Aufsichtsbehörde ist die PCAOB (Public Company Accounting Oversight Board). Ein von der SEC und dem PCAOB empfohlener Standard zur Einrichtung und Überwachung interner Kontrollen ist das sog. COSO-Framework[12], das detaillierte Kontrollstrukturen und Umsetzungsvorschläge enthält und in Deutschland in der Regel auch Maßstab für die Umsetzung der US-amerikanischen Anforderungen ist. Zur Umsetzung der SOX-Anforderungen auf Kontrollen im IT-Bereich hat sich das CoBiT-Rahmenwerk als hilfreich erwiesen. Eine entsprechende Gegenüberstellung von COSO-Regelungen zu den Kontrollempfehlungen von CoBiT wurde vom amerikanischen IT Governance Institute (ITGI) mit dem Leitfaden IT Control Objectives for Sarbanes-Oxley[13] erstellt.

2.2.12 NORMEN (DIN ISO/IEC)

2.2.12.1 ISO/IEC 27001

Die ISO/IEC 27001:2005 wurde aus dem britischen Standard BS 7799-2:2002 entwickelt und als internationale Norm erstmals am 15. Oktober 2005 veröffentlicht. Mit Ausgabe 9.2008 liegt die Norm auch als DIN-Norm DIN ISO/IEC 27001 vor.

12 COSO (Committee of Sponsoring Organizations of the Treadway Commission). Entsprechende Informationen und Detailbeschreibungen des Internal Control Framework nach COSO sind u. a. über folgenden Link verfügbar: http://www.coso.org/guidance.htm.
13 IT Control Objectives for Sarbanes-Oxley. The Role of IT in the Design and Implementation of Internal Control over Financial Reporting, 2nd edition, Sept. 2006: http://www.itgi.org

Der ISO-Standard 27001 „Information technology – Security techniques – Information security management systems requirements specification" ist der erste internationale Standard zum Informationssicherheits-management, der auch eine Zertifizierung ermöglicht. ISO 27001 gibt auf ca. 10 Seiten allgemeine Empfehlungen. In einem normativen Anhang wird auf die Controls aus ISO/IEC 27002 verwiesen. Die Leser erhalten aber keine Hilfe für die praktische Umsetzung.

2.2.12.2 ISO 27002 (VORHER ISO 17799)

Das Ziel von ISO/IEC ISO 27002 „Information technology – Code of practice for information security management" ist es, ein Rahmenwerk für das Informationssicherheitsmanagement zu definieren. ISO 27002 befasst sich daher hauptsächlich mit den erforderlichen Schritten, um ein funktionierendes Informationssicherheitsmanagement aufzubauen und in der Organisation zu verankern. Die erforderlichen Informationssicherheitsmaßnahmen werden kurz auf den ca. 100 Seiten des ISO-Standard ISO/IEC 27002 angerissen. Die Empfehlungen sind auf Management-Ebene und enthalten kaum konkrete technische Hinweise. Ihre Umsetzung ist eine von vielen Möglichkeiten, die Anforderungen des ISO-Standards 27001 zu erfüllen.

2.2.12.3 ISO 27005

Dieser ISO-Standard „Information security risk management" enthält Rahmenempfehlungen zum Risikomanagement für Informationssicherheit. Unter anderem unterstützt er bei der Umsetzung der Anforderungen aus ISO/IEC 27001. Hierbei wird allerdings keine spezifische Methode für das Risiko-management vorgegeben. ISO/IEC 27005 löst den bisherigen Standard ISO 13335-2 ab. Dieser Standard ISO 13335 „Management of information and communications technology security, Part 2: Techniques for information security risk management" gab Anleitungen zum Management von Informationssicherheit.

2.2.12.4 WEITERE STANDARDS DER REIHE ISO 2700X

Die Normenreihe ISO 2700x wird voraussichtlich langfristig aus den ISO-Standards 27000–27019 und 27030–27044 bestehen. Alle Standards dieser Reihe behandeln verschiedene Aspekte des Sicherheits-managements und beziehen sich auf die Anforderungen der ISO 27001. Die weiteren Standards sollen zum besseren Verständnis und zur praktischen Anwendbarkeit der ISO 27001 beitragen. Diese beschäftigen sich beispielsweise mit der praktischen Umsetzung der ISO 27001, also der Messbarkeit von Risiken oder mit Methoden zum Risikomanagement.

2.2.12.5 ZERTIFIZIERUNG NACH ISO 27001 AUF BASIS VON IT-GRUNDSCHUTZ

Das Bundesamt für Sicherheit in der Informationstechnik bietet seit Januar 2006 die ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz an. Hierüber kann nachgewiesen werden, dass in einem Informationsverbund die wesentlichen Anforderungen ISO 27001 unter Anwendung der IT-Grundschutz Vorgehensweise (BSI-Standard 100-2) und gegebenenfalls einer ergänzenden Risikoanalyse (BSI-Standard 100-3) umgesetzt wurden.

Nach Umsetzung aller für die Zertifizierung relevanten Maßnahmen kann die Institution einen beim BSI lizenzierten ISO 27001-Auditor beauftragen, den Informationsverbund gemäß dem Prüfschema des BSI zu überprüfen. Die Ergebnisse dieser unabhängigen Prüfung werden in einem Auditreport festgehalten. Ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz kann zusammen mit der Einreichung des Auditre-ports beim BSI beantragt werden. Nach Prüfung des Reportes durch Experten des BSI erteilt die Zertifizie-rungsstelle das Zertifikat, das ebenso wie die Auditor-Testate vom BSI veröffentlicht wird. Alle zertifizie-rungsrelevanten Informationen wie das Zertifizierungsschema und die Namen der lizenzierten Auditoren sind öffentlich verfügbar und können unter www.bsi.bund.de/gshb/zert eingesehen werden.

3 SAP BusinessObjects Access Control 5.3

3.1 ZIELMARKT

In Kapitel 2.2 ist ausführlich von Gesetzen, Vorschriften und Verordnungen die Rede, die sich in erster Linie an börsennotierte größere Unternehmen sowie größere GmbHs richten. Der Ursprung der Compliance-Idee und des Risikomanagements kommt aus den Staaten; in Europa wurde diese Idee in einer etwas gemilderten Version (8. EU-Richtlinie)[14] in nationale Gesetze umgesetzt. Welche Unternehmen ab welcher Größe sich damit in welcher Form beschäftigen müssen, kann nicht eindeutig zugeordnet werden – jedoch gibt es schlüssige Kriterien.

3.1.1 MITTELSTAND

Mittelständische Unternehmen - mit eigenverantwortlicher IT-Infrastruktur - sind oftmals gesellschaftlich vernetzt und somit an die Vorschriften der Mutter oder der zentralen Revision gebunden; diese hat i.d.R. bereits unternehmensweite Governance-Richtlinien erstellt. Hier stellt sich nicht die Frage „ob", sondern eher „wann" die Umsetzung und in welcher Form durchzuführen ist.

Mittelständische Unternehmen sind oftmals Zulieferer für Konzerne oder deren Vertriebspartner. Diese Konzerne achten verstärkt darauf, dass auch die Partner ihre Regelwerke akzeptieren und – vielleicht nicht in vollem Umfang – implementieren und einhalten.

Fast jedes größere mittelständische Unternehmen ist international aufgestellt und definiert für die Zentrale wie auch für die nationalen Gesellschaften ein internes Kontrollsystem und ein Risikomanagement, um das Zusammenwirken auf eine einheitliche, nachvollziehbare Geschäftsgrundlage zu stellen.

Der globale Wettbewerb zwingt zur Spezialisierung und damit – zunehmend als Wettbewerbsvorteil – auch zu einer Zertifizierung der Produkte und Abläufe; sensible Produktionsverfahren und geschäftskritische Rezepturen sind in mittelständischen Unternehmen genauso verbreitet wie in Großunternehmen und existenziell zu schützen. Eine Zertifizierung ohne sichere IT-Geschäftsprozesse und ausreichendem Datenschutz ist nicht mehr zu erlangen und hierzu gehören als wesentlicher Bestandteil ein risikofreies Rechtewesen und ein zentrales Benutzermanagement mit Transparenz und Nachvollziehbarkeit. Prüfungsgesellschaften sind verpflichtet, die IT-Abläufe mit in ihre Prüfverfahren aufzunehmen und zu bewerten. Da der Mittelstand sich in nicht unerheblichem Maße über Kredite finanziert, ist gelebte IT-Sicherheit und damit ein gutes Audit-Ergebnis mit ein Ausschlag für die Kreditvergabe der Banken und Investoren. Die Liste lässt sich beliebig fortsetzen; es gibt viele Gründe für die Einführung von SAP BusinessObjects GRC bei mittelständischen Unternehmen.

Aus der Beratungserfahrung kann man ableiten, dass heute bereits Unternehmen ab 300-400 ERP-User sich mit dem Gedanken beschäftigen, ein IT-gestütztes Risikomanagement einzuführen – und dies bei überschaubarem Aufwand und Kosten. Meistens beginnt dies mit der Analyse der Berechtigungen; die Analyse ist durch die Implementierung von Risk Analysis and Remediation aus der SAP BusinessObjects GRC-Produktlinie eine der Möglichkeiten, einfach den Status quo zu ermitteln. Sind die Berechtigungen anhand der Ergebnisse von Risk Analysis and Remediation (RAR) sicher überarbeitet, bietet es sich an, diese Funktionalität auch weiterhin zu nutzen, um die Veränderungen IT-gestützt kontrollieren zu können. Ergänzt mit einem Notfall-User-Konzept (Superuser Privilege Management) könnte so für mittelständische Unternehmen ein einfacher und bezahlbarer Weg als sinnvolle erste Ausbaustufe von GRC beschritten werden.

14 RICHTLINIE 2006/43/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 17. Mai 2006

3.1.2 GROSSUNTERNEHMEN/KONZERNE

Eine wirksame und effiziente Corporate Governance zur Sicherstellung einer verantwortungsbewussten, transparenten und risikominimierenden Unternehmensführung steht heutzutage ganz oben auf der Prioritätenliste der börsennotierten deutschen Unternehmen. Danach hat der Vorstand „für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung und Einhaltung durch die Konzernunternehmen hin (Compliance)".[15] Die operative Umsetzung der Corporate Governance erfolgt durch ein unternehmensweites Compliance Management. Compliance-Verstöße können Schadensersatzforderungen, Geldbußen, Strafverfahren und bleibende Imageschäden nach sich ziehen.

Mit der Einführung des Bilanzrechtsmodernisierungsgesetzes (BilMoG) wurden insbesondere Prüfungsausschüsse, beziehungsweise Aufsichtsräte, dazu verpflichtet, Compliance Elemente wie internes Kontrollsystem, internes Risikomanagementsystem sowie das interne Revisionssystem zu überwachen. Diese Regelung verstärkt die bisher schon bestehenden Empfehlungen des Deutschen Corporate Governance Kodex, wonach der Aufsichtsrat einen Prüfungsausschuss (Audit Committee) einrichten soll, der sich u. a. mit Fragen des Risikomanagements und der Compliance beschäftigen soll.[16]

Ein wesentlicher Schutz- und Kontrollbereich im Rahmen des Compliance Managements ist der Zugriff auf Programme und Daten innerhalb der Informationstechnologie (IT). Aufgrund der Komplexität und Vielfalt der eingesetzten Programme und verwendeten Datenbestände sind unterstützende Tools mit präventiven und detektivischen Schutzmechanismen erforderlich. Ideal sind unternehmensweite, integrierte Lösungen mit einem breiten Anwendungsspektrum. Gerade in Großunternehmen und Konzernen mit mehreren tausend SAP Anwendern ist ein wirksames, pro-aktives Identitäts- und Zugriffsmanagement insbesondere auch zur Sicherstellung notwendiger Funktionstrennungsprinzipien nur mit Softwareunterstützung umzusetzen. Insofern ist zumindest für die SAP-Anwendungslandschaft, wie hauptsächlich der Business Suite, die Lösung Access Control ein wesentlicher Grundbaustein innerhalb eines unternehmensweiten Compliance-Konzeptes für den Bereich Identity & Access Management eines Konzerns.

Damit die oftmals erforderlichen risikoeindämmenden Kontrollen im Berechtigungsumfeld, wie z. B. der Abgleich von angelegten Kontenstammsätzen von Zuliefern mit kritischen Kontendaten, auch Bestandteil des internen Kontrollsystems werden, empfiehlt es sich, zudem diese Kontrollen in die Lösung SAP BusinessObjects Process Control zu übernehmen. Dies kann per elektronischem Interface oder aber auch einmalig manuell erfolgen. Für die Identitätssteuerung (also Registrierung, Abteilungswechsel etc.) ist zudem eine Integration der Steuerungs-Workflows mit einem eher technisch orientierten Identity-Management-Produkt wie z. B. SAP NetWeaver Identity Management ratsam.

15 Deutscher Corporate Governance Kodex, Abschnitt 4.1.3 in der Fassung vom 18. Juni 2009
16 Deutscher Corporate Governance Kodex, Abschnitt 5.3.2 in der Fassung vom 18. Juni 2009

3.2 MOTIVATION ZUM EINSATZ VON ACCESS CONTROL

Die Notwendigkeit, SAP BusinessObjects Access Control einzuführen, ist in aller Regel getrieben von der Notwendigkeit eines effektiven und effizienten Identitäts- und Zugriffsmanagements in Verbindung mit der Umsetzung der vorgenannten Compliance-Anforderungen.

Der Einsatz von SAP BusinessObjects Access Control lässt sich in verschiedene Kategorien unterteilen.

1. Einige Unternehmen setzen SAP BusinessObjects Access Control ein, weil derzeit kein Berechtigungskonzept vorhanden ist und das Verständnis für die Notwendigkeit, auch von der Fachseite, fehlt. Aufgrund einer ersten Risikoanalyse mit dem von SAP ausgelieferten Regelwerk können den Fachbereichen und dem verantwortlichen Management die vorhandenen Risiken transparent gemacht werden. Die Transparenz dieser Risiken kann zu verschiedensten Einführungsszenarien führen.

   Eine Einführung des Superuser Privilege Management kann schon erste Beanstandungen hinsichtlich der Profile SAP_ALL und SAP_NEW hinfällig machen. Auch weitere Anforderungen an andere Superuser für die Fachbereiche und die IT können damit abgedeckt werden.

   In dieser Kategorie der Implementierung von SAP BusinessObjects Access Control ist die Risikoanalyse, wie so oft, der zentrale Baustein, d. h., das Unternehmen wird sich zur weiteren Sicherstellung der Compliance dem Ausarbeiten des Regelwerkes widmen. Nach Erstellung/Ausprägung des Regelwerkes erfolgt die Einrichtung der Workflows für das Benutzerantragsverfahren mit integrierter Risikoanalyse, Beantragung von Superuser-Berechtigungen usw.
   Als letzte Komponente wird man sich dann dem Enterprise Role Management zuwenden.

2. Bei anderen Unternehmen sind eingeführte Prozesse für die Themen Benutzer- und Rollenverwaltung vorhanden. Die Lücken in diesen Unternehmen offenbaren sich in der geringen Überprüfbarkeit der Funktionstrennungsrisiken. Eventuell kommt noch erschwerend eine dezentrale Benutzer- und Rollenverwaltung hinzu.

   In diesen Fällen sind auch die Benutzeranträge dezentral (im schlechtesten Fall in Papierform) abgelegt. Eine Nachvollziehbarkeit, welche Benutzeränderung aufgrund welchen Antrages durchgeführt wurde, wird damit erheblich erschwert.

   Um diesen Missstand zu beheben, kann hier das Einführungsszenario so aussehen, dass zuerst das Benutzerantragsverfahren ohne Risikoanalyse eingeführt wird. Erst in einem weiteren Schritt kommen die Komponenten SPM, RAR und ERM hinzu.

3. Eine andere Kategorie von Unternehmen hat ausgearbeitete Berechtigungskonzepte und gelebte Prozesse implementiert. Lediglich die Dokumentation für das IKS und/oder die Wirtschaftsprüfer ist verbesserungswürdig.

   In diesen Fällen erlaubt das Reporting von SAP BusinessObjects Access Control den entsprechenden Nachweis und somit die Sicherstellung der Compliance.

   Die Implementierung von SAP BusinessObjects Access Control erfolgt hier oft in der Reihenfolge RAR und SPM, CUP und ERM.

4. Vorhandene Prozesse und Dokumentationen, aber keine systemübergreifenden Risikoanalysen, schon gar nicht mit Non-SAP-Systemen, bilden eine weitere Kategorie.

   In dieser Kategorie sind die Implementierungsaufwände sowohl personell als auch monetär am höchsten. Je nach Implementierungsszenario sind Real Time Agents (RTA) zu erstellen, das unternehmensindividuelle Regelwerk – auch für die Non-SAP-Systeme – anzupassen und dabei auch deren Berechtigungssystem und -konzept zu berücksichtigen.

   Im Rahmen der Einführung eines Benutzerantragsverfahrens für die Non-SAP-Systeme mit integrierter Risikoanalyse sollte über den Einsatz eines IdM (z. B. SAP NetWeaver Identity Management) nachgedacht werden.

   Die Funktionalitäten des Superuser Privilege Management stehen auf Non-SAP-Systemen nicht zur Verfügung.

Weitere unterschiedliche Ausprägungen sind denkbar, würden aber den Rahmen dieses Leitfadens sprengen.

Zusammenfassend lässt sich feststellen, dass sich die Verwendung von SAP BusinessObjects Access Control in den meisten Fällen von einem reaktiven Ansatz – wenn nur die Risikoanalyse zum Einsatz kommt – zu einem präventiven Ansatz mit allen Komponenten wandelt.

3.3 RAHMENBEDINGUNGEN/ERFOLGSFAKTOREN

Die im Folgenden dargestellten Rahmenbedingungen und Erfolgsfaktoren für ein Access-Control-Projekt basieren auf den Erfahrungen durchgeführter Implementierungsprojekte bei Unternehmen aus unterschiedlichen Branchen und unterschiedlicher Unternehmensgrößen. Dabei hat sich gezeigt, dass Projekte dieser Art als übergreifend anzusehen sind und nicht von der IT alleine durchgeführt werden können. Aus diesem Grund ist es notwendig, alle Interessensgruppen frühzeitig einzubinden (z. B.: Fachbereichsverantwortliche, IT, Internal/External Audit).

Für eine erfolgreiche Projektdurchführung muss das Top-Management die Verantwortung tragen und das Projekt bei notwendigen Entscheidungen begleiten.
Es hat sich als vorteilhaft erwiesen, frühzeitig die Einführungsstrategie festzulegen (siehe Kap. 3.4).

Ein Einführungsprojekt setzt sich grundsätzlich aus unterschiedlichen Projektbeteiligten zusammen. Das Projektteam besteht dabei in der Regel aus Vertretern des Fachbereiches und aus Vertretern des IT-Bereiches. Sofern es sich aber um Projekte im Umfeld von Mitarbeiter-Berechtigungen und dem zugrunde liegenden Change Management Prozess handelt, reicht diese einfache Organisationsstruktur innerhalb eines Projektes nicht aus.

In diesem Zusammenhang werden Fragestellungen zum Datenschutz, zu Möglichkeiten einer Mitarbeiterüberwachung, den regulatorischen Anforderungen und Verantwortlichkeiten aufgeworfen, die nur durch eine intensive Einbeziehung einzelner Gruppen bereits in einer frühen Projektphase beantwortet werden können. Die Bedeutung und Erläuterung dieser These ergibt sich aus den folgenden Beschreibungen der einzelnen Aufgabengebiete.

3.3.1 SAP-BASISBETREUUNG

Die Rolle und Aufgabe der SAP-Basisbetreuung im Umfeld von Berechtigungen im SAP-Umfeld ist ganz vielschichtiger Art. Sie differiert selbst zwischen einzelnen Unternehmen, je nach Größe und interner Organisation. Die SAP-Basisbetreuung kann durch eine eigene IT-Service-Einheit oder durch eine externe IT-Service-Organisation durchgeführt werden. Ihre Aufgabe sollte dagegen aber prinzipiell ähnlich sein. Die SAP-Basisbetreuung ist neben vielen weiteren Aufgaben im Umfeld der SAP-Berechtigungen in der Regel zuständig für folgende Aufgaben:

- Neuanlage von Usern im SAP-System
- Verwaltung von Benutzergruppen
- Zurücksetzen von Passwörtern
- Sperren und Entsperren von Benutzern
- häufig auch: Zuweisen und Erweitern von Berechtigungsrollen

Durch Einführung von Access Control ändert sich das Aufgabengebiet der SAP-Basisbetreuung. Bislang manuell durchgeführte Arbeitsschritte werden nun automatisiert und bedürfen keines manuellen Eingriffs mehr.

3.3.2 SAP BERECHTIGUNGSADMINISTRATOREN

In größeren Organisationen wird bzw. sollte die Benutzer- und Berechtigungsverwaltung getrennt werden (Vier-Augen-Prinzip). Diese Administratoren sind dabei für Erstellung, Anpassung und Zuweisung der Berechtigungsrollen zuständig. Sie arbeiten eng mit den jeweiligen Fachbereichen zusammen und verstehen die Rollen auch fachinhaltlich, um diese entsprechend dem Aufgabengebiet des Mitarbeiters zuweisen zu können.

3.3.3 ORGANISATIONSABTEILUNG

Eine Organisationsabteilung ist oft bei größeren Unternehmen zu finden. Diese unterstützt u. a. bei der Erstellung von Berechtigungsvergabeprozessen. Diese Prozesse und deren Dokumentationen sind notwendig für einen geordneten und nachvollziehbaren Ablauf der Vergabe von Berechtigungen.

3.3.4 SCHLÜSSELPERSONEN AUS DEN FACHBEREICHEN

Die Schlüsselpersonen aus den Fachbereichen spielen eine vermittelnde Rolle zwischen dem Endanwender und den Berechtigungsadministratoren. Über sie wird oft die Berechtigungsanforderung der Endanwender kanalisiert und spezifiziert. Sie unterstützen bei der Definition von Rolleninhalten und Arbeitsplatzbeschreibungen und können einschätzen, ob ein Anwender eine Berechtigung für sein Aufgabengebiet benötigt. Sie haben zudem den Überblick und können die Relevanz der Zugriffsrisiken einschätzen.

3.3.5 ENDANWENDER

Endanwender haben im Wesentlichen Testaufgaben wahrzunehmen, da der Fachbereich innerhalb des Projektes durch die Schlüsselpersonen vertreten ist. Insbesondere sollten sie mitwirken beim Usability Test.

3.3.6 WIRTSCHAFTSPRÜFER

Eine wesentliche Aufgabe des Wirtschaftsprüfers im Rahmen der Prüfung des Jahresabschlusses ist die Einschätzung der sog. Kontrollrisiken, d. h. die Beurteilung der Wirksamkeit des internen Kontrollsystems hinsichtlich der durchzuführenden Prüfungshandlungen. Die Einhaltung von Funktionstrennungsprinzipien u. a. durch ein wirksames Benutzerberechtigungskonzept und dessen organisatorische Umsetzung ist dabei ein wesentlicher Prüfungsbereich. Aufgrund seiner profunden Kenntnisse des internen Kontroll- und Risikomanagementsystems des geprüften Unternehmens und seiner skizzierten Prüfungspflichten sollte der Wirtschaftsprüfer bereits frühzeitig in entsprechende Einführungsprojekte von Access Control einbezogen werden. Projektbegleitend kann er wesentliche Hinweise zur Sicherstellung eines ordnungsmäßigen und sicheren Benutzermanagements geben und damit einen wertvollen Beitrag auch im Sinne einer projektbegleitenden Qualitätssicherung leisen.

Eine frühzeitige Einbeziehung vermeidet auch nicht zielführende Fehlentwicklungen bei der Konzeption und dem Go-live von Access Control, die dann möglicherweise auch dazu führen können, dass zusätzliche Prüfungshandlungen im Rahmen einer Prüfung des Jahresabschlusses erforderlich werden und unter Umständen die Wirksamkeit des internen Kontrollsystems nur mit Einschränkungen bestätigt werden kann.

3.3.7 INTERNE REVISION

Die interne Revision ist Teil des internen Kontrollsystems einer Organisation, ist unabhängig und der obersten Leitung unterstellt. Das Aufgabengebiet besteht vor allem aus organisationsinternen Prüfungen und unterstützt mit Lösungsvorschlägen. So kann die interne Revision dafür zuständig sein, Empfehlungen für ein neues Berechtigungskonzept abzugeben, für den Produktiveinsatz freizugeben und auch entsprechende Prüfungen der ordnungsgemäßen Umsetzung vorzunehmen.

3.3.8 BETRIEBSRAT

Der Betriebsrat hat nach § 87 Abs. 1 Nr. 6 BetrVG ein Mitbestimmungsrecht, wenn es um die Einführung und Anwendung von Einrichtungen geht, die das Verhalten der Arbeitnehmer überwachen können. Grundsätzlich betrifft dies z. B. den Einsatz des Superuser Privilege Management (SPM; vormals Firefighter) und dessen Protokoll-Datei. Es empfiehlt sich, den Betriebsrat frühzeitig als vertrauensbildende Maßnahme über das Projekt zu informieren und in die Entscheidungsprozesse zur Produktivsetzung einzubeziehen.

3.3.9 TOP-MANAGEMENT

Das Top-Management als Projekt-Owner muss die notwendigen Entscheidungen zeitnah herbeiführen und die Umsetzung unterstützen. Dabei werden auch organisatorische Veränderungen entstehen, für die die Fachbereiche motiviert werden müssen.

3.4 EINFÜHRUNGSMANAGEMENT (ROLLOUT INKL. USERTRAINING)

Gemäß der SAP-ASAP-Methodik („Accelerated SAP"), die für die Implementierung und den Rollout von SAP-ERP-Anwendungen vor Jahren schon entwickelt wurde, lässt sich ein SAP-Einführungsprojekt in folgende Hauptphasen einteilen (siehe auch „GRC Implementation Roadmap" verfügbar auf dem SAP Service-Marketplace: http://service.sap.com/roadmaps):

- Projektvorbereitung („Strategie & Planung"): In dieser ersten Phase legen die Entscheidungsträger klare Projektziele und eine effiziente Vorgehensweise zur Entscheidungsfindung fest. Es wird das genaue Projektteam und dessen Kommunikation mit den Fachbereichen festgelegt. Speziell bei einem Einführungsprojekt für SAP BusinessObjects Access Control ist die Kommunikationsstrategie mit den Verantwortlichen aus den Fachbereichen für den Gesamtprojekterfolg von großer Bedeutung. Zudem wird der Projektplan in Abhängigkeit von einer ersten Analyse des bestehenden Berechtigungskonzeptes für SAP, des Systemumfangs, des bestehenden Identity Lifecycle Managements und anderer Abhängigkeitsfaktoren festgelegt.

- Sollkonzeption („Business Blueprint und Design"): In dieser Phase werden die in der Strategiephase festgelegten High-Level-Prinzipien, wie z. B. die technische Architektur für SAP BusinessObjects Access Control, das eventuell notwendige Reengineering des bestehenden SAP-Rollenkonzeptes und des Designs des Risikomanagements mit den notwendigen Provisionierungsworkflows, der Festlegung der Zugriffsrisiken (also Segregation-of-Duties-Konflikte und kritische Transaktionen) in ein Feindesign überführt. Zudem wird auch ein detailliertes Rollendesign für die Steuerung von SAP BusinessObjects Access Control selbst festgelegt.

- Realisierung („Implementierung"): Hauptziel dieser Phase ist die eigentliche Konfiguration des SAP BusinessObjects Access Control Systems (Customizing), um zu einer integrierten und dokumentierten, die Risikomanagement und legale Anforderungen erfüllende Lösung zu gelangen.

- Produktionsvorbereitung („Rollout"): In der Phase Produktionsvorbereitung erfolgt die endgültige Vorbereitung des Systems auf die Produktionsphase. Dazu gehören beispielsweise intensive Tests der eventuell überarbeiteten Berechtigungseinstellungen und der Provisionierungs-Workflows sowie intensive Schulung der Fachbereiche.

- Produktivstart („Support"): Nach dem Abschluss des sog. Go-live, bei dem das System in den Produktivzustand gesetzt wird, konzentriert sich das Projektteam auf die Unterstützung der Benutzer, deren Schulung möglicherweise noch nicht abgeschlossen ist. Es ist gleichermaßen notwendig, Verfahren und Maßstäbe zu entwickeln, anhand derer das ERP-System regelmäßig betriebsbegleitend überprüft wird. Es wird zudem ein Know-how-System mit aufgetretenen Fehlern und entsprechenden Lösungen aufgebaut und an den Help Desk für den First Level Support und auch Second Level Support übergeben.

Die ASAP-Methodik sollte entsprechend auch für SAP BusinessObjects Access Control angewendet werden, wodurch sich die folgenden Hauptarbeitspakete ergeben:

3.4.1 PHASE: PROJEKTVORBEREITUNG („STRATEGIE & PLANUNG“):

> Projektplan Entwurf: Wie für jedes andere Projekt auch, muss in der Strategie & Planungsphase ein detaillierter Projektplan inkl. des genauen Projektteams (Zusammensetzung mit Kundenmitarbeitern, Arbeitsergebnisse, Zeitplan und Erwartungshorizont) festgelegt werden. Dann sollte die genaue Einbeziehung der Fachbereiche in das Projekt wie Kommunikation und Unterstützung festgelegt werden. Zunächst eignet sich ein Draft als Projektplan, da speziell die Themen Überarbeitung des SAP-Rollenkonzeptes oder auch die Festlegung der Risikomatrix meist noch nicht genau bekannt sind und zunächst in der Strategie festgelegt werden.

> Projekt-Kick-off: Mit dem Kernprojektteam muss ein erstes initiales Kick-off-Meeting durchgeführt werden, in dem nochmals die genauen Ziele des Projektes, der vorgesehene Zeitplan, die zu erarbeitenden Arbeitsergebnisse und das Team selbst nochmals vorgestellt werden.

> Analyse des bestehenden SAP-Berechtigungskonzeptes: Mit Hilfe einer sorgfältigen Analyse muss der derzeitige Status quo des SAP-Rollenkonzeptes, inkl. Informationseigentümerprinzip (Rolleneigner), Rollenstruktur, Vererbung, existierendes Beantragungswesen, bestehende Risikomatrix und bestehende Risikomanagementprozesse evaluiert werden. Ziel ist es hierbei festzustellen, inwieweit ein „Reifegrad“ für die Einführung von SAP BusinessObjects Access Control in der Organisation vorhanden ist.

  Die Rechteeinstellung in einem SAP-System ist Grundlage für die Benutzerzuordnung und damit für das Identity-Management (IdM), für die Steuerung von Abläufen und Prozessen, für Audits und Compliance, für das interne Kontrollsystem sowie für das Risikomanagement, um nur einige aufzuzählen. Dabei lauten die Anforderungen eines SAP-Berechtigungskonzeptes:

  > sichere Zugriffe auf Funktionen und Daten
  > Risikoüberwachung/Funktionstrennung
  > Flexibilität und Transparenz
  > klare Verantwortlichkeit für die Rechte
  > einfache Bearbeitung, Change-Management und Qualitätssicherung
  > Investitionsschutz und Wirtschaftlichkeit

Abb. 4: Anforderungen an ein Berechtigungssystem

Die Rollen im Unternehmen sind über Jahre hinweg durch diverse Einflüsse (Upgrade, neue Organisationseinheiten, geänderte Prozesse, neue Module, externe User …) verändert und ergänzt worden und haben dabei in der Regel – hinsichtlich ihrer Rechte – zugenommen. SAP-ERP (ABAP-Stack) besitzt ein so mächtiges Rollensystem, dass beinahe alle Belange von Zugriffen eingeschränkt und auch die Daten geschützt werden können. Diese vielfältigen Möglichkeiten bringen zwangsläufig auch eine Komplexität mit sich, die ab einem gewissen Verflechtungsgrad von Rollen, Profilen und Berechtigungsobjekten kaum noch durchschaubar ist (ca. 75.000 Transaktionen und 1.500 Berechtigungsobjekte beinhaltet heute SAP ERP 6.0!). Eine genaue Analyse ist zwingend erforderlich. Die Ergebnisse dieses Arbeitspaketes fließen dann in die endgültige Projektplanung ein.

> Technische Installation von SAP Business Objects Access Control auf Entwicklungsumgebung: In der Strategiephase ist es wichtig, das bestehende SAP-Rollenkonzept hinsichtlich seines „Reifegrades" bezüglich bestehender Risiken (Segregation of Duties, kritischer Transaktionen) zu überprüfen und auch das Kernprojektteam hinsichtlich der Verwendung der Lösungskomponenten von SAP Business Objects Access Control zu schulen. Zu diesem Zweck sollte die Lösung auf einer Entwicklungsumgebung installiert werden und mit dem entsprechenden SAP-Backend-System (am besten demjenigen, in dem die Hauptgeschäftsprozesse implementiert sind) verbunden werden. Dieses Backend-System sollte das Rollenkonzept der Produktionsumgebung beinhalten.

  Zwei Möglichkeiten zur Durchführung der ersten Risikoanalyse (RAR) bieten sich an:

  > man verwendet die mitgelieferten umfangreichen Standardprüfregeln (Normalfall) oder
  > man erstellt – ggf. auf Basis des mitgelieferten Standards – unternehmensindividuelle Prüfregeln.

Welche Variante auch immer gewählt wird: das Ergebnis wird eine Vielzahl von potenziellen Risiken liefern, unabhängig davon, ob „nur" auf Berechtigungsebene oder auch auf Benutzerebene (mit oder ohne Einbeziehung der Berechtigungsobjekte) selektiert wird.

Die mitgelieferten Prüfregeln innerhalb von SAP BusinessObjects Access Control sind vollumfänglich für große Unternehmen vorgefertigt und enthalten eine Vielzahl von Risiken mit kritischen Funktionskombinationen – abgeleitet aus den Erfahrungen einer Vielzahl von Revisionsprüfungen. Jede dieser dort beschriebenen Funktionen besteht aus einer bis zu mehreren Transaktionen. Bei der Analyse werden diese Funktionen in ihre Transaktionen – und ggf. auch in die Berechtigungsobjekte – aufgelöst, was die Risikomatrix erheblich vergrößert.

Wenn nach Durchlauf von RAR sich Risiken im fünf- und mehrstelligen Bereich ergeben, wird es außerordentlich schwierig werden, daraus Folgerungen für eine Anpassung oder für ein Redesign abzuleiten (z. B. erzeugt eine sehr umfangreiche Berechtigung wie SAP_ALL pro User sehr viele Risikomeldungen).

Das Ergebnis dieser Risikoanalyse muss um die nicht relevanten Risiken reduziert werden, damit eine spätere Auswertung nur die Risiken ausweist, die für IT und Fachbereiche verständlich, diskussionsfähig und entscheidungsfähig sind. Erst nach einer Filterung der Ergebnisse kann – im weiteren Verlauf des Projektes – die Kontrollmatrix auf die Governance-Anforderungen des eigenen Unternehmens angepasst werden, damit daraus letztendlich saubere, überschaubare und transparente Funktionstrennungsvorschriften bzw. kompensierende Kontrollen ableitbar sind.

Die „Treffer" der ersten Risikoanalyse sollten nach folgender Methode gefiltert, heruntergebrochen und überarbeitet werden:

- Schritt Transaktionsgleichheit: die Risiken nachbearbeiten bzw. löschen, in denen rechts und links dieselbe Transaktion als Konflikt steht.
- Schritt Kreuzkonflikte: die Kreuz-Risiken nachbearbeiten bzw. löschen, wo im Risiko (a) TR1 mit TR2 im Konflikt und im Risiko (b) TR2 mit TR1 im Konflikt stehen.
- Schritt prozessualer Verbund: Separierung der Transaktionen in unterschiedliche Einzelrollen, wenn eine Trennung dieses Transaktionspaares operational unschädlich ist (der Prozessdurchlauf dadurch nicht behindert wird!).

In der Praxis hat sich gezeigt, dass sich o.g. Schritte leichter durchführen lassen, wenn man das sehr umfangreiche Datenvolumen des ersten Analyseergebnisses in ein auswertbares Format (z. B. Excel) exportiert. Eine toolgestützte Weiterbearbeitung ist hilfreich und schafft die Grundlage zu eruieren, ob die ausgewiesenen Konflikte für das betrachtete Unternehmen überhaupt relevant sind und ein Risiko darstellen.

Ein zweiter Durchlauf der Risikoanalyse – nach Überarbeitung der Prüfregeln – wird den Erfolg zeigen; ggf. muss dieses Verfahren ein weiteres Mal durchgeführt werden, um zum gewünschten Ergebnis zu gelangen.

Das geschilderte Verfahren bezieht sich auf die Standard-Transaktionen. Zusätzliche Risiken können sich wegen der Nutzung eigenentwickelter Transaktionen ergeben, wobei diese aufgrund intransparenter

Prüflogik schwer erkennbar sind. Hier hilft ein meist nur mittelfristig realisierbares Konzept der Analyse dieser Y-/Z-Transaktionen. Dabei erkennbare kritische eigenentwickelte Transaktionen müssen in die Risiko- und Funktionsdefinition mit aufgenommen werden, um später eine umfassende, unternehmensweite Kontrolle durchführbar zu machen.

Auf Grund des Ergebnisses eines erneuten RAR-Durchlaufes dieser dann „überarbeiteten und gefilterten" Analyse sollte entschieden werden, ob das bestehende Rollenkonzept komplett neu entworfen, geändert oder eventuell „sanft" überarbeitet werden muss.

- Festlegung der Risikomanagement-Richtlinie: Entsprechend den Voraussetzungen von SAP BusinessObjects Access Control sollten folgende Risikomanagement-Richtlinien festgelegt werden:
  - Erste Festlegung des Risikomanagement-Prozesses für die Zugriffssteuerung,
  - Verantwortungen für die Definition von Risikoregeln wie Funktionstrennungsrisiken, kritische Transaktionen und kritische Leseberechtigungen,
  - Verantwortungen für die Definition von kompensierenden Kontrollen,
  - Festlegung der Risikolevel und Bewertung der bestehenden Risiken,
  - Festlegung der Richtlinie für die Ablehnung/Zustimmung mit kompensierenden Kontrollen für Berechtigungsanfragen,
  - Festlegung einer Richtlinie für den Superuser-Zugriff („Firefighter-Konzept"),
  - Festlegung der Rollen im Risikomanagementprozess, wie z. B. Compliance Management, Risikoeigner und Eigner von kompensierenden Kontrollen.

- Evaluierung des Benutzermanagement-Prozesses: Entsprechend den Voraussetzungen von SAP Business Objects Access Control muss ein führender Benutzerpersistenzspeicher festgelegt werden, der zur weiteren Provisionierung der Benutzer-Identitäten in die Zielsysteme notwendig ist. Hierzu muss zudem evaluiert werden, ob SAP BusinessObjects Access Control eventuell auch an ein bestehendes oder neu einzuführendes Identity-Management-System angeschlossen werden soll. Speziell die Verbindung mit SAP NetWeaver Identity Management bietet sich hierbei an. Ziel dieses Arbeitspaketes ist es, die bestehenden Identity-Management-Prozesse und Genehmigungsworkflows für die Verwendung von SAP BusinessObjects Access Control zu adaptieren.

- Festlegung eines Architekturkonzeptes für SAP BusinessObjects Access Control: Auch für SAP BusinessObjects Access Control muss ein Architekturkonzept in Abhängigkeit der gewünschten oder vorgeschriebenen Systemarchitektur, z. B. „Drei Systemlandschaften" wie Entwicklung, Qualitätssicherung und Produktion festgelegt werden. In Abhängigkeit der gewählten Systemlandschaft müssen die Änderungsmanagementprozesse für technische Änderungen, Rollenänderungen und Benutzermanagement definiert werden – auch die Integration mit dem Identity-Management-System.

- Durchführung eines Kernteam-Trainings: Es ist ratsam, schon in der Strategiephase ein erstes Training für das Kernteam aller SAP BusinessObjects Access Control-Komponenten durchzuführen. Dies ermöglicht, die Übertragung der Konzepte auf die Anforderungen der SAP BusinessObjects-Lösung zu erleichtern.

> Strategischer Meilenstein: Neuentwicklung Rollenkonzept oder Adaption des bestehenden Konzeptes: Ein wichtiger Meilenstein ist die Entscheidung für die eventuell komplette Neuentwicklung des Rollenkonzeptes oder dessen sanfte Anpassung. Aufgrund des Resultats der initialen Risikoanalyse mit dem bestehenden Rechtesystem und der Anzahl und Art von aufgetretenen Risiken, der genauen Zuordnung von Rollen zu einem eindeutigen Rolleneigner und der Rollenstruktur muss entschieden werden, ob eine komplette Überarbeitung des SAP-Rollenkonzeptes zur Einführung von SAP BusinessObjects Access Control sinnvoll, machbar und wirtschaftlich vertretbar ist. Sind die bestehenden Konflikte eher gering und können eindeutige Rolleneigner aus den Fachbereichen zugeordnet werden, so kann das Rollenkonzept auch entsprechend durch einfacheres „Splitten" von den Konflikten bereinigt werden. Falls sehr viele Konflikte vorhanden sind, kann mit einem Reverse-Business-Engineering-Ansatz oder mit einem funktionsorientierten Redesign-Ansatz das SAP-Rollenkonzept recht effektiv auf die Anforderungen von SAP BusinessObjects Access Control angepasst werden.

  Es ist nicht einfach, den Ressourcenbedarf für Anpassung oder Überarbeitung bei hohem Sicherheits- und Qualitätsanspruch, Erfüllung der externen Vorschriften sowie einer sehr guten Transparenz (verständliche revisionsgerechte Dokumentation) und leichter Änderbarkeit zu quantifizieren; zwingend ist jedoch, diese Zahlen miteinander zu vergleichen, das Für und Wider abzuwägen und sich dann für einen der Wege festzulegen – insbesondere, wenn für das Reverse Business Engineering und auch für das funktionsorientierte Redesign auf dem Markt Werkzeuge und Methoden vorhanden sind und diese das Projekt erleichten und auch zeitlich deutlich verkürzen können. „Nur" eine Überarbeitung der betroffenen Rollen und Profile stellt sich bei komplexen Berechtigungskonzepten aus Erfahrung immer als schwieriger und langwieriger dar als gedacht.

> Festlegung des strategischen Rollenkonzeptes, falls Rollenredesign beschlossen wurde: Entsprechend den Voraussetzungen von SAP BusinessObjects Access Control muss eine Struktur eines SAP-Rollenkonzeptes festgelegt werden. Strategische Überlegungen sind hierbei:

  > Definition von Informationsverantwortungsbereichen für SAP-Transaktionen und -rollen
  > Verwendung eines arbeitsplatzbasierenden Konzeptes mit Hauptarbeitsplatzrollen, die die Hauptaufgaben der jeweiligen Position umfassen plus einer entsprechenden Flexibilisierung durch Nebenaufgabenrollen, mit der die notwendige Flexibilisierung des organisationsbasierten Konzeptes erreicht wird
  > Verwendung von Sammelrollen oder Einzelrollen zur Abbildung des Konzeptes
  > Verwendung von Ableitungsprinzipien oder Restriktionsrollen
  > Festlegung von Namenskonventionen
  > Festlegung von speziellen Berechtigungen wie Tabellenzugriff, Batch, Druckersteuerung etc.

> Festlegung des strategischen Rollenkonzeptes, falls funktionsorientiertes Redesign beschlossen wurde: Entsprechend den Voraussetzungen von SAP BusinessObjects Access Control muss eine Struktur eines SAP-Rollenkonzeptes mit folgenden strategischen Überlegungen festgelegt werden:

  Ein Redesign der Rechteeinstellungen darf nicht auf der Technikebene ansetzen, sondern beginnt zunächst mit der betriebswirtschaftlichen Definitionsphase der eigenen Prozesse und deren Funktionen. Wenn entsprechende Funktionsbeschreibungen innerhalb des Unternehmens nicht vorliegen, müssen diese zusammen mit den Fachbereichsverantwortlichen erstellt und strukturiert werden; die Fachbereichsverantwortlichen müssen – als sog. Data-Owner – die Verantwortung dafür übernehmen und dazu

auch in der Lage sein (Vorschrift aus IKS und SOX). Die Funktionsbausteine sollen in sich abgeschlossene betriebliche Tätigkeiten beschreiben und untereinander abgegrenzt und nicht redundant sein; ihre Größe richtet sich u. a. nach der Arbeitsteilung im Unternehmen, wobei darauf Wert zu legen ist, sie so klein und überschaubar wie möglich zu halten; sie sind in Anzeige- und Bearbeitungsfunktionen zu trennen. Weiterhin ist darauf zu achten, dass diese Bausteine in sich compliant sind (keine Funktionskonflikte beinhalten). Dabei ergeben sich für ein Fertigungsunternehmen in der Summe leicht an die 1.000 Funktionsbausteine über den gesamten ERP-Zyklus hinweg. Eine große Erleichterung können bereits vorgefertigte Funktionsbausteine bringen, wie sie heute am Markt als sog. „Best Practice" bzw. „Templates" erhältlich und wiederverwendbar sind.

> Finalisierung des Projektplanes: In Abhängigkeit von den getroffenen strategischen Entscheidungen und Konzepten muss der Projektplan finalisiert werden. Der Aufwand sollte neu evaluiert und festgelegt werden, zudem muss der Zeitplan nochmals abgestimmt und verabschiedet werden.

> Meilenstein: Abschluss der Strategiephase

3.4.2 PHASE SOLLKONZEPTION („BUSINESS BLUEPRINT UND DESIGN"):

In der Business-Blueprint-Phase werden die getroffenen strategischen Konzepte weiter verfeinert und im Detail festgelegt. Dies kann nun im Wesentlichen für die vier Hauptkomponenten von SAP BusinessObjects Access Control „Risikoanalyse und Beseitigung", „Unternehmensweites Rollenmanagement", „Management von Superuser-Berechtigungen" sowie „Regel- und gesetzeskonforme Berechtigungsvergabe" parallel mit Abstimmungspunkten durchgeführt werden, wobei übergeordnete Aspekte wie technische Architektur und auch Risikomanagementprozessdesign und Organisation (Definition von Rollen für die Verwendung von SAP BusinessObjects Access Control selbst) für alle Komponenten betrachtet werden müssen. Auch sollte in dieser Phase schon ein entsprechendes Testkonzept der Prozesse und Integrationsabläufe festgelegt werden.

Die folgenden Hauptarbeitspakete sollten pro Komponente betrachtet werden.

3.4.2.1 ARCHITEKTUR & TECHNOLOGIE:

> Detaillierter Blueprint der technischen Architektur: In der Designphase sollte der Blueprint der technischen Architektur festgelegt werden. Es sollte zudem ein Staging-Konzept inklusive Entwicklungs-, Qualitätssicherungs- und Produktionsumgebung für die SAP BusinessObjects Access Control-Lösung festgelegt werden. Dies sollte auch die Änderungsmanagementprozesse für die Rollen und technische Upgrades berücksichtigen. So sollte betrachtet werden, dass z. B. Rollenänderungsprozesse auf der Entwicklungsumgebung stattfinden und entsprechend nach Freigabe über das Transportwesen in die Produktionsumgebung über den Schritt Qualitätssicherung transportiert werden. Die Provisionierung zu den Anwendern kann in der Produktionsumgebung erfolgen. Zudem muss der führende Benutzerspeicher festgelegt werden, von welchem aus die Provisionierung in die Zielsysteme stattfinden kann. Diese Aspekte sind maßgebende Einflussfaktoren für die technische Architektur.

Des Weiteren muss die Integrationsarchitektur mit einem möglichen Identity & Access Management System (z. B. SAP NetWeaver Identity Management) festgelegt werden. Hierzu müssen die technischen Schnittstellen und Konnektoren für die Directory Services im Detail ausgewählt werden.

Sollen Non-SAP-Systeme mit angebunden werden, so stehen beispielsweise für Oracle Financials, JD Edwards, PeopleSoft entsprechende RTAs (Real Time Agent) zur Verfügung. Bei Anbindung einer anderen Software sind ggf. eigenentwickelte Konnektoren zu verwenden. Bei den eigenentwickelten Konnektoren ist das Matching der einzelnen Berechtigungselemente des Non-SAP-Systems zu den Feldern von SAP BusinessObjects Access Control zu beachten. Aufbauend auf diesem Matching ist auch das Regelwerk entsprechend zu erstellen.

> Design der notwendigen Batchprozesse: Auch für die SAP BusinessObjects Access Control-Lösung müssen entsprechende Batchprozesse festgelegt werden, die z. B. den Abgleich der Berechtigungsvorschlagswerte und Objekte aus den Zielsystemen regeln. Dies sollte entsprechend im Blueprint festgelegt werden.

> Installations-, Konfigurations- und Betriebsmanual: Für die technische Installation und Konfiguration muss ein kundenspezifisches Dokument erstellt werden, welches die notwendigen Hauptschritte zur Installation und Konfiguration entsprechend dokumentiert. Dieses dient zudem als Basis für ein Betriebshandbuch, welches zum späteren Betrieb von SAP BusinessObjects Access Control notwendig ist. Hier sollten z. B. die notwendigen Schritte zur Fehlerbehandlung und die Upgradestrategie (z. B. im Fall eines Upgrades auf einen neuen Regelsatz) festgelegt sein.

3.4.2.2 RISIKOANALYSE UND BEREINIGUNG

> Bestimmung der wichtigsten Informationswerte der Geschäftsbereiche als Grundlage für die Risikobewertung: Eine wichtige Grundlage zur Bestimmung von Geschäftsrisiken, die durch betrügerische Handlungen (wegen fehlender Funktionstrennung), kritische Transaktionen oder auch unberechtigte Informationseinsicht hervorgerufen werden, ist die Bestimmung des Wertes der Informationen, welche in den Geschäftsprozessen verarbeitet werden. So sollte eine Vertraulichkeits-, Integritätsbedarfs- und Verfügbarkeitsklassifikation unter Mitwirkung der Fachbereiche festgelegt sein, die entsprechend den Risikolevel bestimmen. Z. B. kann auch schon die Einsicht in Konstruktionsdaten in einem Maschinenbauunternehmen zu einem Risiko führen, wenn durch diese ein bedeutender Wettbewerbsvorteil am Markt erzielt wird.
Dieses Arbeitspaket wird empfohlen, ist aber nicht unbedingt zwingend erforderlich, wenn das Unternehmen oder eine Organisation andere Policies zur Risikobewertung eingeführt hat.

> Festlegung der Zugriffsrisiken (kritische Displayrechte, Transaktionen und Betrugsrisiken durch fehlende Funktionstrennung): SAP BusinessObjects Access Control wird standardmäßig mit einem umfangreichen Satz an Prüfregeln ausgeliefert, welche ein Best-Practice-Katalog von Risiken darstellt. Viele Unternehmen übernehmen diesen Risikoregelsatz direkt in ihren eigenen Risikokatalog. Trotzdem ist es sehr wichtig, dass diese Risiken aufgrund der Bewertung der wichtigen Informationswerte und eigenen Geschäftsprozesse entsprechend mit den Fachbereichen auf deren Gültigkeit und auch auf den vorgegebenen Risikolevels hin überprüft werden. Wird diese Risikobewertung nicht durchgeführt, ist oftmals die Akzeptanz der Fachbereiche für die gewählten Risiken eher niedrig. Zudem sollten die Prüfregeln durch kritische Berechtigungen und auch Displayrechte (welche über bestimmte Berechtigungsobjekte gesteuert werden können) sowie eigenerstellte Transaktionen ergänzt werden.

Die Festlegung der Risiken und Level muss auf jeden Fall mit den Fachbereichen zusammen geschehen. Zudem ist es von Vorteil, wenn ein Risikomanager (oder Compliance Manager) die entsprechenden Workshops leitet. Auch die Abteilung „Internal Audit" sollte vor einer ersten Produktivsetzung die festgelegten Risikodefinitionen akzeptieren.

Die Definition von Zugriffsrisiken muss als fortlaufender Compliance-Prozess innerhalb des Unternehmens gesehen werden und fester Bestandteil des Gesamtrisikomanagements werden. Dies ist dadurch begründet, dass sich Unternehmensprozesse ständig ändern und auch neue Funktionen in SAP ERP und andere Anwendungen ständig hinzukommen.

> **Festlegung von kompensierenden Kontrollen:** Für die im obigen Schritt festgelegten Risiken müssen entsprechende kompensierende Kontrollen festgelegt werden, falls sich das Zugriffsrisiko z. B. durch Funktionstrennung (Trennung der SAP-Rollen) oder auch durch entsprechenden Entzug der Berechtigungen nicht vermeiden lässt. Die kompensierenden Kontrollen definieren dann die notwendigen detektivischen Maßnahmen, die durchgeführt werden müssen, um z. B. betrügerische Handlungen schnell erkennen und entsprechend eindämmen zu können. Diese Kontrollen können teilweise manuell sein, wie z. B. die Durchführung einer Inventur des Lagerbestandes, oder aber auch mit Hilfe von SAP-Reports, mit welchen schnell analysiert werden kann, ob z. B. verdächtige Kontodaten bei Kreditoren eingepflegt wurden. Die Durchführung von kompensierenden Kontrollen muss einem Verantwortlichen zugeordnet werden, der dafür Sorge trägt, dass die Kontrolle im vorgesehenen zeitlichen Intervall durchgeführt und das Ergebnis der Kontrolle auch dokumentiert wird.

Die Ausarbeitung der kompensierenden Kontrollen sollte wiederum mit den Fachbereichen und unter Beteiligung des Risikomanagers (oder Compliance Managers) erfolgen. Auch muss in diesem Zusammenhang eine Richtlinie definiert werden, die genau in Abhängigkeit vom Risikolevel festlegt, ob ein Risiko im Provisionierungsworkflow akzeptiert werden darf, oder unbedingt mit einer kompensierenden Kontrolle versehen werden muss.

> **Festlegung des Rollenkonzeptes für die SAP BusinessObjects Access Control-Lösung selbst:** Auch für die spätere Anwendung der SAP BusinessObjects Access Control-Lösung müssen über die User Management Engine (UME) entsprechende Rollen definiert werden. Dies können z. B. technischer Administrator, Risikomanager (Festlegung der Risikomatrix inkl. Level und kompensierenden Kontrollen), Approver (ist am Workflow z. B. beim Approval der Rollenzuordnung beteiligt) und Auditor (Auswertung von Logs und Überprüfung der Einhaltung der Prozesse) sein. Die Rollen sollten entsprechend dokumentiert werden.

3.4.2.3 UNTERNEHMENSWEITES ROLLENKONZEPT

> **Design des neuen Rollenkonzeptes für die Erfordernisse der Komponente „Unternehmensweites Rollenmanagement“:** In Abhängigkeit des in der Strategiephase festgelegten Konzeptes zum „Bereinigen“ der Risiken im Rollenkonzept können folgende Varianten in Betracht gezogen werden:

Variante A: Das bestehende Rollenkonzept wird in seiner Struktur so belassen und später in der Implementierungsphase entsprechend mit Hilfe von sukzessiv durchgeführten Risikoanalysen (aufgrund der vorher festgelegten Risikomatrix) in risikofreie Rollen entweder mit dem PFCG oder dem ERM aufgeteilt. Allerdings müssen in der Designphase entsprechende Rolleneigner aus den Fachbereichen und weitere organisatorische Ausprägungen für die bestehenden Rollen zugeordnet werden.

Variante B: Falls eine große Anzahl von Risiken im bestehenden Konzept identifiziert wurde, bietet sich ein Reengineering des Rollenkonzeptes mit Hilfe eines Reverse-Business-Engineering-Konzeptes an. In diesem Fall wird durch entsprechendes „Tracing“ der Anwender festgestellt, welche SAP-Funktionen von diesen wirklich benötigt werden und welche eigentlich nicht. Die Erfahrung zeigt, dass durch dieses Verfahren ca. 50–70 Prozent der bestehenden Risiken reduziert werden können. Bei dieser Variante sollten folgende Arbeitspakete angewandt werden:

1. Analyse des Organisations-Charts mit der Identifikation der Positionen und deren Zuordnung zu bestehenden SAP-Anwendern im System.
2. Analyse von eigenentwickelten Z-Transaktionen und deren Dokumentation (falls nicht schon vorhanden).
3. Zuordnung aller SAP-Transaktionen zu Informationseignern der Fachbereiche, die später entsprechend auch die Rolleneignerschaft übernehmen.
4. Durchführung der Reverse-Business-Engineering-Analyse im SAP-System zur Identifikation anhand der gruppierten Positionen der tatsächlich verwendeten SAP-Transaktionen im System und deren Zuordnung zu entsprechenden Informationseignern. Ableitung des Rollenkonzeptes basierend auf Hauptarbeitsplatzrollen plus zusätzlicher Aufgabenrollen, die entsprechend innerhalb der Informationseignerbereiche gebildet werden können. Vorteil dieses Verfahrens ist, dass im ersten Ansatz den bestehenden Anwendern keine Funktionalität entzogen wird, welche sie tatsächlich in ihrer tagtäglichen Arbeit benötigen. Damit kann das Rollout-Risiko der Lösung minimiert werden.
5. Festlegung der notwendigen organisatorischen und funktionalen Ausprägungseinschränkungen (wie z. B. Company Code, Verkaufsorganisation etc.), welche später dann in der Rollenausprägung benötigt werden. Dies muss mit den jeweiligen Fachbereichen erfolgen oder ist als Dokumentation vom bestehenden Konzept noch vorhanden und kann entsprechend übertragen werden.

Variante C: Eine große Anzahl von Risiken im bestehenden Konzept wurde identifiziert. Die existierenden Rollen sind i.d.R. über Jahre gewachsen, unstrukturiert und sehr mächtig geworden und – wie analysiert – mit vielen Funktionstrennungskonflikten behaftet; dann bietet sich eine Neustrukturierung (Redesign) anhand von betrieblich exakt abgegrenzten Funktionsbausteinen an. Die daraus ableitbaren Einzelrollen lassen sich später einfach zu Sammelrollen aggregieren und mittels des ORG-Managements (HR) den Arbeitsplätzen zuordnen; darauf kann dann das IdM und CUP sinnvoll aufsetzen.

Nach der Konzeption und Definition der im Unternehmen erforderlichen betrieblichen Funktionsbausteine kommt man im nächsten Schritt zur Technikebene und zur Umsetzung in Einzelrollen. Hierzu bieten sich sowohl der ERM (Enterprise Role Manager) wie auch der PFCG (Profilgenerator) an oder aber ein toolunterstütztes Vorgehen auf Basis bereits vorgefertigter Funktionsbausteine. ERM hat den Vorteil,

die Rollen nach der Erstellung sofort auf Funktionstrennungsanforderungen (SOD) verproben zu können und über einen Freigabeprozess auch genehmigen zu lassen. Arbeitet man mit geeigneten – am Markt erhältlichen – bereits konfliktfreien „Best-Practice-Bausteinen", können die Einzelrollen aus diesen Funktionsbausteinen mit Hilfe von Werkzeugen direkt abgeleitet und die Organisationsdaten zugesteuert werden.

Eine Namenskonvention der Einzel- und Sammelrollen sowohl im Kurz- wie auch im Langnamen ist verpflichtend. Der Kurznamen enthält Modulbereiche (wie SD, PP …), die betriebliche Funktion und eine eindeutige Nummerierung. Wichtiger ist der Langname; dieser sollte immer und durchgehend 3-teilig aufgebaut sein:

1. Modulkennzeichen und betriebliche Funktion
2. Funktionstyp mit Bearbeiten, Anzeigen …
3. Organisationsebene wie Buchungskreis, Sparte … Kostenstelle.

Eine betriebliche Funktion (Einzelrolle) ist nur dann hinreichend und vollständig beschrieben, wenn sie alle benötigten Transaktionen und auch ihre zugehörigen abgrenzungsrelevanten Organisationsdaten (Berechtigungsobjekte/Felder/Werte) beinhaltet. Teilfunktionale Rollen, Rollen ohne Transaktionen oder Org-Werte, Rollen mit Transaktionsbandbreiten, Rollen mit „Aktivitätscode*" sollten nicht zugelassen werden. Hat man eine starke Verästelung mit vielen Sparten, Kostenstellen etc. im Unternehmen, die eigens abgegrenzt werden müssen, entstehen sehr wohl einige Kopien dieser Bausteine, die jedoch funktional identisch bleiben und sich nur in der Organisationsausprägung unterscheiden. Ob später mit oder ohne Vererbung gearbeitet werden soll, ist beim Design zu berücksichtigen.

Bei eigenentwickelten Transaktionen ist eine Prüfung unerlässlich, ob diese nach dem SAP-Authorization-Check-Verfahren programmiert sind, ggf. eigene Berechtigungsobjekte besitzen oder Standardtransaktionen aufrufen und welche davon überhaupt noch verwendet werden. Kommt man zu dem Ergebnis, dass hier kritische oder unbekannte bzw. nicht dokumentierte Eigenentwicklungen vorliegen und auch noch eingesetzt werden, empfiehlt es sich, diese in eigene Einzelrollen – nach Modulgruppen getrennt – abzulegen und speziell zu benennen. Eine Vermischung zwischen Standard- und den eigenen Y-/Z-Transaktionen sollte vermieden werden, da diese später schwierig zu handhaben sind („die findet man fast nie mehr!").

Zum Schluss ergänze man die so erstellten Rollen um die sog. Notfallrollen, d. h. Rollen zum Customizing sowie zur Entwicklung im Produktivsystem, die Rollen für die Berater, WPs und Steuerprüfer/Finanzamt, den Datenschutzbeauftragen etc. Notfallrollen sollen modulweise abgegrenzt und eingeschränkt werden und die Verwendung nur über den SPM erfolgen.

Die Hauptarbeit eines Rollendesigns ist der Aufbau der Einzelrollen; nach Beendigung sind alle betrieblichen Funktionen – unabhängig, wie und wo sie eingesetzt und verwendet werden – vollumfänglich umgesetzt. Am besten beginnt man mit der größten Funktionsbreite einer Einheit (Hauptgeschäftsprozesse), um ggf. später im Rollout-Verfahren davon neue Einheiten abzuleiten und anzupassen. Hier bieten sich dann zur Arbeitserleichterung Massenkopierverfahren an.

3 SAP BusinessObjects Access Control 5.3

Arbeitsplätze sind in Arbeitsplatzfunktionen aufgeteilt; eine Arbeitsplatzfunktion ist die Aggregierung (Zusammenfassung) betrieblicher Funktionen (Einzelrollen), z. B. in der Abteilung Vertrieb der Vertriebsaußendienst für Deutschland. Wenn man alle Einzelrollen in einer Spalte (z. B. Excel) aufführt und horizontal zusammen mit den Fachbereichsverantwortlichen die Arbeitsplatzfunktionen definiert, können die Arbeitsplätze einfach durch Ankreuzen zusammengestellt werden. Das Excel dient später auch zur Transparenz und beschreibt im Detail die Inhalte dieser Arbeitsplätze mit ihren einzelnen Funktionen. Organisationsänderungen sind leicht und ohne großen Aufwand umzusetzen, wenn sich Funktionen innerhalb der Organisation verschieben; dies bedeutet ein Umhängen der Einzelrollen. die Funktion selbst bleibt i.d.R. innerhalb des Unternehmens unverändert. Bei dieser Vorgehensweise sind Benutzern immer nur Sammelrollen oder Business-Rollen zugewiesen und möglichst keine Einzelrollen. Fachbereiche kennen somit nur eine in sich überschaubare Anzahl ihrer Sammelrollen und dadurch ist eine durchgängige Transparenz und effiziente Handhabung geschaffen.

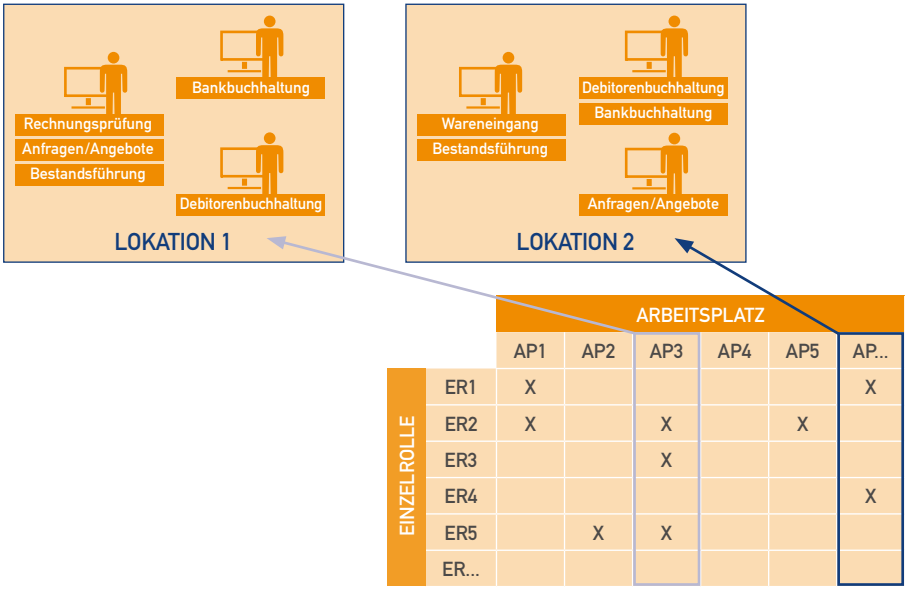

Abb. 5: Aggregierung von Einzelrollen zu Sammelrollen (Arbeitsplätze)

Dieser Redesign-Prozess ist aufwendig und bindet nicht nur die Ressourcen der IT, sondern auch die der Key-User aus den Fachabteilungen. Deshalb ist es wichtig, nach Freigabe und Produktivsetzung der neu gewonnenen Rollen jede Veränderung durch einen Genehmigungsprozess zu initiieren und diese mit Zeitstempel zu dokumentieren - nicht nur aus Revisionssicht, sondern auch aus Investitionsschutz!

Um die Qualität und Veränderung eines Rechtesystems bzgl. sicherer Zugriffe, Funktionstrennung, Flexibilität, Transparenz und klarer Verantwortlichkeit sicherzustellen, helfen der SAP BusinessObjects Access Control-Prozess CUP und ERM; innerhalb ERM gibt es dabei folgende Berichte für das Rollenmanagement:

- Beziehungen zwischen Stamm- und abgeleiteten Rollen (Vererbung)
- Beziehung von Einzel- zu Sammelrolle
- Rollen nach Generierungsdatum
- Transaktionen in Rollen
- Transaktionen in Rollenmenü und produktive Berechtigung vergleichen
- Berechtigungen in Rollen zählen
- Änderungshistorie der Rollen (bis auf Feldebene)
- Rollenvergleich (von 2 bestimmten Rollen – auch für Backend-Systeme ohne Synchronisierung).

3.4.2.4 GESETZESKONFORMES BENUTZERMANAGEMENT

1. **Festlegung und Design der gesetzeskonformen Änderungsmanagementprozesse:** In diesem Arbeitspaket müssen die wichtigsten Änderungsmanagementprozesse zusammen mit den Fachbereichen und dem Compliance Management festgelegt werden, welche sind:

   - Beantragung von Rollen und Berechtigungen durch die Fachbereichsanwender.
   - SAP-Rollenänderungsantrag, Neuanlage oder Löschen einer Rolle in einem bestimmten Informationsverantwortungsbereich mit der Komponente „Unternehmensweites Rollenmanagement".
   - Passwort-Änderungs- oder -Rücksetzungsantrag.
   - Festlegung einer neuen Risikodefinition oder Änderung bzw. Löschung einer bestehenden Risikodefinition.
   - Zuordnung einer kompensierenden Kontrolle zu „risikobehafteten" Anwendern, falls dies nicht schon im Rollenbeantragungsprozess durchgeführt wurde.
   - Änderung oder Neuanlage bzw. Löschung von kompensierenden Kontrollen im bestehenden Katalog.

2. **Festlegung und Design des Blueprints für die Integration mit einem Identity & Access Management System (z. B. SAP NetWeaver Identity Management); siehe auch 3.7:** In der Strategiephase wurde ein entsprechendes High-Level-Konzept festgelegt, wie die Verwaltung der Identitäten für das Unternehmen mit dem Zugriffsrisikomanagement, welches über SAP BusinessObjects Access Control gesteuert wird, integriert werden soll. Für SAP BusinessObjects Access Control ist ein entsprechendes führendes Identity System notwendig, um die weitere Provisionierung der Benutzerkonten (Identity) in die angeschlossenen Zielsysteme (SAP oder auch Non-SAP) durchführen zu können. In diesem Zusammenhang müssen entsprechend die Integrationsprozesse festgelegt werden. Auch müssen die führenden Benutzerattribute pro Quellsystem (z. B. SAP HCM für Mitarbeiter oder SAP ERP für externe temporäre Mitarbeiter etc.) festgelegt werden.

3.4.2.5 SUPERUSER PRIVILEGE MANAGEMENT

1. Festlegung einer Richtlinie für den Superuser-Zugriff: Zusammen mit den Fachbereichen sollte eine Richtlinie für den Zugriff auf höher berechtigte Notfallbenutzer festgelegt werden. Der Zugriff sollte in der Tat nur für den Notfall erlaubt werden und nicht für den Regelfall, da ansonsten das eigentlich definierte Berechtigungskonzept nach und nach unterwandert wird.
   Festzulegen ist auch, ob die Superuser-IDs einzelnen Benutzern permanent zugeordnet werden oder ob für die jeweilige Nutzung einer entsprechenden ID das Benutzerantragsverfahren genutzt werden soll.

2. Detailliertes Design des Superuser Privilege Management mit SAP BusinessObjects Access Control:
   Die Richtlinie wird als Prozess-Blueprints designet und es werden entsprechend die Eigner für die Superuser-IDs festgelegt. Zudem müssen die entsprechenden höherwertigen Berechtigungen pro Superuser-ID bestimmt werden. Dies muss wiederum zusammen mit den Fachbereichen erfolgen. Auch die Auditoren, welche im Nachgang einer Superuser-ID-Verwendung die Änderungsprotokolle auszuwerten haben, müssen pro Fachbereich festgelegt werden. Zudem sind klare Vorgaben zur Auswertung festzulegen. Bei einer Identifikation von Unregelmäßigkeiten in den Änderungsprotokollen müssen zudem die notwendigen reaktiven Schritte festgelegt werden.

3.4.2.6 TESTVORBEREITUNG FÜR ALLE KOMPONENTEN

1. Festlegung der Testfälle: Schon in der Designphase sollten die entsprechenden Testfälle für das getroffene Design festgelegt werden, diese sind:

   > Risikoanalyse
   > Technische Batchprozesse
   > Änderungsworkflows (Provisionierung)
   > Integrationsprozesse für die Identity & Access-Management-Lösung
   > Superuser-Privilege-Zugriffsmanagement
   > Optional: Rollentests nach den vorgegebenen Geschäftsprozessen, falls ein Reengineering für die SAP-Rollen durchgeführt werden soll.

2. Festlegung der Testskripte: Mit Hilfe der Testfälle müssen entsprechend detaillierte Testskripte abgeleitet werden, mit deren Hilfe dann in der Implementierungsphase entsprechend die Tests durchgeführt werden können.

Meilenstein: Finalisierung und Abzeichnung der detaillierten Blueprints und Designs durch die Fachbereiche, SAP-Berechtigungsmanagementteam und Compliance Manager.

3.4.3 PHASE REALISIERUNG („IMPLEMENTIERUNG“)

In der Realisierungsphase werden nun die detaillierten Konzepte und Designs entsprechend in die Testumgebung implementiert und getestet. Dies kann wieder teilweise für die einzelnen Komponenten parallelisiert werden. Aber speziell ein mögliches notwendiges Neuerstellen der Rollen muss mit der Risikoanalyse integriert bzw. teilweise auch iterativ durchgeführt werden.

Im Einzelnen sollten die folgenden Arbeitspakete angegangen werden.

3.4.3.1 ARCHITEKTUR & TECHNOLOGIE

1. Technische Installation aller SAP BusinessObjects Access Control-Komponenten: Entsprechend des technischen Designs werden nun alle Komponenten für die vorgesehene Systemlandschaft installiert. Dabei kann zum Teil die in der Strategiephase bereits installierte Sandbox zur Entwicklungslandschaft weiterentwickelt werden. Je nach Design wird die Entwicklungslandschaft mit einer Qualitätssicherungslandschaft und finalen Produktion erweitert. Zudem müssen die notwendigen Real Time Agents (RTA) je nach gewählter Access-Control-Version und Zielsystemversion auf den Backend-Systemen installiert werden.

2. Finale technische Konfiguration: Nach erfolgter technischer Installation werden die notwendigen Verbindungen zu den Zielsystemen konfiguriert und zudem die notwendigen Batchjobs für die Berechtigungsdatensynchronisation (USOBX_C und USOBT_C) etc. definiert. Zudem müssen die Webservice Interfaces zwischen Risikoanalyse und Bereinigung und gesetzeskonformer Benutzerprovisionierung (Workflow Engine) konfiguriert werden. Auch die Transportmechanismen von Entwicklung zu Produktion für die Risikoregeln werden entsprechend konfiguriert und spezifiziert.

3.4.3.2 RISIKOANALYSE UND BEREINIGUNG

1. Umsetzung der definierten Risiken und Zuordnung der kompensierenden Kontrollen im System: Die in der Blueprint & Design-Phase definierten Risiken und die dazu korrespondierenden kompensierenden Kontrollen werden entsprechend im Entwicklungssystem programmiert und in die Produktionsumgebung transportiert.

2. Einführung des Rollenkonzeptes für SAP BusinessObjects Access Control: Die definierten Rollen für SAP BusinessObjects werden entsprechend in der User Management Engine (UME) des darunter laufenden SAP NetWeaver-Systems umgesetzt.

3. Test der Risikoanalyse mit Beispielrollen: Mit speziellen Testrollen, die z. B. schon „wissentlich“ Risiken enthalten, werden Testrollen vorbereitet, mit deren Hilfe die implementierten Risiken getestet werden.

3.4.3.3 UNTERNEHMENSWEITES ROLLENKONZEPT

Variante A:

1. Hochladen der Backend-Rollen und sukzessive „Bereinigung": Die bestehenden Backend-Rollen werden entsprechend in SAP BusinessObjects Access Control hochgeladen und auf bestehende Risiken analysiert. Beim Hochladen werden entsprechend die Rolleneignerattribute und weitere Attribute wie organisatorische Zuordnungsinformationen (Division, Abteilung, Vertreter etc.) zugeordnet. Bei der Analyse werden die Rollen in weitere Teilrollen (falls Funktionstrennungskonflikte bestehen) getrennt.

2. Notwendige Nachpflege der organisatorischen und sonstigen Berechtigungsreichweiten: Organisatorische Berechtigungen (Buchungskreis, Kostenstellen etc.) plus weitere Berechtigungen müssen mit Hilfe der Komponente „Unternehmensweites Rollenkonzept" nachgepflegt werden.

Variante B und C:

1. Implementierung des neuen Rollenkonzeptes: Die in der Designphase neu erstellten Rollen werden entsprechend mit der Komponente „Unternehmensweites Rollenkonzept" implementiert und Rolleneigner und die weiteren organisatorischen Attribute (wie in Variante A) zugeordnet. Mit Hilfe der Risikoanalyse werden, falls notwendig, bestehende Konflikte im Rollendesign weiter bereinigt. Entsprechend wird auch nochmals das Rollendesign angepasst.

2. Notwendige Pflege der organisatorischen und sonstigen Berechtigungsreichweiten: Organisatorische Berechtigungen (Buchungskreis, Kostenstellen etc.) plus weitere Berechtigungen müssen dann mit Hilfe der Komponente „Unternehmensweites Rollenkonzept" oder im „Rollout-Verfahren" nachgepflegt werden.

3.4.3.4 GESETZESKONFORMES BENUTZERMANAGEMENT

1. Implementierung der Workflows für Benutzer- und Rollenmanagement: Implementierung der notwendigen Änderungsmanagementprozesse für:

   > Beantragung von Rollen und Berechtigungen durch die Fachbereichsanwender.
   > SAP-Rollenänderungsantrag, Neuanlage oder Löschen einer Rolle in einem bestimmten Informationsverantwortungsbereich mit der Komponente „Unternehmensweites Rollenmanagement".
   > Passwort-Änderungs- oder -Rücksetzungsantrag.
   > Definition einer neuen Risikodefinition oder Änderung bzw. Löschung einer bestehenden Risikodefinition.
   > Zuordnung einer kompensierenden Kontrolle zu „risikobehafteten" Anwendern, falls dies nicht schon im Rollenbeantragungsprozess durchgeführt wurde.
   > Änderung oder Neuanlage bzw. Löschung von kompensierenden Kontrollen im bestehenden Katalog.
   > Workflow für Superuser-Zugriffe.

2. Implementierung der Integration mit der Identity & Access-Management-Lösung: Durchführung der technischen Integration mit der gefundenen Identity & Access-Management-Lösung (idealerweise SAP NetWeaver Identity Management). Anpassung der Integrationsworkflows und Implementierung der Integration mit Hilfe der vorgesehenen Webservices.

3.4.3.5 SUPERUSER PRIVILEGE MANAGEMENT

Implementierung des Superuser Privilege Management: Die definierte Richtlinie für das Superuser Privilege Management und die entsprechenden Superuser-IDs werden mit Hilfe der Komponente Superuser Privilege Management umgesetzt. Die entsprechenden Eigner der Superuser-IDs werden benannt und eingetragen.

3.4.3.6 TESTDURCHFÜHRUNG

Durchführung der Tests mit den definierten Testfällen: Die in der Design- und Blueprintphase aufgebauten Testskripte werden nun für die einzelnen Komponenten und Prozesse durchgeführt:

- Risikoanalyse
- Technische Batchprozesse
- Änderungsworkflows (Provisionierung)
- Integrationsprozesse für die Identity & Access-Management-Lösung
- Superuser-Privilege-Zugriffsmanagement
- Optional: Rollentests nach den vorgegebenen Geschäftsprozessen, falls ein Reengineering für die SAP-Rollen durchgeführt werden soll. Auf jeden Fall sollte dies auch für die neu entwickelten Rollen bei Variante A gelten.

3.4.3.7 FACHBEREICHS-TRAINING

Trainingsdurchführung für Schlüsselbenutzer: Die Schlüsselbenutzer aus den Fachbereichen sollten nun entsprechend in der Verwendung der neuen Lösungen geschult und eingeführt werden. Hierzu sind vorher auf die Organisation abgestimmte Schulungsunterlagen zu erstellen, die die Unternehmensspezifika abdecken. Das Training kann als „Train the Trainer"-Konzept ausgerollt werden, um in späteren Phasen den neu ausgebildeten Trainern die Ausbildung der weiteren Anwender zu übertragen. Auf diese Weise kann das „Buy-In" von Seiten der Fachbereiche gestärkt werden.

3.4.4 PHASE PRODUKTIONSVORBEREITUNG („ROLLOUT")

In der Rollout-Phase wird nun ein Pilot für den User Acceptance Test ausgeführt und dann SAP BusinessObjects Access Control in der Fläche ausgerollt. Hier stehen die Optionen „sukzessiver Rollout" bzw. „Big Bang", deren Vor- bzw. Nachteile in einem späteren Kapitel besprochen werden, als Alternativen zur Verfügung. Auch werden in dieser Phase der spätere Support und der Betrieb der Lösung vorbereitet. Das für den Support und den Betrieb der Lösung vorgesehene Team sollte dabei den User Acceptance Test schon begleiten und entsprechend eigenständig eigenes Wissen aufbauen.

Die folgenden Arbeitspakete sollten nun durchgeführt werden:

1. **Durchführung Pilot und User Acceptance Test:** Nach erfolgreicher Implementierung aller Risiken, Workflows und auch neu definierten Rollen müssen diese einem großen Kreis von Fachbereichsteilnehmern, z. B. aus dem Finance & Controlling Bereich zugeordnet werden. Diese müssen dann anhand der definierten Testfälle und Testskripte die entsprechenden Tests mit Begleitung des Supportteams durchführen.
   Bei einem positiven Test kann dann eine Abnahme des Systems durch das Projektleitungskommittee erfolgen und die weiteren Rollouts können angegangen werden.

2. Rollout-Vorbereitung: In der Vorbereitung des Rollouts müssen nun sämtliche notwendigen Attribute der Benutzer (Rollenzuordnung), alle Rolleneigner, organisatorischen Ausprägungen etc. erfasst werden und für die Rollouts dokumentiert werden.

3. Vorbereitung der Support- und Betriebsphase: Aufgrund der Erfahrungen des durchgeführten Piloten und des Trainings wird der Support der Lösung und auch der Betrieb vorbereitet. Hierzu wird der Helpdesk geschult und eine Knowledge-Datenbank aufgebaut.

4. Rollout der Lösung in die weitere Organisation:
   Variante A: Sukzessiver Rollout: Hierbei wird schrittweise vorgegangen und die Lösung entweder für weitere Systeme oder weitere Fachbereiche und Geografien ausgerollt. Hierzu werden weitere Trainings und Schulungen durchgeführt.

   Variante B: Big-Bang-Rollout: Hierbei wird für alle Systeme, Fachbereiche und Geographien ein Rollout, z. B. über ein Wochenende, durchgeführt. Der Aufbau aller notwendigen Rollenzuordnungen, Rolleneigner-ausprägungen etc. wird zuvor vorbereitet.

3.4.5 PHASE PRODUKTIVSTART („SUPPORT“)

Nach erfolgtem Rollout und offizieller Abnahme der eingeführten SAP BusinessObjects Access Control-Lösung kann nun das System offiziell in die Support- und Betriebsphase überführt werden.

Hierzu wird entsprechend der Helpdesk instruiert und das technische Supportteam überwacht die Batchprozesse und Änderungsmanagementprozesse. Zudem überwacht das Risikomanagement die Einhaltung der eingeführten Zugriffssteuerungsprozesse.

3.4.6 IMPLEMENTIERUNGSSZENARIO („SUKZESSIVE“ VERSUS „BIG BANG“)

Wie im vorigen Kapitel dargestellt, kann die Einführung von SAP BusinessObjects Access Control in die gesamte Organisation eines Unternehmens sukzessive oder über einen Big Bang erfolgen. In beiden Fällen sollte eine entsprechende Vorbereitung mit der Strategie-, Design- und Implementierungsphase des Piloten erfolgen.

Bei der sukzessiven Einführung in die Gesamtorganisation sollten folgende Faktoren zunächst betrachtet und evaluiert werden:

- Auswahl der wichtigsten Geschäftsprozesse und der dabei involvierten Fachbereiche: Meist bietet sich in der ersten Phase ein wichtiger Nebenprozess an, wie z. B. der Einkaufsprozess von Gebrauchsgütern.
- Danach müssen die für diesen Geschäftsprozess notwendigen SAP- oder Non-SAP-Systeme ausgewählt werden. Im optimalen Fall sollte dies nur ein System umfassen, um die Komplexität nicht zu erhöhen.
- Auch müssen die Ländergesellschaften ausgewählt werden, die bei der ersten Ausrollphase involviert sein sollen. Auch hier bietet sich an, dass zunächst mit einem Land begonnen wird. Dies hängt vor allem davon ab, ob die Geschäftsprozesse harmonisiert worden sind und nicht zu viele Ausnahmen existieren. Sind die Prozesse harmonisiert, so können auch mehrere Länder in den Rollout einbezogen werden. Ein limitierender Faktor ist die Teamgröße des zur Verfügung stehenden Rollout-Supportteams, da eventuell an verschiedenen Standorten parallel Unterstützung angeboten werden muss.

- Ein weiterer Faktor, der bei der sukzessiven Methode betrachtet werden muss, ist das Vorhandensein eines SAP-Rollenkonzeptes, welches schon zu einem hohen Maß harmonisiert ist und für welches eindeutig die organisatorischen Attribute und Rolleneigner zugeordnet werden können. Ist dies nicht der Fall, so müssen die Abhängigkeiten des Rollendesigns mit anderen Geschäftsprozessen und Fachbereichen analysiert werden. Ist das Rollenkonzept auf Basis von Aufgabenrollen und nicht auf positionsbasierten Rollen aufgebaut, welche auch Funktionalitäten und Berechtigungen anderer Fachbereiche angrenzender Geschäftsprozesse umfassen, so lässt sich ein sukzessiver Rollout einfacher durchführen, da sich in diesem Fall der Umfang der zu migrierenden Rollen und auch die Organisationseinheiten leichter eingrenzen lassen. Die gegenseitigen Abhängigkeiten sind somit geringer, sodass die notwendigen Abstimmungsaufwände zwischen den Fachbereichen kleiner sind.

Wie der Name schon symbolisiert, werden bei einer Big-Bang-Einführung alle neuen Workflows inklusive des Risikomanagements und eventuell alle neu definierten Berechtigungen für alle Geschäftsprozesse und daran beteiligte Fachbereiche sowie SAP- und Non-SAP-Systeme z. B. über ein Wochenende eingeführt. Alle Schritte der Implementierungsphase müssen durchlaufen und auch ein erfolgreicher Pilot durchgeführt sein. Die Einführung kann speziell bei einem notwendigen Reengineering des Rollenkonzeptes auch parallel zum bestehenden Berechtigungskonzept erfolgen, wenn über einen gewissen Zeitraum von z. B. zwei Wochen den Anwendern das neue bereinigte Rollenkonzept parallel zum bestehenden zugeordnet wird und dann später die alten Rollen entzogen werden. Den limitierenden Faktor bei einer Big-Bang-Einführung stellt in der Regel der notwendige Support dar, der normalerweise unmittelbar nach einer Einführung notwendig ist.

Folgende Vor- und Nachteile sind bei beiden Einführungsszenarien zu beachten.

Vorteile einer sukzessiven Einführung:

- Das gesamte Einführungsrisiko ist geringer, da erst nach einer Stabilisierung eines Geschäftsprozessbereiches mit dem nächsten begonnen werden kann. Zudem kann zunächst mit Geschäftsbereichen begonnen werden, die für das Unternehmen weniger kritisch sind, wenn eventuell Ausfallzeiten des SAP-Systems auftreten würden oder einzelne Mitarbeiter ihre geschäftskritischen Arbeiten nicht ausführen könnten.
- Es könnte ebenfalls zunächst mit einem weniger geschäftskritischen SAP-System begonnen werden.
- Das Projektteam muss für den notwendigen Support nach dem Rollout nur einen überschaubaren Fachbereich betreuen und nicht eine gesamte Organisation, z. B. eine Länderorganisation. Es muss daher das Rollout-Team nicht verstärkt werden.
- Der Schulungsbedarf kann auf wenige Schlüsselanwender begrenzt werden.

Nachteile einer sukzessiven Einführung:

- Die Abgrenzung der Geschäftsprozesse und Bereiche sowie deren Abbildung auf die SAP-Systeme können sich bei komplexen Organisationen schwierig gestalten.
- Speziell die Risikomatrixfestlegung muss schon für alle Geschäftsprozesse durchgeführt werden, da die kritischen Funktionstrennungsprobleme auch quer zu parallel verlaufenden Geschäftsprozessen auftreten können.
- Auch bei einer notwendigen Einführung eines überarbeiteten Rollenkonzeptes lässt sich die Abgrenzung zwischen den Geschäftsbereichen oftmals schwierig gestalten, sodass das Reengineering eigentlich für die wichtigsten Geschäftsprozesse parallel durchgeführt werden müsste, da auch Funktionstrennungskonflikte übergreifend zu Geschäftsprozessen vorhanden sind, falls die Anwender (wie im Normalfall) in mehreren Prozessen involviert sind.

> Nach dem Ausrollen eines Fachbereichs ist es eigentlich noch nicht möglich, die entsprechenden Workflows und Self-Services gesamtheitlich live zu schalten, da ansonsten in den betroffenen SAP-Systemen eventuell eine nicht handhabbare Mixtur aus Alt- und Neukonzepten entsteht. Die Änderungen in den ausgerollten Fachbereichen sollten daher minimal sein.

Die Vor- und Nachteile eines Big-Bang-Rollouts stellen sich gerade umgekehrt dar. In der Regel kann in den meisten Fällen nur ein sukzessiver Rollout durchgeführt werden, da bei einem Big Bang die notwendige Support- und Schulungsunterstützung nicht im Einführungsteam verfügbar ist. Auch ist die Rollout-Koordination bei einem Big Bang nur mit entsprechend hohen Aufwänden realisierbar.

3.5 RISIKOBASIERTES BERECHTIGUNGSMANAGEMENT

Das Hauptziel eines Unternehmens, welches SAP BusinessObjects Access Control einführt, sollte speziell der Aufbau eines risikobasierten Managements der Vergabe von SAP-Berechtigungen sein. Eine Berechtigungssteuerung nach dem sogenannten „Need to know"-Prinzip, welches viele Sicherheitsstandards, wie z. B. auch ISO 27001/2, fordern, ist in der Praxis eigentlich nicht umsetzbar und führt in der Regel immer zum gleichen Resultat, dass speziell Fachbereiche genau „Need to know" für die Beantragung von Berechtigungen für die Durchführung von Geschäftsprozessschritten für sich selbst beanspruchen und das daher meist kein adäquates Instrument zur Steuerung der Berechtigungsvergabe darstellt.

Besser ist die Steuerung der Berechtigungsvergabe über vorher mit den Fachbereichen bzw. der Organisation festgelegte fachbereichsspezifische Business-Funktionen und Geschäftsprozessrisiken, wie sie z. B. das fehlende Vier-Augen-Prinzip, kritische Funktionalitäten (SAP T-Codes) oder auch der Zugriff auf kritische Unternehmensdaten (die mit Hilfe von Displayberechtigungen gesteuert werden können) darstellen. Dabei sollte zuvor eine eindeutige Risikodefinition mit den Fachbereichen, basierend auf einer unternehmensweiten Richtlinie, festgelegt werden, die die Risikolevel (niedrig, mittel, hoch und sehr kritisch) vorgibt.

SAP BusinessObjects Access Control liefert eine Risikomatrix auf Basis eines Best-Practice-Ansatzes aus, der aber in jedem Fall nicht einfach „blind" übernommen werden sollte, sondern der auf jeden Fall mit den einzelnen zuständigen Fachbereichen abgestimmt und ergänzt bzw. reduziert werden muss. Zudem sollten mit jedem Fachbereichsverantwortlichen (also z. B. Finance) oder auch Geschäftsprozesseigner (also, z. B. Order To Cash) auch ein jeweiliger Risikoeigner festgelegt werden, der die Autorität hat, den Risikolevel eines jeweiligen Zugriffsrisikos und auch eventuell neue Risiken bestimmen zu dürfen. Der Risikoeigner sollte auch später, sobald die operative Einführung der SAP BusinessObjects Access Control-Lösung erfolgt ist, nur berechtigt sein, Risikodefinitionen einschließlich der Risikolevels in Absprache mit dem Compliance Officer oder auch Risikomanager des Unternehmens ändern zu dürfen. Dies bedeutet, dass der Änderungsprozess für Risikodefinitionen auf jeden Fall ebenfalls einem genau festgelegten Änderungsmanagementprozess unterliegen muss. Bei der erstmaligen Festlegung der Risikomatrix mit den Fachbereichen bei der Einführung der SAP BusinessObjects Access Control-Lösung muss aber auf jeden Fall eine Abnahme der Risikodefinitionen durch die verantwortlichen Fachbereiche erfolgen, da ansonsten später im Betrieb (d. h. bei der Provisionierung von Benutzern und Berechtigungen) wieder „Diskussionen" über die Risikoklassifizierung erfolgen könnten, falls es bei der Zustimmung für Berechtigungen zu Risikoidentifikationen kommt.

Daher ist ebenfalls eine entsprechende verbindliche Richtlinie festzulegen, die den im Provisionierungsprozess beteiligten Personen eine eindeutige Handlungsanweisung im Falle von sehr kritischen, hohen, mittleren und niedrigen Risiken zur Hand gibt. So könnte z. B. bestimmt werden, dass im Falle eines möglichen Auftretens von sehr kritischen Risiken, falls einem Benutzer eine bestimmte Rolle zugewiesen wird, dieser Antrag in jedem Fall abzulehnen ist. Oder dass im Fall von hohen Risiken auf jeden Fall eine kompensierende Kontrolle bei der Zustimmung zuzuordnen ist. Dass bei mittleren und niedrigen Risiken dagegen auch die Zustimmung für den Antrag erfolgen kann, wenn eine entsprechende Begründung im Beantragungsprozess festgelegt und dokumentiert ist. Auf diese Weise erfolgt die Zuordnung von Berechtigungen zu den Benutzern nicht mehr auf dem „Need to know"-Prinzip und den damit allseits verbundenen Diskussionen, was nun wirklich „Need to know" darstellt, sondern auf Basis von eindeutig definierten Funktionen und Zugriffsrisiken, welcher ein Berechtigungsantrag eines Anwenders inhärent beinhalten könnte. Auf diese Weise wird ein klarer Risikomanagementprozess für die Berechtigungsvergabe festgelegt, der Berechtigungsnotwendigkeit („Need to know" aus dem Geschäftsprozess heraus) und Berechtigungsrisiken miteinander abwägt.

Wichtig ist es in diesem Kontext auch, effektive kompensierende Kontrollen festzulegen, die, falls ein Zugriffsrisiko nicht vermeidbar ist, die Auswirkung des Risikos mildern und eindämmen. Dies können z. B. manuelle Kontrollen oder aber auch direkte im SAP-System verankerte kompensierende Kontrollen (z. B. Berichte) sein. Kompensierende Kontrollen müssen dabei wieder einem Eigner zugeordnet sein, der den Inhalt der Kontrolle und auch den Durchführenden der Kontrolle festlegt. Die Festlegung von Kontrollen muss ebenfalls einem Änderungsmanagementprozess folgen. Da kompensierende Kontrollen einen nachgelagerten Ansatz verfolgen und daher meist in der Ausführung und Dokumentation aufwendig sind, sollte die Anzahl nicht „wildwuchsmäßig" später in der operativen Phase erhöht werden, da ansonsten das Management der Kontrollergebnisse, welche in das interne Kontrollsystem des Unternehmens überführt werden sollten, fast unmöglich wird. Denn Ausnahmen, sprich Irregularitäten, müssen schnell durch den Fachbereich und auch den Risikomanager erkannt werden, damit entsprechend Gegenmaßnahmen eingeleitet werden können. Das entsprechende Änderungsmanagement für die Risikofestlegung und auch der kompensierenden Maßnahmen kann ebenfalls mit SAP BusinessObjects Access Control eingeführt werden. Hierfür wird mit Hilfe des Compliant User Managements und des darin enthaltenen Workflow-Systems auch der Workflow zur Steuerung der Risikodefinition und der hierfür notwendigen kompensierenden Kontrollen festgelegt.

Eine häufig verwendete kompensierende Kontrolle ist das Superuser Access Management. In diesem Fall wird dem Anwender temporär eine höhere Berechtigung zugeordnet, welche er mit einem hierfür festgelegten Beantragungsprozess und einer notwendigen Begründung beantragen kann. Der Eigner einer Superuser-ID kann dem Antrag stattgeben, wenn die Notwendigkeit aus dem Geschäftsprozess heraus gegeben ist. In diesem Fall werden aber mit Hilfe eines verbesserten Monitorings im System die Aktivitäten des Anwenders im System mitgeschrieben und müssen später, wenn die Superuser-Berechtigung wieder beendet wurde, ausgewertet werden. Das Ergebnis sollte in der festgelegten kompensierenden Kontrolle dokumentiert und so in das interne Kontrollsystem einfließen.

Werden notwendige kompensierende Kontrollen durch den zugeordneten Durchführungsverantwortlichen nicht durchgeführt, so kann in SAP BusinessObjects Access Control ein entsprechendes Alerting festgelegt werden, das z. B. den Risikomanager des Unternehmens darüber informiert, dass ein Versäumnis in der Durchführung der kompensierenden Kontrolle vorliegt und sich daher z. B. das Betrugsrisiko (bei fehlendem Vier-Augen-Prinzip) erhöht hat. Er hat dann die Möglichkeit, die Durchführung der Kontrolle einfacher und effektiver durchzusetzen.

Insgesamt erhält man auf diese Weise ein „rundes" Risikomanagementkonzept, mit dessen Hilfe das sogenannte „Need to know"-Prinzip eindeutiger und besser umgesetzt werden kann.

3.5.1 ABGRENZUNG VON VERANTWORTUNGSBEREICHEN

Um den Risikomanagementprozess für das Berechtigungsmanagement in einem Unternehmen erfolgreich einzuführen, müssen die Aufgaben und Verantwortungsbereiche für die am Provisionierungsprozess für die Berechtigungsvergabe beteiligten Personen klar voneinander abgegrenzt werden. Zudem müssen die Fachbereiche in diesen Prozess einbezogen werden, da sie ansonsten ihre Verantwortung nicht akzeptieren werden und entsprechend, wie in der Vergangenheit geschehen, das Berechtigungsmanagement komplett als Aufgabe dem Informationstechnologiebereich (IT) übertragen. Indes sollte die IT nur eine unterstützende Verantwortung übernehmen und nicht eine, die die Entscheidung für die „Zuordnung" von Berechtigungen trägt. Denn der IT-Bereich hat im Normalfall keine genaue Kenntnis über die Geschäftsprozesse und kann daher die Vertraulichkeit von Informationen und auch mögliche Geschäftsprozessrisiken nicht einschätzen, geschweige denn die entsprechende Entscheidung fällen.

Folgende im Unternehmen existierende Positionen sollten dabei die folgenden Aufgaben und Verantwortungen übernehmen:

Compliance Officer:
Falls diese Position im Unternehmen etabliert ist, ist die Aufgabe des Compliance Officer, die exakten Vorgaben für die Einhaltung von den für das Unternehmen vorgeschriebenen Gesetzen zu machen. Auch die Entwicklung der entsprechenden Richtlinie für das Berechtigungsmanagement fällt in dessen Aufgabenbereich. So muss sie/er darin auch die weiteren Rollen und Verantwortlichkeiten im Berechtigungsmanagement festlegen. Zudem werden vom Compliance Officer die genauen Berichtsnotwendigkeiten festgelegt und sie/er muss mit Audits deren Einhaltung regelmäßig kontrollieren. Zudem muss der Compliance Officer dafür Sorge tragen, dass die im Zusammenhang mit dem Berechtigungsmanagement festgelegten kompensierenden Kontrollen in das interne Kontrollsystem überführt werden und nach den gesetzlichen Vorgaben gemanagt werden.

Risikomanager:
Falls im Unternehmen ein Risikomanager verankert ist (Anmerkung: Oftmals übernimmt dieser auch die Funktion des Compliance Officers), so ist es dessen Aufgabe, die genaue Risikobewertung für das Berechtigungsmanagement in Übereinstimmung mit der konzernweiten Richtlinienvorgabe festzulegen. Hierzu gehören die Bewertungsschemata für die Festlegung der Vertraulichkeit, Verfügbarkeit und Integrität von Geschäftsinformationen und Ableitung der Risikodefinitionen und Risikolevel. Diese Vorgaben müssen bei der Bewertung der SAP BusinessObjects Access Control-Risiken und bei der Festlegung eigener Risiken durch die Risikoeigner der Fachbereiche berücksichtigt werden. Im späteren operativen Betrieb kann der Risikomanager als überwachende Institution in den Provisionierungsprozess mit eingebunden werden. Er sollte dann überwachen, dass die Risikobewertungen durch die Fachbereiche im Provisionierungsprozess und auch im Rollenänderungsmanagement entsprechend der Richtlinie durchgeführt werden.

Risikoeigner:
Pro Fachbereich oder auch Geschäftsprozess (Anmerkung: dies hängt von der Strukturierung des Unternehmens ab) müssen Risikoeigner für die Risiken des Fachbereichs festgelegt werden. Dieser muss die Befugnis bekommen, die Risikolevel und auch Risikodefinitionen im Namen des Fachbereichsvorstandes oder Geschäftsprozesseigners festlegen zu dürfen. Hierfür benötigt er die Unterschriftsberechtigung. Auch muss der Risikoeigner später bei jedweder Beantragung zur Änderung einer bestehenden Risikodefinition seine Genehmigung erteilen.

Eigner für kompensierende Kontrollen:
Auch bei der Festlegung von kompensierenden Kontrollen zur Eindämmung des Risikos, falls Benutzer aufgrund ihrer Berechtigungen als kritisch einzustufen sind, muss ein Eigner zur Festlegung der Kontrolle aus dem betroffenen Fachbereich oder Geschäftsprozessbereich festgelegt werden. Der Eigner muss dabei nicht selbst die notwendigen Kontrollschritte durchführen, sondern muss die Inhalte, Dokumentationspflichten und den Kontrollausführenden festlegen. Der Eigner hat Sorge zu tragen, dass die Kontrolle zudem in der vorgesehenen Frequenz durchgeführt wird. Zudem muss er die Ergebnisse kontrollieren und bei entsprechender Identifikation von Verstößen oder Irregularitäten die entsprechenden Schritte zur Auflösung der Irregularität einleiten. Hierzu muss zudem ein klarer Eskalationsweg festgelegt werden. Es ist möglich, dass die Position Risikoeigner und Eigner einer hierfür notwendigen kompensierenden Kontrolle durch eine Person übernommen wird. Wieder ist es notwendig, dass bei einer Neuanlage einer kompensierenden Kontrolle oder auch bei der Änderung einer bestehenden der Eigner des Fachbereichs involviert wird und dieser zustimmt.

Rolleneigner:
Eine sehr wichtige Voraussetzung für den effektiven Einsatz von SAP BusinessObjects Access Control ist die Bestimmung von Rolleneignern aus den Fachbereichen, die bei entsprechender Anfrage einer Rolle durch einen Anwender um Zustimmung gefragt werden. Sie sollten zudem die Risikoanalyse auf Basis einer „Was wäre wenn"-Analyse durchführen (Anmerkung: dieser Schritt ist inhärent im Workflow von SAP BusinessObjects Access Control hinterlegbar) und dann auf Basis der festgelegten Richtlinie entscheiden, ob die in der Rolle enthaltenen Berechtigungen dem Antragsteller zugeordnet werden dürfen oder nicht, bzw. ob eine kompensierende Kontrolle notwendigerweise zugeordnet werden muss. Die Durchführung dieser Analyse kann dann in einem nachfolgenden Zustimmungsschritt durch den Risikomanager überprüft werden.

Internal Audit:
Internal Audit sollte in der finalen Abnahme der Risikomatrix beteiligt werden. Zudem muss die Einhaltung der Prozesse und Änderungsbelege durch Internal Audit überprüft und überwacht werden.

Informationstechnologie (SAP Competence Center):
Das SAP-Berechtigungsteam, welches früher vor allem ausführende Befugnis hatte, wird durch den Einsatz von SAP BusinessObjects Access Control in eine mehr beratende und überwachende Funktion zurückgedrängt. Es ist Aufgabe des SAP-Berechtigungsmanagement-Teams, das „Funktionieren" der Prozesse sicherzustellen und auch beratend für die Fachbereiche tätig zu sein. Zudem sollten nach wie vor das Berechtigungsdesign und die dafür notwendigen technischen SAP-Rollen in der ersten Implementierung durch Enterprise Role Management in der Führung bleiben. Es sollten hierzu die fachlichen Anforderungen aus den Fachbereichen aufgenommen werden und anhand des vorgegebenen Rollenkonzeptes in eine technische Umsetzung überführt werden. Bei entsprechender Änderung einer bestehenden Rolle oder Aufsetzung einer neuen Rolle muss aber auf jeden Fall der Rolleneigner des Fachbereichs zustimmen und entsprechend auf Vorhandensein eines Risikos hin überprüfen. Auch muss der SAP-Betrieb die notwendigen technischen Änderungen für die Lösung selbst durchführen und wie bei jeder anderen SAP-Software selbst die technische Überwachung durchführen und somit den Betrieb sicherstellen.

3.5.2 CHANGE MANAGEMENT POLICY + RISIKOPOLICY

Wie schon in der Festlegung der Verantwortungsbereiche beschrieben, ist die Festlegung einer Richtlinie zur Festlegung von Risiken, der entsprechenden Festlegung von Risikolevel, der notwendigen kompensierenden Kontrollen und auch einer Handlungsanweisung für die Fachbereiche bei der Provisionierung von Rollen und Berechtigungen ein wichtiger Schritt. Als Grundlage für die Festlegung von Risiken kann z. B. die Bewertung der im Geschäftsprozess verarbeiteten Informationswerte genommen werden, die dann mit Hilfe von Vertraulichkeits-, Integritäts- und Verfügbarkeitsanforderungen bewertet werden können. Dadurch kann z. B. festgelegt werden, dass schon der reine Displayzugriff auf Stammdaten von Stücklisten ein Risiko für das Unternehmen darstellt, wenn diese Informationen einen bedeutenden Wettbewerbsvorteil für das Unternehmen darstellen. Auch bei entsprechenden Finanztransaktionsdaten kann durch die entsprechende hohe Integritätsanforderung festgelegt werden, dass ein Vier-Augen-Prinzip bei der Weiterbearbeitung, z. B. Auslösung einer Buchung, zwingend erforderlich ist, um betrügerischen Handlungen oder auch einfach „fahrlässiger" Freigabe entgegenzuwirken.

Risiken, die durch betrügerische Handlungen oder einfach durch Fahrlässigkeit begründet sind und die demnach einen direkten hohen materiellen und finanziellen Schaden nach sich ziehen können, sollten als besonders hoch oder sehr kritisch eingestuft werden. Solche Risiken sollten dann im Berechtigungsmanagement z. B. als definitive Vorgabe und Richtlinie für den Rolleneigner und Risikomanager nicht eingegangen werden und müssen entsprechend im Genehmigungsworkflow abgelehnt werden. Auch der Einsatz einer kompensierenden Kontrolle wäre in diesem Fall abzulehnen. In der Richtlinie könnte verankert werden, dass in diesem Fall nur der Superuser Access Management Prozess mit der entsprechenden Protokollierung und Überprüfung des Protokolls als Notmaßnahme zulässig ist.

Risiken, die zu einem Reputationsschaden führen können oder die z. B. auch durch die Verletzung der Vertraulichkeit von Informationen (Preisinformationen, Materialstammdaten, spezifische Stücklisteninformationen, Gehaltsdaten etc.) hervorgerufen werden, sollten als hoch eingestuft werden. Zu dieser Klasse sollten auch Betrugsrisiken zugeordnet werden, die nicht zu einem direkten materiellen oder finanziellen Verlust führen können, wie z. B. fiktive Kundengeschäfte zur „Steigerung" des Unternehmenswertes. In diesem Fall sollte entsprechend in der Richtlinie vorgesehen werden, dass der Rolleneigner und Risikomanager im Genehmigungsworkflow für die Berechtigungsbeantragung nur mit einer entsprechenden Einführung einer kompensierenden Kontrolle zustimmen darf.

Bei mittleren bis niedrigen Risiken, die dadurch entstehen können, dass z. B. Kosten auf falsche Kostenstellen kontiert werden, die allerdings keine Auswirkungen auf die Gesamtbilanz haben, sollte in der Richtlinie für das Rollenantragswesen dem Rolleneigner und Risikomanager vorgegeben werden, dass in diesem Fall eine kompensierende Kontrolle zugeordnet werden sollte, aber dies nicht zwingend erforderlich ist, wenn z. B. im Antragsprotokoll festgehalten wird, warum der Antrag genehmigt wurde und daher das Risiko „bewusst" eingegangen wurde.

Zusammengefasst ist es bei der Einführung von SAP BusinessObjects Access Control wichtig, dass eine solche Richtlinie den später im Änderungsmanagement von Rolleninhalten (also letztendlich den SAP-Berechtigungen) und Rollenzuordnungen zu Endanwendern beteiligten Entscheidern (hauptsächlich Rolleneigner, Risikomanager und Linienvorgesetzte) hilft, die Entscheidungen auf Basis einer klaren Richtlinie und nicht aufgrund von „Gefühlen" zu treffen.
Das Gleiche gilt indes auch für die Definition der Risiken selbst für die Risikoeigner. Es muss dabei als Richtlinie vorgegeben werden, in welchem Fall ein Risiko als „sehr kritisch", hoch, mittel oder niedrig einzuschätzen ist.

3.5.3 REPORTING/MONITORING

Einer der wichtigsten Vorteile, der durch den Einsatz von SAP BusinessObjects Access Control gegenüber traditionellen SAP-Tools (PFCG, SU01 etc.) entsteht, ist die Möglichkeit, für alle durchgeführten Änderungen an Rollen und Rollenvergaben Änderungsprotokolle zu führen, die für einen späteren Audit die entsprechende Evidenz bereitstellen. Durch die Änderungsbelege werden die gesetzlichen Vorgaben und auch die Ziele der internen Kontrolle effizienter erreicht. Zudem können auch freiwillige Compliance-Vorgaben für Security-Normen, wie z. B. der Norm ISO 27001/2, einfacher erfüllt werden.

Eine weitere und sehr wichtige Funktion von SAP BusinessObjects Access Control ist aber durch die geordnete Protokollierung von Aktivitäten und die durchgeführten Änderungen im SAP-System gegeben, wodurch ein Superuser-Management erreicht werden kann. In diesem Fall werden höhere Berechtigungen nur temporär an Antragsteller vergeben und der Antragsteller muss auch eine Begründung angeben, warum sie/er die höheren Berechtigungen für den Geschäftsprozess benötigt. Diese Begründung ist ebenfalls als Auditevidenz später verwendbar. Zudem wird bei der Annahme der höherwertigen Berechtigungen auch die Protokollierung im SAP-System gestartet und die Aktivitäten des Benutzers mit protokolliert. Diese Änderungsbelege müssen dann durch den Eigner der Superuser-ID im Nachgang ausgewertet werden und bei entdeckten Unregelmäßigkeiten müssen die Gegenmaßnahmen über die Eskalationswege ausgelöst werden.

Folgende Grundregeln sollten bei der Einführung eines Superuser Access Managements berücksichtigt werden bzw. in der Richtlinie festgehalten werden:

1. Das Superuser Access Management darf nur für den Notfall verwendet werden, da ansonsten die Gefahr besteht, dass die höherwertigen Berechtigungen für das Tagesgeschäft verwendet werden und nicht für den Notfall. Das eigentliche Berechtigungskonzept würde auf diese Weise unterlaufen werden.

2. Den Superuser-IDs sollten keiner SAP-ALL-Berechtigung zugeordnet werden, sondern wirklich nur höherwertige Berechtigungen beinhalten, welche für den jeweiligen Fachbereich im Notfall notwendig sind. So z. B. für den IT-Bereich die Berechtigung „Öffnen des Mandanten" in einer dedizierten Superuser-ID. Das Gleiche z. B. für den Fachbereich Finanzen und Controlling, wie z. B. „Kontenplan anpassen".

3. Die Eigner der jeweiligen Superuser-IDs müssen verpflichtet sein, die Änderungsbelege nach deren Gebrauch durch einen Antragsteller zu reviewen und nach entsprechenden Unregelmäßigkeiten zu untersuchen. Bei einer entsprechenden Identifikation einer solchen Unregelmäßigkeit sind die Eigner verpflichtet, über einen vorgegebenen Eskalationspfad Gegenmaßnahmen einzuleiten.

4. Bei jeder Beantragung einer Superuser-ID sollte eine nachvollziehbare Begründung durch den Antragsteller gegeben werden.

5. Das Recht, eine bestimmte Superuser-ID für den Notfall verwenden zu dürfen, sollte nur auf Zeit vergeben werden und nicht auf Dauer.

3.6 ROLLENMANAGEMENT

3.6.1 STRUKTURIERUNG/KONZEPTION DER BUSINESS-ROLLEN

Beim Einsatz und der Einführung von SAP BusinessObjects Access Control ist es wichtig, das bestehende Rollenkonzept auf die Voraussetzungen der Lösung anzupassen. Ein wichtiges Grundprinzip ist die Festlegung von Rolleneignern, die aus dem Fachbereich bestimmt werden müssen. Damit dieses Grundprinzip aber eingehalten werden kann, sollte das nachher zu implementierende technische Rollenkonzept einem Business-Rollenansatz folgen. Anhand des Organisationsmodells müssen hierfür zunächst eindeutige Arbeitsplatzbezeichnungen (oder auch Business-Rollen oder Positionen genannt) evaluiert werden. Diese sollten dann, falls diese geografisch unterschiedlich benannt werden, entsprechend in ihrer Bezeichnung harmonisiert werden.

In einem nächsten Schritt muss die Zuordnung der Positionen zu einem Geschäftsprozess durchgeführt werden, sodass ein eindeutiger Geschäftsprozesseigner auf globaler Ebene und ein lokaler Eigner festgelegt werden können. Ein globaler Geschäftsprozesseigner bestimmt dabei die notwendigen Funktionalitäten (z. B. auch SAP-Funktionen), die dieser Position als Aufgaben und Verantwortlichkeiten zugewiesen werden kann. Der lokale Eigner definiert zudem die zugehörigen Berechtigungen, wie z. B. Organisationslevel (Buchungskreise, Werke, Verkaufsorganisationen), für die die Position berechtigt sein wird.

Übersetzt man diese Eignerstrukturen auf die Notwendigkeiten von SAP BusinessObjects Access Control, so wird der globale Geschäftsprozesseigner zum Rolleneigner aus funktionaler Sicht ernannt und muss in den Änderungsmanagementprozess für die Rolle selbst eingebunden werden. Der lokale Geschäftsprozesseigner muss hingegen Eigner für die „abgeleitete" Rolle werden, welche die organisatorischen Berechtigungen enthält. Er muss wiederum in den Rollenprovisionierungsprozess als Haupt-Zustimmungsberechtigter eingebunden werden.

Auf diese Weise werden die Business-Rollen eindeutigen Eignern zugeordnet. Das Prinzip der Informationsverantwortung kann so elegant auf das Rolleneignerprinzip übertragen werden.

De facto hat man auf diese Weise aber auch nur das „indirekte" Rollenkonzept abgebildet, welches auch schon mit einer SAP-HR-Organisationsstruktur abbildbar wäre. Die Nachteile dieses Prinzips sind aber hinlänglich bekannt und ergeben sich meist aus den Ausnahmen im Prozessablauf, die in den verschiedenen Unternehmensteilen „über den Lauf der Jahre" historisch gewachsen sind. Um diese Ausnahmen abbilden zu können und dabei das Informationsverantwortungsprinzip nicht zu untergraben, sollten in jedem Geschäftsprozessbereich neben den positionsbasierten Rollen auch zusätzliche aufgabenspezifische Business-Rollen definiert werden. Diese Aufgaben entsprechen den Ausnahmen in jedem Geschäftsprozessbereich und auch Aufgaben, die der Geschäftsprozessbereich anderen Geschäftsprozessbereichen zur Verfügung stellen kann, bzw. in Rollen übersetzt bedeutet dies, dass diese Rollen durch Mitarbeiter anderer Geschäftsprozessbereiche beantragt werden dürfen, aber nicht die positionsbasierten Rollen. Wiederum werden diese aufgabenspezifischen Rollen dem globalen Geschäftsprozesseigner aus funktionaler Sicht (Stammrolle) und den lokalen Eignern aus berechtigungsspezifischer Sicht zugeordnet.

Dieses Prinzip soll kurz an einem Beispiel erklärt werden: Im Geschäftsprozess „Order To Cash" gibt es eventuell die Position „Key Account Manager", dessen Aufgabe es ist, speziell die wichtigsten Kunden des Unternehmens zu betreuen. Seine spezifischen Aufgaben sind dabei, regelmäßig den Bedarf des Kunden zu erkunden, entsprechend zügig Angebote abzugeben und den Kunden auch immer wieder über neue Angebote zu informieren. Die Aufgaben und Verantwortlichkeiten des Key Account Managers werden daher in der Regel durch den Vertriebsvorstand des Unternehmens festgelegt. Dieser ist somit auch Eigner dieser Position.

Ist der Key Account Manager in einer bestimmten Vertriebsorganisation eines Landes beschäftigt, so wird er nur die Kunden dieses Landes betreuen und auch nur Aufträge für diese Länderkunden und Werke erfassen. Der lokale Vertriebsverantwortliche ist daher der Eigner der spezifischen organisatorischen Berechtigungen. Diese Hauptaufgaben des Key Account Managers bilden sich natürlich entsprechend auf SAP-Funktionalitäten ab und würden dann technisch in eine Hauptrolle des Key Account Managers abgebildet. In der täglichen Arbeit wird aber nun festgestellt, dass der Key Account Manager z. B. auch den Lagerbestand eines bestimmten Produktes abrufen muss, da seine Kunden diese schnelle Auskunft wünschen. Diese Ausnahmeaufgabe sollte daher über eine aufgabenbasierte Rolle des „Logistikbereiches" dem Key Account Manager zur Verfügung gestellt werden.

Auf diese Weise lassen sich Informationsverantwortungsprinzipien durch klare Rolleneignerstrukturen für die Business-Rollen im Unternehmen definieren, die dann mit Hilfe von SAP BusinessObjects und den hierfür vorgesehenen Genehmigungsworkflows und notwendigen Rolleneignern abgebildet werden können.

3.6.2 TECHNISCHE ROLLEN

Das in Kapitel 3.6.1 festgelegte Prinzip für die Business-Rollen, welches einem klaren Informationsverantwortungsprinzip folgt, kann technisch sehr effizient mit einem RBE-Ansatz (Reverse Business Engineering) oder einem funktionsorientierten Redesign-Ansatz umgesetzt werden, falls eine solche Struktur im Unternehmen nicht schon existiert. Zudem erleichtert das Informationsverantwortungsprinzip die Umsetzung in SAP BusinessObjects Access Control, welches sich dieses ebenfalls als Grundprinzip zunutze macht.

Die Abbildung des Business-Rollen-Designs (RBE) in ein technisches Konzept erfolgt dabei wie folgt:

1. Im ersten Schritt werden alle verfügbaren Funktionen (T-Codes, Reports, Webdynpro-Anwendungen etc.) den globalen Geschäftsprozesseignern zugeordnet. Sie werden dann Eigner der jeweiligen Funktionen, die als Teilschritt eines Gesamtgeschäftsprozesses benötigt werden. Die Zuordnung der Funktionen muss von allen Geschäftsprozesseignern akzeptiert und abgezeichnet werden.

2. Mit Hilfe des Organigramms des Unternehmens oder der Organisation werden die vorhandenen Positionen (wie z. B. Key Account Manager, Einkäufer, Vertriebsleiter etc.) im Unternehmen bestimmt und festgelegt. Die Bezeichnungen sollten dabei im Unternehmen harmonisiert werden. Die Positionen sollten zudem den Geschäftsprozessbereichen zugeordnet werden.

3. Den Positionen werden im nächsten Schritt die Stelleninhaber zugeordnet, die derzeit diese Business-Rolle innehaben und auch SAP-Anwender sind.

4. Mit Hilfe des ST03 Traces und dem RBE Report werden nun die in der Vergangenheit (mind. 3 Monate) durchgeführten Aktivitäten eines einer Position zugeordneten Stelleninhabers funktional ausgewertet. Im Normalfall, wenn wirklich die Stelleninhaber nur in den ihnen zugeordneten Geschäftsprozessen involviert waren, sollte sich ein nahezu identisches funktionales Nutzungsbild (also Verwendung der T-Codes) unabhängig von den Berechtigungen wie Buchungskreis etc. ergeben. Die Praxis zeigt indes, dass dies in den meisten Fällen nicht der Fall sein wird, sodass in der Regel zunächst die Summe aller verwendeten Funktionen der Stelleninhaber zur Position gruppiert werden muss. Auf diese Weise können für alle Positionen die eigentlich im Geschäftsprozess prozessseitig verwendeten Funktionen zusammen gefasst werden.
5. Eine einfache Umsetzung der so definierten Business-Rollen in technische Rollen ist aber so nicht

möglich, da nun im nächsten Schritt die Eignerschaft (siehe Schritt 1) der verwendeten Funktionen analysiert und damit die analysierte positionsbasierte Rolle technisch in genau eine Hauptarbeitsplatzrolle plus verschiedene Aufgabenrollen zerlegt werden muss. Die Hauptarbeitsplatzrolle (es darf nur eine pro Position sein) erhält man dadurch, dass die zum eigenen Geschäftsprozessbereich gehörenden Funktionen (T-Codes) zusammengefasst werden, die der Schnittmenge aller „getracten" Stelleninhaber entsprechen. Die anderen durchgeführten Funktionen müssen entsprechend zu eigenen Aufgabenrollen des eigenen Geschäftsprozessbereiches zusammengefasst werden, wenn die durchgeführten Funktionen dem eigenen Geschäftsprozessbereich zugeordnet sind (siehe Schritt 1). Die weiteren „nicht-eigenen" durchgeführten Funktionen werden zu technischen Aufgabenrollen des anderen Geschäftsprozessbereiches zugeordnet. Die technische Zerlegung in die jeweiligen Rollen kann aus dem ST03 Trace einfach mit entsprechenden Datenbank-Abfragen gefunden werden.

In diesem Schritt sollte zudem auch eine entsprechende Namenskonvention für Hauptarbeitsplatzrollen und Aufgabenrollen festgelegt werden.

6. Nach der in Schritt 5 vorgestellten Weise werden nun automatisch die technisch relevanten Rollen definiert, die das in Schritt 1 definierte Informationsverantwortungsprinzip einhalten. Da diese aber nur funktional festgelegt wurden, muss nun im nächsten Schritt die entsprechende Ausprägung für die einzelnen Organisationseinheiten durchgeführt werden. Dies erfolgt für die Hauptarbeitsplatzrollen und Aufgabenrollen. Einfach kann dies mit dem „Ableitungsassistenten" der Komponente „Unternehmensweites Rollenmanagement" von SAP BusinessObjects Access Control durchgeführt werden. In dieser Weise kann dann auch gleichzeitig der notwendige Rolleneigner (der lokale Geschäftsprozesseigner) festgelegt werden.

7. Schritt 5 und 6 müssen eventuell iterativ verfeinert werden, da beim Bau der Rollen mit SAP BusinessObjects Access Control auch gleichzeitig die notwendige Risikoanalyse (also Funktionstrennung, kritische Funktionen und Berechtigungen) durchgeführt werden kann und dann sofort eventuelle Risiken erkannt werden können. Ist dies der Fall, so muss, wenn ein solches Risiko erkannt wird, in der Hauptaufgabenrolle der konfliktverursachende Teil am besten in eine weitere dann „kritische" Aufgabenrolle des eigenen Geschäftsprozessbereiches aufgespalten werden. Ein Funktionstrennungskonflikt in einer Aufgabenrolle sollte eigentlich nicht auftreten, da die Aufgabenrolle in der Regel aus maximal 4 Funktionen besteht. Ist dagegen eine kritische Funktion darin enthalten oder auch eine kritische Berechtigung, so muss die Aufgabenrolle als insgesamt kritisch deklariert werden. Ein weiteres Trennen ist aber nicht notwendig oder kann auch nicht durchgeführt werden.

8. Im letzten Schritt werden die in SAP BusinessObjects Access Control implementierten Hauptarbeitsplatzrollen entsprechend wieder der von ihr abgeleiteten Position den entsprechenden Mitarbeitern (Stelleninhabern) zugeordnet. Die Aufgabenrollen können dann entweder ebenfalls initial zugeordnet werden oder werden noch besser von den einzelnen Stelleninhabern wieder per Workflow-System beantragt, um bei einem Auftreten eines Risikos entsprechend sofort per kompensierender Kontrolle dem Risiko entgegenwirken zu können.

Zusammengefasst bietet der Einsatz eines RBE-basierten Konzeptes für den Aufbau der technischen Rollen folgende Vorteile:

1. Die im alten Berechtigungskonzept meist vielfältig vorhandenen Risiken werden durch RBE meist um ca.

60–70 % reduziert, da das Rollenkonzept auf Basis der wirklich nur benötigten Funktionen aufgebaut wird und nicht nach der dem Stelleninhaber über die Jahre zugeordneten Funktionen, die „auch" mit in den einzelnen Rollen vorhanden waren.

2. Auch die Einführungsproblematik, dass Stelleninhaber ihre Arbeit als Teil eines Geschäftsprozesses nicht erfüllen können, wird deutlich reduziert, da das Rollenkonzept nicht Funktionen entfernt, die der Stelleninhaber auch wirklich benötigt. Die große Anzahl von Helpdesk Calls während der Einführung des neuen Rollenkonzeptes, hervorgerufen von unzufriedenen Mitarbeitern, die ihre Aufgaben nicht durchführen können, wird deutlich reduziert.

3. Das Konzept führt ein konsequentes Informationsverantwortungsprinzip ein, welches mit SAP BusinessObjects Access Control sehr gut unterstützt wird, bzw. sogar eine Voraussetzung für dessen effizienten Einsatz darstellt.

Die Umsetzung des funktionsorientierten Redesign-Ansatzes in ein technisches Konzept erfolgt in 5 Schritten:

1. Projektvorbereitung, Einführung und Abstimmung: Erstellung der unternehmensspezifischen Projektdatenbasis/Erstabstimmung mit den Modulverantwortlichen und Fachabteilungen.

   Für die Realisierung der folgenden Projektschritte werden berechtigungsrelevante Daten (z. B. eingestellte Org.-Werte, eigenentwickelte Transaktionen) und wichtige unternehmensspezifische Feldeinstellungen aus dem SAP-System geladen und für das Projekt aufbereitet. Die im Projekt zu berücksichtigenden Organisationseinheiten (Buchungskreise, Werke etc.), die Methodik für die Definition der Arbeitsplätze, die Unternehmensfunktionen sowie die eigenentwickelten Transaktionen werden identifiziert. Ergebnis aus Schritt 1 ist die Auswahl der benötigten funktionalen Bausteine aus dem vorgefertigten Funktionskatalog für die spätere Erstellung der Einzelrollen sowie die Abstimmung der für die Einzelrollen erforderlichen eigenentwickelten Transaktionen.

2. Konfiguration der funktionenbasierten Einzelrollen: Spezifizierung der Einzelrolleninhalte (Funktionsabgleich, Organisationsstruktur, Übernahme berechtigungsrelevanter ORG-Einstellungen, eigenentwickelte Transaktionen) mit den Modulverantwortlichen.

   Es erfolgen nun modulweise die Detailabstimmungen mit den jeweiligen Verantwortlichen (Fachbereich/Key-User und IT-Administration). Mit Hilfe der in Schritt 1 ausgewählten Funktionsbausteine werden die unternehmensspezifischen Prozesse in kurzer Zeit abgebildet, die bereits standardmäßig zugeordneten SAP-Transaktionen abgeglichen und eigenentwickelte Transaktionen integriert. Nach Zusteuerung der Org.-Werte entsteht das Grundraster der Einzelrollen. Die Konfiguration der Einzelrollen wird anschließend – unter Berücksichtigung der Funktionentrennungsanforderungen – toolgestützt durchgeführt. Die Einzelrollen enthalten automatisiert redundanzfreie Kurz- sowie Langnamen, um die jeweilige betriebliche Funktion entsprechend abzubilden.

3. Bestimmung der Rechte je Arbeitsplatz: Zuordnung der Einzelrollen zu arbeitsplatzbezogenen Sammerollen.

   Auf Basis der in Schritt 2 konfigurierten Einzelrollen wird eine Arbeitsplatzmatrix erarbeitet und die jeweils notwendigen Einzelrollen den Arbeitsplätzen (Sammelrollen) zugeordnet. Die horizontal angeordneten Arbeitsplatzfunktionen liefern die leicht verständliche Basis für die Rollenzuordnung der Testuser sowie für die Rollen-/Userverwaltung im späteren operativen Tagesgeschäft.
4. Erstellung Gesamt-Rollenkonzept: Übernahme der zu testenden Rollen in das SAP-Testsystem.

Die erstellten Rollen werden ins Testsystem übertragen und als erster Referenzbestand gesichert. In der Testphase werden die Rollen auf Funktionsfähigkeit und Vollständigkeit geprüft. Eventuell erforderliche Anpassungen in den Rollen werden zeitnah vorgenommen.

5. Testabnahme und Gesamtdokumentation: Änderungen aus der Testphase werden abgestimmt und der Referenzbestand freigegeben.

   Die – über einen softwaregestützten Abgleich nach Testende – analysierten Abweichungen werden mit den Modulverantwortlichen nochmals abgestimmt und der Referenzbestand dabei aktualisiert. Die Rollen für den operativen Einsatz sind fertiggestellt und der End-Rollenbestand = endgültiger Referenzbestand wird freigegeben. Mitlaufend entsteht die Dokumentation sämtlicher Details. Die freigegebenen Rollen werden ins Produktivsystem transportiert.

   Benutzerzuordnung: Nun können die Arbeitsplatzfunktionen = Sammelrollen den entsprechenden Mitarbeitern (Stelleninhaber) sowohl initial als auch per Workflow (Beantragung und Genehmigung) mit dem GRC CUP zugeordnet werden. Beim Auftreten eines Risikos kann sofort per kompensierender Kontrolle dem Risiko entgegengewirkt oder der Antrag abgelehnt werden. Die bestehenden „alten" Rollen im Produktivsystem werden je nach Zuordnung Schritt für Schritt gelöscht.

Zusammengefasst bietet der Einsatz eines funktionsorientierten Redesign-Konzeptes für den Aufbau der technischen Rollen folgende Vorteile gegenüber einer konventionellen Arbeitsweise:

KONVENTIONELL	FUNKTIONSORIENTIERTES REDESIGN-VERFAHREN
Funktionsbestimmung und -definition für das Berechtigungskonzept	Auswahl der Funktionsbausteine aus einem Funktionskatalog
Ermittlung der passenden Transaktionen, die diese Funktionen repräsentieren (inkl. aller Folgetrans-aktionen)	Transaktionsvorschlag der Wissensdatenbank prüfen, bereinigen und ggf. mit den eigenerstellten Transaktionen ergänzen
Ermittlung der Org.-Einheiten, die in diese Funktionen eingesteuert werden sollen! Erstellung der Rollen mit dem PFCG	Auswahl der relevanten Org.-Einheiten aus dem Org.-Tableau und Zusteuerung. Automatisierte Erstellung der Einzelrollen mit durchgängiger Namensvergabe
Definition und Abstimmung der Arbeitsplätze mit Zuordnung der Einzelrollen über PFCG	Matrixgesteuertes Auswahlverfahren und automatische Rollenaggregierung auf Arbeits-platzebene
Dokumentation der Rolleninhalte (Name, Bezeichnung, Transaktionen, Objekte, Felder, Feldwerte)	Automatisch mitlaufende aktuelle Online-Doku-mentation

Abb. 6: Funktionsorientiertes Redesign-Verfahren im Vergleich
Dieses Vorgehensmodell ermöglicht einen straffen Projektansatz mit geringem Zeit- und Ressourcenbedarf

bei hoher Qualität und Erfüllung der gesetzlichen Vorgaben. Durch die Auswahl der vorgefertigten Funktionsbausteine und individuelle Ergänzung wird ein Berechtigungskonzept realisiert, was alle betrieblichen Funktionen – unabhängig von Arbeitsplätzen und Anwendern – konfliktfrei (Funktionstrennung), strukturiert und sauber abgegrenzt abbildet. Organisationsanforderungen sind durch Aggregierung dieser Einzelrollen zu Sammelrollen leicht erstell- und später auch leicht anpassbar; diese Arbeitsplatzfunktionen können direkt einer Organisationseinheit (z. B. im HR-ORG/Eigentümerprinzip) zugeordnet werden. Die automatisierte Namensvergabe mit der detaillierten, aktuellen Dokumentation schafft Transparenz über die Rolleninhalte sowohl für den Fachbereich wie auch für Organisatoren und Revisoren.

Einer der Vorteile des funktionsorientierten Redesign-Verfahrens ergibt sich daraus, dass nicht die bestehenden – über Jahre gewachsenen – Prozesse mit ihren umfänglichen Möglichkeiten im Ist-Zustand abgebildet werden, sondern die Chance genutzt wird, diese so zu strukturieren, wie es für das Unternehmen sinnvoll und optimal handhabbar ist und das Risiko beherrschbar bleibt.

3.7 INTEGRATION ACCESS CONTROL/IDENTITY MANAGEMENT AM BEISPIEL VON SAP NETWEAVER IDM

Wie in Kapitel 2 beschrieben, rücken Pflichten wie die Einrichtung von internen Kontrollsystemen und Risikomanagementsystemen näher in den Fokus von Aufsichtsräten, Vorständen und Geschäftsführern. Dabei spielen Themen wie Funktionstrennung und sichere Berechtigungskonzepte und -systeme eine besonders große Rolle. Neben dem in Abschnitt 2.1 beschriebenen SAP BusinessObjects-Portfolio, ist es in einigen Unternehmen sinnvoll, zusätzlich ein Identity-Management-System als zentrales Berechtigungs- und Identity-Management-System einzusetzen. In vielen Systemlandschaften hat ein Identity-Management-System eine tragende Rolle für das Berechtigungsmanagement sowie für das Management der Identitäten, derer Benutzerkonten und Personenstammdaten. In einigen Fällen findet man bereits ein Identity-Management-System in den Unternehmen vor, welches durch Funktionalitäten von SAP BusinessObjects Access Control ergänzt werden soll. In anderen Projekten soll Access Control zusammen mit einem Identity-Management-System eingeführt werden. Durch den serviceorientierten Aufbau von SAP BusinessObjects Access Control mit der Bereitstellung der Funktionalitäten durch Webservices ergeben sich unterschiedliche Integrationsszenarien.

Eine sehr enge Integration mit Access Control bietet das Identity-Management-System SAP NetWeaver Identity Management 7.1.[17] SAP NetWeaver IdM wird als Provisioning-System mit zentralem Identity Store, im Vergleich zum SAP BusinessObjects Access Control, eher der IT und dem System-Management zugeordnet und bildet vielfach zentrale Systeme zur Verwaltung von Zugriffsberechtigungen, personenbezogenen Daten und Audit-Informationen. Bei einem integrierten Einsatz ist SAP BusinessObjects Access Control nicht an SAP NetWeaver Identity Management gebunden, sondern kann seine Funktionalitäten auch Identity-Management-Systemen von Drittanbietern bereitstellen.[18] SAP NetWeaver Identity Management basiert jedoch genau wie SAP BusinessObjects Access Control (Abschnitt 2.1) auf der SAP NetWeaver-Plattform und stellt für die Integration ein vorgefertigtes Framework zur Verfügung.[19] Bei der Integration von SAP NetWeaver Identity Management mit Access Control spricht die SAP von Compliant Identity Management (CIM).[20] Sowohl die Funktionalitäten von SAP BusinessObjects Access Control als auch die von SAP NetWeaver IdM können durch den serviceorientierten Aufbau anderen Systemen bereitgestellt werden.

Das vorliegende Kapitel baut auf dem zuvor dargestellten Sachverhalt des Leitfadens auf und greift einige

17 SDN, SAP NetWeaver Identity Management 7.1, http://www.sdn.sap.com/irj/sdn/nw-identitymanagement
18 Integration zu IBM Tivoli, SUN IDM und Novell IDM, https://wiki.sdn.sap.com/wiki/display/BPX/Governance%2C%20Risk%2C%20and%20Compliance%20%28GRC%29%20How-To%20Guides
19 SDN, GRC Provisioning Framework - http://www.sdn.sap.com/irj/sdn/index?rid=/webcontent/uuid/b0196981-09d0-2b10-1b96-9b488d34a317
20 SDN, SAP NtWeaver Identity Management 7.1 – Compliant Identity Management, http://www.sdn.sap.com/irj/scn/index?rid=/library/uuid/60a4802f-b6cd-2b10-1ebf-e269d127a634&overridelayout=true

3 SAP BusinessObjects Access Control 5.3

Best Practices zum integrierten Einsatz von SAP BusinessObjects Access Control und SAP NetWeaver Identity Management auf.

- Der Abschnitt 3.7.1 gibt eine kurz Einführung zu SAP NetWeaver Identity Management (SAP NetWeaver IdM) und stellt es SAP BusinessObjects Access Control (SAP BusinessObjects AC) gegenüber.
- Abschnitt 3.7.2 beschreibt Best Practices zu Compliant Identity Management (CIM), indem es drei integrierte Anwendungsszenarien vorstellt, bei denen SAP NetWeaver Identity Management mit SAP BusinessObjects Access Control-Modulen gemeinsam agieren.
- Der Abschnitt 3.7.3 geht kurz auf Auditing-Informationen ein.
- Der Abschnitt 3.7.4 beschreibt aufbauend auf Abschnitt (Access Control Einführung) die Besonderheiten bei der Einführung von Compliant Identity Management.
- Eine Ergänzung zu Abschnitt 3.7.4 und damit zu Berechtigungen und Rollen liefert Abschnitt 3.7.5. Hier wird auch beschrieben, welche Möglichkeiten einer Berechtigungszuweisung bestehen.
- Die Architektur von Compliant Identity Management stellt Abschnitt 3.7.6 dar.
- Die technischen Voraussetzungen für Compliant Identity Management werden in Abschnitt 3.7.7 erläutert.
- Abschnitt 3.7.8 liefert eine Zusammenfassung zu CIM.

3.7.1 EINFÜHRUNG IN SAP NETWEAVER IDENTITY MANAGEMENT

SAP NetWeaver Identity Management ist das Identity-Management-System der SAP, welches heterogene Systemlandschaften mit SAP- und Non-SAP-Systemen im Fokus hat. Das System kann als zentraler Identity Hub eingesetzt werden, welcher personenbezogene Informationen über einen zentralen Identity Store anderen Anwendungen bereitstellt sowie seine Funktionalitäten wie Provisioning und Deprovisioning in den angeschlossenen Systemen über Identity Services[21] zur Verfügung stellt. Damit ergeben sich unterschiedlichste Integrationsszenarien, die nicht Gegenstand dieses Leitfadens sind. Für diesen GRC-Leitfaden wird das Integrationsszenario Compliant Identity Management beschrieben, welches SAP NetWeaver IdM als zentrales Identity-Management-System um Funktionalitäten der Risikoanalyse von SAP BusinessObjects Access Control erweitert. Einen umfassenden Überblick über Funktionalitäten von SAP NetWeaver Identity Management und weitere Integrationsszenarien liefert das Buch „SAP NetWeaver Identity Management" des SAPPRESS Verlags.[22] Im folgenden Abschnitt wird ein kurzer Überblick über SAP NetWeaver Identity Management gegeben.

3.7.1.1 SAP NETWEAVER IDENTITY MANAGEMENT-ÜBERSICHT

21 SDN, SAP NetWeaver Identity Management Identity Service Configuration Guide, http://www.sdn.sap.com/irj/scn/index?rid=/library/uuid/106ecdec-ddfa-2a10-cf89-c2e75482d090&overridelayout=true

22 SAP NetWeaver Identity Management, Loren Heilig, SAPPRESS, http://www.sappress.de/2007

SAP NetWeaver Identity Management besteht aus zwei Komponenten, die jede für sich oder im Verbund verwendet werden können. Die folgende Abbildung zeigt die Komponenten von SAP NetWeaver Identity Management 7.1.

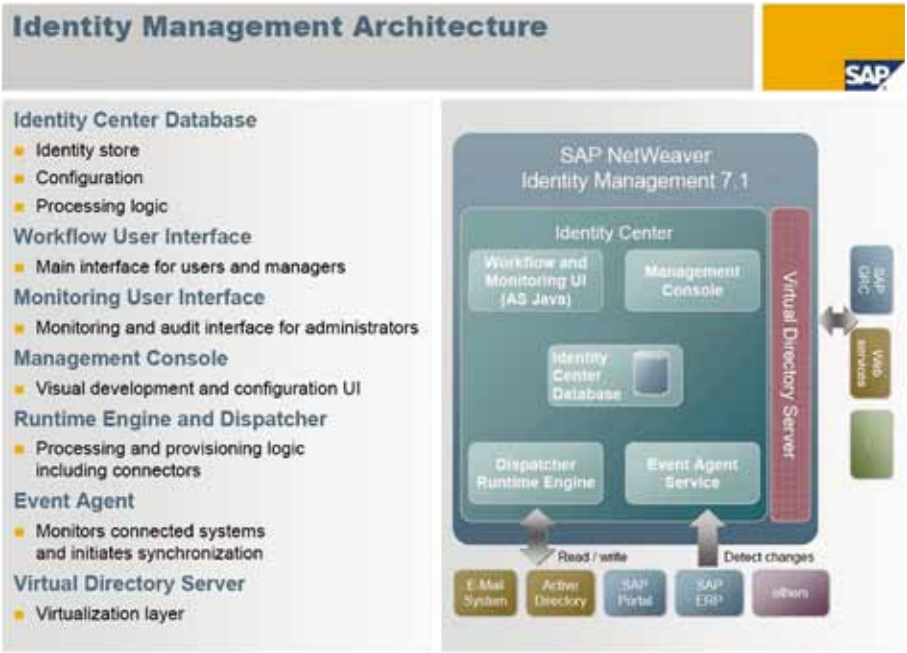

Abb. 7: Übersicht der Komponenten von SAP NetWeaver Identity Management

Die Komponente „Identity Center" wird im folgenden Abschnitt 3.7.1.2 beschrieben, die Komponente „Virtual Directory Server" in Abschnitt 3.7.1.3. Für den integrierten Einsatz von SAP Identity Management mit SAP BusinessObjects Access Control zur kontrollierten Vergabe von ERP-Rollen unter Berücksichtigung von Funktionstrennung mit einer integrierten Risikoanalyse (siehe Abschnitt 3.7.2.1) wird die Komponente „Virtual Directory Server" als eine Art „Middleware" bei der Kommunikation zwischen SAP NetWeaver IdM und SAP BusinessObjects AC eingesetzt.

3.7.1.2 IDENTITY CENTER

3 SAP BusinessObjects Access Control 5.3

Die folgende Abbildung zeigt zunächst die Architektur der SAP NetWeaver Identity Management-Komponente Identity Center in der Version 7.1.

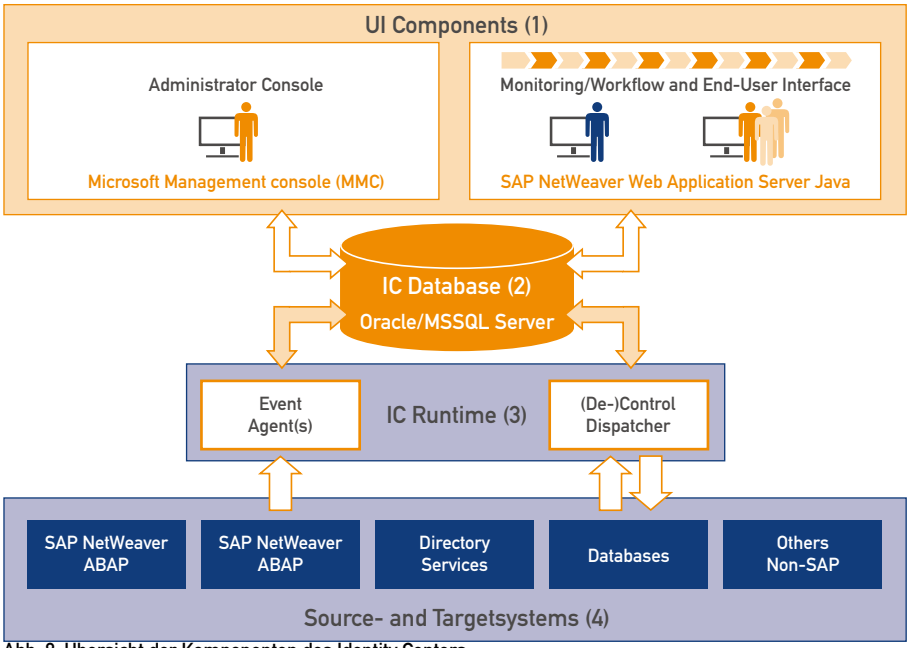

Abb. 8: Übersicht der Komponenten des Identity Centers

Anhand der Abbildung werden die einzelnen Komponenten kurz beschrieben:

1. Das Identity Center besteht aus 2 UI-Komponenten, dem Java-basierten IdM UI, welches den Endanwendern für Workflows, Monitoring und Reporting bereitgestellt wird, und außerdem der Administration Console (Plug-In für die Microsoft Management Console), die zur Entwicklung, Konfiguration und Customizing den Entwicklern dient.
2. In der IdM-Datenbank werden die Customizing-Einstellungen gespeichert sowie die eigentlichen Identitätsdaten (Identity Store).
3. Die Laufzeitkomponente IC Runtime beinhaltet Dispatcher, die die ausführende Komponente in SAP NW IdM darstellen und die Jobs, Workflow- und Provisionierungsaufgaben abarbeiten. Event Agents überwachen Backend-Systeme und können aufgrund einer Veränderung einen Prozess in SAP NW IdM starten.
4. SAP NetWeaver IdM nutzt unterschiedliche Klassen, um die Konnektivität zu Quell- und Zielsystemen herzustellen. Bei der Kommunikation zu Access Control beispielsweise spielt die LDAP-Schnittstelle eine wichtige Rolle, da darüber die Kommunikation zum Virtual Directory Server und damit zum Access Control stattfindet.

Die SAP NetWeaver Identity Management-Komponente Identity Center ist mit dem Identity Store das

zentrale Provisioning- und Identity-Management-System, welches Identitätsdaten und Berechtigungsinformationen zentral an einer Stelle sammelt und auf Basis von regelbasierter Provisionierung (Rule-Based Provisioning) an die angeschlossenen Systeme verteilt. Der Identity Store stellt dafür ein vordefiniertes Datenmodell (Identity Store Schema [23]) bereit, welches die unterschiedlichen Identitätsdaten und Berechtigungsinformationen zentral im Identity Store abbildet. Für die regelbasierte Provisionierung stellt das Identity Center das „SAP Provisioning Framework" bereit, welches wichtige Standard-Provisionierungsregeln abdeckt.

Als zentrales Design-Werkzeug für das Anpassen der Provisionierungsregeln dient die Identity Center Administrator Console (MMC-Plug-In). Neben der Erstellung und Anpassung von Provisionierungsregeln, findet damit auch die Erstellung von Rollen, Datensynchronisation, Prozessen, Workflows, Event-Handlern, (Scheduled) Jobs, Skripten und das Anpassen des Datenmodells statt. Die folgende Abbildung zeigt das Design-Werkzeug „Identity Center Console".

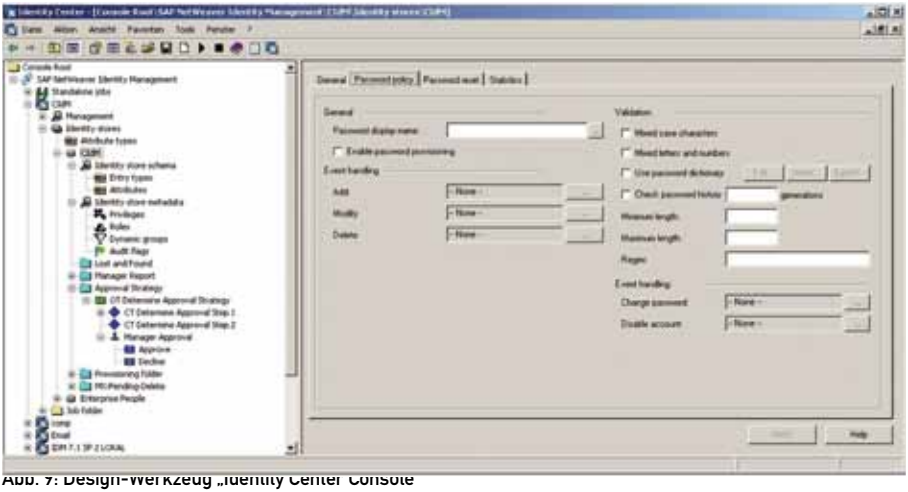

Abb. 9: Design-Werkzeug „Identity Center Console"

Mit dem SAP Provisioning Framework stellt die SAP vordefinierten Content bereit, der mit seinen Prozessen

23 SDN, SAP NetWeaver Identity Management 7.1, Identity Store Schema, http://www.sdn.sap.com/irj/scn/index?rid=/library/uuid/f0d87115-36da-2b10-7b89-996efe422b2a&overridelayout=true

und Regeln das Provisioning von SAP Business Suite, SAP EP, verschiedenen Directories und dem Mail Provisioning abdeckt. Dieser Content dient als Vorlage für die Anbindung der verschiedenen Systeme der heterogenen Systemlandschaft eines Unternehmens. Für die Konnektivität der Systeme liefert das SAP Provisioning Framework Standardschnittstellen (Standard-Konnektoren)[24]. Im SAP NetWeaver Identity Management Identity Center können auf Basis von Java, JScript und VisualBasic weitere Schnittstellen erstellt werden. Sowohl Schnittstellen zu Quell- als auch Zielsystemen werden bei der Prozessmodellierung in der Identity Center Console in Form von Repository-Definitionen verwendet.

Prozesse der Endanwender wie Administratoren, Antragsteller, Genehmiger, Wirtschaftsprüfer etc. finden über das Web-basierte IdM User-Interface (IdM UI) statt. Hierzu zählen Prozesse wie Approval-Workflows, Business-Rollenmodellierung, Stammdatenpflege, Berechtigungszuweisung, Monitoring, Reporting etc. Das IdM UI basiert auf Web Dynpro for Java und kann ins Portal integriert werden. Die Modellierung der Prozesse findet in der Identity Centers Console statt.

Die folgende Abbildung zeigt das webbasierte User-Interface „IdM UI".

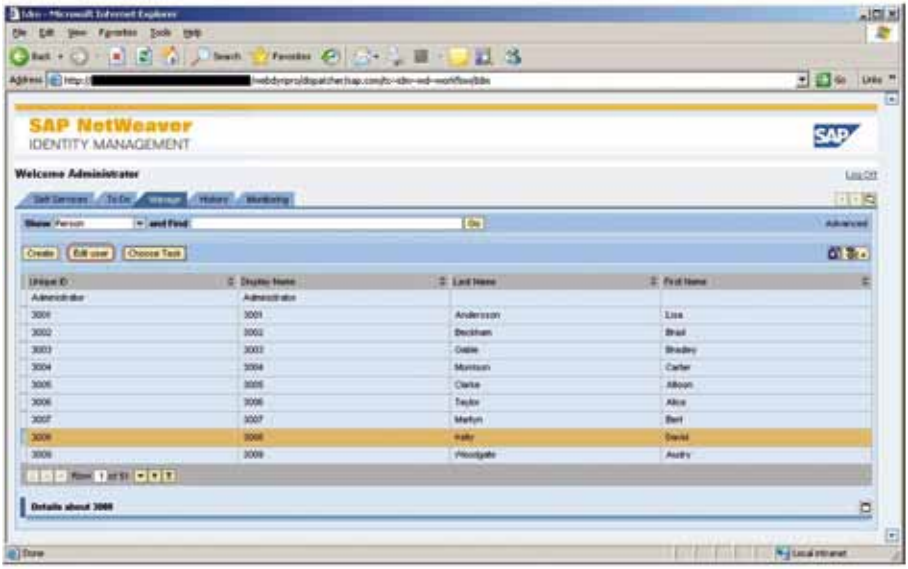

Abb. 16: Workflow-Komponente „IdM UI"

Ein detaillierter Überblick der Komponente „Identity Center" befindet sich im SDN[25].

3.7.1.3 VIRTUAL DIRECTORY SERVER

24 SDN, SAP NetWeaver Identity Management 7.1, Connector Overview, http://www.sdn.sap.com/irj/scn/index?rid=/library/uuid/20a1f8ad-e742-2c10-0e9b-e4e2a21ba96f&overridelayout=true

25 SAP Help Portal, Details zu der SAP NetWeaver Komponente „Identity Center", http://help.sap.com/saphelp_nwidmic71/en/dse.htm

Neben dem Identity Center stellt SAP NetWeaver Identity Management 7.1 mit dem „SAP NetWeaver Identity Management - Virtual Directory Server" (SAP VDS) eine weitere Komponente bereit. Der SAP Virtual Directory Server stellt eine virtuelle Sicht auf verschiedene Backend-Systeme in Form einer virtuellen Directory-Struktur bereit, ohne dabei die backend-Daten zwischen zu speichern. Die Anwendung läuft als (Web) Service auf dem Server und die Definition von Mappingregeln der Attribute und sowie die Regeln für die Manipulation der Attributwerte wird in Form von XML-Konfigurationsdateien auf dem Server abgelegt.

Die folgende Abbildung stellt SAP NetWeaver Identity Management Virtual Directory Server in einer Übersicht dar.

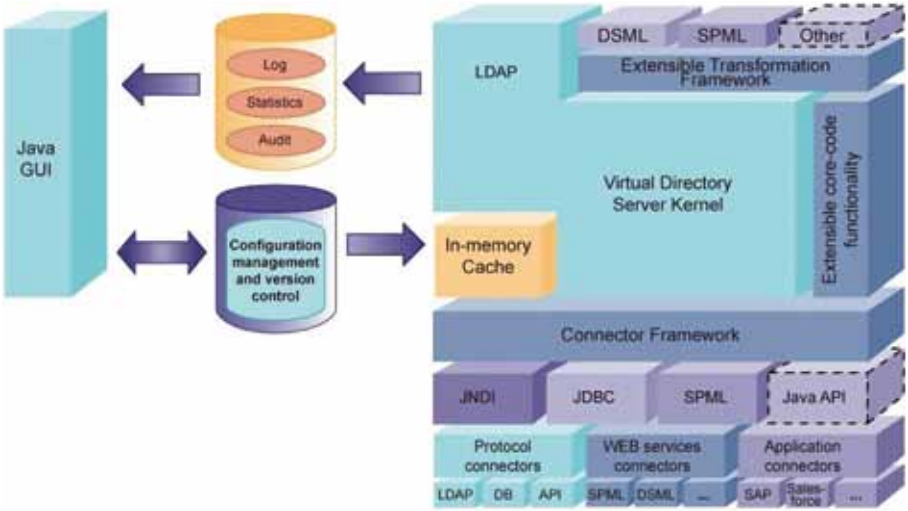

Abb. 11: Übersicht des Aufbaus des „Virtual Directory Servers

Damit ergeben sich unterschiedliche Konfigurationsoptionen mit unterschiedlichen Anwendungsfällen, die in folgender Tabelle dargestellt sind.

KONFIGURATION	ANWENDUNGSFALL	BESCHREIBUNG	SAP NW IDM KOMPONENTEN
Virtual Directory (Backend)	Zusammenfassen mehrerer Systeme (Directories, Datenbanken etc.) zu einem virtuellen Unternehmens-Directory.	Zusammenfügen unterschiedlicher Directories (Backends) zu einem virtuellen Directory.	SAP NW VDS
Virtual Directory (Identity Store)	Nutzen des Identity Stores von SAP NetWeaver Identity Management als Userrepository für LDAP-fähige Anwendungen.	Directory-Sicht (lesender Zugriff) auf den SAP Identity Managements Identity Store (LDAP oder SPML).	SAP NW VDS SAP NW IC
Identity Services	Bereitstellen der Provisioning-Funktionalität von SAP NetWeaver Identity Management Identity Center für andere Applikationen („Identity Management as a Service").[26]	Directory-Sicht (schreibender Zugriff) auf SAP Identity Managements Identity Store (LDAP oder SPML).	SAP NW VDS SAP NW IC
Identity Middleware	Integration von SAP BusinessObjects Access Control-Funktionalitäten in SAP NetWeaver Identity Management 7.1 (Compliant Identity Management)	Standardschnittstelle (Middleware), die über LDAP angesprochen werden kann, die Informationen entgegennimmt und weiterleitet. Wie der VDS mit diesen Anfragen umgeht, kann in der Programmiersprache Java definiert werden (Custom Connector). VDS stellt einige Schnittstellen (u. a. SAP BusinessObjects Access Control) als Template im VDS bereit.	SAP NW VDS SAP NW IC
	Erstellen einer Standardschnittstelle für SAP NetWeaver Identity Management Identity Center durch Programmierung eigener Templates im VDS. (Ergänzend zu den Konnektoren im Identity Center[27])		

Abb. 12: Anwendungsszenarien „Virtual Directory Server"

26 SDN, SAP NetWeaver Identity Management 7.1, Identity Services, http://www.sdn.sap.com/irj/scn/index?rid=/library/uuid/106ecdec-ddfa-2a10-cf89-c2e75482d090&overridelayout=true

27 SDN, SAP NetWeaver Identity Management 7.1, Connector Overview, http://www.sdn.sap.com/irj/scn/index?rid=/library/uuid/20a1f8ad-e742-2c10-0e9b-e4e2a21ba96f&overridelayout=true

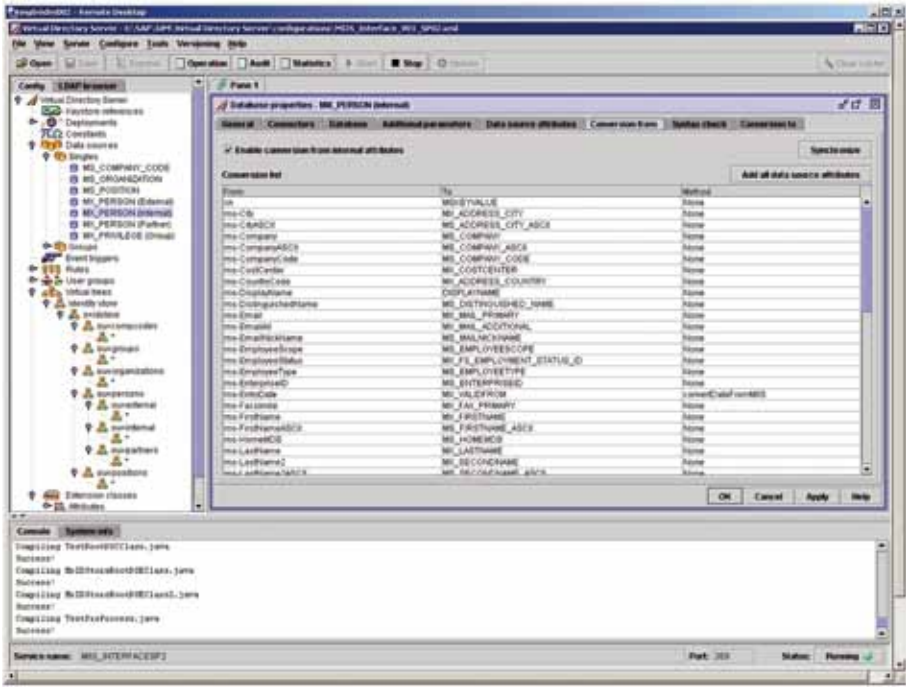

Abb. 13: Konfigurationswerkzeug des „Virtual Directory Servers"

Der Integrierte Einsatz von SAP NetWeaver Identity Management 7.1 und SAP BusinessObject Access Control auf Basis der Konfigurationsoption „Identity Middleware" wird in Abschnitt 3.7.2.1 beschrieben.

3.7.1.4 ABGRENZUNG VON SAP NETWEAVER IDENTITY MANAGEMENT ZU SAP BUSINESSOBJECTS GRC-PORTFOLIO

SAP BusinessObjects Access Control ist das System der Wahl für die Unterstützung bei der Erstellung von sicheren Berechtigungskonzepten (RAR, ERM) sowie der Workflow-basierten Vergabe von kritischen Berechtigungen (CUP, SPM), unter Berücksichtigung von Funktionstrennung mit integrierter Risikoanalyse (RAR).

SAP NetWeaver Identity Management schafft ein zentrales regelbasiertes Provisionierungssystem zur automatisierten Berechtigungsvergabe mit zentralem Identity Store und zentralem User-Interface zur Prozessabbildung (Identity Center) sowie einer virtuellen Sicht auf alle Daten und der serviceorientierten Bereitstellung der Prozesse an andere Anwendungen (Virtual Directory Server).

Da beide Systeme umfangreiche Workflow-Funktionalitäten beinhaltet, kommt es häufig zu Irritationen, da der Eindruck entsteht, dass die SAP mit SAP NetWeaver Identity Management und SAP BusinessObjects Access Control zwei Systeme mit großen Überschneidungen des Funktionsumfangs bereitstellt. Die folgende Abbildung stellt die Schnittmenge der Produkte und schafft damit eine Abgrenzung.

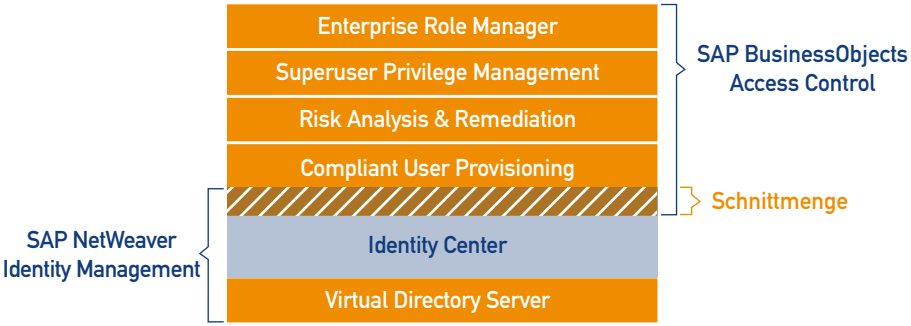

Abb. 14: Produktübersicht und Schnittmenge der Produkte

Die in der Abbildung 14 Produktübersicht und Schnittmenge der Produkte dargestellte Produktübersicht zeigt die Schnittmenge im Funktionsumfang zwischen den Komponenten IdM User-Interface von SAP NetWeaver Identity Management Identity Center (IC) und Compliant User Provisioning (CUP) von SAP BusinessObjects Access Control.

Die Schnittmenge ergibt sich durch die Bereitstellung von Workflow-basierter Berechtigungsvergabe von ERP-Berechtigungen mit anschließender Provisionierung, wobei der Fokus der Systeme abweichend ist:

- Der Fokus vom Identity Center liegt auf einer engen Integration der gesamten SAP Business Suite und Non-SAP-Systemen. Das IdM UI zielt darauf ab, Endanwendern wie Administratoren, Führungskräften und den verschiedenen Mitarbeitern der Fachabteilungen unternehmensweite Workflows bereitzustellen, welche die Prozesse in Bezug auf Identitätsdaten und Berechtigungsinformationen mit Genehmigungsschritten als Delegated-Services und als Self-Service bereitstellt. SAP NetWeaver IdM ermöglicht dabei die zentrale oder dezentrale Modellierung und zentrale Abbildung von systemübergreifenden Business-Rollen (systemübergreifende Fachrollen), um Berechtigungen beispielsweise zu Arbeitsplatzbeschreibungen zusammenzufassen. Dabei können die systemübergreifenden Business-Rollen hierarchisch modelliert werden (siehe Abschnitt 3.7.5).

- CUP dagegen fokussiert auf den Vergabeprozess von ERP-Rollen unter Beachtung von Funktionstrennung und integrierter Risikoprüfung. CUP liefert für ERM die Workflows zur Erstellung von SAP-Einzel- und Sammelrollen (systemspezifisch) unter Berücksichtigung von sauberen Rolleninhalten. Wenn bei der Berechtigungsvergabe oder bei der Berechtigungserstellung Risiken aufgedeckt werden, werden über CUP entsprechende Kontrollen eingeplant und überprüft. Sollte eine Kontrolle nicht eingehalten werden, kann darauf reagiert werden.

Damit zeigt sich bei genauer Betrachtung, dass die Gemeinsamkeiten der Komponenten gering sind und ein integrierter Ansatz Sinn machen kann, da sich die Komponenten gut ergänzen.

3.7.2 CIM BEST PRACTICES

SAP NetWeaver IdM berücksichtigt nur auf Business-Rollen-Ebene eine Funktionstrennung (SoD) bei der Vergabe von Berechtigungen und unterstützt die Unternehmen nicht bei der Erstellung von SAP-Rollen unter der Berücksichtigung von kritischen Berechtigungskombinationen. SAP BusinessObjects Access Control stellt keinen eigenen Identity Store bereit und ist darauf angewiesen, dass Identitäten in angeschlossenen Systemen existieren. Außerdem unterstützt es nur bestimmte ERP-Systeme. Aus den Limitierungen der beiden Systeme ergibt sich die Notwendigkeit einer Kombination.

Die folgende Abbildung stellt den Funktionsumfang der integrierten Lösung Compliant Identity Management dar.

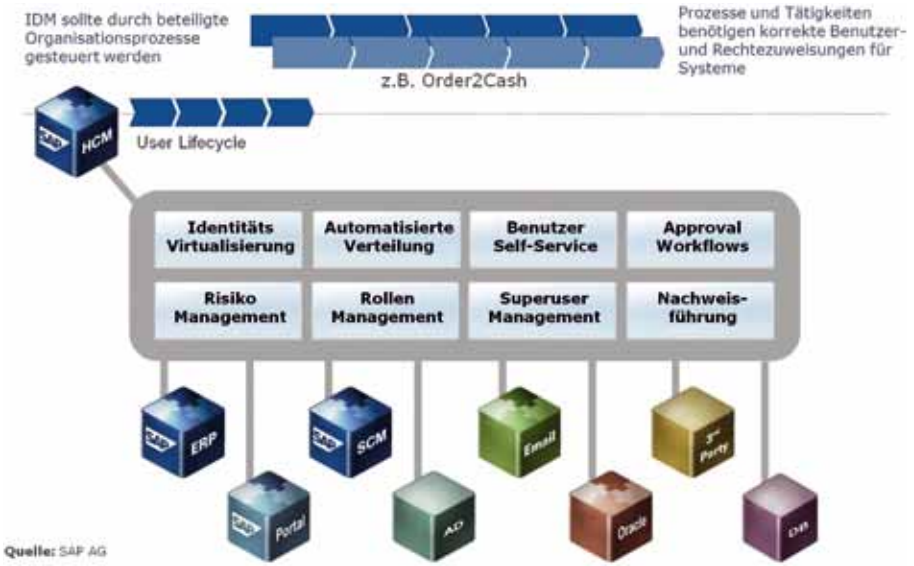

Abb. 15: Funktionsumfang von CIM

3 SAP BusinessObjects Access Control 5.3

Es gibt unterschiedliche Anwendungsszenarien, in denen die Kombination von SAP NetWeaver Identity Management und SAP BusinessObjects Access Control sinnvoll ist. Im Folgenden werden drei Best Practices dargestellt, bei dem die Systeme integriert eingesetzt werden.

> CUP und IdM: Die Beantragung von Berechtigungen findet über SAP IdM statt, sollte eine Berechtigung beantragt worden sein, die einer integrierten Risikoanalyse bedarf, wird der Antrag an CUP weitergeleitet.

> ERM und IdM: Die Erstellung der Berechtigungen findet über ERM (und CUP) statt. SAP-Rollen werden direkt in die SAP-Systeme geschrieben, andere Berechtigungen werden in den Backend-Systemen angelegt. Die Beantragung für die Zuweisung der Berechtigung findet zentral im SAP IdM statt.

> SPM und IdM: Die Beantragung der Zuweisung von Berechtigungen findet zentral in SAP IdM statt. Die Superuser-Berechtigungen kann der Antragsteller über SPM sich selbst zuweisen.

In allen drei CIM-Integrationsszenarien ist SAP NetWeaver Identity Management mit seinem zentralen Identity Store das führende System zur Beantragung der Zuweisung von Berechtigungen. Die Personenstammdaten und die Berechtigungen werden aus den führenden Systemen in den Identity Store importiert und von dort aus synchronisiert.

3.7.2.1 CUP UND IDM

Die folgende Abbildung stellt das CIM-Anwendungsszenario „CUP und IdM" dar, in dem SAP NetWeaver IdM als führendes Provisioning-System die Anfragen für bestimmte Zielsysteme zur Risikoanalyse an SAP BusinessObjects AC weiterleitet.

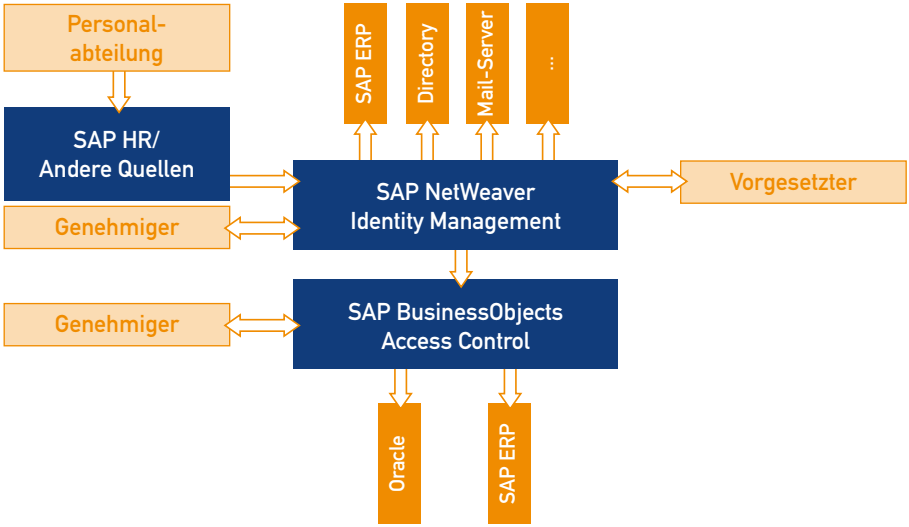

Abb. 16: Prozesssicht des CIM-Integrationsszenario „CUP und IdM"

Das Integrationsszenario wird anhand der Abbildung 16 Prozesssicht des CIM-Integrationsszenarios „CUP und IdM" erläutert. Beim CIM-Integrationsszenario „CUP und IdM" werden interne Mitarbeiter aus dem Personalsystem (z. B. SAP HCM) in den Identity Store importiert, da das Personalsystem das führende System für die interne Mitarbeiteridentität ist. Die Anlage eines internen Mitarbeiters im Personalsystem nimmt SAP NetWeaver IdM zum Anlass, automatisch auf Basis von Rule-Based Provisioning Benutzerkonten mit Identitätsdaten und Berechtigungsinformationen zu provisionieren. Externe und nicht im Personalsystem geführte Mitarbeiter können direkt im Identity Store angelegt werden, was je nach Prozess zuvor Genehmigungsschritte durch Vorgesetzte, System- und/oder Role-Ownern erfordern kann. Die Berechtigungen werden aus den angebundenen Systemen importiert. Beim Rollout wird auch die Verknüpfung von Berechtigung zur Identität aus den Systemen importiert. Ab dem Go-live findet die Beantragung von allen Berechtigungen ausschließlich über das SAP IdM UI statt. Bei einer Neuanlage wird ein Großteil der Berechtigungen auf Basis von regelbasiertem Provisioning auf Basis vom Identity Center den Identitäten automatisch zugewiesen. Der Anteil der über Rule-Based Provisioning automatisch zugewiesenen Rollen variiert stark nach Organisationsstruktur und Unternehmen.

Alle weiteren Berechtigungen werden über das IdM UI beantragt und durchlaufen zunächst den Genehmigungsworkflow in SAP IdM. Für Berechtigungen, die als risikoreich angesehen werden, wird bei der Berechtigungsvergabe ein zusätzlicher Genehmigungsschritt durch einen Compliance-Verantwortlichen über CUP durchgeführt. Hier findet dann eine Genehmigung auf Basis der Risikoanalyse statt. Dieser Schritt beinhaltet eine Risikoanalyse und die Möglichkeit, Kontrollen einzuplanen. Es können beliebige Genehmiger am Workflow beteiligt werden. Wer wann zur Genehmigung in den Prozess eingreifen soll, ist in den beiden Workflow-Komponenten SAP NetWeaver IdM UI und Compliant User Provisioning zu konfigurieren.[28]

In SAP NetWeaver IdM ist es ausschließlich möglich, Risiken in Form von SoD-Konflikten auf Business-Rollen-Ebene zu definieren. Durch das CIM-Integrationsszenario „CUP und IdM" ist es möglich, eine Risikoanalyse auf Basis der in RAR definierten Risikomatrix (SoD-Matrix) durchzuführen. Damit wird der Funktionsumfang von SAP NetWeaver IdM um einen Compliance Check auf Transaktions- und Berechtigungsobjekt-Ebene während des Vergabeprozesses erweitert.

28 Konfiguration von CUP:
https://wiki.sdn.sap.com/wiki/display/BPX/Governance%2C%20Risk%2C%20and%20Compliance%20%28GRC%29%20How-To%20Guides

3 SAP BusinessObjects Access Control 5.3

Die folgende Abbildung stellt das Integrationsszenario „CUP und IdM" in einer Übersicht dar.

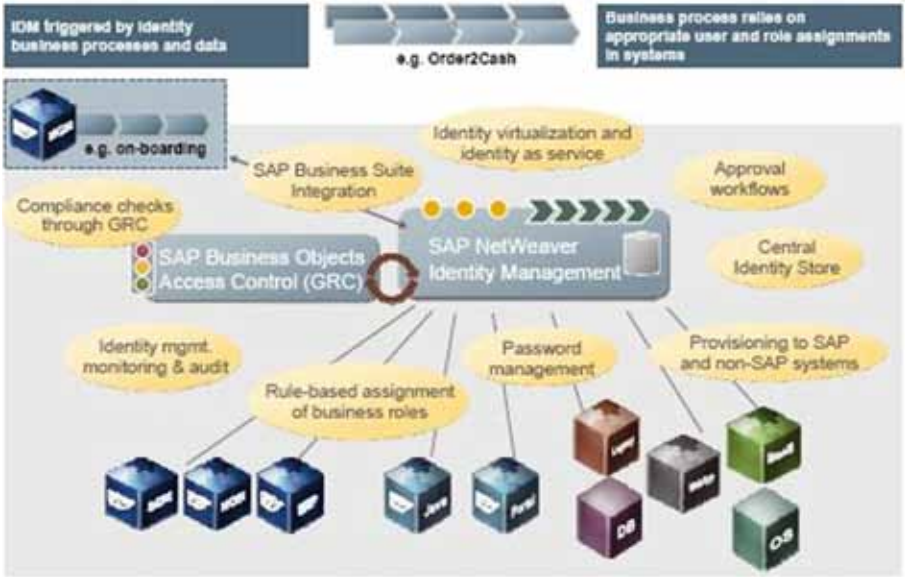

Abb. 17: Übersicht des CIM-Integrationsszenarios „CUP und IdM"

Bei der Provisionierung wird zwischen „Centralized-" und „Distributes-" Provisioning unterschieden.[29] Bei „Centralized Provisioning" ist SAP NW IdM das zentrale Provisioning System. Nach der Risikoanalyse von CUP, bekommt SAP NW IdM das Ergebnis der Risikoanalyse in Form eines Status zurück. Alle Provisionierungen finden nachgelagert über SAP IdM statt. Dagegen werden beim „Distributed Provisioning" die Berechtigungen, für die eine Risikoanalyse notwendig ist, direkt von CUP provisioniert. SAP NW IdM bekommt lediglich einen Status und provisioniert die Berechtigungen, für die keine Risikoanalyse notwendig ist. „Centralized Provisioning" ist erst mit dem GRC-Provisioning Framework in der Version 03/2010 möglich.[30]

Neben dem hier beschriebenen CIM-Integrationsszenario „CUP und IdM", in dem SAP NetWeaver IdM das führende System für die Beantragung von Berechtigungen ist, gibt es noch ein weiteres CIM-Integrationsszenario „CUP und IdM", in dem CUP das führende System für die Beantragung von Berechtigungen ist und Anfragen für nicht ERP-Systeme (Systeme, die nicht über CUP provisioniert werden) über die Identity Services zur Provisionierung an SAP NetWeaver Identity Management weiterleitet werden. Da SAP BusinessObjects Access Control jedoch keinen zentralen Identity Store bereitstellt, müssen die Benutzer in einem zentralen System angelegt sein. Das Integrationsszenario kommt eher selten vor und wird in diesem Leitfaden nicht weiter behandelt. Für Informationen sei an dieser Stelle auf den passenden Configuration Guide zu SAP BusinessObjects Access Control29 und den Configuration Guide zu SAP NetWeaver Identity Management Identity Services30 verwiesen.

29 CIM Architecture overview:
http://www.sdn.sap.com/irj/sdn/go/portal/prtroot/docs/library/uuid/60a4802f-b6cd-2b10-1ebf-e269d127a634
30 Download the new SAP Provisioning Framework:
http://www.sdn.sap.com/irj/sdn/nw-identitymanagement?rid=/webcontent/uuid/b0196981-09d0-2b10-1b96-9b488d34a317

3.7.2.2 ERM UND IDM

Das CIM-Integrationsszenario „ERM und IdM" hat das Ziel, Compliance-Anforderungen durch integrierte Risikoanalyse beim Prozess der SAP-Rollenmodellierung nachzukommen. Dabei ist SAP NW IdM das führende System für die Zuweisung von SAP-Rollen an die Benutzerkonten (für eine integrierte Risikoanalyse bei der Rollenvergabe ist eine Integration mit CUP, wie in Abschnitt 3.7.2.1 zuvor beschrieben, notwendig). Die Modellierung der SAP-Rollen findet nicht direkt in den Backend-Systemen, sondern über SAP BusinessObjects Enterprise Role Management (ERM) statt. Die Rollen werden im ERM designt und der Transport ins Backend-System durch einen Genehmigungsworkflow in CUP bestätigt.
In SAP NW IdM ist es üblich, die gewünschten Berechtigungen über Batchprozesse aus den Backend-Systemen zu importieren. Für den integrierten Einsatz von ERM ist kein zusätzlicher Konfigurationsaufwand notwendig, da in gewissen Abständen (etwa nächtlich) die neuen SAP-Rollen aus den Systemen gelesen werden. Für das Importieren der Rollen liefert SAP NW IdM vordefinierte Batchprozesse („Update-Jobs") für verschiedene SAP- und Non-SAP-Systeme inklusive Delta-Handling mit. Diese werden im SAP NW IdM Identity Center über einen Job-Wizard der aktuellen Konfiguration hinzugefügt. Zu den Batchprozessen legt eine Scheduling Rule fest, in welchen Intervallen der Prozess laufen soll, also wie häufig ein Abgleich zwischen SAP NW IdM Identity Store und dem Backend-System stattfinden soll. Die folgende Abbildung

Abb. 18: Batchprozess zum Import der in ERM modellierten Rollen im Identity Center

Sollte eine in ERM modellierte Rolle direkt nach der Erstellung im Backend in SAP NW IdM verfügbar sein, um sie einem Benutzer zuzuweisen, und kann nicht auf die Ausführung des zeitlich eingeplanten Batchprozesses gewartet werden, kann der Batchprozess auch über eine Web-Oberfläche beispielsweise für Administratoren zur Verfügung gestellt werden und ein Update „On Demand" stattfinden. Damit ist es nicht nötig, ein Intervall abzuwarten, um die eine neue SAP-Rolle einem Benutzer zuzuweisen.

Die folgende Abbildung stellt das Zusammenspiel von SAP NW IdM und SAP BusinessObjects Access Control in der CIM-Integration „ERM und IdM "dar. Dabei steht die Risikoanalyse nach der Rollenmodellierung im Vordergrund. Die Risikoanalyse bei der Rollenzuweisung (hier grau dargestellt) ist in Abschnitt

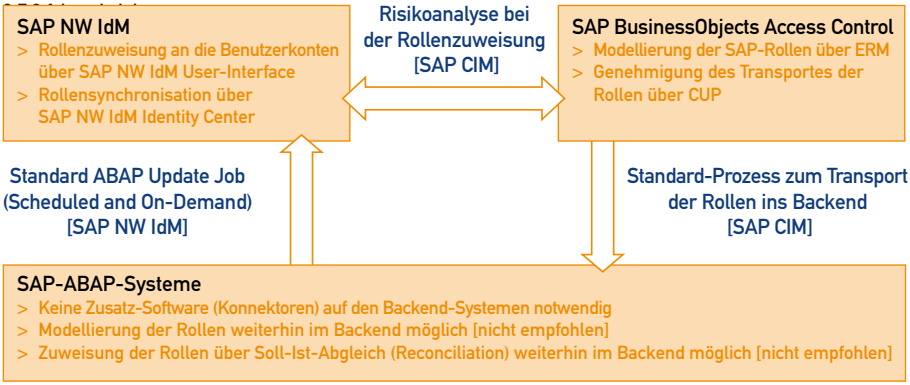

Abb. 19: Datenfluss beim integrierten Ansatz von SAP NW IdM und ERM

Die Abbildung zeigt das Zusammenspiel von SAP NetWeaver Identity Management und SAP BusinessObjects Access Control. Die Rollen werden in ERM modelliert und der Transport in das SAP-Backend-System durch CIM genehmigt. SAP NW IdM Identity Center importiert die neue Rolle nach einem festgelegten Intervall (bzw. „On Demand") in den Identity Store. In SAP NW IdM steht sie anschließend bereit, beantragt und einem Benutzer zugewiesen zu werden. Sowohl für den Transport der Rollen als auch für die Synchronisation der Rollen in SAP NW IdM Identity Store ist keine zusätzliche Software auf den SAP-Backend-Systemen notwendig.

Um durch die integrierte Risikoanalyse und einen Genehmigungsworkflow sicherzustellen, dass SAP-Rollen kontrolliert modelliert werden und in die Backend-Systeme gelangen, wird empfohlen, die Rollenmodellierung ausschließlich in ERM durchzuführen. Bei zusätzlicher Modellierung in der SAP PFCG (im SAP-Backend-System) ist die Modellierung von risikofreien SAP-Rollen nicht mehr gewährleitet. Auch eine kontrollierte Modellierung von risikobehafteten SAP-Rollen durch Einplanen von Kontrollen ist nicht

gegeben. Damit wäre die Einhaltung von Compliance wieder schwer sicherzustellt und eine regelmäßige Analyse mit RAR mit entsprechender Korrektur der Rollen bzw. der Einplanung von Kontrollen notwendig. Um Compliance nachzukommen und die Rollenzuweisung kontrolliert mit einem Genehmigungsworkflow (ggf. einer integrierten Risikoanalyse mit „CUP und IdM", siehe Abschnitt 3.7.2.1) durchzuführen, wird empfohlen, die Rollenzuweisung ausschließlich über SAP NW IdM UI (bzw. „CUP und IdM") durchzuführen. Technisch wird durch die Festlegung der Datenhoheit für die Zuweisung von Rollen an den Benutzer der Synchronisations- und Rekonziliation-Prozess vereinfacht. Ist eine Zuweisung in den Backend-Systemen weiterhin notwendig, können Rollenzuweisungen in den Backend-Systemen direkt, oder mit Bestätigung eines Verantwortlichen, durchgeführt werden. Da jedoch eine Lösung ohne klar definierte Datenhoheit die Gefahr von Dateninkonsistenz birgt, wird empfohlen, die Datenhoheit klar zu definieren und die Zuweisung in SAP NW IdM (bzw. „CUP und IdM") durchzuführen.
Um die Implementierung zu vereinfachen, sollte geprüft werden, ob die Aufgaben wie folgt auf die Systeme verteilt werden können:

- die Rollenmodellierung findet in ERM statt
- die Zuweisung in SAP NW IdM (bzw. „CUP und IdM")

3.7.2.3 SPM UND IDM

SPM kommt zum Einsatz, wenn Superuser-Berechtigungen (wie beispielsweise SAP_ALL oder andere kritische Berechtigungen bzw. Berechtigungskombinationen) nur noch temporär und kontrolliert über SPM in Form von Superusern vergeben werden sollen und damit die identitätsbezogenen Benutzerkonten von diesen Berechtigungen entlastet werden sollen (siehe Abschnitt 3.4.3.5).

Beim CIM-Integrationsszenario „SPM und IdM" ist SAP NetWeaver IdM das führende System für die Beantragung von Berechtigungen, jedoch werden Superuser-Berechtigungen über SPM in Form von Superusern vergeben. Es gibt unterschiedliche Möglichkeiten, wie in einem integrierten Szenario in SAP NetWeaver IdM mit den Superuser-Berechtigungen umgegangen werden soll, deren alleinige Zuweisung bereits ein Risiko verursacht und deshalb in SPM einem Superuser zugeordnet ist. Voraussetzung für den kontrollierten Umgang mit den Superuser-Berechtigungen in SAP NetWeaver IdM" ist, dass diese Superuser-Berechtigungen bekannt sind. Hierzu reicht es beispielsweise, wenn eine Liste (csv-Datei etc.) dieser Superuser-Berechtigungen existiert.

Superuser beinhalten jedoch auch häufig eine kritische Kombination von Berechtigungen, welche jede für sich in SAP NW IdM beantragbar ist. Beantragt ein Benutzer nun eine kritische Berechtigungskombination, wird durch das Intregationsszenario „CUP und IDM" (siehe Abschnitt 3.7.2.1) durch die integrierte Risikoanalyse auf die kritische Berechtigungskombination hingewiesen und eine Ablehnung oder Mitigierung ermöglicht.

Im Folgenden soll jedoch auf den Umgang mit Superuser-Berechtigungen im SAP NW IdM eingegangen werden, deren alleinige Zuweisung bereits ein Risiko darstellt und deshalb im SPM einem Superuser zugeordnet ist. Hierzu werden drei Alternativen beschrieben, wie SAP NW IdM diese Superuser-Berechtigung behandeln kann:

Alternative 1: Beim Import der Berechtigungen aus den Backend-Systemen werden die Superuser-Berechtigungen nicht in SAP NetWeaver IdM importiert. Die Berechtigungen werden ausschließlich in SPM angezeigt.

Alternative 2: Die Superuser-Berechtigungen werden bei einem Import in den Identity Store importiert. Die Superuser-Berechtigungen werden in IdM angezeigt und können beantragt werden. Anstelle einer Provisionierung wird beispielsweise ein Prozess angestoßen, der eine E-Mail-Benachrichtigung versendet.

Dieses Verhalten wird über einen Batchprozess im Identity Center erreicht, der das Attribut MX_REPOSITORYNAME der Superuser-Berechtigung mit dem Systemnamen („SPM") beschreibt. Im Identity Center wird eine Repository Definition für das System SPM mit entsprechenden Repository-Konstanten (MX_PROVISIONINGTASK) erstellt, die bei einer Beantragung der Rolle keine Provisionierung in SAP NetWeaver IdM anstößt, sondern eine E-Mail an den Antragsteller und seinen Vorgesetzten versendet. Die E-Mail verweist auf SPM als führendes System zur Beantragung von Superusern. Die E-Mail an den Vorgesetzten ist sinnvoll, um diesen über die Verwendung von SPM zu informieren. Genau wie in SPM ist die Zuweisung der Superuser-Berechtigung nur temporär und dient nur der Anzeige im IdM UI. In SAP NW IdM kann eine Regel dafür sorgen, dass die Zuweisung der Superuser-Berechtigung nach dem im SPM definierten Zeitraum wieder gelöscht wird.

Alternative 3: Die Superuser-Berechtigungen werden bei einem Import in den Identity Store importiert. Jedoch werden die Berechtigungen nur angezeigt und können nicht beantragt werden.

Dieses Verhalten wird über einen Batchprozess im Identity Center erreicht, der einen beschreibenden Text in das Attribut DESCRIPTION schreibt und damit auf SPM als führendes System zur Beantragung der Superuser-Berechtigung hinweist. Im SAP NW IdM kann dafür gesorgt werden, dass Superuser-Rollen nur im IdM UI angezeigt werden, jedoch nicht zugewiesen werden können. Durch den beschriebenen Text erhält der Antragsteller die Information, dass er sich die Superuser-Berechtigung in Form einer eigenen Superuser-ID direkt in SPM zuweisen kann.

In allen Fällen besteht die Nachvollziehbarkeit der Zuweisung über detailliertes Auditing in SPM (siehe Abschnitt 3.5.3).

3.7.3 AUDITINFORMATIONEN ZENTRAL VERWALTEN

In den dargestellten Integrationsszenarien werden Auditinformationen sowohl in SAP BusinessObjects Access Control als auch in SAP NetWeaver IdM erfasst und gespeichert. Um einen zentrales Auditing in SAP NetWeaver IdM zu erhalten, stellt Access Control Audit-Information über einen Web Service (SAPGRC_AC_IDM_AUDITTRAIL) bereit. SAP NetWeaver IdM stellt eine Built-in-Funktion bereit, mit der die Informationen von Access Control dem zentralen Audit in SAP NW IdM Identity Store hinzugefügt werden können.

3.7.4 DIE EINFÜHRUNG VON CIM

Aufbauend auf Kapitel 3.7.1, in dem schon auf die Einführung von SAP BusinessObject Access Control und einem Identity-Management-System eingegangen wurde, geht das folgende Kapitel auf die Einführung von CIM ein.

Ein wichtiger Faktor für die Planung des Projektplans ist die Qualität des Berechtigungskonzeptes. Ist nicht bekannt,welche Risiken aufgrund des aktuellen Berechtigungskonzeptes bestehen, ist es vielfach sinnvoll, vor der Projektplanung durch die Einführung von RAR und wie in Abschnitt 3.4.1 („Strategie und Planung") beschrieben, auf Basis einer ersten Analyse mit RAR das weitere Vorgehen zu planen. Dies fällt in die Phase Projektvorbereitung.

Wie in Abschnitt 3.4.2 („Business Blueprint und Design") wird beschrieben, wie in einem High-Level-Konzept die Integration zwischen Zugriffsrisikomanagementsystem und Identitätsmanagementsystem aussehen soll. Damit können sich folgende High-Level-Strategien ergeben:

- Ein bestehendes Identity-Management-System wird um Funktionalitäten von SAP BusinessObjects Access Control erweitert.
- SAP BusinessObjects Access Control und SAP NW Identity Management werden parallel eingeführt.
- Access Control wird ohne ein Identity-Management-System eingeführt.

Ob SAP NetWeaver Identity Management das System der Wahl ist oder SAP BusinessObjects Access Control oder gar beide Systeme eingeführt werden sollten und wenn ja, in welcher Reihenfolge, kann von folgenden Fragen abhängen:

- Was soll kurzfristig über eine Investition in die Systeme erreicht werden?
- Was soll langfristig über eine Investition in die Systeme erreicht werden?
- Welche Systeme sind zu provisionieren?
- Liegen die Identitäten bereits in einem zentralen System vor?
- Welche Systeme sind führend für welche Identitäten?
- Wie ist die Datenqualität in den einzelnen Systemen?
- Wie ist das Berechtigungskonzept des Unternehmens?
- Welchen Stellenwert hat die Funktionstrennung für die Einführung des Projektes?

Entscheidend für den Projektverlauf ist natürlich die Ausgangslage des Unternehmens. Im Folgenden wird beschrieben, wie ein Projekt bei der Neueinführung von SAP NetWeaver IdM mit Nutzung der verschiedenen Funktionalitäten von SAP BusinessObjects Access Control ablaufen kann. Häufig finden Identity-Management-Prozesse nicht zentral statt. Dazu kommen Compliance-Anforderungen, die bei Verantwortlichen häufig die Angst vor dem großen, unternehmensweiten, nicht endenden Projekt („Big Bang") hervorrufen. Um dies zu vermeiden, ist eine sinnvolle Aufteilung in einzelne Teilprojekte erforderlich sowie ein koordiniertes, auf das Unternehmen zugeschnittenes Vorgehen innerhalb dieser Teilprojekte. Die einzelnen Teilprojekte müssen bis zur Zusammenführung keine direkten Abhängigkeiten zueinander haben (siehe Abbildung 20 Projektphasen von Compliant Identity Management).

Anhand der folgenden Übersicht soll der Projektablauf eines Compliant Identity Management-Projektes näher erläutert werden.

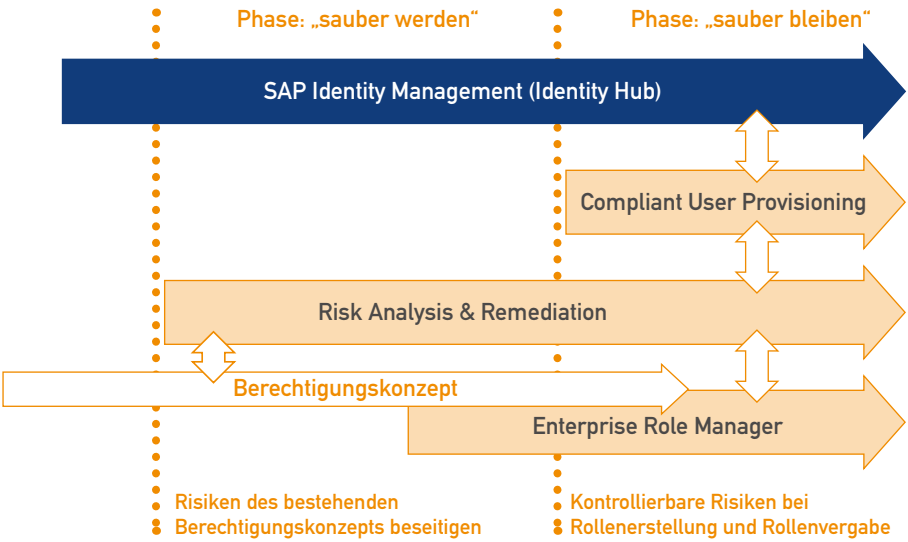

Abb. 20: Projektphasen von Compliant Identity Management

Wie bereits in Abschnitt 3.7.3.1 beschrieben, ist das Konzept von SAP NetWeaver IdM die Schaffung eines zentralen Identity Hubs mit der Bereitstellung der Personen- und Berechtigungsdaten für die relevanten Systeme des Unternehmens. Da die Schaffung eines einheitlichen und durchgängigen Berechtigungskonzeptes ein umfangreiches Projekt, ggf. mit Beratungs-Werkzeugunterstützung, darstellt, sollte es getrennt von der eigentlichen Einführung von SAP NetWeaver IdM und SAP BusinessObjects Access Control erfolgen. Dadurch werden Abhängigkeiten vermieden. Zu dem Projekt „Berechtigungskonzept“ gehört die Erarbeitung des Berechtigungsdesigns mit den Fachabteilungen. Dabei werden sukzessive die einzelnen Key-User der Fachabteilungen über Workshops in das Projekt eingebunden und die einzelnen Berechtigungen und Rollen entworfen und erarbeitet. Während dieser Zeit erleichtert RAR die Erstellung des Rollenkonzeptes durch die Simulations- und Analysefunktionalitäten, weshalb es sich empfiehlt, dieses System bereits im Vorfeld des Projektes „Berechtigungskonzepte“ einzuführen. Häufig ist der erste RAR-Lauf, wie bereits beschrieben, sogar der Auslöser für die Einführung der beschriebenen Systeme und das Infragestellen des Berechtigungskonzeptes.

31 SAP GRC Access Control, SAP Press 2008

SAP NetWeaver IdM stellt keine direkten Funktionalitäten für die Schaffung eines neuen Berechtigungskonzeptes bereit. SAP NetWeaver IdM ermöglicht jedoch die kontrollierte Vergabe der kritischen Berechtigungen auf dem Weg zu einem sauberen Berechtigungskonzept durch umfangreiche Auditing- und Reporting-Funktionalitäten. Zusätzlich ermöglicht SAP NetWeaver IdM die Bereitstellung von Administratoren-Tasks, über die diese „unsauberen" Berechtigungen kontrolliert vergeben werden können. Die Prozesskontrolle erfolgt durch das zentrale Auditing von SAP NetWeaver IdM. Die Phase der Schaffung von „sauberen" Berechtigungsstrukturen wird auch als Phase „sauber werden" bezeichnet. Durch die Aufspaltung in die Teilprojekte „SAP BusinessObjects Access Control Einführung", „SAP NetWeaver IdM Einführung" und dem Projekt „Redesign der Berechtigungseinstellungen" werden drei Teilprojekte geschaffen, die unabhängig voneinander ablaufen und in einer späteren Projektphase miteinander vereint werden. Die Phase, in der die Teilprojekte zusammenlaufen, wird als Phase „sauber bleiben" bezeichnet. Ab dieser Phase wird technisch dafür gesorgt, neu geschaffene Berechtigungen – wie „saubere" SAP Einzeln- und Sammelrollen mit Berücksichtigung von Funktionstrennung (SoD) – an Benutzer zu verteilen. Bei der Erstellung der SAP-Rollen mit ERM wird sichergestellt, dass eine Compliance-Verletzung innerhalb der Rollen frühzeitig erkannt und anschließend korrigiert bzw. durch eine kompensierende Kontrolle das Risiko vermindert wird.

In der Phase „sauber bleiben" wachsen die Applikationen SAP NetWeaver IdM, CUP und RAR sowie ERM und RAR mit IdM zusammen. Das Zusammenwirken der Access-Control-Komponenten untereinander ist detailliert im SAP Press Buch „SAP GRC Access Control"[31] beschrieben, das CIM-Integrationsszenario „CUP und IdM" in Abschnitt 3.7.2.1, „ERM und IdM" in Abschnitt 3.7.2.2 und „SPM und IdM" in Abschnitt 3.7.2.3.

3.7.5 BERECHTIGUNGEN UND SYSTEMÜBERGREIFENDE BUSINESS-ROLLEN (FACHROLLEN)

SAP Identity Management bildet Berechtigungskonzepte ab. Es nimmt Unternehmen jedoch nicht ab, ein Berechtigungskonzept auf Rollen- und/oder Regelbasis zu erstellen. SAP NW IdM stellt unterschiedliche Konzepte bereit, Berechtigungen den Benutzern zuzuweisen. Technische Berechtigungen wie SAP Einzel-/Sammelrollen, SAP Profile, Directory-Gruppen, SAP-UME-Rollen/-Gruppen etc. werden im SAP NetWeaver IdM als Objekte (Entry Types) vom Typ MX_PRIVILEGE abgebildet und aus den angeschlossenen Systemen importiert. Aus technischen Berechtigungen können Business-Rollen (MX_ROLE) erstellt werden. Diese Objekte können geschachtelt sein und über das Identity Management User Interface (IdM UI) in Form von Self-Services oder Delegated-Services beantragt oder manuell über Administratoren-Tasks Workflow-basiert zugewiesen werden. Ein Großteil der Berechtigungen kann jedoch über regelbasierte Provisionierung (Rule-Based Provisioning) auf Basis des SAP Provisioning Framework automatisiert an den Benutzer vergeben werden.

3.7.5.1 RULE-BASED PROVISIONING

SAP NetWeaver IdM verfolgt den Ansatz, Regeln zu definieren, nach denen Benutzern automatisiert Berechtigungen zugewiesen werden. Die Regeln können dabei auf personenbezogenen Informationen (alle Attribute des Identity Stores) aufgebaut werden.

Event Based

Das Event-basierte SAP Provisioning Framework ermöglicht es, auf Events (Add, Modify, Delete) zu reagieren. Diese Events können auf Veränderungen des Identity Stores (Mitarbeiter-Neuanlage, Änderung einer Firmenadresse etc.) regieren. So kann einem Mitarbeiter bei einer Neuanlage im HCM beispielsweise aufgrund seiner organisatorischen Zuordnung und einer Arbeitsplatzbeschreibung ein Großteil seiner Berechtigungen automatisch zugewiesen werden. Mit dem SAP Provisioning Framework stellt SAP vorgefertigten Content bereit, der gängige Regeln und Prozesse abbildet. Auch die Veränderung der Berechtigungslage bei Abteilungswechsel oder Kündigung (Deprovisioning, Sperren, Abgrenzen etc.) wird damit automatisiert, was einen Sicherheitsvorteil darstellt, da Berechtigungsanhäufungen bzw. Benutzerleichen nicht mehr entstehen.

Dynamic Group Based

Einen weiteren Ansatz für die Zuweisung von Berechtigungen an die Person stellt SAP NetWeaver IdM in Form der Bildung von dynamischen Gruppen (MX_DYNAMIC_GROUP) bereit. Diese Gruppen verfolgen mit der Gruppierung von Rollen und der Zuordnung von Regeln den genau umgekehrten Ansatz, da die dynamischen Gruppen Business-Rollen repräsentieren und sich ihre Besitzer über Regeln suchen. Die zugehörigen Regeln und die Zuordnung zur Business-Rolle werden über Batch-Prozesse im Identity Center automatisiert generiert. Eine Regel kann beispielsweise alle internen Mitarbeiter einer bestimmten Org.-Unit an eine dynamische Gruppe und damit die Personen der Business-Rolle zuweisen. Diese Regeln werden in regelmäßigen Abständen ausgeführt (Recalculate), wodurch dynamisch auf die Veränderungen der Benutzerstamms (Wechsel Abteilung/Org.-Unit) reagiert wird.

3.7.5.2 WORKFLOW-BASIERTE ZUWEISUNG

Berechtigungen/Rollen/Gruppen/Verzeichnisse etc. können über das Workflow-basierte Antragsverfahren in SAP NetWeaver IdM in Form von Formularen beantragt werden. Oftmals kann die manuelle Beantragung von technischen Berechtigungen (MX_PRIVILEGE) nur über bzw. mit IT-Mitarbeitern erfolgen, da aufgrund der Fülle der Berechtigungen und der oftmals technischen Benennungen eine Auswahl schwerfällt. Damit auch Fachabteilungen Berechtigungen vergeben können, werden die MX_PRIVILEGE-Objekte zu arbeitsplatzbezogenen Business-Rollen (MX_ROLE) zusammengefasst. Diese haben dann einen sprechenden Namen und einen beschreibenden Text, der die Beantragung erleichtert.

Business-Rollen auf Basis von RBD:

Basierend auf dem in Abschnitt 3.6.2 beschriebenen Business Role Design (RBE), welches ausschließlich Business-Rollen in SAP-Systemen berücksichtigt, können diese systemspezifischen Business-Rollen durch die Abbildung in SAP NW IdM in Form von MX_ROLE Entry Types mit Berechtigungen aus Non-SAP-Systemen erweitert werden und systemübergreifende Business-Rollen (MX_ROLE) erstellt werden. Die Generierung der Business-Rollen auf den systemspezifischen Business-Rollen erfolgt über Batchprozesse im Identity Center.

Business-Rollen-Modell in SAP IdM erstellen:

Wird ein Business-Rollen-Modell neu im SAP IdM erstellt, bietet sich an, das systemübergreifende Business-Rollen-Modell (Fachrollen-Modell) in Form einer Excel-Arbeitsmappe zu modellieren, welche dann über die Standard-File-Schnittstelle des SAP NetWeaver Identity Management Identity Centers dem Datenmodell hinzugefügt wird. Dabei werden die MX_ROLE-Objekte und deren zugehörige Attribute definiert und in den Identity Store importiert. Über das IdM User-Interface können dann den Informationsverantwortlichen und

Fachabteilungen User-Interfaces bereitgestellt werden, in denen sie das Business-Rollen-Modell webbasiert pflegen können. Hierzu zählen Prozesse wie:

- Berechtigungen (MX_PRIVILEGE) einer Business-Rolle (MX_ROLE) entziehen/hinzufügen
- Business-Rollen (MX_ROLE) schachteln
- Business-Rollen-Owner (MX_OWNER) ändern
- etc.

Pflege der Business-Rollen

Die beschriebene Modellierung auf Basis einer zentralen Excel-Arbeitsmappe kann sowohl als initiale Quelle für den Rollout des Business-Rollen-Modells (Berechtigungskonzept) dienen, kann aber auch die dauerhafte zentrale führende Quelle für die Modellierung des Business-Rollen-Modells (Berechtigungskonzeptes) sein und die oben beschriebenen delegierbaren webbasierten Prozesse ersetzen. Dabei können Teile der Arbeitsmappe in die Länder und Fachabteilungen rausgegeben werden. Bei Änderungen oder Erweiterungen (Länder-Rollout) würde dann ein Update des Identity Stores mit der Excel-Arbeitsmappe über eine Standardschnittstelle stattfinden.

Zusätzlich kann über das IdM UI den Fachabteilungen ein User-Interface zur Pflege des Rollenmodells bereitgestellt werden. Dabei ist es möglich, aus dem Set der technischen Berechtigungen (MX_PRIVILEGE) die Business- Rollen (MX_ROLE) zusammenzusetzen, Business hierarchisch zu schachteln sowie Optionen wie Sichtbarkeit, SOD-Definition etc. festzulegen. Die folgende Abbildung zeigt ein User-Interface zur Pflege von Business-Rollen im IdM UI.

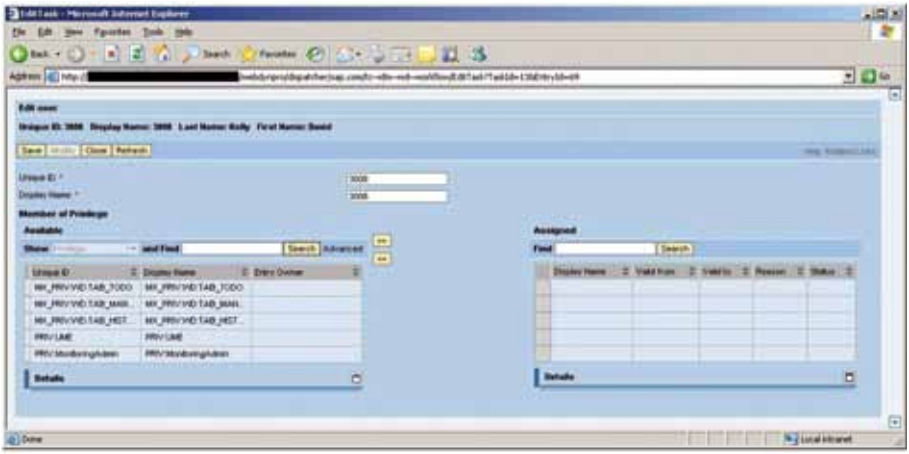

Abb. 21: IdM UI zur Pflege der Business-Rollen

Neben der Pflege und Modellierung der Business-Rolle, gehören die Definitionen einer zugehörigen Approval-Strategie zu weiteren Optionen, die über das IdM UI delegiert werden kann. Die Approval-Strategie beinhaltet Regelwerke zur Festlegung der Personen, welche die Beantragung einer Business-Rolle genehmigen

müssen. Alle genannten Prozesse zur Pflege und Modellierung von Business-Rollen können selbst einen Genehmigungsworkflow auslösen.

Aufbau der Business-Rollen

Das Datenmodell stellt die Zuordnung von Business-Rollen bidirektional in Form einer Container-Beziehung her. Dabei wird in der Business-Rolle (MX_ROLE) im Attribut MXMEMBER_MX_PERSON einer Liste der Personen gespeichert, die dieser Rolle zugeordnet sind. Im Personen-Objekt (MX_PERSON) wird die Referenz zur Rolle (MXREF_MX_ROLE) gespeichert. Die Zuordnung der Berechtigungen (MX_PRIVILEGE) zur Business-Rolle (MX_ROLE) findet ebenfalls über eine bidirektionale Container-Beziehung statt. Dabei werden in der Business-Rolle (MX_ROLE) im Attribut MXMEMEBER_MX_PRIVILEGE die enthaltenen Berechtigungen (MX_PRIVILEGE) gespeichert. Auf Seite der Berechtigungen (MX_PRIVIELGE) wird die Referenz zur Business-Rolle im Attribut MXREF_MX_ROLE gespeichert. Eine Schachtelung von Business-Rollen (MX_ROLE) und von Berechtigungen (MX_PRIVILEGE) findet ebenfalls über eine bidirektionale Container-Beziehung statt. Die folgende Abbildung zeigt die Container-Beziehung im SAP IdM.

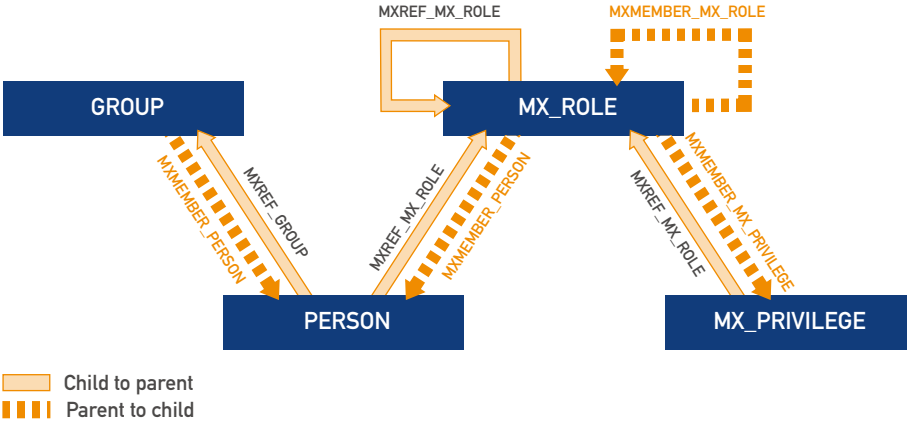

Abb. 22: Aufbau der Business-Rollen

Für weitere Details zur Abbildung des Rollenmodells in SAP NetWeaver Identity Management sei an dieser Stelle auf das SDN verwiesen[32].

Die folgende Abbildung zeigt den Zusammenhang zwischen Business-Rollen (MX_ROLE) und technischen Berechtigungen (MX_PRIVILEGE) und den Berechtigungen im SAP BusinessObjects Access Control.

32 SDN, Identity Store Schema, http://www.sdn.sap.com/irj/scn/go/portal/prtroot/docs/library/uuid/f0d87115-36da-2b10-7b89-996efe422b2a?QuickLink=index&overridelayout=true

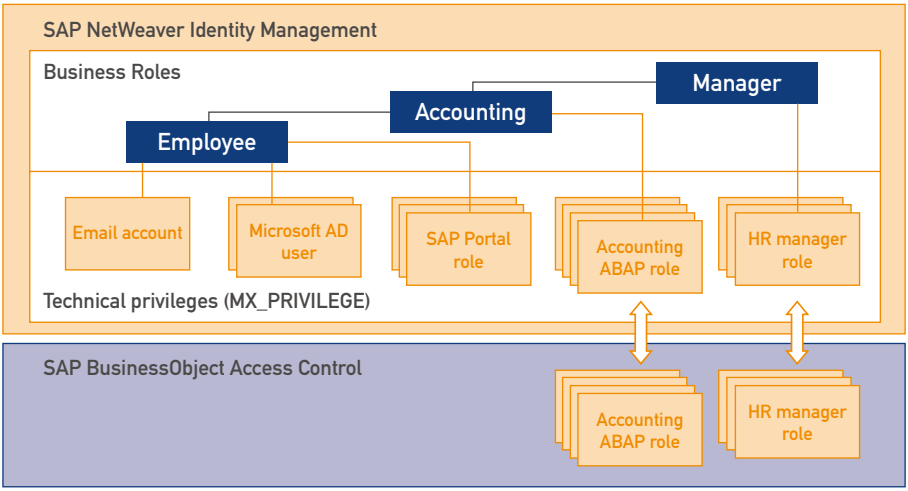

Abb. 23: Berechtigungen und Rollen des CIM-Integrationsszenarios

Die Berechtigungen der Business-Rolle, die keine hohen Compliance-Anforderungen haben, werden automatisiert direkt von SAP NetWeaver Identity Management provisioniert. Business-Rollen mit Berechtigungen mit hohen Compliance-Anforderungen werden nach der Genehmigung mittels Genehmigungs-Workflow im SAP IdM zusätzlich automatisiert an SAP BusinessObjects Access Control zur integrierten Risikoanalyse übergeben.

Wird eine Business-Rolle im SAP NetWeaver IdM einem Benutzer zugewiesen, welche MX_PRIVILEGE-Objekte beinhaltet, die aufgrund der hohen Compliance-Anforderungen über SAP BusinessObjects provisioniert werden sollen, werden die Berechtigungen (MX_PRIVILEGE) gruppiert nach Zielsystem an Access Control übergeben. Dadurch finden keine unnötigen Anfragen an SAP BusinessObjects AC mehr statt und der Austausch der Anfragen wird optimiert. Diese Gruppierung findet über die Attribute MX_PRIV_GROUP_ATTR_OPERATION, MX_PRIV_GROUPING_APPLICATION und MX_PRIV_GROUPING_GUID des MX_PENDING_VALUE Object im SAP NetWeaver IdM statt. Mit der Gruppierung wurde das Integrationsszenario Compliant Identity Management weiter optimiert. Wie der Roadmap von SAP NetWeaver IdM zu entnehmen ist, ist eine enge Integration der Produkte stark im Fokus[33].

3.7.6 BESCHREIBUNG DER CIM-ARCHITEKTUR

Die Architektur von Compliant Identity Management besteht aus Komponenten von SAP NetWeaver IdM und SAP BusinessObjects Access Control. Eine direkte Integration zwischen den Systemen findet über den Virtual Directory Server von SAP NetWeaver IdM und CUP von SAP BusinessObjects Access Control statt. Aufbau und Kommunikationswege des Szenarios werden anhand der folgenden Abbildung erläutert.

33 Fragen Sie Ihren SAP Account Executive nach der aktuellen SAP NetWeaver IdM Roadmap

3 SAP BusinessObjects Access Control 5.3

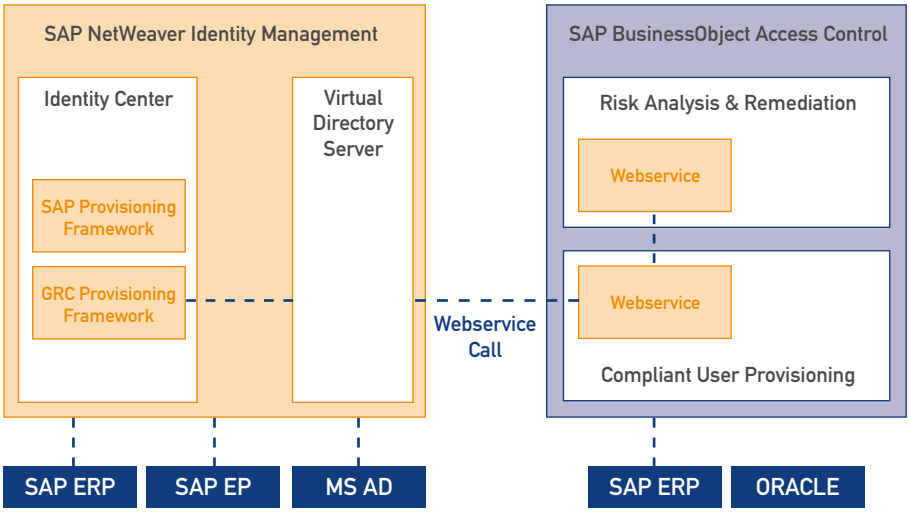

Abb. 24: Architektur von Compliant Identity Management

Für die Integration der Analyse- und Simulationsfunktionalitäten von SAP BusinessObjects Access Control stellt SAP NetWeaver IdM fertigen Provisioning-Content zur Verfügung. Die Provisioning-Logik wird durch das GRC Provisioning Framework bereitgestellt. Dieses Framework stellt Logik speziell für SAP BusinessObjects Access Control im Identity Center bereit. Dieser Content besteht aus Provisionierungsfunktionalität im Identity Center von SAP NetWeaver IdM und wird direkt in das Identity Center importiert. Damit setzt das GRC Provisioning Framework auf dem SAP Provisioning Framework auf, welches Rule-Based Provisioning im SAP NetWeaver IdM ermöglicht. Somit steht im SAP NetWeaver IdM umfangreiche Provisionierungsfunktionalität für die Integration mit SAP BusinessObjects Access Control bereit.

Die Provisioning-Funktionalität ermöglicht es, Regeln festzulegen, mit denen definiert wird, welche Anträge für eine Compliance-Prüfung an SAP BusinessObjects Access Control übergeben werden. Als Schnittstelle dient der Virtual Directory Server von SAP NetWeaver IdM, der eine fertige Schnittstelle zu SAP BusinessObjects Access Control bereitstellt. Die Kommunikation zwischen Identity Center und VDS findet über eine speziell für dieses Integrationsszenario bereitgestellte LDAP-Schnittstelle statt. Die Access-Control-Schnittstelle leitet die Anfragen für Berechtigungen mit hohen Compliance-Anforderungen über Webservices an SAP BusinessObjects Access Control weiter. Sowohl die Schnittstelle zwischen Identity Center und VDS als auch zwischen VDS und Access Control wird „out of the box" verfügbar gemacht und muss lediglich konfiguriert werden. Die Webservices werden durch die Webservice API von SAP BusinessObjects Access Control bereitgestellt.

Die wichtigsten Webservices sind in folgender Tabelle dargestellt.

FUNKTIONALITÄT	WEBSERVICE
Submit Request	SAPGRC_AC_IDM_SUBMITREQUEST gibt einen Antrag an BusinessObjects Access Control.
Select Application	SAPGRC_AC_IDM_SELECTAPPLICATION gibt die in SAP BusinessObject AC konfigurierten Tochtersysteme zurück.
Search Role	SAPGRC_AC_IDM_SEARCHROLES ermöglicht die Suche nach Rollen, bevor ein Antrag an BusinessObjects AC gesendet wird.
Role Details	SAPGRC_AC_IDM_ROLEDETAILS gibt detailierte Informationen zu einer Rolle.
Request Status	SAPGRC_AC_IDM_REQUESTSTATUS gibt Informationen über einen bestimmten Antrag zurück.
Audit Trail	SAPGRC_AC_IDM_AUDITTRAIL gibt die Auditinformationen von GRC Access Control zurück. (Audit Log und historische Provisioning-Informationen-Daten).

Abb. 25: Wichtige Webservices für CIM

SAP BusinessObjects Access Control stellt über eine Webservice API alle wichtigen Funktionalitäten dem SAP NetWeaver Identity Management zur Verfügung. Anhand der Abbildung 25 „Wichtige Webservices für CIM" lässt sich die Kommunikation zwischen SAP NetWeaver IdM und SAP BusinessObjects Access Control verdeutlichen. Zunächst werden über einen vom GRC Provisioning Framework bereitgestellten Job alle Systeme und technischen Rollen, für die eine Compliance-Prüfung notwendig ist und die deshalb bereits am SAP BusinessObjects Access Control angeschlossen sind, in den Identity Store von SAP NetWeaver IdM geladen. Damit wird SAP NetWeaver IdM bekannt gemacht, für welche Systeme die Berechtigungen an SAP BusinessObjects Access Control weitergegeben werden. Die Weitergabe der Anträge erfolgt über den Aufruf des Webservices SAPGRC_AC_IDM_SUBMITREQUEST über die IdM Middleware SAP VDS. Damit wird die Anfrage an SAP BusinessObjects Access Control übergeben. SAP NetWeaver IdM wartet von nun an über den Webservice SAPGRC_AC_IDM_REQUESTSTATUS auf den Status der Anfrage. In SAP BusinessObjects Access Control wird ein Workflow in CUP ausgelöst, der eine Risikoanalyse über RAR beinhaltet. Je nach Konfiguration in CUP kann diese Risikoanalyse automatisch durchgeführt werden oder über einen Button manuell von derjenigen Person angefordert werden, welche die Berechtigungsvergabe genehmigen soll. In beiden Fällen bekommt die Person die Ergebnisse dieser Risikoanalyse, wie in CUP üblich, zur Genehmigung vorgelegt und kann ablehnen oder genehmigen und ggf. eine Kontrolle einplanen. Die Provisionierung wird anschließend von Access Control durchgeführt. SAP NetWeaver IdM erhält die entsprechende Statusmeldung und nimmt die Rollenzuordnung im Identity Center vor.

34 SDN, SAP NetWeaver IdM – Initial Configuration Guide: https://websmp103.sap-ag.de/~sapidb/011000358700001449642008E

Für die Workflowkonfiguration von CUP sei an dieser Stelle auf SAP WIKI verwiesen, in dem verschiedene Möglichkeiten bei der Gestaltung von Workflows beschrieben werden. Der folgende Abschnitt 3.7.7 listet die Voraussetzungen auf, die in den einzelnen Komponenten vorausgesetzt werden sowie die Konfigurationen, die für Compliant Identity Management nötig sind.

3.7.7 TECHNISCHE VORAUSSETZUNGEN

Im Folgenden werden die Voraussetzungen an die Komponenten beschrieben. Auf Seiten von SAP BusinessObjects Access Control sind keine für das Integrationsszenario spezifischen Konfigurationen nötig. Konfigurationen für die Integration sind nur auf Seiten von SAP NetWeaver IdM notwendig. Im Folgenden sind die für das Integrationsszenario notwendigen Voraussetzungen an die Komponenten dargestellt.

Die Konfigurationen sind in der Dokumentation im SDN detailliert nachzuschlagen.[34]

- Die Komponente Identity Center von SAP NetWeaver Identity Management muss installiert und initial konfiguriert werden.
- Das SAP Provisioning Framework muss installiert und initial konfiguriert werden.
- SAP NetWeaver IdM Virtual Directory Server muss installiert sein.

Für die Komponenten von SAP BusinessObjects Access Control wird Folgendes für Compliant Identity Management vorausgesetzt.

- Die Komponente CUP ist zu installieren und initial zu konfigurieren.
- Die gewünschten Genehmigungsschritte und Workflows sind auf die eigenen Bedürfnisse anzupassen.
- Die Komponente RAR muss installiert und initial konfiguriert werden.
- In RAR müssen Kontrollen definiert und die Standardprüfregeln angepasst werden.

Für das Sizing der Systeme sei auf folgende Dokumente verwiesen:

- Sizing Access Control[35]
- Sizing SAP Identity Management[36]

3.7.8 ZUSAMMENFASSUNG

Im Kapitel 3.7 wurden Aspekte einer Integration von SAP NW IdM und Access Control beschrieben. Es wurde dargestellt, wie SAP BusinessObjects Access Control Funktionalitäten dem SAP NetWeaver IdM zur Verfügung stellt. Unternehmen erweitern damit ihre bestehenden Genehmigungsworkflows ihrer Identity-Management-Lösung um eine Risikoanalyse, wodurch technisch gewährleistet wird, dass ein einmal erstelltes Berechtigungskonzept qualitätsgesichert wird. Damit kommen Unternehmen der in Kapitel 2.2 beschriebenen regulatorischen Anforderungen zur Einrichtung eines internen Kontroll- und Risikomanagement Systems nach.

Der integrierte Ansatz unterstützt Unternehmen bei der Einrichtung eines zentralen Identitätsmanagements und Zugriffsmanagements mit integriertem Risikomanagement als Teil des internen Kontrollsystems. SAP Identity Management liefert mit seinem zentralen Identity Store nicht nur die personenbezogenen

35 SAP InstGuides, AccessControl Master Guide, https://websmp109.sap-ag.de/~form/sapnet?_SHORTKEY=00200797470000088116&_SCENARIO=01100035870000000202&_OBJECT=011000358700000343632008E

36 SAP InstGuides, SAP Identity Management 7.1, https://websmp108.sap-ag.de/~form/sapnet?_SHORTKEY=01100035870000706149&_SCENARIO=01100035870000000202&?_SHORTKEY=01100035870000706149&_SCENARIO=01100035870000000202?_SHORTKEY=01100035870000706149&_SCENARIO=01100035870000000202&?_SHORTKEY=01100035870000706149&_SCENARIO=01100035870000000202

Stammdaten und Berechtigungsdaten, sondern auch die Auditing-Informationen des Vergabeprozesses und schafft damit die Datengrundlage für ein erfolgreiches Risikomanagement (Anforderung aus: Corporate Governance Kodex, vgl. Kapitel 2.2.1). In Verbindung mit der Risikodefinition in Access Control ist auch die Datengrundlage zur Risikoerfassung, Bewertung und Steuerung gegeben (Anforderung aus: KonTraG, vgl. Kapitel 2.2.2). Durch den zentralen Identity Store unterstützt SAP NW IdM die Schaffung von Vertraulichkeit, Integrität, Verfügbarkeit, Authentisierung, Authentizität und Verbindlichkeit der angeschlossenen Systeme (Anforderung aus: IDW RS FAIT 1, vgl. Kapitel 2.2.3). Durch die Berücksichtigung der gesamten heterogenen Systemlandschaft ermöglicht SAP IdM die Unterstützung des Berechtigungskonzeptes für kritische Systeme wie Archivierungssysteme (Anforderung aus: IDW RS FAIT 2, vgl. Kapitel 2.2.4). Durch die Umsetzung von Funktionstrennung und Zugriffsbeschränkung ist CIM Teil des internen Kontrollsystems und damit Bestandteil der Umsetzung von Compliance (Anforderung aus: IDW Prüfungsstandards, vgl. Kapitel 2.2.6). Durch Validierung und Konsolidierung der Daten in SAP NW IdM wird die Richtigkeit und Vollständigkeit der Daten sichergestellt (Anforderung aus: IDW PS 330, vgl. Kapitel 2.2.7).

3.8 TECHNISCHE RAHMENBEDINGUNGEN

Aufgrund der Fülle an verfügbarer technischer Dokumentation zum Thema Access Control von Seiten der SAP soll hier auf eine detaillierte Ausführung verzichtet werden. Vielmehr wird hier ein kurzer Überblick gegeben, um dann auf weiterführende Dokumentationen zu verweisen.

3.8.1 INSTALLATIONSVORAUSSETZUNGEN

Vor der Installation von Access Control 5.3 sollten auf dem Server folgende Softwarekomponenten bereits installiert sein:

- SAP NetWeaver 7.0 (2004s) SP12
- SAP Internet Graphics Service (SAP IGS), erforderlich für die Darstellung der Management Reports

Für die Anbindung von Access Control an die jeweiligen Backends sind Real Time Agents (RTA) notwendig, die folgende Voraussetzungen haben:

- SAP ERP 4.6C: Support Pack Stack level 55
- SAP ERP 4.70: Support Pack Stack level 63
- SAP ERP 04: Support Pack Stack level 21
- SAP ERP 6.0: Support Pack Stack level 13

Anmerkung: Es existieren SAP-Notes in den Installationsdokumenten, die auch niedrigere SPs für die RTAs ermöglichen.

37 Vgl. Kapitel 3.8.2.1 Mehrstufige Systemlandschaft

3.8.2 TECHNISCHE ARCHITEKTUR

Access Control wird als Java-Komponenten auf einem SAP NetWeaver Application Server Java 7.0 installiert. In den meisten Fällen wird eine 2-stufige Systemlandschaft gewählt[37]. Die eigentliche Funktionalität entsteht durch die Systemverbindung zu den Backends. Für die „Connectivity" stehen folgende Komponenten zur Verfügung:

- RTA wird als Add-on auf SAP-ABAP-Systemen installiert
- EPRTA wird als Java-Komponente auf SAP NetWeaver Portal installiert
- Identity Management wird per Webservices angebunden
- Greenlight Adapter werden für JDEdwards, Oracle, PeopleSoft genutzt
- Um Risikoprüfungen für Systeme zu machen, die über o.g. Techniken nicht angeschlossen werden können, gibt es die Anbindung über Flat-File

Im Detail nun die Anschlussfähigkeit der jeweiligen Access-Control-Komponenten:

- Risk Analysis and Remediation:
  - SAP-Systeme mit Basis Release 4.6C, 6.20, 6.40 and 7.10
  - SAP NetWeaver Portal 7.0 SP12+
  - PEOPLESOFT, JDE EnterpriseOne, ORACLE mit Greenlight Adapter
  - Legacy Systeme via Flat-File Interface

- Compliant User Provisioning:
  - SAP-Systeme mit Basis Release 4.6C, 6.20, 6.40 and 7.10
  - SAP NetWeaver Portal 7.0 SP12+
  - PEOPLESOFT, JDE EnterpriseOne, ORACLE mit Greenlight Adapter

- Enterprise Role Management:
  - SAP-Systeme mit Basis Release 4.6C, 6.20, 6.40 and 7.10

- Superuser Privilege Management:
  - SAP-Systeme mit Basis Release 4.6C, 6.20, 6.40 and 7.10

Weiterhin werden von Access Control Webservices zur Verfügung gestellt, Identity-Management-Systeme (IdM) anzubinden. Hier gibt es eine besondere Integration zu SAP NetWeaver Identity Management.

Zusätzlich bietet Access Control 5.3 eine Integration mit SAP Business Warehouse 7.0 an, in dem es BI Content zur Verfügung stellt.

3.8.2.1 EINSATZ VON ERM FÜR DIE ROLLENENTWICKLUNG – MEHRSTUFIGE SYSTEMLANDSCHAFT

Die Empfehlung einer mehrstufigen Systemlandschaft für Access Control ist aus den Erfahrungen der ersten Implementierungen der Mitglieder des DSAG-Arbeitskreises abgeleitet und von einigen Rahmenbedingungen wie Unternehmenspolicy sowie technischen Einschränkungen geprägt.

Eine Systemlandschaft muss in enger Anlehnung an die im Unternehmen existierende Policy erstellt werden.

Schreibt diese vor, dass alle Konfigurationsänderungen zunächst nur im Entwicklungssystem (DEV) durchgeführt und danach im Qualitätssicherungssystem (QA) getestet & geprüft und erst nach finaler Freigabe in die Produktion (PROD) übergeführt werden dürfen, so sollte eigentlich auch für Access Control eine zwei- oder dreistufige Landschaft existieren.

Die folgende Abbildung zeigt ein schematisches Beispiel einer in der Praxis häufig vorkommenden zweistufigen GRC Access Control-Systemlandschaft:

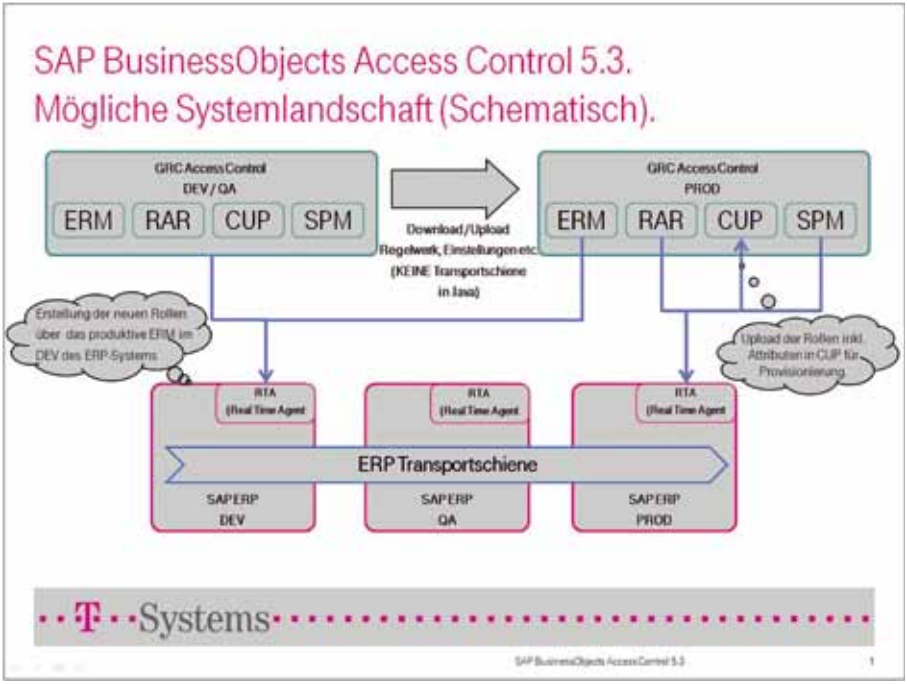

Abb. 26: 2-stufige Systemlandschaft SAP BO Access Control

Folgende Komponenten von Access Control unterliegen in einer mehrstufigen Landschaft Änderungsprozessen:

1. die technische und funktionale Konfiguration von Access Control selbst: technische Updates, Service Packs, Batch Jobs etc.
2. die Risikokontrollmatrix für die Entwicklungs-, QA- und Produktionssysteme, einschließlich von notwendigen neuen und geänderten Risiken und Kontrollen, die aufgrund einer neuen Risikobewertung entstehen
3. die SAP-Rollen für die Entwicklungs-, QA- und Produktionssysteme

3 SAP BusinessObjects Access Control 5.3

Ein klassisches Transportwesen (ABAP-basiertes TMS) bei Access Control für Rollen als auch für die Risikomatrix existiert in den Versionen 5.3 und älter nicht. Ein solches Transportwesen ist erst für die komplett neue Version 2010 vorgesehen. Ab dann wird voraussichtlich das klassische Transportwesen für die Risikomatrix und die mit dem ERM erstellten Rollen (also inkl. der Organisationswerte) durchgängig in Access Control abbildbar sein.

Bis dahin bietet aber auch Access Control 5.3 verschiedene Möglichkeiten des Transports:

1. Für SAP-Rollen im Backend kann der Transport weiterhin klassisch im Backend selbst durch die ABAP-Transportschiene erfolgen. Rollen, die in ERM im DEV-ERP-System entwickelt wurden und nach QA-ERP transportiert wurden, sind dann auch im CUP für die weitere User-Provisionierung erkennbar, falls das DEV-ERP- und QA-ERP-System nur mit einer Access-Control-Instanz betrieben wird. Falls Access Control zwei Instanzen hat, so müssen die Backend-Rollen nach erfolgtem Transport in die Ziel-ERP-Umgebung wieder per Hochlade-Mechanismus von Access Control mit dem entsprechenden Assignment von Organisations-Attributen in die CUP-Komponente hochgeladen werden.

2. Änderungen an der Risikomatrix können durch entsprechenden Download der Matrix im DEV-Access Control System in die Produktionsinstanz von Access Control hochgeladen werden. Einen kontrollierten Transportmechanismus mit Änderungsverfolgung gibt es indes hier noch nicht. Dieser kann durch den Einsatz des von SAP erweiterten Transportwesens „Change and Transport System (CTS+) erreicht werden[38].

Erlaubt die Unternehmenspolicy eine nicht so eng für die Trennung zwischen Entwicklung, QA und Produktion gefasste Implementierung, empfiehlt sich eine zweistufige Architektur für Access Control.

Auch um den vorgenannten Transporteinschränkungen besser gerecht zu werden, wird heute meist ein zweistufiges Access Control dem dreistufigen vorgezogen – ein System für DEV und QA zusammen und ein eigenes System für PROD.

Dies ermöglicht für die Risikokontrollmatrixentwicklung wie auch für die Rollenentwicklung einen durchgängigeren Änderungsmanagementprozess und in der Produktion wird dann nur noch die Rolle durch CUP zugeordnet.

Der Änderungsmanagementprozess würde dann wie folgt ablaufen (siehe auch Abbildung 27):

(A) DEV-QA-Instanz von Access Control:

Testphase:

1. Übernahme (Upload) oder Entwicklung der Risikokontrollmatrix für die Test-Systeme.
2. Entwicklung und Änderung der Rollen mit dem ERM für die Test-Systeme.
3. Durchführung des funktionalen/technischen Tests der Rollen und der Risiken auf den Testsystemen durch Testuser.

38 Die erweiterten Funktionen des CTS stehen mit dem Einspielen des Support Package Stack (SPS) 15 des SAP NetWeaver 7.0 zur Verfügung. Zusätzlich wird ein SAP Application Server Java mit dem gleichen Support-Package-Stand benötigt. SAP empfiehlt die Konfiguration eines Dual-Stack-Systems.

Falls der Test erfolgreich war, werden die Rollen weiter auf die QA-Systeme überführt. Die Risikokontrollmatrix (Masterregelsatz) gilt für beide Backend-Systeme (DEV und QA) und brauchen nicht neu geladen zu werden.

Die Rollen werden mit Hilfe des ABAP-Transportwesens vom DEV-Backend auf das QA-Backend transportiert. ERM wie CUP des DEV-QA Access Control erkennen die Org-Attribute (Rolleneigner, Department, etc.) der bestehenden Rollen des QA-Backend.

Qualitätssicherungsphase:

Hier können eventuell weitere Änderungen an der Risikokontrollmatrix und den Rollen durch Workflow vorgenommen werden.

Sind die prozessualen Tests auf den QA-Systemen abgeschlossen, erfolgt die Übergabe in die Produktions-Backend-Systeme.

Die Risikokontrollmatrix wird vom DEV-QA-Access Control heruntergeladen (Download) und die Rollen per ABAP-Transport von den QA-Systemen in die Produktions-Systeme (Backend) überführt.

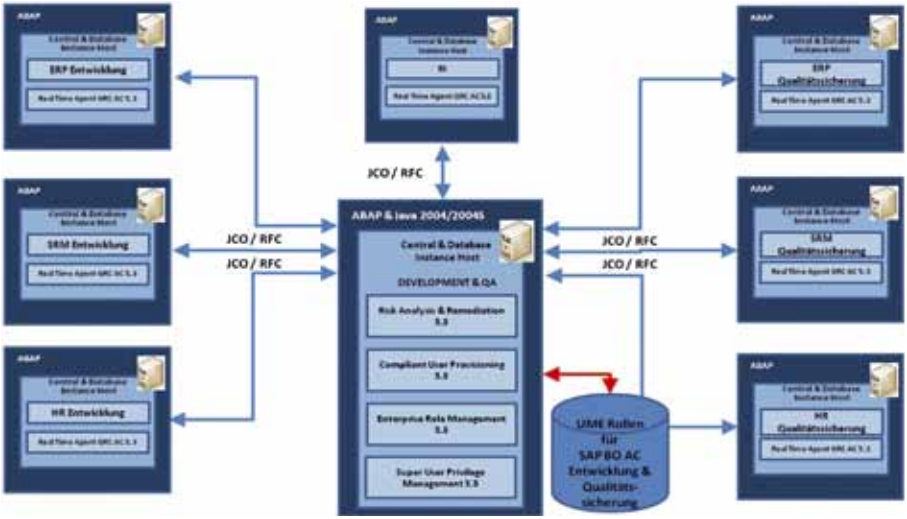

Abb. 27: SAP BO Access Control Entwicklungs- und Qualitätssicherungsumgebung

(B) Produktionsinstanz von Access Control (vgl. Abb. 28):

Im Produktionssystem Access Control muss die Risikokontrollmatrix vom DEV-QA-Access Control hochgeladen werden (Upload).

3 SAP BusinessObjects Access Control 5.3

Die Rollen, die bereits auf das Produktions-Backend-Systemen transportiert wurden, müssen nun auch ins produktive Access Control in die CUP-Komponente hochgeladen werden, um die Attribute der CUP-Komponente (speziell Genehmigungsworkflow) bekannt zu machen.

Produktionsphase:

4. In der Produktion sollten keine Änderung mehr an der Kontrollmatrix wie an den Rollen vorkommen werden, sondern nur noch deren Zuordnung an die Anwender (mit Risikoprüfung!).

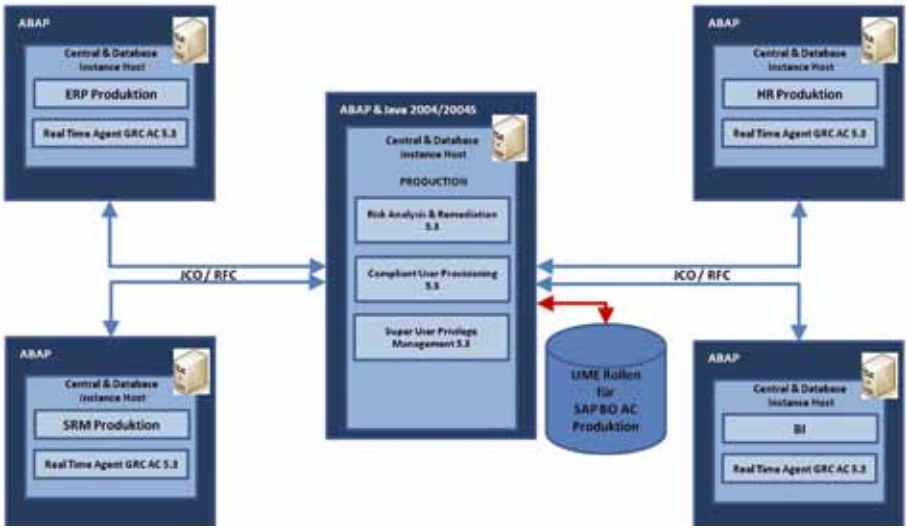

Abb. 28: SAP BO Access Control Produktionsumgebung

3.8.2.2 EINSATZ VON PFCG FÜR DIE ROLLENENTWICKLUNG

Mit den Funktionen der Benutzer- und Rollenverwaltung des AS ABAP verwalten Sie die Benutzer, Rollen und Berechtigungen in ABAP-Systemen. Die Rollenpflege erfolgt dabei mit der Transaktion PFCG. Im Folgenden haben wir die Vorteile und Nachteile der Benutzer- und Rollenverwaltung mittels PFCG der Vollständigkeit halber kurz aufgeführt:

Vorteile des Einsatzes von PFCG:

- Anwender sind meist vertraut im Umgang mit der PFCG
- Menüstrukturen können definiert werden
- Alle Anwendungsarten (wie z. B. BSPs, Webanwendungen, Reports etc.) können ausgeprägt werden
- Risk Terminator (Komponente von Access Control) kann verwendet werden, um eine Risikoanalysestufe in den Prozess einzubauen
- Vorhandene Transport- und Freigabeprozesse können beibehalten werden

Nachteile des Einsatzes von PFCG:

- Komplexere Zustimmungsworkflows für Rollenänderungen sind nicht möglich, weiterhin besteht die Gefahr, dass Rollen zu sehr IT-zentriert entwickelt werden, d. h., Business Owner übernehmen nicht die Verantwortung für die Rollenentwicklung
- Rollen müssen nach dem Transport mit „Hochladeskripten" in die CUP-Komponente (Compliant User Provisioning) von SAP Business Objects Access Control mit Attributen versehen und hochgeladen werden (wie Org-Einheit, Owner etc.)
- Rolleneignerprinzip wird nicht „gelebt"

3.8.3 WEITERFÜHRENDE DOKUMENTATION

Die Standard-Produkt-Dokumentation (Installation, Konfiguration, Master etc.) befindet sich auf SAP Service Marketplace unter http://service.sap.com/instguides -> Access Control.

Ein Sizing Guide befindet sich auf http://service.sap.com/sizing.

SAP veröffentlicht auch zusätzlich eine große Anzahl von „How-to Guides", auf die wir an dieser Stelle hinweisen möchten. Diese befinden sich unter http://www.sdn.sap.com/irj/bpx/grc -> GRC How-to Guides.

Hier möchten wir im Speziellen auf folgende How-to Guides hinweisen:

- SAP Access Control 5.3 - Pre-Installation
- SAP Access Control 5.3 - Post-Installation – RAR, CUP, ERM, SPM
- SAP Access Control 5.3 - How-to - Apply Support Packages in AC5.3
- How-to Configure SAP BusinessObjects Access Control 5.3 for SAP NetWeaver Portal 7.0
- SAP Access Control - How-to - Integrate GRC AC53 CUP and NW IdM
- How-to Integrate Access Control 5.3 and Business Warehouse 7.0

Eine Übersicht aller wichtigen SAP Notes zum Access Control befindet sich auf BPX unter http://www.sdn.sap.com/irj/scn/articles-grc-all -> AC Useful SAP Notes for Access Control Customers.

Die Anwenderdokumentation findet man auf http://help.sap.com -> Business User -> GRC.

4 Premium-Sponsoren

Mit freundlicher Unterstützung von:

T-SYSTEMS INTERNATIONAL GMBH

T-Systems International GmbH
Hahnstr. 43d
60528 Frankfurt am Main

Telefon 0800 TSYSTEMS (0800 87978367)
E-Mail: info@t-systems.com
Internet: www.t-systems.de

LEISTUNGSSPEKTRUM

- Beratung und Analyse
- Enterprise Risk Management
- SAP BO GRC Implementierung

SORGENFREIPAKET FÜR RISIKOMANAGEMENT UND INTERNE KONTROLLSYSTEME

Fast alle Risiken haben ihren Ursprung in den Prozessen. In der Beratungs- und Analysephase nimmt T-Systems alle relevanten IT-Systeme und Prozesse unter die Lupe, um die einzelnen Change-Maßnahmen und notwendigen Kontroll-Automatismen des Internen Kontrollsystems festzulegen. Durch unser bereichsübergreifendes Konzept reduzieren wir das in den Prozessen innewohnende Risiko und stellen eine effizientere Risikoüberwachung sicher. Wie hoch ist Ihr aktuelles Risiko? Ein sorgfältiger Reifecheck verhilft Ihnen zu einem Sorgenfreipaket in exakt der richtigen Dimension. Im Rahmen des Risikomanagements werden Risiken identifiziert, bewertet, dokumentiert, um daraus die notwendigen Maßnahmen ableiten zu können. Speziell in der Harmonisierung von heterogenen Systemlandschaften besitzt T-Systems weitreichende Expertise. Auf dieser Basis und mit bewährten Methoden implementieren wir SAP BO GRC. Ziel ist immer ein insgesamt schlüssig sicheres System zu einem vertretbaren Aufwand. Durch das Zusammenspiel von SAP und T-Systems erhalten Sie eine ideale Kombination aus leistungsfähiger Anwendung und Know-how für die Implementierung.

ÜBER T-SYSTEMS

Mit einer weltumspannenden Infrastruktur aus Rechenzentren und Netzen betreibt T-Systems die Informations- und Kommunikationstechnik (engl. kurz ICT) für multinationale Konzerne und öffentliche Institutionen. Auf dieser Basis bietet die Großkundensparte der Deutschen Telekom integrierte Lösungen für die vernetzte Zukunft von Wirtschaft und Gesellschaft. Rund 45.300 Mitarbeiter verknüpfen bei T Systems Branchenkompetenz mit ICT-Innovationen, um Kunden in aller Welt spürbaren Mehrwert für ihr Kerngeschäft zu schaffen. Im Geschäftsjahr 2009 erzielte die Großkundensparte einen Umsatz von rund 8,8 Milliarden Euro.

Mit freundlicher Unterstützung von:

SAP AG

SAP AG
Dietmar-Hopp-Allee 16
69190 Walldorf
Deutschland

Fon: +49 (0) 08 00 – 5 34 34 24
Fax: +49 (0) 08 00 – 5 34 34 20
E-Mail: info.germany@sap.com
Internet: www.sap.de

LEISTUNGSSPEKTRUM

- Unternehmensweites Risikomanagement
- Automatisiertes Internes Kontrollsystem (IKS)
- Zentralisiertes Zugriffs- und Berechtigungsmanagement

Mit SAP-BusinessObjects-Lösungen für Governance, Risikomanagement und Compliance (GRC) halten Sie Vorschriften sicher ein, berücksichtigen alle wichtigen Governance- Aspekte und steuern nachhaltig Ihre geschäftlichen Risiken.

IHRE VORTEILE

- Alle kritischen Prozesse und Ereignisse in Ihrem Unternehmen lassen sich automatisiert überwachen. Direkt aus der Anwendung heraus werden angemessene Reaktionen eingeleitet.
- Sie werden in die Lage versetzt, automatisierte Kontrollen in allen Geschäftsbereichen zu etablieren und gleichzeitig die Wirksamkeit der Sicherheitsprüfungen zu testen.
- Die Software unterstützt die Prüfung, Kontrolle und Organisation des unternehmensweiten Rollen- und Berechtigungswesens und beugt somit allen Funktionstrennungsrisiken vor: Unberechtigte Zugriffe und krimineller Datenmissbrauch werden verhindert.
- Sie werden unterstützt, im Rahmen eines ganzheitlichen Konzepts zahlreiche branchenübergreifende und -spezifische Gesetze und Vorschriften sicher einzuhalten.

Durchdacht, innovativ und praxisgetrieben, so beschreiben die unabhängigen Analysten der Gartner Group die besonderen SAP-Technologien für „Continuous Controls Monitoring" – und bescheinigen SAP eine marktführende Position.*

* Gartner Report „Magic Quadrant for Continous Controls Monitoring", Datum der Veröffentlichung: 23. März 2010

T · · Systems ·

SAP