Entwicklung einer Methode für die unternehmensweite Autorisierung

D I S S E R T A T I O N
der Universität St. Gallen,
Hochschule für Wirtschafts-,
Rechts- und Sozialwissenschaften (HSG)
zur Erlangung der Würde eines
Doktors der Wirtschaftswissenschaften

vorgelegt von

Felix Wortmann

aus

Deutschland

Genehmigt auf Antrag der Herren

Prof. Dr. Robert Winter

und

Prof. Dr. Walter Brenner

Dissertation Nr. 3185

Difo-Druck GmbH, Bamberg 2006

Die Universität St. Gallen, Hochschule für Wirtschafts-, Rechts- und Sozialwissenschaften (HSG), gestattet hiermit die Drucklegung der vorliegenden Dissertation, ohne damit zu den darin ausgesprochenen Anschauungen Stellung zu nehmen.

St. Gallen, den 17. Januar 2006

Der Rektor:

Prof. Ernst Mohr, PhD

Vorwort

Die vorliegende Arbeit entstand im Rahmen meiner Tätigkeit als wissenschaftlicher Mitarbeiter in den Kompetenzzentren „Application Integration Management“ und „Integration Factory“ am Institut für Wirtschaftsinformatik der Universität St. Gallen. Zum Gelingen der Arbeit haben zahlreiche Menschen beigetragen, bei denen ich mich an dieser Stelle herzlich bedanken möchte.

Besonders danke ich meinem Doktorvater Prof. Dr. Robert Winter. Er hat die Dissertation durch seine inhaltliche Betreuung sowie das ausgezeichnete, praxisnahe Forschungsumfeld massgeblich gefördert. Herrn Prof. Dr. Walter Brenner danke ich für die Übernahme des Korreferates und für seine wertvollen, motivierenden Impulse.

Herrn Dr. Joachim Schelp, Projektleiter der Kompetenzzentren „Application Integration Management“ und „Integration Factory“ danke ich für die sehr freundschaftliche Zusammenarbeit und Unterstützung. Meinen Kolleginnen und Kollegen am Institut Christian Braun, Tobias Bucher, Ronny Fischer, Anke Gericke, Myriam Gröbli, Dr. Martin Hafner, Clemens Herrmann, Mario Klesse, Stephan Kurpjuweit, Florian Melchert, Dr. Jochen Müller, Christian Riege, Josef Rupprecht, Moritz Schmaltz, Alexander Schwinn, Matthias Stutz und Christian Wilhelmi danke ich für die vielen anregenden Diskussionen und die hervorragende Arbeitsatmosphäre. Für zahlreiche aufmunternde Worte und die grosse Unterstützung danke ich insbesondere auch den „guten Seelen“ des Lehrstuhls Monika Schlumpf und Bernadette Mayer-Schawalder.

Diese Arbeit ist in enger Zusammenarbeit mit der Praxis entstanden. Zahlreiche Unternehmensvertreter haben sich im Rahmen dieser Arbeit engagiert und ihr langjähriges Erfahrungswissen eingebracht. Besonders möchte ich mich bei Frau Ghislaine Ackermann Pfluger (Basler Versicherungen), Frau Gritta Wolf (Credit Suisse) und Herrn Jürgen Lorek (Generali Gruppe Schweiz) bedanken. Ausserordentlich viel zu dieser Arbeit haben Thomas Fuhrer und Bruno Honegger beigetragen (beide Winterthur Group). Für ihre freundschaftliche und umfangreiche Unterstützung bin ich ihnen sehr dankbar.

Während der Erstellung der Dissertation musste ich aussergewöhnliche gesundheitliche Herausforderungen meistern. Dabei haben mich zahlreiche Kollegen und Freunde unterstützt. Stellvertretend möchte ich mich an dieser Stelle bei Mark Bitter, Christian Braun, Markus Handke, Dr. Jochen Müller, Dr. Joachim Schelp, Nicola Soccodato und Christian Wilhelmi bedanken.

Mein tiefster Dank gilt meinen Eltern, Geschwistern – insbesondere meinem Bruder Dr. Florian Wortmann – und meiner Freundin Stephanie Braun. Sie alle haben mich jederzeit uneingeschränkt unterstützt und mir stets alle erdenkliche Hilfe zukommen lassen. Ihnen sei diese Arbeit gewidmet.

St. Gallen, 31. Januar 2006 Felix Wortmann

Inhaltsübersicht

Inhaltsverzeichnis

Abkürzungsverzeichnis

ACM	Association for Computing Machinery
ADF	Access Decision Function
AEF	Access Enforcement Function
AIX	Advanced Interactive Executive
AK	Autorisierungskomponente
ASG	Allen Systems Group
BECS	Business Engineering Case Studies
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien
BK	Berechtigungskonzept
BS	British Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Errichtungsgesetz
BVG	Berufliche Vorsorge
CCTA	Central Computer and Telecommunications Agency
CC AIM	Competence Center Application Integration Management
CC IF	Competence Center Integration Factory
CIO	Chief Information Officer
CICS	Customer Information Control System
COBIT	Control Objectives for Information and related Technology
CORBA	Common Object Request Broker Architecture
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CS	Credit Suisse
DIN	Deutsches Institut für Normung
DWH	Data Warehouse
EAI	Enterprise Application Integration
EAM	Enterprise Access Management
EDV	Elektronische Datenverarbeitung
ERBAC	Enterprise Role-Based Access Control
ERP	Enterprise Ressource Planning
FBI	Federal Bureau of Investigation
GCIO	Government Chief Information Office
HSG	Universität St. Gallen (Hochschule St. Gallen)
ICT	Information and Communication Technology

IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IMG	Information Management Group
IMS	Information Management System
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ITIL	IT Infrastructure Library
IWI-HSG	Institut für Wirtschaftsinformatik der Universität St. Gallen
HR	Human Resources
ID	Identifikator
IT	Informationstechnologie
ITSMF	IT-Service-Management Forum
IS	Information System
J2EE	Java 2 Platform Enterprise Edition
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards and Technology
NSW	New South Wales
OA	Office Automation
PCAOB	Public Company Accounting Oversight Board
PL/I	Programming Language One
PT	Personentag
RACF	Resource Access Control Facility
RBAC	Role-Based Access Control
Rep.	Repository
SEC	Securities and Exchange Commission
SOX	Sarbanes-Oxley Act
SWOT	Strength Weaknesses Opportunities Threats
TAP	Technical Application Platform
TP	Transaction Processing
UML	Unified Modeling Language

Abbildungsverzeichnis

Tabellenverzeichnis

Kurzfassung

Eine fundamentale Voraussetzung für die Gewährleistung der Sicherheit von Informationssystemen stellt die adäquate Verwaltung und Kontrolle von Zugriffsberechtigungen dar. Die entsprechenden Aktivitäten, die unter dem Begriff der „Autorisierung“ zusammengefasst werden, sind zentraler Gegenstand der Dissertation. Ziel der vorliegenden Arbeit ist die Definition eines methodischen Vorgehens für die systemübergreifende bzw. unternehmensweite Gestaltung des Autorisierungssystems. Im Mittelpunkt steht dabei zum einen die Entwicklung von Autorisierungsarchitekturen, die die mittel- und langfristige Planung und Gestaltung von Autorisierungsinfrastrukturen zum Gegenstand haben. Zum anderen wird unter dem Stichwort „Integration der Autorisierung“ die systemübergreifende Verknüpfung von Berechtigungen behandelt. Für beide Themenschwerpunkte werden Vorgehensweisen vorgestellt, die detailliert aufzeigen, wie im Rahmen entsprechender Projekte zu verfahren ist. Ausgangspunkt der Methodenableitung bilden eine Literaturanalyse, vier Fallstudien und etablierte Sicherheitsstandards.

Schlüsselwörter: Autorisierung, Administration, Architektur, Berechtigungsmanagement, Business Engineering, Integration, Informationssicherheit, Rollen, Sicherheitsmanagement, Zugriffskontrolle

1 Einleitung

1.1 Ausgangssituation

Die Abwicklung des operativen Geschäfts ist heutzutage ohne eine softwaretechnische Unterstützung kaum noch denkbar. Fehlfunktionen oder der Ausfall von Informationssystemen können zu empfindlichen Geschäftseinbussen führen. Darüber hinaus kann die ungewollte Manipulation und Offenlegung von Daten verheerende Auswirkungen zur Folge haben. Informationssysteme und deren Daten stellen somit besonders zu schützende Ressourcen dar.

Der Autorisierung, also der Verwaltung und Kontrolle von Zugriffsberechtigungen, kommt bei dem Schutz von Informationssystemen eine herausragende Bedeutung zu: Eine von der US-amerikanischen Behörde FBI in Auftrag gegeben Studie ergab, dass 46% der auftretenden Schäden im Bereich Datensicherheit auf Diebstahl von internen Informationen, Netzmissbrauch durch interne Mitarbeiter und finanziellen Betrug zurückgehen.[1]

Die Vergabe von Rechten und die Implementierung geeigneter Autorisierungssysteme stellt die Verantwortlichen vor technische und organisatorische Herausforderungen: Einerseits gilt es, eine Vielzahl von Anforderungen einzubeziehen. Nicht nur die eigenen Bedürfnisse im Bereich der Datensicherheit sind zu beachten. Insbesondere regulatorische Anforderungen wie die Gesetze zum Datenschutz oder der Sarbanes-Oxley-Act, aber auch Anforderungen aus dem Bereich der „Non Governmental Organisations“ müssen berücksichtigt werden. Andererseits stellt die effektive und effiziente Umsetzung der Anforderungen eine Herausforderung dar: Sehr umfangreiche Sicherheitsvorkehrungen sind nur durch einen entsprechend hohen Einsatz von Ressourcen zu implementieren. Geringe Sicherheitsvorkehrungen bergen das Risiko, dass es zu erheblichen Schäden kommt. Daher gilt es, die Sicherheitsmassnahmen in Abhängigkeit vom Risiko zu gestalten. Schliesslich müssen die Sicherheitsmassnahmen in den entsprechenden Systemen softwaretechnisch umgesetzt werden. Dabei ist ein fundiertes Verständnis der technologischen Möglichkeiten und Restriktionen dieser zum Teil sehr heterogenen Systeme unabdingbar.

Trotz zahlreicher Lösungsansätze aus den Bereichen Informatik, Wirtschaftsinformatik, IT-Risikomanagement und Datensicherheit steht den Verantwortlichen in den Unternehmen kein umfassendes methodisches Vorgehen für die Gestaltung des Autorisierungssystems zur Verfügung. Das hier vorgestellte Forschungsvorhaben möchte diese Lücke in Wissenschaft und Praxis unter besonderer Berücksichtigung der Problematik heterogener Applikationslandschaften schliessen.

[1] Vgl. Richardson 2003.

1.2 Einordnung und Zielsetzung der Arbeit

Die Arbeit entstand im Rahmen des Kompetenzzentrums Integration Factory (CC IF, seit 2004) sowie des Vorgängerkompetenzzentrums Application Integration Management (CC AIM, 2002 bis 2004). Beide Projekte sind dem Forschungsprogramm Business Engineering der Universität St. Gallen zuzuordnen. Gegenstand von CC IF und CC AIM sind die nachhaltige, effiziente und effektive Integration operativer Applikationen im unternehmensinternen und -übergreifenden Kontext.[2] Dabei steht nicht nur die kurzfristige Integration neuer Applikationen in die bestehende Systemlandschaft im Mittelpunkt, sondern auch die mittel- und langfristige Gestaltung der Informationssystemlandschaft. Hierdurch kann auch die zukünftige Integration von Applikationen flexibel und effizient erfolgen.

Als zentraler Erfolgsfaktor für die effektive Integration hat sich das Architekturmanagement erwiesen.[3] Architekturen sind ein wichtiger Baustein, um die Applikationslandschaft planen und ihre Entwicklung steuern zu können. Das Architekturmanagement beinhaltet die Prozesse zur strukturierten Durchführung dieser Planung und ihren effizienten Einsatz in der Applikationsentwicklung, in Integrationsprojekten sowie bei Sourcing-Entscheidungen.

Die Dissertation beschäftigt sich mit den Kernthemen von CC IF und CC AIM in Hinblick auf die Thematik Sicherheit bzw. Autorisierung. Jedes Integrationsprojekt ist von dem Thema Sicherheit betroffen, sowohl auf technischer als auch auf organisatorischer Ebene. Um mittel- und langfristig effektiv und effizient integrieren zu können, sind projektübergreifende Konzepte für die Sicherheit und somit auch für die Autorisierung vonnöten.

Ein wechselnder Integrationsfokus[4] und das unzureichende Management der Architekturen führte in der Vergangenheit insbesondere bei mittleren und grossen Unternehmen zu Redundanzen oder Lücken in der Systemlandschaft.[5] In Bezug auf die Sicherheit führte die Entwicklung zu starken Redundanzen. So enthalten die einzelnen Applikationen meist eigenständige Sicherheitsfunktionen und -module, die oft proprietär und inkompatibel zueinander sind.[6] Im Bereich der Architektur gilt es daher, die sicherheitsbezogenen Redundanzen abzubauen und applikationsübergreifende Sicherheitsarchitekturen zu entwickeln.

Die dargestellten Herausforderungen im Umfeld der Autorisierung motivieren die folgende Forschungsfrage:

Forschungsfrage: Wie kann die Autorisierung in Unternehmen effektiv und effizient gestaltet werden?

---

2 Vgl. im Folgenden Schelp 2003, S. 3.
3 Vgl. im Folgenden Schelp 2003, S. 6.
4 Vgl. hierzu auch Kapitel 2.2.4.
5 Vgl. Winter 2003a, S. 7.
6 Vgl. Rupprecht 2002, S. 4.

Aus der Forschungsfrage lassen sich jeweils Gestaltungs- und Erkenntnisziele ableiten.[7] Gestaltungsziele sind Ziele, die auf die Transformation der Realität abzielen. Hingegen streben Erkenntnisziele nach dem Verstehen der Realwelt. Als primäres Gestaltungsziel der Arbeit lässt sich ableiten:

Primäres Gestaltungsziel: Konstruktion einer Methode für die Autorisierung

Für den Gestaltungsbereich der Methode lassen sich dabei folgende Handlungsfelder identifizieren:

- Autorisierungsarchitektur: Der Themenkomplex „Autorisierungsarchitektur“ setzt sich mit der mittel- und langfristigen, unternehmensweiten Gestaltung der Autorisierungsinfrastruktur auseinander.

- Systemübergreifende Autorisierung bzw. Integration der Autorisierung: Das Themengebiet „Integration der Autorisierung“ behandelt den Einsatz von Autorisierungswerkzeugen, die systemspezifische Autorisierungskomponenten auf der Basis systemübergreifender Rollen integrieren. Im Rahmen der Anwendungssystemgestaltung ist die Frage zu beantworten, wie systemübergreifend Benutzerberechtigungen aufgrund eines methodischen Vorgehens systematisch und risikogesteuert abgeleitet werden können (Erstellung Berechtigungskonzept). Im Rahmen der Organisationssystemgestaltung ist insbesondere die Frage zu beantworten, welche Aufgabenträger welche Aufgaben bei der systemübergreifenden Autorisierung wahrzunehmen haben (Erstellung Administrationskonzept).

- Systemspezifische Autorisierung: Im Bereich der systemspezifischen Autorisierung geht es um die Fragestellung, wie ein einzelnes Informationssystem unter dem Aspekt der Autorisierung risikoorientiert zu gestalten ist. Zentrale Gestaltungsaspekte sind wiederum das Berechtigungs- und das Administrationskonzept.

Gegenstand der Dissertation sind entsprechend der Arbeitsschwerpunkte von CC IF und CC AIM die Themenbereiche Autorisierungsarchitektur und Integration der Autorisierung. Kein Gegenstand der Arbeit ist die Erarbeitung eines Referenzprozessmodells für die Administration von Zugriffsberechtigungen, das als Basis für die Erstellung eines unternehmensspezifischen Administrationskonzepts genutzt werden kann.

Die Erkenntnisziele der Arbeit bilden die Grundlage für das Gestaltungsziel der Dissertation. Als primäres Erkenntnisziel ist zu nennen:

Primäres Erkenntnisziel: Zusammenstellung aktueller Grundlagen und Methoden der Autorisierung in Praxis und Forschung durch Literaturanalyse bzw. in Form von Fallstudien.

[7] Vgl. Becker 1995, S. 133.

In Hinblick auf die Ausarbeitung der Dissertation sind folgende Einschränkungen zu berücksichtigen:

- Der Schwerpunkt der Arbeit liegt im Themenumfeld der Autorisierung. Somit stehen IT-Sicherheitsfragestellungen wie z.B. Single-Sign-On, die keinen direkten Bezug zum Thema Autorisierung aufweisen, nicht im Mittelpunkt der Arbeit.

- Die Forschung der Kompetenzzentren CC IF und CC AIM basiert auf der Zusammenarbeit mit Grossunternehmen. Daher bezieht sich die Methode insbesondere auf die in diesen Unternehmen vorzufindende Situation, die von heterogenen, gewachsenen Applikations- und somit auch Sicherheitslandschaften geprägt ist.

- Ein Grossteil der an den Kompetenzzentren CC IF und CC AIM beteiligten Unternehmen gehört der Finanzindustrie an. Die Methodenentwicklung findet daher im Umfeld dieser Branche statt. Die branchenübergreifende Anwendung des Ansatzes ist aufgrund dieser Fokussierung jedoch kaum eingeschränkt, da die Methode nicht systemspezifisch auf Applikationen der Finanzindustrie ausgerichtet wird.

Die Arbeit adressiert gleichermassen Vertreter aus Wissenschaft und Praxis, die sich mit der systematischen Gestaltung von Autorisierungssystemen auseinandersetzen. Folgende Nutzenpotenziale für die Praxis lassen sich nennen:

- Die Bereitstellung einer systematischen Vorgehensweise zur Gestaltung der Autorisierung, die Projekten in diesem Bereich als Grundlage dienen kann.

- Die Bereitstellung eines Metamodells, das in der Praxis insbesondere als Basis einer einheitlichen Kommunikation verwendet werden kann.

Für Wissenschaftler, die sich mit den Themen Autorisierung, Sicherheit und Risikomanagement beschäftigen, bietet die Arbeit folgende Nutzenpotenziale:

- Diskussion einer methodischen Vorgehensweise zur Gestaltung der Autorisierung in Unternehmen.

- Bessere Beurteilung theoretischer Artefakte durch die Bereitstellung von Fallstudien aus der Praxis.[8]

Weitere Nutzenpotenziale für die Wissenschaft liegen beispielsweise in der Verwendung der erarbeiteten Ergebnisse und Fallstudien im Rahmen der Lehre z.B. in Form von Lehrfallstudien.

[8] Vgl. hierzu auch Kremer 2004, S. 4.

1.3 Forschungsmethodik

Die Dissertation entstand im Rahmen der Kompetenzzentren CC AIM und CC IF des Instituts für Wirtschaftsinformatik der Universität St. Gallen. Die verwendete Forschungsmethodik der Dissertation ist daher im Kontext der Wirtschaftsinformatik im Allgemeinen und der Kompetenzzentrumsforschung des Instituts für Wirtschaftsinformatik der Universität St. Gallen im Speziellen zu betrachten.

Die Wirtschaftsinformatik wird als angewandte Wissenschaft charakterisiert.[9] Damit verfügt sie über folgende Merkmale:[10]

- Die Probleme der Wirtschaftsinformatik entstehen in der Praxis.
- Die Wirtschaftsinformatik ist ihrem Wesen nach interdisziplinär.
- Die Wirtschaftsinformatik zielt auf den Entwurf einer neuen Wirklichkeit.
- Nicht die Wahrheit wissenschaftlicher Aussagen steht im Mittelpunkt der Forschung, sondern der zu schaffende Nutzen für die Praxis.
- Eine wertfreie Wirtschaftsinformatik wäre für die Praxis wertlos. Die Aussagen der Wirtschaftsinformatik sollten daher normativ und wertend sein.

Über die adäquaten Forschungsmethoden der Wirtschaftsinformatik besteht keine einheitliche Meinung.[11] Dies liegt unter anderem daran, dass die Wirtschaftsinformatik eine vergleichsweise junge Forschungsdisziplin ist.[12] KÖNIG, HEINZL, RUMPF ermittelten im Zuge einer Delphi-Studie, welche grundlegenden Forschungsmethoden die Wirtschaftsinformatik verwenden soll, um ihre Wettbewerbsposition gegenüber der Betriebswirtschaftslehre und der Informatik zu behaupten.[13] Gefragt wurde nach konstruktiven Methoden, die überwiegend deduktionsgetrieben sind und primär zur Veränderung von Sachverhalten dienen, und empirischen Methoden, die überwiegend induktionsgetrieben sind und primär dem Zweck der Überprüfung von Theorien dienen. Als wesentliche konstruktive Methoden wurden „Entwicklung und Test von Prototypen“, „Simulation“, „Modellierung“, „Deduktion“, „Learning-by-Doing“ und „Kreativitätstechniken“ ermittelt. Als wichtigste empirische Methoden wurden „Exploration mittels Fallstudien und Feldstudien“, „Beobachtung (z.B. des Anwender- oder Systemverhaltens)“, „Referenzmodelle als quasi-empirischer (semi-formaler) Ansatz“, „Mündliche oder schriftliche Befragungen“, „Forschung durch Entwicklung“ und „Ex-Post-Beschreibungen und Interpretationen realer Sachverhalte“ identifiziert.

---

9 Vgl. Frank et al. 1999, S. 50.
10 Vgl. auch im Folgenden Ulrich 1984, S. 202f.
11 Vgl. Frank et al. 1999, S. 71.
12 Vgl. Rolf 1998, S. 3.
13 Vgl. im Folgenden König et al. 1996.

Im Rahmen der Kompetenzzentren wird am Institut für Wirtschaftsinformatik angewandte, konstruktive Forschung betrieben. Zu einem übergeordneten Forschungsthema erarbeiten Unternehmensvertreter zusammen mit Wissenschaftlern des Instituts für Wirtschaftsinformatik Lösungen für Forschungsfragen, die aus der Praxis motiviert sind. Die im Wesentlichen in bilateralen Projekten entwickelten Ergebnisse werden dabei innerhalb von regelmässigen Workshops mit allen Unternehmen des Kompetenzzentrums reflektiert. Im Rahmen der Forschung steht die Erarbeitung von Artefakten wie z.B. Methoden oder Modellen im Vordergrund. Damit lässt sich die Forschungsarbeit am Institut für Wirtschaftsinformatik dem Design-Science-Paradigma zuordnen.

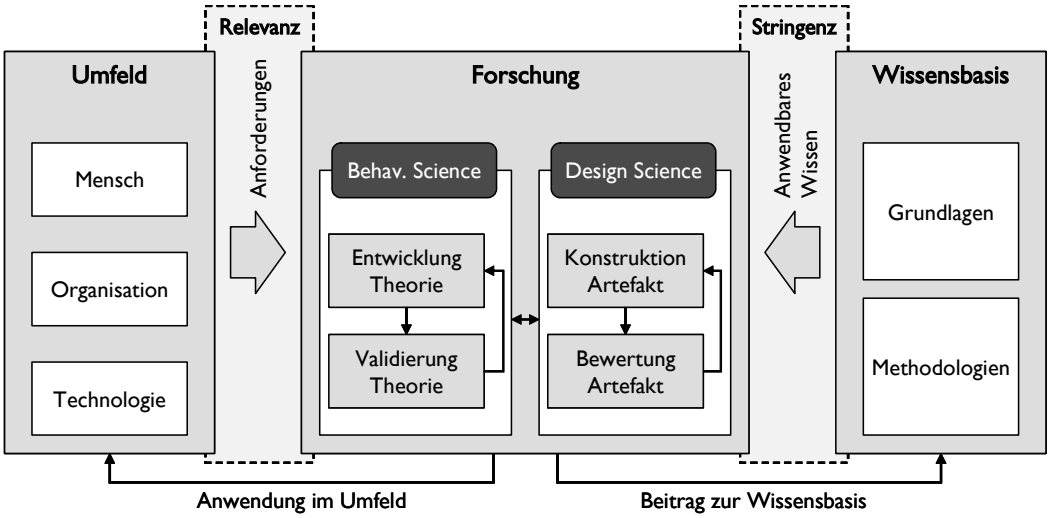

Abbildung 1: Information Systems Research Framework[14]

Das Design-Science-Paradigma ist im Umfeld des „Information Systems Research", dem angelsächsischen Pendant der Wirtschaftsinformatik, wie folgt definiert: „The design-science paradigm is fundamentally a problem-solving paradigm. It seeks to create innovations that define the ideas, practices, technical capabilities, and products through which the analysis, design, implementation, management, and use of information systems can be effectively and efficiently accomplished".[15] Die Lösung von Problemen durch innovative Artefakte ist somit Ziel des Paradigmas. Das Design-Science-Paradigma lässt sich vom Behavioral-Science-Paradigma abgrenzen, in dessen Mittelpunkt die Entwicklung und Validierung von Theorien steht: „The behavioral-science paradigm seeks to develop and justify theories (i.e., principles and laws) that explain or predict organizational and human phenomena surrounding the analysis, design, implementation, management and use of information systems."[16]

Die Abgrenzung lässt sich auch anhand eines Modells nachvollziehen, das wesentliche Elemente des „Information Systems Research" in Bezug zueinander stellt (vgl. Abbildung 1).

14 Vgl. Hevner et al. 2004, S. 80.
15 Hevner et al. 2004, S. 76.
16 Hevner et al. 2004, S. 76.

Dieses „Information Systems Research Framework“ basiert auf folgenden grundlegenden Elementen:[17]

- **Umfeld (Environment):** Das Umfeld definiert den Gegenstandsbereich der Forschung. Im Bereich der Informationssystemforschung setzt sich das Umfeld aus den Dimensionen Mensch, Organisation und Technologie zusammen.

- **Anforderungen bzw. Problem (Business Need bzw. Problem):** Aus den Zielen, Aufgaben, Problemen und Chancen des Umfeldes ergeben sich aus der Perspektive der betroffenen Mitarbeiter Anforderungen. Diese Anforderungen bilden die Ausgangsbasis bzw. definieren das grundlegende Problem des Wissenschaftlers.

- **Forschung (IS Research)**: Aufgabe der behavioristischen Forschung (behavioral science) ist die Entwicklung und Validierung von Theorien, die Phänomene erklären oder vorhersagen, welche in Zusammenhang mit den identifizierten Anforderungen stehen. Aufgabe der entwicklungsorientierten Forschung (design science) ist die Konstruktion und Bewertung von Artefakten, die die identifizierten Anforderungen adressieren.

- **Wissensbasis (Knowledge Base)**: Die Wissensbasis stellt dem Wissenschaftler fundamentale Grundlagen und Methodologien zur Verfügung. Die fundamentalen Grundlagen enthalten Konstrukte wie z.B. Theorien, Methoden oder Modelle. Diese Konstrukte werden für die Entwicklung von Theorien bzw. für die Konstruktion von Artefakten herangezogen. Methodologien enthalten Richtlinien und Verfahren, die für die Validierung von Theorien bzw. die Bewertung von Artefakten herangezogen werden.

- **Anwendbares Wissen (Applicable Knowledge):** In einem konkreten Forschungsprozess steht dem Forscher die Wissensbasis als anwendbares Wissen zur Verfügung.

Die Relevanz der Forschung (Relevance) wird durch die Ausrichtung der Forschungsaktivitäten auf die Anforderungen gewährleistet.[18] Die Stringenz der Forschung (Rigor) wird durch die konsequente, situationsgerechte Einbeziehung der Wissensbasis hergestellt.[19] Der Gesamtbeitrag einer Forschungsarbeit ist laut HEVNER ET AL. zum einen im Hinblick auf die definierten Anforderungen zu bewerten. Zum anderen gilt es, den Beitrag der Forschungsarbeit zur Wissensbasis zu beurteilen.[20]

Der Dissertation wird das Design-Science-Paradigma zugrunde gelegt (vgl. Abbildung 2). Das zu konstruierende Artefakt, die „Methode für die unternehmensweite Autorisierung“, adressiert die Autorisierungsprobleme und -bedürfnisse der Partnerunternehmen des CC AIM, des CC IF und weiterer Unternehmen, die sich im Rahmen der Arbeit durch die Aufnahme

17 Vgl. Hevner et al. 2004, S. 80.
18 Vgl. Hevner et al. 2004, S. 79.
19 Vgl. Hevner et al. 2004, S. 80.
20 Vgl. Hevner et al. 2004, S. 81.

entsprechender Fallstudien engagieren. Die Konstruktion der Methode findet in Form von Projektarbeit, strukturierten Interviews und Desk-Research wie etwa Literaturanalyse statt. Die Reflexion des Vorgehens und der Arbeitsergebnisse basiert auf regelmässig stattfindenden Workshops, Desk-Research und der eigentlichen Entwicklung der Arbeitsergebnisse. Ergebnis des Forschungsprozesses ist die Methode für die Autorisierung mit ihren Methodenelementen.

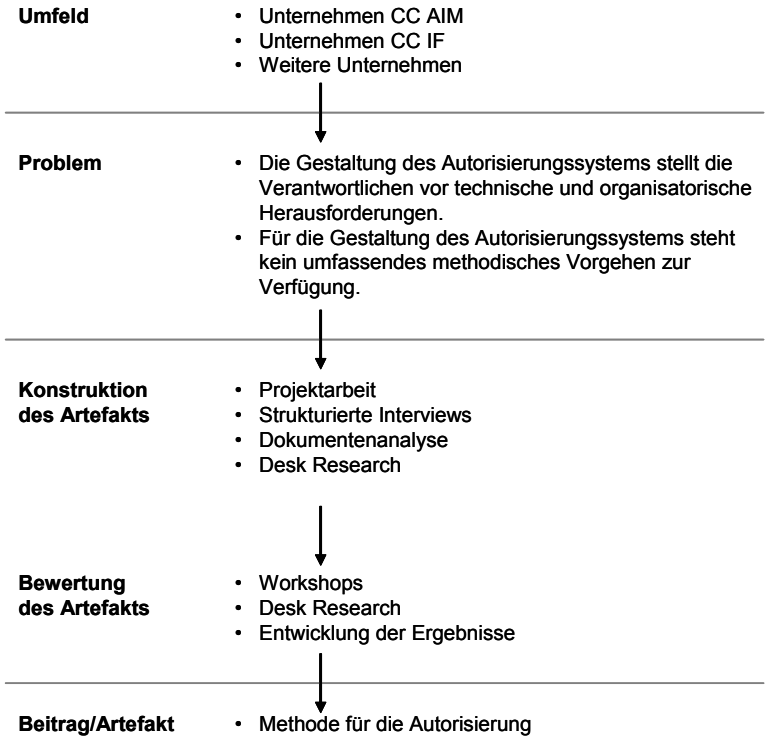

Abbildung 2: Design Science als Grundlage der Dissertation

1.4 Aufbau der Arbeit

Zunächst werden in Kapitel 2 die für die Arbeit relevanten Grundlagen dargestellt und Konsequenzen für die weitere Vorgehensweise abgeleitet. Das Business Engineering stellt dabei den Forschungsrahmen der Arbeit dar. Als elementare Grundlagen bilden die Themengebiete „Sicherheit von Informationssystemen“, „Autorisierung“ und „IT-Risikomanagement“ den Bezugsrahmen der Arbeit.

In Kapitel 3 werden bereits bestehende Ansätze zur Autorisierung selektiert und hinsichtlich der aus den Grundlagen in Kapitel 2 abgeleiteten Konsequenzen bewertet. Es werden dabei Ansätze ausgewählt und analysiert, die einen expliziten Bezug zur Autorisierung aufweisen und Methoden darstellen bzw. methodische Elemente beinhalten.

Die im Rahmen der Literaturanalyse identifizierten Ansätze beinhalten keine umfassende, methodische Sichtweise auf die gewählten Schwerpunkte der Dissertation. Aus diesem Grund dokumentiert Kapitel 4 Praxisprojekte in Form von Fallstudien, die im weiteren Verlauf der Arbeit den Ausgangspunkt des Methodenentwurfes bilden.

In Kapitel 5 erfolgt die Festlegung der wesentlichen Methodengrundlagen. Im Rahmen der Definition der Methodenelemente und -charakteristik werden einerseits die grundlegenden Elemente der zu entwickelnden Methode genau spezifiziert, andererseits Anspruch und Charakteristik der zu entwickelnden Methode diskutiert und festgelegt. Die zu entwerfende Methode strebt u.a. Empfehlungscharakter an, so dass im Anschluss spezielle Anforderungen an die zu entwickelnde Methode abgeleitet werden, die im Rahmen des Methodenentwicklungsprozesses zur Diskussion des Empfehlungsanspruchs herangezogen werden. Kapitel 5 endet mit der Beschreibung eines grundlegenden Metamodells, das wesentliche Entitätstypen der Domäne Autorisierung in Bezug zueinander setzt.

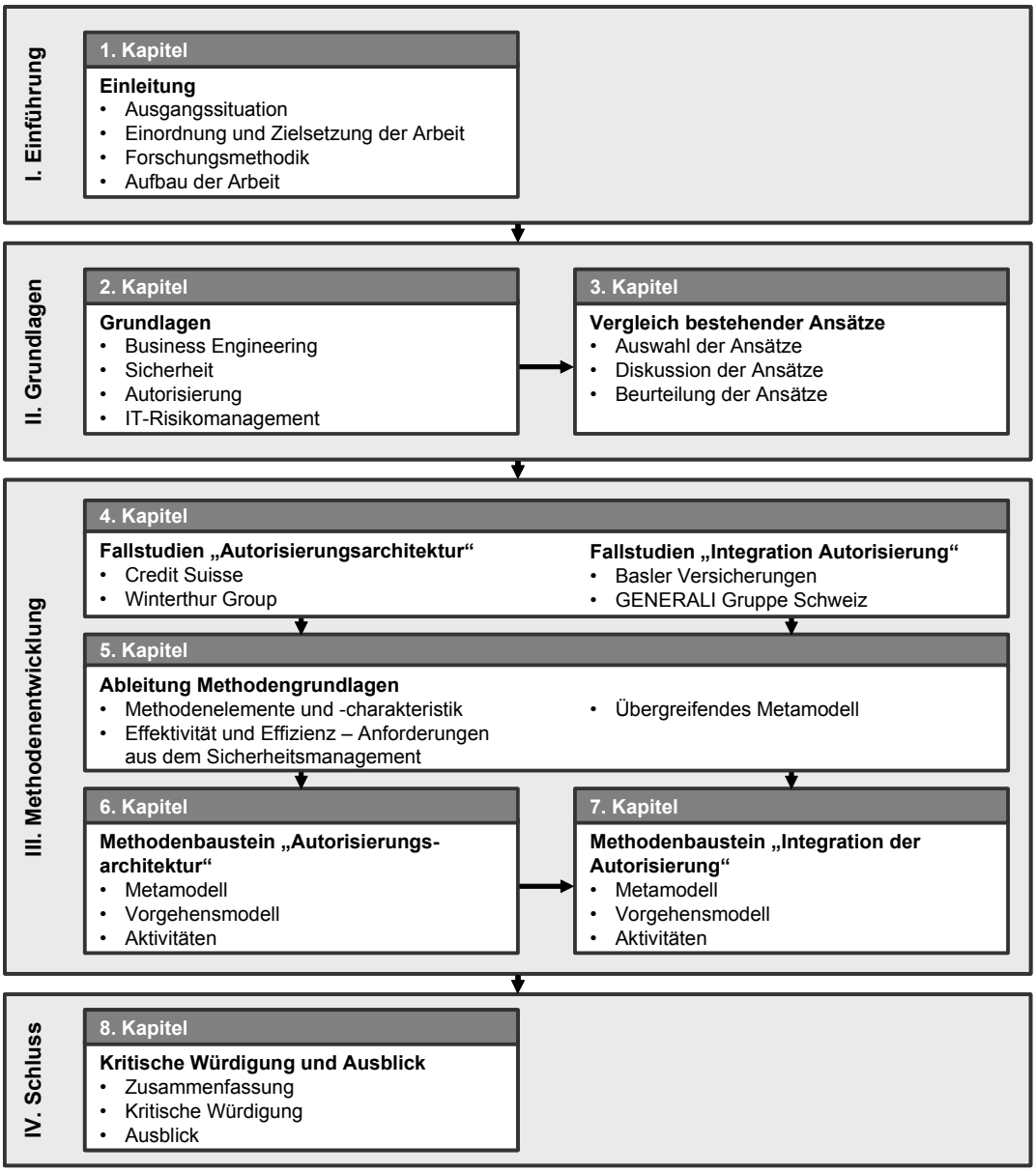

Abbildung 3: Aufbau der Arbeit

In Kapitel 6 und 7 erfolgt die eigentliche Entwicklung der Methode entsprechend der Schwerpunkte „Autorisierungsarchitektur“ und „Integration der Autorisierung“. Für jeden der beiden erarbeiteten Methodenbausteine werden ein Metamodell, ein Vorgehensmodell, ein Doku-

mentationsmodell und ein Rollenmodell entwickelt. Die einzelnen Aktivitäten der beiden Vorgehensmodelle werden darüber hinaus detailliert beschrieben.

Abschliessend erfolgt in Kapitel 8 zunächst die Zusammenfassung und kritische Würdigung der Ergebnisse der Arbeit. Im Ausblick werden schlussendlich Ansatzpunkte zur Weiterentwicklung der vorliegenden Arbeit aufgezeigt.

Abbildung 3 stellt den Aufbau der Arbeit überblicksartig dar.

2 Grundlagen

Das vorliegende Kapitel beschreibt die wissenschaftlichen Grundlagen der Arbeit. Folgende Schwerpunkte bilden den Bezugsrahmen der theoretischen Auseinandersetzung mit dem Thema der Arbeit:

- Business Engineering: Das Business Engineering stellt den Forschungsrahmen dieser Arbeit dar. Als Element des Business Engineering ist das Methoden-Engineering von besonderer Relevanz für die Arbeit. Es sichert das ingenieurmässige Vorgehen bei der Transformation eines Unternehmens.

- Sicherheit: Gegenstand der Sicherheit von Informationssystemen ist insbesondere die sichere Verarbeitung und Speicherung von Daten. Die vier Sicherheitsfunktionen Authentisierung, Autorisierung, Beweissicherung und Übertragungssicherheit bilden die Grundlage zur Erreichung der Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit. Die Informationsverarbeitung in den Unternehmen wird heute nicht mehr von einer einzelnen, sondern von zahlreichen kooperierenden Applikationen realisiert. Diesem Aspekt müssen die Sicherheitsmassnahmen Rechnung tragen.

- Autorisierung: Die Autorisierung beschäftigt sich mit der Verwaltung und Kontrolle von Berechtigungen. In der unternehmerischen Praxis hat sich die rollenbasierte Autorisierung als dominierendes Konzept etabliert. Dieses Konzept wird nicht nur für die Autorisierungskomponenten einzelner Applikationen verwendet, sondern auch für die applikationsübergreifende Integration von Autorisierungskomponenten.

- IT-Risikomanagement: Zu den Teilaufgaben des IT-Risikomanagements gehören die Risikoanalyse und -bewertung sowie die Risikobewältigung und das Risikocontrolling. Die Risikoanalyse identifiziert potenzielle Risiken. Diese werden im Rahmen der Risikobewertung gewichtet, so dass im Zuge der Risikobewältigung geeignete Massnahmen zur Handhabung der Risiken initiiert werden können. Diese Massnahmen werden anschliessend im Risikocontrolling auf ihre Wirksamkeit hin überprüft. Autorisierung als Verwaltung und Kontrolle von Berechtigungen wird implementiert, um potenzielle Schäden zu vermeiden und sich gegen Risiken zu schützen. Autorisierung ist somit ein Element der Risikobewältigung und Teil des Risikomanagements.

Die folgenden Abschnitte konkretisieren die skizzierten Themenschwerpunkte. Der letzte Abschnitt des Kapitels fasst die Erkenntnisse zusammen und formuliert daraus Konsequenzen für die zu erarbeitende Methode.

2.1 Business Engineering

Das Business Engineering bildet den Forschungsrahmen der Dissertation. Im Folgenden werden daher die grundlegende Ausrichtung des Business Engineering, die Gestaltungsebenen des Business Engineering und das Methoden-Engineering vorgestellt.

2.1.1 Grundlagen

Die Wirtschaft befindet sich in einem grundlegenden Transformationsprozess vom Industrie- ins Informationszeitalter.[21] Insbesondere Innovationen aus dem Bereich der Informations- und Kommunikationstechnologie ermöglichen hierbei neue Geschäftslösungen. Um die Transformation systematisch zu gestalten, bedarf es geeigneter Vorgehensmodelle, Methoden und Werkzeuge. Hierdurch kann ein professionelles und ingenieurmässiges Vorgehen sichergestellt werden.[22] Das „Business Engineering" greift den Aspekt der systematischen Transformationsgestaltung auf und beschäftigt sich mit der Methoden- und Konstruktionslehre der Unternehmen des Informationszeitalters.[23] Das Business Engineering weist enge Verbindungen zur Wirtschaftsinformatik, zum Technologiemanagement und zur Organisationslehre auf. Eine Abgrenzung kann wie folgt durchgeführt werden:[24]

- Wirtschaftsinformatik: Die Wirtschaftsinformatik setzt sich insbesondere mit dem Entwurf, der Entwicklung und dem Einsatz computergestützter, betriebswirtschaftlicher Informations- und Kommunikationssysteme in Wirtschaft und öffentlicher Verwaltung auseinander. Das Business Engineering beschäftigt sich darüber hinaus mit der Gestaltung von Geschäftsstrategien, Geschäftsprozessen und Führungssystemen sowie der Analyse und Veränderung von Machtverhältnissen.

- Organisationslehre: Die Organisationslehre beschäftigt sich mit der Nutzung verschiedener Theorien und Modelle zur Bestimmung arbeitsteilig zu bewältigender Aufgaben und der Auswahl geeigneter Koordinationsformen. Im Vergleich zur Organisationslehre betont das Business Engineering in sehr viel stärkerem Masse die Potenziale und Restriktionen, die sich aus der Verwendung von Informations- und Kommunikationstechnik ergeben.

- Technologiemanagement: Das Technologiemanagement setzt sich mit der Entwicklung von Technologiestrategien auseinander. Im Gegensatz dazu bezieht das Business Engineering nicht nur die der Technologiebewertung folgenden Phasen der Strategieentwicklung mit ein, sondern auch die Prozessentwicklung und ggf. die Systementwicklung.

---

21 Vgl. Österle/Winter 2003, S. 4.
22 Vgl. Österle/Winter 2003, S. 7.
23 Vgl. Österle/Winter 2003, S. 7.
24 Vgl. Österle/Winter 2003, S. 13.

Dem Gestaltungsansatz des Business Engineering liegen folgende grundlegende Prinzipien zugrunde:[25]

- Ingenieurmässiges Vorgehen: Der Transformationsprozess des Unternehmens wird durch ein systematisches, methoden- und modellbasiertes Vorgehen bestimmt.
- IT-Innovationen als Potenzial: Insbesondere IT-Innovationen bieten Potenziale für neue Geschäftslösungen.
- Vernetzte Geschäftsarchitekturen: Das Informationszeitalter ist durch vernetzte Geschäftsarchitekturen gekennzeichnet.
- Ganzheitlichkeit: Innovationen können nur erfolgswirksam werden, wenn strategische, prozessuale und systemtechnische Aspekte integriert betrachtet werden.
- Restriktionen durch Informations- und Kommunikationstechnik: Die Informations- und Kommunikationstechnik setzt Restriktionen, die bei der Gestaltung von Geschäftslösungen beachtet werden müssen.

2.1.2 Gestaltungsebenen des Business Engineering

Als wesentliche Aspekte von Veränderungsprozessen werden im Business Engineering die fachliche und die politisch-kulturelle Dimension unterschieden.[26] Die politisch-kulturelle Dimension verhält sich orthogonal zu den fachlichen Ebenen und betrachtet Unternehmenspolitik, Unternehmens- bzw. Veränderungskultur und Verhalten.[27]

Die fachliche Dimension unterscheidet die drei Ebenen Strategie, Prozess und System.[28] Die drei Ebenen bilden eine Zielhierarchie. Zunächst erfolgt die strategische Positionierung eines Unternehmens bzw. einer Geschäftseinheit (Strategieebene). Anschliessend wird auf Basis der Positionierung die Organisation spezifiziert (Prozessebene). Abschliessend wird die Unterstützung geeigneter Aktivitäten durch Informationssysteme bestimmt (Systemebene). Die Ebenen des Business Engineering können wie folgt beschrieben werden:[29]

- Strategieebene: Auf der Strategieebene wird die Rolle des Unternehmens im Wertschöpfungsnetzwerk festgelegt. Die darauf aufbauende Ableitung der wesentlichen Unternehmensleistungen erfolgt auf der Basis der Kundenprozessanalyse.
- Prozessebene: Auf der Prozessebene werden die zur Umsetzung der Strategien notwendigen Geschäftsprozesse definiert. Für jeden Prozess sind die Prozessleistungen, die Pro-

25 Vgl. Österle/Winter 2003, S 13.
26 Vgl. Österle/Winter 2003, S 12.
27 Vgl. Winter 2003b, S. 95.
28 Vgl. im Folgenden Winter 2003b S. 93.
29 Vgl. Winter 2003b, S. 93f.

zessaktivitäten, deren Abfolge und die entsprechenden Verantwortlichkeiten zu spezifizieren. Ebenfalls zu definieren sind die Informationsobjekte und -flüsse.

- Systemebene: Auf der Systemebene wird festgelegt, welche Teilprozesse bzw. Aktivitäten auf welche Weise mit Applikationen (einschliesslich Softwarekomponenten und Datenstrukturen) unterstützt werden.

Die Strategie- und Prozessebene dienen der fachlichen Beschreibung z.B. von Organisationszielen, Geschäftsmodellen oder Organisationsstrukturen.[30] Auf der Systemebene wird mit der Betrachtung von Applikationen zunächst eine primär fachliche Sicht beibehalten. Erst ganz am Ende des skizzierten Prozesses steht die technische Gestaltung von Informationssystemen im Vordergrund.

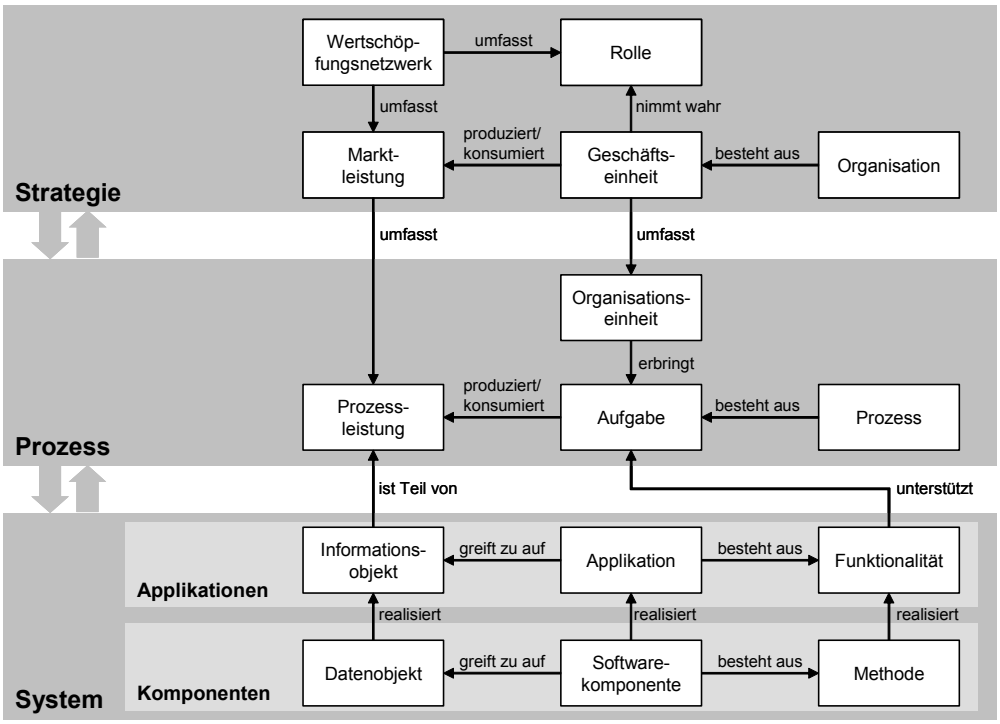

Abbildung 4: Wesentliche Gestaltungselemente des Business Engineering

In Anlehnung an WINTER/SCHELP[31], ÖSTERLE/BLESSING[32] und SCHWINN[33] zeigt Abbildung 4 wesentliche Gestaltungselemente des Business Engineering und ihre Beziehungen auf der Basis der dargestellten Ebenen des Business Engineering auf. Die vorliegende Arbeit fokussiert dabei in erster Linie auf die Applikationen und Komponenten der Systemebene sowie deren Zuordnung zu Prozessen.

30 Vgl. im Folgenden Winter 2003b, S. 95.
31 Vgl. Winter/Schelp 2005, S. 47f.
32 Vgl. Österle/Blessing 2003, S. 81.
33 Vgl. Schwinn 2005, S. 13ff.

2.1.3 Methoden-Engineering

Eine Grundlage für die Entwicklung und Beschreibung von Methoden bildet das Methoden-Engineering. Dieses wurde ursprünglich im Software-Engineering verwendet. Dort dient es dem Prozess der Entwicklung, Modifikation und Anpassung von Software-Engineering-Methoden durch die systematisierte und strukturierte Beschreibung der Methodenkomponenten und ihrer Beziehungen.[34]

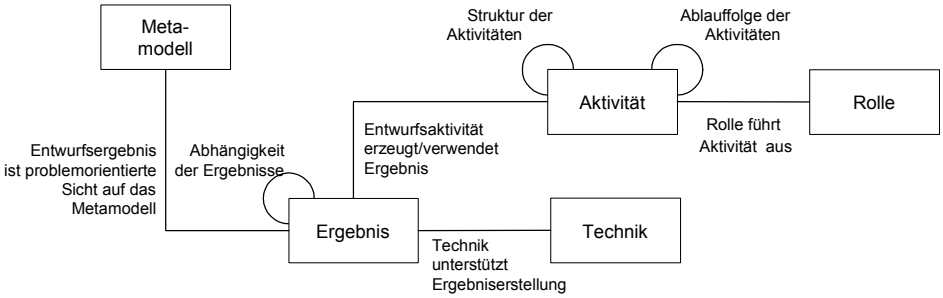

Abbildung 5: Komponenten von Methoden[35]

GUTZWILLER hat zahlreiche Ansätze des Methoden-Engineering analysiert und daraus allgemeingültige Elemente der Methodenbeschreibung abgeleitet. Methoden umfassen demnach fünf Bausteine (vgl. Abbildung 5):[36]

- Aktivität: Eine Aktivität ist eine funktionale Verrichtungseinheit, die Ergebnisse erstellt. Indem Aktivitäten in eine bestimmte Reihenfolge gebracht werden, entsteht ein Vorgehensmodell.

- Technik: Techniken beschreiben, wie Ergebnisse zu erstellen sind. Techniken können ggf. in Schritte untergliedert werden.

- Ergebnis: Ein Ergebnis oder auch Ergebnisdokument hält den Output einer oder mehrerer Techniken fest. Ergebnisse weisen einen Wert gegenüber relevanten Interessensgruppen auf („Stakeholder Value“).

- Rolle: Rollen beschreiben, welche Stellen, Organisationseinheiten oder Personen die Techniken und Aktivitäten ausführen.

- Metamodell: Ein Metamodell beinhaltet die wesentlichen Gestaltungselemente einer Methode und verdeutlicht die Beziehungen, die zwischen den Elementen bestehen.

Die Dissertation verwendet die Methoden-Engineering-Elemente zur Methodenentwicklung und -beschreibung.

---

34 Vgl. Heym 1993, S. 5.
35 Vgl. Gutzwiller 1994, S. 13.
36 Vgl. Gutzwiller 1994, S. 12ff.

2.2 Sicherheit von Informationssystemen

Gegenstand dieses Abschnitts sind der Sicherheitsbegriff und die damit verbundenen Herausforderungen insbesondere im Kontext gewachsener Applikationslandschaften. Abschliessend erfolgt eine Abgrenzung des Begriffs Datenschutz.

2.2.1 Definition

Die inhaltliche Festlegung, was unter Sicherheit in Bezug auf Informationssysteme[37] zu verstehen ist, gestaltet sich schwierig: In der Fachliteratur finden sich unterschiedliche Sicherheitsbegriffe.[38] Erschwerend kommt hinzu, dass der Sicherheitsbegriff umgangssprachlich vorbesetzt ist.[39] LANGE systematisiert die gängigen Sicherheitsbegriffe „Datensicherheit", „IT-Sicherheit", „Informationssicherheit" und „Sicherheit" anhand ihres Verwendungskontextes und ihrer Gestaltungsdimension:

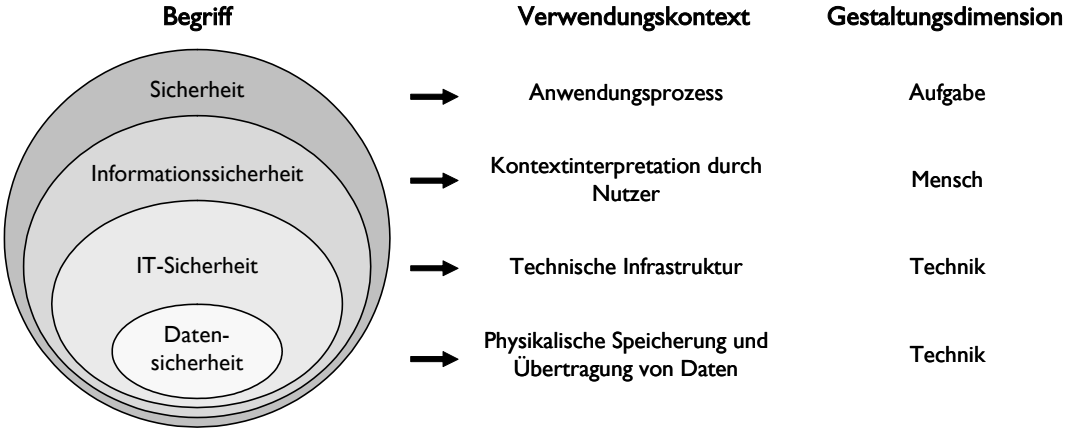

Abbildung 6: Gängige Sicherheitsbegriffe[40]

Die einzelnen Sicherheitsbegriffe lassen sich wie folgt charakterisieren:

- Datensicherheit: Mit dem Begriff der Datensicherheit wird die Betrachtung insbesondere auf die Daten eines Informationssystems fokussiert. Die Sichtweise begrenzt sich somit auf einen Aspekt des Anwendungssystems. Nach dem Normierungsgremium DIN wird unter Datensicherheit die Sachlage verstanden, Daten so weit wie möglich vor Missbrauch und Beeinträchtigung zu schützen.[41]

---

37 Informationssysteme werden in dieser Arbeit als sozio-technische Systeme aufgefasst. Sozio-technische Systeme setzen sich sowohl aus technischen Mitteln zur Aufgabenbewältigung als auch aus den Benutzern bzw. menschlichen Aufgabenträgern zusammen (vgl. Teubner 1997, S. 26; Ferstl/Sinz 1998, S. 5.). Die beiden Komponenten werden im Folgenden als Anwendungssystem bzw. Organisationssystem bezeichnet (vgl. Schütte 1998, S. 67).

38 Vgl. Rupprecht 2002, S. 5.

39 Vgl. Lange 2004, S. 40.

40 Vgl. Lange 2004, S. 41.

41 Vgl. DIN 1988, Teil I.

- IT-Sicherheit: Bei der IT-Sicherheit steht die fortwährende Verfügbarkeit von hard- und softwaretechnischen Systemkomponenten im Mittelpunkt. Darüber hinaus ist die korrekte Ausführung von Datenverarbeitungsprozessen zu gewährleisten.[42] Eine juristische Definition des Begriffs findet sich in § 2 Abs. 2 BSIG. Danach wird IT-Sicherheit durch das Ergreifen von Sicherheitsmassnahmen zur Erreichung definierter Sicherheitsziele für informationstechnische Systeme und deren Komponenten etabliert.[43]

- Informationssicherheit: Durch die kognitiven Fähigkeiten des Menschen, die Daten des Informationssystems im entsprechenden Kontext zu interpretieren, findet ein Wechsel von der Datenverarbeitung zur Informationsverarbeitung statt.[44] Informationssicherheit in einem sozio-technischen System bedeutet somit, dass das System nur solche Systemzustände annimmt, die zu keiner unautorisierten Informationskenntnisnahme oder -veränderung führen.[45]

- Sicherheit: Mit dem Begriff der Sicherheit wird der Begriff der Informationssicherheit um rechtlich-organisatorische Aspekte erweitert.[46] Die Sicherheit sozio-technischer Systeme wird dabei im Kontext der durch den Anwender zu bearbeitenden Aufgabenstellung sowie der damit verbundenen organisatorischen Aspekte betrachtet.[47] Sicherheit ist dann gewährleistet, wenn die mit einem Informationssystem zu bearbeitenden Aufgabenstellungen in technischer, ökonomischer und juristischer Hinsicht von befugten Nutzern erfüllt werden.[48]

Da im Rahmen der Dissertations sowohl die Gestaltung des Anwendungsystems als auch des Organisationssystems thematisiert wird und darüber hinaus auch rechtliche Aspekte nicht aus der Diskussion ausgeschlossen werden sollen, liegt dieser Arbeit das unter dem Begriff „Sicherheit“ diskutierte Verständnis zugrunde.

2.2.2 Ziele

Die Umsetzung von Sicherheit in computergestützten Informationssystemen orientiert sich in der Regel an der Vorgabe und Umsetzung von Zielen. Es existiert eine Vielzahl von Sicherheitszielen, denen je nach Anwendungskontext eine unterschiedliche Gewichtung zukommt.[49] Die Sicherheitsziele, die für alle Informationssysteme gelten, werden Sicherheitsgrund- oder -basisziele genannt:[50]

---

42 Vgl. Amann/Atzmüller 1992, S. 1192; Büllesbach 1999, S. 64.
43 Vgl. Holznagel et al. 2003, S. 11.
44 Vgl. Lange 2004, S. 43.
45 Vgl. Lippold 1992, Sp. 913; Pohl/Weck 1993, S. 21; Eckert 2003, S. 4.
46 Vgl. Lange 2004, S. 44.
47 Vgl. Büllesbach 1999, S. 64; Konrad 1998, S. 12; Röhm 2000, S. 18.
48 Vgl. Stelzer 1990, S. 504.
49 Vgl. Lange 2004, S. 46.
50 Vgl. Federrath/Pfitzmann 2000, S. 705.

- Vertraulichkeit: Mit der Erfüllung des Sicherheitsziels der Vertraulichkeit soll ein unbefugter Informationsgewinn durch eine nicht berechtigte Einsichtnahme von Daten verhindert werden.[51] Dies setzt voraus, dass der Zugriff auf Daten nur durch berechtigte Instanzen erfolgt.[52] Die Vertraulichkeit von Informationen muss sowohl bei direktem als auch bei indirektem Zugriff (Zugriff über mehrere Stufen) gewährleistet sein.[53]

- Integrität: Integrität umfasst drei sich überlappende Ziele:[54] Unterbindung von Datenmodifikationen durch nicht autorisierte Nutzer, Unterbindung von missbräuchlichen und unvorschriftsmässigen Datenmodifikationen durch autorisierte Nutzer sowie die Sicherstellung der internen und externen Datenkonsistenz. Die interne Datenkonsistenz gewährleistet die Widerspruchsfreiheit der unterschiedlichen Datenbestände. Die externe Datenkonsistenz stellt sicher, dass die Daten den Sachverhalt der Realwelt, den sie beschreiben, angemessen repräsentieren. Um die Integrität sicherzustellen, muss die Identität des Datenmanipulators und -nutzers jederzeit eindeutig bekannt sein.[55]

- Verfügbarkeit: Ressourcen und Informationen, die zwar existieren, jedoch nicht in angemessener Zeit verwendet werden können, sind zum Zugriffszeitpunkt wertlos.[56] Die Eigenschaft Verfügbarkeit stellt sicher, dass Ressourcen in definierter Form innerhalb einer nützlichen und angemessenen Zeit zu nutzen sind.[57] Angriffe, die sich gezielt gegen die Verfügbarkeit von Systemen wenden, werden Denial-of-Service-Angriffe genannt.

Als viertes grundlegendes Sicherheitsziel wird teilweise die Verbindlichkeit genannt.[58] Verbindlichkeit ist gewährleistet, wenn nachgewiesen werden kann, wer (Nutzer oder Programm) welche Aktivitäten im Informationssystem durchgeführt hat.[59] Dieses vierte Sicherheitsziel kann jedoch auf die drei anderen zurückgeführt werden,[60] so dass es hier nicht zu den elementaren Sicherheitszielen gezählt wird.

2.2.3 Grundfunktionen

Die wichtigsten Grundfunktionen bei der Entwicklung eines ganzheitlichen Sicherheitskonzepts sind Authentisierung und Identifikation, Autorisierung, Beweissicherung sowie Übertragungssicherung:[61]

---

51 Vgl. Lange 2004, S. 47.
52 Vgl. Holznagel et al. 2003, S. 13; Hoppe/Priess 2003, S. 24.
53 Vgl. Rupprecht 2002, S. 15.
54 Vgl. Fischer-Hübner 2001, S. 36.
55 Vgl. Pipkin 2000, S. 14.
56 Vgl. Rupprecht 2002, S. 15.
57 Vgl. Oppliger 1997, S. 11.
58 Vgl. Fischer-Hübner 2001, S. 36.
59 Vgl. Kersten 1995, S. 7; Eckert 2003, S. 10; Hoppe/Priess 2003, S. 25.
60 Vgl. Fischer-Hübner 2001, S. 36.
61 Vgl. Rupprecht 2002, S. 17.

- Authentisierung und Identifikation: Grundlage für ein sicheres System ist die Erkennung und Verwaltung von Benutzern und Ressourcen (Identifikation).[62] Die Authentisierung validiert eine vorgegebene Identität.[63] Vier Arten der Authentisierung können unterschieden werden:[64] Überprüfung eines Wissensmerkmals (z.B. durch die Abfrage eines Passworts), Überprüfung eines Besitzmerkmals (z.B. durch ein Chipkarte), Überprüfung einer physischen Eigenschaft (z.B. durch die Prüfung des Fingerabdrucks) und Überprüfung eines persönlichen Charakteristik (z.B. durch die Prüfung einer Unterschrift).

- Autorisierung: Autorisierung bezeichnet die Verwaltung und Überprüfung von Zugriffsrechten.[65] Zugriffsrechte bilden die Beziehungen zwischen Subjekten, Objekten und Zugriffsaktivitäten ab.[66] Auf die Autorisierung wird in Kapitel 2.3 detailliert eingegangen.

- Beweissicherung: Die Beweissicherung dokumentiert Informationen über Zugriffe und Zugriffsversuche.[67] So können auch vom System autorisierte Zugriffe, die jedoch gegen geltende Vorschriften verstossen, erkannt und geahndet werden. Ein Bankangestellter darf z.B. Buchungen durchführen. Eine Überweisung auf sein Privatkonto stellt jedoch eine unautorisierte Handlung dar.[68] Darüber hinaus lassen sich durch die Aufzeichnung von durchgeführten Aktivitäten wertvolle Informationen gewinnen, die zu Präventionszwecken genutzt werden können.

- Übertragungssicherheit: Die Sicherheit von Daten und Informationen muss nicht nur innerhalb eines Systems gewährleistet sein. Auch die Übertragung der Daten muss den grundlegenden Sicherheitszielen gerecht werden.[69] Gerade in verteilten Umgebungen spielt dies eine bedeutende Rolle.[70]

Die vorliegende Arbeit konzentriert sich aufgrund des identifizierten Handlungsbedarfs[71] auf die Grundfunktion Autorisierung. Bei der zu entwickelnden Methode gilt es jedoch, eventuelle Abhängigkeiten und Schnittstellen zu den anderen Grundfunktionen aufzuzeigen und zu berücksichtigen.

2.2.4 Sicherheit in gewachsenen Applikationslandschaften

Informationsverarbeitung im Unternehmen wird in der Regel nicht von einer einzigen Applikation unterstützt, sondern von zahlreichen kooperierenden Applikationen.[72] Lange Zeit wur-

62 Vgl. Pipkin 2000, S. 121ff.
63 Vgl. Oppliger 1997, S. 173.
64 Vgl. Fischer-Hübner 2001, S. 78.
65 Vgl. Kersten 1995, S. 91; Schneider 2000, S. 97; Hoppe/Priess 2003, S. 83.
66 Vgl. Jonscher/Dittrich 1994, S. 27f.
67 Vgl. BSI 1998, S. 9.
68 Vgl. Jonscher/Dittrich 1994, S. 26.
69 Vgl. Oppliger 1997, S. 313.
70 Vgl. Rupprecht 2002, S. 20.
71 Vgl. Kapitel 1.1 und Kapitel 3.
72 Vgl. Ferstl/Sinz 1998, S. 202.

den Applikationen entlang der Organisationsstrukturen und Produktlinien geschaffen.[73] Durch die steigende Bedeutung von Datenbanken und Managementinformationssystemen wurden dann vermehrt Applikationen implementiert, die an Informationsobjekten ausgerichtet sind (z.B. Risikomanagementapplikationen). In letzter Zeit standen die Ausrichtung von Applikationen an den Vertriebskanälen und die Realisierung kanalübergreifender Funktionen im Vordergrund.

Der wechselnde Integrationsfokus und das unzureichende Management der Architekturen führte insbesondere bei mittleren und grossen Unternehmen zu Redundanzen oder Lücken in der Systemlandschaft:[74] Einerseits sind bestimmte Funktionalitäten oder Datenverarbeitungstransaktionen in mehr als einer Applikation realisiert. Andererseits sind gewisse Funktionalitäten nicht für jeden Prozess und Kanal verfügbar. In Bezug auf die Sicherheit führte die Entwicklung zu starken Redundanzen. Die einzelnen Applikationen enthalten meist eigenständige Sicherheitsfunktionen und -module, die jedoch oft proprietär und inkompatibel zueinander sind.[75]

Betrachtet man gewachsene Applikationslandschaften unter dem Aspekt der Sicherheit, so können diese als besonders gefährdet bezeichnet werden. Der Analyse können dabei folgende Bedrohungen zugrunde gelegt werden:

Störungen		**Angriffe**	
Fahrlässigkeit	**Höhere Gewalt**	**Aktive Angriffe**	**Passive Angriffe**
• Menschliches Versagen • Mangelhaftes System-Design	• Katastrophen • Technischer Defekt • Systemalterung • Umwelteinflüsse	• Logische Manipulationen • Physische Manipulation	• Abhören • Logischer Diebstahl

Tabelle 1: Bedrohungsarten der Sicherheit[76]

Bedrohungen können einerseits in unbeabsichtigt eingetretene Störungen[77] und andererseits in bewusst und gezielt herbeigeführte Angriffe[78] unterteilt werden. Als Ursache von Störungen können sowohl Fahrlässigkeit als auch höhere Gewalt identifiziert werden.[79] Angriffe können in aktive und passive Angriffe gegliedert werden. Aktive Angriffe zielen auf die Manipulation von Hardware und auf die logische Manipulation von Daten und Funktionen ab.[80] Passive Angriffe richten sich hingegen ausschliesslich gegen die Vertraulichkeit von Informationen.[81]

73 Vgl. auch im Folgenden Winter 2003a, S. 6.
74 Vgl. Winter 2003a, S. 7.
75 Vgl. Rupprecht 2002, S. 4.
76 Vgl. Lange 2004, S. 52.
77 Vgl. Lange 2004, S. 52.
78 Vgl. Raepple 2001, S. 98f.; Hoppe/Priess 2003, S. 34.
79 Vgl. Lange 2004, S. 52f.
80 Vgl. Lange 2004, S. 53.
81 Vgl. Lange 2004, S. 54.

Untersucht man die einzelnen Bedrohungskategorien, so kann für gewachsene Applikationslandschaften mittlerer und grosser Unternehmen festgehalten werden:

- Fahrlässigkeit und höhere Gewalt: Da gewachsene Applikationslandschaften in mittleren und grossen Unternehmen eine Vielzahl von Anwendern aufweisen, ist die Wahrscheinlichkeit für menschliches Versagen entsprechend hoch einzuschätzen. Durch die grosse Anzahl unterschiedlicher Systemelemente ist auch mangelndes System-Design wesentlich wahrscheinlicher als in homogenen Systemlandschaften. Dies gilt auch für technische Defekte und die Systemalterung.

- Aktive und passive Angriffe: Durch die Vielzahl von Systemelementen bieten gewachsene Applikationslandschaften eine grosse Angriffsfläche für Sabotage und Spionage. Mit steigender Zahl der Anwender ist darüber hinaus mit einer wachsenden Anzahl von Angreifern zu rechnen.

Gewachsene Applikationslandschaften sind somit aufgrund ihrer inhärenten Eigenschaften als besonders gefährdete Systeme anzusehen.

2.2.5 Abgrenzung zum Datenschutz

Die Begriffe Datensicherheit und Datenschutz werden oft sehr unterschiedlich und missverständlich verwendet.[82] Datenschutz ist eine Komponente zur Gewährleistung der individuellen Persönlichkeitsrechte. Diese Rechte umfassen drei Elemente:[83]

- Territoriale Persönlichkeitsrechte: Territoriale Persönlichkeitsrechte dienen dem Schutz der physischen Umgebung einer Person.

- Personenbezogene Persönlichkeitsrechte: Personenbezogene Persönlichkeitsrechte zielen auf die Vermeidung unangemessener Beeinträchtigungen ab, die eine Person beispielsweise durch unangemessene Leibesvisitationen oder Drogentests erfährt.[84]

- Informationsbezogene Persönlichkeitsrechte: Informationsbezogene Persönlichkeitsrechte regeln, ob und wie persönliche Daten gesammelt, gespeichert, verarbeitet und verbreitet werden.

Die informationsbezogenen Persönlichkeitsrechte wurden z.B. als „Recht auf informationelle Selbstbestimmung“ explizit durch das deutsche Bundesverfassungsgericht definiert.[85] Sie gewährleisten die „Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“. Datenschutz ist somit der Schutz von

82 Vgl. Heuer/Saake 2000, S. 560.
83 Vgl. Rosenberg 1992.
84 Vgl. Fischer-Hübner 2001, S. 6.
85 Vgl. im Folgenden BVerfGe 1983.

personenbezogenen Daten, um die Persönlichkeitsrechte zu gewährleisten.[86] Alle Datenschutzgesetze und -richtlinien sowohl der Schweiz als auch der Mitgliedstaaten der europäischen Union beziehen sich dabei auf den gesamten Datenbearbeitungsprozess.[87]

Datensicherheit ist eine wichtige Komponente zur Gewährleistung des Datenschutzes.[88] Um personenbezogene Daten zu schützen, sind technische Mechanismen notwendig, die den Grundfunktionen der Datensicherheit zugeordnet werden.[89]

2.3 Autorisierung

Die Sicherheitsgrundfunktion Autorisierung ist zentrales Thema dieser Arbeit. Im Folgenden werden daher grundlegende Konzepte der Autorisierung wie die rollenbasierte Zugriffskontrolle diskutiert. Abschliessend werden zentrale Aufgaben der Autorisierung im Kontext der Arbeit bezüglich des Informationsmanagements positioniert.

2.3.1 Grundlagen

Autorisierung oder synonym Zugriffskontrolle bezeichnet die Überprüfung und Verwaltung von Zugriffsrechten.[90] Die Überprüfung von Zugriffsrechten ist definiert als der Prozess der Vermittlung von Anfragen an Ressourcen und Daten eines Systems und die Entscheidung, ob die Anfrage zugelassen oder zurückgewiesen wird.[91] Die Verwaltung von Zugriffsrechten umfasst das Erteilen, Entziehen und Pflegen von Zugriffsrechten.[92] Drei grundlegende Verwaltungs-Paradigmen werden unterschieden:[93]

- Eigentümer-Paradigma: Beim Eigentümer-Paradigma verwaltet der Eigentümer eines Objektes dessen Zugriffsrechte. Der Erzeuger eines Objektes wird bei der Objekterschaffung automatisch zum Eigentümer. Das Recht zur Verwaltung von Zugriffsrechten kann der Eigentümer auch an andere übertragen.

- Besitzer-Paradigma: Das Besitzer-Paradigma besagt, dass bereits der Besitz eines Rechtes die Vergabe von Berechtigungen autorisiert. Nach Erhalt eines Rechtes kann der Besitzer dieses somit auch an andere übergeben.

86 Vgl. Fischer-Hübner 2001, S. 6.
87 Vgl. Hafner 2002; Schweizer 1999, S. 110ff.
88 Vgl. Schweizer 1999, S. 257.
89 Vgl. Fischer-Hübner 2001, S. 35.
90 Vgl. Jonscher/Dittrich 1994, S. 27f. und Kapitel 2.2.3.
91 Vgl. Samarati/de Capitani di Vimercati 2002, S. 137.
92 Vgl. Rupprecht 2002, S. 22.
93 Vgl. Oppliger 1997, S. 202, Seufert 2001, S. 50.

- Administrator-Paradigma: Beim Administrator-Paradigma verwaltet eine zentrale Instanz die Zugriffsberechtigungen. Die Besitzer und Eigentümer von Rechten haben keine Möglichkeit, Rechte eigenhändig weiterzugeben.

Neben den vorgestellten Reinformen existieren insbesondere in der Praxis weitere Mischformen der Rechtevergabe.[94] Da sich die unternehmensweite Durchsetzung und Überwachung von Sicherheitsrichtlinien auf der Basis des Eigentümer- und Besitzer-Paradigmas sehr schwierig gestaltet, hat sich in der Praxis das Administrator-Paradigma durchgesetzt.[95] Aus diesem Grund wird der Arbeit das Administrator-Paradigma zugrunde gelegt.

Im Laufe der Zeit wurden unterschiedliche Ansätze zur Spezifikation und Implementierung von Berechtigungen entwickelt. Diese Ansätze, die in der Regel an ein Paradigma zur Rechteverwaltung gekoppelt sind, können in drei Klassen eingeteilt werden:[96]

- Benutzerbestimmte Zugriffskontrolle: Die benutzerbestimmte Zugriffskontrolle basiert auf Zugriffsregeln, die direkt angeben, wer welche Aktionen mit welchen Ressourcen durchführen kann.[97] Im Englischen wird die benutzerbestimmte Zugriffskontrolle als „Discretionary Access Control“ („Beliebige Zugriffskontrolle“ oder „dem eigenen Ermessen überlassene Zugriffskontrolle“) bezeichnet, da der Nutzer die Möglichkeit hat, seine Rechte auch an andere Nutzer weiterzugeben.[98] Die Zugriffsmatrix ist das Konzept für die Beschreibung von benutzerbestimmten Zugriffskontrollkonzepten.[99]

- Systembestimmte Zugriffskontrolle: Die systembestimmte Zugriffskontrolle arbeitet auf der Basis von Sicherheitsmarken.[100] Diese beschreiben auf der einen Seite die Vertrauenswürdigkeit des zugreifenden Subjekts. Auf der anderen Seite bestimmen sie die Sensitivität einer Ressource. Die Verwaltung und der Abgleich der Sicherheitsmarken von zugreifenden Subjekten und Ressourcen werden durch eine zentrale Instanz geregelt.[101] Für die Sicherung der Integrität und der Vertraulichkeit existieren jeweils spezielle Konzepte.[102] Im Englischen wird die systembestimmte Zugriffskontrolle in Abgrenzung zur „Discretionary Access Controll“ als „Mandatory Access Control“ („Verbindliche Zugriffskontrolle“) bezeichnet.

- Rollenbasierte Zugriffskontrolle: Bei der rollenbasierten Zugriffskontrolle werden die Rechte nicht direkt an die zugreifenden Subjekte vergeben, sondern zu Rollen zusammengefasst.[103] Die zugreifenden Subjekte werden erst in einem zweiten Schritt den Rollen zu-

94 Vgl. Jonscher/Dittrich 1994, S. 44ff.
95 Vgl. Lau/Gerhardt 1994, S. 61f.
96 Vgl. z.B. Sandhu/Samarati 1994, S. 31ff; Samarati/de Capitani di Vimercati 2002, S. 139.
97 Vgl. Samarati/de Capitani di Vimercati 2002, S. 138.
98 Damit ist die benutzerbestimmte Zugriffskontrolle an das Besitzer-Paradigma gekoppelt.
99 Vgl. Samarati/de Capitani di Vimercati 2002, S. 140.
100 Vgl. im Folgenden Samarati/de Capitani di Vimercati 2002, S. 148; Pernul 1995, S. 245;
101 Vgl. Samarati/de Capitani di Vimercati 2002, S. 148; Pernul 1995, S. 245; Fischer-Hübner 2001, S. 148.
102 Vgl. Pernul 1995, S. 235ff; Samarati/de Capitani di Vimercati 2002, S. 148ff.
103 Vgl. Samarati/de Capitani di Vimercati 2002, S. 180.

geordnet. Rollen stellen somit die Zusammenfassung von Rechten dar, die zur Erfüllung von mit ihnen verbunden Aufgaben notwendig sind.[104] Die Hauptmotivation hinter der rollenbasierten Zugriffskontrolle liegt in der Tatsache, dass bei der Ausführung von Geschäftstätigkeiten nicht die Identität der einzelnen Person, sondern die organisatorischen Verantwortlichkeiten der Person im Vordergrund stehen.[105]

Als dominierendes Verfahren der Zugriffskontrolle etablierte sich in den 1990er Jahren die rollenbasierte Autorisierung.[106] Deshalb wird die Arbeit auf dem rollenbasierten Konzept aufbauen. Dieses soll im Folgenden noch einmal detaillierter vorgestellt werden.

2.3.2 Rollenbasierte Zugriffskontrolle

Obwohl für die rollenbasierte Zugriffskontrolle unterschiedlichste Ansätze vorgestellt und implementiert wurden, sind ihnen allen doch grundlegende Konzepte gemein.[107] Massgeblich vorangetrieben wird die rollenbasierte Zugriffskontrolle vom National Institute of Standards and Technology (NIST),[108] das den „NIST Standard for Role-Based Access Control“ zur rollenbasierten Zugriffskontrolle herausgegeben hat.

Der Standard definiert unterschiedliche Modelle, die eine Menge von Elementen und ihre Beziehungen beschreiben, die typischerweise in rollenbasierten Systemen implementiert sind.[109] Die entwickelten Modelle unterscheiden sich in ihrer Mächtigkeit. Während das Grundlagenmodell „Core RBAC“ lediglich essentielle Konstrukte der rollenbasierten Zugriffskontrolle enthält, verwenden die Modelle „Hierarchical RBAC“, „Static Seperation of Duty“ und „Dynamic Separation of Duty“ erweiterte Konzepte. Um die typischen Elemente zu identifizieren, führte das NIST umfassende Marktanalysen durch und implementierte diverse Prototypen.[110] Die folgenden Ausführungen beziehen sich auf das Modell „Hierarchical RBAC“, da das Modell sich auf die grundlegenden Elemente der rollenbasierten Zugriffskontrolle konzentriert, jedoch die Verschachtelung von Rollen ermöglicht. Die Verschachtelung von Rollen ist ein häufig implementiertes Konzept in kommerziellen Autorisierungsprodukten.[111]

104 Vgl. Lau/Gerhardt 1994, S. 66.
105 Vgl. Samarati/de Capitani di Vimercati 2002, S. 180.
106 Vgl. Herwig/Schlabitz 2004, S. 290.
107 Vgl. Samarati/de Capitani di Vimercati 2002, S. 181.
108 Vgl. Herwig/Schlabitz 2004, S. 290.
109 Vgl. Ferraiolo et al. 2001, S. 227.
110 Vgl. Ferraiolo et al. 2001, S. 225.
111 Vgl. Chandramouli/Sandhu 1998.

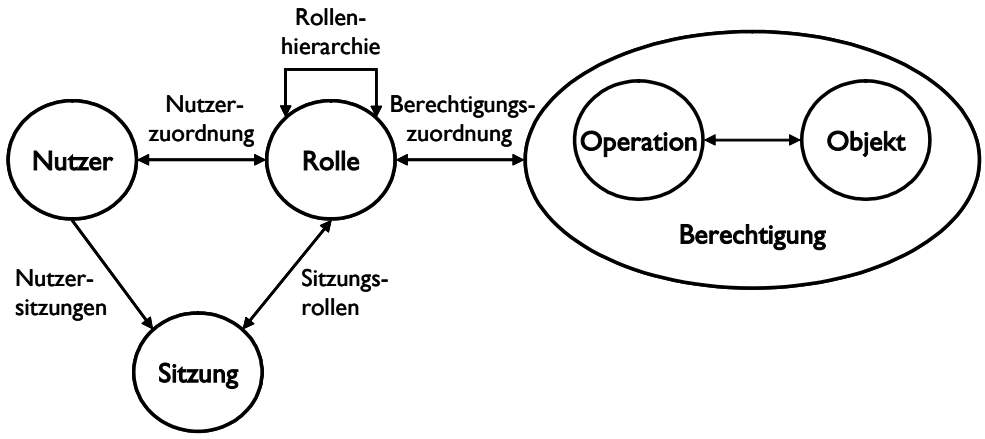

Abbildung 7: Role-Based Access Control (RBAC) Modell[112]

Die wesentlichen Elemente des Standards (vgl. Abbildung 7) sind wie folgt definiert:

- Nutzer: Ein Nutzer bzw. Benutzer ist ein menschliches Wesen.[113] Der Begriff des Nutzers kann auch auf Computerprogramme, Maschinen, Netzwerke oder andere technische Konstrukte ausgeweitet werden, so dass die erfolgte Definition im Standard sehr eng gefasst ist.

- Rolle: Eine Rolle ist eine benannte Beziehung zwischen Berechtigungen und Benutzern.[114] Eine Rolle umfasst die Berechtigungen, die notwendig sind, um eine geschäftliche Aufgabe mit den entsprechenden Verantwortungen und Befugnissen auszuüben.[115]

- Berechtigung: Eine Berechtigung ermöglicht die Ausführung einer Operation auf einem geschützten Objekt.[116] Die Art der Operation und des Objekts hängt von dem jeweiligen System ab, das durch die rollenbasierte Zugriffskontrolle geschützt ist.

- Sitzung: Eine Sitzung ordnet einem Nutzer eine aktivierte Menge von Rollen zu.[117] Somit ist es möglich, dass ein Nutzer zu einem bestimmten Zeitpunkt lediglich einen Teil seiner Berechtigungen ausübt.

Die Nutzerzuordnung und die Berechtigungszuordnung sind viele-zu-viele Beziehungen. Die Rollenhierarchie definiert eine Vererbungsbeziehung zwischen Rollen.[118] Dadurch lassen sich Unternehmensstrukturen einfach und adäquat abbilden.[119] Eine Rolle R1 erbt von einer Rolle R2, wenn R1 alle Berechtigungen von R2 umfasst.[120]

---

112 Vgl. Ferraiolo et al. 2001, S. 235
113 Vgl. im Folgenden Ferraiolo et al. 2001, S. 233.
114 Vgl. Ferraiolo et al. 2001, S. 232.
115 Vgl. Ferraiolo et al. 2001, S. 233.
116 Vgl. auch im Folgenden Ferraiolo et al. 2001, S. 233.
117 Vgl. Ferraiolo et al. 2001, S. 233.
118 Vgl. Ferraiolo et al. 2001, S. 234.
119 Vgl. Rupprecht 2002, S. 35.
120 Vgl. Ferraiolo et al. 2001, S. 235.

Die Modelle „Static Seperation of Duty“ und „Dynamic Separation of Duty“ erweitern das Modell „Hierarchical RBAC“ um Konzepte, die die explizite Trennung von Aufgaben ermöglichen. Bei der statischen Trennung von Aufgaben werden die Zuordnung von Nutzern zu Rollen sowie die Zuordnung von Rollen zu Rollen eingeschränkt.[121] Durch eine Zuordnungskonfliktmatrix kann beispielsweise festgelegt werden, welche Rollen ein Nutzer nicht gleichzeitig innehaben darf.[122] Die dynamische Aufgabentrennung schränkt die Rollen ein, die in einer Sitzung aktiviert werden können:[123] Ein Nutzer besitzt beispielsweise mehrere Rollen, darf sie aber nicht gleichzeitig aktivieren, sondern muss explizit angeben, in welcher Rolle er zu einem bestimmten Zeitpunkt agieren möchte.[124]

2.3.3 Integration der Zugriffskontrolle

Gewachsene Applikationslandschaften sind dadurch gekennzeichnet, dass die einzelnen Applikationen meist eigenständige Sicherheitsfunktionen und -module enthalten.[125] Wenige Applikationen sind durch auf dem Markt verfügbare Zugriffskontrollwerkzeuge gesichert. Die Mechanismen der vorhandenen Sicherheitskomponenten sind oft proprietär und inkompatibel zueinander.[126]

Ein typischer Anwender braucht Zugang zu unterschiedlichen Systemen auf diversen Systemplattformen.[127] Bestehende Berechtigungskonzepte[128] sind jedoch häufig applikations- oder systemspezifisch, so dass die Administration von Berechtigungen weitestgehend unabhängig und unkoordiniert in den einzelnen Komponenten stattfindet.[129]

Um die unkoordinierte Rechtevergabe zu überwinden und somit eine integrierte, effektive und effiziente Administration zu gewährleisten, wurden Konzepte für die systemübergreifende Zugriffskontrolle entwickelt. Das „Enterprise RBAC Model (ERBAC)“[130] und seine Erweiterungen[131] (vgl. Abbildung 8) sind im Kontext dieser Arbeit besonders hervorzuheben, da sie auf der Basis des rollenbasierten NIST-Standards entwickelt wurden. Wie auch der NIST-Standard versucht der ERBAC-Ansatz, die grundlegenden Konzepte der rollenbasierten, systemübergreifenden Zugriffskontrolle darzustellen und zu systematisieren.[132]

---

121 Vgl. Ferraiolo et al. 2001, S. 230.
122 Vgl. Rupprecht 2002, S. 36.
123 Vgl. Ferraiolo et al. 2001, S. 231.
124 Vgl. Jonscher/Dittrich 1994, S. 31.
125 Vgl. im Folgenden Kern et al. 2002, S. 45.
126 Vgl. Kapitel 2.2.4.
127 Vgl. im Folgenden Kern et al. 2002, S. 45.
128 Unter einem Berechtigungskonzept wird im Folgenden eine Menge von Regeln verstanden, die festlegt, welcher Benutzer auf welche Funktionen und Daten zugreifen darf.
129 Vgl. im Folgenden Kern et al. 2002, S. 45.
130 Vgl. Kern et al. 2002, S. 46.
131 Vgl. insbesondere Kuhlmann et al. 2003, S. 183.
132 Vgl. Kern et al. 2002, S. 46.

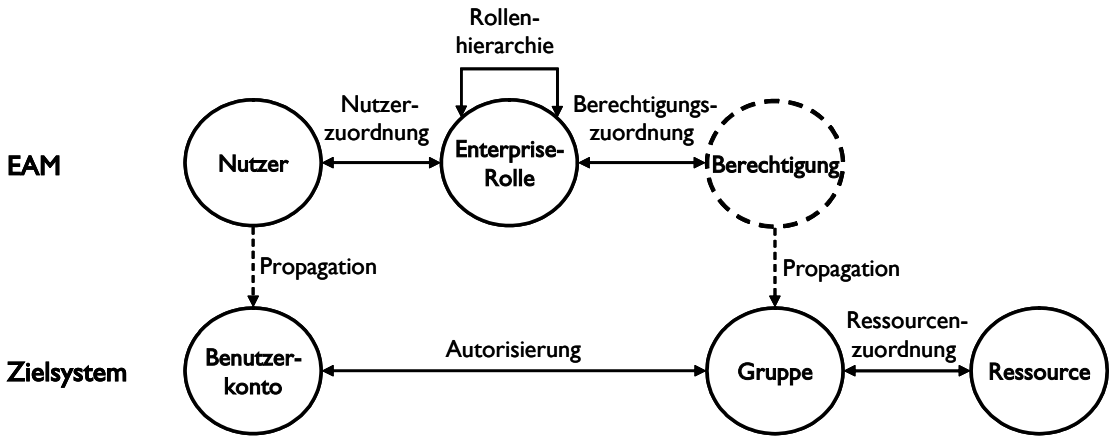

Abbildung 8: Enterprise Role-Based Access Control (ERBAC) Modell[133]

Die wesentlichen Elemente des ERBAC-Ansatz sind:

- Nutzer: Der Nutzer ist analog zum NIST-Standard als menschliches Wesen definiert.[134] Die Berechtigungen der Nutzer werden in einem zentralen Enterprise Access Management Werkzeug (EAM) verwaltet.

- Enterprise-Rolle: Eine Enterprise-Rolle ist eine Rolle[135], die nicht systemspezifisch ist.[136] Somit kann sie Berechtigungen umfassen, die sich auf mehr als ein System beziehen. Enterprise-Rollen können auch andere Enterprise-Rollen enthalten, so dass sie die entsprechenden Berechtigungen erben.[137] Die Enterprise-Rollen werden ebenfalls im zentralen EAM-Werkzeug verwaltet.

- Berechtigung: Der Begriff Berechtigung wird im Rahmen der Ausführungen zum ERBAC-Ansatz nicht explizit definiert.[138] Bei KUHLMANN ET AL. ist das Element Berechtigung dann auch nicht mehr in der Diskussion zu finden:[139] Die Enterprise-Rolle wird direkt der Gruppe zugeordnet. Eine Berechtigung kann somit im Kontext der Enterprise-Rollen als Zuordnung einer Gruppe zu einer Enterprise-Rolle definiert werden.

- Benutzerkonto: Ein Nutzer wird in einem System durch ein Benutzerkonto repräsentiert.[140] Die Definition der Nutzer im EAM-Werkzeug führt zur Generierung von Benutzerkonten in den entsprechenden Zielsystemen.

- Gruppe: Die Vergabe von Rechten erfolgt heute in der Regel über intermediäre Konstrukte wie Rollen oder Gruppen.[141] Ein Nutzer bekommt seine Berechtigungen in den Syste-

133 Vgl. In Anlehnung an Kern et al. 2002, S. 46 und Kuhlmann et al. 2003, S. 183.
134 Vgl. Ferraiolo et al. 2001, S. 233.
135 Vgl. Kapitel 2.3.2.
136 Vgl. Kuhlmann et al. 2003, S. 182.
137 Vgl. im Folgenden Kern et al. 2002, S. 46.
138 Vgl. Kern et al. 2002, S. 46.
139 Vgl. Kuhlmann et al. 2003, S. 182f.
140 Vgl. Kern et al. 2002, S. 46.
141 Vgl. Kuhlmann et al. 2003, S. 182f.

men damit nicht direkt zugeordnet. Eine Gruppe umfasst im Gegensatz zu einer Rolle keine definierte Menge von Rechten, sondern eine Menge von Nutzern.[142] Im Kontext des hier diskutierten Modells bezeichnet eine Gruppe jedoch nicht ausschliesslich eine Menge von Nutzern. Vielmehr ist eine Gruppe im Kontext des Ansatzes ein intermediäres, systemspezifisches Konstrukt zur Berechtigungsvergabe.[143] Eine Gruppe kann so beispielsweise eine Gruppe in Windows NT oder auch eine Rolle in SAP repräsentieren. Sind den Enterprise-Rollen entsprechende Gruppen zugewiesen, so können bei der Zuordnung eines Nutzers zu einer Enterprise-Rolle die entsprechenden Gruppen- bzw. Rollenzugehörigkeiten in den Zielsystemen automatisch vom EAM-Werkzeug vorgenommen werden.

- Ressource: Der Begriff Ressource wird im Rahmen der Ausführungen zum ERBAC-Ansatz ebenfalls nicht explizit definiert.[144] Die Verwendung des Begriffs im Kontext der einschlägigen Arbeiten[145] zeigt jedoch Parallelen zur NIST-Definition des Begriffs Berechtigung auf: Der Zugriff auf eine Ressource kommt somit der Ausführung einer Operation auf einem geschützten Objekt[146] gleich. Die Ressourcen der einzelnen Systeme sind systemspezifischen Gruppen zugeordnet. Diese können damit auf die entsprechenden Ressourcen zugreifen.

Die einzige Entität im NIST-Standard, die sich nicht im ERBAC-Modell wiederfindet, ist die Sitzung. Der Grund dafür liegt darin, dass die eigentliche Zugriffskontrolle nach wie vor bei den einzelnen Systemen liegt. Zur Laufzeit wird das EAM-Werkzeug nicht in Zugriffskontrollprozess einbezogen. Das laufzeitspezifische Element Sitzung hat somit im ERBAC-Modell keine Relevanz.[147]

Nachdem grundlegende Konzepte und Standards der Autorisierung dargestellt wurden, werden im Folgenden zentrale Aufgaben der Autorisierung im Kontext der Arbeit bezüglich des Informationsmanagements positioniert.

2.3.4 Autorisierung im Informationsmanagement

Das Informationsmanagement beschäftigt sich mit der Identifikation und Umsetzung der Potenziale der Informations- und Kommunikationstechnik und ist damit Teil der Unternehmensführung.[148] Die Aufgaben des Informationsmanagements können in drei Bereiche untergliedert werden.[149] Im Mittelpunkt der Informationsbewussten Unternehmensführung steht der effektive Einsatz von IT-Ressourcen unter einer gesamtunternehmerischen Perspektive. Das

142 Vgl. Sandhu 1996, S. I-25.
143 Vgl. Kuhlmann et al. 2003, S. 182f.
144 Vgl. Kern et al. 2002, S. 46.
145 Vgl. Kern et al. 2002, S. 46f.; Kuhlmann et al. 2003, S. 183f.
146 Vgl. Ferraiolo et al. 2001, S. 233.
147 Vgl. Kern et al. 2002, S. 46.
148 Vgl. Zarnekow et al. 2004, S. 4f.
149 Vgl. im Folgenden Winter 2002, S. 944f.; Zarnekow et al. 2004, S. 5.

Management des Informationssystems betrachtet die Entwicklung und den Betrieb des Informationssystems als Ganzes, d.h. die Summe aller einzelnen Informationssysteme im Unternehmen. Das Management der Informatik konzentriert sich auf die personellen Ressourcen und die technische Infrastruktur zur Entwicklung und zum Betrieb des Informationssystems.

In der Praxis wird das Informationsmanagement traditionell in die Kernphasen Planung (Plan), Entwicklung (Build) und Betrieb (Run) unterteilt (vgl. Abbildung 9).[150] Die Planung umfasst den ganzheitlichen, unternehmensweiten Blick auf den IT-Einsatz, die Entwicklung konzentriert sich auf den Entwurf und die Implementierung des Informationssystems und die Produktion umfasst Tätigkeiten des Betriebs und der Wartung. Jeder Phase sind spezifische Aufgaben zugeordnet. Neben den phasenspezifischen Aufgaben umfasst das Informationsmanagement in der Praxis auch Querschnittsaufgaben wie z.B. Controlling oder Qualitätsmanagement.

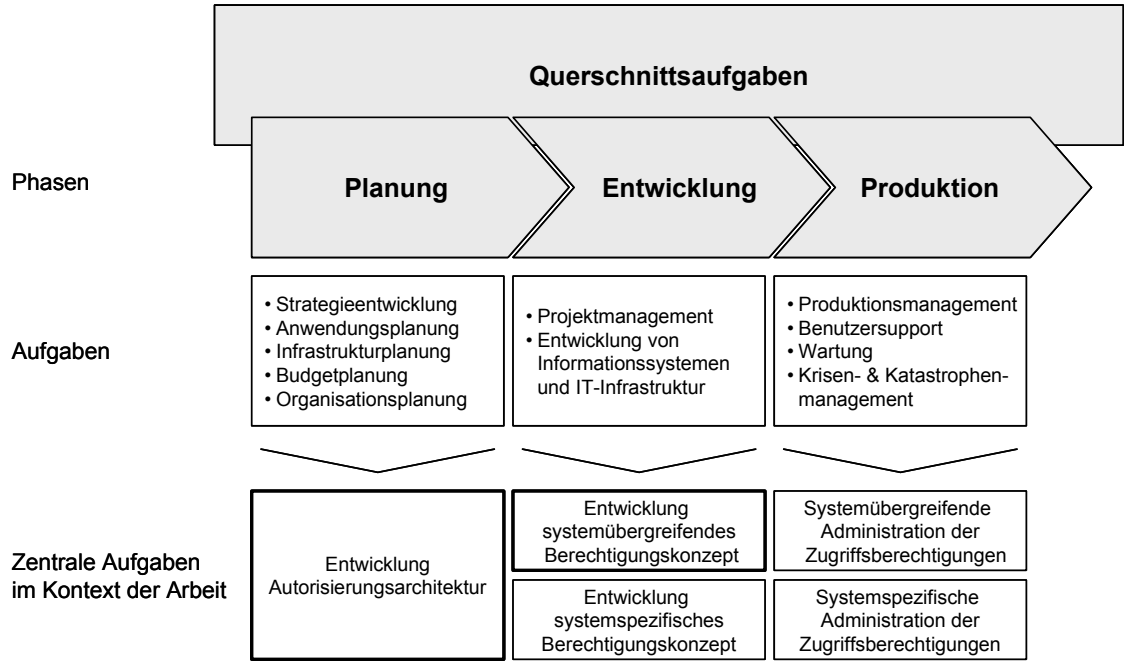

Abbildung 9: Autorisierung im Kontext des Informationsmanagements[151]

Abbildung 9 ordnet zentrale Aufgaben der Autorisierung, die im unmittelbaren Kontext der Dissertation stehen,[152] den Phasen des Informationsmanagements zu. Der Entwicklung einer Autorisierungsarchitektur liegt eine ganzheitliche, unternehmensweite Perspektive zugrunde, so dass sie der Planungsphase zugeordnet werden kann. Die Entwicklung von systemspezifischen und systemübergreifenden Berechtigungskonzepten ist der Entwicklungsphase zuzuordnen. Die systemspezifische und systemübergreifende Administration der Zugriffsberechtigungen kann schlussendlich der Phase Produktion zugerechnet werden. Die Arbeit fokussiert sich auf die hervorgehobenen Aufgaben „Entwicklung Autorisierungsarchitektur“ und „Entwicklung systemübergreifendes Berechtigungskonzept“ und adressiert damit die

150 Vgl. Zarnekow et al. 2004, S. 6.
151 Vgl. Zarnekow et al. 2004, S. 7.
152 Vgl. Kapitel 1.2.

Themenschwerpunkte Architektur und Integration der Kompetenzzentren CC AIM und CC IF, in deren Umfeld sie entstanden ist.[153]

2.4 IT-Risikomanagement

Risikomanagement beschäftigt sich mit der systematischen Bewältigung von Risiken.[154] Autorisierung als Zugriffskontrolle und -verwaltung wird implementiert, um potenzielle Schäden zu vermeiden und sich gegen Risiken zu schützen. Autorisierung ist somit ein Element der Risikobewältigung und Teil des Risikomanagements. Im Folgenden werden daher die grundlegenden Konzepte des IT-Risikomanagements dargestellt, soweit sie im Kontext dieser Arbeit relevant sind.

2.4.1 Grundlagen

Bevor auf den Begriff des IT-Risikomanagements eingegangen wird, werden nachfolgend zunächst die Begriffe Risiko, Schaden und Risikomanagement definiert.

Dieser Arbeit liegt ein entscheidungsbezogenes Risikoverständnis zugrunde.[155] Danach resultiert Risiko ursachenbezogen aus der Unsicherheit zukünftiger Ereignisse (Bedrohungen) und schlägt sich wirkungsbezogen in einer negativen Abweichung von einer festgelegten Zielgrösse nieder.[156] Dem ursachenbezogenen Begriff des Risikos steht der wirkungsbezogene Begriff des Schadens gegenüber. Schaden bezeichnet das „ungünstige Ergebnis der getroffenen Entscheidung“.[157]

Zu den Aufgaben des Risikomanagements zählen die Risikoanalyse, die Risikobewertung sowie die Risikobewältigung und das Risikocontrolling.[158] Die Risikoanalyse identifiziert die auf das Unternehmen einwirkenden Risiken. Die Risikobewertung nimmt eine Gewichtung der identifizierten Risiken vor. Die beiden Aufgaben Risikoanalyse und -bewertung bilden die Grundlage dafür, dass Risiken wirkungsvoll durch die Aufgabe Risikobewältigung adressiert werden können.[159] Die dabei definierten Massnahmen werden im Rahmen des Risikocontrol-

153 Vgl. Kapitel 1.2.
154 Vgl. dazu die Ausführungen im folgenden Abschnitt 2.4.1.
155 Nach IMBODEN lassen sich die gängigsten Risikobegriffe in die drei Klassen extensiver Risikobegriff, entscheidungsbezogener Risikobegriff und informationsorientierter Enscheidungsbegriff unterteilen (vgl. Imboden 1983, S. 41.): Die extensiven Definitionen sehen die Ursachen des Risikos nicht im Entscheidungsprozess, sondern in den Begleiterscheinungen jeder wirtschaftlichen Tätigkeit. Der entscheidungsbezogene Risikobegriff sieht die Gefahr der Fehlentscheidung als konstituierendes Element, mit der Unsicherheit des Aktors als Hauptproblem. Die informationsorientierte Fassung sieht das Risiko nicht als Gefahr, sondern als unsichere Informationsstruktur. Da diese Arbeit im Sinne des Methoden-Engineering einen problemlösenden, entscheidungsunterstützenden Charakter hat, wird im Folgenden der entscheidungsorientierte Informationsbegriff zugrunde gelegt.
156 Vgl. Schulte 1997, S. 12.
157 Vgl. Phillipp 1976, Sp. 3455.
158 Vgl. Wolf/Runzheimer 2000, S. 25.
159 Vgl. Laing/Forzi 2003, S. 108.

lings auf ihre Wirksamkeit überprüft. Die Aufgaben des Risikomanagements sind als Zyklus zu interpretieren.[160]

Das IT-Risikomanagement konzentriert sich auf die systematische Bewältigung von IT-Risiken.[161] IT-Risiken ergeben sich aus der Verwendung von Informationssystemen und sind Teil des operationellen Risikos.[162] Das operationelle Risiko ist „die Gefahr von Verlusten, die infolge einer Unzulänglichkeit oder des Versagens von internen Verfahren, Menschen und Systemen oder infolge externer Ereignisse eintreten".[163] Die Bedeutung des operationellen Risikos und somit die des IT-Risikos steigt:[164] Mittlerweile stufen deutsche Banken das operationelle Risiko beispielsweise als zweitwichtigste Risikokategorie ein.[165]

2.4.2 IT-Risikoanalyse

Ziel der Risikoanalyse ist es, Störfaktoren und deren Wirkung zu identifizieren und zu analysieren.[166] Unterschieden werden können die progressive und die retrograde Risikoidentifikation. Während die progressiven Ansätze von den Risikoursachen ausgehen,[167] setzen die retrograden Methoden bei den Sicherheitszielen[168] an, um Risken zu identifizieren[169].

Im Bereich der IT-Risikoanalyse werden beide Ansätze verwendet. Zum einen hat sich in der Praxis die Verwendung bereits vorgefertigter Gefährdungskataloge bewährt.[170] Die Verwendung dieser Kataloge entspricht der progressiven Risikoidentifikation. Zum anderen wird die retrograde Identifikation von Risiken praktiziert, z.B. indem eine Bedrohungsanalyse in Bezug auf die grundlegenden Ziele der IT-Sicherheit „Verfügbarkeit", „Integrität" und „Vertraulichkeit" durchgeführt wird.[171]

Um die Risikoanalyse und Bewertung sozio-technischer Systeme zu unterstützen, haben sich im Laufe der Zeit zahlreiche Kriterienkataloge etabliert.[172] Diese meist von gemeinnützigen Organisationen entwickelten Kataloge bilden die Basis für eine unabhängige Bewertung der Systeme. Die unterschiedlichen Kriterienkataloge können zum einen nach ihrem Fokus unterschieden werden:[173] Einige Kataloge konzentrieren sich auf einzelne, spezifische System-

160 Vgl. Wolf/Runzheimer 2000, S. 25.
161 Zum Verhältnis Risikomanagement und IT vgl. z.B. Laing/Forzi 2003, S. 109; Theil 1995, S. 22.
162 Vgl. Jörg/Rossbach 2002, S. 73f.
163 Vgl. Basler Ausschuss für Bankenaufsicht 2004, S. 127.
164 Vgl. Jörg/Rossbach 2002, S. 71f.
165 Banken sind verpflichtet, entsprechend ihres Risikos Eigenkapitel zu hinterlegen. Dieses steht somit nicht für anderweitige wirtschaftliche Zwecke wie z.B. die Kreditvergabe zur Verfügung (vgl. Jörg/Rossbach 2002, S. 75ff).
166 Vgl. Haller 1986, S. 28ff.
167 Vgl. Fürer 1990, S. 65.
168 Vgl. Kapitel 2.2.2.
169 Vgl. Wolf/Runzheimer 2000, S. 35.
170 Vgl. Laing/Forzi 2003, S. 109.
171 Vgl. z.B. ISF 2003.
172 Vgl. im Folgenden Fischer-Hübner 2001, S. 90.
173 Vgl. im Folgenden Initiative D21 2001, S. 7.

komponenten. Andere betrachten hingegen das gesamte Informationssystem einer Unternehmung. Zum anderen erlaubt die jeweils eingenommene Sicht eine Klassifizierung der Kataloge:[174] Kriterienkataloge mit primär technischer Perspektive, Kriterienkataloge mit primär organisatorischer Perspektive und Kriterienkataloge mit bewusst ausgeglichener Betrachtung können unterschieden werden. Da dieser Arbeit eine ganzheitliche Sichtweise zugrunde liegt, sind die Kriterienkataloge, die eine ausgeglichene Perspektive mit dem Fokus auf das Gesamtsystem aufweisen, von besonderem Interesse für diese Arbeit.

2.4.3 IT-Risikobewertung

Wie die Risikoidentifikation dient die Risikobewertung als Entscheidungsgrundlage für die Ableitung von Risikobewältigungsmassnahmen. Bei den für die Bewertung wesentlichen Parametern handelt es sich zum einen um das Schadensausmass, also die Höhe der negativen Zielabweichungen, zum anderen um deren Eintrittswahrscheinlichkeiten, also Informationen über die Häufigkeit negativer Zielabweichungen.[175]

Die unterschiedlichen Verfahren für die IT-Risikobewertung können anhand ihrer Vorgehensweise in zwei Klassen geteilt werden. Methodische Ansätze wie z.B. die Schutzbedarfsfeststellung des IT-Grundschutzhandbuchs[176] unterscheiden nicht explizit zwischen Schadensausmass und Schadenseintrittswahrscheinlichkeit und kommen so direkt zu einer einzigen Risikobewertungszielgrösse. Andere Verfahren hingegen ermitteln erst die Schadenshöhe (z.B. anhand von Schadenskategorien) und die Schadenswahrscheinlichkeit (z.B. anhand von Bedrohungen), um diese dann in einem zweiten Schritt zu verdichten.[177]

2.4.4 IT-Risikobewältigung

Ziel der Risikobewältigung ist die Ausarbeitung und Implementierung von Massnahmen, um sämtliche als kritisch eingestufte Risiken auf ein akzeptables Restrisiko zu reduzieren.[178] Dabei wird zwischen ursachen- und wirkungsbezogenen Massnahmen unterschieden. Während die ursachenbezogenen Massnahmen auf die Risikovermeidung, -verminderung und -streuung zielen, umfassen die wirkungsbezogenen Massnahmen die Risikoüberwälzung, -übernahme und -versicherung (vgl. Abbildung 10):[179]

- Risikovermeidung: Die Risikovermeidung versucht als defensive Taktik, die Risiken anzugehen und vollständig zu beseitigen.

---

174 Vgl. im Folgenden Initiative D21 2001, S. 7.
175 Vgl. Theil 1995, S. 79.
176 Vgl. BSI 2004, Kapitel 2.2.
177 Vgl. z.B. Zentrum für sichere Informationstechnologie - Austria 2004, Kapitel 3.2.
178 Vgl. Laing/Forzi 2003, S. 110.
179 Vgl. Wolf/Runzheimer 2000, S. 71ff.

- Risikoverminderung: Die Risikoverminderung versucht, die Eintrittswahrscheinlichkeiten (Schadensverhütung) und die Auswirkungen (Schadensherabsetzung) von Schäden zu reduzieren.

- Risikostreuung: Die Risikostreuung versucht durch eine gezielte Abstimmung von Einzelmassnahmen, die Summe der Einzelrisiken herabzusetzen.

- Risikoüberwälzung: Die Risikoüberwälzung bezeichnet die Übertragung von Risiken auf Dritte z.B. durch Factoring, Leasing oder die Verwendung von Allgemeinen Geschäftsbedingungen. Nicht unter den Begriff der Schadenüberwälzung fällt die Überwälzung von Risiken auf Versicherungen.

- Risikoübernahme: Die Risikoübernahme bezeichnet das bewusste, aktive Selbsttragen von Risiken, welches z.B. mit Massnahmen wie der Bildung von Rückstellungen einhergeht.

- Risikoversicherung: Die Risikoversicherung bezeichnet die Übertragung von Risiken an Versicherungen.

Autorisierung als Verwaltung und Überprüfung von Zugriffsrechten[180] ist den ursachenbezogenen Teilgebieten der Risikobewältigung „Risikovermeidung“ und „Risikoverminderung“ zuzuordnen.

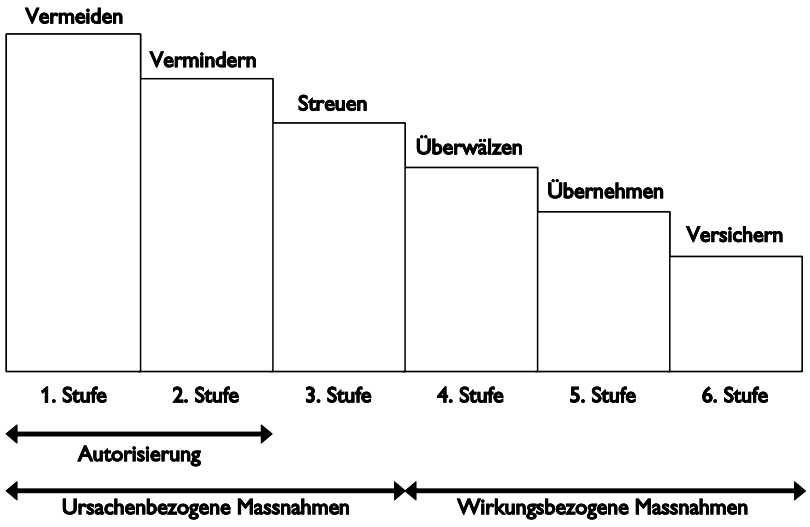

Abbildung 10: Optionen der Risikobewältigung[181]

2.4.5 IT-Risikocontrolling

Unter Risikocontrolling wird die Messung und Überwachung von Risikopositionen verstanden.[182] Darüber hinaus kann die Berichterstattungsfunktion zu diesem Begriffsverständnis

180 Vgl. Kapitel 2.3.1.
181 Vgl. Wolf/Runzheimer 2000, S. 70.
182 Vgl. z.B. Bundesaufsichtsamt für das Kreditwesen 1996.

hinzugerechnet werden.[183] GROSS/KNIPPSCHILD betonen dabei den unternehmensweiten Fokus des Risikocontrollings, das sich u.a. durch eine unternehmensweite Perspektive auf das Risiko auszeichnet und unternehmensweite Standards zum Risikomanagement setzt.[184]

Dem vorgestellten Begriffsverständnis entgegen steht ein weiter gefasster Risikocontrolling-begriff.[185] Demnach umfasst das Risikocontrolling die Planung, Steuerung, Informations-versorgung und Kontrolle des Risikomanagementprozesses mit seinen Phasen Risiko-identifikation, -bewertung und -bewältigung. In diesem Sinne kommt dem Riskocontrolling auch im Bereich der IT eine besondere Bedeutung zu: Im Rahmen der Beurteilung von Informationssystemen durch externe Gutachter steht die Bewertung des Risikocontrollingprozesses noch vor der Prüfung des eigentlichen sozio-technischen Systems.[186] Sollte der Risikocontrollingprozess Schwächen aufweisen, so erfolgt eine intensivere Überprüfung des eigentlichen Systems.[187]

2.5 Konsequenzen für die Methode

Aus den diskutierten Themengebieten Business Engineering, Sicherheit, Autorisierung und IT-Risikomanagement lassen sich folgende Konsequenzen für die weitere Vorgehensweise ermitteln:[188]

- **Methodisches Vorgehen**: Im Business Engineering stellt das Methoden-Engineering das methodische, ingenieurmässige Vorgehen sicher. Die zu entwickelnde Methode soll daher alle Gestaltungselemente des Methoden-Engineering[189] berücksichtigen, um die vom Business Engineering geforderte systematische Transformation zu erzielen.

- **Ganzheitlichkeit**: Dieser Arbeit liegt ein umfassender Sicherheitsbegriff zugrunde,[190] dem die zu entwickelnde Methode gerecht werden muss. Dieses umfassende Begriffsverständnis geht über die rein technische Betrachtung von Sicherheit hinaus. Daher müssen nicht nur technische, sondern auch organisatorische und rechtliche Sicherheitsaspekte in die Methodenentwicklung einfliessen.

- **Rollenbasierte Autorisierung**: Als dominierendes Verfahren der Zugriffskontrolle etablierte sich in den 1990er Jahren die rollenbasierte Autorisierung. Die im Rahmen der Dissertation zu entwickelnde Methode soll daher auf dem rollenbasierten Konzept aufbauen.

---

183 Vgl. Gross/Knippschild 1996, S. 94.
184 Vgl. Gross/Knippschild 1996, S. 94.
185 Vgl. Wolf/Runzheimer 2003, S: 93.
186 Vgl. ISACA 2000, S. 25.
187 Vgl. ISACA 2000, S. 25.
188 Die Ableitung der Konsequenzen erfolgt in Anlehnung an Kremer 2004, S. 33.
189 Vgl. Kapitel 2.1.3.
190 Vgl. Kapitel 2.2.1.

- **Systemunabhängigkeit**: Obwohl unterschiedlichste Ansätze für die rollenbasierte Zugriffskontrolle vorgestellt und implementiert wurden, sind die grundlegenden Konzepte allen Ansätzen gemein. Um eine maximale Anwendbarkeit der Methode sicherzustellen, soll die Methode systemunabhängig und, wo möglich, standardbasiert[191] gestaltet werden.

- **Risikogesteuerte Vorgehensweise**: Autorisierung ist eine ursachenbezogene Massnahme zur Bewältigung von Risiken. Sehr umfangreiche Sicherheitsmassnahmen sind nur durch einen entsprechend hohen Einsatz von Ressourcen umzusetzen. Geringe Vorkehrungen bergen das Risiko, dass es zu erheblichen Schäden infolge mangelnder Sicherheit kommt. Daher gilt es, die Sicherheitsmassnahmen in Abhängigkeit vom Risiko zu gestalten. Eine risikogesteuerte Vorgehensweise ist geboten.

Das folgende Kapitel diskutiert bestehende methodische Ansätze anhand der abgeleiteten Konsequenzen.

[191] Vgl. hierzu die Standards RBAC und ERBAC in Kapitel 2.3.

3 Vergleich bestehender Ansätze

In den vergangenen Jahren haben sich einige wenige methodische Ansätze entwickelt, die sich mit dem Thema Autorisierung auseinandersetzen. Im Folgenden werden die für diese Arbeit wesentlichen Ansätze vorgestellt und bewertet.

3.1 Auswahl der relevanten Ansätze

Für die folgende Diskussion wurden Ansätze ausgewählt, die sich im Hinblick auf die Entwicklung einer Methode für die Autorisierung verwerten lassen und somit:

- Einen expliziten Bezug zur Autorisierung aufweisen
- Methoden darstellen oder methodische Elemente beinhalten
- Bezüglich ihres Abstraktionsgrads eine hinreichend konkrete Diskussion erlauben
- Umsetzungsorientiert sind bzw. bereits in der Praxis eingesetzt wurden

Die Analyse umfasst die in Tabelle 2 aufgeführten Ansätze.

Ansatz	Themenschwerpunkt: Autorisierungs-architektur	Themenschwerpunkt: System-übergreifende Berechtigungs-konzepte	Themenschwerpunkt: System-spezifische Berechtigungs-konzepte	Kurzbeschreibung
Observations on the Role Life-Cycle in the Context of Enterprise Security Management (Kern et al. 2002)	◑	●	○	Vorgehensmodell zur Einführung einer unternehmensweiten Autorisierungslösung auf der Basis von systemübergreifenden Rollen
Process-Oriented Approach for Role-Finding to Implement Role-Based Security Administration in a Large Industrial Organization (Roeckle et al. 2000)	◑	●	○	Ansatz zur Ableitung von systemübergreifenden Rollen
PROMET PSI: Methode zur Prozess und Systemintegration (IMG 1996)	○	◑	○	Methodisches Vorgehen für die Implementierung von Prozessen mittels Workflow-Systemen
Prozessbasierte Gestaltung von (Aufbau-) Organisation und Berechtigungskonzept am Beispiel SAP R/3 (Vieting/Kumpf 2002)	○	○	●	Ansatz zur Einführung von SAP-Berechtigungskonzepten
Role Mining – Revealing Business Roles for Security Administration using Data Mining Technology (Kuhlmann et al. 2003)	○	●	○	Ableitung von systemübergreifenden Rollen mittels Data-Mining-Technologien
SAP Berechtigungswesen (Hartje et al. 2003)	○	○	●	Ansatz zur Einführung von SAP-Berechtigungskonzepten

Legende: ● Intensiv behandelt ◑ Teilweise behandelt ○ Nicht bzw. rudimentär behandelt

Tabelle 2: Übersicht der analysierten Ansätze

Die berücksichtigten Ansätze sind in Tabelle 2 nach ihrem inhaltlichen Schwerpunkt positioniert. Ausgewählt wurden Arbeiten, die sich wenigstens einem der beiden Arbeitsschwerpunkte „Architektur“ und „Integration“ (bzw. „Systemübergreifende Berechtigungskonzepte“) im Kontext der Autorisierung widmen. Bei der Auswahl der Ansätze wurden zudem Beiträge berücksichtigt, die sich intensiv mit systemspezifischen Berechtigungskonzepten auseinandersetzen, da sich die dort entwickelten Vorgehensweisen ggf. auch auf die Entwicklung systemübergreifender Berechtigungskonzepte übertragen lassen. Im folgenden Abschnitt werden die einzelnen Ansätze zunächst vorgestellt und dann abschliessend bewertet.

3.2 Diskussion der relevanten Ansätze

Die Diskussion der Ansätze erfolgt unter Berücksichtigung der Aspekte Fokus, Methodenelemente, Metamodell und Vorgehensmodell. Abschliessend werden die Ansätze im Hinblick auf die Arbeit beurteilt.

3.2.1 Observations on the Role Life-Cycle (Kern et al. 2002)

Fokus: Der Beitrag von KERN ET AL. präsentiert das ERBAC-Model für die systemübergreifende, unternehmensweite Autorisierung.[192] Darüber hinaus diskutiert er ein Vorgehensmodell zur Einführung einer unternehmensweiten Autorisierung auf der Basis von systemübergreifenden Rollen. Im Besonderen wird dabei auf die Analyse, das Design, das Management und die Wartung von systemübergreifenden Rollen eingegangen.

Methodenelemente: Im Rahmen der Ausführungen präsentieren KERN ET AL. neben einem Metamodell für die unternehmensweite, systemübergreifende Autorisierung auch ein Vorgehensmodell für die Implementierung der unternehmensweiten, rollenbasierten Autorisierung. Aufgrund der Kürze des Beitrags (8 Seiten) werden die wesentlichen Aktivitäten des Vorgehensmodells lediglich kurz beschrieben. Auf einzelne Techniken oder Ergebnisdokumente wird dabei nicht eingegangen. Ein Rollenmodell ist ebenfalls nicht in den Ausführungen enthalten.

Metamodell: Im Rahmen der Arbeit wird das bereits in Kapitel 2.3.3 vorgestellte ERBAC-Modell (vgl. Abbildung 11) entwickelt, welches daher im Folgenden nur kurz beschrieben wird. Im systemübergreifenden Autorisierungswerkzeug (Enterprise Access Management Werkzeug – EAM) werden die Berechtigungen der Nutzer über die einzelnen Systeme hinweg administriert. Enterprise-Rollen fassen Berechtigungen systemübergreifend zusammen. Den Berechtigungen sind wiederum systemspezifische Gruppen und Rollen zugeordnet, die Zugriff auf systemspezifische Ressourcen ermöglichen. Die systemspezifischen Benutzerkonten sowie die Zuordnungen von systemspezifischen Benutzerkonten zu Gruppen werden vom

[192] Vgl. Kapitel 2.3.3.

EAM-Werkzeug aufgrund der Beziehungen zwischen den Nutzern, Enterprise-Rollen und Gruppen angelegt.

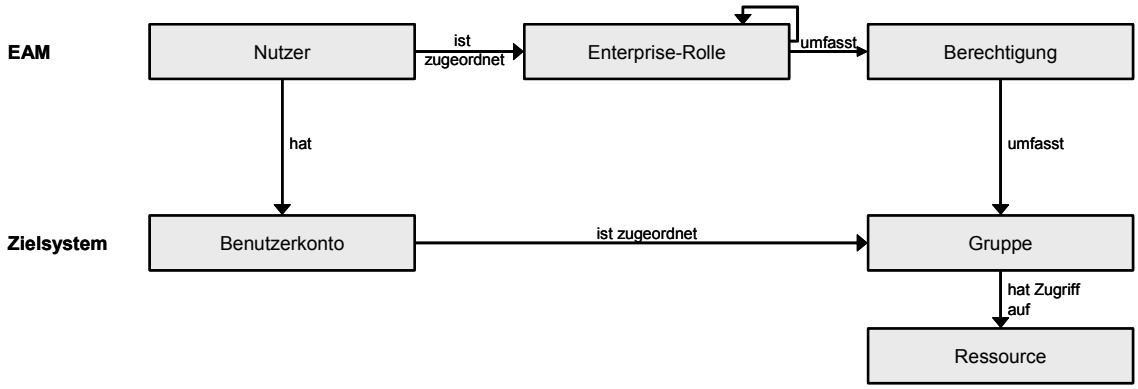

Abbildung 11: Metamodell Observations on the Role Life-Cycle (ERBAC-Modell)[193]

Vorgehensmodell: Das Vorgehensmodell (vgl. Abbildung 12) ist in vier Phasen unterteilt. In der ersten Phase werden als Aktivitäten die Einführung des EAM-Werkzeugs, die Konsolidierung von Nutzern, Gruppen, Sicherheitsrichtlinien und Zugriffsrechten sowie die Rollenanalyse angeführt. Die Rollenanalyse identifiziert dabei mögliche Enterprise-Rollen. KERN ET AL. empfehlen eine gemischte „Top-Down"- und „Bottom-Up"-Vorgehensweise als Methodik. Somit werden die Rollen teilweise ausgehend von bereits existierenden Systemrollen, teilweise ausgehend von prozessualen Elementen wie z.B. Stellen abgeleitet. Im Rahmen der nächsten Phase erfolgt die Aufbereitung der Rollen, so dass diese später im EAM-Werkzeug implementiert werden können. Um eine weitgehend automatisierte Administration zu realisieren, wird das EAM-Werkzeug an das Informationssystem angeschlossen, das als Werkzeug zum Anlegen neuer und zur Modifikation bestehender Nutzer verwendet wird (typischerweise das HR-System). In der dritten Phase des Vorgehensmodells erfolgen die Produktivsetzung der rollenbasierten Autorisierung und die Einführung weiterer Administrationswerkzeuge, wie z.B. Passwortsynchronisierungs- oder Administrationsworkflowwerkzeuge. Innerhalb der letzten Phase werden ein Berechtigungsberichtswesen für interne und externe Anspruchsgruppen etabliert sowie die Change-Management-Prozesse implementiert. Teil des Change-Management-Prozesses sind das Rollenmanagement und die Rollenwartung. Im Rahmen des Rollenmangements werden geringfügige Änderungen wie z.B. das Entfernen oder die Neueinführung von Nutzern und Rollen durchgeführt. Umfangreichere Überarbeitungen von ganzen Teilen des Rollenkonzepts werden im Rahmen der Rollenwartung umgesetzt.

193 Vgl. Kern et al. 2002, S. 46 sowie Kapitel 2.3.3.

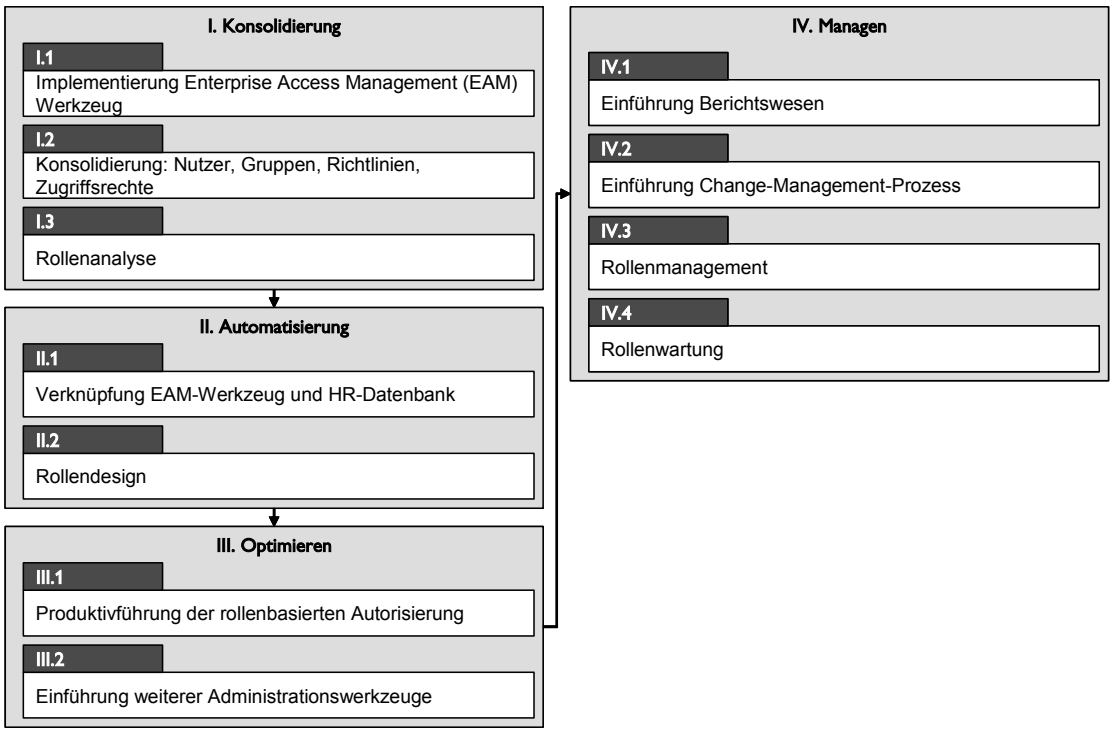

Abbildung 12: Vorgehensmodell Observations on the Role Life-Cycle[194]

Bewertung: Im Hinblick auf die Dissertation ist insbesondere das ERBAC-Modell von Bedeutung. Dieses Modell gilt es im zu entwickelnden Metamodell der Arbeit zu berücksichtigen. Darüber hinaus gibt das Vorgehensmodell eine gute Übersicht über die Einführung eines EAM-Werkzeugs zur systemübergreifenden Autorisierung. Die Ausführungen sind jedoch sehr knapp gehalten.

3.2.2 Process-Oriented Approach for Role-Finding (Roeckle et al. 2000)

Fokus: Der Beitrag von ROECKLE ET AL. beschreibt einen Ansatz zur Ableitung von Rollen u.a. anhand einer Fallstudie, die die Anwendung der entwickelten Methodik bei Siemens ICN schildert. Ausgangspunkt der Arbeiten ist dabei die Prozessebene mit den Tätigkeiten, die die Mitarbeiter im Rahmen ihrer Arbeit ausführen. Der Fokus der Ausführungen liegt auf der Identifikation systemübergreifender Rollen. Im Mittelpunkt stehen dabei ein Metamodell zur Autorisierung und ein Vorgehensmodell, das den Rollenableitungsprozess beschreibt.

Methodenelemente: Das Vorgehensmodell zur Ableitung der Rollen[195] besteht aus sieben Schritten, die nicht weiter gruppiert oder untergliedert sind (Abbildung 14 gliedert das Vorgehensmodell aus Gründen der Übersichtlichkeit nach den Ebenen des präsentierten Metamodells). Ergebnisdokumente werden im Rahmen der Ausführungen nicht präsentiert. Jedoch liegt ein Rollenmodell für die Autorisierung vor, das die wesentlichen Aufgabenträger der Sicherheitsadministration und ihre Aufgaben aufzeigt.

194 Vgl. Kern et al. 2002, S. 46.

195 Das Vorgehensmodell wird in Roeckle et al. 2000 nur kurz beschrieben. Ausführlichere Informationen inkl. einer grafischen Abbildung des Vorgehens finden sich in Roeckle 1999.

Metamodell: Das Metamodell des Ansatzes (vgl. Abbildung 13) umfasst folgende Ebenen:

- Prozessebene: Die Prozessebene erlaubt die Auseinandersetzung mit der organisatorischen Perspektive der Rechtevergabe. Die zentrale Entität auf Prozessebene ist die „Tätigkeit". Unter dieser Entität werden die EDV-unterstützten Tätigkeiten subsumiert. Die Tätigkeiten können beliebig ineinander verschachtelt und ggf. zu „Arbeitsplätzen" zusammengefasst werden. Merkmalsausprägungen erlauben die Parametrisierung von Tätigkeiten. So können für eine Tätigkeit beispielsweise Bearbeitungslimits oder bestimmte Kundengruppen festgelegt werden.

- Rollenebene: Die Rollenebene umfasst die Entitäten, die typischerweise von systemübergreifenden Autorisierungswerkzeugen implementiert werden. Dabei repräsentieren die Entitäten Teilrolle bzw. Rolle die Entitäten Tätigkeit bzw. Arbeitsplatz der Prozessebene. Einem Berechtigungsbündel werden die Zugriffsrechte zugewiesen, die notwendig sind, um eine Tätigkeit durchzuführen. Rollen und Teilrollen sind dabei systemübergreifend.

- Zugriffskontrollebene: Die Zugriffskontrollebene enthält die Entitäten, die typischerweise die Werkzeuge implementieren, die die eigentliche Zugriffskontrolle durchführen. Die Entität „Ressourcengruppe" repräsentiert die Daten und Funktionen, auf die ein Zugriff erfolgen kann. Durch die Zuordnung von Ressourcengruppen zu Benutzergruppen können die Mitglieder der entsprechenden Gruppe auf die zugeordneten Ressourcen zugreifen. Die Verbindung zwischen Rollen- und Zugriffskontrollebene wird zum einen durch die Zuordnung von Benutzergruppen zu Rollen und Teilrollen erzielt. Zum anderen werden die Berechtigungsbündel auf die Ressourcengruppen abgebildet.

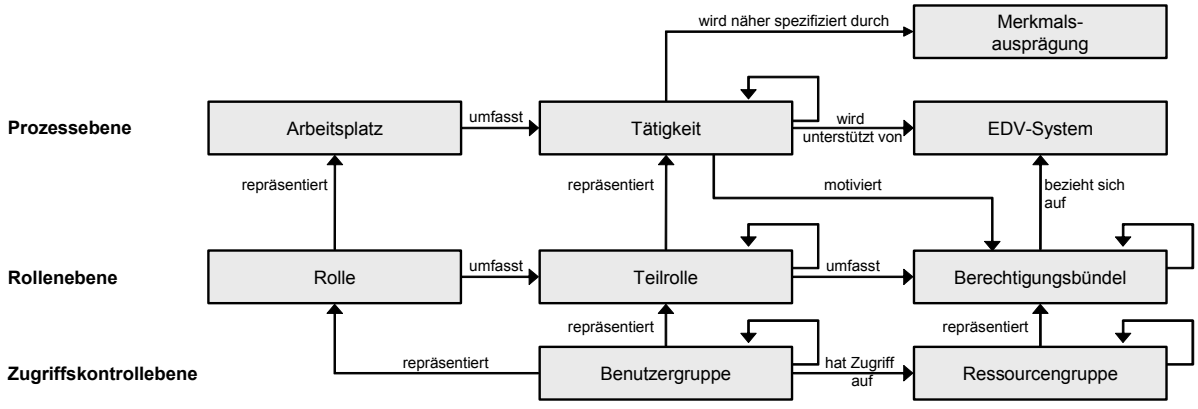

Abbildung 13: Metamodell Process-Oriented Approach for Role-Finding[196]

Vorgehensmodell: Das Vorgehensmodell zur Ableitung von Rollen (vgl. Abbildung 14) legt in einem ersten Schritt die für die Rollenableitung verantwortliche Unternehmenseinheit fest. Die anschliessenden vier Schritte beschäftigen sich mit der Rollenbildung auf Prozessebene. Nachdem die EDV-unterstützten Tätigkeiten mit den entsprechenden Merkmalsausprägungen

196 Vgl. Roeckle et al. 2000, S. 107.

identifiziert wurden, erfolgt die Zusammenfassung der Tätigkeiten zu Arbeitsplätzen. Die Ableitung der Rollenebene ergibt sich, indem für jeden Arbeitsplatz und jede Tätigkeit eine Rolle bzw. Teilrolle definiert wird. Die Berechtigungsbündel, die die Teilrollen mit den entsprechenden Berechtigungen versehen, werden anschliessend von Systemadministratoren mit Zugriffsrechten ausgestattet.

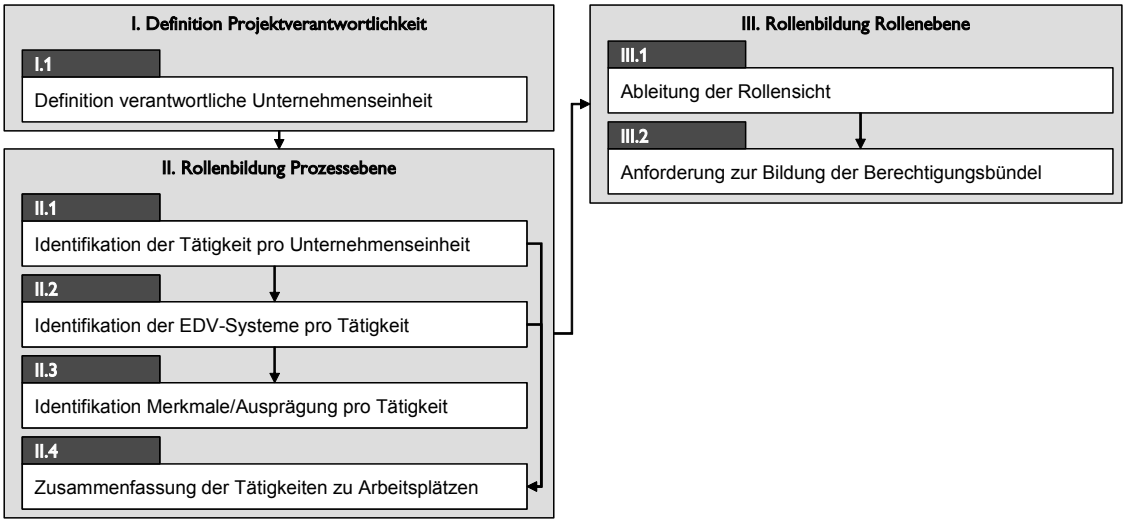

Abbildung 14: Vorgehensmodell Process-Oriented Approach for Role-Finding

Das grafisch abgebildete Vorgehensmodell[197] endet mit der Ableitung der Rollenebene, die schriftlichen Ausführungen gehen jedoch darüber hinaus. Die Verknüpfung der Rollen- mit der Zugriffskontrollebene wird, wie bereits beschrieben, zum einen durch die Zuordnung von Benutzergruppen zu Rollen und Teilrollen erzielt. Zum anderen werden die Berechtigungsbündel auf die Ressourcengruppen abgebildet.

Bewertung: Die Stärken des Ansatzes im Hinblick auf die Arbeit liegen in der Präsentation eines Vorgehensmodells, das insbesondere auch die Ableitung systemübergreifender Rollen thematisiert. Darüber hinaus wird ein Metamodell präsentiert, das wesentliche Gestaltungselemente im Umfeld der unternehmensweiten Autorisierung zusammenhängend aufzeigt. Ebenfalls präsentiert wird ein Rollenmodell für die Administration der Berechtigungen. Als Schwäche der diskutierten Ausführungen ist insbesondere der geringe Umfang der öffentlich verfügbaren Dokumentation zu nennen. Ein Erschliessen des Inhalts ist teilweise nur durch ein bereits vorhandenes, tief greifendes Verständnis der Thematik möglich. Handbücher, die primär als vertiefende Materialien referenziert werden, sind öffentlich nicht verfügbar.

3.2.3 PROMET PSI (IMG 1996)

Fokus: Die Methode PROMET PSI (Prozess- und Systemintegration) beschreibt ein methodisches Vorgehen für die Implementierung von Prozessen mittels Workflow-Systemen. Die Me-

197 Das Vorgehensmodell wird in Roeckle et al. 2000 nur kurz beschrieben. Ausführlichere Informationen inkl. einer grafischen Abbildung des Vorgehens finden sich in Roeckle 1999.

thode ist unabhängig von einem spezifischen Workflow-System und baut in Teilen auf weiteren Methoden wie z.B. PROMET BPR[198] auf. Im Rahmen der Arbeit wird auch das Thema Autorisierung behandelt: Die Technik „Workflowplanung“ bringt unter anderem das Entwurfsergebnis „Berechtigungskonzept“ hervor. Die folgenden Ausführungen beziehen sich daher im Wesentlichen auf diesen Teilbereich der Arbeit.

Methodenelemente: Das Vorgehensmodell der Methode PROMET PSI besteht aus insgesamt vier Phasen, denen jeweils Ergebnisse zugeordnet sind. Die Ergebniserstellung wird mittels Techniken, die jeweils weiter in Schritte untergliedert sind, beschrieben. Die Autorisierung wird lediglich in einer Technik angesprochen. Die Methode umfasst die drei Metamodelle „Ablaufsteuerung“, „Berechtigungskonzept“ und „Desktop Integration“, von denen für die Autorisierung das Metamodell „Berechtigungskonzept“ relevant ist. Die wesentlichen Begriffe des Metamodells sind im Rahmen der Ausführungen zum Modell und im Glossar definiert.

Metamodell: Im Rahmen der Arbeit wird ein Metamodell „Berechtigungskonzept“ entwickelt:

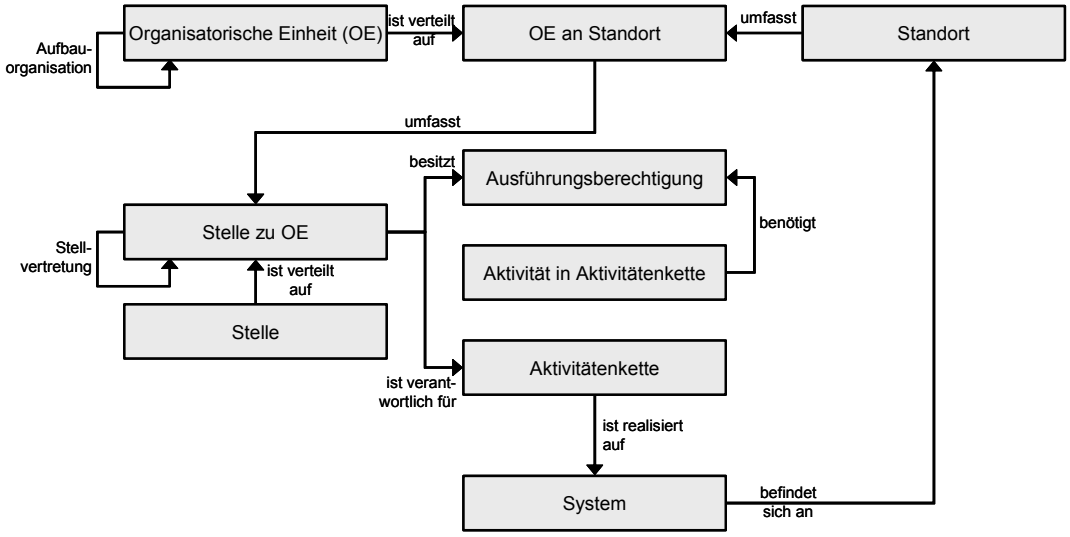

Abbildung 15: Metamodell Berechtigungskonzept PROMET PSI[199]

Die einzelnen Elemente sind wie folgt definiert:

- Organisatorische Einheit, Standort und Stelle: Ausgangspunkt für das Berechtigungskonzept von PROMET PSI bilden die organisatorischen Einheiten, die auf unterschiedliche Standorte verteilt sind. Je Standort sind den organisatorischen Einheiten Stellen[200] zugewiesen.

- Aktivitätenkette, Ausführungsberechtigung und System: Eine Stelle, die einer organisatorischen Einheit zugeordnet ist, besitzt Ausführungsberechtigungen für die Ausführung ei-

198 Vgl. IMG 1997.
199 Vgl. IMG 2001, S. 254.
200 Eine Stelle bildet die kleinste aufbauorganisatorische Einheit. Sie entsteht durch die dauerhafte Zuordnung von Aufgaben auf eine oder mehrere Personen (vgl. Schulte-Zurhausen 1999, S. 141).

ner oder mehrerer Aktivitäten einer Aktivitätenkette, welche auf einem oder mehreren Systemen abläuft. Eine Aktivitätenkette umfasst eine Menge von Aktivitäten, für deren Ablaufsteuerung das Workflow-System verantwortlich ist.

Vorgehensmodell: Die Implementierung von Prozessen mittels Workflow-System wird in PROMET PSI innerhalb der vier Phasen „Voruntersuchung", „Konzeption", „Realisierung" und „Einführung" erzielt:

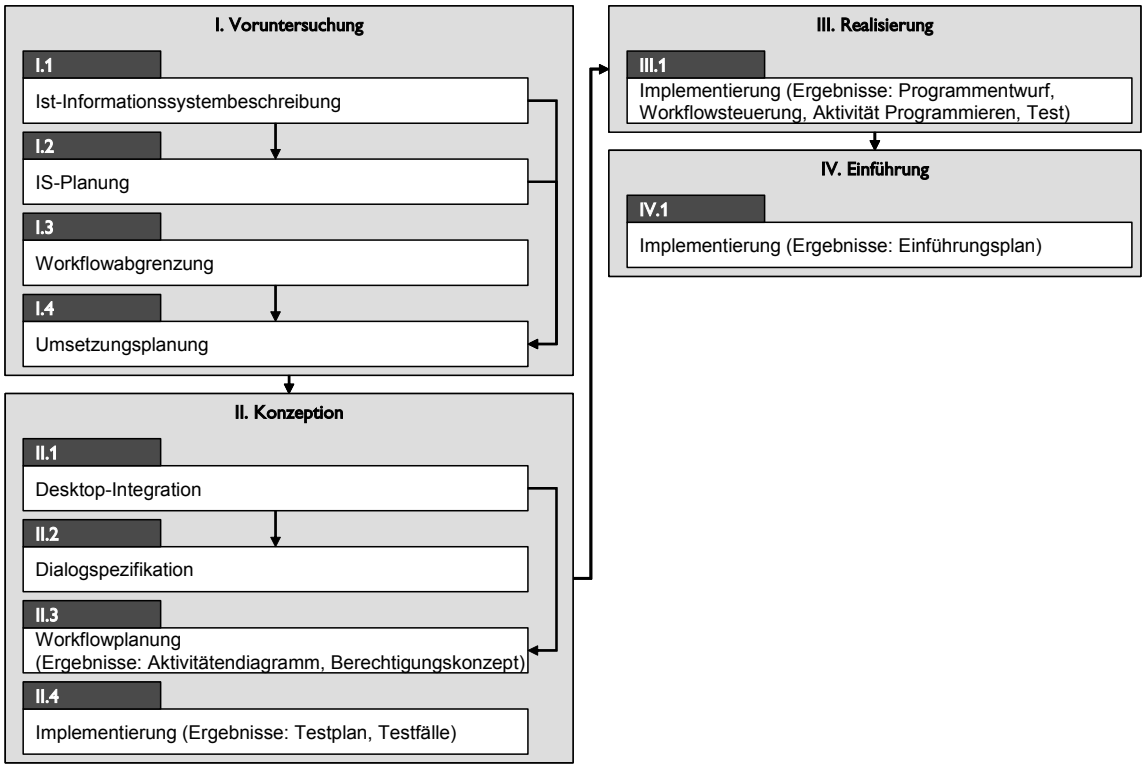

Abbildung 16: Überblick Vorgehensmodell PROMET PSI[201]

Im Rahmen der Konzeption erstellt die Technik „Workflowplanung" im Schritt „Verantwortliche Stellen identifizieren" als zentrales Ergebnis das Berechtigungskonzept. Ausgangspunkt der Erstellung des Berechtigungskonzepts sind Informationen über die Aufbauorganisation, insbesondere Stellenbeschreibungen und Organigramme. Aus diesen lassen sich elementare Informationen zur Ableitung des Berechtigungssystems gewinnen: Informationen darüber, welche Stelle an welchem Standort existiert, welche Stelle welcher Organisationseinheit zugeordnet ist und welche Organisationseinheit an welchem Standort vertreten ist. In einer zentralen Matrix werden dann die einzelnen Rechte vergeben. Dabei wird für jeden Workflow festgelegt, welche Stelle welche Rechte bezüglich welcher Workflowaktivität innehat. Die Spezifikation der Berechtigungen erfolgt auf einer sehr grobgranularen Ebene.

Bewertung: Die Stärken von PROMET PSI im Hinblick auf diese Arbeit liegen vor allen Dingen in der Bereitstellung des Metamodells „Berechtigungskonzept". Das Metamodell

201 Eine direkte Zuordnung von Techniken zu Aktivitäten oder Phasen nimmt PROMET PSI nicht vor. Das dargestellte Vorgehensmodell ordnet den Phasen die jeweiligen Techniken auf der Basis der Ausführungen von IMG 2001, Kapitel 2 zu.

zeigt die wesentlichen Entitäten im Bereich Organisation auf, an die ein Berechtigungskonzept anknüpfen muss. Die Schwächen der Arbeit liegen bei dem geringen Detaillierungsgrad der Beschreibungen im Bereich Autorisierung. Lediglich drei der ca. 300 Seiten beinhalten detaillierte methodische Ausführungen zum Thema Autorisierung. Darüber hinaus spielt die rollenbasierte Autorisierung keine Rolle. Auch die systemübergreifenden Aspekte der Autorisierung werden nur sehr eingeschränkt dargestellt.

3.2.4 Gestaltung eines SAP Berechtigungskonzepts (Vieting/Kumpf 2002)

Fokus: Der Beitrag von VIETING/KUMPF beschäftigt sich mit der Überführung SAP R/3-unterstützter Geschäftsprozesse in die Linienorganisation. Der Schwerpunkt liegt dabei auf der Entwicklung eines entsprechenden Berechtigungskonzepts. Der Beitrag präsentiert ein Vorgehensmodell, das wesentliche Schritte bei der Erstellung und Überführung eines SAP-Berechtigungskonzepts umfasst. Der Ansatz setzt voraus, dass bereits ein Geschäftsprozessmodell vorliegt. Dieses muss einen solchen Detaillierungsgrad aufweisen, dass sich den Prozessschritten die notwendigen SAP-Transaktionen eindeutig zuordnen lassen.

Methodenelemente: Neben dem Vorgehensmodell wird ein einzelnes Ergebnisdokument präsentiert. Dieses zeigt auf, wie eine Spezifikation der Berechtigungen für einen Prozess erfolgen kann. Ein Rollenmodell wie auch ein Metamodell werden nicht diskutiert.

Metamodell: Der Ansatz baut auf den Berechtigungselementen von SAP R/3 auf. Die SAP R/3 Version, auf die sich die Ausführungen beziehen, entspricht mit ihrem Berechtigungskonzept jedoch nicht mehr den aktuellen SAP R/3-Versionen (Version 4.6). Ergänzt werden die wesentlichen Gestaltungselemente um organisatorisch, prozessuale Elemente. Im Rahmen der Ausführungen wird kein Metamodell präsentiert. Aufgrund der Erläuterungen[202] kann jedoch in Anlehnung an KUHLMANN ET AL.[203]ein Modell erstellt werden, das die wesentlichen Gestaltungselemente zueinander in Bezug setzt (vgl. Abbildung 17). Die Elemente dieses Metamodells können wie folgt beschrieben werden:

- Prozess, Aufgabenbündel: Ein Prozess des Prozessmodells kann in mehrere Aufgabenbündel zerlegt werden. Aufgabenbündel umfassen eine Menge von zeitlich-logischen Prozessschritten, deren weitere Unterteilung nicht sinnvoll oder nicht gewünscht ist.

- Mitarbeiter, Mitarbeitertyp: Die einzelnen Mitarbeiter werden Mitarbeitertypen zugeordnet. Der Begriff Mitarbeitertyp wird von VIETING/KUMPF synonym zum organisatorischen Begriff Stelle verwendet. Die Mitarbeitertypen sind standortspezifisch definiert. So existieren beispielsweise die Mitarbeitertypen „Lagerist Standort A“ und „Lagerist Standort B“. Den Mitarbeitertypen werden entsprechende Aufgabenbündel zugeordnet.

---

202 Vgl. insbesondere Vieting/Kumpf 2002, S. 412-417.
203 Vgl. Kuhlmann et al. 2003, S. 182f.

- R/3 Benutzer, Sammelaktivitätsgruppe, Aktivitätsgruppe, Transaktion: Auf technischer R/3-Ebene ist dem Mitarbeiter ein R/3-Benutzer zugeordnet, dem Mitarbeitertyp eine Sammelaktivitätsgruppe und dem Aufgabenbündel die Aktivitätsgruppe. Unterschieden werden dabei generische und funktionale Aktivitätsgruppen. Generische Aktivitätsgruppen repräsentieren im Gegensatz zu funktionalen Aktivitätsgruppen Aufgabenbündel, die nicht an spezifische organisatorische oder funktionale Aspekte angepasst sind. So legt beispielsweise die generische Aktivitätsgruppe „Auftrag erfassen“ nicht fest, für welchen Standort Aufträge erfasst werden können oder welche Auftragsarten abgewickelt werden können. Die Aktivitätsgruppen beinhalten SAP-Transaktionen, die von organisatorischer Seite bereits von den Aufgabenbündeln referenziert werden.

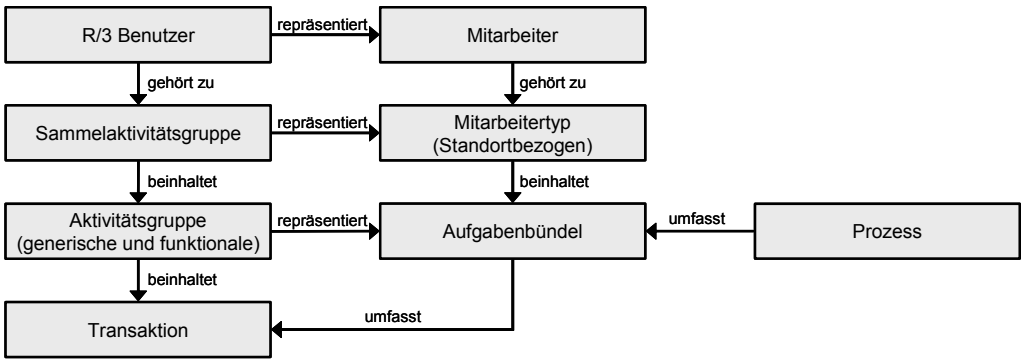

Abbildung 17: Metamodell Gestaltung Berechtigungskonzept am Beispiel SAP

Vorgehensmodell: Abbildung 18 zeigt das diskutierte Vorgehensmodell.[204] Bevor die eigentliche Entwicklung des Berechtigungskonzepts beginnt, erfolgt die Identifikation von Aufgabenbündeln und die Zuordnung der Aufgabenbündel zu Mitarbeitertypen. Diese Schritte werden ausgeführt, wenn sich das zu entwickelnde Berechtigungskonzept über mehrere Organisationseinheiten erstreckt. Anschliessend werden die den Aufgabenbündeln entsprechenden Aktivitätsgruppen in SAP definiert. Sammelaktivitätsgruppen werden in einem nächsten Schritt für die jeweiligen Mitarbeitertypen angelegt. Dabei werden den Sammelaktivitätsgruppen die notwendigen Aktivitätsgruppen zugewiesen. Nachdem die Entwicklung des Berechtigungskonzepts abgeschlossen ist, erfolgt der Übergang in die Produktion. Das Berechtigungssystem muss getestet und anschliessend mit allen Nutzern und Berechtigungen befüllt werden.

[204] Zu beachten ist, dass der Ansatz keine grafische Präsentation des Vorgehensmodells vornimmt und aus der Analyse des Textes nicht eindeutig hervorgeht, welche Aktivitäten in welcher Reihenfolge ausgeführt werden müssen.

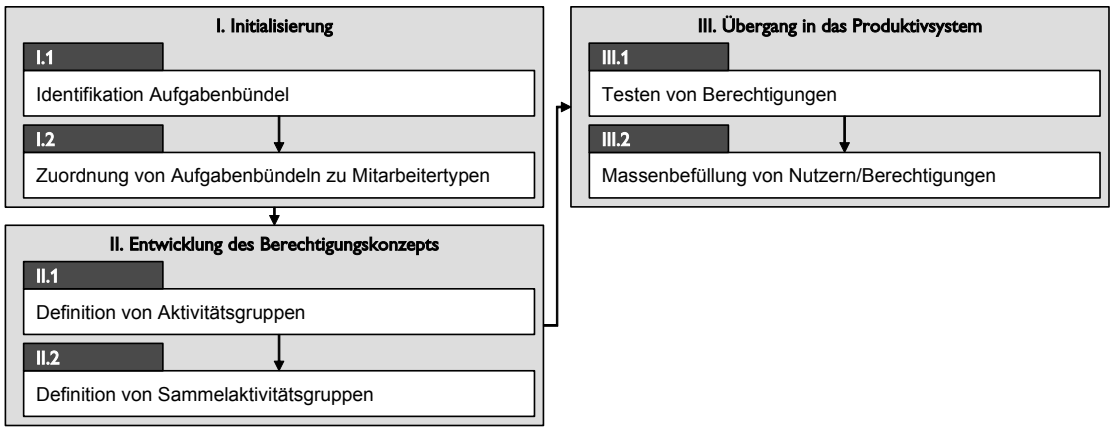

Abbildung 18: Vorgehensmodell Gestaltung Berechtigungskonzept am Beispiel SAP

Bewertung: Die Stärken des Ansatzes im Hinblick auf diese Arbeit liegen insbesondere in der Methodik zur Ableitung von Berechtigungen auf der Basis eines vorliegenden Prozessmodells. Als nachteilig für die Dissertation erweist sich die Konzentration des Ansatzes auf die Software SAP R/3. Die methodischen Schwächen sind das fehlende Meta- und Rollenmodell. Inhaltliche Schwächen liegen in dem zum Teil intransparenten Vorgehensmodell.

3.2.5 Role Mining (Kuhlmann et al. 2003)

Fokus: Der Ansatz von KUHLMANN ET AL. untersucht die Ableitung von systemübergreifenden Rollen mittels Data-Mining-Technologien. Im Gegensatz zu anderen methodischen Ansätzen werden die systemübergreifenden Rollen jedoch nicht „Top-Down“, also ausgehend von der organisatorisch prozessualen Sichtweise, abgeleitet, sondern „Bottom-Up“. Somit werden die systemspezifischen Rollen und Gruppen mit Hilfe analytischer Verfahren semiautomatisch zu systemübergreifenden Rollen zusammengefasst.

Methodenelemente: Im Rahmen der Ausführungen präsentieren KUHLMANN/SCHIMPF ein einfaches Metamodell, das die wesentlichen Gestaltungselemente aufzeigt. Das diskutierte Vorgehensmodell zur Ableitung der systemübergreifenden Rollen umfasst sieben Schritte. Ergebnisdokumente werden nicht vorgestellt. Ein Rollenmodell liegt ebenfalls nicht vor.

Metamodell: Der Ansatz unterscheidet die beiden Gestaltungsebenen „Globale Ebene“ und „Zielsystemebene“(vgl. Abbildung 19).

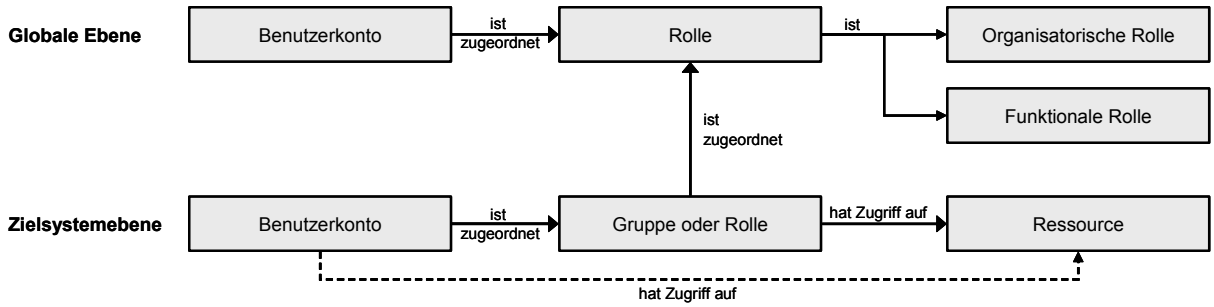

Abbildung 19: Metamodell Role Mining[205]

Die beiden Ebenen sind wie folgt definiert:

- Globale Ebene: Die globale Ebene umfasst die zur systemübergreifenden Berechtigung notwendigen Entitäten. Die zentrale Entität dieser Ebene ist die „Rolle". Eine Rolle auf dieser Ebene ist entweder eine organisatorische oder eine funktionale Rolle. Jedem Nutzer ist genau eine organisatorische Rolle zugeordnet. Dieser Rolle sind alle Berechtigungen zugeordnet, die der Nutzer für die Ausführung der Tätigkeiten braucht, die er aufgrund seiner Stellung im Unternehmen durchführt. Sollte ein Nutzer zusätzliche Rechte z.B. aufgrund von Projektmitgliedschaften brauchen, so werden hierfür funktionale Rollen verwendet.

- Zielsystemebene: Die Zielsystemebene beinhaltet die Entitäten der Systeme, die die eigentliche Autorisierung durchführen. Diese Systeme verwenden typischerweise Gruppen oder Rollen, um Berechtigungen nicht einzeln an Nutzer zu vergeben. Teilweise erfolgt auch die direkte Vergabe von Berechtigungen an Nutzer. Die beiden Ebenen werden im Rahmen des Ansatzes durch die Zuweisung von systemspezifischen Gruppen und Rollen zu systemübergreifenden Rollen miteinander verknüpft.

Vorgehensmodell: Das Vorgehensmodell von KUHLMANN/SCHIMPF kann in drei Phasen geteilt werden (vgl. Abbildung 20). Noch vor der eigentlichen Ableitung der Rollen findet die Zusammenstellung und Aufbereitung der notwendigen Informationen statt. Nachdem erste Erfahrungen mit den gesammelten Daten gemacht wurden (Schritt „Exploration und Lernen"), erfolgt die eigentliche Ableitung der Rollen beginnend mit der Erstellung der organisatorischen Rollen. Eine Clusteranalyse erstellt auf der Basis nutzerspezifischer Informationen die organisatorischen Rollen. Zu den grundlegenden Informationen gehören dabei systemspezifische Informationen wie z.B. das benutzereigene Netzlaufwerk des eingesetzten Betriebssystems und systemübergreifende Informationen wie z.B. die Sprache des Nutzers. Dann wird eine Assoziationsanalyse verwendet, um den systemübergreifenden Rollen systemspezifische Gruppen und Rollen zuzuordnen. Die genaue Vorgehensweise der Ableitung wird nicht geschildert. Beispielsweise bleibt unklar, in welcher Weise die funktionalen Rollen gebildet werden. In einer letzten Phase werden die ermittelten Rollen auf ihre Plausibilität hin analysiert und implementiert. Abschliessend werden den ermittelten

[205] Das Modell basiert auf den Ausführungen in Kuhlmann et al. 2003, S. 182f.

siert und implementiert. Abschliessend werden den ermittelten Rollen die entsprechenden Benutzerkonten zugewiesen.

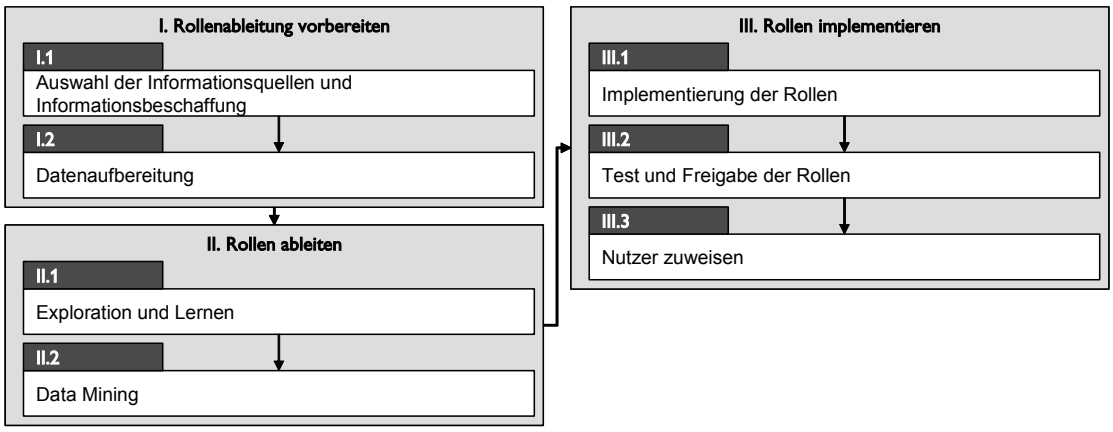

Abbildung 20: Vorgehensmodell Role Mining[206]

Bewertung: Die Stärken des Ansatzes im Hinblick auf die Dissertation liegen insbesondere im beschriebenen „Bottom-Up"-Vorgehen zur Ermittlung der systemübergreifenden Rollen. Im Gegensatz zum „Top-Down"-Vorgehen ist die vorgeschlagene Methodik ein pragmatischer Ansatz, der schnell und kosteneffizient zu einem Ergebnis führt. Leider sind die Ausführungen sehr kurz gehalten, so dass das beschriebene Vorgehen nicht immer vollständig nachvollzogen werden kann.

3.2.6 SAP Berechtigungswesen (Hartje et al. 2003)

Fokus: HARTJE ET AL. stellen ein Vorgehensmodell zur Entwicklung und Einführung eines SAP-Berechtigungskonzepts vor. Dabei erläutern die Autoren zu Beginn die grundlegenden Autorisierungsfunktionalitäten und -konzepte von SAP R/3. Im weiteren Verlauf des Buches gehen sie darauf ein, wie die Rollen und Berechtigungen im Rahmen eines SAP-Customizing-Projektes abgeleitet werden können. Darüber hinaus stellen sie Administrationskonzepte vor, die wesentliche Aufgabenträger und deren Aufgaben beschreiben.

Methodenelemente: Das präsentierte Vorgehensmodell besteht aus zwölf Phasen, die nicht weiter gruppiert oder explizit in Aktivitäten und Schritte heruntergebrochen sind. Die textuellen Ausführungen zu den einzelnen Phasen enthalten auch beispielhafte Ergebnisdokumente. Für die einzelnen Aktivitäten sind Rollenmodelle vorhanden. Metamodelle werden der Arbeit nicht explizit zugrunde gelegt. Es existieren jedoch Grafiken, die für Teilbereiche der Arbeit wesentliche Gestaltungselemente aufzeigen.

Metamodell: Der Ansatz basiert auf dem Rollenkonzept von SAP R/3. Abbildung 21 zeigt die wesentlichen Gestaltungselemente auf:

206 Das Modell basiert auf den Ausführungen Kuhlmann et al. 2003, S. 183f.

- R/3 Benutzer, Sammelrolle, Rolle, Transaktion und Berechtigungsobjekt: Ein R/3 Benutzer ist Mitglied einer oder mehrerer Sammelrollen, die wiederum Rollen umfassen. Den Rollen sind letztendlich Transaktionen zugeordnet. SAP realisiert somit ein zweistufiges Berechtigungskonzept. Berechtigungsobjekte sind die technischen Konstrukte von SAP, über die die eigentliche Vergabe der Berechtigungen erfolgt.

- Mitarbeiter, Funktion, Aufgabe und Tätigkeit: Während Benutzer, Sammelrolle, Rolle und Transaktion die technische Systemelemente sind, stellen Mitarbeiter, Funktion, Aufgabe und Tätigkeit die organisatorische Sichtweise des Berechtigungswesens dar.

- Gesetzliche Anforderung, „Best Practice“ und Kritische Kombinationen: Um gesetzlichen Anforderungen und „Best Practices“ zu genügen, werden kritische Berechtigungskombinationen ermittelt, die nicht in einer Sammelrolle oder Rolle kombiniert auftreten dürfen.

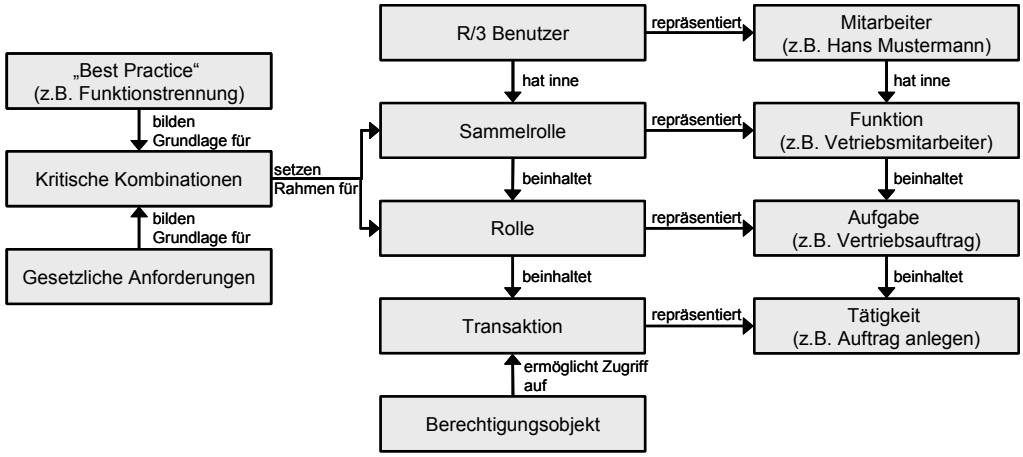

Abbildung 21: Metamodell SAP Berechtigungswesen[207]

Vorgehensmodell: Das Vorgehensmodell (Abbildung 22 zeigt das Vorgehensmodell untergliedert in Phasen) definiert in der ersten Phase die Anforderungen und Rahmenbedingungen für die Entwicklung des entsprechenden SAP-Berechtigungskonzepts. Anschliessend erfolgt die Zuordnung von Rollen und Berechtigungen zu Nutzern. Die Zuordnung erfolgt in drei Schritten. Zuerst werden die „Funktionen“ definiert. Eine genaue Definition des Begriffes erfolgt im Rahmen der Ausführungen nicht. Im Wesentlichen erfolgt jedoch eine Gleichsetzung des Begriffs mit dem SAP-Gestaltungselement „Sammelrolle“. Nachdem die Sammelrollen bestimmt sind, erfolgt in einem zweiten Designschritt die Zuordnung von SAP-Transaktionen zu den bereits definierten Sammelrollen. Gleiche Zugriffsberechtigungen auf Transaktionen werden dabei zu Rollen gebündelt, so dass eine Sammelrolle eine oder mehrere Rollen enthält. Diese erlauben dann den Zugriff auf eine oder mehrere Transaktionen. Der letzte Designschritt erstellt das Berechtigungsfeinkonzept. Die bereits definierten Sammelrollen und Rollen sind bisher weitestgehend organisationsunabhängig und noch nicht detailliert spezifiziert, so dass nun die Ausdefinition der Rollen erfolgt. Die folgenden vier Schritte widmen

[207] Vgl. Hartje et al. 2003, S. 56.

sich der Umsetzung des entwickelten Designkonzepts in SAP R/3. Anschliessend erfolgt die Erstellung des Betreuungskonzepts. Neben den beiden von SAP entwickelten Administrationskonzepten werden zwei weitere Konzepte zur Administration der Berechtigungen vorgeschlagen. Die letzten drei Schritte widmen sich der Überführung des entwickelten Konzepts in den Live-Betrieb und dem eigentlichen Betrieb der entwickelten Lösung.

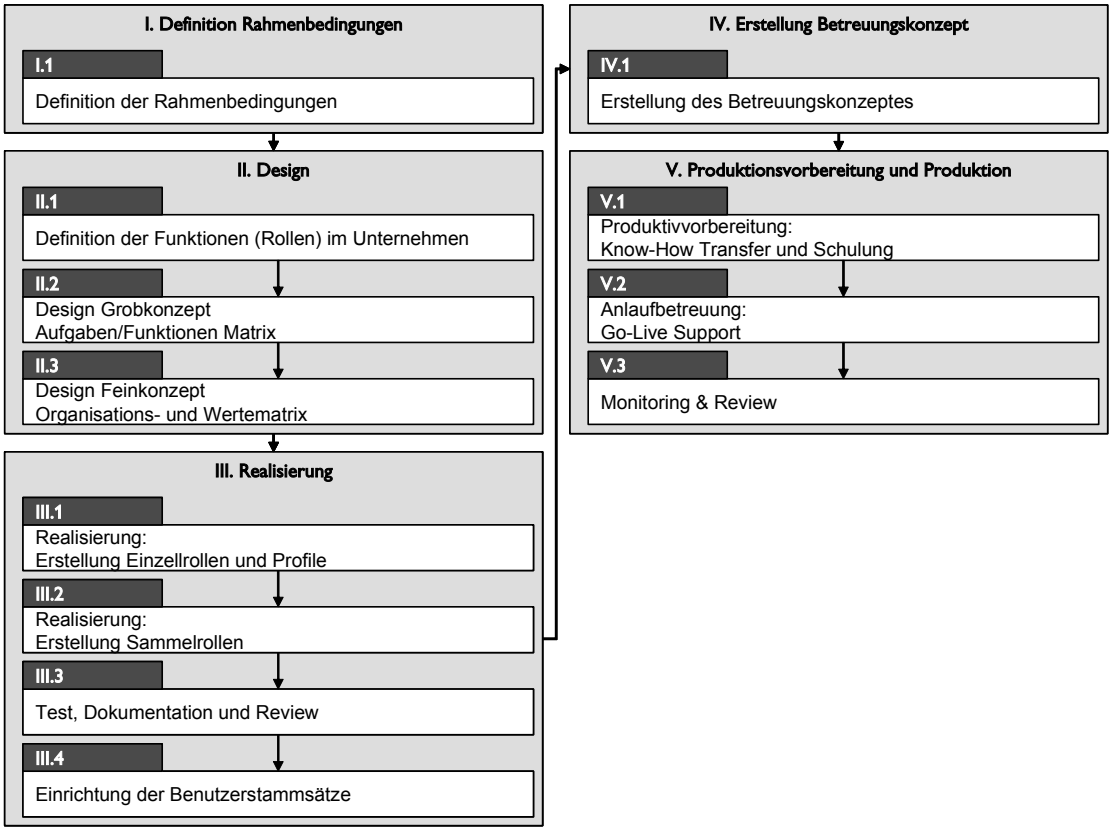

Abbildung 22: Vorgehensmodell SAP Berechtigungswesen[208]

Bewertung: Die Stärken des Ansatzes liegen in der detaillierten Ausarbeitung eines Vorgehensmodells zur Entwicklung eines Berechtigungskonzepts. Darüber hinaus wird auch ein Rollenmodell für die Administration der Berechtigungen vorgestellt. Die Schwächen dieses Ansatzes liegen – vor dem Hintergrund einer Verwendung innerhalb dieser Dissertation – vor allem in der Systemabhängigkeit des Vorgehensmodells: Der Ansatz konzentriert sich auf die Ableitung von Rollen und Rechten innerhalb eines Systems. Eine weitere Schwäche liegt in der eingeschränkten Untersuchung des Schutzbedarfes. Eine risikoorientierte Vorgehensweise nach dem Prinzip „soviel Schutz wie nötig“ wird nur in Ansätzen thematisiert. Darüber hinaus ist die Verständlichkeit wegen der Verwendung unzureichend definierter Begriffe teilweise erschwert. Hierzu trägt auch die eingeschränkte Verwendung von Metamodellen bei.

208 Vgl. Hartje et al. 2003, S. 138.

3.3 Beurteilung der relevanten Ansätze

Die Entwicklung einer neuen Methode ist nur dann sinnvoll, wenn keine Methode vorhanden ist oder existierende Methoden im Hinblick auf die gestellten Anforderungen unvollständig sind.[209] Im Folgenden werden daher die analysierten Ansätze anhand der in Kapitel 2.5 abgeleiteten Kriterien bewertet.

	Inhaltliche Kriterien				Methodenelemente			
Ansatz	Ganzheitlichkeit	Rollenbasierte Autorisierung	Systemunabhängigkeit	Risikogesteuerte Vorgehensweise	Vorgehensmodell / Aktivitäten	Techniken / Ergebnisdokumente	Metamodell	Rollen
Observations on the Role Life-Cycle in the Context of Enterprise Security Management (Kern et al. 2002)	◑	●	●	○	◑	○	●	○
Process-Oriented Approach for Role-Finding to Implement Role-Based Security Administration in a Large Industrial Organization (Roeckle et al. 2000)	◑	●	●	○	◑	○	●	◑
PROMET PSI: Methode zur Prozess und Systemintegration (IMG 1996)[210]	◑	○	●	○	◑	○	●	○
Prozessbasierte Gestaltung von (Aufbau-) Organisation und Berechtigungskonzept am Beispiel SAP R/3 (Vieting/Kumpf 2002)	◑	●	○	○	◑	◑	○	○
Role Mining – Revealing Business Roles for Security Administration using Data Mining Technology (Kuhlmann et al. 2003)	◑	●	●	○	◑	○	◑	○
SAP Berechtigungswesen (Hartje et al. 2003)	●	●	○	◑	●	●	◑	●

Legende: ● Intensiv behandelt/gegeben ◑ Teilweise behandelt/gegeben ○ Nicht bzw. rudimentär behandelt/gegeben

Tabelle 3: Bewertung der relevanten Methoden

Bei der Bewertung der vorgestellten Ansätze nach den in Kapitel 2.5 abgeleiteten Konsequenzen ergibt sich folgende Beurteilung (vgl. Tabelle 3):

- **Ganzheitlichkeit:** Die vorgestellten Ansätze gehen bei ihren Ausführungen über eine rein technische Betrachtung des Themas Sicherheit hinaus. Der Ansatz von HARTJE ET AL. ist dabei hervorzuheben. Er nimmt mit der intensiven Betrachtung von organisatorischen und rechtlichen Aspekten die umfassendste Perspektive ein.

- **Rollenbasierte Autorisierung:** Alle betrachteten Ansätze bauen auf rollenbasierten Konzepten auf. Eine Ausnahme bildet lediglich die Methode PROMET PSI.

[209] Vgl. hierzu auch Kremer 2004, S. 34.
[210] Die Bewertung findet in Hinblick auf das Thema Autorisierung statt.

- **Systemunabhängigkeit:** Die systemübergreifenden Ansätze zur Autorisierung können unabhängig vom einem spezifischen Werkzeug verwendet werden, obwohl die Ausführungen in drei von vier Fällen beispielhaft an einem bestimmten Werkzeug aufgezeigt werden.[211] Die diskutierten systemspezifischen Ansätze beziehen sich demgegenüber auf SAP R/3, sind somit nicht systemunabhängig.

- **Risikogesteuerte Vorgehensweise:** Sehr umfangreiche Sicherungsmassnahmen sind nur durch einen entsprechend hohen Einsatz von Ressourcen umzusetzen. Geringe Vorkehrungen bergen das Risiko, dass es zu erheblichen Schäden infolge mangelhafter Sicherheit kommt. Diese Überlegungen greifen in Ansätzen lediglich HARTJE ET AL. auf.

- **Methodisches Vorgehen (Methodenelemente):** Alle Ansätze präsentieren ein Vorgehensmodell, das die wesentlichen Aktivitäten des entsprechenden Ansatzes umfasst und einen Überblick über den zeitlichen Ablauf der Aktivitäten gibt. Detaillierte Techniken und Ergebnisdokumente werden jedoch nur teilweise dargestellt. Eine wirklich umfangreiche Diskussion mit Techniken und beispielhaften Ergebnisdokumenten präsentieren ausschliesslich HARTJE ET AL. Die Ansätze verfügen sämtlich über ein Metamodell für die Autorisierung, wenn dies auch überwiegend nicht explizit als solches ausgewiesen wird. Eine Ausnahme bildet hier lediglich der Beitrag von VIETING/KUMPF. Ein Rollenmodell für die Autorisierung, das wesentliche Aufgabenträger benennt und deren Aufgaben umschreibt, behandeln zwei der sechs Ansätze.

Die Bewertung der Ansätze anhand der inhaltlichen Kriterien zeigt vor allem Lücken in Bezug auf die risikogesteuerte Vorgehensweise auf. Hinsichtlich der Methodenelemente kann festgestellt werden, dass nur eine einzige Arbeit durchgängig detaillierte, methodische Elemente umfasst. Diese Arbeit setzt sich mit der Entwicklung systemspezifischer Berechtigungskonzepte auseinander (vgl. Tabelle 2) und widmet sich damit nur im Ansatz den Themenschwerpunkten der vorliegenden Arbeit. Ein Grossteil der diskutierten Beiträge präsentiert lediglich wesentliche Aktivitäten und ein Metamodell. Techniken, Ergebnisdokumente und Rollenmodelle stehen nicht im Fokus der Arbeiten.

Zusammenfassend lässt sich festhalten, dass kein Ansatz eine umfassende, methodische Sichtweise auf die gewählten Schwerpunkte der Dissertation gewährleistet und die Bewertung der Ansätze Lücken hinsichtlich inhaltlicher und methodischer Kriterien aufzeigt. Aufgrund dessen soll im Rahmen der Dissertation ein eigener Methodenvorschlag erarbeitet werden, der die präsentierten Ansätze berücksichtigt.

---

[211] Diese Aussage trifft für die Beiträge Kern et al. 2002, Roeckle et al. 2000 und Kuhlmann et al. 2003 zu.

4 Fallstudien

Die untersuchten Ansätze zur Autorisierung beinhalten keine umfassende, methodische Sichtweise auf die gewählten Schwerpunkte der Dissertation.[212] Daher dokumentiert dieses Kapitel der Arbeit Praxisprojekte in Form von Fallstudien, die im Weiteren den Ausgangspunkt des Methodenentwurfs bilden. Jeweils zwei Fallstudien widmen sich dabei einem der beiden Themenschwerpunkte der Arbeit (vgl. Tabelle 4).

Fallstudie	Themenschwerpunkt	
	Autorisierungs-architektur	Integration der Autorisierung
Basler Versicherungen		●
Credit Suisse	●	
GENERALI Gruppe Schweiz		●
Winterthur Group	●	

Tabelle 4: Übersicht über die erhobenen Fallstudien

Jede Fallstudie wird gleichermassen bei der Methodenentwicklung berücksichtigt und deckt jeweils den ganzen Betrachtungsgegenstand des Themenschwerpunkts ab. Die beiden Methodenbausteine „Autorisierungsarchitektur“ und „Integration der Autorisierung“ werden also nicht aus Versatzstücken unterschiedlicher Herkunft gebildet. Die Ableitung der Methode erfolgt vielmehr auf der Basis einer Identifikation von Gemeinsamkeiten und dem Prinzip der Induktion[213]. Bei der Erhebung der Fallstudien wurde darauf geachtet, dass die Spezifikation der Vorgehensweisen, die in Zusammenarbeit mit den verantwortlichen Unternehmensvertretern durchgeführt wurde,[214] auf dem gleichen Detaillierungsgrad erfolgt.

Die Dokumentation der Fallstudien basiert auf der Methode Promet Business Engineering Case Studies (BECS)[215], die im gleichen Forschungsprogramm wie die vorliegende Arbeit entwickelt wurde. Damit sind die wesentlichen Kernbereiche der Betrachtung die alte Lösung (Ausgangsituation), das (Transformations-)Projekt und die neue Lösung.[216] Die Fallstudiendokumentation geht jeweils zunächst auf wesentliche Eckdaten und elementare Herausforderungen ein, deren Kenntnis für das Verständnis der Fallstudie erforderlich ist und die die Bedeutung der dargestellten Lösung für das Unternehmen aufzeigen.[217] Anschliessend erfolgt die Beschreibung der Ausgangssituation, die die bisherige Situation und den daraus hervorgehenden Leidensdruck aufzeigt. Schliesslich werden das eigentliche Projekt sowie die neue Lö-

212 Vgl. Kapitel 3.2.6.
213 Zur Induktion vgl. Chalmers 1989, S. 10 ff.
214 Die detaillierten Vorgehensmodelle der einzelnen Fallstudien werden im Rahmen der Methodenableitung in Kapitel 6 und 7 präsentiert.
215 Vgl. Senger/Österle 2004.
216 Vgl. Senger/Österle 2004, S. 15.
217 Vgl. im Folgenden Senger/Österle 2004, S. 17f.

sung dargestellt und charakterisiert. Abbildung 23 zeigt überblicksartig die wesentlichen Fragestellungen einer Business Engineering Fallstudie auf.

Abbildung 23: Wesentliche Fragestellungen einer Business Engineering Fallstudie[218]

Im Folgenden werden zunächst die beiden Fallstudien zum Themenschwerpunkt „Autorisierungsarchitektur“ vorgestellt. Anschliessend werden die Fallstudien zum Schwerpunkt „Integration der Autorisierung“ dokumentiert.

4.1 Autorisierungsarchitektur bei der Credit Suisse

Die folgende Fallstudie wurde ausgewählt, da sich das Architekturmanagement bei der Credit Suisse aufgrund ihrer langjährigen Erfahrung durch ein hohes Mass an Vollständigkeit und Professionalität auszeichnet.[219] Die Credit Suisse betreibt darüber hinaus seit vielen Jahren eine umfangreiche Sicherheits- und Autorisierungsinfrastruktur.

4.1.1 Unternehmen

Die Credit Suisse ist eine von drei Geschäftseinheiten der Credit Suisse Group.[220] Neben der Credit Suisse umfasst die Credit Suisse Group die Geschäftseinheiten Credit Suisse First Boston und Winterthur.[221] Die Credit Suisse First Boston dient institutionellen Kunden, Unternehmen, staatlichen Körperschaften und vermögenden Privatkunden als Finanzintermediär. Sie bietet eine umfassende Palette von Produkten wie Wertpapierverkauf und -handel, Finanzberatung und Private-Equity-Anlagen an. Die Geschäftseinheit Winterthur deckt das Ver-

218 Vgl. Senger/Österle 2004, S. 16.
219 Vgl. Hafner 2005, S. 112.
220 Vgl. im Folgenden Credit Suisse Group 2005, S. 1ff.
221 Zum 1.1.2006 werden Credit Suisse und Credit Suisse First Boston zu einer Geschäftseinheit zusammengefasst.

sicherungs- und Vorsorgegeschäft für Privat- und Firmenkunden im europäischen, nordamerikanischen und in ausgewählten asiatischen Märkten ab. Da die Integration von Bank- und Versicherungsgeschäft nicht mehr Teil der Strategie der Credit Suisse Group ist, wird die Winterthur als Finanzinvestition weitergeführt und für einen möglichen Börsengang vorbereitet.

Die Credit Suisse (vgl. Tabelle 5) selbst setzt sich aus den Segmenten „Private Banking“ und „Corporate & Retail Banking“ zusammen:[222] Der Bereich „Private Banking“ bietet Dienstleistungen und massgeschneiderte Finanzlösungen für vermögende Kunden in der Schweiz und in zahlreichen anderen Ländern an. Der Bereich „Corporate & Retail Banking“ offeriert Firmen- und Privatkunden in der Schweiz Bankprodukte und -dienstleistungen. In diesem Geschäftsumfeld ist die Credit Suisse die zweitgrösste Bank der Schweiz. Das Schweizer Vertriebsnetz der Credit Suisse umfasste Ende 2004 214 Geschäftsstellen. Darüber hinaus gehörten zu diesem Zeitpunkt 50 Private-Banking-Standorte ausserhalb der Schweiz zur Credit Suisse.

Kategorie	Ausprägung
Gründung	1856
Firmensitz	Zürich, Schweiz
Branche	Finanzdienstleistungen
Geschäftsbereiche	Corporate & Retail Banking Private Banking
Organisationsstruktur	Frontdivisionen: Corporate & Retail Banking, Private Banking Switzerland, Private Banking International und Private Banking Europe Privatbanken: Bank Leu, Bank Hofmann, BGP Banca di Gestione Patrimoniale, Clariden Bank Back-Office: Information Technology und Operations, Investment Management, Trading & Sales
Nettoertrag	10.5 Mrd. CHF
Geschäftsaufwand	6.2 Mrd. CHF
Reingewinn	3.4 Mrd. CHF
Mitarbeiter	20’656

Tabelle 5: Grundlegende Unternehmensdaten der Credit Suisse 2004[223]

Die Strategie der Credit Suisse sieht vor, hinsichtlich Kundenzufriedenheit, Mitarbeiterkompetenz und Shareholder Return die führende globale Privatbank und die führende Bank in der Schweiz zu werden.[224] Um dieses Ziel zu erreichen, wird die Credit Suisse in Märkte und Geschäftsfelder mit überdurchschnittlichem Wachstum oder Wachstumspotenzial investieren. Durch einen weiteren Ausbau der Marktstellung in der Schweiz soll die Profitabilität der Unternehmung gestärkt werden. Eine breite geografische Abstützung mit innovativen Produkten und Lösungen in Verbindung mit einer kontinuierlichen Produktivitätssteigerung soll langfristiges Wachstum sichern. Die Nutzung von Synergien bei Kundenbeziehungen, Produkten und Infrastruktur dient dazu, das integrierte Geschäftsmodell zu festigen.

222 Vgl. im Folgenden Credit Suisse Group 2005, S.14.
223 Vgl. Credit Suisse Group 2005.
224 Vgl. im Folgenden Credit Suisse Group 2005, S. 15.

4.1.2 Ausgangssituation

Die folgende Fallstudie bezieht sich auf die „Swiss Banking IT Plattform“ der Credit Suisse. Mit dieser Plattform bedient die Credit Suisse über drei Millionen Kunden.[225] Ca. 22’000 Mitarbeiter arbeiten auf Basis dieser Plattform. 2’200 Informatikmitarbeiter betreiben und entwickeln sie kontinuierlich weiter. Auf der Plattform werden pro Tag bis zu einer Million Zahlungen abgewickelt, wozu bis zu 21 Millionen IMS-Transaktionsaufrufe notwendig sind.

Die Plattform verfügt über ca. 300 Grossrechner-Applikationen und mehr als 150 Client-Server-Applikationen. Die Applikationen sind weitestgehend Eigenentwicklungen und bestehen aus insgesamt ca. zwölf Millionen Zeilen Code PL/1 (Host) und ca. sechs Millionen Zeilen Java-, HPS- und Smalltalk-Code. Als Datenbanken dienen insbesondere IBM DB2, IBM IMS und Oracle. Die Infrastruktur besteht aus 1'000 dezentralen Netzwerk-Servern und 850 zentralen Servern. Darüber hinaus werden im Rechenzentrum der Credit Suisse über 20 Grossrechner auf der Basis von z/OS betrieben.

Die Applikationen sind über eine Integrationsinfrastruktur integriert. Diese basiert insbesondere auf dem Standard CORBA. Im Umfeld der asynchronen Kommunikation ist IBM WebSphere MQ im Einsatz. Als Applikationsserver wird BEA WebLogic verwendet. Auf die Plattform kann über diverse automatisierte Zugangskanäle wie Internet, Videotext, Telefon oder Bankomat zugegriffen werden.

Im Jahr 2000 wurden wesentliche Autorisierungssysteme der „Swiss Banking IT Plattform“ im Rahmen einer detaillierten Analyse bewertet. Die Bewertung ergab zum einen, dass die Verwaltung der Berechtigungen stark durch manuelle Abläufe bestimmt und sehr komplex war. Zum anderen zeigte sich, dass die Vergabe von Berechtigungen in der Vergangenheit vor allem infolge technischer Sachzwänge zum Teil eher grosszügig gehandhabt worden war: Einzelne Mitarbeiter hatten zum Bewertungszeitpunkt umfassendere Berechtigungen, als es das Vergabeprinzip „Need to Know“ vorsieht. Als zentrale Ursachen für die erkannten Potenziale wurden unterschiedliche Herausforderungen identifiziert.

Eine wesentliche Herauforderung stellte die *inhomogene Administrationslandschaft* der Credit Suisse dar. Im Bereich der Eigenentwicklungen existierten im Host-Umfeld drei Autorisierungslösungen von besonderer Bedeutung: Das Zugriffssystem „IMS-Sicherheit“ bestand seit Anfang der 1980er Jahre und war eine Eigenentwicklung der Credit Suisse. Das System arbeitete auf der Basis von Access Capability Lists, die die Berechtigungen eines Benutzers beinhalteten. Das Zugriffssystem „access control system (acs)“ bestand seit Anfang der 1990er Jahre und lief unter CICS. Das System war regelbasiert, d.h. die Berechtigungen wurden aufgrund von Regeln festgelegt. Das System „Object Authorization System“ wurde zum Schutz des elektronischen Archivs verwendet. Analog zum „access control system“ handelte es sich um ein regelbasiertes System. Neben diesen drei zentralen Autorisierungskomponenten exis-

[225] Vgl. im Folgenden Siegrist 2003, S. 6.

tierten weitere Lösungen zum Schutz der Applikationen, die im Umfeld von Eigenentwicklungen verwendet wurden. Auch die Autorisierungskomponenten der eingekauften Softwarelösungen waren in ihrer Gesamtheit sehr heterogen. Obwohl sich z.B. durch den RBAC-Standard in den letzten Jahren eine Grundlage für die Entwicklung von Autorisierungskomponenten etabliert hat, unterscheiden sich die Autorisierungskomponenten von Drittherstellern auch heute noch erheblich voneinander. Die Systemlandschaft der Credit Suisse umfasste somit zahlreiche isolierte Autorisierungskomponenten, die unterschiedlichste Autorisierungsparadigmen implementierten und über diverse Werkzeuge administriert wurden. Eine Homogenisierung der Autorisierungskomponenten über die unterschiedlichen Plattformen der Credit Suisse war somit anzustreben.

Eine weitere Herausforderung stellte die *komplexe Administration* der Berechtigungen dar. Die Administrationsprozesse der einzelnen Applikationen wurden über diverse Werkzeuge abgewickelt. Dies war ein Grund dafür, dass sich die konsistente Vergabe von Berechtigungen über unterschiedliche Plattformen hinweg schwierig gestaltete. Durch die komplexen Berechtigungsstrukturen und den Druck, den fortlaufenden Betrieb von Applikationen zu gewährleisten, kam es vor allem beim Wechsel eines Mitarbeiters auf eine neue Stelle nicht immer sofort zum Entzug aller Berechtigungen, die der Mitarbeiter für seine neue Stelle nicht mehr benötigte. Die Überprüfung von Berechtigungen war darüber hinaus zeitaufwändig, da die entsprechenden Listen eine Vielzahl von Berechtigungen enthielten, die nur von Spezialisten zu beurteilen waren. Vor diesem Hintergrund galt es somit, ein zeitgemässes Administrationssystem für die rollen- und regelbasierte Autorisierung zu entwickeln, das Berechtigungen weitestgehend automatisiert vergibt.

Die Credit Suisse verfügte zum Bewertungszeitpunkt über etablierte Autorisierungskomponenten, die die effektive Vergabe und Kontrolle von Berechtigungen ermöglichten. Die Autorisierungskonzepte, auf denen diese Komponenten basierten, entsprachen jedoch teilweise nicht mehr dem aktuellen Stand der Entwicklung. So waren die verwendeten *Autorisierungskonzepte zum Teil unflexibel* und nur schwer an neue Anforderungen anzupassen. Die durchgängige Einführung der rollen- und regelbasierten Administration wurde daher als Ziel definiert.

4.1.3 Projekt und Projektvorgehen

Die Entwicklung und Umsetzung der heutigen Autorisierungsarchitektur der Credit Suisse begann im Jahr 2000, nachdem die Revision Verbesserungspotenziale bei der Vergabe von Berechtigungen nach dem „Need to Know“ Prinzip aufgezeigt hatte. Das „Positionspapier Zugriffskontrolle“ zeigte Mitte 2000 zunächst den Ist-Zustand der Autorisierung, insbesondere im Host-Umfeld, zusammenfassend auf und entwickelt auf dieser Basis erste Lösungsansätze für die identifizierten Herausforderungen. Im Anschluss hieran wurde die konzeptionelle Arbeit im Rahmen zweier Projekte fortgeführt: Die „Authorization Architecture“ spezifizierte

die Soll-Situation der Autorisierung in Form von Standards, die grundlegende Aspekte der Autorisierung verbindlich festlegen. Parallel hierzu erfolgte die Entwicklung der umfassenderen „Security Architecture“, die die in der „Authorization Architecture“ entwickelten Massnahmen bewertet und so für den Budgetierungsprozess aufbereitet. Die wesentlichen Aktivitäten zur Entwicklung der Autorisierungsarchitektur werden im Folgenden näher erläutert.

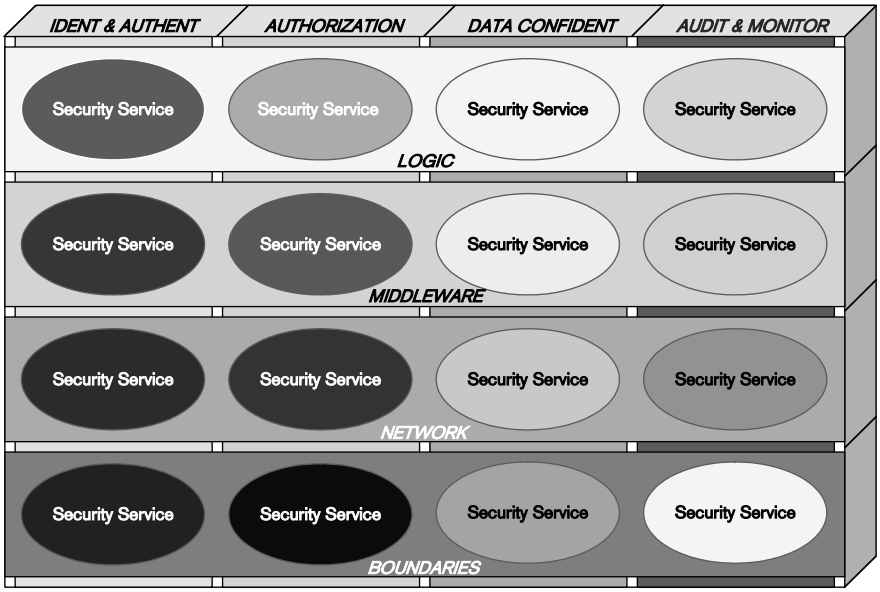

Abbildung 24: „Security Architecture Model“ der Credit Suisse

Zu Beginn der konzeptionellen Arbeiten erfolgte die *Erarbeitung der wesentlichen Grundlagen*. Im Rahmen der „Security Architecture“ wurde das „Security Architecture Model“ entwickelt (vgl. Abbildung 24). Dieses Modell zeigt wesentliche Sicherheitskomponenten und ihr Zusammenwirken auf. Das Modell dient damit insbesondere der Abgrenzung unterschiedlicher Teilbereiche. Das Modell beinhaltet vier Ebenen: Der „Logic Layer“ enthält die Logik, die die Datenmanipulation und -präsentation vornimmt. Der „Middleware Layer“ umfasst die Software, die den Informationsaustausch zwischen den Applikationen ermöglicht. Der „Network Layer“ adressiert den Transport von Informationen über Netzwerke. Die als „Boundaries“ bezeichnete Ebene umfasst schlussendlich die Aspekte, die bei der Kommunikation zwischen unterschiedlichen internen und externen Geschäftseinheiten zu berücksichtigen sind. Neben den vier Ebenen verfügt das Modell über vier Services: Der „Identification & Authentication Service“ thematisiert die Bereiche Identifikation und Authentisierung. Der „Authorization Service“ adressiert das Gebiet Autorisierung. Der „Data Confidentiality Service“ beschäftigt sich mit der sicheren Speicherung und dem sicheren Austausch von Daten. Der „Auditing und Monitoring Service“ setzt sich mit der Protokollierung und Kontrolle von sicherheitsrelevanten Aktivitäten auseinander. Die Kombination eines Services mit einer Ebene wird als Komponente bezeichnet. Die „Authorization Architecture“ ist dem „Authorization Service“ zuzuordnen und setzt sich insbesondere mit dem „Logic Layer“ auseinander.

Die Entwicklung der „Security Architecture“ und der „Authorization Architecture“ erfolgte auf der Basis international anerkannter Standards: Im Rahmen der „Authorization Architecture“ wurde intensiv auf den Standard ISO/IEC 10181-3 Bezug genommen, der wesentliche

Teilkomponenten einer Autorisierungslösung definiert und beschreibt. Die Standards, die im Zusammenhang der einzelnen Architekturen Verwendung finden, sind in den entsprechenden Dokumentationen so aufgearbeitet worden, dass sie den Bedürfnissen der Credit Suisse entsprechen.

Auf der Basis des Sicherheitsstandards ISO/IEC 17799 erfolgte die Ausarbeitung zentraler Sicherheitsanforderungen, die im Rahmen der angestrebten Lösungen zu berücksichtigen waren. Die Anforderungen wurden im Rahmen der „Security Architecture" dokumentiert und den einzelnen Komponenten des „Security Architecture Model" zugeordnet.

Schlussendlich wurden zentrale Begriffe definiert und in Form eines Glossars zusammengestellt. Um Sprachkonflikte zu vermeiden, sind zur eigentlichen Definition jeweils Synonyme in deutscher und englischer Sprache aufgeführt. Das Glossar ist Teil der „Security Architecture".

Im Rahmen der *Aufnahme der Ist-Situation* erfolgte die Analyse ausgewählter Autorisierungskomponenten. Zentrale Komponenten wurden hierbei u.a. anhand der Kriterien „Einsatzgebiet", „Datenbasis" „Zugriffsrechte" und „Sicherheitsprüfung" evaluiert. Unter dem Stichwort „Einsatzgebiet" wird jeweils die Verwendung der einzelnen Autorisierungskomponente beschrieben. Der Abschnitt „Datenbasis" thematisiert die Datenbestände, auf deren Grundlage die Autorisierungsprüfungen durchgeführt werden. Unter den Stichworten „Zugriffsrechte" und „Sicherheitsprüfungen" werden das grundlegende Autorisierungskonzept der jeweiligen Komponente sowie Art und Umfang der existierenden Berechtigungen beschrieben. Die Ergebnisse der Bewertung sind im „Positionspapier Zugriffskontrolle" dokumentiert. Ebenfalls bei Erstellung des „Positionspapier Zugriffskontrolle" erfolgte die Identifikation bestehender sowie neuer Autorisierungsanforderungen.

Die *Definition der Soll-Situation* für die Autorisierung begann bereits Mitte 2000 mit der Erarbeitung grundlegender Architekturkonzepte, die im „Positionspapier Zugriffskontrolle" in Form mittel- und langfristiger Lösungsszenarien auf hohem Abstraktionsniveau beschrieben wurden. Mit der „Authorization Architecture" erarbeitete die Architekturarbteilung schliesslich eine detaillierte Beschreibung der Soll-Situation durch die Definition von Standards, die grundlegende Aspekte der Autorisierung verbindlich festlegen. Eine Zusammenfassung der Soll-Situation findet sich in der „Roadmap" der „Security Architecture".

Die *Ableitung von Initiativen und Massnahmen* für die Autorisierung umfasste die Entwicklung von Massnahmenkomplexen im Rahmen der „Authorization Architecture". Die Priorisierung der Massnahmenkomplexe erfolgte dann als Teil der „Security Architecture" im Dokument „Roadmap". Als Bewertungskriterien dienten dabei die Kosten der Massnahmenkomplexe und ihr Nutzen in Form des erwarteten Sicherheitsgewinns. Diese Bewertungen bilden die Grundlage für den Budgetierungsprozess.

4.1.4 Zentrale Lösungsansätze

Die Autorisierungsarchitektur der Credit Suisse spezifiziert mit explizit definierten Regelungen, die als Standards bezeichnet werden, die Soll-Situation und die weiteren Entwicklungen im Bereich der Autorisierung. Unter anderem adressieren die Standards die folgenden wesentlichen Aspekte:

- Voraussetzungen der Autorisierung: Jedem Autorisierungsobjekt wie z.B. Daten, Benutzern oder Systemen muss eine verantwortliche Person zugeordnet sein.

- Grundlegendes Modell: Die Systeme der Credit Suisse werden von ca. 45'000 internen und über 300'000 externen Benutzern verwendet. Für all diese Benutzer müssen Berechtigungen verwaltet werden. Autorisierungsmechanismen, wie z.B. Access Capability Lists, stossen bei der Vielzahl der Benutzer und der hohen Anzahl der zu schützenden Daten an ihre Grenzen. Die rollen- und regelbasierte Autorisierung wird hier als adäquates Autorisierungskonzept angesehen. Um den Administrationssaufwand so gering wie möglich zu halten, sollen soweit möglich Regeln die Zuordnung von Nutzern zu Rollen automatisch vornehmen.

- Autorisierungskonzept: Die Credit Suisse unterscheidet zwei Autorisierungsebenen. Die unternehmensweite Autorisierungsebene umfasst alle existierenden Autorisierungskomponenten. Auf dieser Ebene werden Benutzer und Rollen systemübergreifend implementiert. Die systemübergreifenden Rollen werden dabei als Enterprise Rollen bezeichnet. Die systemspezifische Autorisierungsebene implementiert die Benutzer und Berechtigungen so, wie es das einzelne System verlangt. Die unternehmensweite Autorisierungsebene basiert auf der rollen- und regelbasierten Autorisierung. Die Umsetzung der Berechtigungen in den einzelnen Systemen erfolgt mit den von den einzelnen Systemen bereitgestellten Autorisierungsmechanismen. Priorisiert wird hierbei der Einsatz von Rollen und Regeln. Vision ist es, lediglich eine zentrale Instanz für die Administration der Berechtigungen zu etablieren. Über diese zentrale Instanz werden die Enterprise Rollen administriert, die die einzelnen systemspezifischen Berechtigungen umfassen, und den einzelnen Benutzern zugeordnet. Berechtigungen werden explizit auf eine genehmigte Anfrage hin vergeben. Die Vergabe richtet sich nach dem „Need to Know“ Prinzip, so dass ein Benutzer nur die Berechtigungen erhält, die er benötigt, um seine geschäftlichen Tätigkeiten auszuüben.

- Implementierung der rollen- und regelbasierten Autorisierung: In einem ersten Schritt gilt es, ein übergreifendes Rollenkonzept zu erarbeiten, das die wesentlichen Rollen aus dem Fachbereich und der IT umfasst, und im zentralen Administrationswerkzeug zu implementieren. In einem zweiten Schritt müssen dann die einzelnen Systeme an das zentrale Werkzeug angeschlossen werden. Die Berechtigungen werden weiterhin von den Projekten spezifiziert, die die entsprechende Applikation bzw. das entsprechende System implementieren. Bei der Spezifikation der Berechtigungen bilden die geschäftlichen Anforderungen die Ausgangsbasis. Nach ihnen richtet sich die Granularität der vergebenen Be-

rechtigungen. Auch bei hohen Sicherheitsanforderungen muss beachtet werden, dass die Anzahl der abgeleiteten Rollen und Regeln nur so hoch sein darf, dass eine effektive und effiziente Administration noch gewährleistet ist.

- Organisation und Prozesse der Autorisierung: Rollendefinitionen müssen durch die betroffenen Prozess- und Datenverantwortlichen sowie durch Vertreter des Risikomanagements und der Abteilung „Compliance“ abgenommen werden. Ebenfalls in diesen Prozess involviert ist das Rollen-Kompetenzzentrum, das als zentrale Einheit die systemübergreifende Entwicklung von Rollen vorantreibt. Rollen können zum einen automatisch über Regeln an Benutzer vergeben werden. Diese Regeln müssen durch das Rollen-Kompetenzzentrum und die entsprechenden Prozessverantwortlichen sowie durch Vertreter der Sicherheitsadministration, des Risikomanagements und der Abteilung „Compliance“ abgenommen werden. Zum anderen kann die Zuweisung von Rollen manuell erfolgen. Hierbei gilt es, speziell bei geschäftsbereichsübergreifenden oder externen Zugriffen, die Genehmigung der entsprechenden Prozess- und Datenverantwortlichen einzuholen. Die einzelnen Genehmigungsprozesse sind klar zu definieren und mit den Prozessbeteiligten abzustimmen.

- Zugriffskontrolle zur Laufzeit: Zur Laufzeit, d.h. zum Zeitpunkt, zu dem ein Mitarbeiter auf eine Applikation zugreift, muss überprüft werden, ob der Mitarbeiter die gewünschte Transaktion auf den entsprechenden Daten durchführen darf. Theoretisch kann eine Applikation diese Überprüfung selbst vornehmen oder durch eine speziell hierfür vorgesehene Komponente durchführen lassen. Die Applikationen der Credit Suisse dürfen keine Autorisierungslogik implementieren und realisieren somit letztere Lösung: Die Autorisierung wird im Rahmen der Infrastruktur durch zentrale Autorisierungsmodule vorgenommen. Die Applikationen greifen auf diese zentralen Komponenten über vordefinierte Schnittstellen zu.

- Autorisierung in mehrschichtigen Umgebungen: Um das „Need to Know“ Prinzip umzusetzen und einen ausreichenden Schutz zu gewährleisten, muss die Zugriffskontrolle so nah wie möglich an den zu schützenden Objekten stattfinden. Ausnahmen hiervon sind bei entsprechender Begründung und Genehmigung möglich. Die Informationen, die zur Autorisierung notwendig sind, werden in einer zentralen Datenbank verwaltet. Repliken dieser Datenbank können verwendet werden. Die Pflege der Berechtigungen erfolgt jedoch lediglich auf der führenden Datenbank.

- Credit Suisse-spezifische und systemspezifische Autorisierung: Die systemspezifische Autorisierung muss immer dann verwendet werden, wenn ein System ein eigenes Autorisierungskonzept implementiert, das nicht ersetzt werden kann. Dies ist vor allem bei eingekaufter Software gegeben. Die Credit Suisse-spezifische Autorisierung kommt immer dann zur Anwendung, wenn die zentral vorgehaltenen Infrastrukturmodule für die Autorisierung verwendet werden können. Dies ist insbesondere für alle selbstentwickelten Systeme der Fall. Sollte eine systemspezifische Autorisierung notwendig sein, so ist zu prü-

fen, inwieweit auf bereits definierte Rollen zurückgegriffen werden kann. Somit ist in jedem Fall Rücksprache mit dem Rollen-Kompetenzzentrum zu nehmen.

- Umliegende Systeme: Alle Systeme zur Administration von Berechtigungen sind auf Daten angewiesen, die bereits in anderen Systemen verfügbar sind. Diese Quellsysteme sind dabei für die Qualität der zur Verfügung gestellten Daten verantwortlich. Die Daten, die beispielsweise Benutzer- oder Aufbauorganisationsinformationen umfassen, werden in die Autorisierungssysteme importiert. Das Anlegen neuer Quellsysteme ist ebenso wie das manuelle Einpflegen von Daten, die bereits in anderen Systemen vorhanden sind, untersagt.

Zur Umsetzung der definierten Autorisierungsarchitektur wurden unterschiedliche Projekte in folgenden Bereichen gestartet:

- Credit Suisse-spezifische Autorisierung: Mit dem Projekt „AURA“ wurde die rollen- und regelbasierte Autorisierung für die Mainframe-Applikationen eingeführt. Die Zugriffskontrollsysteme „IMS-Sicherheit“ und „access control system“ wurden dabei in einem ersten Schritt durch eine neu entwickelte Lösung ersetzt, die auf der Basis des „Need to Know“ Prinzips konzipiert wurde. Die Lösung basiert auf dem Werkzeug SAM Jupiter der Beta Systems Software AG. Das Werkzeug wurde aufgrund seiner Funktionalität dem Werkzeug CONTROL-SA der Firma BMC vorgezogen, obwohl letzteres bereits im Unternehmen verwendet wird. Im Rahmen einer Machbarkeitsstudie wurde analysiert, ob die entwickelte Lösung auch auf die FrontNet-Plattform der Credit Suisse übertragen werden soll. Diese Intranet-Umgebung bietet den Kundenbetreuern der Credit Suisse einen zentralen Zugriff auf sämtliche kundenrelevanten Informationen und Transaktionen. Eine Entscheidung wurde noch nicht gefällt und wird auch erst zu gegebenem Zeitpunkt gefällt werden. Ein Projekt zur Implementierung der erarbeiteten Autorisierungslösung auf die zentralen Server ist ebenfalls initiiert. Die Autorisierung der Applikationen auf der „Java Application Plattform“ soll auf Basis der entwickelten Lösung umgesetzt werden.

- Systemspezifische Autorisierung: Ein weiteres Projekt befasst sich mit dem Einsatz des Werkzeugs Control SA im Bereich der systemspezifischen Autorisierung. Die Systeme Sun Solaris, AIX und Oracle stehen hierbei im Mittelpunkt. Die Einführung von Control SA stellt eine taktische Lösung dar, da das Werkzeug in diesem Umfeld bereits im Einsatz ist. Langfristiges Ziel ist die Ablösung der taktischen Lösung durch SAM Jupiter.

- Prozesse und Organisation: Durch die Einrichtung eines Rollen-Kompetenzzentrums wird eine Organisationseinheit geschaffen, die sich systemübergreifend mit der Implementierung der rollen- und regelbasierten Autorisierung beschäftigt. Das Rollen-Kompetenzzentrum nimmt unterschiedlichste Aufgaben im Umfeld der Autorisierung wahr. Zum einen begleitet es die Entwicklung geeigneter Infrastrukturlösungen für die Autorisierung. Zum anderen hat das Kompetenzzentrum zu verhindern, dass Autorisierungslösungen implementiert werden, die nicht den Vorgaben bzw. dem Credit Suisse-

Standard entsprechen. Darüber hinaus zeichnet es sich für das Management der systemübergreifenden Rollen verantwortlich und koordiniert die Verantwortlichen, die in den Rollendefinitionsprozess involviert sind. Schlussendlich unterstützt es die einzelnen Projekte bei der Definition von Rollen. Die Kompetenzen der Organisationseinheit liegen damit insbesondere bei der Definition von Standards für die Anwendung der rollen- und regelbasierten Autorisierung in einzelnen Entwicklungsprojekten sowie der Abnahme von Berechtigungskonzepten, die die einzelnen Projekte im Rahmen ihrer Arbeit entwickeln. Zur Ableitung der systemübergreifenden Enterprise Rollen hat die Credit Suisse auch Verfahren und Lösungen des Data Mining evaluiert. Die unter dem Schlagwort „Role Mining" vertriebenen Werkzeuge leiten systemübergreifende Rollen auf der Basis bereits vergebener Berechtigungen ab. Im Zuge einer ersten Evaluation wurden die Produkte SAM Jupiter Role Miner und Eurekify Sage analysiert. Auf der Basis der Eurekify-Lösung ist die Durchführung eines Piloten geplant.

Weitere Projekte, die in den Bereich Autorisierung fallen, sind angedacht:

- „Single Point of Administration": Die Schaffung einer zentralen Administrationslösung auf der Basis eines einzigen Werkzeugs erleichtert die konsistente Administration und Auswertung der Berechtigungen über alle Systeme hinweg.

- Zentraler „Security Data Mart": Zur zentralen Analyse, Auswertung und Kontrolle von Autorisierungsinformationen soll ggf. ein zentrale Datenquelle geschaffen werden. Diese zentrale Datenquelle wäre eine Interimslösung auf dem Weg zum „Single Point of Administration".

- Konsolidierung der Datenquellen: Autorisierungswerkzeuge sind auf Daten angewiesen, die bereits in anderen Systemen verfügbar sind. Eine Konsolidierung dieser Datenquellen bietet weitere Synergien.

4.1.5 Erfolgsfaktoren und Herausforderungen

Zentraler Erfolgsfaktor für die Umsetzung der Autorisierungsarchitektur war zum einen, die Verantwortlichen aus dem Fachbereich und der IT von der Vorteilhaftigkeit der Projekte zu überzeugen, um zunächst das notwendige *Budget* zu erhalten. Während der Laufzeit der Projekte musste darüber hinaus sichergestellt werden, dass die vorgesehenen Ziele und Lösungsansätze konsequent verfolgt werden.

Ein weiterer Erfolgsfaktor bei der Umsetzung der Autorisierungsarchitektur war darüber hinaus die *Zusammenarbeit der IT mit dem Fachbereich*. Die Bestimmung von Berechtigungen ist ein aufwendiger Prozess zwischen Fachbereich und IT, für den von beiden Seiten Ressourcen zur Verfügung gestellt werden müssen. Die beteiligten Mitarbeiter müssen darüber hinaus über die Kompetenz verfügen, die existierenden, komplexen Berechtigungsstrukturen zu ver-

stehen sowie neue angemessene und gut pflegbare Berechtigungen zu definieren. Eine gemeinsame Sprache zwischen IT und Fachbereich ist hierfür unabdingbar.

Die *Herausforderungen aus technischer Perspektive* resultierten insbesondere aus den heterogenen Autorisierungslösungen, die bereits im Unternehmen verwendet werden. Trotz existierender Standards unterscheiden sich die vorhandenen Lösungen erheblich voneinander. Diese Tatsache zieht eine Komplexität nach sich, die es im Rahmen der Projekte zu bewältigen gilt.

Obwohl Standards z.B. für die rollenbasierte Autorisierung existieren, bleiben *wesentliche Entwurfsfragestellungen* zunächst unbeantwortet. Insbesondere die Frage, wie detailliert Berechtigungen zu definieren sind, damit sie einerseits dem „Need to Know"-Prinzip entsprechen und gleichzeitig eine pflegbare Anzahl nicht übersteigen, wird durch die Standards nicht beantwortet und muss eigenverantwortlich, d.h. in Zusammenarbeit der IT-Beteiligten mit dem Fachbereich, bestimmt werden.

Eine weitere Herausforderung stellte die *Migration auf neue Autorisierungskomponenten* dar. Die Berechtigungskonzepte, die neu einzuführenden Komponenten zugrunde liegen, müssen zum einen tragfähig sein: Ein flächendeckender Einsatz der entwickelten Lösungen muss möglich sein. Dies bedingt einfache Lösungskonzepte. Zum anderen muss die Tragweite der Migration realistisch eingeschätzt werden. Änderungen einer Autorisierungskomponente wirken sich auf alle Applikationen aus, die auf diese Komponente angewiesen sind. Die Applikationen selbst müssen so ggf. ebenfalls im Quellcode modifiziert werden.

Bei der Einführung neuer Autorisierungswerkzeuge war weiterhin zu entscheiden, ob *Eigenentwicklungen oder Softwareprodukte von Drittherstellern* eingesetzt werden. Aufgrund der eigendefinierten Anforderungen und der bereits verwendeten Autorisierungskomponenten müssen ggf. auch Softwareprodukte von Drittherstellern angepasst werden. Die zentrale Fragestellung hierbei ist, wie umfangreich die Anpassungen sein müssen und inwieweit bestehende Systeme und Prozesse an das neue Werkzeug angepasst werden können.

4.2 Autorisierungsarchitektur bei der Winterthur Group

Die folgende Fallstudie wurde ausgewählt, da die Winterthur Group über ein langjähriges Erfahrungswissen bei der Entwicklung und dem Unterhalt von Architekturen verfügt. Darüber hinaus weist das beschriebene Projekt einen unternehmensweiten Charakter auf, der dem Anspruch der vorliegenden Arbeit gerecht wird. Schlussendlich unterhält die Winterthur seit vielen Jahren eine umfangreiche Sicherheits- und Autorisierungsinfrastruktur.

4.2.1 Unternehmen

Die Winterthur Group (vgl. Tabelle 6) nahm 1875 die Geschäfte auf und ist heute einer der grössten Versicherer in Europa.[226] Ihr Angebot umfasst Versicherungs- und Vorsorgelösungen für Private sowie für kleinere und mittlere Firmenkunden. Das Unternehmen ist vorwiegend auf westeuropäische Märkte ausgerichtet und darüber hinaus in Mittel- und Osteuropa, Nordamerika und ausgewählten asiatischen Ländern tätig. In der Schweiz ist die Winterthur Marktführerin.

Die Winterthur Group gliedert sich in die zwei Segmente Life & Pensions und Non-Life. Das Segment Life & Pensions bietet Versicherungsprodukte für Firmenkunden sowie Lebensversicherungs- und Rentenprodukte für Privatkunden an. Das Segment Non-Life deckt die Versicherungsbedürfnisse von Privaten sowie kleineren und mittleren Unternehmen ab. Es bietet eine umfangreiche Palette von Versicherungsprodukten wie Motorfahrzeug-, Feuer-, Sach- und allgemeine Haftpflichtversicherung sowie Unfall- und Krankenversicherungslösungen an. In den beiden Segmenten Life & Pensions und Non-Life setzt die Winterthur Group je nach Markt Agenten, Broker, Banken oder Direktvertriebskanäle ein.

Die Winterthur ist in die vier regionale Einheiten Schweiz, Deutschland, Market Group 1 und Market Group 2 aufgeteilt. Die Market Group 1 umfasst Grossbritannien, Spanien, Belgien, Tschechische Republik, Polen, Ungarn und die Slovakische Republik. Die Market Group 2 umfasst die USA, Japan, Hong Kong, Niederlande, Kanada, Taiwan und Indonesien.

Kategorie	Ausprägung
Gründung	1875
Firmensitz	Winterthur, Schweiz
Branche	Versicherungen
Geschäftsbereiche	Winterthur Life & Pensions Winterthur Non-Life
Regionale Einheiten	Schweiz Deutschland Market Group 1: Grossbritannien, Spanien, Belgien, Tschechische Republik, Polen, Ungarn, Slovakische Republik Market Group 2: USA, Japan, Hong Kong, Niederlande, Kanada, Taiwan, Indonesien.
Geschäftsvolumen	27.3 Mrd. CHF
Bruttoprämien	21.4 Mrd. CHF
Reingewinn	699 Mio. CHF
Mitarbeiter	19’020

Tabelle 6: Grundlegende Unternehmensdaten der Winterthur 2004[227]

Im Jahr 2003 erfolgte im Rahmen des Wechsels von einer Wachstums- hin zu einer Rentabilitätsstrategie die Reorganisation der Unternehmung. Die Neuorganisation betraf insbesondere das Group Head Office und das Versicherungsgeschäft in den europäischen Hauptmärkten, wo die jeweiligen Segmente Life & Pensions und Non-Life unter ein gemeinsames Manage-

226 Vgl. im Folgenden Winterthur Group 2005.
227 Vgl. Winterthur Group 2005.

ment zusammengeführt werden. Hierbei stehen Massnahmen zur Effizienzsteigerung und Kostensenkung im Vordergrund.

Die Winterthur Group ist seit 1997 eine hundertprozentige Tochtergesellschaft der Credit Suisse Group. Ende 2004 hat sich die Credit Suisse Group dafür entschieden, die Winterthur Group auf den Börsengang vorzubereiten.

Die folgenden Ausführungen beziehen sich im Wesentlichen auf die IT der Winterthur Schweiz. Diese erbringt jedoch auch Dienstleistungen an die ausländischen Markteinheiten.

4.2.2 Ausgangssituation

Durch die langjährige Selbständigkeit der Unternehmensbereiche Life & Pensions und Non-Life sind die IT-Organisation und die Applikationslandschaft der Winterthur sehr dezentral durch die drei Hauptbereiche Life & Pension, Non Life und Corporate Center geprägt. Organisation und Applikationslandschaft weisen heute daher folgende Eigenschaften auf:

- Vielzahl von heterogenen Applikationen: Die Applikationslandschaft der Winterthur umfasst eine Vielzahl heterogener Applikationen. Dies wurde vor allem dadurch gefördert, dass jede der drei Organisationseinheiten eigene Systeme entwickelt, eingekauft und betrieben hat. Die Applikationen wurden in der Vergangenheit zunächst grösstenteils selbst entwickelt. Heutzutage wird mit der Strategie „Buy before Make“ der Einkauf von Applikationen präferiert. Ein wesentlicher Teil der älteren Applikationen wird auf den Mainframe-Systemen der Winterthur betrieben. Neuere Applikationen basieren vor allem auf der Unix-Plattform der Winterthur.

- Applikationslandschaft von hoher Komplexität: Insgesamt weist die Applikationslandschaft der Winterthur eine hohe Komplexität auf. Das Konfigurationsmanagement zeigte sich in diesem Zusammenhang als zentrale Herausforderung. Durch die Verwendung unterschiedlicher Applikationen auf der einen und die Verbreitung verteilter, mehrschichtiger Softwaresysteme auf der anderen Seite erwies es sich als schwierig, auftretende Konfigurationsprobleme zu lokalisieren. Die Abhängigkeiten zwischen den einzelnen Softwarekomponenten, die mit der Verbreitung mehrschichtiger Softwaresysteme einhergingen, machten systemübergreifende Prozesse unabdingbar, die ein umfassendes Know-how voraussetzten. Beides mussten in entsprechenden Projekten aufgebaut und erarbeitet werden.

- Keine zentrale, integrierte Verwaltung und Kontrolle der Zugriffsberechtigungen: Durch die dezentrale Aufstellung der Winterthur begünstigt, entstanden an unterschiedlichen Stellen der Organisation Einheiten, die die Verwaltung von Zugriffsberechtigungen verantworteten. Übergreifende Administrationsprozesse wurden nur partiell klar definiert, so

dass die Verantwortlichkeiten und Ansprechpartner zwischen den Organisationseinheiten nur teilweise abgestimmt waren.

Im Jahr 2003 erfolgte eine organisatorische Restrukturierung der Winterthur. Dabei wurde die regionale Divisionalisierung auf Unternehmensebene in den Vordergrund gestellt und die starke Selbstständigkeit der Einheiten Winterthur Life & Pension und Winterthur Non Life aufgehoben. Folgende zentrale Entwicklungen gingen und gehen mit der Restrukturierung einher:

- Aufbau einer starken, zentralen Governance: In der Vergangenheit war die IT der Winterthur durch eine stark dezentrale Entscheidungsfindung gekennzeichnet. Im Rahmen der Restrukturierung wurde diese durch eine zentrale Entscheidungsfindung und -kontrolle abgelöst. Zentrale Einheiten wie „Architektur“ oder „Engineering“ setzen Standards IT-übergreifend durch.

- Klare Definition und Standardisierung der IT-Prozesse: Mit Einführung der „IT Infrastructure Library“ erfolgte die Definition und Standardisierung der IT-Prozesse. Im Bereich der Softwareentwicklung wird mit der Definition des „Solution Delivery Process“ die Entwicklung und Überführung von Software in die Produktion standardisiert.

- Konsolidierung und Standardisierung der Systemlandschaft: Durch die Einführung von „Technical Application Platforms“ (TAPs) erfolgte die Konsolidierung und Standardisierung der Applikationen und Systeme. Im Rahmen der TAP-Strategie wurden folgende Plattformen definiert: Die „Transaction Processing Platform“ umfasst die operativen Systeme; die Plattform „Data Warehouse“ beinhaltet die Applikationen und Systeme zur Analyse der Informationsbestände; die „Office Automation Platform“ enthält die Applikationen und Systeme zur Büroautomation; die „Enterprise Application Integration Plattform“ beinhaltet die Systeme zur Applikationsintegration. Die „Transaction Processing Platform“ untergliedert sich noch einmal in die „Centralized Transaction Platform“, die die Applikationen und Systeme der Mainframe-Umgebung umfasst, und die „Decentralized Transaction Platform“, die die Applikationen und Systeme der dezentralen, J2EE-basierten Produktionsumgebung beinhaltet.

Wesentliche Treiber der Entwicklung waren regulatorische Anforderungen, insbesondere der Sarbanes-Oxley Act. Dieser betrifft die Winterthur als Tochtergesellschaft der Credit Suisse Group. Da die Credit Suisse Group an der amerikanischen Börse notiert ist, unterliegt auch sie dem Geltungsbereich des Sarbanes-Oxley Act.

Die bisher dezentral geprägte Organisation der Winterthur stellt die Unternehmung besonders auch auf dem Gebiet der Autorisierung vor Herausforderungen. Dies betrifft zum einen die Systemlandschaft:

- Zentrale Autorisierungsinfrastruktur: Zur zentralen Autorisierungsinfrastruktur gehören Autorisierungskomponenten, die von mehreren unterschiedlichen Applikationen verwendet werden. Diese zentralen Komponenten werden bei der Winterthur auch als Autorisierungsdienstleister bezeichnet. Die Administration der Berechtigungen einer einzelnen Applikation findet somit nicht mehr in applikationsspezifischen Komponenten statt, sondern in zentral vorgehaltenen Infrastrukturkomponenten, den Autorisierungsdienstleistern. Die einzelnen Dienstleister basieren auf systemspezifischen, rollenbasierten Autorisierungskonzepten. Sie erlauben eine detaillierte Spezifikation der Berechtigungen. Bei der Winterthur existieren aufgrund der historischen Trennung der Organisation mehrere zentrale Autorisierungsdienstleister, die eine redundante Funktionalität anbieten. Den einzelnen Applikationen war es in der Vergangenheit überlassen, ob und wenn ja welchen Dienstleister sie verwenden. Verbesserungspotenzial existiert neben dem anzustrebenden Abbau dieser Redundanzen auch bei der Hinterlegung der Berechtigungen. Eine übersichtliche Dokumentation der Berechtigungen im System ist nur teilweise gegeben.

- Applikationen und Systeme: Die einzelnen Applikationen verfügen zum Teil über eigene Autorisierungskomponenten. Insbesondere ältere Applikationen basieren dabei partiell auf nicht mehr zeitgemässen Autorisierungskonzepten. Durch die zunehmende Vernetzung der Applikationen und Systeme, die bei der Winterthur auf der Basis einer Service-orientierten Architektur erfolgt, wird diese ursprünglich lokale Gegebenheit zum Problem. Selbst neue Systeme, die auf diese alten Kernsysteme zugreifen, sind dazu gezwungen, die veralteten Autorisierungsmechanismen zu verwenden. Eine Ablösung dieser alten Autorisierungskonzepte wird somit zunehmend aufwändiger. Eine weitere Herausforderung liegt in der gewachsenen, dezentralen Verteilung berechtigungsrelevanter Daten. Um eine Zugriffsentscheidung zu treffen, sind in der Regel unterschiedliche Autorisierungskomponenten zu konsultieren.

- Zentrales Verwaltungswerkzeug für Enterprise Rollen: Noch verfügt die Winterthur über kein Werkzeug für die Dokumentation eines durchgängigen, systemübergreifenden Rollenkonzepts auf der Basis von Enterprise Rollen und der automatisierten Zuweisung von Zugriffsrechten. Ohne Enterprise Rollen ist über die Systeme hinweg nur sehr schwer nachvollziehbar, warum ein Anwender eine bestimmte Berechtigung in einer Applikation bzw. in einem System innehat.

Hinsichtlich der Prozesse existieren folgende Herausforderungen:

- Entwicklungsprozesse: Für die Entwicklung von Berechtigungskonzepten ist ein erhebliches fachliches Wissen über die entsprechenden Geschäftsprozesse notwendig. Daher ist es unvermeidlich, den Fachbereich in die Spezifikation der Berechtigungskonzepte mit einzubeziehen. Der Fachbereich ist sich der Verantwortung bei der Spezifikation jedoch nur eingeschränkt bewusst, so dass die Beteiligung der Fachbereiche oftmals sehr kurz kommt. In der Spezifikationsphase wird darüber hinaus häufig die Tragweite des Berech-

tigungskonzeptes unterschätzt. Erst wenn Mitarbeiter ihnen zugedachte Aufgaben aufgrund mangelnder Berechtigungen nicht richtig ausführen können oder eine Überprüfung der Zugriffsberechtigung jedes einzelnen Mitarbeiters stattfindet, wird ihnen die Bedeutung des Berechtigungskonzeptes klar. Ein weiteres Problem liegt in der schwankenden Prozessqualität der Spezifikation von Berechtigungskonzepten. Ein geregelter Prozess für die Spezifikation mit Checklisten, Beispielen und vorgefertigten Mustern wird gerade erarbeitet.

- Administrationsprozesse: Bei der Administration der Berechtigungen im Betrieb kommt es insbesondere bei der administrative Grenzen überschreitenden Verwaltung von Zugriffsberechtigungen zu Problemen. Die Ursache liegt in unklaren, nicht spezifizierten Prozessabläufen. Darüber hinaus macht eine Vielfalt an Werkzeugen den Administrationsprozess komplex und teilweise ineffizient. Hierzu trägt auch der geringe Automatisierungsgrad der Administrationsprozesse bei.

4.2.3 Projekt und Projektvorgehen

Die Erarbeitung einer umfassenden Autorisierungsarchitektur für die Winterthur fand im Rahmen zweier Projekte statt. Das Winterthur-Projekt „CC AIM“ erstellte 2004 in Zusammenarbeit mit dem Competence Center Application Integration Management (CC AIM) der Universität St. Gallen erste Lösungsansätze im Bereich Autorisierung. Im Jahr 2005 knüpfte das Projekt „Security Architecture Winterthur“ an die Arbeit des Projekts CC AIM an. Als eine von vier Arbeitsgruppen setzte die Arbeitsgruppe „Autorisierung“ die Arbeit des Projektes CC AIM fort. Das Kernteam des Projektes CC AIM und der Arbeitsgruppe Autorisierung umfasste jeweils drei bzw. vier Personen aus den Bereichen Architektur und zentrale Administration sowie einen wissenschaftlichen Assistenten der Universität St. Gallen. Zu den einzelnen Sitzungen und Fragestellungen der Teams wurden je Diskussionsschwerpunkt Spezialisten aus den unterschiedlichsten Bereichen der Winterthur hinzugezogen.

Das Projektvorgehen in den Projekten erfolgte iterativ. Ein sequentielles Abarbeiten einzelner Projektphasen wie im klassischen Wasserfallmodell fand somit nicht statt. Vielmehr wurden die Projektphasen in mehreren Iterationen durchlaufen, vergleichbar dem Spiralmodell[228] der Softwareentwicklung.

In der ersten Phase des Projekts erfolgte die Erarbeitung der *Grundlagen*. Ausgehend von den Themenbereichen Datenschutz und Datensicherheit wurde das Gebiet Autorisierung aufgearbeitet. Die Arbeitsgruppe diskutierte unterschiedliche Autorisierungskonzepte aus dem Umfeld benutzerbestimmte, systembestimmte und rollenbasierte Zugriffskontrolle jeweils vor dem Hintergrund ihrer potenziellen Anwendung bei der Winterthur.

---

[228] Vgl. Balzert 1998, S. 129f.

Die rollenbasierte Zugriffskontrolle wurde als grundlegendes Autorisierungsparadigma ausgewählt und anhand von Fallstudien und Literatur auf ihre Anwendung in heterogenen Systemlandschaften untersucht. Auf dieser Basis konnte die Arbeitsgruppe bereits erste konkrete Lösungsszenarien für die Winterthur erörtern. Anforderungen, die bei der Autorisierung in heterogenen Systemlandschaften zu beachten sind, wurden daraufhin auf der Grundlage internationaler Sicherheitsstandards diskutiert.

Auf Grundlage der erörterten Anforderungen und der diskutierten Lösungsszenarien wurde die gegebene *Ist-Situation* analysiert. Ausgewählte Applikationen wurden in Bezug auf die Autorisierung untersucht. Im Vordergrund stand dabei unter anderem der Ablauf der Berechtigungsprüfungen zur Laufzeit der Applikationen. Einzelne Applikationen benötigen verschiedene Autorisierungssysteme für die Berechtigungsprüfung, so dass es zu teilweise komplexen Abläufen kommt, die entsprechendes Verbesserungspotenzial aufweisen. Ebenfalls diskutiert wurden Administrationsprozesse, die wie die Prüfungsabläufe mit steigender Anzahl von Autorisierungskomponenten an Komplexität zunehmen.

Neben den Applikationen untersuchte und bewertete die Arbeitsgruppe einzelne Autorisierungskomponenten. Dabei wurden, ausgehend von den Sicherheitszielen Vertraulichkeit, Integrität und Verfügbarkeit, Evaluationskriterien abgeleitet. Diese Kriterien fanden im Rahmen einer SWOT-Analyse Anwendung auf einzelne Systeme, um auf diese Weise die heutigen Stärken und Schwächen der Lösungen auszumachen und die Chancen und Risiken ihrer weiteren Verwendung zu betrachten.

Die Analyse der ausgewählten Applikationen und Systeme schloss mit der Identifikation zentraler Problemfelder. Einzelne Ergebnisse aus den zuvor durchgeführten Analysetätigkeiten wurden zu wesentlichen Problemfeldern zusammengefasst, um auf diese Weise die zentralen Herausforderungen im Bereich Autorisierung transparent kommunizieren zu können. Die Aufarbeitung und Zusammenfassung wurde so vorgenommen, dass auch das Management die wesentlichen Probleme nachvollziehen kann.

Die anschliessende Definition der *Soll-Situation* umfasste die Erarbeitung grundlegender Architekturkonzepte, die Festlegung zentraler Verantwortlichkeiten und Regelungen im Rahmen der ausgewählten Architekturszenarien sowie die Definition und Spezifikation ausgewählter Lösungsbausteine.

Die Erarbeitung grundlegender Architekturkonzepte umfasst die Auswahl zentraler Lösungsansätze. Die Entscheidung für oder gegen eine zentralisierte Administration von Berechtigungen auf der Basis von Enterprise Rollen stellt beispielsweise eine solche Auswahl dar. Eine weitere Entscheidung fundamentaler Art ist z.B. die langfristige Konsolidierung aller Autorisierungsdienstleister.

Im Rahmen der Definition von zentralen Verantwortlichkeiten und Standards thematisierte die Arbeitsgruppe unterschiedliche Aspekte der Autorisierung. Beispielsweise galt es, die

Verantwortlichkeitsbereiche bei der zentralisierten Administration von Berechtigungen auf der Basis von Enterprise Rollen festzulegen. Ein weiterer wesentlicher Diskussionspunkt war die Frage, in welcher Softwareschicht die Prüfung der Zugriffsberechtigung erfolgen sollte.

Um zu beurteilen, ob einzelne Autorisierungsarchitekturen bei der Winterthur umsetzbar sind, waren ausgewählte Lösungsbausteine der Soll-Lösung detailliert zu betrachten und zu spezifizieren. So wurde beispielsweise ein zentraler Autorisierungsservice, den eine Vielzahl unterschiedlicher Applikationen verwenden, komplett spezifiziert, um Komplexität und Machbarkeit der konkreten Lösung abschätzen zu können. Ein weiteres Beispiel ist die Definition einer Methodik zur Ableitung von Berechtigungskonzepten. Hier stand die Frage im Mittelpunkt, ob es möglich ist, für verschiedenartige Applikationen eine einzige Methodik zu entwickeln.

In der letzten Phase erfolgte die Ableitung der *Initiativen und Massnahmen.* Auf Grundlage der ermittelten Verbesserungspotenziale und der erarbeiteten Soll-Lösungen wurden Massnahmenkomplexe identifiziert. Die einzelnen Massnahmen dieser Komplexe wurden beschrieben und kurz charakterisiert, die Abhängigkeiten zwischen den Massnahmen festgehalten und Verantwortlichkeiten zugewiesen.

4.2.4 Zentrale Lösungsansätze

Im Rahmen der Projektarbeit wurden Lösungsansätze entwickelt und Massnahmen zu ihrer Umsetzung definiert. Diese Lösungsansätze und Massnahmen werden im Folgenden beschrieben.

Eine wesentliche Voraussetzung für die effiziente und effektive Autorisierung sind *konsistente und widerspruchsfreie Nutzerinformationen*. Weiterhin erforderlich ist die *Vorhaltung von Strukturdaten* über die Aufbauorganisation der Unternehmung. Folgende Massnahmen sind erarbeitet worden, um diese Ziele zu erreichen:

- Abbildung der Aufbauorganisation im Meta Directory: Das Meta Directory der Winterthur stellt eine integrierte Sicht auf die internen und externen Mitarbeiter der Winterthur dar. Wie in einem Operational Data Store werden Daten aus Quellsystemen bezogen und integriert, um schliesslich von Zielsystemen abgerufen zu werden. Eine direkte Manipulation von Daten durch einen Anwender findet im Meta Directory nicht statt. Grundlegende Informationen wie z.B. Name, Vorname, Adresse, Telefonnummer eines Mitarbeiters sind bereits im Meta Directory der Winterthur vorhanden. Die Aufbauorganisation der Winterthur wird nun ebenfalls in das Meta Directory aufgenommen und in die bereits vorhandenen Daten integriert.

- Abbildung der Organisationseinheiten, die am Prozess der Berechtigungsverwaltung beteiligt sind: Um die Zuweisung von Berechtigungen z.B. auf der Basis eines Workflow-

managementsystems durchführen zu können, müssen die entsprechenden Organisationseinheiten und Mitarbeiter im System erfasst und einander zugeordnet sein. Bei der Abbildung der Aufbauorganisation spielen die entsprechenden Organisationseinheiten mit ihren Mitarbeitern daher eine besondere Rolle.

- Klare Verantwortlichkeiten für die Quellsysteme des Meta Directory: Die Datenquelle, die Daten an das Meta Directory liefert, ist für die Qualität des Inhalts verantwortlich. Welches System welche Daten liefert ist genau definiert.

- Durchsetzung eines Mitarbeiteridentifikators: Im Laufe der Jahre haben sich für einen Mitarbeiter unterschiedliche Identifikatoren (Nutzer IDs) etabliert. Ziel muss es sein, den zur allgemeinen Verwendung bereits ausgewählten Identifikator in den Systemen durchzusetzen.

- Struktur- und Benutzerdatenverwaltung neu implementieren: Um die Nutzer- und Strukturdaten der Winterthur zu verwalten, ist eine zentral geführte Lösung notwendig.

- Durchsetzung des Meta Directories: Um das Meta Directory erfolgreich in der Organisation zu etablieren, müssen die einzelnen Entwickler dieses durchgängig verwenden. Die Zielsetzung ist nur durch eine angemessene Kommunikation und Prüfungen zu erreichen. Darüber hinaus müssen die technischen Voraussetzungen in Form von einfachen Schnittstellen geschaffen werden.

Ein weiteres Ziel ist die *nachvollziehbare, auditierungssichere Vergabe von Berechtigungen*, die durch folgende Aspekte sichergestellt wird:

- Jedes Geschäftsobjekt wird klar zugewiesen: Für die regulatorisch geforderte Revalidierung von Rechten, also den Abgleich der im System vergebenen Berechtigungen mit den Soll-Berechtigungen, ist die durchgängige Definition von Geschäftsobjekteigentümern notwendig.

- Der Eigentümer bestimmt, welche Rollen zugreifen dürfen: Durch die Einführung von Rollen werden die Berechtigungen zum Zugriff auf ein Geschäftsobjekt nicht direkt an den einzelnen Nutzer vergeben. Rollen dienen hier als intermediäres Konstrukt. Ob eine Rolle auf ein Geschäftsobjekt zugreifen darf, bestimmt der jeweilige Eigentümer.

Um die *Vision einer einheitlichen Autorisierungsinfrastruktur* mittelfristig zu realisieren, wurden folgende Massnahmen erarbeitet:

- Ablösung nicht mehr zeitgemässer Autorisierungskonzepte: In älteren Systemen werden Berechtigungen teilweise durch die Spezifikation von Zeichenketten festgelegt. Die Gewährleistung der Sicherheit ist zwar grundsätzlich auch mit solchen Systemen gegeben, diese sind jedoch sehr pflegeintensiv. Darüber hinaus ist die Länge der Zeichenketten begrenzt, so dass auf Dauer keine weiteren Berechtigungen mehr spezifiziert werden kön-

nen. Vor allem auf dem Mainframe existieren Standardsysteme, die die Autorisierung auf der Basis des anfragenden Terminals vornehmen. Die Hersteller dieser Systeme stellen Lösungen zur Verfügung, die das Problem zwar umgehen, aber letztlich nicht lösen können. Die nicht mehr zeitgemässen Autorisierungskomponenten müssen somit abgelöst werden. Umfangreiche Projekte sind hierzu notwendig. Dabei gilt es insbesondere die Abhängigkeiten zu den Systemen zu beachten, die auf die abzulösenden Systeme aufbauen.

- Migration applikationsspezifischer Autorisierungslösungen: Die selbstentwickelten Applikationen, die auf einer eigenen, proprietären Autorisierungskomponente aufbauen, werden langfristig auf einen Autorisierungsdienstleister migriert. Ausgenommen von dieser Regelung ist Software von Drittherstellern, die nur mit unangemessenem Aufwand portiert werden kann. Diese Massnahme ist im Wege einer langfristig angesetzten Portierung der Autorisierungslogik im Rahmen ohnehin anstehender Weiterentwicklungen der betroffenen Applikationen zu lösen.

- Kurzfristige Konsolidierung der Autorisierungsdienstleister: Aufgrund der historischen Trennung der organisatorischen Teilbereiche der Winterthur existieren Dienstleister, die allein aus historischen Gründen unterschiedliche Systeme bilden. Diese Systeme gehen ursprünglich auf einen einzigen Dienstleister zurück, der bereits vor der Trennung existierte. Die Migration dieser fast identischen Komponenten stellt den ersten Schritt zur Konsolidierung aller Autorisierungsdienstleister dar.

- Mittelfristige Konsolidierung der Autorisierungsdienstleister: Mittelfristig werden sowohl die Host-basierten Dienstleister als auch die Dienstleister der dezentralen Plattform zusammengefügt. Die Prüfung der Berechtigung wird als Service von den einzelnen Applikationen aufgerufen. Die eigentlichen Berechtigungen werden in einem zentralen System gepflegt.

Ein weiteres Ziel sind *klar definierte Entwicklungs- und Betriebsprozesse*. Folgende Massnahmen operationalisieren dieses Ziel:

- Definition und Dokumentation Entwicklungsprozesse: Die Spezifikation von systemübergreifenden Enterprise Rollen wird mit Hilfe von Checklisten und Templates sowie einem definierten Vorgehen unterstützt. Hierdurch wird der Ableitungsprozess von Enterprise Rollen festgelegt und Verantwortungen innerhalb des Prozesses geregelt. Bei der Zusammenfassung von Berechtigungen zu Enterprise Rollen sind die entsprechenden Aufgaben, Kompetenzen und Verantwortungen zu definieren. Für den Entwicklungsprozess der systemspezifischen Rollen und Berechtigungen gilt dies entsprechend. Eine genaue Definition und Dokumentation dieser Prozesse empfiehlt sich gerade vor dem Hintergrund der geltenden regulatorischen Anforderungen. Für die initiale Definition und Einführung der Enterprise Rollen ist ein entsprechendes Projekt notwendig.

- Definition und Dokumentation Betriebsprozesse: Die täglichen Administrationsprozesse der Autorisierung beinhalten insbesondere die Zuweisung von Nutzern zu Rollen. Darüber hinaus müssen teilweise geringfügige Änderungen an Berechtigungsstrukturen vorgenommen werden. Auch für die Betriebsprozesse empfiehlt sich angesichts der regulatorischen Anforderungen eine genaue Definition und Dokumentation.

Um die *Vision der zentralen Benutzeradministration* umzusetzen, wurden folgende Massnahmen erarbeitet:

- Stärkung der zentralen Administration: Eine hohe Anzahl an dezentral verteilten Administratoren führt zu komplexen Administrationsprozessen und erschwert die Nachvollziehbarkeit der Berechtigungen und die konsistente Rechtevergabe. Daher werden die Administrationsprozesse soweit möglich zentralisiert.

- Auswahl eines Werkzeugs für die zentrale Benutzeradministration: Um eine zentrale Rechtevergabe auf der Basis von Enterprise Rollen zu realisieren, bedarf es geeigneter Werkzeuge zur strukturierten Ablage und Verwaltung der Rollen und Berechtigungen. Darüber hinaus ermöglicht die Verwendung von Werkzeugen eine weitgehende Automatisierung der Administrationsprozesse.

4.2.5 Erfolgsfaktoren und Herausforderungen

Ein wesentlicher Erfolgsfaktor im Rahmen der Projektarbeit war die *Person des Projektleiters*. Zum einen lag es in seiner Verantwortung die Projektergebnisse dem Management vorzustellen, um die weitere Unterstützung und Umsetzung der erarbeiteten Ergebnisse zu gewährleisten. Zum anderen hatte er sicherzustellen, dass das Projektteam trotz Zeitdruck motiviert und pünktlich die vereinbarten Ergebnisse lieferte.

Neben einem engagierten Projektleiter erwies sich das sehr gut funktionierende *Team* als wesentliche Voraussetzung für den Projekterfolg. Um neben der täglichen, operativen Arbeit an dem Projekt mitarbeiten zu können, mussten die Projektmitglieder ihren eigentlichen Arbeitsumfang teilweise erheblich erhöhen. Ohne eine gute Grundstimmung im Team wären negative Auswirkungen auf die Produktivität der Gruppe kaum zu vermeiden gewesen.

Ein weiterer Erfolgsfaktor des Projekts war die *breite Verankerung des Projektteams* in der Organisation. Um die Akzeptanz der erarbeiteten Lösung sicherzustellen, sollten Mitarbeiter aus allen entscheidenden Bereichen in das Projekt integriert werden. Eine Umsetzung von Massnahmen gegen den Willen einzelner einflussreicher Mitarbeiter ist nur sehr eingeschränkt möglich.

Der *Einbezug externen Wissens* stellte ebenfalls eine wichtige Voraussetzung dar. Die Hinzuziehung externer Fachleute empfiehlt sich insbesondere bei der Aufarbeitung der thematischen Grundlagen sowie des aktuellen Forschungs- und Technologiestandes. Zum Abgleich

erarbeiteter Zwischenergebnisse bietet sich darüber hinaus der Austausch mit anderen Unternehmen an. Auf diese Weise lässt sich eine Diskussion der Umsetzbarkeit und Risiken geplanter Lösungen etablieren.

Um die Qualität der erarbeiteten Ergebnisse sicherzustellen, ist hinreichend *Zeit für die Projektarbeit* einzuplanen. Erste Lösungsansätze sind schnell erarbeitet. Die grundlegenden Architekturentscheidungen haben jedoch eine erhebliche Tragweite. Um zu einer realistischen Abschätzung der Vor- und Nachteile einer Lösung zu gelangen, müssen daher einzelne Aspekte zum Teil detailliert analysiert werden.

Die *Kooperation mit anderen Initiativen* innerhalb der Winterthur wie z.B. der Umsetzung des Sarbanes-Oxley Act kam auch dem durchgeführten Architekturprojekt zu Gute. Da der Sarbanes-Oxley Act regulatorische Anforderungen an die Sicherheit der Informationssysteme stellt und die Bedeutung des Sarbanes-Oxley Act für die Winterthur entsprechend hoch ist, war die Unterstützung des Projektes durch das Management jederzeit gegeben.

Mit dem internationalen Sicherheitsstandard ISO 17799 lag zudem ein *unternehmensweit gültiger Anforderungskatalog* vor. Das zentrale Problem bei der Definition von Sicherheitslösungen ist die Frage, wann eine Lösung sicher ist und wann nicht. Diese Diskussionen konnten im Fall des durchgeführten Projektes auf einer definierten Basis, dem genannten ISO-Standard, stattfinden.

Im Rahmen des Projektes waren einige zentrale Herausforderungen zu bewältigen. Eine wesentliche Herausforderung bestand in der eingeschränkten *Verfügbarkeit von detailliertem Erfahrungswissen* bei einzelnen Altsystemen. Ohne dieses Wissen ist bereits die realistische Einschätzung der Ist-Situation schwierig. Eine Spezifikation geeigneter Massnahmen zur Verbesserung der Ist-Situation kann ohne dieses Wissen zudem nur auf sehr hohem Abstraktionsniveau erfolgen.

Eine weitere wesentliche Herausforderung ist die *Beurteilung von Lösungen* unter Sicherheitsaspekten. Mit dem angewendeten Standard ISO 17799 stand zwar ein Anforderungskatalog zur Verfügung. In Bezug auf konkrete Lösungen bietet dieser jedoch regelmässig erheblichen Interpretationsspielraum.

Bei der Umsetzung der erarbeiteten Massnahmen sind kritische Herausforderungen zu überwinden. Insbesondere müssen die entsprechenden *Ressourcen zur Umsetzung der Massnahmen* tatsächlich zur Verfügung gestellt werden. Dies umfasst nicht nur die Bewilligung der Massnahmen durch das Management sondern auch die Verfügbarkeit von qualifiziertem Personal, das neben seiner operativen Tätigkeit geplante Lösungen implementiert.

Darüber hinaus geht mit der angestrebten Zentralisierung von Prozessen und Systemen eine *Entmachtung dezentraler Einheiten* und der dort eingesetzten Mitarbeiter einher. Auf die Kooperation dieser Wissensträger ist die Unternehmung angewiesen, um eine erfolgreiche Zen-

tralisierung zu realisieren. Neben der Zentralisierung der Sicherheit existieren in der Winterthur, wie beschrieben, weitere Zentralisierungsinitiativen. Für einen einzelnen Mitarbeiter kann dies eine erhebliche Veränderung seines Arbeitsumfelds bedeuten. Diese fundamentalen Änderungen stossen partiell auf entsprechenden Widerstand, den es zu überwinden gilt.

4.3 Integration der Autorisierung bei den Basler Versicherungen

Die folgende Fallstudie wurde ausgewählt, da im Rahmen der Fallstudie zahlreiche Berechtigungen unterschiedlicher Systeme auf der Basis systemübergreifender Rollen integriert werden. Darüber hinaus wird die erarbeitete Lösung seit mehr als drei Jahren erfolgreich betrieben und fortlaufend auf weitere Systeme ausgedehnt. Die erarbeitet Lösung sowie die entsprechende Vorgehensweise haben sich somit in der Praxis bewährt.

4.3.1 Unternehmen

Die Bâloise-Gruppe (vgl. Tabelle 7) mit Sitz in Basel ist ein in verschiedenen europäischen Ländern tätiger Anbieter von Lösungen für Versicherung, Vorsorge und Vermögensbildung.[229] Ihre Landesgesellschaften befinden sich in Belgien, Deutschland, Kroatien, Luxemburg, Österreich und der Schweiz.

Kategorie	Ausprägung
Firmensitz	Basel, Schweiz
Branche	Versicherungen, Banken
Geschäftsbereiche	Nichtlebensversicherung Lebensversicherung Bank
Regionale Einheiten	Belgien: Mercator Verzekeringen Deutschland: Basler Securitas, Deutscher Ring Versicherungen Kroatien: Basler Osiguranje Luxemburg: Bâloise Assurances Österreich: Basler Versicherungen Schweiz: Basler Versicherungen, Bâloise Bank
Geschäftsvolumen	7.5 Mrd. CHF
Bruttoprämien	7.0 Mrd. CHF
Konzerngewinn	221.7 Mio. CHF
Mitarbeiter	8’090

Tabelle 7: Grundlegende Unternehmensdaten der Bâloise 2004[230]

Die Basler Schweiz ist die grösste Einheit der Bâloise-Gruppe und gehört zu den führenden Schweizer Anbietern von Versicherungs- und Vorsorgeprodukten für Privatkunden sowie kleinere und mittelständische Unternehmen. Sie ist die viertgrösste Schweizer Versicherung

229 Vgl. im Folgenden Bâloise-Holding 2005.
230 Vgl. Bâloise-Holding 2005.

und beschäftigt rund 3'550 Mitarbeiter. Die Versicherungsprodukte werden durch die Angebote der Bâloise Bank SoBa um weitere Finanzdienstleistungen ergänzt.

Die Basler Schweiz bietet in ihrem Geschäftsbereich Lebensversicherung Lebens- und Rentenversicherungen für Privatpersonen sowie Versicherungslösungen im Rahmen der beruflichen Vorsorge (BVG), der Unfallversicherung und im Bereich des Krankentaggeldes für Unternehmen an. Im Bereich Nichtleben bietet das Unternehmen eine breite Palette von Versicherungslösungen wie Motorfahrzeug-, Feuer-, Sach- und allgemeine Haftpflichtversicherung an.

4.3.2 Ausgangssituation des Projektes

Die Applikationen der Basler Schweiz bauen insbesondere auf Eigenentwicklungen im Host-Umfeld auf. Diese Eigenentwicklungen sind vor allem auf Basis von IMS realisiert. Die IMS-basierten Applikationen verfügen über eine eigene Benutzerverwaltung. Zentrale Komponente zur Ablage und Verwaltung von Berechtigungen ist hierbei RACF (Resource Access Control Facility). RACF ist die Autorisierungskomponente von IBM, die die Vergabe von Berechtigungen im Host-Umfeld ermöglicht.

Die neueren, Java-basierten Applikationen werden ebenfalls über RACF administriert. Das RACF-System bildet somit eine zentrale Komponente zur Administration von „neuen", Java-basierten und „alten", Host-basierten Applikationen. Eine weitere Applikationsplattform liegt in Form von DB2 Universal Database und CICS (Customer Information Control System) vor.

Im Bereich „Netzwerk" verfügt die Basler Versicherung über eine Novell-Lösung. Anwendungen im Umfeld E-Mail und Kollaboration werden durch IBM Lotus Notes realisiert. Das Rechnungswesen wird über ein SAP-System abgewickelt. Im Bereich Personalwesen findet die Lösung HR Access Verwendung.

Die Vielzahl von unterschiedlichen Applikationen und Systemen stellt die effiziente und effektive Autorisierung vor zahlreiche Herausforderungen. Wesentliche Treiber und Herausforderungen, die die Einführung einer zentralen, systemübergreifenden, rollenbasierten Nutzerverwaltung motivierten, waren:

- Klonen von Benutzerberechtigungen: Die Vergabe von Berechtigungen orientierte sich an existierenden Benutzerkonten. Die Berechtigungen z.B. beim Eintritt eines Mitarbeiters wurden in der Regel auf der Basis bereits angelegter Benutzerkonten von Arbeitskollegen vergeben. Die Frage, ob der Mitarbeiter einzelne Berechtigungen wirklich benötigt, stand dabei nicht so sehr im Vordergrund wie die Frage, ob der Mitarbeiter störungsfrei arbeiten kann.

- Verlust von Wissensträgern: Um Berechtigungen lediglich an die Mitarbeiter zu vergeben, die wirklich auf diese angewiesen sind, ist die genaue Kenntnis der Berechtigungen unab-

dingbar. Durch den – vor allem infolge von Umstrukturierungen und Kompetenzverschiebungen auftretenden – Verlust von „Wissensträgern“, die als einzige ausgewählte Berechtigungen verstehen, ist die gezielte und angemessene Vergabe der Berechtigungen im betroffenen Bereich nicht mehr geben. Das notwendige Wissen muss neu aufgebaut werden. Kurzfristig war in der Vergangenheit die grosszügige Vergabe von Berechtigungen die einzige Möglichkeit, den durchgängigen Betrieb einer Lösung sicherzustellen.

- Grosszügige Vergabe von Berechtigungen: Damit die Mitarbeiter des Unternehmens ihren Aufgaben angemessen nachkommen können, sind entsprechende Berechtigungen in den Informationssystemen notwendig. Um Vorfälle zu vermeiden, in denen ein Mitarbeiter den ihm zugedachten Aufgaben nicht nachkommen kann, erfolgte die Vergabe der Berechtigungen im Zweifelsfall eher grosszügig.

- Eingeschränkter Entzug von Berechtigungen: Wechselt ein Mitarbeiter seine Stellung im Unternehmen, so sind seine Berechtigungen entsprechend anzupassen. Gegebenenfalls sind auch Berechtigungen zu entziehen. Um den ungestörten Betrieb zu gewährleisten, wurde im Zweifelsfall auf einen Berechtigungsentzug verzichtet. Insbesondere bei langjährigen Mitarbeitern kann dies zu einer umfangreichen Ansammlung unangemessener Berechtigungen führen.

- Feingranulare Vergabe von Berechtigungen: Im Umfeld von IMS erfolgt die Vergabe von Berechtigungen auf der Ebene von Transaktionen. Ein Benutzer bekommt direkt Transaktionen zugewiesen. Diese sehr feingranulare, ineffiziente und intransparente Vergabe von Berechtigungen kann systembedingt nicht vereinfacht werden: Konstrukte zur Zusammenfassung von Berechtigungen wie Gruppen oder Rollen existieren im Umfeld von IMS nicht.

- Eingeschränkte Transparenz und Nachvollziehbarkeit der Berechtigungen: Durch die Vielzahl der Anwender, Applikationen und Systeme sowie durch die gewachsenen Strukturen waren die Transparenz und Nachvollziehbarkeit der vergebenen Berechtigungen lediglich eingeschränkt gegeben. Die zentralen Fragen „Welcher Mitarbeiter hat in welcher Applikation bzw. in welchem System welche Berechtigungen?“ und „Warum hat ein Mitarbeiter eine bestimmte Berechtigung?“ konnten somit nur unzureichend beantwortet werden.

Die angemessene Vergabe der Berechtigungen unter den dargestellten Bedingungen konnte nur aufgrund des umfangreichen Wissens einzelner, weniger Mitarbeiter gewährleistet werden. Hierdurch war die Unternehmung in einem hohen Masse von diesen Wissensträgern abhängig.

4.3.3 Projekt und Projektvorgehen

Das Projekt zur Schaffung einer zentralen, systemübergreifenden Administrationslösung wurde im Jahr 2001 initiiert. Ausgangspunkt war eine zentral durchgeführte Risikoanalyse, die einen entsprechenden Handlungsbedarf aufgezeigt hatte und den Projektauftrag massgeblich bestimmte.

Wesentliches Ziel, das mit dem Projekt umgesetzt werden sollte, war die Schaffung von Transparenz und Nachvollziehbarkeit bei der Vergabe von Berechtigungen. Darüber hinaus sollten, soweit möglich, Systeme konsolidiert und eine Vereinfachung der Systemlandschaft erzielt werden. Allgemein stand die verbesserte Vergabe von Berechtigungen im Sinne einer effektiven und qualitativ hochwertigen Administration im Vordergrund. Kosteneinsparungen waren somit nicht primärer Projekttreiber.

Das Projektteam bestand zum einen aus einem Sicherheitsbeauftragten, der seine Expertise aus dem Umfeld der Sicherheit von Informationssystemen in das Projekt einbrachte. Darüber hinaus gehörten die Mitarbeiter der zentralen Benutzerverwaltung dem Projektteam an. Auftraggeber des Projektes war der damalige Informatikleiter der Basler Versicherungen. Je nach Themengebiet wurden interne Experten zum Projekt hinzugezogen. Vier Mitarbeiter vertraten beispielsweise treuhänderisch die Interessen des Fachbereiches. Spezialisten aus der IT brachten das notwendige Wissen über einzelne Systeme in die Projektarbeit ein.

Der Fokus des Projektes lag auf den Organisationseinheiten Basler Versicherungen und Konzern Schweiz. Die ausländischen Organisationseinheiten waren nicht in das Projekt involviert. In einem ersten Schritt wurden die erarbeiteten Konzepte in der Informatik der Basler Versicherungen umgesetzt. Erst im Anschluss an diese erfolgreiche Umsetzung erfolgte die Implementierung der Lösung im Fachbereich.

Das Projekt adressierte zwei Aspekte. Zum einen wurde ein technisches Konzept entwickelt, das die zukünftige technische Architektur im Bereich Authentisierung und Autorisierung bestimmte. Wesentliche Diskussionspunkte waren hierbei:

- Meta Directory: Zur Integration und Konsolidierung von verteilten Benutzerinformationen wurde der Einsatz einer entsprechenden Integrationslösung (Meta Directory) diskutiert. Da jedoch ein einheitlicher Benutzeridentifikator auf Basis der Personalnummer in den vorhandenen Systemen bereits etabliert war, entschied sich das Projekt gegen eine kurzfristige Meta Directory Einführung.

- Single Sign-on: Nach der Analyse existierender Lösungen für die einmalige, integrierte Authentisierung (Single Sign-on) beschloss das Projekt, auf einen Einsatz dieser Produkte zu verzichten, da die verfügbaren Lösungen für einen grossflächigen Einsatz im Unternehmen noch nicht reif genug waren. Um die Authentisierungsprozesse zu vereinfachen, wurden diese jedoch auf die vorhandene RACF-Lösung fokussiert.

- Public Key Infrastructure: Die Einführung einer Lösung, die die Vertraulichkeit und Integrität der Kommunikation auf der Basis von Zertifikaten sicherstellt (Public Key Infrastructure), stand im Rahmen des Projektes ebenfalls zur Diskussion. Aufgrund der bereits eingesetzten, qualitativ hochwertigen Verfahren und der Reife der existierenden Produkte wurde jedoch vorläufig auf eine Einführung verzichtet.

- Automatische Vergabe von Berechtigungen: Zur Automatisierung der Berechtigungsvergabe wurden unterschiedliche Werkzeuge evaluiert. Schliesslich erfolgte die Auswahl des Werkzeuges ASG-Entact der Firma Allen Systems Group (ASG).

Neben den vorgestellten technischen Architekturaspekten entwickelte das Projekt ein Konzept für die systemübergreifende Administration von Berechtigungen, welches im Rahmen des Projektes auch implementiert wurde. Im Folgenden werden die erarbeitete Lösung und das Vorgehen des Projektes vertieft dargestellt.

4.3.4 Neue Lösung

Das entwickelte Administrationskonzept baut auf zwei zentralen Konstrukten auf. Zum einen sind dies Ressourcen, die system- bzw. applikationsspezifische Berechtigungen beinhalten. Zum anderen sind dies Rollen, die eine definierte Menge von Ressourcen umfassen und Mitarbeitern zugewiesen werden. Die Ressourcen einer Rolle können dabei zu unterschiedlichen Systemen und Applikationen gehören. Eine Rolle ist damit ein systemübergreifendes Konstrukt, das eine Zusammenfassung von Zugriffsrechten nach fachlichen Tätigkeiten darstellt.

Aufgaben	Kompetenzen	Verantwortungen
▪ Anlegen von Rollen ▪ Löschen von Rollen ▪ Modifikation von Rollen ▪ Beantragung von Ressourcen für eine Rolle ▪ Zuweisung von Mitarbeitern zu Rollen	▪ Definition der Rollen ▪ Zuweisung von Mitarbeitern zu Rollen	▪ Sicherstellung, dass eine Rolle die notwendigen Berechtigungen umfasst ▪ Sicherstellung, dass eine Rolle nur den Benutzern zugewiesen ist, die sie auch wirklich benötigen

Tabelle 8: Aufgaben, Kompetenzen, Verantwortungen Rollenowner

Das Anlegen, Löschen und die Modifikation der Rollen wird durch Rollenowner verantwortet und durchgeführt (vgl. Tabelle 8). Der Verantwortungsbereich eines Rollenowner ist klar definiert und orientiert sich an der Organisationsstruktur der Unternehmung, insbesondere an den Abteilungen. Für die Mitarbeiter seines Verantwortungsbereichs legt der Rollenowner die Rollen fest, indem er diese im dafür vorgesehenen System anlegt, ihnen die notwendigen Ressourcen zuteilt und abschliessend die Mitarbeiter den Rollen zuweist. Die Zuweisung der Ressourcen bedarf der Zustimmung des Ressourcenowner, der eine Zuordnung ggf. auch ablehnen kann. Es liegt in der Verantwortung des Rollenowner sicherzustellen, dass eine Rolle alle Berechtigungen umfasst, die die entsprechenden Mitarbeiter benötigen. Darüber hinaus muss

er gewährleisten, dass eine Rolle nur den Benutzern zugewiesen wird, die diese auch wirklich benötigen.

Aufgaben	Kompetenzen	Verantwortungen
▪ Anlegen von Ressourcen ▪ Löschen von Ressourcen ▪ Modifikation von Ressourcen ▪ Bestätigung bzw. Ablehnung von Anträgen zur Ressourcennutzung	▪ Definition der Ressourcen ▪ Zuweisung von Ressourcen zu Rollen	▪ Sicherstellung, dass eine Ressource nur den Rollen zugewiesen wird, die sie auch wirklich benötigen

Tabelle 9: Aufgaben, Kompetenzen, Verantwortungen Ressourcenowner

Das Anlegen, Löschen und die Modifikation von Ressourcen obliegt den Ressourcenownern (vgl. Tabelle 9). Um sicherzustellen, dass eine Ressource nur den Rollen zugewiesen wird, die sie auch wirklich benötigen, ist es Aufgabe der Ressourcenowner, Anträge der Rollenowner zur Ressourcennutzung anzunehmen oder abzulehnen.

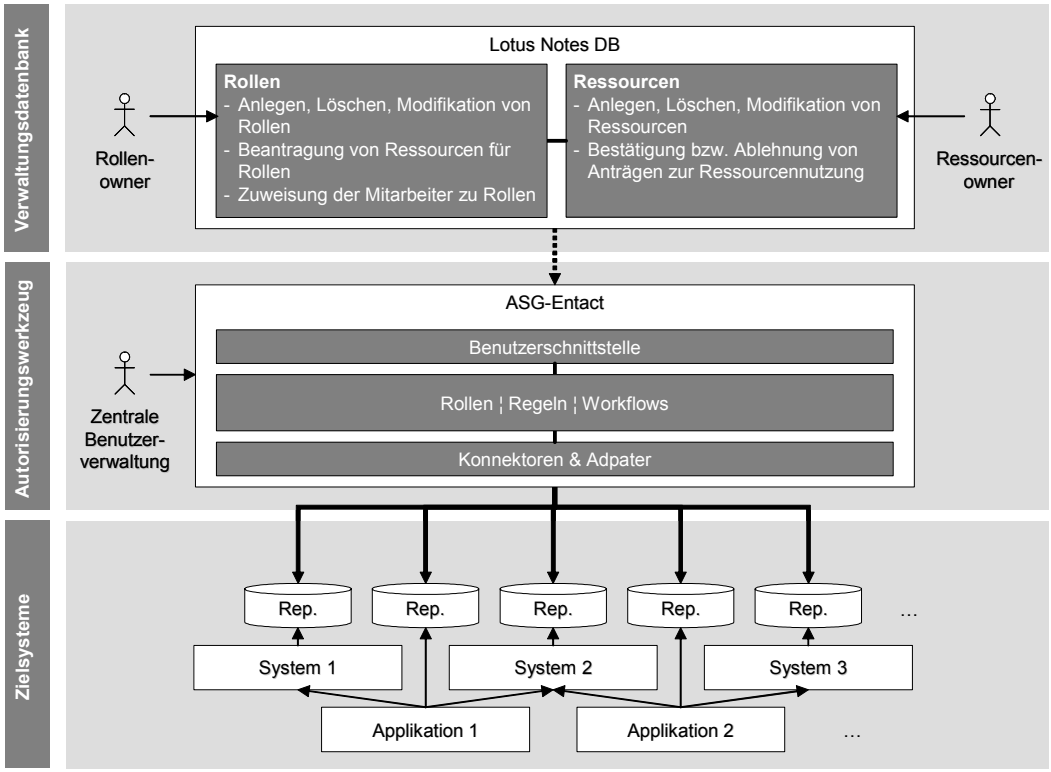

Abbildung 25: Vereinfachte Darstellung der Administrationslösung

Zur einfachen Verwaltung der Rollen und Ressourcen wurde eine Datenbank auf der Basis von Lotus Notes entwickelt (vgl. Abbildung 25). Die Rollenowner müssen dort ihre Rollen definieren und entsprechende Ressourcen sowie Mitarbeiter zuweisen. Bei der Vergabe der Rollennamen können die Rollenowner gemäss ihrer Bedürfnisse eigene Namenskonventionen verwenden. Zur Überprüfung der Rollen stellt die Datenbank eine Funktion bereit: Jedes halbe Jahr schickt das System automatisch eine Benachrichtigung an die Rollenowner, damit diese die Korrektheit der Rollen und ihrer Zuweisungen bestätigen. Durch die Betätigung einer

explizit hierfür vorgesehenen Schaltfläche im System wird die Validierung einer Rolle abgeschlossen. Die Erfassung und Aktualisierung der Ressourcen in der Notes-Umgebung erfolgt durch die Ressourcenowner. Die Ressourcen sind im Werkzeug nach den Kategorien Produktion, Integration und Test geordnet. Hauptanliegen ist es, die Ressourcen möglichst sprechend und ohne verwirrende Kodes oder technische Angaben zu hinterlegen. Bei der Zuordnung einer Ressource zu einer Rolle bekommt der Ressourcenowner eine entsprechende Benachrichtigung zugestellt. Im System kann er die Anfrage dann annehmen oder zurückweisen.

Die Mitarbeiter der zentralen Benutzerverwaltung übertragen die Rollen und die technischen Ressourcen-Kodes manuell in das Autorisierungswerkzeug ASG-Entact. Darüber hinaus werden Abläufe soweit möglich auch vollständig automatisiert. So können beispielsweise bestimmte Rollen auf der Basis hinterlegter Regeln durch das Werkzeug zugewiesen werden. Bereits existierende Benutzerinformationen wie die Kostenstellenzugehörigkeit eines Mitarbeiters werden hierbei als Grundlage verwendet. Das Werkzeug ASG-Entact ist dann auf Basis der spezifizierten Informationen in der Lage, die Berechtigungen mittels entsprechender Adapter in den Zielsystemen einzutragen.

4.3.5 Projektvorgehen zur Definition und Implementierung der Rollen

Vor der eigentlichen Definition und der anschliessenden Implementierung der Rollen erfolgte mit der Festlegung des Rollen- und Organisationskonzepts sowie der Inventarisierung der Ressourcen die Erarbeitung wesentlicher *Grundlagen*.

Im Rahmen der Definition des Rollenkonzeptes wurden vier Layer bestimmt, an denen sich die erstellten Rollen ausrichten (vgl. Tabelle 10). Auf der untersten Ebene befinden sich die „Default-Rollen“, die grundlegende Rechte für alle Mitarbeiter umfassen. Default-Rollen regeln beispielsweise den Zugriff auf das Intranet oder auf das Mailsystem. Die zweite Ebene umfasst die „Abteilungs-Rollen“, die elementare Berechtigungen für alle Mitarbeiter einer Abteilung beinhalten. Die dritte Ebene umfasst die „Standard-Rollen“, die die Berechtigungen umfassen, die mehrere Mitarbeiter einer Abteilung benötigen. Diese Mitarbeiter haben dieselben Aufgaben und vertreten sich gegenseitig. Die vierte Ebene beinhaltet die „Spezial-Rollen“, die ausgewählte, besonders kritische Berechtigungen umfassen.

Das definierte Organisationskonzept bestimmt die Aufgaben, Kompetenzen und Verantwortlichkeiten der Rollen- und Ressourcenowner (vgl. Abschnitt 4.3.4) sowie deren Herkunft und Bestimmung. Sowohl Rollen- als auch Ressourcenowner kommen aus dem Fachbereich. Die Rollenowner werden jeweils von den Abteilungs- bzw. Bereichsleitern benannt. Zurzeit sind ca. 90 Rollenowner im Unternehmen aktiv. Die Ressourcenowner sind im Rahmen ihrer Tätigkeit als Application Owner für die Applikationen des Unternehmens verantwortlich. Unterstützt werden sie dabei von den Application Supportern, die als Mitarbeiter der IT insbesondere bei informationstechnischen Fragestellungen Unterstützung bieten.

Layer	Rolle	Anwendungsbeispiele
Layer 4	Spezial-Rolle	Lohnrelevante Applikation
Layer 3	Standard-Rolle	Renten: Anfrage und Mutation
Layer 2	Abteilungs-Rolle	Abteilung Renten Abfrage
Layer 1	Default-Rolle	Intranet

Tabelle 10: Rollen im Layer-Prinzip

Vor der eigentlichen Definition der Rollen erfolgte die Inventarisierung der Berechtigungen. Alle Berechtigungen der Systeme und Applikationen wurden in Zusammenarbeit mit dem Ressourcenowner in der Lotus Notes Datenbank aufgenommen, strukturiert und mit einem sprechenden Kurztext beschrieben. Die Berechtigungen sind dort für alle Mitarbeiter des Unternehmens einsehbar.

Im Anschluss an die Erarbeitung der Grundlagen erfolgte die *Definition der Rollen*. Diese Projektphase umfasste die Auswahl der Rollenowner, die eigentliche Definition der Rollen sowie die Zuweisung von Ressourcen.

Die Auswahl der Rollenowner beinhaltete die Bestimmung der Mitarbeiter aus dem Fachbereich, die die Rollendefinition für ihren Bereich durchführen und diese im laufenden Betrieb pflegen. Nachdem den Bereichsleitern das Projekt sowie die Aufgaben der Rollenowner vorgestellt worden waren, erfolgte die Ernennung der Rollenowner durch die Bereichsleiter. Dabei wurden den Bereichsleitern solche Mitarbeiter als Rollenowner vorgeschlagen, die bereits Erfahrungen bei der Berechtigungsvergabe gesammelt hatten, über ein umfängliches fachliches Wissen verfügen und im operativen Umfeld tätig sind.

Die eigentliche Definition der Rollen erfolgte in mehreren Schritten. Zuerst bestimmten die Rollenowner die „Abteilungs-Rollen“, die jedem Mitarbeiter entsprechend seiner Zugehörigkeit zugeordnet werden. Im Anschluss hieran erfolgte die Definition der „Standard-Rollen“, die für ausgewählte Mitarbeiter einer Abteilung relevant sind. Abschliessend wurden besonders kritische Berechtigungen durch die Bildung von „Spezial-Rollen“ berücksichtigt. Die Berechtigungen der Leiter der jeweiligen Bereiche und Abteilungen wurden mit diesen besprochen und individuell festgelegt.

Nachdem die Rollenowner ihre Rollen definiert hatten, legten sie den Berechtigungsumfang der Rollen fest. Diese erste Zuweisung von Ressourcen zu Rollen wurde nicht in der Lotus Notes Datenbank durchgeführt, sondern individuell durch den Rollenowner mit dem Werkzeug seiner Wahl dokumentiert.

Im Anschluss an die Definition der Rollen erfolgte die *Implementierung der Rollen*. Die Implementierung der Rollen wurde in zwei Schritten durchgeführt. Vor der eigentlichen Implementierung stand die Pilotierung der Rollen.

Um die reibungslose Einführung der Rollen sicherzustellen, entwickelten die Rollenowner in Zusammenarbeit mit der zentralen Benutzerverwaltung Rollenpiloten. Dazu wurde jeweils ein repräsentativer Mitarbeiter einer zu implementierenden Rolle mit seinem damaligen Berechtigungsprofil detailliert analysiert. Kritisch hinterfragt wurde hierbei insbesondere, ob dieser Mitarbeiter die einzelnen Berechtigungen wirklich benötigt. Auf der Basis dieser Analyse spezifizierte der jeweilige Rollenowner in Zusammenarbeit mit der zentralen Benutzerverwaltung die Rollen mit ihren Ressourcen im Lotus Notes System. Traten beim Test der Rolle durch den ausgewählten Mitarbeiter Probleme auf, wurde die Rollenspezifikation entsprechend angepasst und erneut getestet. Für einfache Rollen dauerte die Testphase drei bis fünf Tage. Komplexe Rollen wurden bis zu einem Monat getestet.

Nach der erfolgreichen Pilotierung einer Rolle wurden alle Mitarbeiter einer Rolle entsprechend angepasst und konfiguriert. Damit war die Implementierung der Rollen abgeschlossen. Zurzeit existieren ca. 500 Rollen, die über 4'000 Mitarbeiter mit Berechtigungen versorgen (vgl. Abbildung 26).

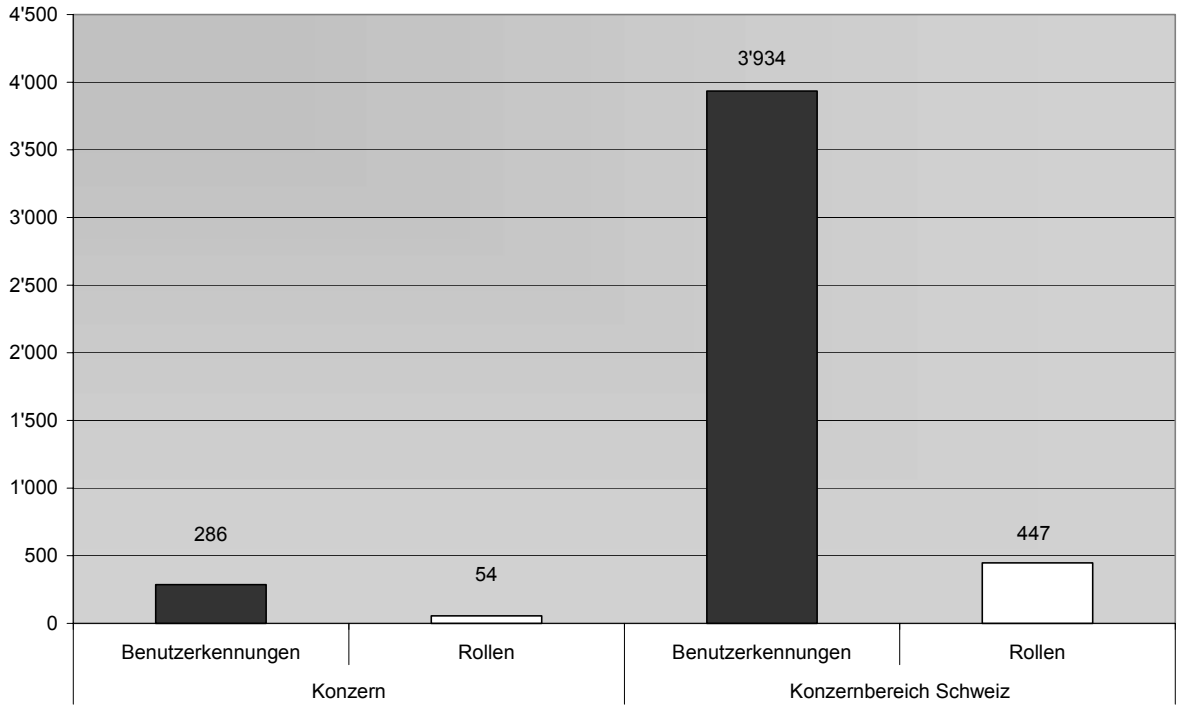

Abbildung 26: Anzahl Rollen und administrierte Benutzerkennungen bei der Basler Schweiz

4.3.6 Kritische Erfolgsfaktoren und Herausforderungen des Projektes

Ein wesentlicher Erfolgsfaktor war die *Unterstützung des Projektes* durch das Management. Da der Projektauftraggeber im Laufe des Projektes zum CIO des Unternehmens ernannt wurde, war die Unterstützung von höchster Ebene gegeben. Neben dem Interesse des Managements, das Projekt erfolgreich umzusetzen, strebte auch die zentrale Benutzerverwaltung eine schnelle, qualitativ hochwertige Umsetzung der Lösung an. Im Bereich der IT waren somit die entscheidenden Mitarbeiter am Gelingen des Projektes interessiert.

Ein weiterer zentraler Erfolgsfaktor ist die *Beteiligung der Fachabteilung* bei der Entwicklung und Wartung der Rollen. Dadurch, dass Rollen- und Ressourcenowner aus dem Fachbereich kommen, ist der Fachbereich direkt in die Lösung eingebunden. Zum einen ist hiermit die Qualität der vergebenen Berechtigungen gesichert: Nur die Mitarbeiter des Fachbereichs kennen ihre Prozesse und können beurteilen, welche Berechtigungen einem Mitarbeiter über eine Rolle zugeteilt werden müssen. Zum anderen ist dadurch auch die Akzeptanz der Lösung im Fachbereich gegeben. Durch die eigenständige Verwaltung der Rollen im Fachbereich bekommt die IT lediglich eine unterstützende und beratende Funktion. Insbesondere im Rahmen von umfangreicheren Restrukturierungen, in denen sich das eingeführte Rollenkonzept bewährt hat, erwies sich die Einbindung des Fachbereiches als sehr wertvoll.

Um Rollen- und Ressourcenowner aus dem Fachbereich zu gewinnen, ist die *Bereitschaft des Fachbereichs* notwendig, sich mit informationstechnischen Aspekten wie der Vergabe von Berechtigungen zu beschäftigen. Diese Bereitschaft und das notwendige technische Wissen, das zur Vergabe der Berechtigungen sowie zur Verwaltung der Ressourcen notwendig ist, konnte erst in den letzten Jahren aufgebaut werden.

Ein weiterer Erfolgsfaktor liegt in der Bestimmung der *Anzahl der Rollenowner*. Die Anzahl der Rollen, die ein Rollenowner definiert, ist erfahrungsgemäss weitgehend unabhängig von der Anzahl der Mitarbeiter, die ein Rollenowner mit Berechtigungen versorgt. Bei der Bestimmung der Rollenowner ist dieser Aspekt zu beachten, um nicht eine ungewollt hohe Anzahl von Rollen zu erhalten, die nur mit beträchtlichem Aufwand gepflegt werden können.

Ebenfalls von zentraler Bedeutung war die Bestimmung der *Rollenowner* für den *Aussendienst*. Um nicht für jede regionale Direktion unterschiedliche Rollen zu entwickeln, wurden zentrale Rollenowner bestimmt. Diese Rollenowner definierten Rollen, die in allen Direktionen verwendet werden.

4.3.7 Weiterentwicklung der Lösung

Die geschaffene Autorisierungslösung wird fortlaufend weiterentwickelt. Konkret sind Folgende Erweiterungen geplant:

- Erschliessung weiterer Systeme: Noch werden nicht alle Berechtigungen über die erarbeitete Lösung bewirtschaftet. Bewusst wurden zuerst die Systeme ausgewählt, die von vielen Mitarbeitern genutzt werden und einen entsprechenden Administrationsaufwand verursachen. Weitere Systeme mit Ihren Berechtigungen werden in Kürze ebenfalls integriert.

- Integration der Werkzeuge: Die zentrale Benutzerverwaltung überträgt zurzeit die in der Lotus Notes Datenbank verwalteten Rollen manuell in das Autorisierungswerkzeug ASG-

Entact. Ein weitgehend automatisierter Informationsaustausch dieser beiden Systeme ist geplant.

- Benchmarking Autorisierungswerkzeug: Das eingesetzte Autorisierungswerkzeug wird von den Analysten zur Zeit der Kategorie „Nischenprodukt“ zugeordnet. Durch die Evaluation weiterer Autorisierungswerkzeuge soll die Leistungsfähigkeit des eigenen Werkzeugs kritisch überprüft werden, um dieses ggf. zu ersetzen.

4.4 Integration der Autorisierung bei der GENERALI Gruppe Schweiz

Die folgende Fallstudie wurde ausgewählt, da im Rahmen der Fallstudie die Berechtigungen zahlreicher Systeme auf der Basis systemübergreifender Rollen verknüpft wurden. Die erarbeitete Lösung wird darüber hinaus seit mehr als zwei Jahren erfolgreich in der Praxis eingesetzt und stetig ausgebaut. Die praktizierte Vorgehensweise und das erarbeitete Lösungskonzept haben sich somit bewährt.

4.4.1 Unternehmen

Unter dem Dach der GENERALI (Schweiz) Holding sind die Lebensversicherungs-, Nichtlebensversicherungs- und Investmentaktivitäten der GENERALI Gruppe Schweiz zusammengefasst.[231] Die italienische GENERALI Gruppe übernahm 1994 die Aktienmehrheit der Holding der Fortuna Lebens-Versicherungs-Gesellschaft und benannte diese 1996 in GENERALI (Schweiz) Holding um. In den folgenden Jahren wurden weitere Unternehmen wie z.B. die Schweizer-Union-Gruppe und die Secura Versicherungen in die Unternehmung integriert.

Das Nichtlebengeschäft wird durch die GENERALI Allgemeine Versicherungen, die Fortuna Rechtsschutz-Versicherungs-Gesellschaft und die GENERALI Group Partner AG erbracht. Im Geschäftsumfeld Leben sind die GENERALI Personenversicherungen und die Fortuna Lebens-Versicherungs AG Vaduz positioniert. Vier Servicegesellschaften für das Management des Fondgeschäftes in der Schweiz und in Liechtenstein ergänzen die Marktaktivitäten.

Die GENERALI Gruppe Schweiz (vgl. Tabelle 11) konzentriert ihre Geschäftstätigkeiten auf ihre Kernkompetenzen. Im Bereich der Lebensversicherung sind dies fondsgebundene Lebensversicherungen für Privatkunden. In der Nichtlebensversicherung ist dies eine breite Palette von Versicherungslösungen für Privatpersonen sowie Klein- und Mittelbetriebe.

Nach den negativen Entwicklungen der Versicherungsbranche in den Vorjahren hat die GENERALI Gruppe Schweiz bereits 2003 wieder ein positives Gesamtergebnis erwirtschaftet. Projekte zur Konzentration der Organisation und Führung, von Standorten und Informatiksystemen haben hierzu beigetragen.

---

[231] Vgl. im Folgenden GENERALI 2005.

Kategorie	Ausprägung
Firmensitz	Adliswil, Schweiz
Branche	Versicherungen
Geschäftsbereiche	Nichtlebensversicherung Lebensversicherung
Gesellschaftsstruktur	Nichtleben: GENERALI Allgemeine Versicherungen, Fortuna Rechtsschutz-Versicherungs-Gesellschaft, GENERALI Group Partner AG Leben: GENERALI Personenversicherungen, Fortuna Lebens-Versicherungs AG Vaduz Investments: GENERALI Investment Consulting AG, Fortuna Investment AG, Fortuna Investment AG Vaduz
Bruttoprämien	1.9 Mrd. CHF
Bruttoprämien Kerngeschäft	1.3 Mrd. CHF
Gesamtergebnis	65.3 Mio. CHF
Mitarbeiter	2'063

Tabelle 11: Grundlegende Unternehmensdaten des GENERALI Konzerns Schweiz 2004[232]

4.4.2 Ausgangssituation des Projektes

Die Applikationen der GENERALI sind überwiegend Eigenentwicklungen, die in der Vergangenheit vor allem im Host-Umfeld (Bull und AS/400) entwickelt wurden. Aktuelle Eigenentwicklungen basieren auf der Client-Server-Architektur. Als relationale Datenbank wird hierbei Oracle verwendet, das unter Sun Solaris betrieben wird. Im Bereich Infrastruktur und Büroautomation setzt die GENERALI weitestgehend Standardsoftware ein. Das interne Netzwerk wird unter Microsoft Windows betrieben.

Die Systemlandschaft der GENERALI umfasst somit eine Vielzahl heterogener Systeme und Applikationen. Das Spektrum reicht dabei von etablierten, hochverfügbaren Applikationen auf der Basis von hierarchischen Datenbanken bis hin zu modernen Client-Server-Applikationen auf der Basis relationaler Datenbanken.

Durch die heterogene Systemlandschaft bedingt, existierten vor Einführung einer zentralen Sicherheitslösung zahlreiche isoliert administrierte Autorisierungslösungen. Die übergreifenden Administrationsprozesse gestalteten sich somit schwierig: Zahlreiche Stellen waren in die einzelnen Prozesse involviert, so dass entsprechend lange Prozessdurchlaufzeiten die Regel waren. Darüber hinaus war die Qualität der vergebenen Berechtigungen teilweise verbesserungswürdig. Einige Systeme enthielten beispielsweise Benutzerkonten, die Mitarbeitern zugeordnet waren, die die Unternehmung bereits verlassen hatten.

232 Vgl. GENERALI (Schweiz) Holding 2005.

Bezüglich der dargestellten Ausgangssituation wurde folgendes Verbesserungspotenzial identifiziert, das durch die Einführung einer zentralen Autorisierungslösung realisiert werden sollte:

- Steigerung von Verfügbarkeit und Produktivität: Der Einsatz einer zentralen, einheitlichen Administrationslösung reduziert den manuellen Administrationsaufwand und erhöht somit die Produktivität. Die Verwendung einer qualitativ hochwertigen Infrastrukturlösung sichert darüber hinaus die Verfügbarkeit und Qualität der Systemlandschaft.

- Senkung von Verwaltungs- und Betriebskosten: Die Erhöhung der Produktivität, die aus einer effektiveren und effizienteren Systemnutzung im operativen Tagesgeschäft hervorgeht, ermöglicht die Reduktion der Verwaltungs- und Betriebskosten.

- Sicherheits-, Komfort-, und Vertrauensgewinn: Die Anwendung von Rollen als zentrales Berechtigungskonstrukt ermöglicht die transparente und nachvollziehbare Vergabe von Berechtigungen. Dieser Zugewinn an Sicherheit erhöht das Vertrauen von Mitarbeitern und Kunden in die tägliche Geschäftsabwicklung.

- Kostenreduktion durch Konsolidierung heterogener Dienste: Durch die Einführung eines zentralen Administrationswerkzeuges können sowohl Administrationskomponenten als auch -prozesse konsolidiert, vereinfacht und standardisiert werden.

- Konkurrenzstrategie durch Leistungsdifferenzierung: Die schnelle und sichere Abwicklung von Geschäftstransaktionen ist ein wesentlicher Wettbewerbsfaktor insbesondere in der Versicherungsbranche. Die substanzielle Verbesserung der Sicherheit von Applikationen und Systemen trägt somit unmittelbar zum Erfolg des Unternehmens bei.

4.4.3 Projekt und Projektvorgehen

Das Projekt zur Einführung einer zentralen Benutzerverwaltung wurde Ende 2001 gestartet. Es setzte sich aus unterschiedlichen Unterprojekten zusammen. Das Unterprojekt „Organisation“ thematisierte die grundlegenden konzeptionellen Fragestellungen, die Einführung und Integration des Autorisierungswerkzeuges sowie die Anbindung dieses Systems an die HR- und Partner-Systeme. Das Unterprojekt „Sun Solaris“ verantwortete die Integration der Solaris-Benutzerverwaltung, der Oracle-Benutzerverwaltung und der Oracle-Applikationsverwaltung. Die Arbeitsgruppe „Windows“ setzte sich mit der Anbindung der Windows-Benutzerverwaltung auseinander, die auf den Active Directory Services aufbaut. Weitere Aspekte, die in Unterprojekten adressiert wurden, waren beispielsweise die Integration des SAP-Systems und die Anbindung der Legacy-Systeme.

Das Projektmanagement bestand aus einem Projektleiter und je einem Vertreter aus den Unternehmensbereichen GENERALI Allgemeine Versicherungen und GENERALI Personenversicherungen. Darüber hinaus war ein Mitarbeiter des Outsourcingpartners Boss Lab im

Gremium präsent. Das Projekt wurde zum einen durch das Inspektorat unterstützt, das die Perspektive der Internen Revision in das Projekt einbrachte. Zum anderen brachte Siemens Consulting Expertise in Bezug auf das eingesetzte Autorisierungswerkzeug ein. Im Steering Committee des Projektes war die IT-Leitung der GENERALI Gruppe Schweiz vertreten.

Das Projekt zur effektiveren und effizienteren Benutzerverwaltung verfolgte folgende wesentlichen Zielsetzungen:

- Zentrale und automatisierte Benutzerverwaltung: Die zu entwickelnde Lösung für die Benutzerverwaltung sollte zentral administriert werden. Darüber hinaus sollten die Administrationsprozesse weitestgehend automatisiert ablaufen.

- Umfassende Lösung: Die zu entwickelnde Lösung sollte langfristig alle Angestellten im Innen- und Aussendienst mit Berechtigungen versorgen. Darüber hinaus sollten alle bestehenden IT-Systeme der GENERALI in die Lösung integriert werden.

- Ablösung dezentraler Verwaltungsapplikationen: Durch die Einführung einer zentralen Lösung sollten die dezentralen Verwaltungsapplikationen ersetzt werden.

- Vereinfachte Authentisierung: Langfristiges Ziel war die Einführung einer Lösung für die einmalige, integrierte Authentisierung (Single Sign-on). Kurzfristig sollte durch die Verwendung gleicher Anmeldeinformationen (Benutzername und Passwort) die Authentisierung vereinheitlicht werden: Bei diesem als „Consistency Sign-on“ bezeichneten Verfahren kann ein Benutzer sich bei unterschiedlichen Applikationen mit denselben Anmeldeinformationen authentisieren.

- Standardbasierte Lösung: Die zu implementierende Lösung sollte soweit möglich auf Standards basieren. Im Bereich der rollenbasierten Autorisierung ist insbesondere der RBAC Standard[233] zu berücksichtigen. Das Repository zur Ablage der Berechtigungen und Benutzerinformationen muss dem Standard „Lightweight Directory Access Protocol (LDAP)“ entsprechen.

- Flexibel erweiterbare Lösung: Die entwickelte Lösung sollte u.a. auch auf die Projektorganisation und die Kunden der GENERALI erweiterbar sein, um die Berechtigungen aller Vertragsbeteiligten einheitlich administrieren zu können. Hierzu ist insbesondere die Integration der Web-Plattformen der GENERALI notwendig.

Das Projekt zur Umsetzung der Ziele startete im vierten Quartal 2001 mit der Vorstudie und Grob-Spezifikation erster Lösungsansätze. Ausgangspunkt waren Geschäftsanforderungen und die Analyse der Aufbau- und Ablauforganisation. Sowohl für die Aufbau- wie auch für die Ablauforganisation wurde ein so genanntes „Business Modell“ erstellt. Diese Modelle

[233] Vgl. Ferraiolo et al. 2001, S. 224ff.

dienten zur Beantwortung der Frage, wie die Ablauf- und Aufbauorganisation zur Vergabe der Berechtigungen in einem Administrationswerkzeug abgebildet werden müssen.

Im zweiten Quartal 2002 erfolgte die Evaluation von Werkzeugen, die die zentrale Administration von Berechtigungen auf der Basis von Rollen ermöglichen. Evaluiert wurden Werkzeuge von Novell, Microsoft, Siemens, Computer Associates und Critical Path. Die Projektphase wurde im dritten Quartal 2002 abgeschlossen. Der „Proof-of-Concept“ erfolgte schliesslich mit der Siemens-Lösung „DirXmetaRole“ im vierten Quartal 2002.

Im Dezember 2002 wurde der Projektantrag zur Umsetzung der Lösung bewilligt. Die detaillierte Spezifikation der Lösung und ihre Realisierung inkl. Systemaufbau und Integration erfolgte im Anschluss hieran. Die Integration umfasst neben der Anbindung der Systeme und Applikationen insbesondere auch die Integration der internen HR-Lösung LOGA, ein Standardsoftwareprodukt der Firma Personal und Informatik AG.

4.4.4 Neue Lösung

Die Prozesse der neuen zentralen Benutzerverwaltungslösung basieren insbesondere auf dem Zusammenspiel des Autorisierungswerkzeugs DirXmetaRole und des HR-Systems LOGA (vgl. Abbildung 27). Um die Vergabe der Berechtigungen zu automatisieren, müssen initial zentrale Informationen in den beiden Werkzeugen erfasst werden. Zum einen gilt es, die Organisation der Unternehmung abzubilden. Dazu werden im Autorisierungswerkzeug Rollen angelegt (A), denen system- und applikationsspezifische Berechtigungen zugeordnet werden (B). Zum anderen müssen die in DirXmetaRole spezifizierten Stellen in das HR-System exportiert werden (C). In LOGA werden die Rollen als Stellen in das systemspezifische Repository importiert. Das System bietet die Möglichkeit, die Rollen bzw. Stellen zu historisieren. Damit ist jederzeit nachvollziehbar, welcher Mitarbeiter zu welcher Zeit welche Rolle innegehabt hat.

Nachdem die grundlegenden Organisations- und Berechtigungsinformationen in den Systemen gepflegt sind, können den Benutzern Rollen zugewiesen werden. Die Erfassung der Personalien eines Mitarbeiters inkl. Stellenbesetzung erfolgt durch einen Personalmitarbeiter (1), der auch den Zeitraum der Stellenzuweisung spezifiziert. Die eingegebenen Informationen werden dann an das Autorisierungswerkzeug DirXmetaRole übertragen (2). Das Autorisierungswerkzeug legt im Weiteren für den Mitarbeiter vollautomatisch die Berechtigungen in den Systemen und Applikationen der GENERALI an (3). Dazu greift es auf die im Werkzeug hinterlegten Rollenspezifikationen zurück, die die zuzuweisenden Berechtigungen enthalten.

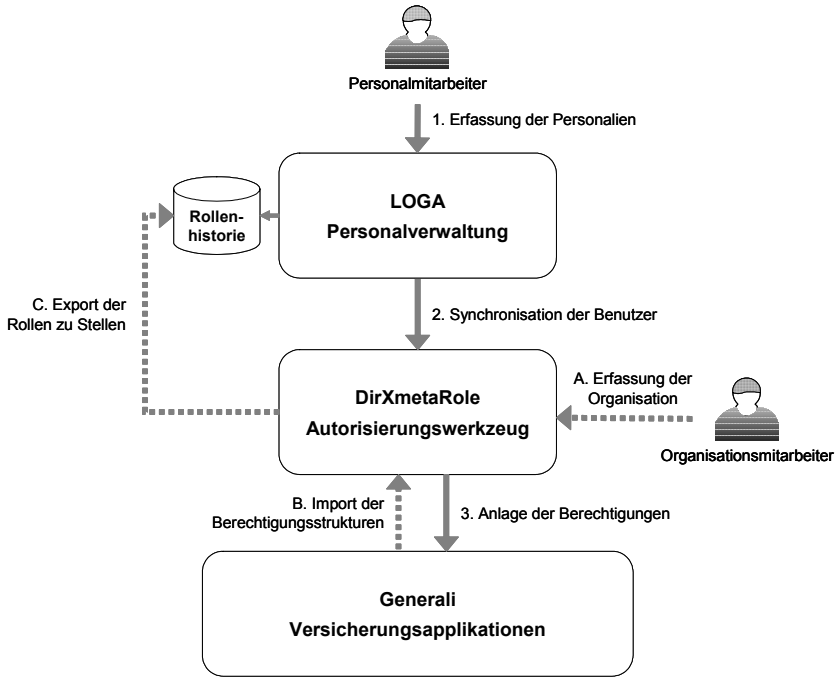

Abbildung 27: Zusammenspiel der Komponenten bei der GENERALI[234]

Die GENERALI untergliedert ihre Rollen in drei Kategorien (vgl. Abbildung 28). Rollen der Kategorie „Business Processes“ wie z.B. „Individual Life“ umfassen dabei die Berechtigungen, die im Rahmen der internen Organisation zu vergeben sind. Durch die Ausrichtung der Rollen an Prozessen bleiben Rollen bei einer Umstrukturierung der Aufbauorganisation weitestgehend unverändert. Rollen der Kategorie „Business Projects“ umfassen die Berechtigungen, die im Rahmen der Projektorganisation von Projektmitarbeitern benötigt werden. Die Kategorie „Customer Processes“ enthält die Kundenrollen, die getrennt von der internen Organisation verwaltet werden.

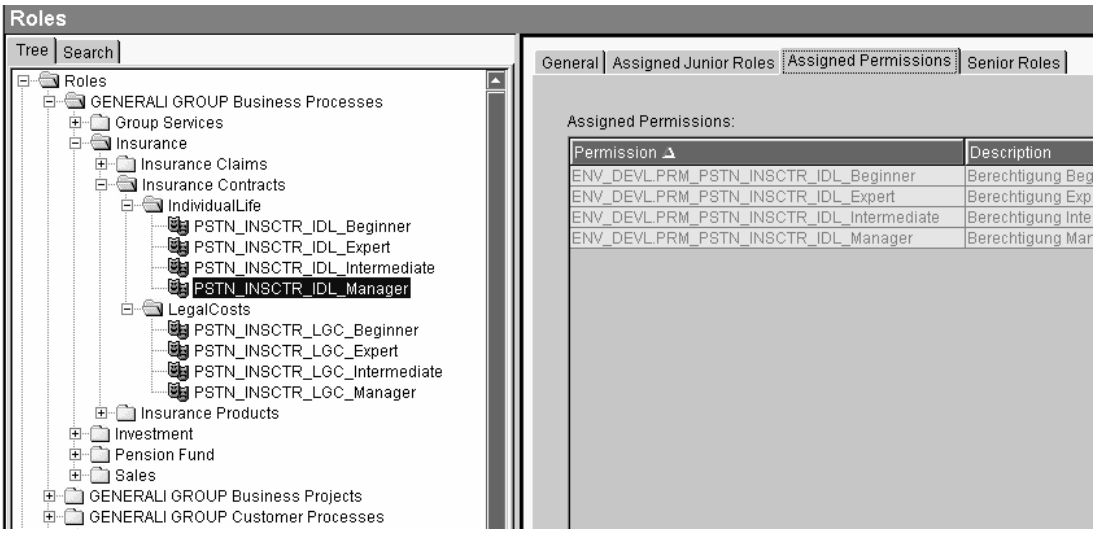

Abbildung 28: Rollen und Berechtigungen bei der GENERALI[235]

234 Vereinfachte Darstellung in Anlehnung an Lorek 2004, S. 13.
235 Vgl. Lorek 2004, S. 15.

Die Rollen der Kategorie „Business Processes“ weisen ein vierstufiges Rollenprofil auf. Rollen vom Typ „Beginner“ enthalten die grundlegenden Berechtigungen eines Bereiches. Rollen vom Typ „Intermediate“ umfassen zusätzliche Berechtigungen. Spezialisten eines Bereiches bekommen die entsprechende „Expert“-Rolle zugewiesen. Leitenden Mitarbeitern wird die Rolle „Manager“ zugeordnet.

Ein klar definiertes Vererbungskonzept legt fest, welche Berechtigungen einer Rolle an die nächsthöhere Stufe weitervererbt werden. Als „Junior Roles“ werden dabei die Rollen bezeichnet, von denen eine Rolle die Berechtigungen erbt. „Senior Roles“ sind die Rollen, die eine Rolle beerbt.

Eine Rolle umfasst Berechtigungen („Permissions“) (vgl. Abbildung 28). Die Berechtigungen selbst beinhalten Gruppen („Groups“) (vgl. Abbildung 29). Diese Gruppen entsprechen Berechtigungsbündeln wie z.B. Rollen in Oracle, die in den Systemen und Applikationen der Unternehmung vorliegen. Das einzelne System, das eine oder mehrere Gruppen beinhaltet, wird als Zielsystem („Target System“) bezeichnet. Bei der GENERALI werden drei unterschiedliche Typen von Permissions unterschieden: Permissions enthalten entweder Berechtigungen für die Produktions-, die Test- oder die Entwicklungsumgebung. Die Einbindung weiterer Umgebungen wie z.B. der Preproduction-Plattform ist möglich.

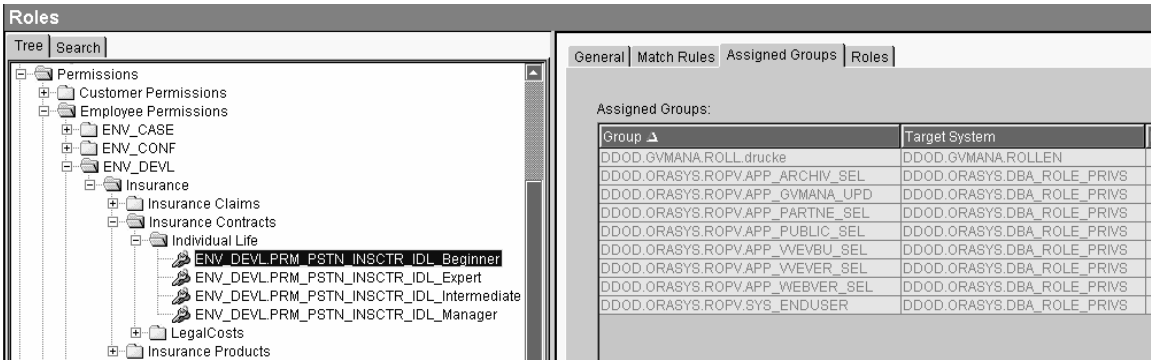

Abbildung 29: Berechtigungen und Gruppen bei der GENERALI[236]

Die Synchronisation der Zielsysteme mit dem Autorisierungswerkzeug erfolgt über die Komponente DirXmetaHub. Drei Workflows müssen pro Zielsystem spezifiziert und programmiert werden. Der „Initial-Workflow“ importiert die Gruppen der Zielsysteme in das zentrale Autorisierungswerkzeug. Der „Synchronisations-Workflow“ (vgl. Abbildung 30) aktualisiert die Berechtigungen in den Zielsystemen auf der Basis der Rollen und ihrer Zuweisungen zu Mitarbeitern. Der „Validate-Workflow“ gleicht die Einstellungen in der Autorisierungslösung mit den Zielsystemen ab.

236 Vgl. Lorek 2003, S. 16.

Abbildung 30: Synchronisations-Workflow bei der GENERALI[237]

Im Bereich der Authentisierung setzt die GENERALI auf die Synchronisation von Passwörtern (vgl. Abbildung 31). Bei einer Passwortänderung durch einen Nutzer oder einen Administrator wird diese durch eine entsprechende Komponente („Password Listener“) aufgezeichnet, verschlüsselt und an die Zielsysteme Oracle und Unix propagiert. Die Passwörter liegen im Active Directory sowie im eingesetzten LDAP-Verzeichnis des DirX-Servers verschlüsselt vor.

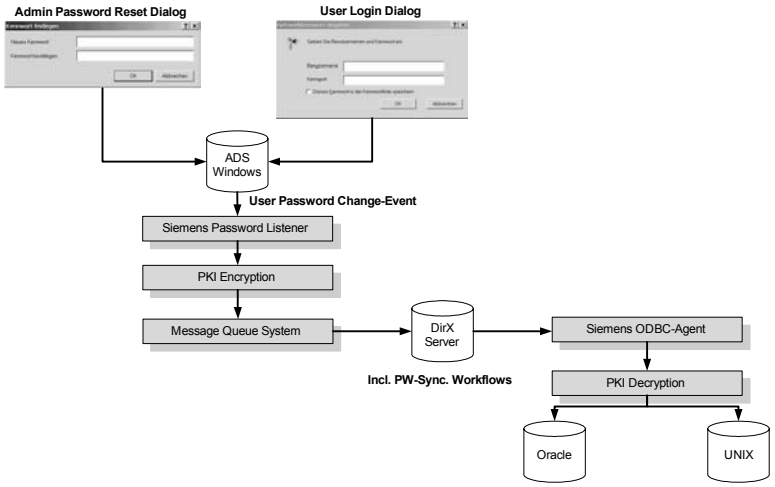

Abbildung 31: Passwort-Synchronisation bei der GENERALI[238]

4.4.5 Projektvorgehen zur Definition und Implementierung der Rollen

Nachdem das Projekt mit den einzelnen Projektphasen und der neuen Lösung im Überblick dargestellt wurde, sollen im Folgenden die wesentlichen Schritte zur Definition und Implementierung der Rollen in ihrem zeitlichen Ablauf dargestellt werden.

237 Vgl. Lorek 2003, S. 21.
238 Vgl. Lorek 2004, S. 17.

Vor der eigentlichen Definition und Implementierung der Rollen erfolgte die Spezifikation von „Business-Modellen“ im Rahmen der *Vorstudie* und die *Spezifikation erster Lösungsansätze*. Die Definition der „Business-Modelle“ der Aufbau- und Ablauforganisation beantwortete die Frage, wie die Organisation eines Unternehmens mittels technischer Strukturen abgebildet werden kann. Ausgangspunkt des Definitionsprozesses waren betriebswirtschaftliche Definitionen von Aufbau- und Ablauforganisation. Die Erstellung der Modelle berücksichtigte sowohl die primären, dauerhaften Organisationsstrukturen der Unternehmung, als auch die sekundären Organisationseinheiten der Projektorganisation. Zentrale Entität der erarbeiteten Modelle ist die Rolle („Business-Role“), die den Aufgabenträger der Aufbauorganisation mit den Aufgaben der Ablauforganisation verknüpft. Die definierten Modelle dienten als Diskussions- und Entscheidungsgrundlage zur weiteren Steuerung des Projektes.

Im Zuge der ersten Implementierungen erfolgte die *Definition der grundlegenden Konzepte*, die die Spezifikation des Rollen-, Vererbungs- und Struktur- sowie Ablaufkonzeptes umfasst.

Die Festlegung des Rollenkonzeptes umfasste die Spezifikation der Rollenkategorien „Business Processes“, „Business Projects“ und „Customer Processes“. Darüber hinaus wurde die Rollenkategorie „Business Processes“ in die vier Rollenprofile „Beginner“, „Intermediate“, „Expert“ und „Manager“ unterteilt. Die Ausrichtung der Rollen dieser Kategorie erfolgte an den Prozessen des Unternehmens.

Um eine transparente und einfache Administration zu gewährleisten, wurde im Anschluss an die Definition der Rollenkategorien ein Vererbungs- und Strukturkonzept für die „Business Roles“ definiert: Eine „Business Role“ z.B. eine „Intermediate Role“ erbt von zwei so genannten „Component Roles“. Die erste dieser „Component Roles“ enthält die Berechtigungen, die nicht an die mächtigeren Rollen „Expert“ und „Manager“ weitervererbt werden und somit alleine für die „Intermediate Rolle“ relevant sind. Die zweite „Component Role“ erbt Berechtigungen von der „Component Role“ der direkt untergeordneten Rolle und vererbt ihre Rechte weiter an die „Component Role“ der nächstmächtigeren Rolle.

Im Rahmen der Spezifikation des Ablaufkonzeptes erfolgte die Definition der Administrationsprozesse. Dabei galt es, das Zusammenspiel zwischen Administratoren und technischen Komponenten effektiv und effizient zu gestalten. In Bezug auf die Definition von Rollen musste insbesondere festgelegt werden, welche Organisationseinheiten bzw. welche Mitarbeiter für die eigentliche Rollendefinition und -implementierung verantwortlich sind.

Das erarbeitete Rollenkonzept sieht pro Unternehmensprozess vier *Rollen* vor, die es zu *implementieren* gilt. Die initiale Ausstattung dieser Rollen mit Berechtigungen geschieht durch entsprechende Mitarbeiter der IT mit Unterstützung durch den Fachbereich. Ausgangspunkt der Zuweisung sind zum Definitionszeitpunkt bereits vergebene Berechtigungen. Die Abstimmung der Berechtigungen einer Rolle erfolgt daraufhin mit dem Fachbereich. Die eigentliche Implementierung der Rollen im Administrationswerkzeug wird wiederum durch Mitarbeiter der IT vorgenommen. Neben dem Anlegen der Rolle im System und der Zuweisung

und Definition entsprechender „Permissions“ müssen ggf. so genannte „Match Rules“ spezifiziert werden. Berechtigungsrelevante, personenabhängige Eigenschaften können auf Basis dieser Regeln automatisiert Einfluss auf die Vergabe der Berechtigungen nehmen.

4.4.6 Kritische Erfolgsfaktoren und Herausforderungen des Projektes

Ein wesentlicher Erfolgsfaktor des Projektes waren die intensiven *konzeptionellen Vorarbeiten*. Vor der Auswahl des Autorisierungswerkzeugs wurde ein werkzeug-unabhängiges Lösungskonzept auf der Basis von „Business Modellen“ erstellt. Damit war eine konkrete, qualitativ hochwertige Diskussionsbasis für die Beurteilung der Lösung noch vor der eigentlichen Implementierung vorhanden. Vor- und Nachteile von Lösungsvarianten bzw. einzelne Lösungsaspekte konnten somit in einer sehr frühen Projektphase beispielsweise mit Vertretern der Revision oder des Fachbereichs diskutiert werden. Ebenfalls von zentraler Bedeutung war die anschliessende Übertragung der erarbeiteten, konzeptionellen Lösungsansätze auf das ausgewählte Autorisierungswerkzeug.

Als entscheidender Faktor stellte sich zudem die *Zusammenarbeit mit dem Fachbereich* heraus. Die erarbeiteten Rollen mit ihren Berechtigungen müssen in Zusammenarbeit mit den Fachbereichsabteilungen bestimmt werden, da diese die von ihnen abgewickelten Geschäftsprozesse am besten kennen und somit beurteilen können, welche Berechtigungen von welchem Mitarbeiter wirklich benötigt werden. Daher galt es, insbesondere die Bereichsleiter von der Vorteilhaftigkeit der zu entwickelnden Lösung zu überzeugen, damit die einzelnen Abteilungen ihren Beitrag zur erfolgreichen Umsetzung des Systems leisten.

Ein weiterer wichtiger Erfolgsfaktor war die *„Rückwärtskompatibilität“* der eingeführten Lösung: Die bestehenden Berechtigungsstrukturen der Client-Server-Systeme wurden ohne Modifikationen in die neue Lösung eingebettet. Hierdurch konnte der reibungslose Betrieb der existierenden Systeme gewährleistet werden.

4.4.7 Weiterentwicklung der Lösung

Die umgesetzte Lösung zur Autorisierung und Authentisierung wird fortlaufend weiterentwickelt. Wesentliche Erweiterungen sind:

- Erschliessung weiterer Systeme und Bereiche: Noch sind nicht alle Systeme der GENERALI in die entwickelte Lösung integriert. Mittelfristig sollen jedoch die wesentlichen Systeme über die Lösung administriert werden. Darüber hinaus sollen weitere Bereiche und Abteilungen in die Lösung eingebunden werden, so dass die Anzahl der über das System administrierten Mitarbeiter weiter steigen wird.

- Administration der Projektorganisation: Die Administration der Projektorganisation erfolgt zurzeit noch nicht über das zentrale Autorisierungswerkzeug. Die Vergabe von Be-

rechtigungen für Projektmitarbeiter soll mittelfristig ebenfalls über dieses Werkzeug abgewickelt werden.

- Realisierung Single Sign-on: Mit der Einführung der Passwort-Synchronisation ist ein wesentlicher Schritt zur Vereinfachung der Authentisierung bereits abgeschlossen. Langfristig soll durch die Implementierung einer Single Sign-on Lösung die einmalige, integrierte Authentisierung realisiert werden.

5 Ableitung der Methodengrundlagen

Im Folgenden werden wesentliche Methodengrundlagen festgelegt. Im Rahmen der Definition der Methodenelemente und -charakteristik werden einerseits die grundlegenden Elemente der zu entwickelnden Methode spezifiziert. Andererseits werden der Anspruch und die Charakteristik der Methode diskutiert. Die Methode muss zu einer effektiven und effizienten Autorisierung beitragen, so dass im Anschluss konkrete Anforderungen an die zu entwickelnde Methode abgeleitet werden. Das Kapitel endet mit der Beschreibung eines grundlegenden Metamodells, das wesentliche Entitätstypen der Domäne „Autorisierung“ in Bezug zueinander setzt.

5.1 Definition der Methodenelemente und -charakteristik

Vor der eigentlichen Ableitung der Methode werden im folgenden Abschnitt auf Basis des Methoden-Engineering zunächst die grundlegenden Elemente der Methode definiert. Anschliessend werden dann der Anspruch und die Charakteristik der zu entwickelnden Methode festgelegt.

5.1.1 Definition der Methodenelemente

Im Business Engineering stellt das Methoden-Engineering nach GUTZWILLER die Grundlage der Methodenentwicklung dar.[239] Trotz Vorliegens eines Metamodells sowie entsprechender Ausführungen kommt es bei dem Entwurf von Methoden im Kontext des St. Galler Business Engineering zu einer unterschiedlichen Verwendung der Methodenelemente. Folgende Beispiele sollen dies exemplarisch in Bezug auf die Entitäten „Aktivität“ und „Technik“ aufzeigen:

- HAFNER entwickelt in seiner Dissertation eine Methode für das Management der Informationssystemarchitektur.[240] Im Rahmen der Methodenentwicklung wird für jede Aktivität genau eine Technik entwickelt, so dass den Entitäten Aktivität und Technik im Rahmen der Dissertation eine ähnliche Bedeutung zukommt.

- KREMER definiert in seiner Dissertation eine Methode für das Information Retrieval in Portalen.[241] In seiner Arbeit werden Techniken in mehrere Aktivitäten zerlegt. Aktivitäten stellen somit die konkreten Handlungsanweisungen dar.

- SCHWINN entwickelt in seiner Dissertation eine Methode für Applikationsintegration.[242] Er baut ebenfalls auf dem Methoden-Engineering nach GUTZWILLER auf. In seiner Arbeit un-

239 Vgl. Kapitel 2.1.
240 Vgl. Hafner 2005.
241 Vgl. Kremer 2004.
242 Vgl. Schwinn 2005.

terstützt eine Technik, die die detaillierten Handlungsanweisungen zur Erstellung von Ergebnisdokumenten spezifiziert, mehrere Aktivitäten.

Eine Ursache für die unterschiedliche Verwendung der Methodenelemente liegt in deren Spezifikation. Das Modell des Methoden-Engineering, das die wesentlichen Methodenelemente und ihr Zusammenwirken aufzeigt, beinhaltet zum einen keine Kardinalitäten, so dass entsprechende Interpretationsspielräume gegeben sind. Darüber hinaus enthält es nur absolut essentielle Entitäten: Die Entität „Phase“ ist beispielsweise nicht im Modell enthalten, obwohl sie regelmässig in der Methodenentwicklung Verwendung findet. Das Metamodell des Methoden-Engineering soll daher im Folgenden geringfügig erweitert und mit Kardinalitäten versehen werden, um so die Methodenelemente und ihr Zusammenwirken verbindlich und präzise für die vorliegende Dissertation zu definieren.

Abbildung 32 zeigt das erweiterte Modell auf Basis der UML-Standardnotation[243] für Klassendiagramme.[244]

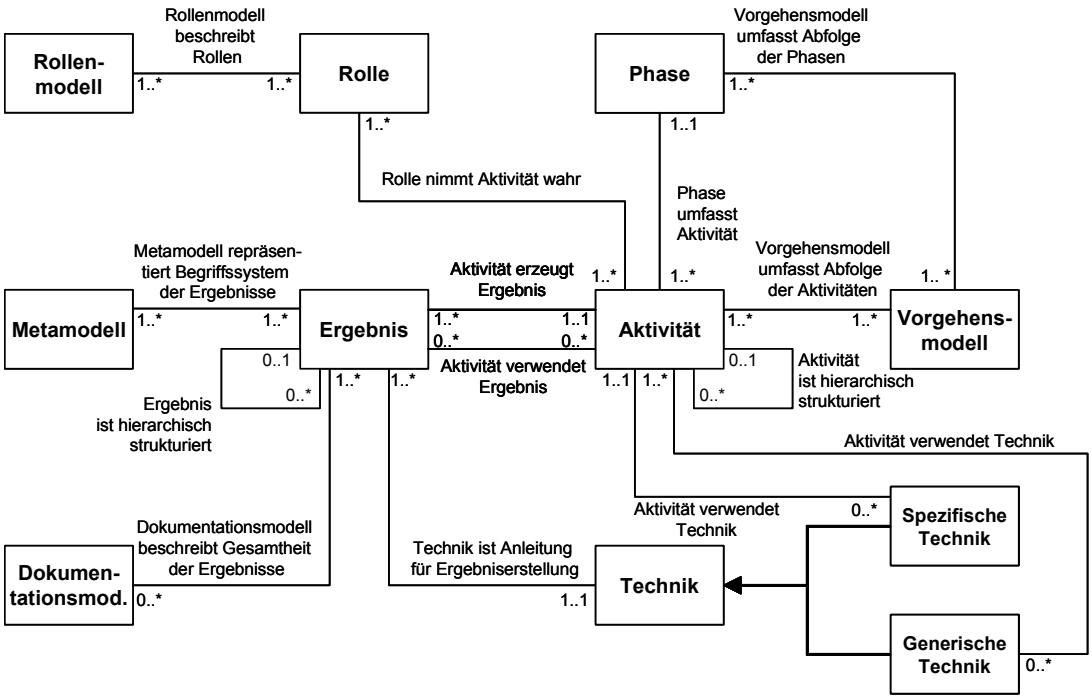

Abbildung 32: Methodenelemente der Dissertation

Folgende wesentliche Erweiterungen wurden vorgenommen:

- Aufnahme der Entität „Phase“: Eine Phase ergibt sich aus der Bündelung von Aktivitäten.[245] Der Begriff der „Phase“ geht in der Regel mit der Gruppierung von Aktivitäten

[243] Die Darstellung fusst auf der UML-Notation, da diese sich als führender Notationsstandard in Praxis und Wissenschaft etabliert hat (vgl. z.B. Balzert 2000, S. V).

[244] Zur Notation vgl. z.B. Balzert 2000, S.151 ff.

[245] In Anlehnung an Greiffenberg 2004, S. 109.

nach zeitlichen Kriterien einher.[246] Allgemein können jedoch beliebige sachlogische Kriterien zur Bündelung herangezogen werden.

- Aufnahme der Entität „Vorgehensmodell“: Das Vorgehensmodell beschreibt das Vorgehen im Grossen:[247] Es legt fest, wann welche Ergebnisse durch Aktivitäten erzeugt werden. Damit spezifiziert es die zeitliche Abfolge der Phasen mit ihren Aktivitäten.

- Aufnahme der Entität „Rollenmodell“: Das Rollenmodell beschreibt die Rollen, die an der Durchführung der Aktivitäten beteiligt sind.[248]

- Aufnahme der Entität „Dokumentationsmodell“: Die Gesamtheit aller Ergebnisse einer Methode wird durch das Dokumentationsmodell beschrieben.[249] Die wesentlichen Ergebnisse werden dazu mit ihren Beziehungen integriert dargestellt.[250] Die Beziehungen repräsentieren dabei sowohl inhaltliche als auch zeitliche Abhängigkeiten.

- Spezifikation der Beziehung zwischen „Aktivität“ und „Technik“: Während das Vorgehensmodell das Vorgehen im Grossen definiert, beschreiben Techniken das Vorgehen im Kleinen.[251] Aktivitäten spezifizieren, wann welche Ergebnisse produziert werden.[252] Techniken liefern die detaillierten Handlungsanweisungen zur Erstellung der Ergebnisse.[253] Im Rahmen seiner Spezifikation geht GUTZWILLER nicht auf die Kardinalität der Beziehung von Aktivität und Technik ein. Da ein Ergebnis im Rahmen einer Aktivität produziert wird und GUTZWILLER den Begriff der „Technik“ nach seiner Definition[254] auf ein Ergebnis bzw. zusammengehörige Ergebnisse fokussiert, bietet es sich auch aus Gründen der Komplexitätsreduktion an, den Begriff der „Technik“ aktivitätsspezifisch im Sinne einer Dekomposition[255] zu verwenden (spezifische Technik). Es kann jedoch sinnvoll sein, eine Technik im Rahmen unterschiedlicher Aktivitäten zu verwenden, beispielsweise eine universell einsetzbare Technik zur Kosten-Nutzen-Beurteilung (generische Technik).

Das erweiterte Metamodell des Methoden-Engineering dient im Folgenden als Grundlage der Methodenspezifikation.

246 Vgl. im Folgenden Greiffenberg 2004, S. 109f.
247 Vgl. Gutzwiller 1994, S. 14.
248 Vgl. Herrmann 2006, Kapitel 4.3.5.
249 Vgl. Gutzwiller 1994, S. 14.
250 Vgl. im Folgenden auch Herrmann 2006, Kapitel 4.3.3.
251 Vgl. Gutzwiller 1994, S. 14.
252 Vgl. Gutzwiller 1994, S. 14.
253 Vgl. Gutzwiller 1994, S. 14; Winter 2003b, S. 88.
254 Gutzwiller 1994, S. 14: „Techniken sind Anleitungen, wie ein Entwurfsergebnis oder eine Gruppe logisch zusammengehöriger Entwurfsergebnisse erzeugt werden.“
255 Vgl. Winter 2003b, S. 90.

5.1.2 Anspruch und Charakteristik der zu entwickelnden Methode

Um den Anspruch und Charakter der zu entwickelnden Methode festzulegen, soll ihr Profil anhand ausgewählter Merkmale des Methoden-Engineering und der Referenzprozessmodellierung verdeutlicht werden.[256] Während der Rückgriff auf das Methoden-Engineering unmittelbar einsichtig ist, soll der Bezug zur Referenzprozessmodellierung kurz begründet werden. Der Begriff der Modellierung bezeichnet den „Vorgang der Konstruktion eines Abbilds realer oder gedachter Sachverhalte […], welcher auf der Grundlage der Wahrnehmung dieser Sachverhalte durch den/die Modellierer/in erfolgt und durch den jeweiligen Modellierungszweck beeinflusst wird“[257]. Das Ergebnis der Modellierung sind Modelle. Ein Referenzmodell ist ein Modell, das zwei spezifische Merkmale aufweist:[258] Referenzmodelle sind unter bestimmten, im Modell definierten Voraussetzungen allgemeingültig, d.h. für eine Klasse von Anwendungsfällen anwendbar. Darüber hinaus besitzen sie Sollcharakter gegenüber unternehmensspezifischen Modellen. Da es sich auch bei der Spezifikation einer Methode um die Konstruktion eines Abbilds von Sachverhalten im Sinne der angeführten Definition handelt, umfasst der Begriff der Modellierung auch die Methodenentwicklung. Der Methodenbegriff impliziert darüber hinaus einen Sollcharakter sowie den Anspruch auf allgemeine Verwendbarkeit in definierten Grenzen.[259] Methoden können somit als Referenzmodelle aufgefasst werden. Diese Auffassung wird beispielsweise auch von STAHLKNECHT/HASENKAMP gestützt, die unter einem Referenzmodell „jede modellhafte, abstrahierende Beschreibung von Vorgehensweisen, Richtlinien, Empfehlungen oder Prozessen“[260] verstehen.

Die *Methodenentwicklung* kann analog zur Referenzmodellierung in die zwei Vorgänge Konstruktion und Anwendung zerlegt werden:[261] Der Konstruktionsvorgang verfolgt die Zielsetzung, eine Methode zu entwickeln, die Gültigkeit für eine Klasse von Unternehmen hat und in unterschiedlichen Situationen verwendet werden kann. Die Anwendung der konstruierten Methode erfolgt im Anschluss an den Konstruktionsprozess im jeweiligen unternehmensspezifischen Kontext. Die Anwendung umfasst Modifikationen aufgrund unternehmensspezifischer Anforderungen, die nicht durch die entwickelte Methode in Form von Varianten abgedeckt werden, sondern durch manuelle Modifikationen durch den Anwender vorgenommen werden.[262] Die in dieser Arbeit zu entwickelnde Methode konzentriert sich auf den Vorgang der Methodenkonstruktion.

Unter dem Aspekt der *Allgemeingültigkeit* wird analog zur Referenzmodellierung diskutiert, inwieweit eine entwickelte Methode von unterschiedlichen Unternehmen verwendet werden kann.[263] Im Bereich der Referenzmodellierung werden vor allem branchenspezifische und bra-

256 Die Diskussion folgt der Struktur von Herrmann 2006, Kapitel 4.
257 Winter 2003b, S. 89.
258 Vgl. Herrmann et al. 2004, S. 4.
259 Vgl. Braun et al. 2004, S. 3.
260 Stahlknecht/Hasenkamp 1999, S. 237.
261 Vgl. im Folgenden Fettke/Loos 2002, S. 10.
262 Vgl. Schütte 1998, S. 318; Herrmann 2006, Kapitel 4.3.2.9.
263 Vgl. im Folgenden vom Brocke 2003, S. 31f.

chenneutrale Anwendbarkeit unterschieden.[264] Das Kriterium der Allgemeingültigkeit ist dabei insbesondere unter konstruktivistischer Perspektive als kritisch zu betrachten, da eine objektive Anwendbarkeit konstruktivistisch nicht existiert:[265] Die Akzeptanz der Methode ergibt sich allein aus der Wahrnehmung des einzelnen Subjekts. Wenn auch die Allgemeingültigkeit einer Methode mithin nur eingeschränkt erzielt werden kann, hat die zu entwickelnde Methode dennoch einen branchenübergreifenden Allgemeingültigkeitsanspruch. Nach dem gesetzten Fokus[266] soll sie für Grossunternehmen verwendbar sein, die von heterogenen, gewachsenen Applikations- und somit auch Sicherheitslandschaften geprägt sind. Im Rahmen der Methodenentwicklung soll das Kriterium der Allgemeingültigkeit explizit im Kontext des jeweiligen Methodenbausteins thematisiert werden.

Der *Empfehlungscharakter* einer Methode beinhaltet den Anspruch, vorbildliche Eigenschaften im Sinne eines Sollvorgehens zu beinhalten.[267] GREIFFENBERG beschäftigt sich in diesem Kontext mit der Qualitätssicherung in der Methodenentwicklung.[268] Den Ausgangspunkt der Qualitätssicherung bildet die Definition von Anforderungen durch die Methodenanwender. Die angemessene Berücksichtigung der priorisierten Anforderungen sichert im Weiteren die Qualität der zu entwickelnden Methode. Problematisch erweist sich dabei wie in der Referenzmodellierung die Überprüfbarkeit des Gehalts der Empfehlung.[269] Ob ein Empfehlungscharakter vorliegt, entscheidet sich erst in der Methodenanwendung und damit in Abhängigkeit der wahrgenommenen Adäquanz der Methode unter Beachtung subjekt-, sach- und umfeldbedingter Gegebenheiten. Für die Referenzmodellierung stellt SCHÜTTE heraus, dass die Entwicklung eines Referenzmodells auf der Basis eines definierten Ziel- bzw. Anforderungssystems nur eingeschränkt möglich sei, da kein allgemeingültiges Zielsystem aufgestellt werden könne:[270] Die Ziele und insbesondere ihre Beziehungen differieren in Abhängigkeit vom Verwendungskontext des Referenzmodells erheblich. Der Empfehlungscharakter der zu entwickelnden Methode kann daher auf der Basis von Zielen und Anforderungen nur eingeschränkt sichergestellt und nachgewiesen werden. Im Rahmen dieser Arbeit soll der Allgemeingültigkeit des Anforderungssystems dadurch Rechnung getragen werden, dass die vorzunehmende Ableitung konkreter Methodenanforderungen ausschliesslich auf Basis etablierter Sicherheitsstandards erfolgt.

Die Entwicklung einer Methode kann induktiv, deduktiv oder durch Kombination beider *Erkenntnisprozesse* erfolgen.[271] Während die Deduktion auf den Gesetzen der Logik basiert und auf der Grundlage von Gesetzen und Theorien verschiedenartige Schlussfolgerungen ableitet,

264 Vgl. vom Brocke 2003, S. 98f.
265 Vgl. vom Brocke 2003, S. 31f.
266 Vgl. Kapitel 1.2.
267 Vgl. Braun et al. 2005, S. 1295ff.
268 Vgl. Greiffenberg 2004, S. 162ff.
269 Vgl. im Folgenden in Bezug auf die Referenzmodellierung vom Brocke 2003, S. 32.
270 Vgl. Schütte 1998, S. 237.
271 Vgl. Braun et al. 2005, S. 1298; in Bezug auf die Referenzmodellierung vgl. Becker et al. 2002, S. 1393.

erzielt die Induktion Erkenntnisse auf Basis von Beobachtung und Verallgemeinerung.[272] Im Rahmen der Referenzmodellierung wird die Bedeutung der Induktion hervorgehoben, die auch auf die Methodenentwicklung übertragen werden kann: Die Identifikation von Strukturanalogien bzw. Mustern bildet einen wesentlichen Ausgangspunkt, damit der Forderung nach Allgemeingültigkeit Rechnung getragen werden kann.[273] Entsprechend der Unterteilung in Struktur und Verhalten kann eine strukturelle und eine verhaltensstrukturelle Identität unterschieden werden. Im Rahmen der Methodenentwicklung sind für die Entwicklung des Vorgehensmodells und der Techniken insbesondere die verhaltensstrukturellen Identitäten von Bedeutung. Bei der Entwicklung von Referenzmodellen und Methoden spielen lediglich semantikbehaftete Strukturanalogien eine Rolle, die Identität der Strukturbausteine lässt sich also inhaltlich erklären. Die Methodenentwicklung in dieser Arbeit trägt der Bedeutung der Induktion Rechnung und basiert insbesondere auf der Verallgemeinerung von Fallstudien. Im Rahmen der Entwicklung soll jedoch auch deduktiv bzw. argumentativ vorgegangen werden, um die induktiven Erkenntnisse zu stützen und zu erweitern.

Die Wahl des geeigneten *Abstraktionsgrades* der Standardisierung ist für die Referenzmodellierung und daher auch für die Methodenentwicklung von elementarer Bedeutung.[274] Beide haben den Anspruch, allgemein verwendbare Artefakte zu entwickeln. Die angestrebte Allgemeingültigkeit bedingt die Frage, welcher Abstraktionsgrad bei der Entwicklung zu wählen ist. Eine zu ausgeprägte Konkretisierung schränkt den Anwendungsbereich des zu entwickelnden Artefakts sehr stark ein.[275] Eine zu grosse Allgemeingültigkeit verhindert mögliche Standardisierungsvorteile. Erschwert wird die Festlegung des Abstraktionsgrades durch die unterschiedlichen Adressaten des zu konstruierenden Artefakts.[276] Im Rahmen der vorliegenden Arbeit bieten sich in diesem Kontext zwei Möglichkeiten der Methodenentwicklung an: Bei der Wahl eines niedrigeren Abstraktionsgrads erfolgt die Spezifikation der standardisierten Methodenelemente bis auf die Ebene der Techniken. Einzelne Techniken werden dabei detailliert ausgearbeitet. Bei der Wahl eines höheren Abstraktionsgrades erfolgt die Spezifikation der standardisierten Methodenelemente bis auf die Ebene der Aktivitäten. Pro Aktivität wird das Spektrum möglicher Techniken aufgezeigt. Anstatt eine Technik detailliert darzustellen, werden unterschiedliche Handlungsoptionen aufgezeigt und erläutert. In der Methodenanwendung muss dann eine Handlungsoption ausgewählt und weiter ausspezifiziert werden. Im Rahmen der Entwicklung der einzelnen Methodenbausteine soll eine der beiden Optionen kontextbezogen ausgewählt werden. SCHÜTTE definiert für die Wahl des Abstraktionsgrades ein Kriterium, das auch im Rahmen dieser Arbeit verwendet wird:[277] Es ist zu untersuchen, inwieweit die Varietät der Anforderungen mit zunehmender Detaillierung proportional bzw. überproportional ansteigt. Besteht beispielsweise Konsens über das Vorgehen zur Ablei-

272 Vgl. Chalmers 1989, S. 10 ff.
273 Vgl. im Folgenden Schütte 1998, S. 237f.
274 Vgl. im Folgenden Schütte 1998, S. 235.
275 Vgl. Marent 1995, S. 312.
276 Vgl. Schütte 1998, S. 235.
277 Vgl. Schütte 1998. S. 236.

tung einer Autorisierungsarchitektur auf Ebene der Aktivitäten, so ist zu analysieren, wie gross die Unterschiede der Anforderungen bei weiterer Konkretisierung werden.[278] Sollten nahezu identische Anforderungen existieren und ähnliche Techniken im Rahmen der Aktivitäten Verwendung finden, wäre eine weitere Konkretisierung vorzunehmen. Sollten jedoch wegen unterschiedlicher Anforderungen verschiedene Techniken verwendet werden, bietet sich eine weitere Standardisierung nicht an.

Zur kontextspezifischen Anpassung einer Methode sind wie bei der Referenzmodellierung eine Vielzahl von Entscheidungen zu treffen, damit die Methode den situativen Anforderungen genügt.[279] Neben der individuellen Adaption der Methode durch den Anwender spielt hierbei die *Konfiguration* der Methode durch den Entwickler eine entscheidende Rolle.[280] Durch Adaptionsmassnahmen, die im Rahmen der Konstruktion vorgedacht werden, erfolgt die Schaffung einer Ausgangsbasis für die unternehmensspezifische Modifikation.[281] Umfangreiche Konfigurationsmöglichkeiten wie z.B. die in der Referenzprozessmodellierung diskutierte Erarbeitung von Alternativen auf der Basis von speziellen Operatoren[282], die nur im Referenzmodell gelten, bleiben im Rahmen der Dissertation aus Komplexitätsgründen unberücksichtigt. Einfache Konfigurationsmöglichkeiten, die die Angabe optionaler Aktivitäten beinhalten, werden jedoch entwickelt.

Abbildung 33 zeigt anhand der hervorgehobenen Ausprägungen die Eigenschaften der zu entwerfenden Methode zusammenfassend auf.

Merkmal	Merkmalsausprägung		
Methodenentwicklung	Konstruktion	Anwendung	
Allgemeingültigkeit	Keinen Allgemeingültigkeitsanspruch	Allgemeingültigkeitsanspruch	
Empfehlungscharakter	Istvorgehen	Sollvorgehen	
Erkenntnisprozess	Deduktion	Induktion	
Abstraktionsgrad	Gering	Hoch	Kontextabhängig
Konfiguration	Keine Konfigurationsmöglichkeiten	Einfache Konfigurationsmöglichkeiten	Umfängliche Konfigurationsmöglichkeiten

Abbildung 33: Charakteristik der zu entwickelnden Methode

278 Beispiel in Anlehnung an Schütte 1998, S. 236.
279 In Bezug auf die Referenzmodellierung vgl. vom Brocke 2003, S. 101; Herrmann 2006, Kapitel 4.3.1.2.
280 In Bezug auf die Referenzmodellierung vgl. Herrmann 2006, Kapitel 4.3.1.2.
281 In Bezug auf die Referenzmodellierung vgl. Herrmann 2006, Kapitel 4.3.1.2; Schwegmann 1999, S. 178f.
282 Vgl. z.B. Schütte 1998, S. 244ff.

5.2 Effektivität und Effizienz – Anforderungen aus dem Sicherheitsmanagement

Die Forschungsfrage „*Wie kann die Autorisierung in Unternehmen effektiv und effizient gestaltet werden?*“ kann in zwei wesentliche Problemstellungen zerlegt werden. Zum einen ergibt sich die Fragestellung, was im Kontext der Autorisierung unter Effektivität und Effizienz zu verstehen ist („WAS-Frage“). Zum anderen stellt sich die in der Forschungsfrage hervorgehobene Herausforderung, wie die geforderte Effektivität und Effizienz zu realisieren sind („WIE-Frage“).

Die Effektivität der Autorisierung bestimmt sich durch die Erreichung der Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit.[283] Diese Ziele müssen gerade vor dem Hintergrund regulatorischer Anforderungen definiert und umgesetzt werden. Das Kriterium der Effizienz fordert, dass jede Tätigkeit in ökonomischen Institutionen dem Wirtschaftlichkeitsprinzip genügen muss.[284] Dieses allgemeine Gebot, das aus dem Grundphänomen wirtschaftlicher Probleme, der Knappheit von Ressourcen resultiert, gilt auch für die Autorisierung.

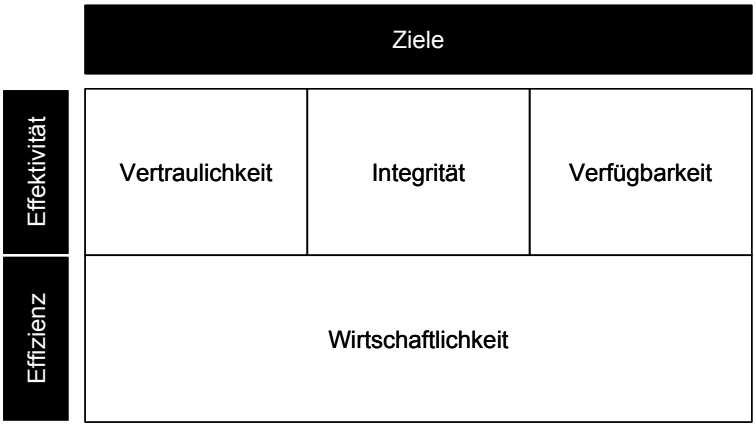

Abbildung 34: Effizienz und Effektivität der Autorisierung[285]

Zwischen den diskutierten Effektivitäts- und Effizienzzielen (vgl. Abbildung 34) bestehen Interdependenzen, die auch Zielkonflikte enthalten. Die situationsgerechte Operationalisierung und der Ausgleich der Ziele obliegen dem IT-Risikomanagement.[286] Im Folgenden werden daher Vorgehensweisen des IT-Risikomanagements vorgestellt, die unter dem Begriff „Sicherheitsmanagement“ diskutiert werden.[287] Im Rahmen des Sicherheitsmanagements wird allgemein auf Kriterienkataloge zurückgegriffen, die grundlegende Sicherheitsanforderungen u.a. für die Autorisierung spezifizieren. Im Weiteren werden nach der Diskussion verschiedener Ansätze des Sicherheitsmanagements ausgewählte Kriterienkataloge präsentiert. Abschliessend erfolgt die auf den Sicherheitskontext bezogene Ableitung konkreter Anforderungen an die zu entwickelnde Methode.

283 Vgl. hierzu auch Kapitel 2.2.
284 Vgl. im Folgenden Schütte 1998, S. 114.
285 Die Darstellung basiert auf vom Brocke 2003, S. 149.
286 Vgl. Kapitel 2.4.
287 Vgl. im Folgenden auch BITKOM 2005a, S. 6.

5.2.1 Vorgehensweisen im Sicherheitsmanagement

Seit einigen Jahren werden auf nationaler und internationaler Ebene verstärkt Anstrengungen unternommen, einheitliche Verfahren zur Gewährleistung der Sicherheit von Informationssystemen zu erarbeiten.[288] Den folgenden Ausführungen wird der ISO/EIC-Standard 13335 „Guidelines for the Management of IT Security" als ein derartiges einheitliches Verfahren zugrunde gelegt, da er weithin akzeptiert ist und die Organisation und Umsetzung von Sicherheit in Gestalt eines Leitfadens ausführlich behandelt.[289] Die breite Akzeptanz des Standards kann darauf zurückgeführt werden, dass zahlreiche europäische Länder an seiner Entwicklung beteiligt waren.

Der ISO-Standard definiert Sicherheitsmanagement als einen Prozess, der die adäquate Gewährleistung der Sicherheitsziele bezweckt: „IT Security management is a process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity and reliability."[290] Dieser Sicherheitsmanagementbegriff ist enger gefasst als der in Kapitel 2.4 definierte Begriff des IT-Risikomanagements. Während im Rahmen des IT-Risikomanagements alle Risiken, die sich allgemein aus der Verwendung von Informationssystemen ergeben, berücksichtigt werden,[291] fokussiert das Sicherheitsmanagement auf die Risiken, die sich in Bezug auf die Sicherheit von Informationssystemen ergeben. So werden etwa IT-Projektrisiken[292], die sich auf die Abwicklung von IT-Vorhaben beziehen und keinen sicherheitsrelevanten Bezug aufweisen, nicht durch das Sicherheitsmanagement adressiert.

Der zweite Teil des ISO-Standards „Managing and Planning IT Security" beschreibt die Aktivitäten des Sicherheitsmanagements,[293] die im Rahmen des Österreichischen Sicherheitshandbuches wie folgt zusammengefasst werden (vgl. Abbildung 35):[294]

- Entwicklung einer organisationsweiten IT-Sicherheitspolitik (Corporate IT Security Policy): Die organisationsweite Sicherheitspolitik umfasst die Leitlinien und Vorgaben, die die grundlegenden Ziele, Strategien, Verantwortlichkeiten und Methoden für die Gewährleistung der IT-Sicherheit festlegen.

- Risikoanalyse: Eine wesentliche Aufgabe des Sicherheitsmanagements ist das Erkennen und Einschätzen von Sicherheitsrisiken sowie deren Reduktion auf ein angemessenes Mass.

- Erstellung eines Sicherheitskonzeptes: Auf der Basis der identifizierten Risiken gilt es, Massnahmen abzuleiten, um das verbleibende Risiko auf ein angemessenes Mass zu redu-

288 Vgl. Zentrum für sichere Informationstechnologie - Austria 2004, S. 11.
289 Vgl. im Folgenden BITKOM 2005a, S. 17f.
290 Vgl. ISO 1997, Kapitel 6.
291 Vgl. Kapitel 2.4.
292 Vgl. Keil et al. 1998, S. 76ff.
293 Vgl. ISO 1997.
294 Vgl. Zentrum für sichere Informationstechnologie - Austria 2004, S. 13f.

zieren. Für komplexe IT-Systeme sollten eigene IT-Sicherheitspolitiken erarbeitet werden, die sowohl Leitlinien und Vorgaben für dieses System als auch konkrete Sicherheitsmassnahmen und ihre Umsetzung beschreiben. Im IT-Sicherheitsplan werden alle Massnahmen festgehalten und ihre Umsetzung beschrieben.

- Umsetzung eines Sicherheitsplanes: Die Umsetzung der erarbeiteten Massnahmen muss von Sensibilisierungs- und Schulungsmassnahmen begleitet werden. Darüber hinaus muss sichergestellt werden, dass die konkreten Implementierungen den erarbeiteten Leitlinien und Vorgaben genügen („Akkreditierung").

- IT-Sicherheit im laufenden Betrieb: Sicherheitsmanagement beinhaltet ebenfalls die Aufgabe, die Sicherheit im laufenden Betrieb aufrechtzuerhalten und ggf. anzupassen.

Der skizzierte Prozess kann sowohl auf eine Organisation als auch auf Teilbereiche Anwendung finden.[295]

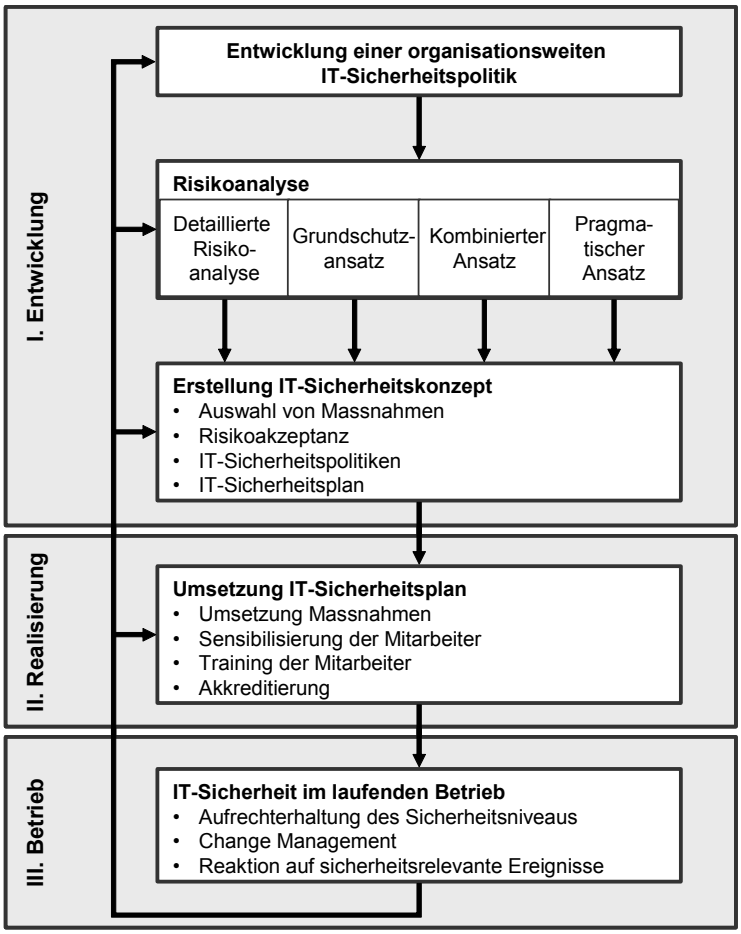

Abbildung 35: Aktivitäten im Rahmen des Sicherheitsmanagements[296]

Lediglich in der Aktivität „Risikoanalyse" unterscheidet der ISO-Standard fundamental unterschiedliche Vorgehensweisen. Differenziert werden die Detaillierte Risikoanalyse, der Grundschutzansatz, der Kombinierte Ansatz und der Pragmatische Ansatz. Letzterer wird jedoch

295 Vgl. Zentrum für sichere Informationstechnologie - Austria 2004, S. 12.
296 Vgl. Zentrum für sichere Informationstechnologie - Austria 2004, S. 12.

aufgrund seiner Problematik nicht weiter ausgeführt und findet somit z.B. im Österreichischen Sicherheitshandbuch keine Berücksichtigung. Die vier Ansätze werden im Folgenden aufgrund ihrer zentralen Bedeutung für die zu leistende Methodenentwicklung kurz vorgestellt. Im Rahmen der Anforderungsableitung wird abschliessend die Rolle der einzelnen Ansätze im Hinblick auf die zu entwickelnde Methode erläutert.

5.2.1.1 Detaillierte Risikoanalyse

Die Detaillierte Risikoanalyse (vgl. Abbildung 36) umfasst die Identifikation und Bewertung der bedrohten Objekte sowie die explizite Aufnahme und Gewichtung ihrer Bedrohungen und Schwachstellen.[297] Die Ergebnisse dieser Analyse werden dann zur Ermittlung des Risikos herangezogen, das als Ausgangspunkt der Ableitung von Schutzmassnahmen dient. Abbildung 36 zeigt die einzelnen Aktivitäten dieser Vorgehensweise.

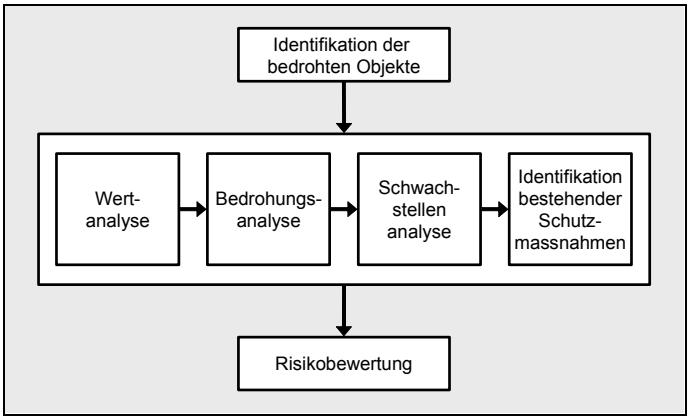

Abbildung 36: Ablauf Detaillierte Risikoanalyse[298]

Die Identifikation der bedrohten Objekte umfasst die systematische Aufnahme aller Objekte, die zu schützen sind.[299] Der Standard definiert zu schützende Objekte als die Komponenten oder Teile eines Systems, die für die Unternehmung einen unmittelbaren Wert besitzen. Darunter fallen z.B. Hardware, Software, Daten aber auch immaterielle Werte wie der Ruf der Unternehmung.

Im Rahmen der Wertanalyse erfolgt die Bewertung der bedrohten Objekte.[300] Die Bewertung sollte dabei einerseits in Zusammenhang mit den Kosten der Beschaffung und des Unterhaltes der Objekte stehen. Anderseits sollte die Bewertung die Kosten eines möglichen Verlustes an Vertraulichkeit, Integrität und Verfügbarkeit reflektieren. Die Bewertungsmethodik sollte auf der Basis von qualitativen und quantitativen Skalen stattfinden, da die durchgängige Verwendung von quantitativen Skalen in der Praxis regelmässig nicht möglich ist.

297 Vgl. ISO 1998, Kapitel 8.3.
298 Vgl. Zentrum für sichere Informationstechnologie - Austria 2004, S. 36.
299 Vgl. im Folgenden ISO 1998, Kapitel 9.3.2.
300 Vgl. im Folgenden ISO 1998, Kapitel 9.3.3.

Die Bedrohungsanalyse identifiziert und bewertet Bedrohungen und ordnet diese den Objekten zu.[301] Dabei gilt es, die Eintrittswahrscheinlichkeit einer Bedrohung z.B. auf einer qualitativen Skala zu ermitteln. Auf der Basis der Bedrohungsanalyse findet die Schwachstellenanalyse statt.[302] Die Existenz einer Schwachstelle kann nur dann zu einem Schaden führen, wenn eine Bedrohung existiert, die diese Schwachstelle ausnutzt. Daher muss für jede Schwachstelle festgehalten werden, wie wahrscheinlich es ist, dass sie durch eine Bedrohung ausgenutzt wird. Nach der Beurteilung der Bedrohungen und Schwachstellen erfolgt die Erhebung bereits umgesetzter oder geplanter Schutzmassnahmen.[303]

Auf der Basis der ermittelten Ergebnisse erfolgt die Identifikation und Bewertung der Risiken, um geeignete und gerechtfertigte Sicherheitsmassnahmen auszuwählen.[304] In die Risikobewertung gehen die Werte der bedrohten Objekte, die Eintrittswahrscheinlichkeiten der Bedrohungen und Schwachstellen sowie die vorhandenen und geplanten Schutzmassnahmen ein. Die eigentliche Bewertungsmethodik, die jederzeit nachvollziehbar und wiederholbar sein muss, wird durch den ISO-Standard nicht festgelegt.

Die Detaillierte Risikoanalyse ermittelt effektive und angemessene Sicherheitsmassnahmen.[305] Sie ist jedoch sehr ressourcenintensiv und setzt eine entsprechende Kompetenz voraus. Neben hohen Kosten kann dies auch dazu führen, dass Sicherheitsmassnahmen erst sehr spät initiiert werden.

5.2.1.2 Grundschutzansatz

Beim Grundschutzansatz erfolgt die Auswahl der Sicherheitsmassnahmen auf der Basis vorgegebener Kataloge.[306] Diese Kataloge werden von internationalen und nationalen Standardisierungsgremien zur Verfügung gestellt. Teilweise existieren auch industriespezifische Standards und Empfehlungen.

Das Vorgehen des Grundschutzansatzes kann in zwei Phasen untergliedert werden.[307] Zum einen erfolgt eine Zuordnung der umzusetzenden Grundschutzmassnahmen, zum anderen ein Soll-Ist-Vergleich der vorhandenen und empfohlenen Massnahmen. In der ersten Phase gilt es, die Massnahmen des Grundschutzkataloges auf die eigene Organisation zu übertragen. Hier muss die grundlegende Frage beantwortet werden, wo welche empfohlenen Massnahmen anzuwenden sind. Der Abgleich von empfohlenen und vorhandenen Massnahmen ergibt die Massnahmen, die noch zu implementieren sind.

---

301 Vgl. im Folgenden ISO 1998, Kapitel 9.3.4.
302 Vgl. im Folgenden ISO 1998, Kapitel 9.3.5.
303 Vgl. im Folgenden ISO 1998, Kapitel 9.3.5.
304 Vgl. im Folgenden ISO 1998, Kapitel 9.3.6.
305 Vgl. Zentrum für sichere Informationstechnologie - Austria 2004, S. 33.
306 Vgl. ISO 1998, Kapitel 9.2; Zentrum für sichere Informationstechnologie - Austria 2004, S. 46.
307 Vgl. im Folgenden Zentrum für sichere Informationstechnologie - Austria 2004, S. 47ff.

Eine Ableitung von Sicherheitsmassnahmen auf der Basis des Grundschutzansatzes erfordert im Vergleich zur Detaillierten Risikoanalyse nur einen minimalen Ressourceneinsatz.[308] Dabei decken die Grundschutzmassnahmen in der Regel die häufigsten Bedrohungen ab. Allerdings kann der Grundschutz für das analysierte System unangemessen ausfallen. Dies führt bei zu hohem Grundschutz zu einem unnötigen Verbrauch von Ressourcen. Bei zu geringem Grundschutz bleiben ggf. untragbare Risiken bestehen.

5.2.1.3 Kombinierter Ansatz

Der Kombinierte Ansatz (vgl. Abbildung 37) baut auf der Detaillierten Risikoanalyse und dem Grundschutzansatz auf.[309] In einem ersten Schritt wird dabei untersucht, welche Systeme hohe Sicherheitsanforderungen haben. Die Systeme mit den hohen Sicherheitsanforderungen werden der Detaillierten Risikoanalyse unterzogen. Alle anderen Systeme werden einer Grundschutzanalyse unterzogen. Alternativ kann auch der Grundschutz aller Systeme umgesetzt werden. Die Systeme mit hohen Sicherheitsanforderungen werden anschliessend einer detaillierten Risikoanalyse unterworfen.

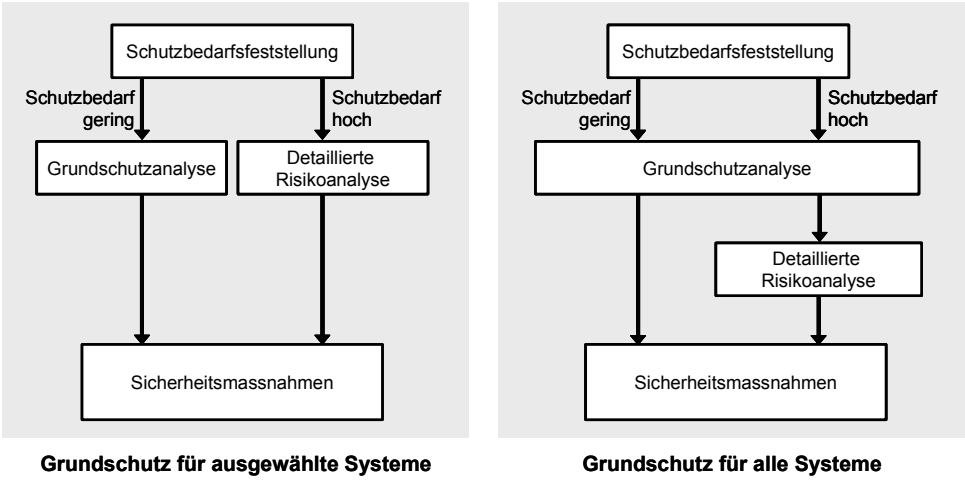

Abbildung 37: Ablauf Kombinierter Ansatz[310]

Der Vorteil der Vorgehensweise liegt darin, mit verhältnismässig wenig Aufwand ein angemessenes Sicherheitslevel für alle Systeme zu etablieren.[311] Der Grossteil der Ressourcen kann dabei für hochsicherheitsbedürftige Systeme verwendet werden. Das Verfahren findet in der Regel hohe Akzeptanz, da es mit überschaubarem Initialaufwand in kurzer Zeit sichtbare Ergebnisse liefert. Die einzige Gefahr des Ansatzes liegt in der anfänglichen Fehlklassifikation eines Systems mit hohen Sicherheitsanforderungen. Ein solches System würde dann auf der Basis von Grundschutzmassnamen nur unzureichend geschützt.

---

308 Vgl. im Folgenden Zentrum für sichere Informationstechnologie - Austria 2004, S. 46.
309 Vgl. ISO 1998, Kapitel 8.4; Zentrum für sichere Informationstechnologie - Austria 2004, S. 51.
310 Vgl. Zentrum für sichere Informationstechnologie - Austria 2004, S. 51.
311 Vgl. ISO 1998, Kapitel 8.4; Zentrum für sichere Informationstechnologie - Austria 2004, S. 52.

5.2.1.4 Pragmatischer Ansatz

Beim Pragmatischen Ansatz folgt die Risikoanalyse einer informalen, pragmatischen Vorgehensweise.[312] Der Ansatz basiert damit nicht auf definierten Methoden sondern auf der Erfahrung und dem Wissen einzelner Mitarbeiter. Er erfordert in der Regel geringen Aufwand:[313] Im Bereich Risikoanalyse muss kein neues Wissen aufgebaut werden und eine pragmatische Vorgehensweise ist schneller durchgeführt als eine detaillierte Risikoanalyse. Allerdings besteht ohne die Anwendung einer definierten, etablierten Methodik die Gefahr, Risiken nicht adäquat zu adressieren. Eine mangelhafte Identifikation und Bewertung von Risiken erschwert darüber hinaus die Rechtfertigung der aufgestellten Sicherheitsmassnahmen. Eine formale Vorgehensweise bietet darüber hinaus den Vorteil, dass subjektive Vorurteile und Wünsche Einzelner im Wege der formalen Bewertung wenigstens einer grundlegenden Prüfung unterzogen werden.

5.2.2 Anforderungen an die Autorisierung

In Bezug auf die Sicherheit von Informationssystemen und somit auch auf die Autorisierung ergibt sich eine komplexe Vorschriften- und Anforderungslage.[314] Es gibt kein einheitliches Sicherheits- oder Autorisierungsgesetz bzw. keinen einheitlichen Standard, der Prinzipien und Massnahmen abschliessend festlegt.[315] Dies stellt die Unternehmen vor Herausforderungen, da die Konsequenzen unzureichender Sicherheit schwerwiegend sein können: Neben Haftungsansprüchen drohen je nach nationaler Gesetzeslage auch steuer- und strafrechtliche Konsequenzen.[316] Geschäftsführer und Vorstände können ggf. persönlich haftbar gemacht werden, wenn sie in ihrem Unternehmen keine hinreichenden Sicherheitsmassnahmen treffen.[317]

In der Praxis hat sich eine Vielzahl von Anforderungskatalogen entwickelt, auf die insbesondere im Rahmen der Grundschutzanalyse zurückgegriffen wird. Diesen Katalogen, die auch als Sicherheitsstandards bezeichnet werden, kommt eine besondere Bedeutung zu.[318] Der Einsatz dieser Standards im Unternehmen oder in einzelnen Bereichen verbessert die sicherheitsrelevanten Prozesse zum Vorteil des Unternehmers, seiner Kunden sowie seiner Mitarbeiter. Um ggf. die Angemessenheit der getroffenen Sicherheitsmassnahmen nachzuweisen, ist darüber hinaus die Verwendung allgemein akzeptierter Sicherheitsstandards unabdingbar.

Im Rahmen einer umfassenden Untersuchung analysierte und klassifizierte der deutsche Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) im

312 Vgl. ISO 1998, Kapitel 8.2.
313 Vgl. ISO 1998, Kapitel 8.2.
314 Vgl. für Deutschland z.B. BITKOM 2005b
315 Vgl. in Bezug auf die Themenstellung Kontinuitätsmanagement vgl. von Rössing 2005, S. 38.
316 Vgl. für Deutschland z.B. BITKOM 2005b, S. 8ff.
317 Vgl. für Deutschland z.B. BITKOM 2005b, S. 5.
318 Vgl. im Folgenden BITKOM 2005a, S. 5.

März 2005 etablierte Sicherheitsstandards und -vorschriften (vgl. Abbildung 38).[319] Als bekannteste Sicherheitsstandards wurden dabei ISO/IEC 17799, BS 7799-2 und das IT-Grundschutzhandbuch identifiziert.[320] Als etablierte Standards, die Sicherheitsaspekte berücksichtigen, werden Cobit und ITIL genannt.

		Bekannteste Sicherheits-standards			IT-Standards mit Sicherheitsaspekten		Standards für spezifische Sicherheitsaspekte						Physikalische Sicherheit								Sicherheit in Produkten			Vorschriften			
		ISO 17799	BS 7799-2	IT-GSHB	Cobit	ITIL	SP 800-14	SP 800-27	IS 13569	IS 13335	IS 18044	SSE - CMM	BS I7500	EN 1047-1	EN 1047-2	DIN 4102	EN 60529	EN 1143-1	EN 1627	DIN 18095	FIPS 140-2	ITSEC	CC	KonTraG	Basel II	SOX	BDSG
Merkmale	Produktorientiert												●			●		●	●	●	●	●	●				
	Systemorientiert	●	●	●	●					●	•			●	●		●										●
	Technisch			●		·		●			●		●			•	•	●	●	●	●	●	●				•
	Organisatorisch	●	●	●	•	●	●	●	•	●		●												●	●	●	•
	Strategisch	●	●	●	●	●	●	●	●	●		●		●	●									•	•	•	
	Konzeptionell	●	●	●	●	●	●	●	●	●		•												·	·	·	
	Operationell			●	●	●	●	●				•		●	●		●	●	●						·	·	
Sonst.	Zertifizierung		✓	✓																	✓	✓	✓				
	Umfang (Seiten)	84	40	2k	75		56	21	96	206	50	120									61					66	
	Kostenpflichtig	✓	✓		✓	✓			✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓							

Legende
● Hohe Relevanz
• Mittlere Relevanz
· Niedrige Relevanz

Abbildung 38: IT-Sicherheitsstandards im Überblick[321]

Wie dargelegt, kann kein konsolidierter, universell gültiger Anforderungskatalog für die Sicherheit allgemein und die Autorisierung im Besonderen entwickelt werden. Jede Unternehmung muss die für sie relevanten Anforderungen identifizieren und konsolidieren. Mit allgemein akzeptierten Sicherheitsstandards steht den einzelnen Unternehmen jedoch eine wesentliche Ausgangsbasis zur Ableitung geeigneter Anforderungen zur Verfügung. Da diese Arbeit einen Fokus auf international tätige Grossunternehmen setzt,[322] werden zum einen in den nächsten Abschnitten die Standards ISO 17799 und BS 7799-2 sowie Cobit und ITIL mit ihren jeweiligen Aussagen zur Autorisierung vorgestellt. Gemäss der BITKOM-Analyse (vgl. Abbildung 38) sind auf diese Weise die international etabliertesten Standards berücksichtigt. Zum anderen wird der Sarbanes-Oxley Act vorgestellt und damit aktuellen Entwicklungen im Entstehungsumfeld der Dissertation Rechnung getragen.

319 Vgl. BITKOM 2005a, S. 1ff.
320 Vgl. im Folgenden BITKOM 2005a, S. 7
321 Vgl. BITKOM 2005a, S. 9. Eine Definition der einzelnen Evaluationskriterien erfolgt im Rahmen der Ausführungen des BITKOM nicht.
322 Vgl. Kapitel 1.2.

5.2.2.1 ISO/IEC 17799 und BS 7799-2

Der Standard ISO/IEC 17799 entspricht dem ersten Teil des BS (British Standard) 7799 (BS 7799-1) und trägt den Titel „Information Technology – Code of Practice for Information Security Management“.[323] Der Standard wurde in Grossbritannien zwischen 1995 und 2000 entwickelt. Eine Gruppe von Praktikern hat dabei in mehrjähriger Arbeit einen Kriterienkatalog zusammengestellt, der zur Beurteilung und Verbesserung der Sicherheit von Informationssystemen herangezogen werden kann.

Der Standard besteht aus 127 Kontrollzielen, die in 10 Kapiteln beschrieben werden.[324] Jedes der 127 Kontrollziele wird dabei weiter operationalisiert und detailliert beschrieben. Der Standard versteht sich als Ausgangpunkt für die Entwicklung organisationsspezifischer Regelungen. Nicht alle spezifizierten Kontrollziele müssen für eine Unternehmung relevant sein. Darüber hinaus sind in einer Unternehmung ggf. weitere Kontrollziele zu berücksichtigen.

Der Standard BS 7799-2 „Information Security Management System – Specification with Guidance for Use“ umfasst ebenfalls die 127 Kontrollziele des ISO/IEC 17799. Dabei wird jedoch auf eine ausführliche Darstellung der Kontrollziele verzichtet und auf den Standard ISO/IEC 17799 verwiesen.[325] Neben den Kontrollzielen spezifiziert der Standard ein Modell für den Aufbau und das Management eines Informationssicherheitsmanagementsystems (ISMS). Das ISMS umfasst Organisationsstrukturen, Weisungen, Planungsaktivitäten, Verantwortlichkeiten, Verfahren, Methoden, Prozesse und Ressourcen.[326] Ziel des ISMS ist es, die Sicherheit von Informationssystemen auf der Basis von Geschäftsrisiken zu gewährleisten und zu verbessern.

BS 7799-2 ist bisher lediglich ein britischer Standard, der sich aber international weitgehend durchgesetzt hat und daher in naher Zukunft ebenfalls den Status einer ISO-Norm erhalten wird.[327] Aufgrund der engen methodischen Anlehnung an den Qualitätsmanagementstandard ISO 9000 und wegen der weltweiten Akzeptanz werden ISO 17799 und BS 7799-2 als Qualitätsstandards für das Management der Informationssicherheit bezeichnet.

Die 127 Kontrollziele der beiden Standards werden in den zehn Kernkapiteln zusammengefasst:[328]

Kapitel	Titel	Beschreibung
Kapitel 3	Security Policy	Das Kapitel „Security Policy“ setzt sich mit der Definition grundlegender Sicherheitsleitlinien in Form von Sicherheitspolitiken auseinander.

323 Vgl. im Folgenden Vossbein 2002, S. 25f; BITKOM 2005a, S. 11.
324 Vgl. im Folgenden ISO 2000a, S. xi.
325 Vgl. im Folgenden British Standards Institution 2002, Kapitel 0.
326 Vgl. im Folgenden British Standards Institution 2002, Kapitel 3.2.
327 Vgl. im Folgenden BITKOM 2005a, S. 11.
328 Vgl. Vossbein 2002, S. 27ff.

Kapitel 4	Organizational Security	Das Kapitel „Organizational Security“ widmet sich der Regelung organisatorischer Sicherheitsaspekte.
Kapitel 5	Asset Classification and Control	Im Rahmen des Kapitels „Asset Classification and Control“ wird die Klassifikation und Bewertung der bedrohten Objekte ebenso wie die Schaffung klarer Objektverantwortlichkeiten thematisiert.
Kapitel 6	Personnel Security	Das Kapitel „Personnel Security“ umfasst Massnahmen zur personellen Sicherheit von Stellenbeschreibungen über Schulungen bis hin zu Verhaltensweisen bei Sicherheitsvorfällen.
Kapitel 7	Physical and Environmental Security	Das Kapitel „Physical and Environmental Security“ widmet sich der Sicherung der physischen Infrastruktur insbesondere auch der Gebäudesicherheit eines Unternehmens.
Kapitel 8	Communications and Operations Management	Mit dem Betrieb von Informationssystemen beschäftigt sich das Kapitel „Communications and Operations Management“.
Kapitel 9	Access Control	Das Kapitel „Access Control“ adressiert die Themenstellung Zugriffskontrolle.
Kapitel 10	Systems Development and Maintenance	Im Rahmen des „Systems Development and Maintenance“ werden die Entwicklung und Wartung von Informationssystemen behandelt.
Kapitel 11	Business Continuity Management	Das Kapitel „Business Continuity Management“ beschreibt Massnahmen zur Aufrechterhaltung des Geschäftsbetriebs.
Kapitel 12	Compliance	Mit der Einhaltung gesetzlicher, behördlicher und vertraglicher Verpflichtungen setzt sich das abschliessende Kapitel „Compliance“ auseinander.

Tabelle 12: Aufbau ISO/IEC 17799

Das Kapitel „Access Control“ widmet sich ausschliesslich der Autorisierung. Tabelle 13 gibt die Kontrollziele dieses Kapitels in gekürzter Form wieder:[329]

9.1 Business requirements for access control
Objective: To control access to information Access to information and business processes should be controlled on the basis of business and security requirements. This should take account of policies for information dissemination and authorisation.
9.2 User access management
Objective: To prevent unauthorised access to information systems Formal procedures should be in place to control the allocation of access rights to information systems and services. The procedures should cover all stages in the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate to the need to control the allocation of privileged access rights that allow users to override system controls.
9.3 User responsibilities
Objective: To prevent unauthorised user access The co-operation of authorised users is essential for effective security. Users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.
9.4 Network access control
Objective: Protection of networked services Access to both internal and external networked services should be controlled. This is necessary to ensure that users who have access to networks and network services do not compromise the security of these network services […].

329 Vgl. ISO 2000b, Kapitel 9.

9.5 Operating system access control
Objective: To prevent unauthorised computer access Security facilities at the operating system level should be used to restrict access to computer resources. […]
9.6 Application access control
Objective: To prevent the unauthorised access to information held in information systems. Security facilities should be used to restrict access within application systems. Logical access to software and information should be restricted to authorised users. […]
9.7 Monitoring system access and use
Objective: To detect unauthorised activities Systems should be monitored to detect deviation from access control policy and record monitorable events to provide evidence in case of security incidents. System monitoring allows the effectiveness of controls adopted to be checked and conformity to an access policy model to be verified.
9.8 Mobile computing and teleworking
Objective: To ensure information security when using mobile computing and teleworking facilities The protection required should be commensurate with the risks these specific ways of working cause. When using mobile computing the risks of working in an unprotected environment should be considered and appropriate protection applied. In the case of teleworking the company should apply protection to the teleworking site and ensure that suitable arrangements are in place for this way of working.

Tabelle 13: ISO/IEC 17799 Kontrollziele mit direktem Bezug zur Autorisierung

5.2.2.2 Control Objectives for Information and Related Technology

Zur Unterstützung des Managements wurde mit den Control Objectives for Information and Related Technology (Cobit) von der ISACA (Information Systems Audit and Control Association) ein umfangreiches Kontrollsystem entwickelt.[330] Cobit berücksichtigt die Aspekte des IT-Einsatzes von der Planung über den Betrieb bis zur Entsorgung und nimmt somit eine umfassende Sicht auf die IT ein. Ziel der ISACA ist es, Unternehmen bei der Organisation, Kontrolle, und Qualitätssicherung von Informationen, Systemen sowie Technologie durch die Bereitstellung von Forschungsarbeiten, Standards und Praktiken zu unterstützen.[331] Im Rahmen dieser Zielsetzung wurde Cobit 1996 erstmals von der ISACA veröffentlicht und seitdem ständig aktualisiert.[332]

Das Cobit-Framework unterscheidet vier Domänen.[333] Diesen sind insgesamt 34 kritische Prozesse zugeordnet. Die Domäne „Planung und Organisation“ widmet sich strategischen und taktischen Aspekten, die sich aus der Verwendung von Informationstechnologie ergeben. Um die IT-Strategie umzusetzen, müssen IT-Lösungen identifiziert, entwickelt oder beschafft und implementiert sowie integriert werden. Dieser Themenkomplex wird durch die Domäne „Beschaffung und Implementation“ adressiert. Die Domäne „Betrieb und Unterstützung“ betrifft die effektive Bereitstellung der gewünschten Dienstleistungen. Die Domäne „Überwachung“ beschäftigt sich schlussendlich mit der Sicherstellung der Qualität der IT-Prozesse.

330 Vgl. im Folgenden BITKOM 2005a, S. 14.
331 Vgl. Hochstein/Hunziker 2003, S. 50.
332 Vgl. ISACA Switzerland Chapter 2001, A 1.
333 Vgl. im Folgenden ISACA Switzerland Chapter 2001, B 4.

Für jeden der 34 kritischen Prozesse werden Kontrollziele angegeben, mit derer Hilfe die Erfüllung der Geschäftsanforderungen überwacht wird.[334] Darüber hinaus sind seit der dritten Cobit-Auflage für jeden Prozess Kernziele (key goal indicators), kritische Erfolgsfaktoren (critical success factors) sowie messbare Leistungsindikatoren (key performance indicators) aufgeführt.[335]

Vier der 34 Prozesse weisen einen unmittelbaren Bezug zur Sicherheit von Informationssystemen auf:

- Sicherstellung der Einhaltung externer Anforderungen: Der Prozess setzt sich mit der Identifikation und Analyse externer Anforderungen hinsichtlich ihrer Auswirkungen auf die IT sowie mit der Ergreifung geeigneter Massnahmen auseinander. [336] Der Prozess ist der Domäne „Planung und Organisation“ zugeordnet.

- Risikobeurteilung: Die Risikobeurteilung setzt sich mit der Identifikation von IT-Risiken, der Analyse von Auswirkungen und dem Ergreifen von Massnahmen zur Verminderung der Risiken auseinander.[337] Der Prozess ist der Domäne „Planung und Organisation“ zugeordnet.

- Sicherstellen der kontinuierlichen Dienstleistung: Der Prozess gewährleistet die Sicherstellen der Verfügbarkeit der IT-Dienste und ist der Domäne „Auslieferung und Unterstützung“ zugeordnet.[338]

- Sicherstellen der Systemsicherheit: Der Prozess stellt den Schutz von Informationen vor unberechtigter Verwendung, Aufdeckung oder Änderung sicher und ist der Domäne „Auslieferung und Unterstützung“ zugeordnet.[339]

Der Prozess „Sicherstellen der Systemsicherheit“ nimmt explizit auf Aspekte der Autorisierung Bezug. Tabelle 14 stellt die direkt betroffenen Kontrollziele in gekürzter Form dar:[340]

AU 5.1: Handhabung von Sicherheitsmassnahmen
IT-Sicherheit sollte so gehandhabt werden, dass die Sicherheitsmassnahmen mit den Geschäftsanforderungen in Einklang stehen. […]
AU 5.2: Identifikation, Authentisierung und Zugriff
Der logische Zugriff auf und die Verwendung von IT-Rechnerressourcen sollte durch die Einführung von angemessenen Identifikations-, Authentisierungs- und Autorisierungsmechanismen beschränkt werden, welche Benutzer und Ressourcen mit Zugriffsregeln verknüpft. […]

334 Vgl. Hochstein/Hunziker 2003, S. 50f.
335 Vgl. ISACA Switzerland Chapter 2001, S. 15.
336 Vgl. ISACA Switzerland Chapter 2001, C. 19.
337 Vgl. ISACA Switzerland Chapter 2001, C. 21.
338 Vgl. ISACA Switzerland Chapter 2001, C. 53.
339 Vgl. ISACA Switzerland Chapter 2001, C 57.
340 Vgl. ISACA Switzerland Chapter 2001, C 57f.

AU 5.3: Sicherheit des Direktzugriffs auf Daten
In einer Online-IT-Umgebung sollte das IT-Management in Einklang mit dem Sicherheitskonzept Verfahren zur Bereitstellung einer Zugriffskontrolle implementieren, welche auf der erwiesenen Notwendigkeit der einzelnen Person basiert, Daten einzusehen, hinzuzufügen, zu ändern oder zu löschen.
AU 5.4: Verwaltung der Benutzerkonten
Das Management sollte Verfahren einrichten, um ein rechtzeitiges Handeln bezüglich Anforderung, Einrichtung, Herausgabe, Suspendierung und Schliessung von Benutzerkonten sicherzustellen. […]
AU 5.5: Überprüfung der Benutzerkonten durch das Management
Das Management sollte einen Kontrollprozess implementiert haben, um Zugriffsrechte periodisch zu überprüfen und zu bestätigen. […]
AU 5.6: Überprüfung der Benutzerkonten durch die Benutzer
Benutzer sollten systematisch die Aktivität ihrer eigenen Benutzerkonten kontrollieren. […]
AU 5.9: Zentrale Verwaltung von Identifikation und Zugriffsrechten
Kontrollen sind vorhanden, um sicherzustellen, dass die Identifikation und Zugriffsrechte von Benutzern, ebenso wie die Identität von System- und Dateneignern eindeutig und zentral eingerichtet und verwaltet werden, um Konsistenz und Wirtschaftlichkeit des globalen Zugriffsschutzes zu erlangen.
AU 5.10: Rapportierung von Verstössen und Sicherheitsaktivitäten
Die IT-Sicherheitsadministration sollte gewährleisten, dass regelmässig Verstösse und Sicherheitsaktivitäten protokolliert, gemeldet, überprüft und geeignet eskaliert werden, um Vorfälle mit unberechtigten Aktivitäten zu identifizieren und abzuklären. Der logische Zugriff auf Nachvollziehbarkeitsinformationen der Rechnerressourcen (Sicherheits- und andere Protokolle) sollte basierend auf dem Prinzip des „least privilege“ oder „need-to-know“ gewährt werden.

Tabelle 14: Cobit Kontrollziele mit direktem Bezug zur Autorisierung

5.2.2.3 IT Infrastructure Library

Ende der 80er Jahre entwickelte die Central Computer and Telecommunications Agency (CCTA) der britischen Regierung in Zusammenarbeit mit IT-Spezialisten, Rechenzentrumsbetreibern und Beratern die IT Infrastructure Library (ITIL) ein Referenzmodell für die Planung, Überwachung und Steuerung von IT-Leistungen.[341] Im Laufe der Zeit hat sich ITIL zum internationalen De-facto-Standard für IT-Dienstleister entwickelt. ITIL bildet als Sammlung von „Best Practices“ die Grundlage des international agierenden IT-Service-Management Forum (ITSMF), das mittlerweile mehr als 1.000 Partnerunternehmen aufweist. Das Framework wird durch Anwender, Berater und Hersteller kontinuierlich weiterentwickelt.

ITIL besteht im Wesentlichen auf fünf Prozessbereichen, die jeweils von einem ITIL-Band behandelt werden:[342]

- Die „Business Perspective“ behandelt die strategischen Prozesse des IT-Servicemanagements. Dazu gehören beispielsweise IT-Alignment oder Relationship Management.

- Das „Service Delivery“ umfasst die Planung, Überwachung und Steuerung von IT-Leistungen.

341 Vgl. Hochstein/Hunziker 2003, S. 47.
342 Vgl. Hochstein/Hunziker 2003, S. 47f.

- Das „Service Support“ thematisiert die Umsetzung der Serviceprozesse und den User-Support im Rahmen der Leistungsbereitstellung.

- Das Lebenszyklus-übergreifende Management von Applikation wird durch das „Application Management“ adressiert.

- Sämtliche Aspekte des Infrastrukturmanagements werden durch das „ICT Infrastructure Management“ behandelt.

Neben diesen Kernbereichen adressiert ITIL mit dem Band „Security Management“[343] auch die Themenstellung Sicherheitsmanagement. Dieser ITIL-Band behandelt das Thema Sicherheitsmanagement insbesondere auf der Basis der Prozessbereiche „Service Delivery“ und „Service Support“.[344] Wie dargelegt, gehört der ITIL-Band jedoch nicht zu den Kernelementen des Standards. Im Kontext aller ITIL-Publikationen kommt dem Thema Sicherheitsmanagement daher eine untergeordnete Rolle zu. Dies schlägt sich beispielsweise auch darin nieder, dass ITIL keine eigenen IT-Sicherheitsmassnahmen definiert.[345] Der Standard bezieht sich hier vielmehr auf die Massnahmen von BS 7799 bzw. ISO/IEC 17799.

5.2.2.4 Sarbanes-Oxley Act

Der Sarbanes-Oxley Act (SOX) ist ein US-amerikanisches Gesetz, welches am 23. Januar 2002 als Reaktion auf diverse Finanzskandale von Firmen wie z.B. Enron oder Worldcom erlassen wurde.[346] Der Name des Gesetzes geht auf die beiden Senatoren Sarbanes und Oxley zurück, die massgeblich an dessen Entwicklung beteiligt waren. Ziel des Gesetzes ist es, Investoren durch eine genaue und verlässliche Rechnungslegung zu schützen und entsprechendes Vertrauen wiederzugewinnen. Das Gesetz regelt die Zusammenarbeit zwischen Wirtschaftsprüfern und Unternehmensleitung und verlangt darüber hinaus von den Unternehmen den Nachweis, dass sie über ein funktionsfähiges internes Kontrollsystem verfügen. Die Regelungen des Gesetzes betreffen die Unternehmen, die an einer amerikanischen Wertpapierbörse notiert sind. Unter Umständen sind auch deren Tochterfirmen betroffen.[347]

Aus der Perspektive der Sicherheit von Informationssystemen ist insbesondere die Sektion 404 des Sarbanes-Oxley Act relevant.[348] Hierbei wird auf die Managementverantwortung zur Einrichtung und zum Betrieb von angemessenen internen Kontrollen und Prozessen zum Finanz-Reporting hingewiesen. Bezüglich der Rolle von Informationstechnologie und Informationssystemen stellen die verantwortlichen Behörden fest: „The nature and characteristics of a

343 Cazemier 1999.
344 Vgl. im Folgenden BITKOM 2005a, S. 16.
345 Vgl. BITKOM 2005a, S. 16.
346 Vgl. BITKOM 2005a, S. 23.
347 Vgl. BITKOM 2005a, S. 23.
348 Vgl. im Folgenden BITKOM 2005a, S. 23.

company's use of information technology in its information system affect the company's internal control over financial reporting".[349]

Die Kontrollen müssen nach den Regelungen der amerikanischen Börsenaufsicht SEC (Securities and Exchange Commission) auf der Basis eines anerkannten Kontrollstandards erfolgen.[350] Das hierzu empfohlene COSO (Committee of Sponsoring Organizations of the Treadway Commission) Framework adressiert die Verwendung von Informationssystemen jedoch nur ansatzweise. SEC und PCAOB (Public Company Accounting Oversight Board) fordern daher IT-Kontrollen ein, die über die grobgranularen COSO-Kontrollen hinausgehen. Um den Forderungen der SEC bezüglich anerkannter Kontrollstandards nachzukommen, empfiehlt sich auch im IT-Umfeld die Verwendung von Standards wie ISO/IEC 17799, Cobit oder ITIL. Gegenstand und Ausmass der Kontrollen müssen jedoch dem Kontext der jeweiligen Unternehmung angemessen sein, so dass die Ausgestaltung der IT-Kontrollen individuell vom Unternehmen vorzunehmen ist.[351]

5.2.3 Anforderungen an die zu entwickelnde Methode

Auf Basis der Aktivitäten des Sicherheitsmanagements und der unterschiedlichen, diskutierten Sicherheitsstandards werden im Folgenden Anforderungen entwickelt, die im Zuge der Arbeit bei der Ableitung der zu entwickelnden Methode herangezogen werden.

Die Methode soll auf etablierten Ansätzen aufbauen, die eine adäquate Adressierung der Sicherheitsziele gewährleisten. Die Methode widmet sich insbesondere der konzeptionellen Entwicklung von Autorisierungsarchitekturen und Berechtigungskonzepten, so dass die Entwicklungsaktivitäten des Sicherheitsmanagements die relevante Ausgangsbasis bilden. Aus den Entwicklungsaktivitäten des Sicherheitsmanagements können folgende Methodenanforderungen abgeleitet werden:

Aktivität des Sicherheitsmanagements	Anforderung an die Methode	Beschreibung der Anforderung
Entwicklung einer organisationsweiten IT-Sicherheitspolitik	Berücksichtigung existierender Sicherheitsleitlinien und -vorgaben	Die Entwicklung einer organisationsweiten IT-Sicherheitspolitik ist nicht Gegenstand der zu entwickelnden Methode. Die Methodik muss jedoch existierende Sicherheitsleitlinien und -vorgaben berücksichtigen.
Risikoanalyse	Durchführung einer Risikoanalyse	Im Rahmen der zu entwickelnden Methodenbausteine, gilt es, Risiken systematisch zu adressieren. Je nach Situation sollte die Detaillierte Risikoanalyse, der Grundschutzansatz oder der Kombinierte Ansatz verwendet werden.[352] Der Pragmatische Ansatz ist aufgrund seiner Schwächen nur mit Vorbehalt zu verwenden.[353]

349 Vgl. IT Governance Institute 2004, S. 12.
350 Vgl. im Folgenden IT Governance Institute 2004, S. 49.
351 Vgl. IT Governance Institute 2004, S. 8.
352 Vgl. Kapitel 5.2.1.
353 Vgl. Kapitel 5.2.1.4.

Erstellung eines IT-Sicherheitskonzeptes	Ableitung angemessener Massnahmen	Auf Basis der identifizierten Risiken gilt es, Massnahmen abzuleiten, um das verbleibende Risiko auf ein angemessenes Mass zu reduzieren. Kosten und Nutzen einer Massnahme müssen in einem angemessenen Verhältnis stehen.
	Definition von Leitlinien (optional)	Für komplexe IT-Systeme sollten eigene Leitlinien erarbeitet werden, die konkrete Handlungsanleitungen darstellen.

Tabelle 15: Anforderungen an die Methode

In die Methodenentwicklungen fliessen ausgewählte Anforderungen der dargestellten Anforderungskataloge ein. Die zu entwickelnde Methodik selbst wird jedoch nicht auf einem spezifischen Anforderungskatalog aufsetzen, da mehrere etablierte Kataloge existieren[354] und eine Fokussierung zu einer unnötigen Einschränkung führen würde. Die bei der Methodenanwendung zu verwendenden Kataloge ergeben sich vielmehr aus der abgeleiteten Anforderung „Berücksichtigung existierender Sicherheitsleitlinien und -vorgaben“ (vgl. Tabelle 15): Im Rahmen der Methodenanwendung sollten die Kataloge zugrunde gelegt werden, die bereits unternehmensweit eingesetzt oder durch die sicherheitsverantwortlichen Organisationseinheiten empfohlen werden.

5.3 Metamodell der Autorisierung

Das Metamodell einer Methode stellt das konzeptionelle Datenmodell ihrer Ergebnisse dar.[355] Um die Komplexität des Gesamtmodells zu beherrschen, werden im Weiteren problemorientierte Sichten verwendet.[356] Ausgangspunkt der Zuweisung von Berechtigungen bilden die Aufbau- und Ablauforganisation eines Unternehmens,[357] so dass die Metamodelle „Ablauforganisation“ und „Aufbauorganisation“ wesentliche Gestaltungselemente der Organisationstheorie beschreiben. Erst im Anschluss an die Definition dieser beiden Modelle erfolgt die Vorstellung des Metamodells „Autorisierung“, das grundlegende Entitätstypen zur Verwaltung und Kontrolle von Zugriffsberechtigungen in Zusammenhang setzt und definiert.

Die in diesem Abschnitt präsentierten Metamodellsichten werden im Rahmen der folgenden Methodenentwicklung als Ausgangspunkt zur Entwicklung weiterer problemorientierter Sichten verwendet. Die Darstellung des Metamodells erfolgt auf Basis der UML-Notation, da diese sich als führender Notationsstandard in Praxis und Wissenschaft etabliert hat.[358]

354 Vgl. Kapitel 5.2.2.
355 Vgl. Gutzwiller 1994, S. 14.
356 Zur Komplexitätsreduktion durch Sichten vgl. Sinz 1999, S. 1036.
357 Vgl. Seufert 2002, S. 4.
358 Vgl. z.B. Balzert 2000, S. v.

5.3.1 Metamodell „Ablauforganisation“

Abbildung 39 zeigt das Metamodell „Ablauforganisation“. Das Metamodell fusst im Wesentlichen auf dem Metamodell der Methode Promet BPR, da letzteres dem Forschungsprogramm zuzurechnen ist, dem auch diese Arbeit entstammt.

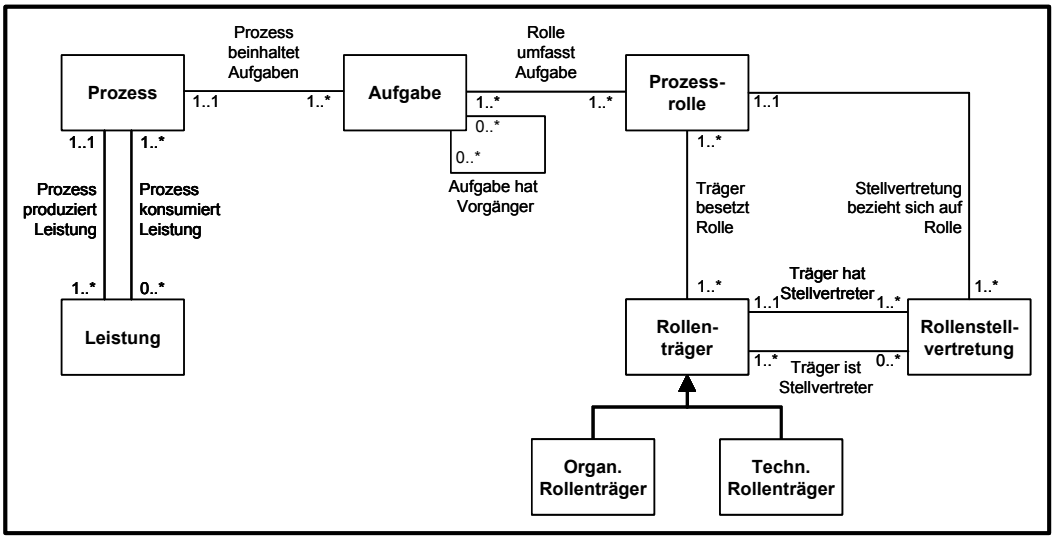

Abbildung 39: Metamodell „Ablauforganisation“

Wesentliches Kernelement des Modells ist der Prozess[359], der sich aus einer Menge von Aufgaben zusammensetzt, die in einer prozessspezifischen Ablauffolge ausgeführt werden. Die einzelnen Aufgaben werden zu Prozessrollen gebündelt, die letztendlich von Menschen (organisatorischen Rollenträgern) oder Maschinen (technischen Aufgabenträgern) wahrgenommen werden. Ein Rollenträger kann im Rahmen einer Rollenstellvertretung in Bezug auf eine Prozessrolle durch einen oder mehrere Rollenträger vertreten werden.

Tabelle 16 zeigt zusammenfassend die Definitionen der Metaentitätstypen sowie gängige Synonyme der Metaentitätstypen.

Entitätstyp	Kurzdefinition	Synonym
Aufgabe	„Eine Aufgabe ist eine betriebliche Funktion mit einem bestimmbaren Ergebnis. Sie wird von Menschen und/oder Maschinen ausgeführt.“[360]	Aktivität
Leistung	„Leistungen sind die Ergebnisse (der Output) eines Prozesses [...]. Empfänger einer Leistung ist ein anderer Prozess [...].“ [361]	Output
Prozess	Ein Prozess setzt sich aus einer Menge von Aufgaben zusammen, die in einer prozessspezifischen Ablauffolge ausgeführt wird.[362]	-
Prozessrolle	Eine Prozessrolle stellt eine ablauforganisatorische Bündelung von Aktivitäten dar.[363]	Rolle

359 Vgl. IMG 1997, Meta 3.
360 IMG 1997, Meta 8.
361 IMG 1997, Meta 10.
362 Vgl. IMG 1997, Meta 3.
363 In Anlehnung an Rosemann/zur Mühlen 1997, S. 101.

Rollenstellvertretung	Unter einer Rollenstellvertretung werden alle Massnahmen eines begrenzten oder unbegrenzten Einsatzes einer oder mehrerer Rollenträger für einen anderen Rollenträger verstanden, sowohl in räumlicher, funktionsmässiger als auch in zeitlicher Hinsicht.[364]	-
Rollenträger	Organisationseinheiten bzw. die ihnen zugeordneten Mitarbeiter (organisatorische Rollenträger) und/oder Maschinen (technische Rollenträger) führen Aufgaben aus.[365]	-

Tabelle 16: Definitionen Metamodell „Ablauforganisation“

5.3.2 Metamodell „Aufbauorganisation“

Abbildung 40 zeigt das Metamodell „Aufbauorganisation“. Das Metamodell knüpft durch den Metaentitätstyp „Organisatorischer Rollenträger“ am Metamodell „Ablauforganisation“ an. Letztendlich verbirgt sich hinter einem organisatorischen Rollenträger immer eine Person. Um eine Vielzahl von direkten Zuweisungen zu vermeiden, wird z.B. in Workflowmanagementsystemen von einer indirekten Zuweisung von Personen zu Prozessrollen über organisatorische Konstrukte wie Stellentyp, Stelle oder Organisationseinheit Gebrauch gemacht.[366]

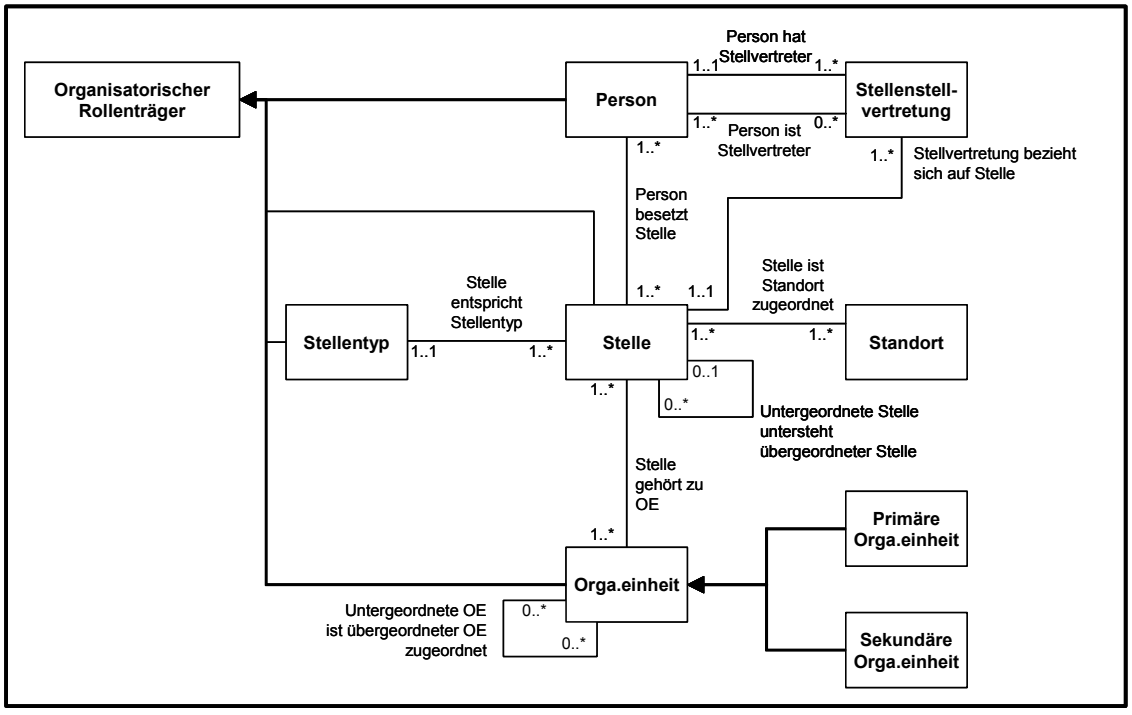

Abbildung 40: Metamodell „Aufbauorganisation“

Wesentlicher Metaentitätstyp des Metamodells „Aufbauorganisation“ ist die Stelle, die synonym auch als Arbeitsplatz bezeichnet wird. Eine Stelle stellt analog zur Prozessrolle eine Zusammenfassung von Aufgaben dar.[367] Die Bündelung der Aufgaben erfolgt dabei nicht auf der Basis ablauforganisatorischer Aspekte. Vielmehr steht die Zusammenfassung von Aufga-

364 In Anlehnung an Blümle 1975, Sp. 1888ff.
365 In Anlehnung an IMG 1997, Meta 3.
366 Vgl. Rosemann/zur Mühlen 1997, S. 100ff.
367 Vgl. im Folgenden Rosemann/zur Mühlen 1997, S. 102.

ben im Vordergrund, die eine derartige Kapazitätsnachfrage bilden, dass sie einer Person übertragen werden können und diese dauerhaft bei definierter, im Regelfall kontinuierlicher Arbeitszeit auslasten. Stellen werden zu Organisationseinheiten zusammengefasst.[368] Temporär bestehende Organisationseinheiten werden als sekundäre Organisationseinheiten bezeichnet. Diese sind zumeist orthogonal zu den dauerhaften Organisationseinheiten (primären Organisationseinheiten) positioniert. Eine Stelle wird von einer oder mehreren Personen besetzt. Im Rahmen einer Stellenstellvertretung wird ein Stelleninhaber durch einen oder mehrere Stellvertreter vertreten.

Tabelle 17 zeigt zusammenfassend die Definitionen der Metaentitätstypen sowie gängige Synonyme der Metaentitätstypen.

Entitätstyp	**Kurzdefinition**	**Synonym**
Organisatorischer Rollenträger	Siehe Metamodell „Ablauforganisation“	-
Organisationseinheit	Stellen werden zu Organisationseinheiten zusammengefasst. Die Beziehungen zwischen den Organisationseinheiten bilden die Aufbauorganisation in einem Unternehmen.[369] Nur temporär bestehende Organisationseinheiten, die z.B. der Abwicklung von Projekten dienen, werden als sekundäre Organisationseinheiten bezeichnet.[370] Diese sind zumeist orthogonal zu den dauerhaften Organisationseinheiten (primären Organisationseinheiten) positioniert.	-
Person	Eine Person ist ein menschlicher Aufgabenträger, der eine oder mehrere Stellen besetzt.[371]	Mitarbeiter
Standort	Ein Standort ist ein geographischer Punkt, an dem sich eine oder mehrere Organisationseinheiten befinden.[372]	-
Stelle	Eine Stelle bezeichnet eine Zusammenfassung von Aufgaben, die eine derartige Kapazitätsnachfrage bilden, dass sie einer Person übertragen werden können und diese dauerhaft bei definierter, im Regelfall kontinuierlicher Arbeitszeit auslasten.[373]	Arbeitsplatz
Stellenstellvertretung	Unter einer Stellenstellvertretung werden alle Massnahmen eines begrenzten oder unbegrenzten Einsatzes eines oder mehrerer Stelleninhaber für einen anderen Stelleninhaber verstanden, sowohl in räumlicher, funktionsmässiger als auch in zeitlicher Hinsicht.[374]	-
Stellentyp	Stellentypen fassen Stellen mit gleichen Kompetenzen zusammen (z. B. Stellentyp „Sekretär“ im Gegensatz zur Stelle „Sekretär von Prof. Winter“).[375]	-

Tabelle 17: Definitionen Metamodell „Aufbauorganisation“

368 Vgl. im Folgenden Rosemann/zur Mühlen 1997, S. 103.
369 Vgl. Rosemann/zur Mühlen 1997, S. 103.
370 In Anlehnung an Rosemann/zur Mühlen 1997, S. 103.
371 In Anlehnung an Rosemann/zur Mühlen 1997, S. 102.
372 Vgl. IMG 1997, Meta 15.
373 In Anlehnung an Rosemann/zur Mühlen 1997, S. 102.
374 In Anlehnung an Blümle 1975, Sp. 1888ff.
375 Vgl. Rosemann/zur Mühlen 1997, S. 102.

5.3.3 Metamodell „Autorisierung“

Abbildung 41 zeigt das Metamodell „Autorisierung“. Das Metamodell knüpft durch die Metaentitätstypen „Person“, „Prozessrolle“ und „Aufgabe“ an das Metamodell „Ablauforganisation“ an. Damit die menschlichen Aufgabenträger die informationstechnisch unterstützten Aufgaben durchführen können, müssen sie über entsprechende Systemberechtigungen verfügen. Diese Berechtigungen regeln den Zugriff auf die Methoden und Datenobjekte der existierenden Softwarekomponenten und werden über Benutzerkonten den Aufgabenträgern zugeordnet.

Im Rahmen der Fallstudien zeigte sich, dass die Zuweisung der Berechtigungen zu Benutzerkonten über intermediäre Konstrukte erfolgt, die in der Praxis als Ressourcen bezeichnet werden. Eine Ressource umfasst eine oder mehrere Berechtigungen und stellt wie die Entitätstypen „Benutzerkonto“ und „Berechtigung“ ein systemspezifisches Konstrukt dar. Die Fallstudien zeigen ausserdem, dass die Definition von Ressourcen nur sehr eingeschränkt auf aufbauorganisatorisch spezifizierten Elementen wie z.B. Stellen basiert. In den einzelnen Organisationseinheiten existiert vielmehr eine Vielzahl von informellen, nicht dokumentierten Stellvertretungen und ablauforganisatorischen Aufgaben- bzw. Kompetenzverteilungen, die es im Rahmen der Ressourcendefinition zu berücksichtigen gilt. Aus Komplexitätsgründen werden Stellvertretungen nur in Ausnahmefällen informationstechnisch abgebildet:[376] Eine zu vertretende Person und ihre Stellvertreter werden vielmehr mit gleichen Berechtigungen ausgestattet.

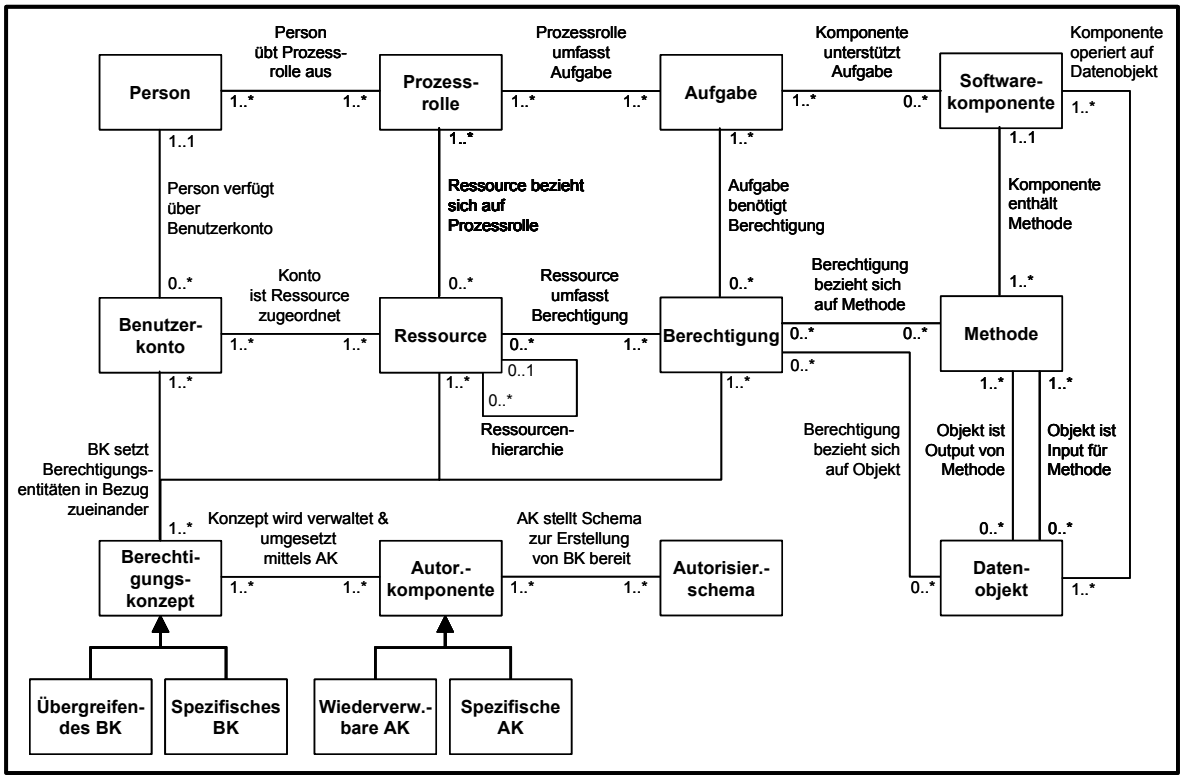

Abbildung 41: Metamodell „Autorisierung“

Die Verwaltung und Kontrolle der Berechtigungen erfolgt in Autorisierungskomponenten, die systemspezifisch (spezifische Autorisierungskomponente) oder systemübergreifend (wiederverwendbare Autorisierungskomponente) eingesetzt werden können. Das Berechtigungsschema einer Autorisierungskomponente legt analog zum Datenschema[377] die im Rahmen der Spezifikation zu verwendenden Berechtigungsentitäten und die Eigenschaften der zu erfassenden Berechtigungen fest.[378] Ein Berechtigungskonzept umfasst entweder systemspezifische (spezifisches Berechtigungskonzept) oder systemübergreifende (übergreifendes Berechtigungskonzept), informationstechnisch abgebildete Regelungen, die festlegen, welcher Benutzer auf welche Methoden und/oder Datenobjekte zugreifen darf. Ein Berechtigungskonzept entspricht dem Autorisierungsschema der Autorisierungskomponente, die das Berechtigungskonzept zur Administration und Umsetzung speichert.

Tabelle 18 zeigt zusammenfassend die Definitionen der Metaentitätstypen:

Entitätstyp	Kurzdefinition	Synonym
Aufgabe	Siehe Metamodell „Ablauforganisation“	Aktivtät
Autorisierungs-komponente	Eine Autorisierungskomponente ist eine Softwarekomponente, die Funktionalitäten zur Verwaltung und/oder Kontrolle von Berechtigungen bereitstellt. Eine spezifische Autorisierungskomponente stellt Autorisierungsfunktionalitäten für ein spezifisches System zur Verfügung. Eine wiederverwendbare Autorisierungskomponente, die in der Praxis auch als Autorisierungsdienstleister bezeichnet wird,[379] stellt Autorisierungsfunktionalitäten für mehrere Systeme zur Verfügung.	Administrations-komponente, Autorisierungssystem, Zugriffskontroll-komponente
Autorisierungsschema	In einer Autorisierungskomponente werden durch das verwendete Berechtigungsschema analog zum Datenschema Berechtigungsentitäten und Eigenschaften der zu erfassenden Berechtigungen festgelegt.[380]	Berechtigungs-schema, Zugriffskontrollschema
Benutzerkonto	Ein Benutzerkonto repräsentiert eine Person im Inform.system.[381]	Account
Berechtigung	Eine Berechtigung ermöglicht die Ausführung einer Operation auf einem geschützten Objekt.[382] Die Art der Operation und des Objekts hängt von dem jeweiligen System ab, das es zu schützen gilt.	Systemspezifische Berechtigung, Recht, Zugriffsberechtigung
Berechtigungskonzept	Ein Berechtigungskonzept umfasst die informationstechnisch abgebildeten Regelungen, die festlegen, welcher Benutzer auf welche Methoden und/oder Datenobjekte zugreifen darf.[383] Ein Berechtigungskonzept entspricht dem Autorisierungsschema der Autorisierungskomponente, die das Berechtigungskonzept zur Administration und Umsetzung speichert. Ein spezifisches Berechtigungskonzept umfasst systemspezifische Regelungen. Ein übergreifendes Berechtigungskonzept umfasst systemübergreifende Regelungen.	Autorisierungs-konzept, Zugriffskontrollkonzept
Datenobjekt	Ein Datenobjekt stellt eine Kategorie dauerhaft gespeicherter Daten dar, auf die wiederholt von Softwarekomponenten zurückgegriffen wird.[384]	Objekt, Datum

376 Vgl. hierzu die Fallstudien in Kapitel 4.3 und Kapitel 4.4.
377 Vgl. hierzu z.B. Winter et al. 2003, S. 5.
378 Vgl. im Folgenden auch Seufert 2001, S. 31f.
379 Vgl. Kapitel 4.2.
380 In Anlehnung an Winter et al. 2003, S. 5.
381 Vgl. Kern et al. 2002, S. 46.
382 In Anlehnung an Ferraiolo et al. 2001, S. 233.
383 Vgl. hierzu auch Seufert 2001, S. 31f.
384 Vgl. Schwinn 2005, S. 23.

Methode	Die von einer Softwarekomponente implementierte Funktionalität wird in Form von Methoden zur Verfügung gestellt.[385]	Operation, Funktion
Person	Siehe Metamodell „Aufbauorganisation“	Mitarbeiter
Prozessrolle	Siehe Metamodell „Ablauforganisation“	Rolle
Ressource	Eine Ressource umfasst eine oder mehrere Berechtigungen und stellt ein system- bzw. applikationsspezifisches Berechtigungsbündel dar.[386]	Systemspezifische Rolle, Profil, Kompetenz
Softwarekomponente	Eine Softwarekomponente ist ein abgeschlossener Softwarebaustein, der eine definierte Funktionalität anbietet.[387]	Softwarebaustein

Tabelle 18: Definitionen Metamodell „Autorisierung“

Nach der Definition der grundlegenden Metaentitätstypen erfolgt im Weiteren die eigentliche Methodenkonstruktion.

385 Vgl. Schwinn 2005, S. 22.
386 Die Definition ergibt sich aus der Analyse der Fallstudien. Vgl. insbesondere Kapitel 4.3.
387 In Anlehnung an Schwinn 2005, S. 22.

6 Methodenbaustein Autorisierungsarchitektur

Im Folgenden wird auf Basis der beschriebenen Fallstudien und der analysierten Literatur ein Vorgehensmodell für die Entwicklung einer Autorisierungsarchitektur abgeleitet. Als Ausgangspunkt dienen dabei Ansätze aus dem Bereich des Architekturmanagements, auf die in Abschnitt 6.1 eingegangen wird. Vor der eigentlichen Ableitung (vgl. Abschnitt 6.3) und Beschreibung des Vorgehensmodells (vgl. Abschnitt 6.4) wird zunächst das zugrunde liegende Metamodell thematisiert (vgl. Abschnitt 6.2). Abschliessend wird in den Abschnitten 6.5 und 6.6 das Dokumentations- und Rollenmodell des Methodenbausteins dargestellt.

6.1 Ausgangspunkt des Methodenentwurfs

In diesem Abschnitt werden die elementaren Grundlagen für den Entwurf des Methodenbausteins „Autorisierungsarchitektur“ vorgestellt. Hierzu soll insbesondere die Dissertation HAFNERS „Entwicklung einer Methode für das Management der Informationssystemarchitektur im Unternehmen“[388] herangezogen werden. Diese Arbeit stellt ein Vorgehensmodell für das Management der unternehmensweiten IS-Architektur zur Verfügung und ist demselben Forschungsprogramm zuzurechnen wie die vorliegende Arbeit.

6.1.1 Architekturbegriff

Ausgehend von dem bereits in Kapitel 5 diskutierten Begriff der Modellierung wird im Folgenden unter Anlehnung an HAFNER der im Weiteren massgebliche Architekturbegriff entwickelt.

Systeme können aus den unterschiedlichsten Perspektiven und für die unterschiedlichsten Zwecke modelliert[389] werden.[390] Zur Komplexitätsbewältigung hat sich die Bildung einer Hierarchie von Modellierungsebenen bewährt. Die Ebenen der Modellierung unterscheiden sich dabei hinsichtlich des Aggregationsgrads und/oder der jeweiligen Ziele der Modellbildung. Neben der Bildung von Ebenen hat sich die Verwendung von Sichten zur Komplexitätsbewältigung durchgesetzt. Sichten beschränken sich auf die Abbildung eines bestimmten Teilaspekts.[391] In Anlehnung an HAFNER[392], der dem IEEE-Standard 1471[393] folgt, werden im Rahmen dieser Arbeit Sichten als ein ebenenübergreifendes, problemorientiertes Konzept aufgefasst. In der Praxis wird im Zusammenhang mit Sichten häufig synonym der Begriff der Ar-

388 Hafner 2005.
389 Zum Begriff der Modellierung vgl. Kapitel 5.1.2.
390 Vgl. im Folgenden Winter 2003b, S. 91f.
391 Vgl. Winter 2003b, S. 90.
392 Vgl. Hafner/Winter 2005, S. 27ff.
393 Vgl. IEEE 2000.

chitektur verwendet. Typische Architekturen der Praxis sind Sicherheits,- Integrations-, Informations- oder auch Datenarchitektur.[394]

Aufbauend auf den Begriffen Modell, Ebene und Sicht wird der Arbeit folgende Architekturdefinition zugrunde gelegt: Eine Architektur umfasst Modelle und Handlungsanweisungen für einen betrachteten Gegenstandsbereich.[395] Der Gegenstandsbereich einer Architektur ergibt sich aus einzelnen Ebenen oder Sichten sowie deren Kombination. Die Unternehmensarchitektur stellt die Gesamtheit der unternehmensweit gültigen Modelle und Handlungsanweisungen zur Verfügung. Aufgabe des Architekturmanagements ist es, die unterschiedlichen Architekturen effektiv und effizient miteinander zu koordinieren.[396]

6.1.2 Bestandteile von Architekturen

HAFNER definiert und charakterisiert typische Bestandteile von Architekturen, die im Rahmen des Architekturmanagements spezifiziert werden.[397] Solche Bestandteile werden im Rahmen dieser Arbeit auch als „Artefakte“ bezeichnet.[398] Zu den Architekturartefakten, die grundlegende Zusammenhänge und Regelungen aufzeigen bzw. festlegen, gehören:

- Architekturprinzipien: Architekturprinzipien stellen verbindliche Leitkriterien zur Entwicklung, zur Gestaltung, zum Aufbau und zur Implementierung des Informationssystems dar.[399] Die Prinzipien sollten explizit formuliert werden, um kommuniziert werden zu können, nachhaltige Wirksamkeit zu erzielen sowie Interpretationsspielräume innerhalb des Architekturmanagements zu vermeiden.[400]

- Roadmaps: Eine Roadmap definiert den rahmengebenden Zeitplan für die strategische Weiterentwicklung eines Architekturbereichs.[401] Die Weiterentwicklung der Architektur erfolgt vielfach aus Entwicklungsprojekten heraus, welche ihrerseits aus geschäftlichem oder technischem Handlungsbedarf resultieren.[402] Für den reibungslosen Verlauf der Projekte ist somit die abgestimmte Bereitstellung von Architekturartefakten von Bedeutung. Damit das Architekturmanagement seiner Koordinationsrolle nachkommen kann, sind realistisch umsetzbare Roadmaps erforderlich, die längere Planungshorizonte mit komplexen Abhängigkeiten erfassen.[403]

394 Vgl. Hafner 2005, S. 30.
395 In Anlehnung an Hafner 2005, S. 31.
396 Vgl. Hafner/Winter 2005, S. 3.
397 Vgl. im Folgenden Hafner 2005, S. 59ff.
398 Vgl. Birkhölzer/Vaupel 2003 2003, S. 27.
399 Vgl. Hafner 2005, S. 59.
400 Vgl. Hafner 2005, S. 60.
401 Vgl. Hafner 2005, S. 175.
402 Vgl. Hafner 2005, S. 60.
403 Vgl. Birkhölzer/Vaupel 2003 2003, S. 125.

- Modelle des Gesamtzusammenhangs: Strukturelle Sachverhalte in den einzelnen Architekturbereichen werden mit Hilfe differenzierter, aggregierter, statischer Modelle wiedergegeben.[404] Diese Modelle des Gesamtzusammenhangs dienen v.a. der Kommunikation und Koordination. Um die Kommunikation zwischen den unterschiedlichsten fachlichen und technischen Vertretern zu erleichtern, zeichnen sich die Modelle des Gesamtzusammenhangs vielfach durch einen geringen Formalitätsgrad aus.[405] Die Modelle des Gesamtzusammenhangs werden in der Praxis auch als Architekturen bezeichnet.

Zu den Architekturartefakten, die Zusammenhänge und Regelungen zielgruppenspezifisch aufzeigen bzw. festlegen, zählen:

- Direktiven: Unter den Begriff der Direktive werden im Rahmen dieser Arbeit sowohl Standards als auch Regeln subsumiert.[406] Als Standard bezeichnet die ISO/IEC:[407] „a document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context“. Unter dem allgemeineren Begriff der Regel werden Festlegungen verstanden, auf deren Basis Veränderungen gestaltet und überwacht werden.[408] Ziel von Direktiven ist es, Aussagen zu treffen, die auf eine möglichst umfassende Grundgesamtheit an Problemstellungen anwendbar sind.[409] Dabei ist zu beachten, dass es sich bei Direktiven um wiederverwendbare Spezifikationen, nicht aber um Implementierungen handelt.[410] Direktiven sind im Vergleich zu Prinzipien präziser und zuweilen nur auf konkrete Problemsituationen anwendbar.[411] In der Praxis werden im Zusammenhang von Direktiven sehr uneinheitlich Begriffe wie „Standards“, „Regeln“, „Leitlinien“, „Richtlinien“ oder „Weisungen“ verwendet.

- Entwurfsmuster: Entwurfsmuster sind allgemeingültige Strukturen, die sich für eine bestimmte Problemstellung mehrfach bewährt haben.[412] Entwurfsmuster bestehen aus vier elementaren Bestandteilen, die klar zu spezifizieren sind:[413] (1) Der Bezeichnung des Musters, der insbesondere aus Kommunikationsgründen eine wichtige Rolle zukommt, (2) der Beschreibung des Anwendungskontextes, d.h. des initialen Problems und der Prämissen zur Anwendung des Musters, (3) der Beschreibung der Lösung, die die Lösungselemente, deren Beziehungen und eventuelle Zuständigkeiten und Interaktionen festlegt, sowie (4) der Darstellung der Konsequenzen eines Einsatzes des Musters, die z.B. durch die Beschreibung von Vor- und Nachteilen des Musters erfolgen kann.

404 Vgl. auch im Folgenden Hafner 2005, S. 61.
405 Vgl. Hafner 2005, S. 62.
406 In Anlehnung an Hafner 2005, S.62.
407 Vgl. ISO 2004, S. 8.
408 In Anlehnung an Hafner 2005, S. 63.
409 Vgl. Hafner 2005, S. 63.
410 Vgl. Birkhölzer/Vaupel 2003, S. 47.
411 Vgl. Birkhölzer/Vaupel 2003, S. 125.
412 Vgl. Birkhölzer/Vaupel 2003, S. 47f.
413 Vgl. Birkhölzer/Vaupel 2003, S. 73; Gamma et al. 1996, S. 3f.

- Leitelemente: Obwohl sich das Architekturmanagements primär mit der Strukturierung des Informationssystems auseinandersetzt, werden im Rahmen des Architekturmanagements auch konkrete Artefakte wie z.B. Softwarespezifikationen oder -komponenten mit Referenzcharakter von zentraler Bedeutung entwickelt.[414] Potenzielle Nutzer können diese Artefakte direkt verwenden. Die Leitelemente werden in der Regel mit Unterstützung des Architekturmanagements in regulären Entwicklungsprojekten realisiert.[415]

- Kennzahlen: Kennzahlen sind Zahlen, die quantitativ erfassbare Sachverhalte in konzentrierter Form erfassen.[416] Das Architekturmanagement bedarf geeigneter Kennzahlen im Zuge der Qualitätssicherung.[417] Die entsprechenden Kennzahlen sind aus den Zielen des Architekturmanagements abzuleiten, die ihrerseits auf Anforderungen aus dem Umfeld der Architektur basieren.[418] Im Mittelpunkt der Bewertung stehen z.B. die Qualität von Architekturartefakten und -aktivitäten, Ressourcenersparnis sowie die Vermeidung von Fehlern. Vielfach sind hier subjektive Expertenschätzungen notwendig, um wenig aussagekräftige Metriken zu vermeiden.[419]

6.1.3 Vorgehensmodell zum Management der IS-Architektur

Auf der Basis von Praxisfallstudien und einer breiten Literaturanalyse entwickelt HAFNER ein Vorgehensmodell für das Management der unternehmensweiten IS-Architektur.[420] Nach der Definition HAFNERS umfasst die IS-Architektur die Applikationsarchitektur, die Softwarearchitektur und die Technische Architektur.[421] Der Gegenstandsbereich der IS-Architektur entspricht somit der Systemebene[422] des Business Engineering. Die einzelnen Architekturen sind wie folgt definiert:[423]

- Applikationsarchitektur: In Anlehnung an WINTER ist die Applikationsarchitektur ein aggregiertes Modell eines Informationssystems aus fachlicher Sicht.[424] Sie beschreibt das Zusammenwirken von Applikationen in Form von Informationsflüssen. Die Gestaltung der Applikationsarchitektur basiert auf den Ergebnissen der Organisationsgestaltung und liefert Vorgaben für die Softwarearchitektur. Flexibilität, Integration und Redundanzminimierung sind die Gestaltungsziele der Applikationsarchitektur.[425]

414 Vgl. Birkhölzer/Vaupel 2003, S. 48.
415 Vgl. Birkhölzer/Vaupel 2003, S. 49.
416 Vgl. Reichmann/Lachnit 1976, S. 706.
417 Vgl. Hafner 2005, S. 67.
418 Vgl. im Folgenden Birkhölzer/Vaupel 2003, S. 29, 203f.
419 Vgl. Birkhölzer/Vaupel 2003, S. 202.
420 Vgl. Hafner 2005, 203ff.
421 Vgl. Hafner 2005, S. 42.
422 Vgl. Kapitel 2.1.2.
423 Vgl. Hafner 2005, S. 42ff.
424 Vgl. im Folgenden Winter 2004b, S. 11; Hafner 2005, S. 42.
425 Vgl. Krallmann 2003, S. 6; Winter 2004a, S. 3.

- Softwarearchitektur: Die Softwarearchitektur beschreibt den Zusammenhang zwischen Softwarekomponenten[426] und Datenstrukturen[427]. Darüber hinaus umfasst sie Gestaltungsregeln, die die Realisierung von Softwarekomponenten und Datenstrukturen festlegen.[428] Die Softwarearchitektur setzt sich mit der inneren Gestaltung einer Applikation auseinander. Ziel hierbei ist es, die Abhängigkeiten der Komponenten zu reduzieren und sie applikationsintern und -übergreifend wiederzuverwenden.[429]

- Technische Architektur: Die technische Architektur widmet sich dem technischen Basissystem, den technischen Konzepten, Standards und Produktvorgaben.[430] Sie fokussiert somit auf die technische Infrastruktur bestehend aus Hardware und systemnaher Software.[431] Hierbei treten technologische Fragestellungen in den Vordergrund.[432]

Das *Vorgehensmodell* für das Management der unternehmensweiten IS-Architektur umfasst die drei Phasen Architekturführung, Architekturweiterentwicklung und Architekturvertretung.[433]

Die Phase Architekturführung hat rahmengebenden Charakter und wird daher in längerfristigen Zyklen durchlaufen. Innerhalb der Phase werden die strategischen Anforderungen aufgenommen und als Grundlage für die Beurteilung der vorliegenden IS-Architektur verwendet. Auf dieser Basis werden sodann Massnahmenkomplexe abgeleitet. Die Phase umfasst folgende Aktivitäten:[434]

- Strategieanforderungen identifizieren: Um die Ausrichtung der IS-Architektur an übergeordneten Zielsetzungen zu gewährleisten, gilt es, die strategischen Anforderungen des Informationsmanagements zu erheben. Im Anschluss daran sind die Zusammenhänge und Prioritäten der Anforderungen festzulegen.

- Architekturbereiche strategisch beurteilen: Auf der Basis der Architekturprinzipien werden die einzelnen Bereiche der IS-Architektur hinsichtlich ihres Ist-Zustandes und der geplanten Weiterentwicklung bewertet. Aus der Beurteilung ergeben sich Massnahmen, die dazu dienen, Lücken zwischen Architekturprinzipien und Ist-Zustand der IS-Architektur zu schliessen. Analysiert werden sowohl einzelne Komponenten wie z.B. einzelne Applikationen als auch aggregierte Strukturen wie z.B. Applikationsdomänen.

426 Vgl. Turowski 2001, S. 269.
427 Vgl. Winter 2004b, S. 3.
428 Vgl. im Folgenden Garlan 1995, S. 269.
429 Vgl. auch Birkhölzer/Vaupel 2003, S. 22.
430 Vgl. Brenner et al. 2003, S. 157.
431 Vgl. Dern 2003, S. 27.
432 Vgl. Brenner et al. 2003, S. 159.
433 Vgl. im Folgenden Hafner 2005, S. 203ff.
434 Vgl. im Folgenden Hafner 2005, S. 204f.

- Massnahmenkomplexe ableiten: Die abgeleiteten Massnahmen sind auf gegenseitige Abhängigkeiten zu untersuchen. Redundante Massnahmen sind so z.B. zusammenzuführen. Abschliessend werden die Massnahmen zu Massnahmenkomplexen zusammengefasst.

- Fundamentale Architekturartefakte aktualisieren: Die identifizierten Massnahmenkomplexe werden nun zeitlich aufeinander abgestimmt. Der Zeitplan muss ggf. auch verschiedene Varianten strategischer Massnahmenkomplexe berücksichtigen. Meilensteine in Form von Sollbeschreibungen der IS-Architekturbereiche zeigen dabei den Weg zu einer langfristigen Zielarchitektur auf.

- Architektureffektivität beurteilen: Zur wirtschaftlichen Rechtfertigung des IS-Architekturmanagements muss seine Wirkung transparent gemacht werden. Auslastung und Nachfrage des Architekturmanagements sind dabei keine geeigneten Grössen, um ein umfängliches Architekturmanagement zu rechtfertigen. Vielmehr gilt es hier, alternative Kennzahlen zu implementieren, die den Nutzen des Architekturmanagements überzeugend vermitteln.

In der Phase Architekturweiterentwicklung werden IS-Architekturartefakte auf der Grundlage strategischer Architekturartefakte und operativer Anforderungen entwickelt. Diese Anforderungen treten kontinuierlich auf, so dass diese Phase in deutlich kürzeren Zyklen zu durchlaufen ist als die Phase der Architekturführung. Die Phase umfasst folgende Aktivitäten:[435]

- Operative Anforderungen identifizieren: Operative Anforderungen werden üblicherweise im Rahmen von IS-Entwicklungsprojekten identifiziert oder gehen auf den Betrieb zurück. Die Anforderungen sind mit Hilfe des IS-Architekturmanagements zu formulieren, um erste Abstimmungen sicherzustellen.

- Lösungen entwerfen: IS-Architekturartefakte werden im Rahmen der Aktivität „Lösungen entwerfen“ auf Basis operativer Anforderungen pilotiert. Dies umfasst die detailgenaue Spezifikation des Artefakts, seiner fachlichen und wirtschaftlichen Auswirkungen und seine Erprobung in einem ausgewählten Teilbereich der IS-Architektur.

- Architekturartefakte entwickeln: Auf der Grundlage der operativen Anforderungen und des Pilots werden die Artefakte abschliessend entwickelt. Artefakte, die im Rahmen dieser Aktivität entstehen, sind Direktiven, Muster oder Leitelemente.

- Abstimmung herbeiführen: Während der Weiterentwicklung der Architektur ist eine kontinuierliche Abstimmung zwischen den verschiedenen Interessengruppen notwendig. Im Rahmen der Entwicklungsaktivitäten ist davon auszugehen, dass konträre Interessen entstehen, die abzustimmen sind. Ist eine Abstimmung zwischen den Interessengruppen nicht möglich, müssen definierte Eskalationspfade zur Lösung führen.

---

435 Vgl. im Folgenden Hafner 2005, S. 206f.

Die Phase Architekturvertretung widmet sich der Vertretung der erarbeiteten Artefakte nach aussen hin. Eine vorhabens- und projektunabhängige Kommunikation ist dabei ebenso wichtig wie die vorhabens- und projektabhängige Kommunikation. Die Phase Architekturvertretung umfasst folgende Aktivitäten:[436]

- Architekturartefakte kommunizieren: Die Kommunikation von Architekturartefakten erfolgt über verschiedene Kanäle, um unterschiedliche Zielgruppen mit differierenden Informationsbedürfnissen und Arbeitsweisen erreichen zu können. Reine Informationsveranstaltungen bieten die Möglichkeit, überblicksartig Entwicklungen darzustellen und den Nutzen des Architekturmanagements aufzuzeigen. Individuelle Detailinformationen werden schriftlich zur Verfügung gestellt oder mittels Intranetlösungen von den Nutzern bezogen.

- Architekturzielgruppenprojekte beurteilen: Projekte, die in den Verantwortungsbereich des IS-Architekturmanagements gehören, müssen auf ihre Architekturkonformität überprüft werden. Die Prüfung erfolgt im Rahmen einer umfassenden Projektprüfung, welche die IS-Architektur als einen Teilaspekt umfasst. Ergebnis dieser Bewertung ist die Ablehnung oder Freigabe des Projekts.

- Architekturzielgruppenprojekte unterstützen: Wenn ein Projekt aus Sicht des Architekturmanagements besondere Relevanz aufweist oder Unterstützung anfordert, wird es vom Architekturmanagement unterstützt. Typischerweise werden Inkonsistenzen zusammen erörtert oder Leitelemente für die Entwicklung entworfen.

6.1.4 Konsequenzen für den Methodenentwurf

Die obigen Ausführungen zeigen drei potenzielle Anknüpfungspunkte an die Arbeit HAFNERS auf, die wie folgt berücksichtigt werden:

- Architekturbegriff: In Anlehnung an HAFNER umfasst eine Architektur Modelle und Handlungsanweisungen für einen betrachteten Gegenstandsbereich, der sich aus einzelnen Ebenen oder Sichten sowie deren Kombination ergibt.[437] Eine Autorisierungsarchitektur ist folglich eine Architektur, deren Gegenstandsbereich die Autorisierung darstellt. Entsprechend der vorgestellten Definitionen[438] ergibt sich der Gegenstandsbereich der Autorisierungsarchitektur ebenenübergreifend aus einer spezifischen Sicht.

- Bestandteile von Architekturen: Die von HAFNER identifizierten Architekturbestandteile können im Rahmen der zu entwickelnden Methode ohne weitere Modifikationen verwen-

[436] Vgl. im Folgenden Hafner 2005, S. 207f.
[437] Vgl. Kapitel 6.1.1.
[438] Vgl. Kapitel 6.1.1.

det werden. Die definierten Artefakte werden den folgenden Ausführungen daher unverändert zugrunde gelegt.

- Vorgehensmodell zum Management der IS-Architektur: HAFNERS Vorgehensmodell abstrahiert von einem spezifischen Gegenstandsbereich wie z.B. Autorisierung und stellt somit ein generisches Modell[439] dar. Damit besteht die Möglichkeit, die zu leistende Methodenentwicklung durch eine Anpassung des bereits existierenden Vorgehensmodells unter Berücksichtigung der erhobenen Fallstudien zu realisieren. Die erhobenen Fallstudien sind jedoch nicht unmittelbar mit der von HAFNER identifizierten Vorgehensweise in Einklang zu bringen: Die Fallstudien erstrecken sich insbesondere auf die Aktivitäten der Phasen Architekturführung und Architekturweiterentwicklung. Zum einen umfassen sie dabei Aktivitäten wie z.B. die Identifikation von Schwachstellen, die nicht unmittelbar in HAFNERS Vorgehensweise enthalten sind. Zum anderen beinhaltet HAFNERS Vorgehensmodell Aktivitäten wie „Architekturbereiche strategisch beurteilen“, die im Rahmen der vorliegenden Fallstudien nicht wie spezifiziert durchgeführt worden sind. Zudem sind die von HAFNER beschriebenen Aktivitäten im Kontext des vorliegenden Themenschwerpunkts sehr abstrakt, so dass sie als Ausgangspunkt der Methodenentwicklung kaum Nutzen bringen. Im Folgenden wird daher auf Basis der Fallstudien ein Vorgehensmodell abgeleitet, das das von HAFNER entwickelte Vorgehensmodell nicht unmittelbar berücksichtigt: Lediglich einzelne Aktivitäten der von HAFNER entwickelten Methode werden in die Methodenausarbeitung einbezogen. Diese Aktivitäten beschreiben Vorgehensweisen, die auch im Kontext der analysierten Fallstudien Verwendung gefunden haben.

Nach Darstellung des Ausgangspunkts der zu entwickelnden Methode soll nachfolgend die eigentliche Methodenentwicklung aufgezeigt werden.

6.2 Metamodell

Die im Rahmen dieses Kapitels zu entwickelnde Vorgehensweise ist von den drei Domänen „Architekturmanagement“, „Sicherheitsmanagement“ und „Autorisierung“ geprägt. Während der Gegenstandsbereich der Autorisierung im Rahmen des Metamodells „Autorisierung“ thematisiert wird, ist das Metamodell „Autorisierungsarchitektur“ insbesondere den beiden Domänen „Architektur-“ und „Sicherheitsmanagement“ gewidmet.

Eine Autorisierungsarchitektur wird im Wesentlichen durch Modelle, Direktiven und Leitelemente spezifiziert (vgl. Abbildung 42).[440] Massnahmen, die identifizierte Schwachstellen adressieren und nach inhaltlichen Gesichtspunkten zu Massnahmenkomplexen zusammengefasst werden, beschreiben die Umsetzung der Autorisierungsarchitektur. Aus der Perspektive des Sicherheitsmanagements kommt der Berücksichtigung von Anforderungen sowie der

439 Vgl. Winter 2003b, S. 90.
440 Vgl. Kapitel 6.1.2.

Identifikation und Bewältigung von Risiken eine zentrale Bedeutung zu.[441] Die Risiken ergeben sich dabei ursachenbezogen aus dem Zusammenwirken existierender Bedrohungen wie Industriespionage und vorhandener Schwachstellen wie unzureichend abgesicherten Datenbankservern.[442]

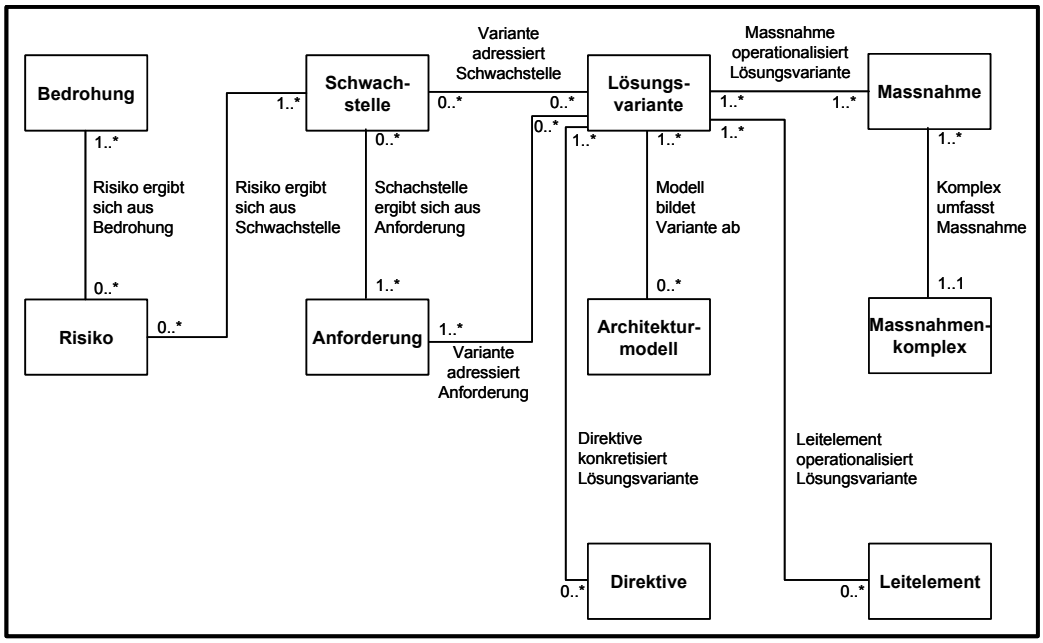

Abbildung 42: Metamodell „Autorisierungsarchitektur“

Tabelle 19 zeigt zusammenfassend die Definitionen der Metaentitätstypen sowie gängige Synonyme der Metaentitätstypen.

Entitätstyp	Kurzdefinition	Synonym
Anforderung	Anforderungen legen die qualitativen und quantitativen Eigenschaften eines zu gestaltenden Objekts fest.[443]	-
Architekturmodell	Ein Architekturmodell ist ein Modell, das einer oder mehreren Architekturen zugeordnet ist.[444]	-
Bedrohung	Eine Bedrohung ist ein Anlass für ein unerwünschtes Ereignis, das zu einem Schaden führen kann.[445]	-
Direktive	Direktiven sind Regelungen, auf deren Basis Veränderungen gestaltet und überwacht werden.[446]	Standard, Regel
Leitelement	Leitelemente sind konkrete Artefakte wie z.B. Softwarespezifikationen oder -komponenten mit Referenzcharakter, die im Rahmen einer Architektur von zentraler Bedeutung sind.[447]	-
Lösungsvariante	Eine Lösungsvariante beschreibt eine Möglichkeit, wie eine Problemstellung adressiert werden kann.[448]	Gestaltungsoption
Massnahme	Eine Massnahme umfasst Tätigkeiten, die auf die Erhöhung der Effizienz und/oder Effektivität des zu gestaltenden Gegenstandsbereiches abzielen.[449]	-

441 Vgl. Kapitel 5.2.
442 Vgl. Brauhäuser et al. 2003, S. 57.
443 In Anlehnung an Balzert 2000, S. 98; Vgl. auch Hafner 2005, S. 148f.
444 In Anlehnung an Hafner 2005, S. 154.
445 Vgl. Zentrum für sichere Informationstechnologie - Austria 2004, S. 85.
446 In Anlehnung an Hafner 2005, S. 62f; Kapitel 6.1.2.
447 In Anlehnung an Hafner 2005, S. 66; Kapitel 6.1.2.
448 Vgl. auch Hafner 2005, S. 168.

Massnahmenkomplex	Ein Massnahmenkomplex fasst Massnahmen nach inhaltlichen Gesichtspunkten zusammen.[450]	-
Risiko	Risiko bezeichnet die Gefahr von Verlusten.[451] Risiko resultiert ursachenbezogen aus der Unsicherheit zukünftiger Ereignisse und schlägt sich wirkungsbezogen in einer negativen Abweichung von einer festgelegten Zielgrösse nieder.[452]	-
Schwachstelle	Eine Schwachstelle bezeichnet eine Ineffizienz und/oder eine Ineffektivität des betrachteten Gegenstandsbereiches.[453]	-

Tabelle 19: Definitionen Metamodell „Autorisierungsarchitektur"

Mit der Definition der Metaentitätstypen ist die Spezifikation des Metamodells abgeschlossen, so dass im Weiteren die Ableitung des Vorgehensmodells erfolgt.

6.3 Vorgehensmodell

Um das Vorgehensmodell des Methodenbausteins „Autorisierungsarchitektur" systematisch abzuleiten, werden die relevanten Fallstudien zuerst auf ihre Aktivitäten und deren Abfolge hin untersucht. Durch Induktion erfolgt schlussendlich die Ableitung des Vorgehensmodells.

6.3.1 Vorgehensmodell Fallstudie Credit Suisse

Abbildung 43 zeigt das Vorgehen zur Ableitung der Autorisierungsarchitektur bei der CS.

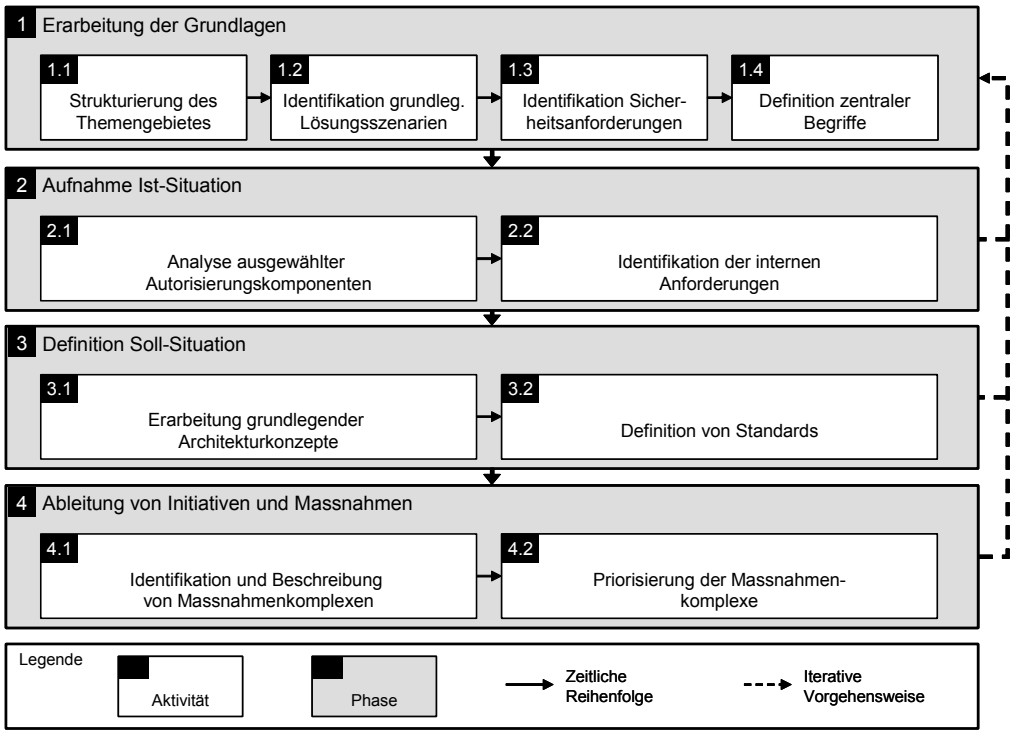

Abbildung 43: Vorgehensmodell Credit Suisse[454]

449 Vgl. auch Zentrum für sichere Informationstechnologie - Austria 2004, S. 87.
450 In Anlehnung an Hafner 2005, S. 168.
451 Vgl. Basler Ausschuss für Bankenaufsicht 2004, S. 127; Kapitel 2.4.
452 Vgl. Schulte 1997, S. 12.
453 Vgl. auch Zentrum für sichere Informationstechnologie - Austria 2004, S. 87.

Dargestellt werden die wesentlichen Projektphasen und ihre Aktivitäten.[455] Pfeile symbolisieren die zeitlichen Abhängigkeiten der Aktivitäten. Der gestrichelte Pfeil deutet das iterative Vorgehen an: Im Laufe der Zeit wurden die entwickelten Konzepte immer detaillierter ausgestaltet.

Die einzelnen Aktivitäten können wie folgt zusammengefasst werden (vgl. Tabelle 20):

Nr.	Aktivität	Beschreibung	Zentrale Ergebnisse
1 Erarbeitung der Grundlagen			
1.1	Strukturierung des Themengebietes	Identifikation und Beschreibung wesentlicher Sicherheitskomponenten und ihres Zusammenwirkens im „Security Architecture Model". Das „Security Architecture Model" ist Teil der „Security Architecture".	„Security Architecture Model"
1.2	Identifikation grundlegender Lösungsszenarien	Analyse existierender Standards als Grundlage für zukünftige Lösungen. Dokumentation und Aufarbeitung der Standards in der „Security Architecture".	Aufgearbeitete Standards
1.3	Identifikation von Sicherheitsanforderungen	Analyse des Sicherheitsstandards ISO/IEC 17799. Herausarbeitung zentraler Sicherheitsanforderungen, die im Rahmen der zu erarbeitenden Lösungen zu berücksichtigen sind. Die Anforderungen werden im Rahmen der „Security Architecture" dokumentiert.	Sicherheitsanforderungen
1.4	Definition zentraler Begriffe	Zusammenstellung und Definition der zentralen Begriffe in Form eines Glossars. Das Glossar ist Teil der „Security Architecture".	Glossar
2 Aufnahme Ist-Situation			
2.1	Analyse ausgewählter Autorisierungskomponenten	Evaluation zentraler Autorisierungskomponenten u.a. anhand der Kriterien „Einsatzgebiet", „Datenbasis" „Zugriffsrechte" und „Sicherheitsprüfung". Dokumentation der Ergebnisse im „Positionspapier Zugriffskontrolle".	Komponentenbewertungen
2.2	Identifikation der internen Anforderungen	Identifikation bestehender sowie neuer Autorisierungsanforderungen. Zusammenfassung der Anforderungen im „Positionspapier Zugriffskontrolle".	Interne Anforderungen
3 Definition Soll-Situation			
3.1	Erarbeitung grundlegender Architekturkonzepte	Spezifikation erster mittel- und langfristiger Lösungsszenarien auf einem hohen Abstraktionsniveau im „Positionspapier Zugriffskontrolle".	Autorisierungsarchitekturen
3.2	Definition der Standards	Definition und Erläuterung der Standards, die grundlegende Aspekte der Autorisierung verbindlich für die Credit Suisse festlegen, in der „Authorization Architecture". Zusammenfassung der Soll-Situation, die durch die Standards beschrieben wird, in der „Roadmap" der „Security Architecture".	Autorisierungsstandards
4 Ableitung von Initiativen und Massnahmen			
4.1	Identifikation und Beschreibung von Massnahmenkomplexen	Entwicklung der Massnahmenkomplexe im Rahmen der „Authorization Architecture".	Massnahmenkomplexe

454 Darstellung in Anlehnung an Herrmann 2006, Kapitel 4.3.1.3.
455 Vgl. hierzu auch die ausführliche Beschreibung in Kapitel 4.1.

4.2	Priorisierung der Massnahmenkomplexe	Bewertung der Massnahmenkomplexe im Rahmen der „Security Architecture“ im Teildokument „Roadmap“. Als Bewertungskriterien werden die Kosten und der Zugewinn an Sicherheit der Massnahmenkomplexe herangezogen. Die Bewertungen bilden die Grundlage für den Budgetierungsprozess.	Bewertete Massnahmenkomplexe

Tabelle 20: Aktivitäten Credit Suisse

6.3.2 Vorgehensmodell Fallstudie Winterthur

Abbildung 44 zeigt das Projektvorgehen zur Ableitung der Autorisierungsarchitektur bei der Winterthur.[456]

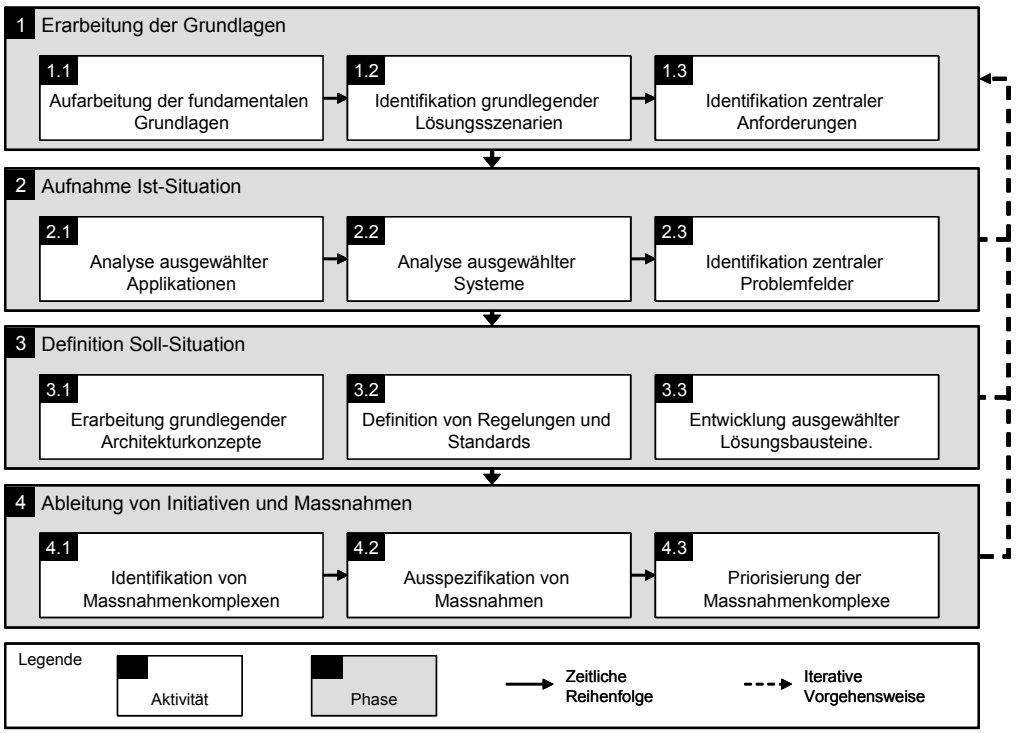

Abbildung 44: Vorgehensmodell Winterthur

Dargestellt werden wiederum die wesentlichen Projektphasen und ihre Aktivitäten. Eine Besonderheit stellt die Phase „Definition Soll-Situation“ dar: Ihre Aktivitäten werden in permanenter Abstimmung untereinander parallel durchgeführt. Der gestrichelte Pfeil deutet auch hier das iterative Vorgehen an.

Die einzelnen Aktivitäten können wie folgt zusammengefasst werden (vgl. Tabelle 21):

Nr.	Aktivität	Beschreibung	Zentrale Ergebnisse
1 Erarbeitung der Grundlagen			
1.1	Aufarbeitung der fundamentalen Grundlagen	Aufarbeitung und Abgrenzung der Themenbereiche Sicherheit und Datenschutz. Analyse grundlegender Autorisierungskonzepte. Positionierung des Projektes innerhalb der Themengebiete.	Abgegrenzte Themengebiete

[456] Vgl. hierzu auch die ausführliche Beschreibung in Kapitel 4.2.

1.2	Identifikation grundlegender Lösungsszenarien	Identifikation von grundlegenden Lösungsszenarien der Autorisierung auf der Basis von Fallstudien und Literatur.	Grundlegende Lösungsszenarien
1.3	Identifikation zentraler Anforderungen	Erörterung der Anforderungen, die bei der Autorisierung in heterogenen Systemlandschaften zu beachten sind, auf der Basis internationaler Sicherheitsstandards.	Anforderungen an die Autorisierung
2 Aufnahme Ist-Situation			
2.1	Analyse ausgewählter Applikationen	Untersuchung ausgewählter Applikationen mit dem Fokus auf das Zusammenwirken unterschiedlicher Autorisierungskomponenten.	Applikationsbewertungen
2.2	Analyse ausgewählter Systeme	Bewertung zentraler Autorisierungskomponenten im Hinblick auf ihre Stärken und Schwächen sowie die Chancen und Risiken der weiteren Verwendung.	Systembewertungen
2.3	Identifikation zentraler Problemfelder	Zusammenfassung der Bewertungsergebnisse zu zentralen Problemfeldern.	Zentrale Problemfelder
3 Definition Soll-Situation			
3.1	Erarbeitung grundlegender Architekturkonzepte	Die Erarbeitung grundlegender Architekturkonzepte umfasst die Auswahl zentraler Lösungsansätze.	Grundlegende Architekturkonzepte
3.2	Definition von Regelungen und Standards	Die Definition von Regelungen und Standards umfasst die Spezifikation zentraler Verantwortlichkeiten und Prinzipien.	Regelungen und Standards
3.3	Entwicklung ausgewählter Lösungsbausteine	Um zu beurteilen, ob einzelne Konzepte umsetzbar sind, gilt es, ausgewählte Lösungsbausteine der Soll-Lösung detailliert zu betrachten und zu spezifizieren.	Lösungsbausteine
4 Ableitung von Initiativen und Massnahmen			
4.1	Identifikation von Massnahmenkomplexen	Die Identifikation von Massnahmenkomplexen umfasst die Ableitung von Massnahmen und deren Bündelung zu Massnahmenkomplexen.	Massnahmenkomplexe
4.2	Ausspezifikation von Massnahmen	Die Ausspezifikation von Massnahmen beinhaltet die Beschreibung und Bewertung der Massnahmen.	Massnahmenbeschreibungen
4.3	Priorisierung der Massnahmenkomplexe	Um ggf. einzelne Massnahmenkomplexe zu realisieren, erfolgt die Priorisierung der Massnahmenkomplexe.	Priorisierte Massnahmenkomplexe

Tabelle 21: Aktivitäten Winterthur

6.3.3 Ableitung des Vorgehensmodells

Die Induktion des Vorgehensmodells umfasst zwei Schritte. In einem ersten Schritt werden die Aktivitäten der Fallstudien analysiert und konsolidiert. Dabei werden Aktivitäten, die eine ähnliche funktionale Verrichtung umfassen, im induzierten Vorgehensmodell zusammengefasst. Eine besondere Rolle spielen hierbei die Ergebnisse der Aktivitäten. Aktivitäten mit gleichen oder ähnlichen Ergebnissen deuten auf zu konsolidierende Verrichtungseinheiten hin. Tabelle 22 zeigt das Ergebnis der Konsolidierung. Für jede induzierte Aktivität werden die konsolidierten Ergebnisse sowie die korrespondierenden Aktivitäten der Fallstudien dargestellt. Die Aktivitäten sind in der Tabelle bereits den induzierten Phasen zugeordnet. Die Ableitung der Phasen erfolgt analog zur Bestimmung der Aktivitäten durch die Zusammenfassung der Phasen, die ähnliche Verrichtungseinheiten umfassen. Aktivitäten, die ihren Ur-

sprung lediglich in einer der analysierten Fallstudien haben, werden im Sinne der Konfiguration[457] als „optional“ gekennzeichnet.

Nr.	Aktivität	Ergebnisse	Aktivität aus Fallstudie	
			Credit Suisse	Winterthur
1 Vorstudie				
1.1	Themengebiet strukturieren und abgrenzen	Abgegrenzte Themengebiete	1.1	1.1
1.2	Potenzielle Lösungsbeiträge erheben und auswerten	Aufgearbeitete Lösungsbeiträge	1.2	1.2
1.3	Autorisierungsanforderungen erheben	Autorisierungsanforderungen	1.3, 2.2	1.3
1.4	Zentrale Begriffe definieren (optional)	Glossar	1.4	–
2 Aufnahme Ist-Situation				
2.1	Ausgewählte Applikationen bewerten (optional)	Applikationsbewertungen	–	2.1
2.2	Ausgewählte Autorisierungssysteme bewerten	Autorisierungssystembewertungen	2.1	2.2
2.3	Zentrale Problemfelder identifizieren	Zentrale Problemfelder	2.1	2.3
3 Definition Soll-Situation				
3.1	Autorisierungsarchitektur festlegen	Autorisierungsarchitektur	3.1, 3.2	3.1
3.2	Direktiven spezifizieren	Direktiven	3.2	3.2
3.3	Leitelemente definieren (optional)	Leitelemente	–	3.3
4 Definition Massnahmenkomplexe				
4.1	Massnahmenkomplexe ableiten	Massnahmenkomplexe	4.1	4.1, 4.2
4.2	Massnahmenkomplexe bewerten	Priorisierte Massnahmenkomplexe	4.2	4.3

Tabelle 22: Aktivitäten des induzierten Vorgehensmodells „Autorisierungsarchitektur“

In einem zweiten Schritt erfolgt die Ableitung des Vorgehensmodells. Die Definition der zeitlichen Abläufe zwischen den Phasen und Aktivitäten im induzierten Vorgehensmodell erfolgt auf der Basis von verhaltensstrukturellen Identitäten[458]: Ähnliche Aktivitätsabfolgen werden im induzierten Vorgehensmodell zusammengefasst. Abbildung 45 zeigt das induzierte Vorgehensmodell mit den vier Phasen „Vorstudie“, „Aufnahme Ist-Situation“, „Definition Soll-Situation“ sowie „Definition Massnahmenkomplexe“. Der gestrichelte Pfeil deutet das induzierte iterative Vorgehen an, das beide Fallstudien der Induktionsbasis aufweisen: Die entwickelten Ergebnisse wurden im Projektverlauf sukzessive detaillierter ausgestaltet. Die einzelnen Phasen werden im Folgenden überblicksartig dargestellt.

457 Vgl. Kapitel 5.1.2.
458 Vgl. Kapitel 5.1.2.

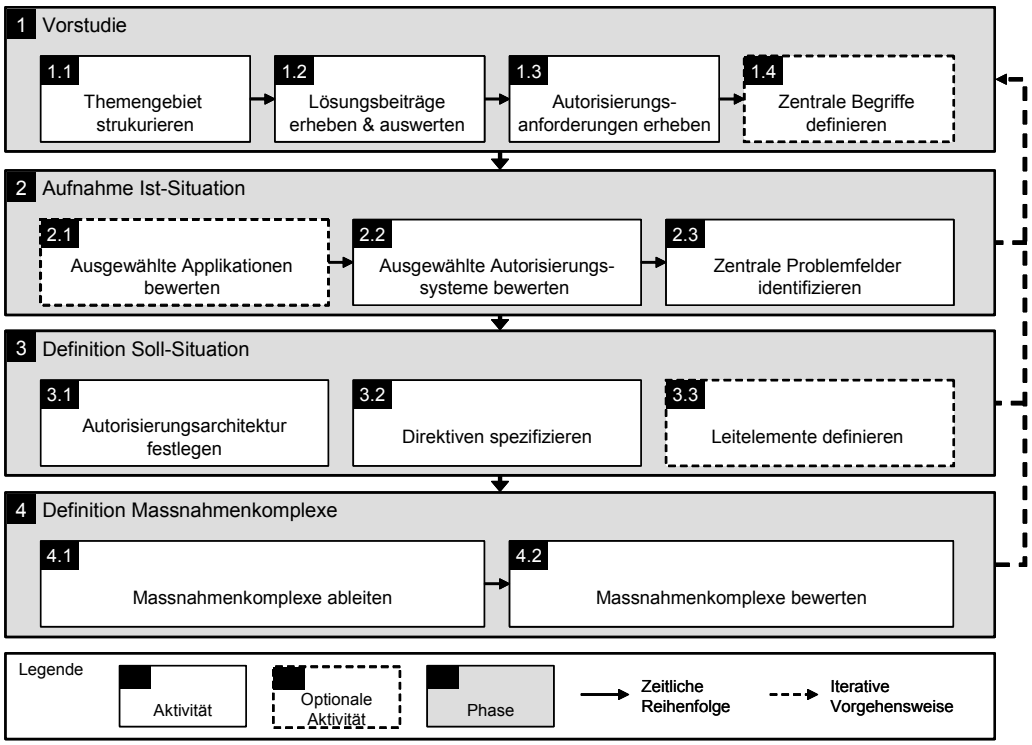

Abbildung 45: Induziertes Vorgehensmodell „Autorisierungsarchitektur“

Phase 1: Vorstudie

Im Rahmen der Vorstudie werden die wesentlichen Grundlagen zur Entwicklung der Autorisierungsarchitektur gelegt. Zu Beginn der Phase gilt es, den Gegenstandsbereich der zu entwickelnden Architektur abzugrenzen und zu untergliedern (Aktivität 1.1). Die Entwicklung der Autorisierungsarchitektur kann auf bereits existierende Beiträge aus Wissenschaft und Praxis aufbauen, die z.B. in Form von Literatur oder Standards zur Verfügung stehen. Diese Beiträge müssen erhoben und entsprechend dem Anwendungskontext aufgearbeitet werden (Aktivität 1.2). Sicherheitsstandards wie der ISO/IEC 17799 fordern, dass Anforderungen an die Autorisierung erhoben und dokumentiert werden.[459] Die Anforderungen müssen somit vor der eigentlichen Definition der Architektur bestimmt werden (Aktivität 1.3). Um eine einheitliche Sprache im Bereich der Autorisierung zu fördern, bietet sich darüber hinaus die Einführung eines Glossars an, das die verwendeten Fachbegriffe verbindlich definiert und dokumentiert (Aktivität 1.4).

Phase 2: Aufnahme Ist-Situation

In der zweiten Phase erfolgt die Ermittlung von Schwachstellen, die als Ausgangspunkt der Architekturentwicklung dienen. Um die Schwächen einzelner Autorisierungskomponenten angemessen zu berücksichtigen, erfolgt die Evaluation ausgesuchter Autorisierungskomponenten (Aktivität 2.2). Um auch systemübergreifende Schwachstellen der Autorisierung zu identifizieren, bietet sich darüber hinaus die Analyse ausgewählter Applikationen an (Aktivität 2.1). Schliesslich erfolgt die Konsolidierung der Ergebnisse aus den vorangegange-

459 Vgl. ISO 2000a, Kapitel 9.1; Kapitel 5.2.2.

nen Aktivitäten: Zentrale Problemfelder werden durch die Zusammenführung der ermittelten Schwachstellen identifiziert und gewichtet (Aktivität 2.3).

Phase 3: Definition Soll-Situation

Ziel dieser Phase ist es, wesentliche Gestaltungsoptionen und Handlungsanweisungen zur Lösung bzw. Regelung der identifizierten Schwachstellen zu erarbeiten. Durch die Definition und Auswahl zentraler Gestaltungsoptionen werden essentielle Aspekte der Soll-Autorisierungsarchitektur festgelegt (Aktivität 3.1). Wesentliche Lösungsprinzipien, die den erarbeiteten Gestaltungsoptionen zugrunde liegen, werden in Form von Direktiven schriftlich fixiert und detailliert (Aktivität 3.2). Einzelne Gestaltungsoptionen werden darüber hinaus durch die Spezifikation oder Entwicklung konkreter Infrastrukturkomponenten auf ihre Anwendbarkeit hin untersucht (Aktivität 3.3). Im Rahmen der Fallstudien zeigte sich, dass die Aktivitäten dieser Phase in enger Abstimmung untereinander parallel durchgeführt werden.

Phase 4: Definition Massnahmenkomplexe

In der letzten Phase erfolgt die Identifikation von Massnahmenkomplexen zur Umsetzung der erarbeiteten Lösungsansätze. Hierzu müssen in einem ersten Schritt Massnahmen auf Grundlage der bereits erarbeiteten Ergebnisse abgeleitet und unter Berücksichtigung inhaltlicher Verflechtungen zu Massnahmenkomplexen gebündelt werden (Aktivität 4.1). Abschliessend gilt es, die ermittelten Massnahmenkomplexe zu priorisieren und zu prüfen, ob die identifizierten Massnahmenkomplexe eine angemessene Reduktion der aufgedeckten Risiken gewährleisten (Aktivität 4.2).

6.3.4 Bewertung des konsolidierten Vorgehensmodells

Die zu entwickelnde Methode erhebt Anspruch auf Allgemeingültigkeit und strebt darüber hinaus Empfehlungscharakter an.[460] Im Folgenden wird dargelegt, inwieweit die induktiv abgeleitete und zu detaillierende Vorgehensweise diesen beiden Aspekten gerecht werden kann.

Die Identifikation von Strukturanalogien bildet einen wesentlichen Ausgangspunkt, damit der Forderung nach *Allgemeingültigkeit* Rechnung getragen werden kann.[461] Eine Analyse der Fallstudien im Hinblick auf Strukturanalogien zeigt zahlreiche Gemeinsamkeiten auf.[462] Beide Fallstudien weisen entsprechende Phasen mit übereinstimmenden Kernaktivitäten auf: Zunächst erfolgt die Erarbeitung der Grundlagen, dann die Analyse der Ist-Situation, gefolgt von der Definition der Soll-Situation. Abschliessend werden auf Basis der durchgeführten Aktivitäten Massnahmenkomplexe abgeleitet. Das Vorgehen sieht damit in Anlehnung an die Ansätze des Sicherheitsmanagements zunächst eine Identifikation und Bewertung existierender

460 Vgl. Kapitel 5.1.2.
461 Vgl. Kapitel 5.1.2; Schütte 1998, S. 237f.
462 Vgl. hierzu auch im Folgenden Tabelle 22.

Schwachstellen vor, um dann risikoorientiert Massnahmen zur Beseitigung der Schwachstellen zu entwickeln. Bei den Gemeinsamkeiten der Fallstudien handelt es sich um semantikbehaftete Strukturanalogien:[463] Die Identität der Strukturbausteine lässt sich inhaltlich erklären. Die Übereinstimmung der Fallstudien und die Parallelen zum Sicherheitsmanagement rechtfertigen somit den Anspruch der konsolidierten Vorgehensweise auf Allgemeingültigkeit.

Der *Empfehlungscharakter* einer Methode kann nur eingeschränkt sichergestellt und nachgewiesen werden.[464] Hierbei spielt die Allgemeingültigkeit des Anforderungssystems an die Methode eine besondere Rolle. Diesem Aspekt wird dadurch Rechnung getragen, dass die Ableitung der Anforderungen auf Basis etablierter Sicherheitsstandards erfolgt.[465] Die ermittelten Anforderungen[466] werden durch das induktiv abgeleitete Vorgehensmodell wie folgt adressiert:

- Einbezug existierender Leitlinien und Vorgaben: Im Rahmen des induzierten Vorgehensmodells werden existierende Leitlinien und Vorgaben, die in den Unternehmen vor allem in Form von Weisungen vorliegen, durch die Aktivität „Autorisierungsanforderungen erheben“ der Phase „Vorstudie“ berücksichtigt.

- Durchführung einer Risikoanalyse: Um dem Wirtschaftlichkeitsprinzip gerecht zu werden, müssen existierende Schwachstellen identifiziert, bewertet und erst dann risikogerecht adressiert werden. Das induzierte Vorgehensmodell greift diese Aspekte in der Phase „Aufnahme Ist-Situation“ auf. Durch die Analyse von Applikationen und Systemen werden Risiken identifiziert und abschliessend bewertet.

- Ableitung angemessener Massnahmen: Auf Basis der identifizierten Risiken müssen Massnahmen abgeleitet werden, die die Risiken auf ein angemessenes Mass reduzieren. Das induzierte Vorgehensmodell berücksichtigt diese Anforderungen in den Phasen „Definition Soll-Situation“ und „Definition Massnahmenkomplexe“. Die Phase „Definition Soll-Situation“ umfasst die Aktivitäten zum Entwurf von Gestaltungsoptionen und -richtlinien. Die Phase „Definition Massnahmenkomplexe“ bündelt Massnahmen, die zur Umsetzung der Gestaltungsoptionen notwendig sind, zu Massnahmenkomplexen. Diese werden sodann bewertet, um die Umsetzung der Massnahmenkomplexe zu fördern, die das beste Kosten-Nutzen-Verhältnis aufweisen.

- Definition von Leitlinien: Sicherheitsstandards sehen für komplexe IT-Systeme die Erarbeitung von Leitlinien vor, die konkrete Handlungsanleitungen darstellen. Dem entspricht die Erarbeitung von Direktiven, die innerhalb der Aktivität „Direktiven spezifizieren“ durchzuführen ist.

---

463 Vgl. Kapitel 5.1.2.
464 Vgl. im Folgenden Kapitel 5.1.2.
465 Vgl. Kapitel 5.1.2.
466 Vgl. Kapitel 5.2.

Das induzierte Vorgehensmodell adressiert folglich die identifizierten Anforderungen. Die adäquate Berücksichtigung der Anforderungen innerhalb der Entwicklung der einzelnen Aktivitäten sichert den Empfehlungscharakter der Vorgehensweise.

6.4 Aktivitäten

Im Folgenden soll das induzierte Vorgehensmodell detaillierter dargestellt werden. Das Vorgehen wird im Rahmen der weiteren Ausführungen in Aktivitäten, nicht in Techniken zerlegt. Diese Entscheidung lässt sich wie folgt begründen:

Eine Technik stellt im Business Engineering eine Vorschrift zur Erstellung und Dokumentation von Ergebnissen dar.[467] Im Rahmen der folgenden Ausführungen wird nur eingeschränkt darauf eingegangen, wie einzelne Ergebnisse zu dokumentieren sind. Die Sprache bzw. Notation der Ergebnisse steht nicht im Vordergrund. Da die Analyse der Fallstudien die Verwendung unterschiedlicher Notationen zur Spezifikation der Ergebnisse gezeigt hat, entspricht die Vorstellung einer ausgewählten Sprache bzw. Notation nicht dem Allgemeingültigkeitsanspruch und Empfehlungscharakter der Methode.

Die Wahl des geeigneten Abstraktionsgrades der Standardisierung ist für die Methodenentwicklung von elementarer Bedeutung.[468] Eine zu ausgeprägte Konkretisierung schränkt den Anwendungsbereich der zu entwickelnden Methode sehr stark ein. Für jede Aktivität wird daher in den Fällen, in denen unterschiedliche Vorgehensweisen praktikabel sind, das Spektrum möglicher Techniken aufgezeigt. Anstatt eine Technik detailliert darzustellen, werden unterschiedliche Handlungsoptionen innerhalb einer Aktivität aufgezeigt und erläutert.

6.4.1 Aktivitäten der Phase „Vorstudie“

6.4.1.1 Themengebiet strukturieren und abgrenzen

Zielsetzung der Aktivität „Themengebiet strukturieren und abgrenzen“ ist es, den Gegenstandsbereich der zu entwickelnden Architektur abzugrenzen und zu untergliedern, um so eine vollständige, überschneidungsarme und arbeitsteilige Entwicklung der Architektur zu gewährleisten.

Zur Abgrenzung und Strukturierung bietet sich die Entwicklung eines Ordnungsrahmens an. Ein Ordnungsrahmen ist ein Modell, dessen Konstruktion Verzeichnisbereiche liefert.[469] Mit der Bereitstellung von Denkstrukturen und Verzeichnisbereichen liefern Ordnungsrahmen methodische Unterstützung in Entwicklungsprozessen. Um die Konstruktion von Ordnungs-

467 Vgl. Winter 2003b, S. 88: Kapitel 5.1.1.
468 Vgl. Kapitel 5.1.2.
469 Vgl. im Folgenden vom Brocke 2003, S. 128.

rahmen zu unterstützen, werden u.a. Gliederungsprinzipien zur Verfügung gestellt, nach denen gesonderte Verzeichnisbereiche zu bilden sind.[470] Im Sinne dieser Unterstützung werden im Folgenden unterschiedliche Gliederungsdimensionen für die Themengebiete Sicherheit und Autorisierung vorgestellt.

Das Themengebiet Autorisierung kann zum einen auf der Basis der Grundfunktionen der Sicherheit abgegrenzt werden. Neben der Autorisierung sind somit die Identifikation und Authentisierung, die Beweissicherung sowie die Übertragungssicherung als Themengebiete relevant.[471] Der Standard ISO/IEC 10181 verwendet eine ähnliche Abgrenzung, die beispielsweise im Rahmen der Fallstudie Credit Suisse Berücksichtigung findet:[472] Neben den Themengebieten Authentisierung und Autorisierung werden die Sicherheitsziele Nichtabstreitbarkeit, Vertraulichkeit und Integrität in die Abgrenzung mitaufgenommen.[473]

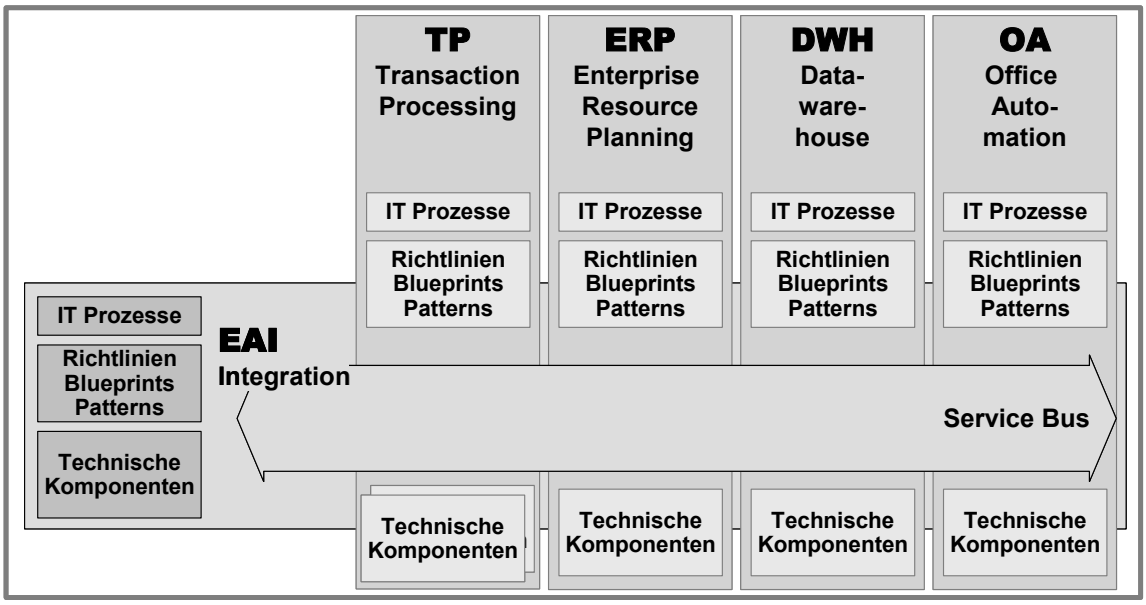

Abbildung 46: Plattformen bei der Winterthur[474]

Die Strukturierung der zu entwickelnden Autorisierungsarchitektur kann weiterhin nach der unternehmensspezifischen Untergliederung der Applikations- bzw. Systemlandschaft erfolgen. Gewachsene Applikationslandschaften mit vielen hundert Applikationen lassen sich nicht als Ganzes steuern.[475] Die Gesamtlandschaft wird daher in handhabbare Einheiten zerlegt. Bei der Credit Suisse wurden zu diesem Zweck sogenannte „Applikationsdomänen" definiert. Es handelt sich dabei um Gruppierungen von Applikationen und Daten, die einem gemeinsamen Business-Bereich zugerechnet werden können. Insgesamt sind ca. 20 solche Applikationsdomänen definiert. Bei der Winterthur sind die Applikationen mit ihren Systemen in fünf technische „Plattformen" unterteilt (vgl. Abbildung 46). Neben den vier primären Platt-

470 Vgl. vom Brocke 2003, S. 128f.
471 Vgl. Kapitel 2.2.3.
472 Vgl. Kapitel 4.1.
473 Vgl. ISO 1996a.
474 Vgl. hierzu auch Kapitel 4.2.
475 Vgl. im Folgenden Schwinn/Hagen 2006, S. 11.

formen „Transaction Processing“, „Enterprise Ressource Planning“, „Data Warehouse“ und „Office Automation“ existiert die Integrationsplattform „Enterprise Application Integration (EAI)“.

Zur weiteren Untergliederung des Themengebietes Autorisierung bieten sich auch die bereits im Unternehmen verwendeten Sicherheitsstandards an. Der international etablierteste Sicherheitsstandard ISO/IEC 17799 untergliedert das Themengebiet Autorisierung beispielsweise in acht Unterkapitel.[476] Die drei Unterkapitel „Application Access Control“, „Operating System Access Control“ und „Network Access Control“ thematisieren die Autorisierung aus der Perspektive unterschiedlicher Softwareschichten. Die Kapitel „Business Requirements for Access Control“, „User Access Management“, „User Responsibilities“ und „Monitoring System Access and Use“ greifen schichtenübergreifende Anforderungen an die Autorisierung auf. Das Kapitel „Mobile Computing and Teleworking“ behandelt schliesslich ausgewählte Aspekte der Autorisierung im Umfeld besonderer Risiken.

Das Themenfeld Autorisierung kann weiterhin nach den handelnden Akteuren in die Bereiche „Applikationen“ und „zentrale Autorisierungsinfrastruktur“ untergliedert werden: Während die einzelnen Applikationen für die Entwicklung ihrer Berechtigungskonzepte verantwortlich sind, stellen die zentralen Autorisierungsinfrastrukturanbieter die Werkzeuge zur Kontrolle und Verwaltung der Zugriffsberechtigung systemübergreifend zur Verfügung. Analog zur Fallstudie Winterthur können die Anbieter der Autorisierungsinfrastruktur weiter untergliedert werden:[477] So bieten einige Anbieter ihre Dienste unterschiedlichen Applikationen in einem begrenzten Umfeld z.B. plattformbezogen an. Andere Anbieter erbringen ihre Dienstleistungen hingegen global für alle Applikationen des Unternehmens.

Bei der Entwicklung eines Ordnungsrahmens für die Autorisierung sind bereits existierende Ordnungsrahmen zu berücksichtigen. Strukturen bestehender Ordnungsrahmen wie z.B. Plattformen sind soweit möglich zu übernehmen, um auf bekannte und etablierte Gliederungsdimensionen zurückzugreifen. Sollten neue Dimensionen notwendig sein, bietet es sich an, den neu konzipierten Ordnungsrahmen zu den etablierten Ordnungsrahmen abzugrenzen und existierende Abhängigkeiten und Zusammenhänge aufzuzeigen. Der entwickelte Ordnungsrahmen sollte im Rahmen des Architekturprojektes frühzeitig kommuniziert werden, um bereits im Vorfeld späteren Modifikationen vorzubeugen, die ggf. eine umfassende Restrukturierung der ganzen Architektur nach sich ziehen. Da der Ordnungsrahmen als zentrales Gliederungsinstrument eine herausragende Bedeutung hat, sollte er allgemein akzeptiert sein. Eine Ablehnung des Ordnungsrahmens durch einzelne projektentscheidende Mitarbeiter kann ein Akzeptanzproblem für die ganze Architektur nach sich ziehen.

476 Vgl. im Folgenden ISO 2000a, Kapitel 9.
477 Vgl. Kapitel 4.2.

6.4.1.2 Potenzielle Lösungsbeiträge erheben und auswerten

Im Rahmen der Entwicklung einer Autorisierungsarchitektur kann in weiten Teilen auf bereits existierenden Grundlagen aufgebaut werden, die etwa in Form von Standards zur Verfügung stehen. Die Verwendung von allgemein akzeptierten und erprobten Grundlagen ermöglicht die effiziente Entwicklung qualitativ hochwertiger Lösungen. Die Zielsetzung dieser Aktivität ist es deshalb, eine adäquate Wissensgrundlage für die Architekturentwicklung auf Basis des ermittelten Ordnungsrahmens zusammen zu stellen. Dabei können Lösungsbeiträge aus der Literatur und Lösungsbeiträge aus der Praxis unterschieden werden.[478]

Lösungsbeiträge aus der Literatur stehen in Form von Publikationen zur Verfügung. Im Bereich der Autorisierung sind hier vor allem etablierte Standards von Bedeutung. Diese lassen sich in zwei Klassen unterteilen. Standards wie der bereits zuvor diskutierte ISO/IEC 17799[479] definieren Anforderungen an die Sicherheit von Informationssystemen und somit auch an die Autorisierung. Publikationen wie der RBAC-Standard[480] beschäftigen sich hingegen mit der Gestaltung von Autorisierungskomponenten und -systemen. Im Rahmen der Fallstudien fanden folgende Quellen bzw. Standards besondere Berücksichtigung:

Quelle	Kurzbeschreibung	Verwendung
Quellen bzw. Standards im Umfeld Anforderungen		
ISO/IEC 17799[481]	International etablierter Anforderungskatalog für die Sicherheit von Informationssystemen	Basis zur Erhebung von Anforderungen an die Autorisierung
Grundschutzhandbuch[482]	Umfassender Katalog von Sicherheitsmassnahmen, entwickelt vom deutschen Bundesamt für Sicherheit in der Informationstechnik	Ergänzender Einsatz zum ISO/IEC 17799
The Standard of Good Practice for Information Security [483]	Umfangreicher Anforderungskatalog für die Sicherheit von Informationssystemen	Ergänzender Einsatz zum ISO/IEC 17799
Quellen bzw. Standards im Umfeld Autorisierungskomponenten bzw. Autorisierungssysteme		
NIST Standard for Role-Based Access Control[484]	Standard für die rollenbasierte Autorisierung: Definiert wesentliche Entitäten eines rollenbasierten Autorisierungskonzepts sowie ihr Zusammenwirken	Grundlage für die Entwicklung und Beurteilung einzelner Autorisierungskomponenten
ISO/IEC 10181-3[485]	Framework für die Autorisierung: Beschreibt u.a. einzelne Autorisierungskomponenten und ihr Zusammenwirken	Grundlage für die Entwicklung und Beurteilung von Autorisierungskomponenten in verteilten Systemen
ERBAC[486]	Konzept für die systemübergreifende, rollenbasierte Autorisierung: Definiert wesentliche Entitäten eines systemübergreifenden rollenbasierten Autorisierungskonzepts sowie ihr Zusammenwirken	Grundlage für die Entwicklung systemübergreifender Berechtigungskonzepte

478 Vgl. hierzu Herrmann 2006, Kapitel 4.3.2.2.2.
479 Vgl. Kapitel 5.2.2.1; ISO 2000a.
480 Vgl. Kapitel 2.3.2; Ferraiolo et al. 2001.
481 Vgl. Kapitel 5.2.2.1; ISO 2000a.
482 BSI 2004.
483 ISF 2003.
484 Vgl. Kapitel 2.3.2; Ferraiolo et al. 2001.
485 ISO 1996b.
486 Vgl. Kapitel 2.3.3; Kern et al. 2002.

Symposium on Access Control Models and Technologies[487]	Diverse Quellen zum Thema Autorisierung	Grundlage für die Entwicklung und Beurteilung von Autorisierungs-lösungen

Tabelle 23: Wesentliche in den Fallstudien verwendete Quellen

Zusätzlich zur Erhebung von Publikationen empfiehlt sich der direkte Austausch mit anderen Praktikern, Beratern, Herstellern und Wissenschaftlern. Zum einen bieten Tagungen und Konferenzen einen geeigneten Rahmen zur vertieften Diskussion. Zum anderen kann auch der direkte Kontakt zu Ansprechpartnern gesucht werden, die mit der Thematik befasst sind. Ein persönlicher Austausch mit fachlichen Kollegen verspricht eine differenzierte Darstellung der Vor- und Nachteile einer Lösung.

Je nach Anzahl der identifizierten Lösungsbeiträge empfiehlt sich eine Auswahl der Beiträge, die eine möglichst umfassende und hochwertige Abdeckung des Problembereichs sicherstellen.[488] Dabei können inhaltliche und formale Kriterien Anwendung finden. Inhaltliche Kriterien sind beispielsweise Aktualität, Qualität und Detaillierungsgrad des Lösungsbeitrags. Als formales Kriterium kann beispielsweise der Abdeckungsgrad des Beitrags bezüglich der zu behandelnden Fragestellungen herangezogen werden.

6.4.1.3 Autorisierungsanforderungen erheben

Ziel der Aktivität „Autorisierungsanforderungen erheben“ ist es, die Anforderungen an die Autorisierung zu ermitteln und zu konsolidieren. Um die einzelnen Anforderungen fokussiert adressieren zu können, empfiehlt es sich, die Anforderungen den unterschiedlichen Teilbereichen des entwickelten Ordnungsrahmens zuzuordnen.

Sicherheitsstandards wie der ISO/IEC 17799 verlangen explizit, dass fachliche Anforderungen an die Autorisierung erhoben und dokumentiert werden.[489] Entsprechende Mitarbeiter des Fachbereichs sind daher durch Interviews bei der Erhebung der Anforderungen zu berücksichtigen. Relevant sind hier zum einen die Mitarbeiter, die in Zusammenarbeit mit der IT die Zugriffsberechtigungen definieren. Zum anderen ist das Management des Fachbereichs zu involvieren, da es letztendlich die Kosten und Risiken, die mit der Autorisierung einhergehen, trägt. Im Umfeld der IT gilt es einerseits technische Anforderungen zu beachten, die durch eine Befragung der Autorisierungsinfrastrukturanbieter ermittelt werden. Andererseits sind Organisationseinheiten wie die „Zentrale Benutzerverwaltung“ zu berücksichtigen, die für die Pflege der Zugriffsberechtigungen verantwortlich sind.

Neben Interviews kommt insbesondere bestehenden Weisungen und intern verwendeten Sicherheitsstandards eine zentrale Bedeutung bei der Berücksichtigung von Anforderungen zu. Sicherheitsstandards wie der ISO/IEC 17799 fordern präzise definierte und dokumentierte

487 Vgl. die Konferenzbände unter http://portal.acm.org/toc.cfm?id=SERIES10694.
488 Vgl. Herrmann 2006, Kapitel 4.3.2.2.
489 Vgl. ISO 2000a, Kapitel 9.1

Zugriffsregelungen.[490] Diese Regelungen müssen den gesetzlichen und vertraglichen Verpflichtungen Rechnung tragen. Um Weisungen und interne Sicherheitsstandards angemessen einzubeziehen, empfiehlt sich eine Rücksprache mit den Mitarbeitern der verantwortlichen Abteilungen wie Revision, Risiko- oder Sicherheitsmanagement.

Die identifizierten Anforderungen sind zu konsolidieren, um redundante Aussagen zu eliminieren und die Anzahl der Anforderungen auf ein überschaubares Mass zu reduzieren.[491] Die Anforderungen sind dazu auf Korrelation, Komplementarität und Konkurrenz zu prüfen. Korrelierende Aussagen werden zu einer Aussage zusammengefasst. Komplementäre Anforderungen, die sich neutral zueinander verhalten, bleiben ebenso wie konkurrierende Anforderungen separat erhalten.

Nicht jede Anforderung hat die gleiche Relevanz für die Unternehmung, so dass sich vor allem bei einer Vielzahl von Anforderungen eine Priorisierung empfiehlt. Die Priorisierung erfolgt durch eine Gewichtung der einzelnen Anforderungen. Regulativen und vertraglichen Anforderungen sollte dabei eine hohe Gewichtung zukommen. In gleicher Weise sollten Anforderungen berücksichtigt werden, die auf der Basis von Sicherheitsstandards ermittelt wurden.[492]

Um die Anforderungen im weiteren Verlauf des Projektes nicht zu vernachlässigen, bietet es sich an, die einzelnen Anforderungen den unterschiedlichen Themenkomplexen der Autorisierung zuzuordnen. Zur Strukturierung kann dabei der bereits erstellte Ordnungsrahmen herangezogen werden (vgl. Tabelle 24). Im weiteren Verlauf des Projektes ist dann nachzuhalten, ob eine Anforderung im vorgesehenen Themenkomplex berücksichtigt wurde.

Nr.	Anforderung	Bereich des Ordnungsrahmens		
		Application Access Control	Operating System Access Control	Network Access Control
1	Begrenzter Zugriff auf Netzwerkressourcen nach dem „Need to Know“ Prinzip			●
2	Zugriff auf die Daten einer Applikation erfolgt auf der Basis eines definierten Sicherheitskonzepts	●		
3	Gescheiterte Autorisierungsversuche werden aufgezeichnet	●	●	●
…	…			

Tabelle 24: Zuordnung der Anforderungen zu den Bereichen des Ordnungsrahmens (Beispiel)

490 Vgl. ISO 2000a, Kapitel 9.1
491 Vgl. im Folgenden auch Hafner/Winter 2005, S. 213f.
492 Zur Bedeutung von Sicherheitsstandards vgl. Kapitel 5.2.2.

6.4.1.4 Zentrale Begriffe definieren

Zielsetzung dieser Aktivität ist es, eine einheitliche Sprache im Bereich der Autorisierung zu fördern. Dazu werden die verwendeten Fachbegriffe in einem Glossar definiert und dokumentiert.[493] Im Umfeld international tätiger Unternehmen bietet sich hierbei die Berücksichtigung unterschiedlicher Sprachen an. Während die bedeutenden Sicherheitsstandards in der Regel in englischer Sprache verfasst sind, existieren im Unternehmen etablierte Begriffe auch in der Muttersprache der verantwortlichen Mitarbeiter.

Vor allem in den frühen Phasen der Architekturentwicklung, in denen die unterschiedlichen Begriffsverständnisse der beteiligten Mitarbeiter noch sehr ausgeprägt sind, kann ein Glossar die Kommunikation verbessern. Dies gilt insbesondere für das Themengebiet der Autorisierung, in dem einzelne Mitarbeiter traditionell sehr dezentral und eher isoliert agieren.[494] Mit zunehmender Anzahl der am Projekt beteiligten Mitarbeiter steigt der Nutzen eines Glossars.[495] Ein kritischer Punkt bei der Erstellung eines Glossars ist die Vermeidung von Sprachdefekten. In diesem Zusammenhang unterscheidet ORTNER fünf Arten potenzieller Defekte und zeigt Möglichkeiten ihrer Behebung auf (vgl. Tabelle 25).

Begriffsdefekt	Beschreibung	Behebung
Synonym	Unterschiedliche Bezeichnungen mit identischer Bedeutung	Einsatz eines Synonymwörterbuchs
Homonym	Gleiche Bezeichnungen mit unterschiedlicher Bedeutung	Beseitigung durch die Schaffung eindeutiger Bezeichnungen
Äquipollenz	Unterschiedliche Bezeichnungen, die in ihrer Bedeutung lediglich teilweise übereinstimmen	Aufdeckung und bei grosser Überlappung Beseitigung
Vagheit	Mangelnde Abgrenzung von Begriffen	Genaue Definition von Begriffen mit expliziter Abgrenzung
Falsche Bezeichnung	Abweichung der tatsächlichen von der zunächst suggerierten Wortbedeutung	Einführung von Bezeichnungen, die der suggerierten Bedeutung nicht entgegenstehen

Tabelle 25: Begriffsdefekte und Möglichkeiten ihrer Behebung[496]

Bei der Erarbeitung eines unternehmensspezifischen Glossars empfiehlt sich als Ausgangspunkt ein bereits existierendes Glossar. Gängige Sicherheitsstandards umfassen in der Regel ein Glossar, so dass sie eine geeignete Ausgangsbasis darstellen (vgl. Tabelle 26). Um die Akzeptanz und Anwendbarkeit eines Glossars im Unternehmen sicherzustellen, ist es im Hinblick auf unternehmensspezifische Gegebenheiten anzupassen und zu erweitern.

493 Vgl. Herrmann 2006, Kapitel 4.3.2.10.3.
494 Vgl. Kapitel 4.1 und 4.2.
495 Vgl. Herrmann 2006, Kapitel 4.3.2.10.3.
496 Vgl. Ortner 1997, S. 176.

Sicherheitsstandard	Umfang	Sprache
International bedeutende Standards (kostenpflichtig)		
BS 7799-2[497]	12 Begriffe	Diverse, u.a. Englisch, Deutsch
ISO/IEC 17799[498]	6 Begriffe	Diverse, u.a. Englisch, Deutsch
Standards mit umfangreichem Glossar (frei verfügbar)		
Information Security Guideline for New South Wales Government[499]	> 100 Begriffe	Englisch
IT-Grundschutzhandbuch[500]	> 100 Begriffe	Deutsch

Tabelle 26: Ausgewählte Sicherheitsstandards mit Glossar

6.4.2 Aktivitäten der Phase „Aufnahme Ist-Situation“

6.4.2.1 Ausgewählte Applikationen bewerten

Ziel der Aktivität ist es, ausgewählte Applikationen auf existierende Autorisierungsschwächen zu untersuchen. Im Sinne der effektiven und effizienten Autorisierung[501] gilt es, einerseits Sicherheitsrisiken und andererseits Ineffizienzen aufzudecken.

Grosse Unternehmen verfügen über eine Vielzahl von Applikationen, die aus Gründen der Wirtschaftlichkeit nicht alle in die Analyse miteinbezogen werden können. Daher müssen für die durchzuführende Analyse gezielt Applikationen ausgewählt werden. Folgende Kriterien bieten sich u.a. für die Auswahl an:[502]

- Berücksichtigung von Applikationen unterschiedlicher Business-Bereiche und Plattformen: Steht die gesamte Applikationslandschaft im Mittelpunkt der Analyse, so sollten repräsentative Applikationen aus den unterschiedlichen Business-Bereichen[503] ausgewählt werden. Darüber hinaus sollten die unterschiedlichen technischen Plattformen[504] einer Unternehmung bei der Auswahl der Applikationen Berücksichtigung finden.

- Berücksichtigung geschäftskritischer Applikationen: Die eingeschränkte Verwendung, der Missbrauch oder der Ausfall von geschäftskritischen Applikationen stellen besondere Risiken für die Unternehmung dar. Um diese Risiken angemessen zu berücksichtigen, empfiehlt sich eine Analyse der geschäftskritischen Applikationen.

497 British Standards Institution 2002, S. 3f.
498 ISO 2000a, S. 1.
499 NSW GCIO 2003a, S. 73ff.
500 BSI 2005.
501 Vgl. Kapitel 5.2.
502 Ausgangspunkt: Fallstudie Winterthur, vgl. Kapitel 4.2.
503 Vgl. im Folgenden Schwinn/Hagen 2006, S. 11 und Kapitel 6.4.1.1.
504 Vgl. hierzu auch Kapitel 6.4.1.1.

- Berücksichtigung von Applikationen, die sich über mehrere Business-Bereiche bzw. Plattformen erstrecken: Verwenden unterschiedliche Business-Bereiche eine Applikation, so ist eine Kooperation dieser Bereiche z.B. im Umfeld der Berechtigungsadministration notwendig, die ggf. Abstimmungsprobleme nach sich zieht. Basieren Applikationen auf mehreren Plattformen, so sind auch hier technische und administrative Prozessschnittstellen zu schaffen. Beide Aspekte sind bei der Auswahl der Applikationen zu beachten.

Die eigentliche Bewertung der Applikationen vollzieht sich in zwei Schritten. Zunächst sind die einzelnen Applikationen zu analysieren. Anschliessend werden die ermittelten Schwächen übergreifend zusammengefasst. Der Analyse muss eine der vier Risikoanalysestrategien „Pragmatischer Ansatz", „Grundschutzansatz", „Detaillierte Risikoanalyse" oder „Kombinierter Ansatz"[505] zugrunde gelegt werden.[506] Kapitel 5.2 thematisiert die Vor- und Nachteile bzw. den empfohlenen Anwendungskontext der unterschiedlichen Strategien.

Dem Ansatz der *Pragmatischen Risikoanalyse* folgend, kann auf eine methodenbasierte Analyse verzichtet werden.[507] Da der Ansatz nicht auf definierten Methoden basiert, sondern auf der Erfahrung und dem Wissen einzelner Mitarbeiter, erfordert er in der Regel geringen Aufwand. Um dennoch eine strukturierte Analyse sicherzustellen, bietet sich die Verwendung von Dimensionen an, die eine vollständige und ganzheitliche Analyse fördern. Beispielsweise können in Anlehnung an das Business Engineering die Kategorien „Prozess" und „System" verwendet werden. Die Kategorie „Prozess" kann z.B. weiter in „Definition der Berechtigungen" und „Zuweisung von Berechtigungen an Mitarbeiter" zerlegt werden. Die Kategorie „System" kann u.a. in die Subkategorien „Zusammenspiel der Komponenten" und „Aufbau der Komponenten" unterteilt werden. Sicherheitsrisiken werden unter Berücksichtigung der definierten Dimensionen abschliessend als Schwächen erhoben (vgl. Tabelle 27) und ggf. gewichtet.

Nr.	Schwäche	Prozess		System	
		Definition Berechtigungen	Zuweisung Berechtigungen	Zusammenspiel Komponenten	Aufbau Komponenten
1	Fachbereich nicht involviert	●			
2	Kein durchgängiges, systemübergreifendes Rollenkonzepte	●			
3	Keine dokumentierten Prozesse	●	●		
4	Zahlreiche Autorisierungskomponenten am Zugriffskontrollprozess beteiligt			●	
	…				

Tabelle 27: Bewertung einer Applikation nach dem Pragmatischen Ansatz (Beispiel)

505 Da sich der Kombinierte Ansatz aus dem Grundschutzansatz und der Detaillierten Risikoanalyse zusammensetzt (vgl. Kapitel 5.2.1) wird im Folgenden nicht explizit auf den Kombinierten Ansatz eingegangen.

506 Vgl. Kapitel 5.2.1.

507 Vgl. im Folgenden Kapitel 5.2.1.4.

Erfolgt die Bewertung auf Basis des *Grundschutzansatzes*, sind die ausgewählten Applikationen auf Grundlage vorgegebener Kataloge zu analysieren.[508] Dazu sind die vordefinierten Massnahmen und Anforderungen auf Existenz bzw. Umsetzung zu prüfen. In einem ersten Schritt ist es erforderlich, die relevanten Massnahmen und Anforderungen zu ermitteln. Anschliessend erfolgt die Beurteilung ihrer Umsetzung und Erfüllung. In der Praxis werden hierfür unterschiedliche Bewertungsskalen verwendet. Tabelle 28 zeigt exemplarisch eine sechsstellige Bewertungsskala.

Bewertung	Beschreibung	Erklärung
1	Exzellent	Die Anforderungen sind in jeder Beziehung erfüllt.
2	Überdurchschnittlich	Die Anforderungen werden den Erwartungen entsprechend erfüllt. Verbesserungen sind möglich, aber nicht notwendig.
3	Durchschnittlich	Die Anforderungen sind mit ausreichender Qualität erfüllt. Planung und Umsetzung sind verbesserungswürdig.
4	Moderater Handlungsbedarf	Lediglich Minimalanforderungen sind erfüllt. Es besteht ein moderater Handlungsbedarf.
5	Hoher Handlungsbedarf	Minimalanforderungen sind nicht erfüllt. Es besteht ein hoher Handlungsbedarf.
6	Anforderungen nicht erfüllt	Die Anforderungen werden nicht im Mindesten erfüllt. Sofortmassnahmen müssen eingeleitet werden.

Tabelle 28: Bewertungsskala Grundschutzansatz (Beispiel)[509]

Entsprechend der *Detaillierten Risikoanalyse* können die einzelnen Applikationen auf der Basis existierender Risikoanalysetechniken bewertet werden.[510] Unterschieden werden dabei quantitative und qualitative Vorgehensweisen.[511] Das IT-Sicherheitshandbuch des deutschen Bundesamtes für Sicherheit in der Informationstechnik schlägt beispielsweise eine quantitative Risikobewertung auf einer verhältnisskalierten Skala anhand von Schadensausmass und Eintrittswahrscheinlichkeit vor.[512] Anschliessend erfolgt dann eine qualitative Einteilung der Risiken in „tragbar“ und „untragbar“. Es existiert eine Vielzahl unterschiedlicher Techniken zur Detaillierten Risikoanalyse (vgl. Tabelle 29).[513] Im Rahmen der Techniken kann auf existierende Bedrohungskataloge und beispielhafte Auflistungen von Schwachstellen zurückgegriffen werden (vgl. Tabelle 29). Grundsätzlich empfiehlt es sich wiederum, Verfahren zu verwenden, die bereits im Unternehmen eingesetzt werden.

Im Rahmen der vier Risikoanalysestrategien steht die Sicherheit der Applikationen im Mittelpunkt der Bewertung. Ineffizienzen, die keinen Einfluss auf die Sicherheit haben, werden daher nicht berücksichtigt und sind abschliessend gesondert zu identifizieren. Hierzu kann das Strukturierungsraster der beschriebenen *Pragmatischen Analyse* verwendet werden. Die Bewertung der Ineffizienzen kann durch eine Gewichtung oder eine Abschätzung der Einspa-

508 Vgl. Kapitel 5.2.2: Einzelne Kataloge werden dort ausführlich vorgestellt.
509 Vgl. Jörg/Rossbach 2002, S. 84
510 Vgl. Kapitel 5.2.1.
511 Vgl. Zentrum für sichere Informationstechnologie - Austria 2004, S. 45
512 Vgl. BSI 1992, S. 63f und 231ff.
513 Vgl. Zentrum für sichere Informationstechnologie - Austria 2004, S. 45; von Rössing 2005, S. 114.

rungspotenziale erfolgen. Auch die Ermittlung der Ineffizienzen erfolgt in zwei Schritten. Nach der Analyse der einzelnen Applikationen werden die ermittelten Schwächen übergreifend zusammengefasst.

Quelle	Beitrag		
	Technik	**Bedrohungen**	**Schwachstellen**
Information Security Guideline for New South Wales Government[514]	Part 1	Part 2	Part 2
ISO/IEC 13335-3[515]	Annex E	Annex C	Annex D
IT-Sicherheitshandbuch[516]	S. 63ff, S. 231ff	S. 207ff	S. 199ff
NIST Risk Management Guide for Information Technology Systems[517]	S. 8ff		

Tabelle 29: Ausgewählte Quellen zur Detaillierten Risikoanalyse

6.4.2.2 Ausgewählte Autorisierungssysteme bewerten

Der Bewertung der Applikationen liegt eine systemübergreifende, applikationsspezifische Sichtweise zugrunde. Um ergänzend auch die Schwächen einzelner Autorisierungskomponenten angemessen zu berücksichtigen, erfolgt im Rahmen dieser Aktivität die Evaluation ausgesuchter Autorisierungskomponenten. Analog zur Bewertung der Applikationen besteht auch das Ziel dieser Aktivität darin, Sicherheitsrisiken und Ineffizienzen aufzudecken.

Die Auswahl der im Einzelnen zu untersuchenden Autorisierungskomponenten sollte vor allem eigenentwickelte Komponenten berücksichtigen. Im Rahmen der Fallstudien zeigte sich, dass diese Komponenten teilweise nicht mehr über zeitgemässe Autorisierungskonzepte verfügen. Darüber hinaus bietet es sich an, besonders häufig wiederverwendete Komponenten zu evaluieren, die auch kritische Geschäftsapplikationen schützen.[518] Schliesslich sollte die Auswahl alle technischen Plattformen berücksichtigen.

Auch dieser Aktivität ist eine der vier Risikoanalysestrategien „Pragmatischer Ansatz“, „Grundschutzansatz“, „Detaillierte Risikoanalyse“ oder „Kombinierter Ansatz“ zugrunde zu legen. Im Rahmen dieser Ansätze steht die Sicherheit im Mittelpunkt der Bewertung. Ineffizienzen, die keinen Einfluss auf die Sicherheit haben, müssen gesondert berücksichtigt werden. Das Vorgehen dieser Aktivität ist somit identisch zur Bewertung der Applikationen.

514 NSW GCIO 2003b.
515 ISO 1998.
516 BSI 1992.
517 NIST 2002.
518 Zur Argumentation vgl. auch im Folgenden Kapitel 6.4.2.1.

In Anlehnung an die Fallstudie Winterthur können für die systematische Bewertung der Autorisierungskomponenten (Pragmatischer Ansatz) folgende Bewertungskriterien verwendet werden:[519]

- Berechtigungskonzept: Untersucht werden Entitäten wie „Nutzer", „Rolle" oder „Recht", die eine Autorisierungskomponente zur Vergabe von Berechtigungen bereitstellen, sowie die Beziehungen, die zwischen den Entitäten möglich sind. Festzustellen ist, ob das Berechtigungskonzept feingranular genug ist, um eine adäquate Vertraulichkeit sicherzustellen. Darüber hinaus sollte das Berechtigungskonzept eine konsistente Vergabe von Berechtigungen erlauben, eine effiziente Administration der Berechtigungen begünstigen und intuitiv verständlich sein.

- Werkzeug: Auch die Autorisierungskomponente selbst sollte eine effiziente Administration z.B. durch eine angemessene Benutzeroberfläche begünstigen. Falls das Werkzeug eine wiederverwendbare Infrastrukturkomponente darstellt, müssen funktional angemessene und gut dokumentierte Schnittstellen zur Verfügung stehen.

- Organisation: Die Administrationsprozesse zur Pflege der Berechtigungen sollten entsprechend vorhandener Regelungen klar geregelt und dokumentiert sein. Darüber hinaus ist ggf. eine Trennung von Administrationsaktivitäten, z.B. in Form des Vier-Augen-Prinzips, zu gewährleisten.

- Methodik: Für die Entwicklung von Berechtigungskonzepten sollten vor allem die wiederverwendbaren Infrastrukturautorisierungskomponenten eine methodische Unterstützung in Form von Checklisten, Vorgehensmodellen u.ä. bieten.

Im Rahmen der Fallstudien zeigte sich, dass eine zentrale Ursache von Problemen bei der Entwicklung und Pflege von Berechtigungen in den Berechtigungsschemata der entsprechenden Komponenten liegt.[520] Während die grundlegenden Entitäten „Nutzer", „Rolle" und „Berechtigungen" in allen Systemen gemäss gängiger Standards[521] vorhanden und umgesetzt sind, bestehen bei der detaillierten Spezifikation der einzelnen Berechtigungen erhebliche qualitative Unterschiede. Teilweise werden Zugriffsberechtigungen auf Daten und Funktionen in einen Datenstring kodiert, der ohne zusätzliche Dokumentation nicht zu entschlüsseln ist. Dem gegenüber ermöglichen es vor allem Standardlösungen wie SAP, die einzelnen Berechtigungen im System differenziert und dokumentiert zusammenzustellen (vgl. Abbildung 47). Dabei sind für eine Berechtigung Typinformationen hinterlegt, wodurch die einzelnen Werte, aus denen sich eine Berechtigung zusammensetzt, eindeutig z.B. als Funktion oder Verkaufsregion gekennzeichnet werden.

519 Vgl. Kapitel 4.2
520 Vgl hierzu insbesondere Fallstudie Winterthur, Kapitel 4.2.
521 Vgl. z.B. Ferraiolo et al. 2001, S. 224ff.

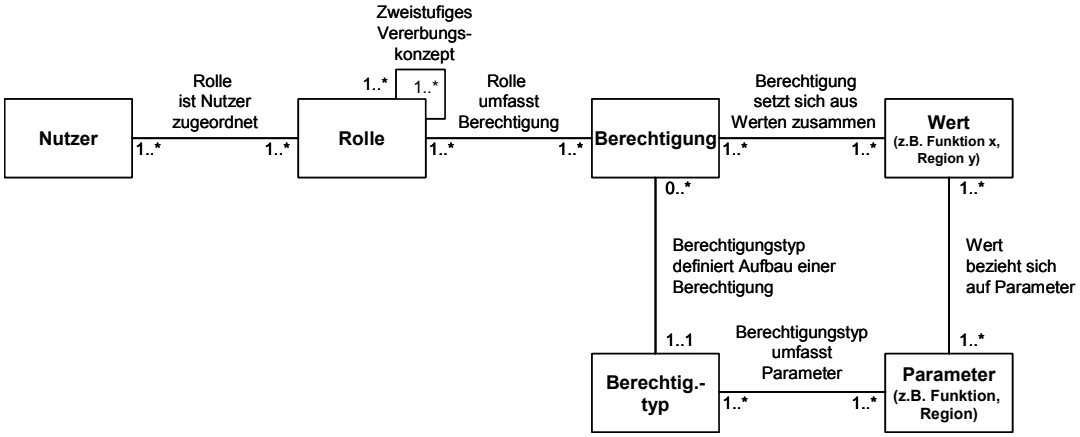

Abbildung 47: Vereinfachte Darstellung Berechtigungskonzept SAP[522]

6.4.2.3 Zentrale Problemfelder herausarbeiten

In der letzten Aktivität dieser Phase erfolgt die Zusammenführung der Ergebnisse aus den vorangegangenen Aktivitäten. Ziel ist es, durch Konsolidierung der ermittelten Schwachstellen zentrale Problemfelder zu identifizieren und zu gewichten. Um die Problemfelder auf ein überschaubares Mass zu reduzieren, gilt es, korrelierende Schwachstellen zusammenzufassen.

Skala	Eintrittswahrscheinlichkeit		Schadensausmass	
	Kategorie	Beschreibung	Kategorie	Beschreibung
5	Sehr häufig	Mehrmals am Tag	Sehr hoch	> 1 Mio. CHF
4	Häufig	Einmal am Tag oder weniger	Hoch	> 100'000 CHF
3	Mittel	Einmal im Monat oder weniger	Mittel	> 10'000 CHF
2	Selten	Einmal im Jahr oder weniger	Gering	> 1'000 CHF
1	Sehr selten	Einmal in fünf Jahren oder weniger	Sehr gering	< 1'000 CHF

Tabelle 30: Skalen für die Detaillierte Risikoanalyse (Beispiel)[523]

Um die Schwachstellen mit dem grössten Handlungsbedarf angemessen vorrangig zu behandeln, empfiehlt sich eine Gewichtung der konsolidierten Sicherheitsschwachstellen entsprechend der *Detaillierten Risikoanalyse*. Üblich ist eine Bewertung auf der Basis von Eintrittswahrscheinlichkeit und Schadensausmass,[524] die sowohl quantitativ als auch qualitativ ermittelt werden können.[525] Da eine quantitative Bewertung in vielen Fällen eine Genauigkeit vortäuscht, die durch die Methode der Schätzung nur eingeschränkt zu gewährleistet ist, werden in den letzten Jahren bevorzugt qualitative Skalen verwendet. Bewährt haben sich drei- bis

522 In Anlehnung an Hartje et al. 2003, S. 56ff.
523 In Anlehnung an NSW GCIO 2003c, Kapitel 4 und Zentrum für sichere Informationstechnologie - Austria 2004, S. 42.
524 Vgl. z.B. NIST 2002, S. 24.
525 Vgl. im Folgenden Zentrum für sichere Informationstechnologie - Austria 2004, S. 42.

fünfteilige Skalen, die für den jeweiligen Anwendungsbereich zu konkretisieren sind (vgl. Tabelle 30).

Die Aggregation von Schadensausmass und Eintrittswahrscheinlichkeit erfolgt bei qualitativen Verfahren auf der Basis von Matrizen (vgl. Tabelle 31).[526] Die einzelnen Risikokategorien, zu denen Schadensausmass und Eintrittswahrscheinlichkeit verdichtet werden, sind zu konkretisieren, wobei der aus der Risikokategorie resultierende Handlungsbedarf in die Definition einfliesst.[527] So könnte der Handlungsbedarf der Risikokategorie „Hoch" durch den Zusatz „kurzfristige Massnahmen sind dringend notwendig" aufgezeigt werden. Ergebnis der Bewertung ist dann eine Liste von konsolidierten Schwachstellen bzw. Risiken mit der entsprechenden Einstufung bezüglich Schadensausmass, Eintrittswahrscheinlichkeit und Risikohöhe.

Risikohöhe		Schadensausmass				
		Sehr gering	**Gering**	**Mittel**	**Hoch**	**Sehr Hoch**
Wahrscheinlichkeit	**Sehr selten**	Gering	Gering	Gering	Gering	Gering
	Selten	Gering	Mittel	Mittel	Mittel	Hoch
	Mittel	Gering	Mittel	Hoch	Hoch	Kritisch
	Häufig	Gering	Mittel	Hoch	Kritisch	Kritisch
	Sehr häufig	Gering	Hoch	Kritisch	Kritisch	Extrem

Tabelle 31: Aggregation von Schadensausmass und Eintrittswahrscheinlichkeit (Beispiel)[528]

Im Rahmen der geschilderten Vorgehensweise steht die Sicherheit im Mittelpunkt der Bewertung. Ineffizienzen, die keinen Einfluss auf die Sicherheit haben, sind wiederum gesondert zu berücksichtigen. Die Bewertung der Ineffizienzen kann quantitativ durch die Abschätzung monetärer Einsparungspotenziale oder qualitativ durch die Zuweisung entsprechender Potenzialkategorien durchgeführt werden.[529]

6.4.3 Aktivitäten der Phase „Definition Soll-Situation"

6.4.3.1 Autorisierungsarchitektur erarbeiten

Das Ziel der Aktivität „Autorisierungsarchitektur erarbeiten" besteht darin, wesentliche Gestaltungsoptionen zur Lösung der identifizierten Schwachstellen zu erarbeiten. Durch die Definition und Auswahl zentraler Gestaltungsoptionen werden essentielle Aspekte der Soll-Autorisierungsarchitektur determiniert. Die Spezifikation der Gestaltungsoptionen erfolgt

526 Vgl. im Folgenden NIST 2002, S. 24f.
527 Vgl. im Folgenden NIST 2002, S. 25.
528 In Anlehnung an NSW GCIO 2003c, Attachment 1.
529 Vgl. Kapitel 5.2.1.

durch Entwicklung entsprechender Modelle und eine textuelle Beschreibung der zu realisierenden Sachverhalte.

Aus der Perspektive des Sicherheitsmanagements kommt der Aktivität die Aufgabe zu, potenzielle Möglichkeiten zur Eliminierung oder Reduktion der identifizierten Risiken aufzuzeigen.[530] Die Ableitung von Massnahmen zur Umsetzung der Architektur sowie eine entsprechende Kosten-Nutzen-Analyse der notwendigen Massnahmen erfolgt in weiteren, sich anschliessenden Aktivitäten.

Im Rahmen der Fallstudien werden drei grundlegende, zentrale Problemstellungen adressiert:

- Integration der Autorisierung: Die systemübergreifende Administration von Berechtigungen motiviert die Fragestellung, ob und wie Berechtigungen unterschiedlicher Autorisierungskomponenten systemübergreifend integriert werden können. Der Einsatz dedizierter Integrationswerkzeuge, die systemübergreifende Berechtigungskonzepte realisieren, verspricht Vorteile in Wartung und Pflege.

- Zentralisierung der Autorisierungsinfrastruktur: Ein wesentlicher Aspekt bei der Gestaltung der Autorisierungsarchitektur ist die Fragestellung, in welchem Umfang und für welche Applikationen zentrale Autorisierungskomponenten als Infrastruktur zur Verfügung gestellt werden können. Die universelle Nutzung zentraler Infrastrukturkomponenten empfiehlt sich insbesondere aus der Perspektive der Wiederverwendung.

- Autorisierung in mehrschichtigen Systemen: Ein weiterer wesentlicher Diskussionspunkt ist die Frage, wie in mehrschichtigen Softwaresystemen mit der Autorisierung zu verfahren ist. Um die redundante Implementierung von Autorisierungsmechanismen zu vermeiden, bietet sich die gezielte Auswahl einer bestimmten Softwareebene an, die die Aufgaben der Autorisierung wahrnimmt.

Für diese drei zentralen Fragestellungen werden im Folgenden unterschiedliche Lösungsansätze auf Vor- und Nachteile untersucht. Um den heterogenen Anforderungen, Teilbereichen und Systemlandschaften einer Unternehmung Rechnung zu tragen, können im Rahmen der Methodenanwendung durchaus unterschiedliche Lösungsansätze innerhalb eines Unternehmens verwendet werden.

Fragestellung 1: Integration der Autorisierung

Ein zentraler Aspekt der unternehmensweiten Autorisierung ist die Fragestellung, auf welche Weise die Berechtigungen systemübergreifend gepflegt werden. Bei Eintritt, Austritt oder Stellenwechsel innerhalb der Unternehmung sind die entsprechenden Berechtigungen eines Mitarbeiters in der Applikationslandschaft der Unternehmung anzupassen. Hierzu werden in

[530] Vgl. NIST 2002, S. 26.

der Praxis entsprechende Anträge manuell oder mittels Workflowmanagementsystem erzeugt und bewilligt.[531]

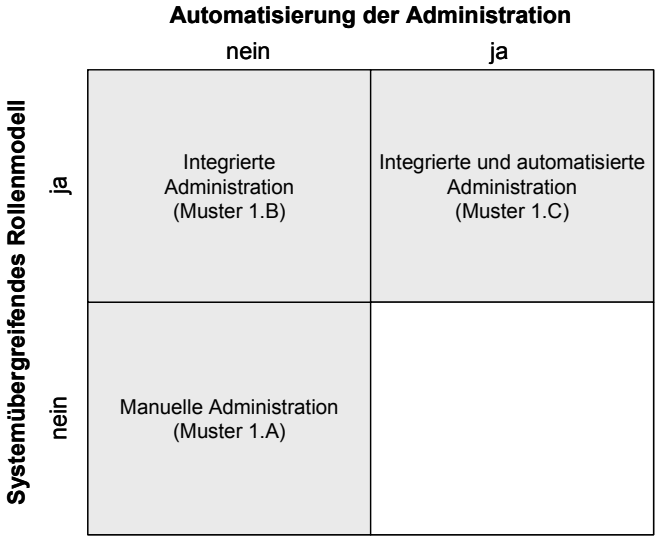

Abbildung 48: „Integration der Autorisierung": Positionierung der Muster

Drei Szenarien bzw. Muster zur Administration der Berechtigungen können unterschieden werden (vgl. Abbildung 48). Das Szenario „manuelle Administration" verzichtet auf eine automatisierte Verwaltung der Berechtigungen. Das Szenario „integrierte Administration" verzichtet ebenfalls auf eine Automatisierung, basiert jedoch auf einem Rollenmodell, das systemübergreifende Rollen[532] sowie deren Beziehungen beschreibt bzw. umfasst. Im Szenario „integrierte und automatisierte Administration" dient das übergreifende Rollenmodell als Ausgangspunkt für eine umfängliche Automatisierung der Administrationsprozesse.

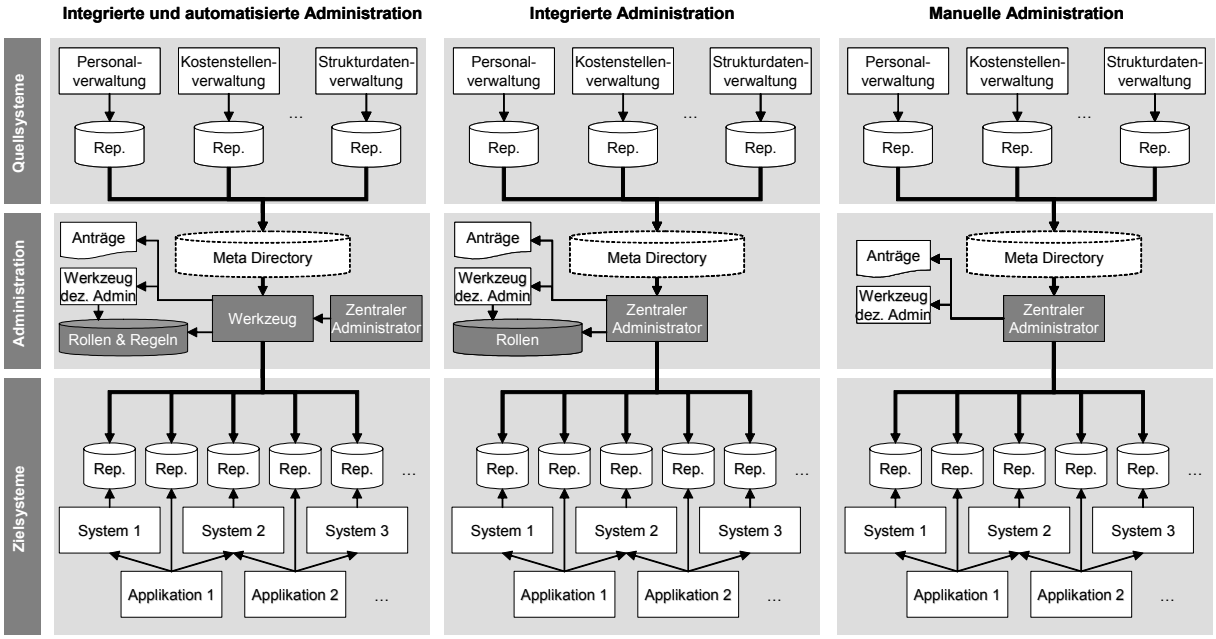

Abbildung 49: Muster „Integration der Autorisierung"

531 Vgl. Kern et al. 2002, S. 46f.
532 Vgl. Kapitel 2.3.3.

In allen drei Szenarien (vgl. Abbildung 49) wird zur Vergabe der Berechtigungen auf Daten zurückgegriffen die z.B. in Personal-, Kostenstellen- oder Strukturdatenverwaltungssystemen bereits erfasst sind. Teilweise liegen diese Daten in einem Meta Directory in integrierter Form vor.[533] Ein Beispiel soll die Bedeutung dieser Daten bei der Vergabe von Berechtigungen verdeutlichen: Wenn ein Mitarbeiter im Personalsystem mit seiner Stelle und seiner Organisationszugehörigkeit gepflegt ist, so reichen diese Informationen unter Umständen aus, um daraus alle Berechtigungen abzuleiten, die der Mitarbeiter in den Applikationen und Systemen der Unternehmung benötigt. Die drei Szenarien werden im Folgenden hinsichtlich ihrer Vor- und Nachteile untersucht.

Muster 1.A: Manuelle Administration

Bei der Lösung „Manuelle Administration" erfolgt die Vergabe der Berechtigungen manuell durch einen zentralen Administrator, ggf. in Kooperation mit weiteren, dezentralen Administratoren. Das Muster eignet sich insbesondere für Applikationslandschaften, die über wenige Applikationen verfügen. Die Administration von Berechtigungen ist unter solchen Voraussetzungen auch manuell mit geringem Aufwand realisierbar. Darüber hinaus ist die manuelle Pflege von Berechtigungen dann sinnvoll, wenn ein Unternehmen in kurzfristigen Zyklen umfassend reorganisiert wird: Die automatisierte Pflege von Berechtigungen basiert auf einem übergreifenden Rollenmodell, das sich aus der Aufbau- und Ablauforganisation der Unternehmung ableitet.[534] Änderungen in der Organisation müssen somit im Rollenmodell nachvollzogen werden.

Manuelle Administration
Anwendungsbereiche
• Applikationslandschaft verfügt über wenige Applikationen • Unternehmen wird in regelmässigen, kurzfristigen Zyklen umfassend reorganisiert
Vorteile
• Keine aufwendige Spezifikation systemübergreifender Rollen • Keine aufwendige Implementierung systemübergreifender Rollen
Nachteile
• Geringer Automatisierungsgrad der Administration • Geringe Transparenz der vergebenen Berechtigungen über die Applikationen hinweg • Aufwendige Überprüfung der vergebenen Berechtigungen auf Korrektheit und Angemessenheit

Tabelle 32: Charakteristika „Manuelle Administration"

Die Nachteile der Lösung liegen zum einen im geringen Automatisierungsgrad. Alle Berechtigungen eines Benutzers müssen manuell durch einen Administrator vergeben werden. Da ein Anwender in der Regel auf eine Vielzahl von Applikationen und Systemen Zugriff hat,

533 Vgl. Kremer 2004, S. 178.
534 Vgl. Kern et al. 2002, S. 48.

sind so etwa beim Eintritt eines neuen Mitarbeiters zahlreiche manuelle Eingriffe notwendig. Zum anderen ist ohne ein übergreifendes Rollenmodell die Information, in welchen Systemen und Applikationen ein Benutzer über welche Berechtigungen verfügt, nicht unmittelbar abrufbar. Dieser Mangel an Transparenz erschwert insbesondere auch die regelmässig notwendige Überprüfung der vergebenen Berechtigungen auf Korrektheit und Angemessenheit.[535] Tabelle 32 fasst die Anwendungsbereiche sowie die Vor- und Nachteile des Musters zusammen.

Muster 1.B: Integrierte Administration

Bei der Lösung „Integrierte Administration“ erfolgt die Vergabe von Berechtigungen auf der Basis eines übergreifenden Rollenmodells, welches auf systemübergreifenden Rollen fusst. Das übergreifende Rollenmodell bildet bei der eigentlichen Berechtigungsvergabe die Grundlage für die manuelle Administration: Ein Administrator nimmt die notwendigen Anpassungen manuell anhand des spezifizierten Rollenmodells vor.

Der Einsatz eines übergreifenden Rollenmodells empfiehlt sich, wie bereits bei der Diskussion des Musters „Manuelle Administration“ begründet, nur bei relativ stabiler Aufbau- und Ablauforganisation. Die Entwicklung eines übergreifenden Modells, das nicht zur automatisierten Vergabe von Berechtigungen verwendet wird, bietet sich insbesondere dann an, wenn die Automatisierung einen unter Wirtschaftlichkeitsaspekten nicht gerechtfertigten Aufwand verursacht. Dies kann zum einen dann der Fall sein, wenn zahlreiche heterogene Applikationen und Systeme innerhalb eines Unternehmens verwendet werden. Zum anderen kann die technische Anbindung von übergreifenden Administrationswerkzeugen zur Automatisierung den wirtschaftlichen Einsatz einer solchen Lösung verhindern. Diese ist teilweise nur durch erhebliche Eigenentwicklung zu realisieren.

Integrierte Administration
Anwendungsbereiche
• Anbindung eines übergreifenden Administrationswerkzeugs zur Automatisierung an die existierenden Applikationen und Systeme wirtschaftlich nicht sinnvoll • Heterogene Applikationslandschaft • Unternehmen wird nicht in kurzfristigen Zyklen umfassend reorganisiert
Vorteile
• Systemübergreifende Transparenz der vergebenen Berechtigungen • Systemübergreifende Konsistenz der vergebenen Berechtigungen • Keine Implementierung des Rollenmodells notwendig
Nachteile
• Geringer Automatisierungsgrad der Administration • Spezifikation eines übergreifenden Rollenmodells notwendig

Tabelle 33: Charakteristika „Integrierte Administration“

[535] Vgl. hierzu auch ISO 2000a, Kapitel 9.

Die Vorteile des Musters liegen in der geschaffenen Transparenz. Das in einem zentralen Repository vorgehaltene Rollenmodell zeigt den Zusammenhang von Berechtigungen über einzelne Applikationen und Systeme hinweg auf. Diese Transparenz fördert die konsistente Vergabe von Berechtigungen. Nachteilig ist der geringe Automatisierungsgrad der Lösung. Darüber hinaus ist die Spezifikation eines übergreifenden Rollenmodells aufwendig: Da ein systemübergreifendes Rollenmodell eine Vielzahl von Applikationen und Systeme umfasst, geht mit der Spezifikation des Modells eine erhebliche Komplexität einher. Tabelle 33 fasst die Anwendungsbereiche sowie die Vor- und Nachteile des Musters zusammen.

Muster 1.C: Integrierte und automatisierte Administration

Bei der Lösung „Integrierte und automatisierte Administration“ erfolgt die Administration der Berechtigungen weitestgehend vollautomatisch durch ein Werkzeug. Sind die Rollen eines Mitarbeiters bei seinem Eintritt in das Unternehmen bekannt, können entsprechende Berechtigungen auf der Basis des übergreifenden Rollenmodells automatisch in den Systemen vergeben werden. Bekommt ein Mitarbeiter nachträglich eine Rolle zugewiesen oder wird eine Rolle entzogen, können auch diese Änderungen automatisch umgesetzt werden.

Bei vollautomatisierten Administrationslösungen werden neben Rollen auch Regeln verwendet.[536] Diese bilden die Basis der Automatisierung. Im folgenden Beispiel wird die Vergabe einer Rolle („TELLER“) auf der Basis eines Benutzerattributs („USER_JOB_FCT“), das z.B. in einem Personalverwaltungssystem gepflegt wird, realisiert:

```
If USER_JOB_FCT is TELLER then
  assign USER to Role TELLER
```

Abbildung 50: Regel zur Automatisierung der Administration (Beispiel)[537]

Die Umsetzung der Lösungsvariante empfiehlt sich nur bei relativ stabiler Aufbau- und Ablauforganisation einer Unternehmung.[538] Darüber hinaus sollte das Werkzeug entsprechende Adapter für die Zusammenarbeit mit den im Unternehmen vorhandenen Applikationen und Systemen bereitstellen, um aufwändige Eigenentwicklungen zu vermeiden. Muss die Vergabe von Berechtigungen in den einzelnen Applikationen und Systemen benutzerindividuell erfolgen, ist eine Automatisierung nur eingeschränkt empfehlenswert: Eine Vielzahl von zu spezifizierenden Rollen und Regeln erzeugt eine Komplexität, die den Implementierungsaufwand einer Automatisierung stark ansteigen lässt.

536 Vgl. Kern 2002, S. 3.
537 In Anlehnung an Kuhlmann 2005, S. 42.
538 Vgl. Kern et al. 2002, S. 48.

Integrierte und automatisierte Administration
Anwendungsbereiche
• Kein Umfeld, das eine benutzerindividuelle Vergabe von Berechtigungen verlangt • Anbindung eines übergreifenden Administrationswerkzeugs zur Automatisierung an die existierenden Applikationen und Systeme möglich und wirtschaftlich sinnvoll • Unternehmen wird nicht in kurzfristigen Zyklen umfassend reorganisiert
Vorteile
• Hoher Automatisierungsgrad der Administration • Systemübergreifende Transparenz der vergebenen Berechtigungen • Systemübergreifende Konsistenz der vergebenen Berechtigungen
Nachteile
• Spezifikation eines übergreifenden Rollenmodells notwendig • Softwaretechnische Umsetzung des Rollenmodells notwendig

Tabelle 34: Charakteristika „Integrierte und automatisierte Administration“

Der Vorteil der Lösung liegt einerseits in der Transparenz und der daraus folgenden Konsistenz der vergebenen Berechtigungen. Diese wird durch den Einsatz eines übergreifenden Rollenmodells erzielt. Andererseits wirkt sich der hohe Automatisierungsgrad positiv auf die laufenden Betriebskosten der Lösung aus. Ein Nachteil dieser Lösungsvariante liegt zum einen in der aufwendigen Spezifikation des übergreifenden Rollenmodells. Darüber hinaus ist mit der Spezifikation der Regeln weitere konzeptionelle Arbeit zu leisten. Schlussendlich müssen Rollen und Regeln in einer Softwarelösung implementiert werden. Tabelle 34 fasst die Anwendungsbereiche sowie die Vor- und Nachteile des Musters zusammen.

Fragestellung 2: Zentralisierung der Autorisierungsinfrastruktur

Aufbauend auf dem Standard ISO/IEC 10181-3 kann der Ablauf der Autorisierung zur Laufzeit in fünf wesentliche Schritte unterteilt werden (vgl. Abbildung 51):[539] In einem ersten Schritt versucht der Benutzer über eine Applikation auf eine geschützte Ressource zuzugreifen (1). Innerhalb der Applikation wird die Anfrage an eine Zugriffskontrollfunktion (Access Enforcement Function, AEF) weitergeleitet (2). Die Zugriffskontrollfunktion leitet die Anfrage an die Zugriffsentscheidungsfunktion (Access Decision Function, ADF) weiter (3). Dabei werden Daten wie der aufrufende Benutzer, die zu startende Transaktion und ggf. weitere Attribute, die das Verhalten der Transaktion steuern, übergeben. Die Zugriffsentscheidungsfunktion gleicht daraufhin die im Repository hinterlegten Berechtigungen mit den übergebenen Daten ab (4). Je nach Ergebnis des Abgleichs lässt die AEF den Zugriff zu oder untersagt ihn (5).

[539] Vgl. Kern et al. 2004a, S. 2ff.

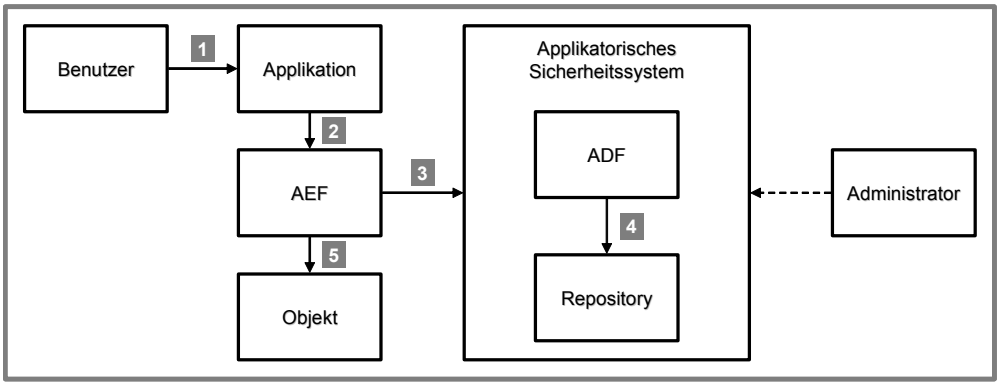

Abbildung 51: Ablauf der Autorisierung nach ISO/IEC 10181-3 [540]

Um Berechtigungen innerhalb einer Applikation zu prüfen, bedarf es einer Softwarekomponente, die die Prüfung zur Laufzeit der Applikation wahrnimmt. Die Softwarekomponente besteht, wie diskutiert, aus den Teilkomponenten AEF, ADF und dem Repository. ADF und Repository bilden das Sicherheitssystem, das neben diesen beiden Laufzeitkomponenten auch über eine Administrationsschnittstelle verfügt. Die Teilkomponenten können auf verschiedene Art und Weise zusammenarbeiten. Im Folgenden werden drei Ansätze diskutiert, wie die Verteilung und Zusammenarbeit der Teilkomponenten realisiert werden kann. Die Ansätze unterscheiden sich hinsichtlich Reichweite und Ausmass der Wiederverwendung einzelner Teilkomponenten.

Muster 2.A: Applikationsspezifische Autorisierungsinfrastruktur

Im Rahmen der Lösung „applikationsspezifische Autorisierungsinfrastruktur“ werden alle Komponenten, die zur Berechtigungsprüfung notwendig sind, applikationsspezifisch implementiert (vgl. Abbildung 52). Existierende Plattformen, die eine einheitliche Infrastruktur für Applikationen bieten,[541] stellen somit keine zentrale, plattformspezifische Autorisierungslösung zur Verfügung.

Insbesondere bei Applikationslandschaften, die durch Standardsoftware geprägt sind, ist es kaum möglich und ökonomisch sinnvoll, eine gemeinsame, zentrale Autorisierungsinfrastruktur zu realisieren: Bei einer Modifikation der Basisfunktionalität einer Standardlösung, wie sie ein Austausch der Autorisierungskomponente darstellt, ist unter Umständen auch die Updatefähigkeit des betroffenen Systems nicht mehr gegeben. Ebenfalls nicht empfehlenswert ist die unmittelbare Implementierung einer zentralen Autorisierungsinfrastruktur bei Eigenentwicklungen, denen sehr unterschiedliche Autorisierungsschemata zugrunde liegen. Eine Portierung der Applikationen auf eine zentrale Autorisierungslösung ist in diesem Fall kurzfristig nur mit hohem Aufwand zu realisieren, da nicht nur einzelne Teile der Applikation modifiziert werden müssen, sondern jede Zugriffsüberprüfung im Quellcode zu ändern ist.

---

[540] Vgl. Kern et al. 2004a, S. 2.
[541] Vgl. z.B. Klesse/Wortmann 2004, S. 17f.

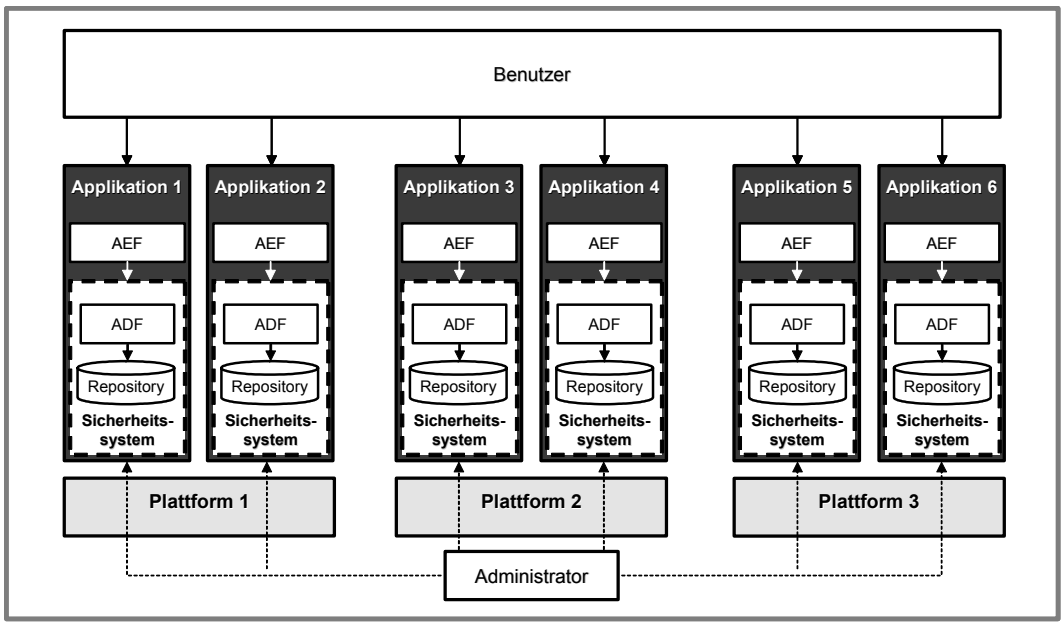

Abbildung 52: Applikationsspezifische Autorisierungsinfrastruktur

Auf der anderen Seite steigt durch die Redundanz der Autorisierungskomponenten die Komplexität der Systemlandschaft. Darüber hinaus können grundlegende Daten wie z.B. die Aufbauorganisation einer Unternehmung, die für die Autorisierung in unterschiedlichsten Applikationen notwendig sind, nicht zentral vorgehalten werden. Die Aktualisierung und Pflege dieser Daten ist somit entsprechend aufwendig. Ebenfalls schwierig gestaltet sich die Durchsetzung einheitlicher Prozesse z.B. für die Spezifikation neuer Berechtigungen. Tabelle 35 fasst die Anwendungsbereiche sowie die Vor- und Nachteile des Musters zusammen.

Applikationsspezifische Autorisierungsinfrastruktur
Anwendungsbereiche
• Applikationslandschaft wird durch Standardsoftware dominiert • Eigenentwicklungen basieren auf sehr unterschiedlichen Autorisierungsschemata
Vorteile
• Keine Abstimmung zwischen den Applikationen notwendig • Autorisierungskomponenten können genau auf die Bedürfnisse der Applikation zugeschnitten werden
Nachteile
• Redundante Infrastrukturfunktionalität • Hohe Gesamtkomplexität durch eine Vielzahl heterogener Komponenten • Entwicklung einheitlicher Prozesse schwierig • Redundante Speicherung und Verwaltung grundlegender Autorisierungsdaten

Tabelle 35: Charakteristika „Applikationsspezifische Autorisierungsinfrastruktur“

Muster 2.B: Plattformspezifische Autorisierungsinfrastruktur

Das Muster „Plattformspezifische Autorisierungsinfrastruktur“ sieht die zentrale Implementierung von Komponenten zur Berechtigungsprüfung vor. Pro Plattform wird dabei eine Auto-

risierungskomponente zur Verfügung gestellt, die die Berechtigungsprüfungen für die Applikationen der entsprechenden Plattform vornimmt (vgl. Abbildung 53).

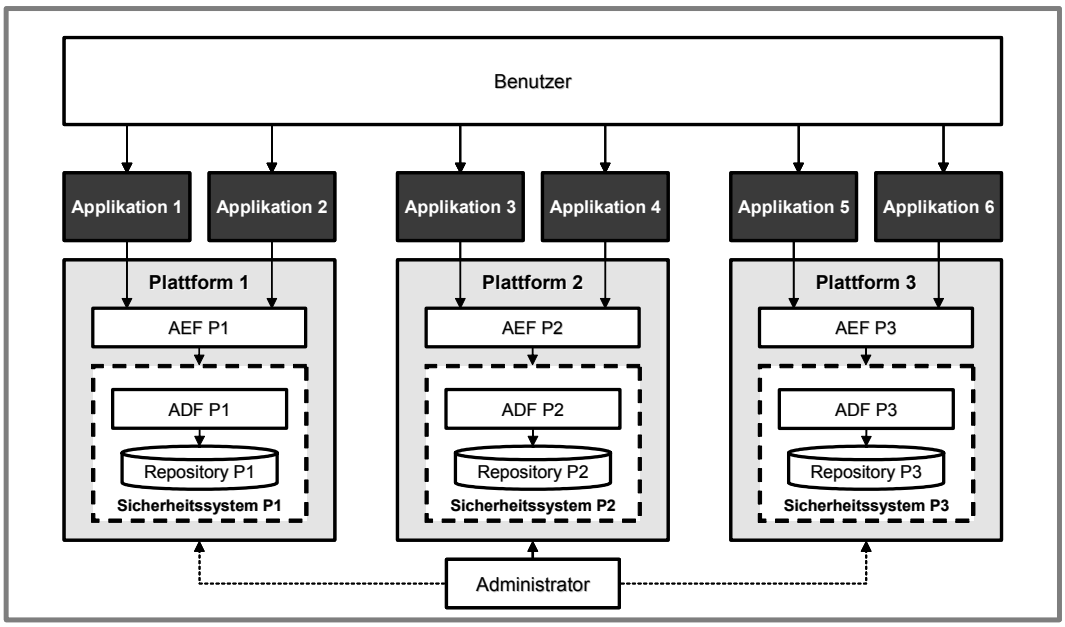

Abbildung 53: Plattformspezifische Autorisierungsinfrastruktur

Die Verwendung einer zentralen Autorisierungskomponente pro Plattform bietet sich dann an, wenn die Applikationen einer Plattform auf ähnlichen Autorisierungsschemata aufbauen. Dies ist im Regelfall gegeben, da das Konzept der Plattform vorsieht, dass die Applikationen einer Plattform auf der gleichen Infrastruktur aufbauen, die von einer IT-Einheit verantwortet wird.[542] Sollten die Autorisierungsschemata der Applikation verschiedener Plattformen ebenfalls weitestgehend übereinstimmen, so bietet sich eine plattformübergreifende Infrastrukturlösung an, die dem Muster „Zentrale Autorisierungsinfrastruktur" entspricht.

Plattformspezifische Autorisierungsinfrastruktur
Anwendungsbereiche
• Applikationslandschaft basiert auf unterschiedlichen Plattformen • Autorisierungsschemata der Applikationen einer Plattform sind ähnlich • Autorisierungsschemata der Applikationen verschiedener Plattformen unterscheiden sich
Vorteile
• Zentralisierte, wiederverwendbare Autorisierungsfunktionalität • Unterstützung verschiedener, plattformspezifischer Autorisierungsschemata
Nachteile
• Redundante Infrastrukturfunktionalität • Komplexität durch heterogene Komponenten • Entwicklung einheitlicher, plattformübergreifender Prozesse schwierig • Redundante Speicherung und Verwaltung grundlegender Autorisierungsdaten

Tabelle 36: Charakteristika „Plattformspezifische Autorisierungsinfrastruktur"

542 Die Aussage beruht auf den Fallstudien Credit Suisse und Winterthur, vgl. Kapitel 4.1 und 4.2.

Wie bei der Lösung „Applikationsspezifische Autorisierungsinfrastruktur“ resultieren aus dem redundanten Betrieb von Autorisierungskomponenten Nachteile: Durch die plattformspezifischen Lösungen sind die Umsetzung einheitlicher Prozesse und die integrierte Nutzung von Autorisierungsdaten erschwert. Tabelle 36 fasst die Anwendungsbereiche sowie die Vor- und Nachteile des Musters zusammen.

Muster 2.C: Zentrale Autorisierungsinfrastruktur

Bei der Lösung „Zentrale Autorisierungsinfrastruktur“ führt eine zentrale Komponente die Berechtigungsprüfung für die Applikationen aller Plattformen durch (vgl. Abbildung 54). Ein zentrales Sicherheitssystem enthält die ADF und das Berechtigungsrepository sowie die Benutzerschnittstelle zur Administration der Applikationen. Jede Plattform enthält eine plattformspezifische AEF, die die Applikationen der Plattform zur Überprüfung von Berechtigungen in ihren Quellcode einbinden. Aufgabe einer plattformspezifischen AEF ist die Aufbereitung und Übergabe der berechtigungsrelevanten Daten an die zentrale AEF. Auf Grundlage dieser Lösung ist es möglich, unterschiedlichste Plattformen wie z.B. Host-Umgebungen und moderne Java-Lösungen auf die Basis einer zentralen Autorisierungslösung zu stellen.

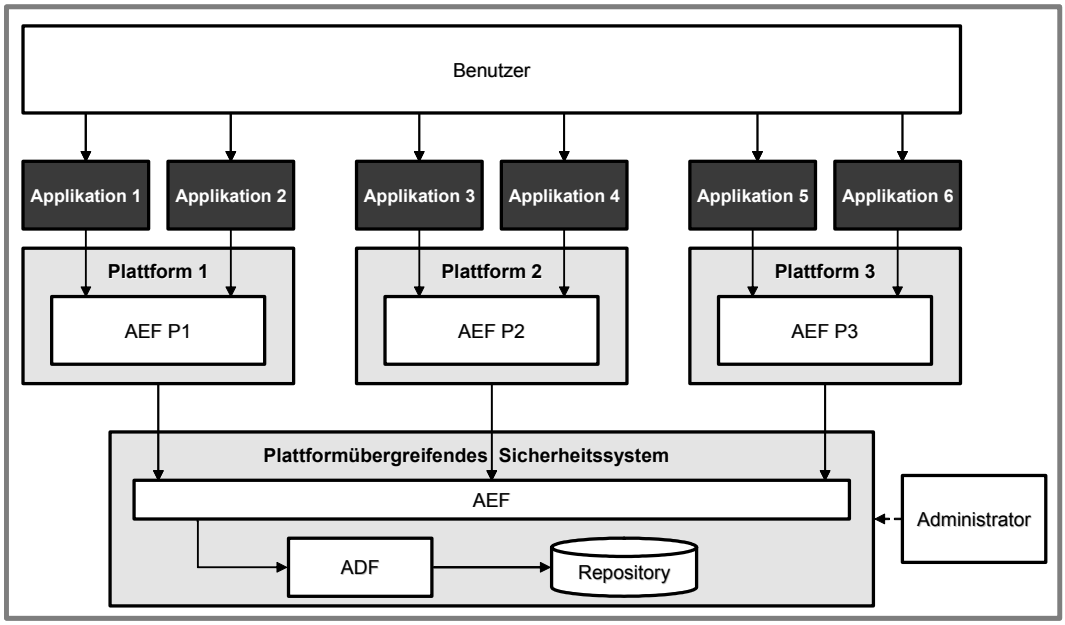

Abbildung 54: Zentrale Autorisierungsinfrastruktur

Die kurzfristige Einführung einer zentralen Autorisierungskomponente empfiehlt sich vor allem dann, wenn den betroffenen Applikationen ähnliche Autorisierungsschemata zugrunde liegen. Eine Portierung aller Applikationen auf eine zentrale Autorisierungslösung ist bei heterogenen Schemata ad hoc nur mit hohem Aufwand zu realisieren.[543] Dieser Aufwand ist auf der Basis von Wirtschaftlichkeitsüberlegungen nur eingeschränkt zu rechtfertigen, da den hohen Portierungskosten in der Regel lediglich eine eingeschränkte Verbesserung der Sicherheit

[543] Die folgenden Aussagen beruhen auf Analysen, die im Rahmen der beschriebenen Projektarbeit bei der Winterthur durchgeführt wurden, vgl. Kapitel 4.2.

entgegensteht. Einsparungen aufgrund zentralisierter Prozesse wirken sich zudem eher langfristig aus.

Zentrale Autorisierungsinfrastruktur
Anwendungsbereiche
• Autorisierungsschemata der existierenden Applikation sind ähnlich
Vorteile
• Keine redundante Autorisierungsfunktionalität • Entwicklung einheitlicher Prozesse möglich • Integrierte Nutzung von Autorisierungsdaten möglich
Nachteile
• Unterstützung eines einzigen Autorisierungsschemas • Anforderungen einer einzelnen Applikation können nur eingeschränkt berücksichtigt werden • Änderung und Ausfall der zentralen Autorisierungskomponente betrifft eine Vielzahl von Applikationen

Tabelle 37: Charakteristika „Zentrale Autorisierungsinfrastruktur“

Die Nachteile dieser zentralen Lösung liegen zum einem in der Bereitstellung einer einzigen Autorisierungslösung, so dass die besonderen Anforderungen einzelner Applikationen nur eingeschränkt berücksichtigt werden können. Zum anderen wirken sich Änderungen und Ausfälle der zentralen Autorisierungskomponente auf die ganze Applikationslandschaft aus. Tabelle 37 fasst die Anwendungsbereiche sowie die Vor- und Nachteile des Musters zusammen.

Fragestellung 3: Autorisierung in mehrschichtigen Systemen

Grosse betriebliche Informationssysteme werden heutzutage meist in Form von mehrschichtigen Client/Server-Systemen realisiert.[544] Dabei werden Datenhaltung, Geschäftslogik und Präsentation sowohl konzeptionell als auch technisch voneinander getrennt. Die Aufbereitung der Präsentation, die Ausführung der Geschäftslogik und die Datenhaltung werden auf spezialisierten Servern durchgeführt, während der Client für die eigentliche Präsentation der Daten zuständig ist.

Mit der Einführung mehrschichtiger Systeme ging die zunehmende Verteilung der Geschäftslogik einher: Aktuell werden beispielsweise unter dem Stichwort „Service-orientierte Architektur“ Gestaltungsgrundsätze diskutiert, die insbesondere eine Partitionierung der Geschäftslogik in unabhängige Module bzw. Services vorsieht.[545] Einzelne Module sollen dabei flexibel eingefügt, neu kombiniert oder entfernt werden können, um die sich ändernden Geschäftspro-

[544] Vgl. im Folgenden Schätzle et al. 2002, S. 217f.
[545] Vgl. Endrei et al. 2004, S. 20f.

zesse zu unterstützen.[546] Bei einer Verteilung der Geschäftslogik stellt sich aus Sicht der Autorisierung die Frage, welche Komponenten die Aufgaben der Autorisierung wahrnehmen.

Bei mittleren und grossen Unternehmen, die im Fokus der Arbeit stehen,[547] stellt sich die Frage der Autorisierungsverantwortung insbesondere im Hinblick auf die etablierten Backend-Applikationen. Einerseits kann die Überprüfung der Berechtigungen in den neu entwickelten, Backend-übergreifenden Applikationen stattfinden, andererseits kann die Überprüfung auch im Backend selbst realisiert werden. Darüber hinaus wäre auch eine Prüfung der Rechte in beiden Schichten möglich. Im Folgenden werden diese drei Lösungsvarianten im Hinblick auf ihre Vor- und Nachteile untersucht.

Muster 3.A: Autorisierung in der Applikation

Das Muster „Autorisierung in der Applikation“ sieht die Überprüfung der Berechtigungen in den Backend-übergreifenden Applikationen vor, ohne dabei jedoch gänzlich auf eine Prüfung im Backend zu verzichten. Der Ablauf der Autorisierung erfolgt in vier Schritten (vgl. Abbildung 55): Im ersten Schritt identifiziert und authentisiert sich der Benutzer bei der Applikation z.B. durch die Eingabe seines Benutzernamens und -passwortes (1). Das Sicherheitssystem der Applikation prüft bei Aufruf einer Transaktion, ob der Benutzer die notwendigen Berechtigungen zum Aufruf der Transaktion und zum Lesen bzw. Schreiben der angeforderten Daten hat (2). Muss innerhalb dieser Transaktion auf eine Backend-Applikation zugegriffen werden, so leitet die Applikation den Zugriff entsprechend weiter (3). Dabei ist die Identität des Benutzers nur dann an das Backend weiterzugeben, wenn dort die Information nachgehalten werden muss, welcher Benutzer welche Transaktion im Backend durchführt. Ist eine Aufzeichnung dieser Informationen im Backend nicht erforderlich, so wird in der Praxis häufig ein „technischer Nutzer“ zur Identifikation und Autorisierung im Backend verwendet.[548] Dieser Nutzer ist nicht personengebunden und trägt in der Regel den Namen der aufrufenden Applikation. Im Backend findet im Folgenden nur eine rudimentäre, sehr grobgranulare Zugriffskontrolle statt (4). Diese Kontrolle verhindert lediglich den unkontrollierten Zugang zum Backend durch nicht autorisierte Applikationen.

Sind zum Schutz der Backend-Daten komplexe Zugriffskontrollen zu realisieren und erfolgt die Kontrolle der Berechtigungen nicht im Backend, so muss jede zugreifende Applikation den aufwendig zu realisierenden Schutz der Backend-Daten eigenständig realisieren. Daher empfiehlt sich eine Anwendung dieser Lösung insbesondere dann, wenn zum Schutz der Backend-Daten keine komplexen Zugriffskontrollen notwendig sind.

Der Vorteil der Lösungsvariante „Autorisierung in der Applikation“ liegt darin, dass eine detaillierte Zugriffskontrolle lediglich auf einer Ebene stattfindet. Darüber hinaus sind die Be-

546 Vgl. Dangelmaier et al. 2002, S. 61.
547 Vgl. Kapitel 1.2.
548 Die folgenden Aussagen beruhen auf den erhobenen Fallstudien, vgl. Kapitel 4.

rechtigungen auf der Ebene der Backend-übergreifenden Applikationen in der Regel besser nachvollziehbar, da sie sich unmittelbar aus dem Anwendungskontext der Applikation ergeben. Berechtigungen im Backend lassen sich hingegen nicht direkt auf den ursächlichen Anwendungskontext zurückführen, so dass ihre Angemessenheit nur eingeschränkt beurteilt werden kann.

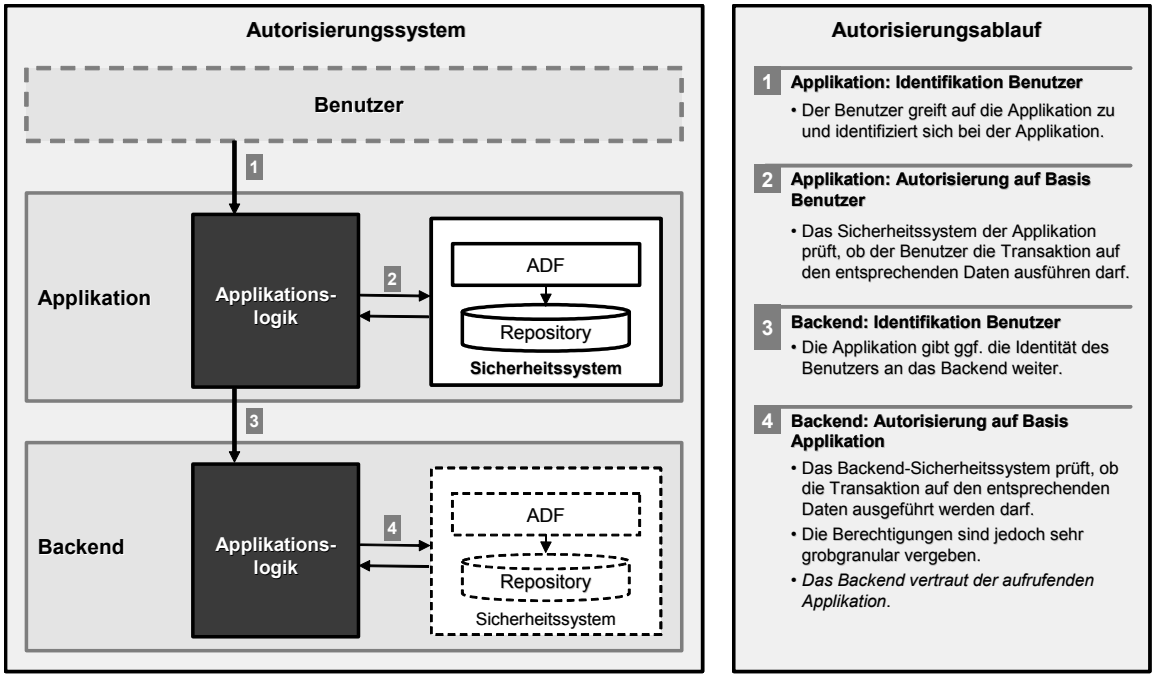

Abbildung 55: Autorisierung in der Applikation

Nachteil dieser Lösung ist, dass jede Backend-übergreifende Applikation für den angemessenen Schutz der Backend-Daten Sorge tragen muss. Zu bedenken ist zudem, dass gerade im Umfeld der Backend-Applikationen langjähriges Erfahrungswissen über die zu schützenden Daten aufgebaut wurde, das für eine effektive Sicherung der Daten unabdingbar ist. Tabelle 38 fasst die Anwendungsbereiche sowie die Vor- und Nachteile des Musters zusammen.

Autorisierung in der Applikation
Anwendungsbereiche
• Komplexe Zugriffskontrollen zum Schutz der Backend-Daten nicht notwendig
Vorteile
• Detaillierte Zugriffskontrolle lediglich auf einer Ebene • Gute Nachvollziehbarkeit der vergebenen Berechtigungen
Nachteile
• Jede Applikation muss für den angemessenen Schutz der Backend-Daten sorgen • Backend verfügt über detailliertes Wissen hinsichtlich der zu schützenden Daten

Tabelle 38: Charakteristika „Autorisierung in der Applikation“

Muster 3.B: Autorisierung im Backend

Der Lösungsansatz „Autorisierung im Backend“ sieht die Überprüfung der Berechtigungen in den Backend-Applikationen vor (vgl. Abbildung 56). Der Ablauf der Autorisierung gestaltet sich in diesem Szenario wie folgt: Der Benutzer identifiziert sich bei der Backend-übergreifenden Applikation (1). Die Applikation überlässt die eigentliche Prüfung der Zugriffsberechtigungen den Backend-Applikationen. Insbesondere bei der Kombination von Informationen, die durch Zugriffe auf unterschiedliche Backend-Applikationen gewonnen werden, kann jedoch eine zusätzliche Kontrolle von Berechtigungen durch die Applikation notwendig sein (2). Die Identität des Benutzers ist daher an die Backend-Applikation zu übergeben (3), damit dort geprüft werden kann, ob der Benutzer eine Transaktion auf den angeforderten Daten ausführen darf (4).

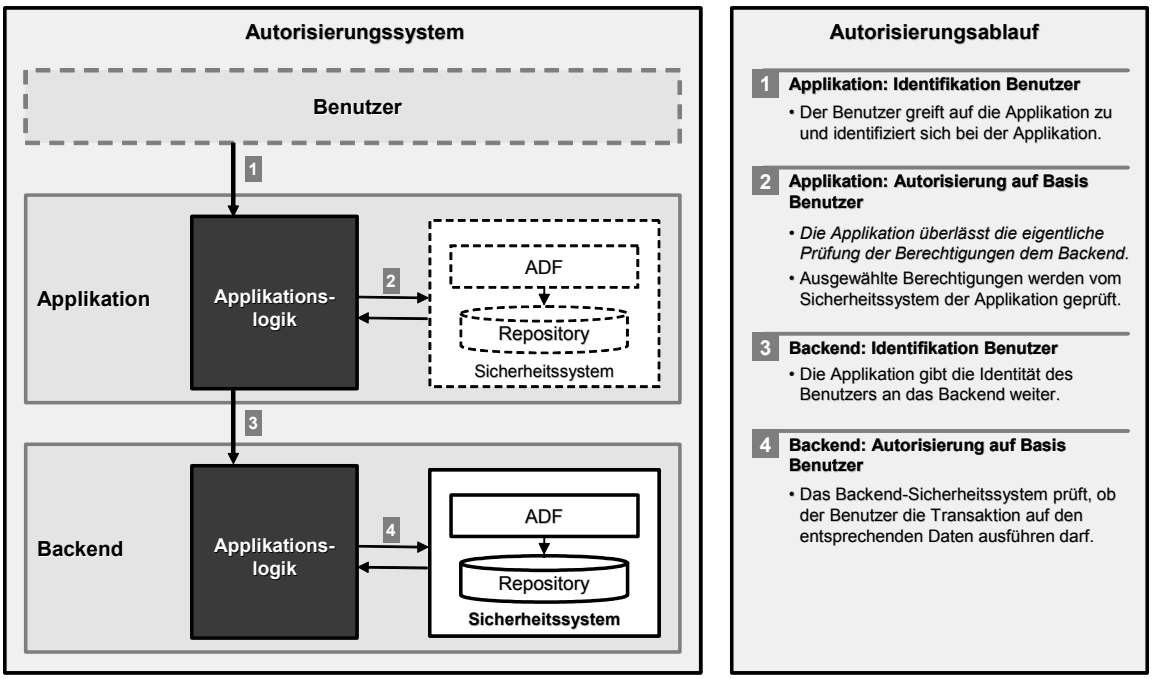

Abbildung 56: Autorisierung im Backend

Eine Anwendung dieses Musters empfiehlt sich insbesondere dann, wenn eine Backend-Applikation von zahlreichen Backend-übergreifenden Applikationen verwendet wird. In dieser Situation muss nicht jede Backend-übergreifende Applikation den Schutz der Backend-Daten realisieren. Eine Wiederverwendung von Autorisierungslogik bietet sich an. Einen weiteren Vorteil dieser Lösung stellt das vorhandene Erfahrungswissen im Backend-Bereich dar, das eine Voraussetzung für die angemessene Gewährleistung von Sicherheit ist.

Ein Nachteil der Lösung ist die bereits diskutierte, eingeschränkte Nachvollziehbarkeit der vergebenen Berechtigungen im Backend. Ebenfalls zu bedenken ist, dass Backend-übergreifende Applikationen in der Regel auf jeden Fall Berechtigungen prüfen müssen. Allein für den Aufbau der Benutzerschnittstelle, der u.a. die Ausblendung und Deaktivierung von Steuerelementen und Transaktionen umfasst, ist eine Prüfung von Berechtigungen not-

wendig. Tabelle 39 fasst die Anwendungsbereiche sowie die Vor- und Nachteile des Musters zusammen.

Autorisierung im Backend
Anwendungsbereiche
• Backend-Applikationen werden von zahlreichen Backend-übergreifenden Applikationen verwendet
Vorteile
• Backend verfügt über detailliertes Wissen über die zu schützenden Daten • Wiederverwendung der Autorisierungslogik
Nachteile
• Eingeschränkte Nachvollziehbarkeit der vergebenen Berechtigungen im Backend • Backend-übergreifende Applikationen müssen in der Regel auf jeden Fall Autorisierungslogik implementieren

Tabelle 39: Charakteristika „Autorisierung im Backend“

Muster 3.C: Autorisierung auf beiden Ebenen

Das Muster „Autorisierung auf beiden Ebenen“ sieht die Überprüfung der Berechtigungen sowohl in den Backend-übergreifenden Applikationen, als auch im Backend selbst vor. Der Ablauf der Autorisierung erfolgt analog zu den bereits diskutierten Szenarien (vgl. Abbildung 57): Im ersten Schritt identifiziert sich der Benutzer bei der Applikation (1). Die Applikation prüft, ob der Anwender die Transaktion auf den entsprechenden Daten durchführen darf (2). Bei Aufruf einer Backend-Applikation erfolgt die Übergabe der Benutzeridentifikation an die Backend-Applikation (3), die ebenfalls eine detaillierte Überprüfung der Berechtigungen vornimmt.

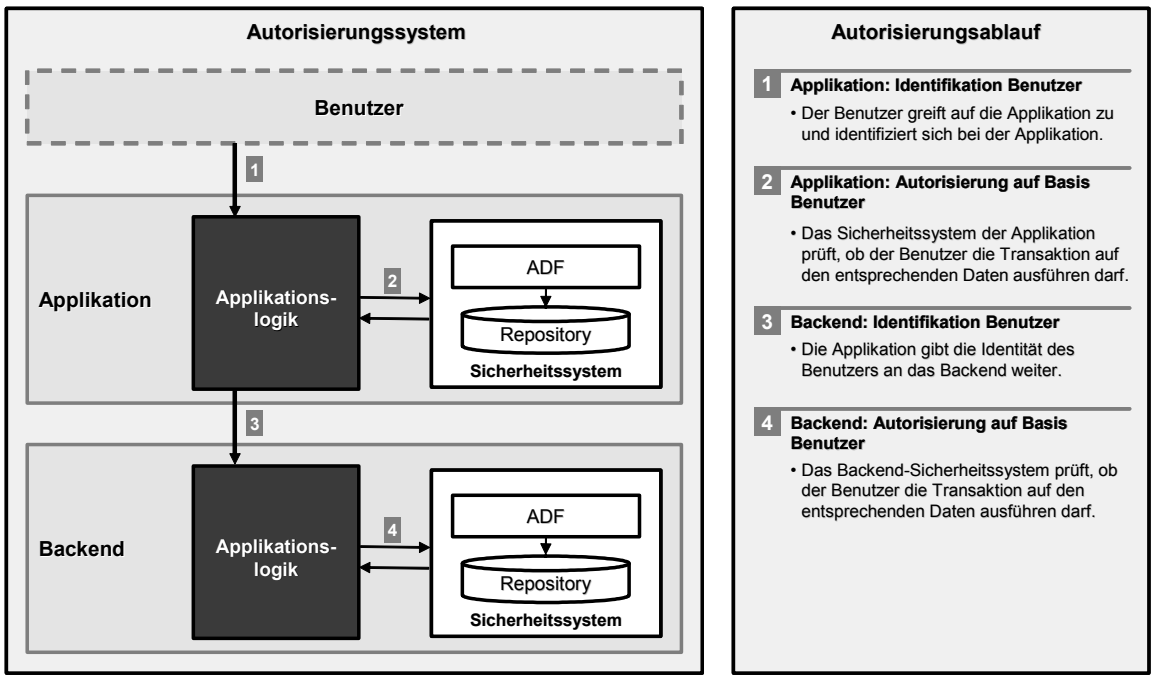

Abbildung 57: Autorisierung auf beiden Ebenen

Diese Lösung bietet sich vor allem dann an, wenn sowohl im Backend als auch in den entsprechenden Backend-übergreifenden Applikationen umfangreiche Prüfungen, z.B. aus regulativen oder vertraglichen Gründen, unabdingbar sind. Jede Komponente schützt in dieser Situation das Umfeld, für welches das jeweilige Erfahrungswissen vorliegt.

Autorisierung auf beiden Ebenen
Anwendungsbereiche
• Sowohl in der Backend-Applikation als auch in der Backend-übergreifenden Applikation sind umfangreiche Prüfungen unabdingbar
Vorteile
• Jede Komponente schützt das Umfeld, für welches das jeweilige Erfahrungswissen vorliegt
Nachteile
• Aufwendige Prüfung auf beiden Ebenen • Abstimmung der Berechtigungen beider Ebenen notwendig • Hohe Komplexität der Lösung

Tabelle 40: Charakteristika „Autorisierung auf beiden Ebenen“

Ein Nachteil dieser Lösung ist der Aufwand, der mit der Administration der Autorisierungskomponenten auf beiden Ebenen einhergeht. Darüber hinaus müssen die Berechtigungen über beide Ebenen hinweg aufeinander abgestimmt und konsistent sein. Die Lösung stellt aufgrund ihrer Komplexität hohe Anforderungen an die Administration. Tabelle 40 fasst die Anwendungsbereiche sowie die Vor- und Nachteile des Musters zusammen.

6.4.3.2 Direktiven spezifizieren

Ziel dieser Aktivität ist die Bereitstellung von Architekturdirektiven, die sowohl in einzelnen Projekten verwendet werden können als auch in weitergehenden, architekturrelevanten Vorhaben Anwendung finden können.[549] Die abschliessende Entwicklung und Abstimmung von Direktiven erfolgt in der Regel mit Vertretern der beteiligten Interessengruppen.

Die Spezifikation von Autorisierungsdirektiven schliesst sich an die Definition und Auswahl wesentlicher Gestaltungsoptionen an. Wesentliche Lösungsprinzipien, die den erarbeiteten Gestaltungsoptionen zugrunde liegen, werden hierbei schriftlich fixiert und detailliert. In der Praxis werden Direktiven synonym auch als „Standards“, „Regeln“, „Leitlinien“, „Richtlinien“ oder „Weisungen“ bezeichnet.[550] Ziel von Direktiven ist es, verbindliche Aussagen zu treffen, die die Lösung einer Problemstellung möglichst allgemeingültig festlegen. Tabelle 41 zeigt typische Metadaten einer Direktive.[551] Neben der Festlegung des Anwendungskontexts gilt es, den Verbindlichkeitsgrad der Kernaussage zu spezifizieren. Der Verbindlichkeitsgrad

549 Zur Bereitstellung von Architekturdirektiven vgl. Hafner 2005, S. 252.
550 Vgl. im Folgenden Kapitel 6.1.2.
551 Vgl. im Folgenden Hafner 2005, S. 255.

kann sowohl positiv („Verpflichtung“ oder „Empfehlung“) als auch negativ („Verbot“) sein. Die Begründung für die Entwicklung der Direktive folgt aus dem zu erwartenden Nutzen, potenziellen Kosteneffizienzen und möglichen Qualitätsverbesserungen. Abschliessend ist auf die Konsequenzen des Einsatzes der Direktive hinzuweisen.

Architekturdirektive: ST_AUT_08		
Grundlagen	Kurzbezeichnung:	ST_AUT_08
	Name:	Keine Autorisierungslogik im Programmcode
	Kernaussage:	Applikationen dürfen keine eigene Autorisierungslogik implementieren.
	Anwendungskontext:	Eigenentwicklungen
Verbindlichkeit	Verpflichtung:	Ja
	Empfehlung:	Nein
	Verbot:	Nein
Begründung	Nutzen:	Autorisierungsinfrastruktur wird applikationsübergreifend entwickelt und gewartet.
	Kosten:	Kosteneinsparung durch Wiederverwendung.
	Qualität:	Zentrale Entwicklung und Wartung von Autorisierungskomponenten sichert Qualität der Komponenten insbesondere im Hinblick auf regulatorische Anforderungen.
Konsequenzen	Auswirkungen:	-
	Einschränkungen:	Standardsoftware ist von der Direktive ausgeschlossen.
	Hinweise:	Alle Zugriffskontrollen erfolgen über zentral bereitgestellte Schnittstellen.

Tabelle 41: Architekturdirektive (Beispiel)[552]

6.4.3.3 Leitelemente definieren

Obwohl die Gestaltung der Architektur primär die Strukturierung eines Informationssystems vorsieht, stellt sie auch konkrete Komponenten zur Verfügung.[553] Ziel der Aktivität „Leitelemente definieren“ ist es, einzelne Gestaltungsoptionen durch die Spezifikation oder Entwicklung konkreter Infrastrukturkomponenten auf ihre Anwendbarkeit hin zu untersuchen.

Die Entwicklung erster Komponentenversionen entspricht dem Konzept des Prototyping.[554] Das Prototyping wird entsprechend der verfolgten Ziele in drei Klassen unterteilt:[555]

- Exploratives Prototyping: Absicht des explorativen Prototyping ist es, eine vorliegende Problemstellung zu konkretisieren. Initiale Ideen werden umgesetzt, um die Anforderungen der Anwender abzuklären. Eine besondere Bedeutung hierbei hat die Realisierung unterschiedlicher Implementierungsvarianten. Durch seine Arbeit erhält der Entwickler einen Einblick in das Themengebiet und die spezifischen Probleme der Anwender.

552 In Anlehnung an Hafner 2005, S. 255.
553 Vgl. Hafner 2005, S. 62.
554 Vgl. Lichter et al. 1993, S. 222
555 Vgl. Lichter et al. 1993, S. 222f.

- Experimentelles Prototyping: Das experimentelle Prototyping fokussiert auf die technische Realisierung eines Entwicklungsziels. Durch Experimentieren sind die Anwender in der Lage, ihre Anforderungen zu konkretisieren. Im Gegensatz zum explorativen Prototyping steht nicht die Implementierung unterschiedlicher Varianten, sondern das Experimentieren der Anwender im Vordergrund.

- Evolutionäres Prototyping: Evolutionäres Prototyping löst den Begriff des „Protytyping" aus dem Kontext eines dedizierten Entwicklungsprozesses heraus. Im Sinne des evolutionären Prototyping ist Softwareentwicklung kein in sich geschlossenes Projekt, sondern ein kontinuierlicher Prozess, der sich über den ganzen Lebenszyklus eines Systems erstreckt. Dies beeinflusst die Rolle des Entwicklers. Er arbeitet in enger Zusammenarbeit mit dem Anwender an der kontinuierlichen Weiterentwicklung eines Systems.

Im Rahmen der Architekturentwicklung sind insbesondere das explorative und das experimentelle Prototyping von Bedeutung. Beide Ansätze ermöglichen es, einzelne Gestaltungsoptionen zu detaillieren, um so Vor- und Nachteile der unterschiedlichen Lösungsansätze genau zu untersuchen. Im Rahmen der Fallstudien wurde das Prototyping insbesondere auch als Verfahren eingesetzt, um die Abschätzung von Kosten und Risiken neuer Lösungsansätze zu verbessern.[556]

6.4.4 Aktivitäten der Phase „Definition Massnahmenkomplexe"

6.4.4.1 Massnahmenkomplexe ableiten

Ziel dieser Aktivität ist es, Massnahmen zur Umsetzung der erarbeiteten Lösungsansätze abzuleiten, die die identifizierten Schwächen adressieren. Abschliessend erfolgt die Bündelung der ermittelten Massnahmen unter Berücksichtigung inhaltlicher Verflechtungen zu Massnahmenkomplexen.

Die Ausgangsbasis für die Auswahl von Massnahmen bilden die bereits existierenden und geplanten Massnahmen sowie die ermittelten Schwachstellen und Lösungsansätze der vorangegangenen Aktivitäten. Wurde im Rahmen der vorausgehenden Aktivitäten eine Grundschutzanalyse durchgeführt, so berücksichtigt die Auswahl der Massnahmen insbesondere auch den verwendeten Grundschutzkatalog.[557] Die im Katalog adressierten Bedrohungen werden ohne weitere Risikoanalyse als relevant erachtet und die insofern vorgeschlagenen Massnahmen ohne weitere Prüfungen übernommen.

Es erfolgt dann ein Abgleich der ermittelten Massnahmen mit existierenden und bereits geplanten Massnahmen. Die noch zu realisierenden Massnahmen werden in einer Liste zusam-

556 Zur Abschätzung von Kosten und Risiken im Kontext des Prototyping vgl. Lichter et al. 1993, S. 221.
557 Vgl. im Folgenden Zentrum für sichere Informationstechnologie - Austria 2004, S. 65.

mengefasst und einzeln beschrieben. Tabelle 42 zeigt exemplarisch die Beschreibung einer Massnahme, die eine Kosten-Nutzen-Betrachtung umfasst. In der Regel stehen alternative, sich ausschliessende Massnahmen zur Auswahl.[558] Um die sowohl aus Sicherheits- wie auch aus Wirtschaftlichkeitsüberlegungen zu bevorzugende Massnahme zu ermitteln, kann im Einzelfall ein direkter Vergleich der Massnahmen und somit eine Bewertung einzelner Massnahmen notwendig sein.

Massnahme M1: Unterstützung und Anpassung des Entwicklungsprozesses		
Allgemeines		
Beschreibung	Um die Erfüllung rechtlicher und regulatorischer Anforderungen sicherzustellen, muss der Softwareentwicklungsprozess durch die Bereitstellungen von Checklisten, Best Practices oder Methoden unterstützt und angepasst werden. Zu adressieren sind die Gestaltung der Rechte- und Rollendefinitionen, die Gestaltung der Administrationsprozesse und der Review der Applikationen.	
Aufwand	Ermittlung bzw. Zusammenstellung der Anforderungen: ca. 20 PT Erstellung Checklisten, Best Practices oder Methoden: ca. 20 PT Ausarbeitung Reviewverfahren: ca. 20 PT Anpassung des Softwareentwicklungsprozesses: ca. 5 PT	
Bewertung Nutzen		
Kosteneinsparung	Gering:	Geringes Kostensenkungspotenzial durch die Verwendung von Best Practices
Sicherheit	Hoch:	Systematische Adressierung von Sicherheitsanforderungen muss gewährleistet werden.
Bewertung Kosten		
Impl.kosten	Mittel:	Aufwand ca. 65 PT
Risiko	Gering:	Geringes Risiko durch mögliche Nichtbeachtung der Vorgaben.

Tabelle 42: Massnahmendefinition (Beispiel)

Im Anschluss an die Ableitung von Massnahmen erfolgt die Zusammenstellung von Massnahmen zu Massnahmenkomplexen. Eine Rolle spielen hierbei insbesondere die inhaltlichen Verflechtungen der Massnahmen untereinander.[559] Weiterhin ist die Priorität der einzelnen Massnahmen von Bedeutung. Die Zusammenfassung von Massnahmen erfordert ein hohes Mass an Wissen über die Zusammenhänge sowie die politisch-kulturellen Implikationen der betroffenen Massnahmen. Eine Standardisierung oder gar Automatisierung dieser Aufgabe ist kaum möglich.[560]

Die Massnahmen zur Reduzierung identifizierter Risiken können unterschiedliche Aspekte abdecken: Sie können u.a. der Vorbeugung, der Aufdeckung, der Abschreckung, der Schadensbegrenzung sowie der Bildung eines Sicherheitsbewusstseins dienen.[561] Welche dieser Eigenschaften eine Massnahme aufzuweisen hat, muss situationsabhängig entschieden werden. Im Allgemeinen werden Massnahmen bzw. Massnahmenkomplexe bevorzugt, die mehrere der genannten Aspekte abdecken. Es ist darauf zu achten, dass die Gesamtheit der Mass-

558 Vgl. Zentrum für sichere Informationstechnologie - Austria 2004, S. 64.
559 Vgl. Hafner 2005, S. 226.
560 Vgl. Hafner 2005, S. 226.
561 Vgl. Zentrum für sichere Informationstechnologie - Austria 2004, S. 64.

nahmen alle Aspekte ausgewogen berücksichtigt, so dass beispielsweise nicht ausschliesslich vorbeugende oder abschreckende Massnahmen umgesetzt werden.

6.4.4.2 Massnahmenkomplexe bewerten

Ziel der Aktivität „Massnahmenkomplexe bewerten“ ist es, die ermittelten Massnahmenkomplexe zu priorisieren. Abschliessend muss geprüft werden, ob die identifizierten Massnahmenkomplexe eine angemessene Reduktion der aufgedeckten Risiken gewährleisten.

Die Bewertung einzelner Massnahmen empfiehlt sich insbesondere dann, wenn alternative, sich ausschliessende Massnahmen gegeneinander abzuwägen sind.[562] Die Priorisierung der Massnahmenkomplexe empfiehlt sich generell, um unter Sicherheits- und Wirtschaftlichkeitsüberlegungen die Massnahmenkomplexe zu ermitteln, die im Rahmen der Umsetzung zu bevorzugen sind. Die Bewertung der Komplexe erfolgt dabei analog zur Bewertung einzelner Massnahmen auf der Basis qualitativer oder quantitativer Verfahren.[563] Grundsätzlich ist für jeden Massnahmenkomplex zu prüfen, ob die Umsetzung der Massnahmen die zu erwartende Risikoreduktion bzw. die zu erwartenden Effizienzgewinne rechtfertigt. In der Regel ist der Nutzen einer Massnahme, der aus einer zu erwartenden Risikoreduktion hervorgeht, nur schwer quantifizierbar.[564] Entsprechende Bewertungsunsicherheiten sind somit gegeben. Die abschliessende Entscheidung, ob ein Sicherheitsrisiko zu adressieren oder zu tragen ist, ist in diesen Fällen vom Risikoträger zu treffen.

Absolute Sicherheit ist auch nach der Umsetzung aller Sicherheitsmassnahmen nicht erreichbar.[565] Um zu entscheiden, ob die identifizierten Massnahmenkomplexe eine angemessene Reduktion der aufgedeckten Risiken herbeiführen, sind weitere Schritte durchzuführen. Zunächst sind die verbleibenden Restrisiken zu ermitteln. Dabei empfiehlt sich die Anwendung der Verfahren, die bereits im Rahmen der Risikoanalyse innerhalb der Ist-Aufnahme verwendet wurden.[566] Die verbleibenden Restrisiken sind nun als „akzeptabel“ oder „nicht akzeptabel“ einzustufen. Die weitere Behandlung nicht-akzeptabler Restrisiken obliegt dem Management: Einerseits können weitere risikominimierende Massnahmen initiiert werden. Anderseits können z.B. aus Wirtschaftlichkeitsüberlegungen heraus Risiken bewusst akzeptiert werden. Für diese Risiken gilt es, Verantwortlichkeiten festzulegen und eine entsprechende Dokumentation zu erstellen.

562 Vgl. Kapitel 6.4.4.1.
563 Vgl. im Folgenden NIST 2002, S. 38.
564 Vgl. NIST 2002, S. 39.
565 Vgl. im Folgenden Zentrum für sichere Informationstechnologie - Austria 2004, S. 67.
566 Vgl. Kapitel 6.4.2.1.

6.5 Dokumentationsmodell

Das Dokumentationsmodell stellt die Ergebnisse und die Beziehungen zwischen den Ergebnissen dieses Methodenbausteins dar (vgl. Tabelle 43). Die dargestellten Beziehungen implizieren inhaltliche sowie zeitliche Abhängigkeiten. Wie dargelegt, berücksichtigen die Ausführungen zur Methode zwar Ergebnisse, die Frage, auf Basis welcher Notation einzelne Ergebnis zu spezifizieren sind, wird im Rahmen der Ausführung jedoch nicht abschliessend festgelegt.[567] Da die Ergebnisse bereits im Rahmen der Ableitung sowie innerhalb der einzelnen Aktivitäten beschrieben wurden, erfolgt die Darstellung überblicksartig unter besonderer Berücksichtigung der Beziehungen der Ergebnisse.

A basiert auf B	**Ergebnis B**			
Ergebnis A	**1 Vorstudie**	**2 Aufnahme Ist-Situation**	**3 Definition Soll-Situation**	**4 Definition Massn.komplexe**
1 Vorstudie				
1.1 Abgegrenzte Themengebiete				
1.2 Aufgearbeitete Lösungsbeiträge	*1.1*			
1.3 Autorisierungsanforderungen	*1.1*, 1.2			
1.4 Glossar	1.1, 1.2, 1.3			
2 Aufnahme Ist-Situation				
2.1 Applikationsbewertungen	1.1, 1.2, *1.3*, 1.4			
2.2 Systembewertungen	1.1, 1.2, *1.3*, 1.4	2.1		
2.3 Zentrale Problemfelder	1.1, 1.2, *1.3*, 1.4	2.1, *2.2*		
3 Definition Soll-Situation				
3.1 Autorisierungsarchitektur	1.1, 1.2, *1.3*, 1.4	2.1, 2.2, *2.3*		
3.2 Direktiven	1.1, 1.2, *1.3*, 1.4	2.1, 2.2, *2.3*	*3.1*	
3.3 Leitelemente	1.1, 1.2, *1.3*, 1.4	2.1, 2.2, *2.3*	*3.1*	
4 Definition Massnahmenkomplexe				
4.1 Massnahmenkomplexe	1.1, 1.2, *1.3*, 1.4	2.1, 2.2, *2.3*	*3.1*, 3.2, 3.3	
4.2 Priorisierte Massn.komplexe	1.1, 1.2, *1.3*, 1.4	2.1, 2.2, *2.3*	*3.1*, 3.2, 3.3	*4.1*

Legende: Essentielle Ergebnisabhängigkeiten sind kursiv dargestellt

Tabelle 43: Dokumentationsmodell Autorisierungsarchitektur

Das resultierende Dokumentationsmodell zeigt, dass einmal entwickelte Ergebnisse in fast jede folgende Aktivität und somit auch in deren Ergebnisse eingehen. Dies gilt insbesondere für die Ergebnisse, die in der *Vorstudie* produziert werden: Die Gliederung des Themengebietes, die aufgearbeiteten Lösungsbeiträge, die ermittelten Anforderungen sowie die definierten Begrifflichkeiten bilden die Grundlage für die Erstellung der weiteren Ergebnisse. Die Ergebnisse der *Ist-Aufnahme* sind für die folgenden Aktivitäten der Soll-Definition sowie der Ableitung der Massnahmen relevant. Dies gilt vor allem für die konsolidierten Problemfelder. Für die Abklärung von Detailfragestellungen sind weiterhin die einzelnen Applikations- und Sys-

567 Zur Begründung vgl. die Einleitung in Kapitel 6.4.

tembewertungen relevant. Analog verhält es sich mit den Ergebnissen der *Soll-Definition*. Die erarbeiten Lösungsansätze der Architektur sind zwingend im Weiteren zu berücksichtigen. Die Direktiven und Leitelemente sind wiederum für die sich ergebenden Detailfragestellungen von Interesse.

6.6 Rollenmodell

Im Rahmen der Fallstudien zeichnete sich jeweils eine Arbeitsgruppe für die Entwicklung der Autorisierungsarchitektur verantwortlich. Alle Aktivitäten, die zur Entwicklung der Architektur notwendig waren, wurden von ihr verantwortet und durchgeführt. Der Arbeitsgruppe stand ein Gruppenleiter aus dem Bereich Architektur vor, der für die koordinativen und administrativen Tätigkeiten verantwortlich war. Für die Arbeitsgruppe empfehlen sich insbesondere folgende Vertreter:[568]

- Vertreter Architektur: Die Vertreter der Architektur bringen die konzeptionelle, ganzheitliche Perspektive des Architekturmanagements in die Arbeitsgruppe ein. Die Mitarbeiter der Architektur sind u.a. für die Abstimmung der Autorisierungsarchitektur mit anderen Architekturen verantwortlich.

- Vertreter Entwicklung: Die Vertreter der Entwicklung verfügen über Erfahrung bei der Entwicklung von Berechtigungskonzepten und der Verwendung von Autorisierungskomponenten. Als Anwender der Autorisierungskomponenten bringen sie die Kundenperspektive in die Arbeitsgruppe ein.

- Vertreter Betrieb: Aus dem Bereich Betrieb sind insbesondere die Mitarbeiter der zentralen Benutzeradministration für die Arbeitsgruppe von Bedeutung, da sie mit den operativen Administrationsprozessen vertraut sind. Aufgrund ihrer Arbeit verfügen sie über ein umfangreiches Prozess- und Systemwissen im Hinblick auf die Autorisierung. Da sie eine Vielzahl von Applikationen und Systemen administrieren, kennen sie die unterschiedlichen Autorisierungsansätze und -werkzeuge die im Unternehmen verwendet werden.

Im Rahmen der durchgeführten Fallstudienprojekte wurden weitere Mitarbeiter in die Projektarbeit involviert. Hierzu gehörten insbesondere:

- Mitarbeiter Fachbereich: Sicherheitsstandards wie der ISO/IEC 17799 verlangen explizit, dass fachliche Anforderungen an die Autorisierung erhoben und dokumentiert werden.[569] Zu berücksichtigen sind zum einen die Mitarbeiter, die in Zusammenarbeit mit der IT die Zugriffsberechtigungen definieren. Zum anderen ist das Management des Fachbereichs zu involvieren, da es letztendlich die Kosten und Risiken, die mit der Autorisierung einhergehen, trägt.

568 Die Empfehlung basiert auf den Fallstudien, vgl. hierzu Kapitel 4.1 und 4.2.
569 Vgl. im Folgenden Kapitel 6.4.1.3.

- Mitarbeiter Revision, Risiko- und Sicherheitsmanagement: Bei der Entwicklung der Autorisierungsarchitektur müssen existierende Weisungen und intern verwendete Sicherheitsstandards Berücksichtigung finden.[570] Um diese angemessen einzubeziehen, empfiehlt sich die Rücksprache mit den Mitarbeitern der verantwortlichen Abteilungen wie Revision, Risiko- oder Sicherheitsmanagement.

Die im Rahmen der Fallstudien eingesetzten Arbeitsgruppen bestanden aus wenigen Mitarbeitern, so dass die entsprechenden Projektorganisationen keine umfänglichen Aufgabenteilungen aufwiesen. Auf der Basis der Fallstudien lassen sich lediglich die typischen Projektrollen Projektsponsor, Projektleiter und Projektmitarbeiter unterscheiden. Der Projektsponsor stellt die finanziellen Mittel zur Projektdurchführung zur Verfügung.[571] Darüber hinaus überwacht er den Projektfortschritt und unterstützt das Projekt bei der Umsetzung der Lösung. Im Rahmen der aufgenommenen Fallstudien nahm das Topmanagement der IT diese Rolle wahr. Der Projektleiter ist für das operative Management des Projektes verantwortlich.[572] Zu seinen Aufgaben gehören insbesondere auch administrative Tätigkeiten wie z.B. die Organisation von Arbeitsgruppentreffen oder die Abwicklung des Projektreporting. Der Projektleiter hat in der Regel keine formale Autorität über die Projektmitarbeiter d.h. er verfügt über keinerlei disziplinarische Vollmachten.[573] Im Rahmen der Fallstudien wurde diese Rolle durch einen Vertreter der Architektur besetzt. Die Projektmitarbeiter führen die eigentliche Projektarbeit durch.[574] Im Rahmen der Fallstudien nahmen die Vertreter der dargestellten Bereiche diese Rolle wahr. Die spezifizierten Aktivitäten des Vorgehensmodells wurden von den Projektmitarbeitern gemeinschaftlich erbracht.

570 Vgl. Kapitel 6.4.1.3.
571 Vgl. hierzu z.B. auch Balzert 2000, S. 60 und 98f.
572 Vgl. im Folgenden auch Balzert 1998, S. 86f; Krasna et al. 1998, S. 120.
573 Vgl. hierzu auch Balzert 1998, S. 81.
574 Vgl. im Folgenden auch Balzert 1998, S. 86f.

7 Methodenbaustein Integration der Autorisierung

Im Rahmen des vorherigen Kapitels wurden unterschiedliche Gestaltungsoptionen der Autorisierung diskutiert.[575] Die Integration systemspezifischer Berechtigungskonzepte auf der Basis systemübergreifender Rollen hat sich dabei als ein Lösungsansatz herausgestellt, der massgeblich zu einer effizienten und effektiven Autorisierung beitragen kann.[576] Im Folgenden wird daher – dem Themenfokus der Arbeit entsprechend[577] – auf der Grundlage der beschriebenen Fallstudien und der analysierten Literatur ein Vorgehensmodell für die Integration der Autorisierung abgeleitet. Ausgehend von der systemspezifischen Autorisierung wird in Abschnitt 7.1 zunächst die Integrationsleistung der zu entwickelnden Vorgehensweise charakterisiert und festgelegt. Die eigentliche Ableitung (vgl. Abschnitt 7.3) und Beschreibung des Vorgehensmodells (vgl. Abschnitt 7.4) schliesst sich an die Vorstellung eines grundlegenden Metamodells an (vgl. Abschnitt 7.2). Abschliessend werden in den Abschnitten 7.5 und 7.6 das Dokumentations- und das Rollenmodell des Methodenbausteins dargestellt.

7.1 Ausgangspunkt des Methodenentwurfs

Die folgenden Abschnitte befassen sich mit der Darstellung der elementaren Grundlagen für den Entwurf des Methodenbausteins „Integration der Autorisierung“. Ausgehend von der systemspezifischen Autorisierung wird die Integrationsleistung der zu entwickelnden Vorgehensweise charakterisiert und festgelegt.

7.1.1 Systemspezifische Autorisierung

Die systemspezifische Autorisierung wird in die zwei Teilbereiche applikatorische Autorisierung und Systemautorisierung unterteilt.[578] Während die Systemautorisierung Infrastruktursysteme wie z.B. Betriebs-, Firewall- oder Middlewaresysteme zum Gegenstand hat, setzt sich die applikatorische Autorisierung mit der Verwaltung und Kontrolle von Zugriffsberechtigungen in Geschäftsanwendungen auseinander. Im Gegensatz zur Systemautorisierung stellt die applikatorische Autorisierung eine besondere Herausforderung dar:[579]

- Komplexität: Im Rahmen der Systemautorisierung muss eine Vielzahl von Nutzern auf eine grosse Anzahl von Objekten (z.B. Verzeichnisse oder Dateien) zugreifen. Jedoch ist die Anzahl der Operationen, die auf den Objekten durchgeführt werden können (z.B. Lesen, Schreiben, Ausführen) in der Regel sehr gering. Die applikatorische Autorisierung ist ebenfalls durch eine Vielzahl von Nutzern und Objekten bzw. Daten gekennzeichnet. Die Anzahl unterschiedlicher Operationen ist jedoch typischerweise wesentlich höher.

575 Vgl. Kapitel 6.4.
576 Vgl. Kapitel 6.4.3.1.
577 Vgl. Kapitel 1.2.
578 Vgl. im Folgenden Kern et al. 2004b. S. 88.
579 Vgl. Kern et al. 2004b, S. 89ff.

- Wandel: Unternehmen sind einem stetigen Wandel ausgesetzt. Applikatorische Berechtigungskonzepte müssen den Änderungen im Geschäftsumfeld Rechnung tragen und unterliegen somit ihrerseits permanenten Änderungen. Da Infrastruktursysteme den Betrieb von Anwendungen unabhängig von einer bestimmten Anwendung ermöglichen,[580] sind deren Berechtigungskonzepte wesentlich unabhängiger von Veränderungen im geschäftlichen Umfeld.

- Generische Autorisierungsansätze: Unternehmen müssen eine Vielzahl unterschiedlicher Objekte wie z.B. Partner oder Verträge schützen, die über verschiedene Attribute verfügen und durch diverse Operationen manipuliert werden können. Um diese Vielfältigkeit im Rahmen der Applikationen zu beherrschen, sind im Gegensatz zur Systemautorisierung sehr generische Berechtigungsstrukturen notwendig. Durch die Freiheitsgrade, die diese Strukturen bei der Spezifikation von Berechtigungen bieten, gestaltet sich die Entwicklung applikatorischer Berechtigungskonzepte grundsätzlich schwieriger als der Entwurf von Berechtigungskonzepten für Infrastruktursysteme.

Hinsichtlich der zu entwickelnden Integrationsvorgehensweise gilt es, beide Arten der Autorisierung zu berücksichtigen. Die besonderen Herausforderungen der applikatorischen Autorisierung sind in die Methodenentwicklung einzubeziehen.

7.1.2 Gegenstand und Art der zu realisierenden Integration

Den Ausgangspunkt der zu entwickelnden Integrationsvorgehensweise bilden die existierenden Berechtigungskonzepte der Systeme einer Unternehmung. Diese sind auf Basis der zu entwickelnden Vorgehensweise zu integrieren.

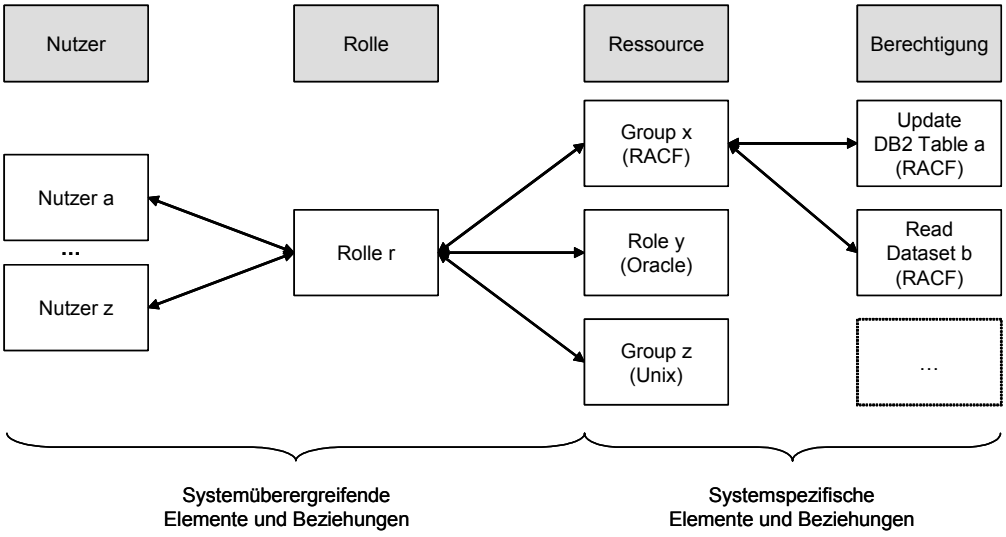

Abbildung 58: Integration der Ressourcen auf der Basis von Rollen[581]

[580] Vgl. z.B. Winter 2002, S. 936.
[581] In Anlehnung an Kern 2002, S. 5.

Ansatzpunkt der Integration sind nicht die feingranularen Berechtigungen der einzelnen Systeme, sondern systemspezifische Berechtigungsbündel, die implementierungsspezifisch in der Praxis auch als Rollen, Profile oder Gruppen bezeichnet werden. In Anlehnung an die analysierten Fallstudien werden diese Berechtigungsbündel in dieser Arbeit als Ressourcen bezeichnet.[582] Abbildung 58 veranschaulicht die Verknüpfung zwischen systemspezifischen Ressourcen und übergreifenden Rollen. Um den Charakter der zu entwickelnden Integrationsvorgehensweise aufzuzeigen, soll ihr Profil im Folgenden anhand ausgewählter Merkmale der Integration dargestellt werden

Bezüglich des *Integrationsgegenstandes* lassen sich die Daten-, Anwendungs- und Prozessintegration unterscheiden.[583] Bei der Datenintegration erfolgt die Verknüpfung unterschiedlicher Systeme durch die Nutzung gleicher Datenbestände oder Datenstrukturen.[584] Die Integration auf Anwendungsebene basiert auf der Verknüpfung von Methoden, Funktionen oder Prozeduren der zu integrierenden Applikationen.[585] Bei der Prozessintegration steht die Verknüpfung und durchgängige Unterstützung von Teilaufgaben eines Arbeitsablaufes im Vordergrund.[586] Die Integration von systemspezifischen Berechtigungskonzepten basiert auf der Verknüpfung von Datenstrukturen und Daten und ist somit primär der Datenintegration zuzuordnen. Die Datenintegration bildet die Grundlage für die Verknüpfung und durchgängige Abwicklung der Administrationsprozesse. Damit ist insbesondere auch die Prozessintegration das Ziel der zu entwickelnden Vorgehensweise.

Es sind zwei *Integrationsrichtungen* zu unterscheiden, die die grundsätzliche Art der Integration bestimmen.[587] Die horizontale Integration bezieht sich auf die Verbindung von Teilsystemen in der betrieblichen Wertschöpfungskette. Die vertikale Integration beschäftigt sich hingegen mit der Verknüpfung der Planungs- und Kontrollsysteme mit den Administrations- und Dispositionssystemen. Die zu entwickelnde Integrationsvorgehensweise adressiert die Integration operativer und dispositiver Systeme aus der Perspektive der Autorisierung und ist damit sowohl der horizontalen als auch der vertikalen Integration zuzurechnen.

Bezüglich der *Integrationsreichweite* wird zwischen der innerbetrieblichen und der zwischenbetrieblichen Integration unterschieden.[588] Die innerbetriebliche Integration beschränkt den Betrachtungsfokus auf ein rechtliches Unternehmen. Dabei kann sich die Integration auf einen oder mehrere Bereiche eines Unternehmens auswirken. Die zwischenbetriebliche Integration stellt eine Weiterführung der innerbetrieblichen Integration dar. Das Betrachtungsfeld wird auf mehrere rechtlich selbständige Unternehmen erweitert. Die zu realisierende Integrations-

582 Vgl. Kapitel 4.
583 Vgl. Wortmann 2004, S. 8ff.
584 Vgl. hierzu auch Kaib 2002, S. 17.
585 Vgl. Wortmann 2004, S. 9.
586 Vgl. Kaib 2002, S. 17.
587 Vgl. im Folgenden Kaib 2002, S. 18.
588 Vgl. im Folgenden Kaib 2002, S. 19f.

vorgehensweise konzentriert sich auf die innerbetriebliche Integration der Autorisierung, so dass sich auch die erhobenen Fallstudien auf diesen Gegenstandsbereich fokussieren.

Die Integration von Systemen kann zu unterschiedlichen Zeitpunkten realisiert werden.[589] Liegt der *Integrationszeitpunkt* vor der eigentlichen Implementierung und Einführung eines oder mehrerer Systeme, so wird von einer Ex-ante-Integration gesprochen. Bei der Entwicklung eines modularen Anwendungssystems kann beispielsweise bereits in der Entwurfsphase die Erarbeitung einer integrierten Datenbasis Gegenstand der Analyse sein. Bei der Ex-post-Integration müssen Systeme verknüpft werden, die oft nicht dafür konzipiert sind, mit anderen Systemen zu kommunizieren. Darüber hinaus erschwert die Existenz unterschiedlicher Technologien und Realisierungsparadigmen die nachträgliche Integration der Systeme. Diese Heterogenität ist insbesondere auf die Einführung immer neuer Anwendungssysteme zurückzuführen, die ohne eine architektonische Gesamtplanung vorgenommen wurde. Im Mittelpunkt der zu entwickelnden Integrationsvorgehensweise steht die Ex-post-Integration bestehender Berechtigungskonzepte. Entsprechend wird im weiteren Verlauf dieser Arbeit der Integrationsbegriff im Sinne der Ex-post-Integration gebraucht.

Abbildung 59 zeigt abschliessend das Profil der zu entwickelnden Integrationsvorgehensweise im Überblick. Die hervorgehobenen Ausprägungen verdeutlichen die Eigenschaften der zu realisierenden Integration.

Merkmal	Merkmalsausprägung		
Integrationsgegenstand	Daten	Anwendungen	Prozesse
Integrationsrichtung	Horizontal	Vertikal	
Integrationsreichweite	Innerbetrieblich	Zwischenbetrieblich	
Integrationszeitpunkt	Ex-ante-Integration	Ex-post-Integration	

Abbildung 59: Charakteristik der zu entwickelnden Integrationsvorgehensweise

7.1.3 Konsequenzen für den Methodenentwurf

Die Integration der systemspezifischen Berechtigungskonzepte ist Gegenstand der zu entwickelnden Vorgehensweise. Für den Methodenentwurf ergeben sich aus den obigen Ausführungen folgende Konsequenzen:

- Systemspezifische Autorisierung: Im Rahmen der zu entwickelnden Integrationsvorgehensweise muss sowohl die applikatorische Autorisierung wie auch die Systemautorisierung berücksichtigt werden. Da die Methode auf einer induktiven Ableitung basiert,

[589] Vgl. im Folgenden Kaib 2002, S. 20f.

tragen die Fallstudien wesentlich zur angemessenen Erfüllung dieser Anforderungen bei. Die zur Induktion herangezogenen Fallstudien setzen sich mit der Integration von Berechtigungskonzepten auseinander, die sowohl Applikationen als auch Infrastruktursystemen zuzurechnen sind. Damit werden beide Typen der Autorisierung durch die induzierte Vorgehensweise adressiert.

- Gegenstand und Art der zu realisierenden Integration: Zentraler Gegenstand der zu erarbeitenden Vorgehensweise ist die Ex-post-Integration von systemspezifischen Berechtigungskonzepten. Diese Tatsache muss bei der Entwicklung der Vorgehensweise berücksichtigt werden. Die zu spezifizierenden Aktivitäten sollen sich daher auf die Verrichtungseinheiten konzentrieren, die sich unmittelbar mit dem erstmaligen Entwurf und der Implementierung von Rollen auseinandersetzen.

Nach der Darstellung des Ausgangspunkts der zu entwickelnden Methode folgt nun die eigentliche Methodenentwicklung.

7.2 Metamodell

Abbildung 60 zeigt das Metamodell „Integration der Autorisierung“, das auf dem Metamodell „Autorisierung“[590] und dem ERBAC-Standard[591] aufbaut. Das Metamodell umfasst die bereits im Metamodell „Autorisierung“ definierten organisatorischen Metaentitätstypen „Person“, „Prozessrolle“ und „Aufgabe“. Darüber hinaus sind die für die informationstechnische Verarbeitung von Zugriffsberechtigungen relevanten Metaentitätstypen „Benutzerkonto“, „Ressource“ und „Berechtigung“ im Modell vorhanden. Zusätzlich zum Metamodell „Autorisierung“ sind jedoch die Entitätstypen „zentrales Benutzerkonto“, „Rolle“ und „Rollenklasse“ entsprechend dem ERBAC-Standard[592] in das Modell integriert.

Die Integration der systemspezifischen Ressourcen erfolgt auf der Basis von Rollen, die die systemspezifischen Ressourcen zu systemübergreifenden Berechtigungsbündeln zusammenfassen.[593] Im ERBAC-Standard werden die Rollen als Enterprise-Rollen bezeichnet, um ihren systemübergreifenden Charakter hervorzuheben und sie von systemspezifischen Rollen abzugrenzen. Letztere werden im Kontext dieser Arbeit in Anlehnung an die Terminologie der Fallstudien[594] und zur Vermeidung von Missverständnissen als Ressourcen bezeichnet.[595] Im Mittelpunkt der zu entwickelnden Integrationsvorgehensweise steht die Implementierung von systemübergreifenden Rollen. Daher wird der Rollenbegriff im weiteren Verlauf dieser Arbeit im Sinne der Enterprise Rolle gebraucht.

590 Vgl. Kapitel 5.3.3.
591 Vgl. Kapitel 2.3.3.
592 Vgl. Kapitel 2.3.3.
593 In Anlehnung an Kern et al. 2002, S. 46ff; vgl. Kapitel 2.3.3.
594 Vgl. hierzu insbesondere Fallstudie Basler Versicherungen, Kapitel 4.3.
595 Vgl. Kapitel 5.3.3.

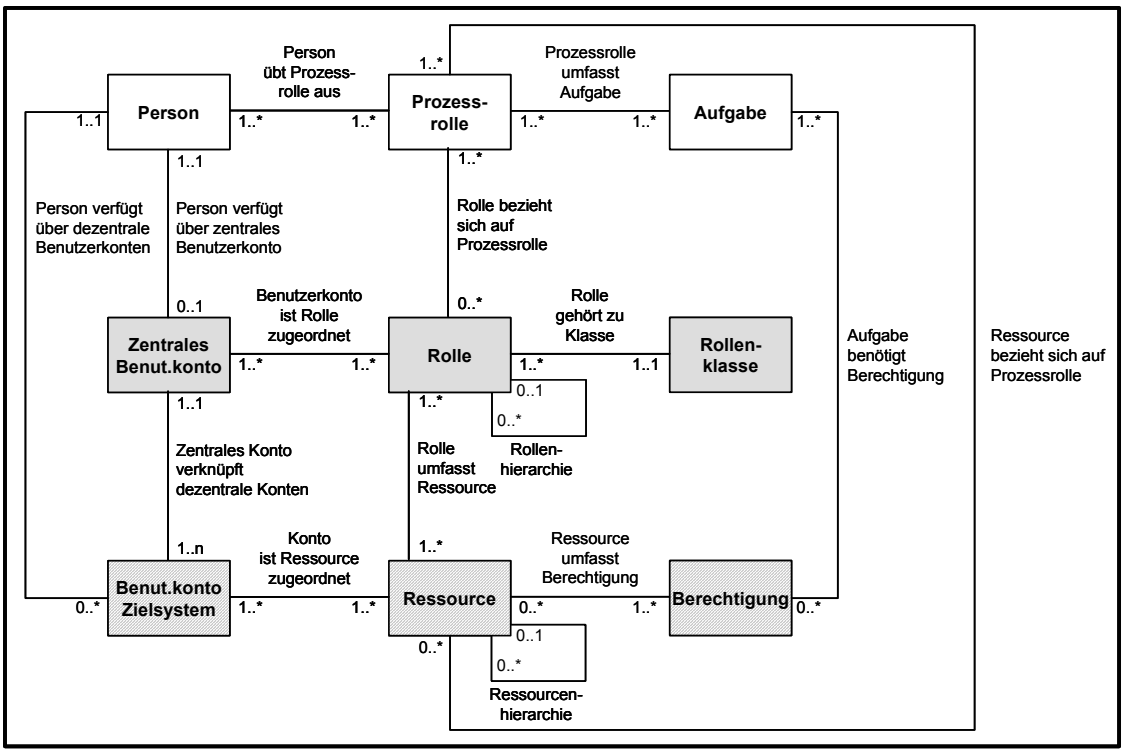

Abbildung 60: Metamodell „Integration der Autorisierung“

Bei einer näheren Betrachtung der Fallstudien zeigt sich, dass analog zur Definition der Ressourcen auch die Definition der Rollen nur eingeschränkt auf aufbauorganisatorischen Elementen wie z.B. Stellen basiert. In den einzelnen Organisationseinheiten existieren vielmehr eine Vielzahl von informellen, nicht dokumentierten Stellvertretungen und ablauforganisatorischen Aufgaben- und Kompetenzverteilungen, die den Definitionsprozess massgeblich bestimmen.

Jede Rolle gehört einer Rollenklasse an, die in ihrer Gesamtheit den Rollenentwicklungs- und -implementierungsprozess strukturieren. Eine Rollenklasse umfasst eine Menge von Rollen, die aufgrund gemeinsamer Merkmale in Abgrenzung zu anderen Rollen zu einer Gruppe zusammengefasst werden. Rollen werden systemübergreifenden, zentral vorgehaltenen Benutzerkonten zugeordnet, die der Verknüpfung systemspezifischer Benutzerkonten dienen und eine systemübergreifende Benutzerrepräsentation darstellen.

Während die in Abbildung 60 schraffiert dargestellten Metaentitätstypen in dezentralen Autorisierungskomponenten administriert werden, erfolgt die Verwaltung der grau hinterlegten Metaentitätstypen in einer zentralen, übergreifenden Autorisierungskomponente, die im ERBAC-Standard als Enterprise Access Management Werkzeug bezeichnet wird.[596]

Entitätstyp	Kurzdefinition	Synonym
Aufgabe	Eine Aufgabe ist eine betriebliche Funktion mit einem bestimmbaren Ergebnis. Sie wird von Menschen und/oder Maschinen ausgeführt.[597]	Aktivität

596 Vgl. Kapitel 2.3.3.
597 Vgl. IMG 1997, Meta 3.

Benutzerkonto	Ein Benutzerkonto (Benutzerkonto Zielsystem) repräsentiert eine Person in einem spezifischen Informationssystem.[598] Ein integriertes Benutzerkonto (Zentrales Benutzerkonto) dient der Verknüpfung systemspezifischer Benutzerkonten und stellte eine systemübergreifende Benutzerrepräsentation dar.	Account
Berechtigung	Eine Berechtigung ermöglicht die Ausführung einer Operation auf einem geschützten Objekt.[599] Die Art der Operation und des Objekts hängt von dem jeweiligen System ab, das es zu schützen gilt.	Systemspezifische Berechtigung, Recht, Zugriffsberechtigung
Person	Eine Person ist ein menschlicher Aufgabenträger, der eine oder mehrere Stellen besetzt.[600]	Mitarbeiter
Prozessrolle	Eine Prozessrolle stellt eine ablauforganisatorische Bündelung von Aufgaben bzw. Aktivitäten dar.[601]	Rolle
Ressource	Eine Ressource umfasst eine oder mehrere Berechtigungen und stellt ein systemspezifisches Berechtigungsbündel dar.[602]	Systemspezifische Rolle, Profil, Kompetenz
Rolle	Eine Rolle fasst systemspezifische Ressourcen zu systemübergreifenden Berechtigungsbündeln zusammen.[603]	Applikationsübergreifende Rolle, Systemübergreifende Rolle, Enterprise Rolle
Rollenklasse	Eine Rollenklasse bezeichnet eine Menge von Rollen, die aufgrund gemeinsamer Merkmale in Abgrenzung zu anderen Rollen zu einer Gruppe zusammengefasst werden.[604]	Rollentyp, Rollenkategorie

Tabelle 44: Definitionen „Integration der Autorisierung“

Tabelle 44 zeigt zusammenfassend die Definitionen der Metaentitätstypen sowie gängige Synonyme der Metaentitätstypen.

7.3 Vorgehensmodell

Um das Vorgehensmodell des Methodenbausteins „Integration der Autorisierung“ abzuleiten, werden zunächst die entsprechenden Fallstudien auf ihre Aktivitäten und deren Abfolge hin untersucht. Durch Induktion erfolgt schlussendlich die Ableitung des konsolidierten Vorgehensmodells.

7.3.1 Vorgehensmodell Fallstudie Basler Versicherungen

Abbildung 61 zeigt das Projektvorgehen zur Definition und Implementierung der systemübergreifenden Rollen bei den Basler Versicherungen.[605] Dargestellt werden die wesentlichen Projektphasen und ihre Aktivitäten. Die Pfeile verdeutlichen die zeitlichen Abhängigkeiten der Aktivitäten. Die Erarbeitung der Grundlagen erfolgt in parallel durchgeführten Aktivitäten einmalig. Die Definition und Implementierung der Rollen wiederholt sich für jeden Unter-

598 Vgl. Kern et al. 2002, S. 46.
599 In Anlehnung an Ferraiolo et al. 2001, S. 233.
600 In Anlehnung an Rosemann/zur Mühlen 1997, S. 102.
601 In Anlehnung an Rosemann/zur Mühlen 1997, S. 101.
602 Die Definition ergibt sich aus der Analyse der Fallstudien, vgl. insbesondere Kapitel 4.3.
603 In Anlehnung an Kern et al. 2002, S. 46ff.
604 In Anlehnung an Brockhaus 2005.
605 Vgl. hierzu auch die ausführliche Beschreibung in Kapitel 4.3.

nehmensbereich. Eine Beschleunigung der Umsetzung ist durch die Parallelisierung der Aktivitäten dieser Phasen möglich: Mehrere Rollen können gleichzeitig definiert und implementiert werden, da unterschiedliche Rollenowner in den Prozess involviert sind.

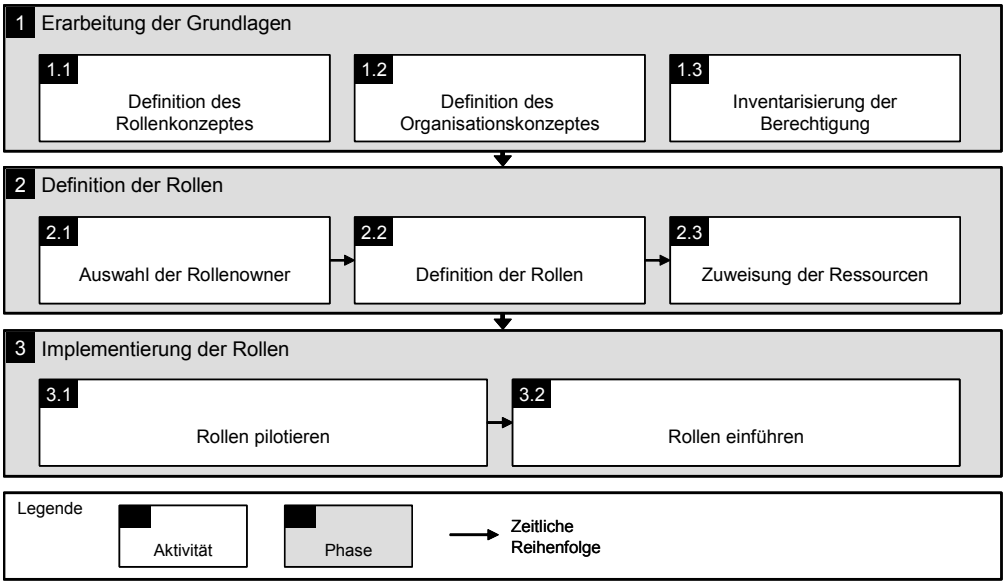

Abbildung 61: Vorgehensmodell Basler Versicherungen

Die einzelnen Aktivitäten können wie folgt zusammengefasst werden (vgl. Tabelle 45):

Nr.	Aktivität	Beschreibung	Zentrale Ergebnisse
1 Erarbeitung der Grundlagen			
1.1	Definition des Rollenkonzeptes	Festlegung der grundlegenden Rollentypen Default-, Abeilungs-, Standard- und Spezial-Rolle.	Rollenkonzept
1.2	Definition des Organisationskonzeptes	Definition der Aufgaben, Kompetenzen und Verantwortlichkeiten der Rollen- und Ressourcenowner sowie deren Herkunft.	Organisationskonzept
1.3	Inventarisierung der Berechtigung	Alle Berechtigungen der Systeme und Applikationen werden in der hierfür vorgesehenen Lotus Notes Datenbank aufgenommen und beschrieben.	Berechtigungsinventar
2 Definition der Rollen			
2.1	Auswahl der Rollenowner	Vor der eigentlichen Definition der Rollen erfolgt die Auswahl der Mitarbeiter, die diese Aufgabe durchführen.	Rollenowner
2.2	Definition der Rollen	Ermittlung der Abteilungs-, Standard-, und Spezial-Rollen.	Rollendefinitionen
2.3	Zuweisung der Ressourcen	Grobe Definition des Berechtigungsumfangs der Rollen. Die Definition wird individuell durch die Rollenowner durchgeführt.	Rollendefinitionen mit Rechten
3 Implementierung der Rollen			
3.1	Rollen pilotieren	Pilotierung der Rollen. Pro Rolle dient ein ausgewählter Mitarbeiter als Ausgangspunkt für die detaillierte Spezifikation, die Implementierung und den Test der Rolle.	Rollenpiloten
3.2	Rollen einführen	Alle Mitarbeiter einer Rolle werden angepasst und konfiguriert.	Implementierte Rollen

Tabelle 45: Aktivitäten Basler Versicherungen

7.3.2 Vorgehensmodell Fallstudie GENERALI

Abbildung 62 zeigt das Projektvorgehen zur Definition und Implementierung der systemübergreifenden Rollen bei der GENERALI.[606] Dargestellt werden wiederum die wesentlichen Projektphasen und ihre Aktivitäten. Durch Pfeile sind die zeitlichen Abhängigkeiten der Aktivitäten gekennzeichnet.

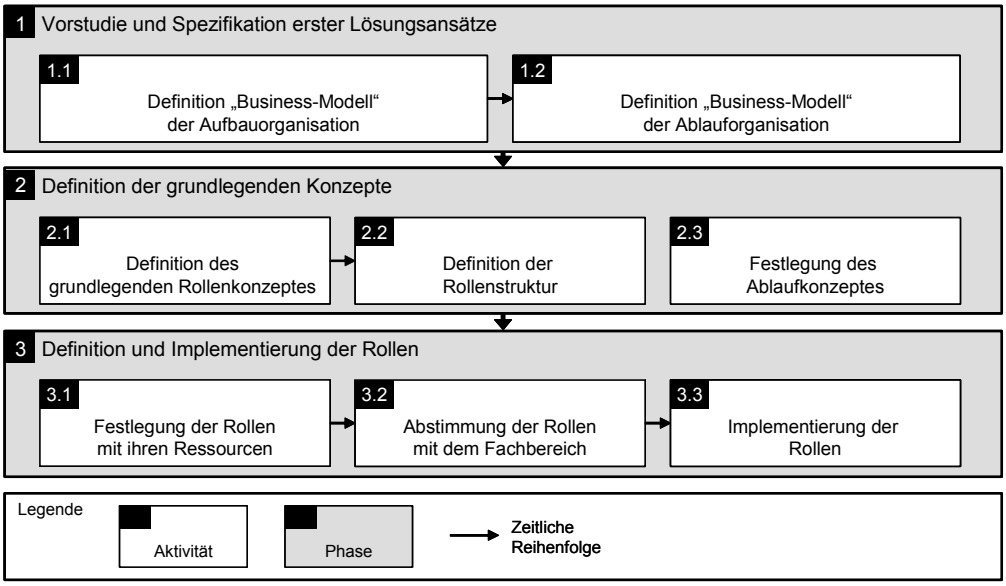

Abbildung 62: Vorgehensmodell GENERALI

Die einzelnen Aktivitäten können wie folgt zusammengefasst werden (vgl. Tabelle 46):

Nr.	Aktivität	Beschreibung	Zentrale Ergebnisse
1 Vorstudie und Spezifikation erster Lösungsansätze			
1.1	Definition „Business-Modell“ der Aufbauorganisation	Analyse, wie die Aufbauorganisation eines Unternehmens mittels technischer Strukturen zwecks automatisierter Berechtigungsvergabe abgebildet werden kann.	„Business-Modell“ der Aufbauorganisation
1.2	Definition „Business-Modell“ der Ablauforganisation	Analyse, wie die Ablauforganisation eines Unternehmens mittels technischer Strukturen zwecks automatisierter Berechtigungsvergabe abgebildet werden kann.	„Business-Modell“ der Ablauforganisation
2 Definition der grundlegenden Konzepte			
2.1	Definition des grundlegenden Rollenkonzeptes	Festlegung der grundlegenden Rollenkategorien und -profile.	Rollenkategorien, Rollenprofile
2.2	Definition der Rollenstruktur	Festlegung der Vererbungsbeziehungen zwischen Rollen und Definition der Zusammenhänge zwischen Rollen, „Permissions“ und „Target Groups“.	Rollenstruktur
2.3	Festlegung Ablaufkonzept	In Bezug auf die Definition von Rollen muss insbesondere festgelegt werden, welche Organisationseinheiten und Mitarbeiter für die Rollendefinition und -implementierung verantwortlich sind.	Ablaufkonzept
3 Definition und Implementierung der Rollen			
3.1	Festlegung der Rollen mit ihren Ressourcen	Initiale Ausstattung einer Rolle mit Berechtigungen. Ausgangspunkt der Zuweisung sind zum Definitionszeitpunkt bereits vergebene Berechtigungen.	Rollendefinitionen

606 Vgl. hierzu auch die ausführliche Beschreibung in Kapitel 4.4.

3.2	Abstimmung der Rollen mit dem Fachbereich	Die eigentliche Abstimmung der Berechtigungen einer Rolle erfolgt in Zusammenarbeit mit dem Fachbereich.	Abgestimmte Rollendefinitionen
3.3	Implementierung der Rollen	Die Implementierung der Rollen wird durch die entsprechenden Mitarbeiter im Autorisierungswerkzeug „DirXmetaRole“ vorgenommen. Dabei weist der Mitarbeiter den Rollen im Werkzeug entsprechende „Permissions“ zu. Die Zuweisung der Mitarbeiter zu Rollen erfolgt im Betrieb durch die Personalmitarbeiter aufgrund der Weisung der Linienvorgesetzten. Diese administrieren die Stellenzuweisungen (die den Rollenzuweisungen entsprechen) der Mitarbeiter über das Personalverwaltungssystem.	Implementierte Rollen

Tabelle 46: Aktivitäten GENERALI

7.3.3 Ableitung des Vorgehensmodells

Die Induktion des Vorgehensmodells umfasst wiederum zwei Schritte.[607] Zuerst werden die Aktivitäten, die eine sich ähnelnde funktionale Verrichtung umfassen, im induzierten Vorgehensmodell zusammengefasst. Tabelle 47 stellt das Ergebnis der Induktion dar. Für jede abgeleitete Aktivität werden die konsolidierten Ergebnisse sowie die korrespondierenden Aktivitäten der Fallstudien aufgeführt. Die Aktivitäten sind in der Tabelle bereits den induzierten Phasen zugeordnet. Die Ableitung der Phasen erfolgt analog zur Bestimmung der Aktivitäten durch eine Zusammenfassung der Phasen, die ähnliche Verrichtungseinheiten umfassen. Als „optional“ gekennzeichnete Aktivitäten haben ihren Ursprung in lediglich einer der analysierten Fallstudien.

Nr.	Aktivität	Zentrale Ergebnisse	Aktivität aus Fallstudie	
			Basler	GENERALI
1 Vorstudie System				
1.1	Grundlegendes Lösungskonzept ausarbeiten (optional)	Metamodell	–	1.1, 1.2
1.2	Rollenkonzept definieren	Rollenkonzept	1.1	2.1, 2.2
2 Vorstudie Organisation				
2.1	Aufgaben, Kompetenzen und Verantwortlichkeiten definieren	Administrationsrollen	1.2	2.3
2.2	Verantwortliche bestimmen	Administratoren	2.1	2.3
3 Rollendefinition				
3.1	Ressourcen bereinigen und inventarisieren (optional)	Ressourceninventar	1.3	–
3.2	Rollengrobspezifikationen festlegen	Rollengrobspezifikationen	2.2	3.1
3.3	Rollenfeinspezifikationen festlegen	Rollenfeinspezifikationen	2.3	3.2
4 Rollenimplementierung				
4.1	Rollen pilotieren	Rollenpiloten	3.1	3.2, 3.3
4.2	Rollen einführen	Implementierte Rollen	3.2	3.3

Tabelle 47: Aktivitäten des induzierten Vorgehensmodells „Integration der Autorisierung“

Anschliessend erfolgt die Ableitung des Vorgehensmodells.[608] Dabei werden ähnliche Aktivitätsabfolgen im Vorgehensmodell zusammengefasst. Abbildung 63 zeigt das induzierte Vorgehensmodell mit den vier Phasen „Vorstudie System“, „Vorstudie Organisation“, „Rollendefinition“ sowie „Rollenimplementierung“. Die einzelnen Phasen werden im Folgenden überblicksartig charakterisiert.

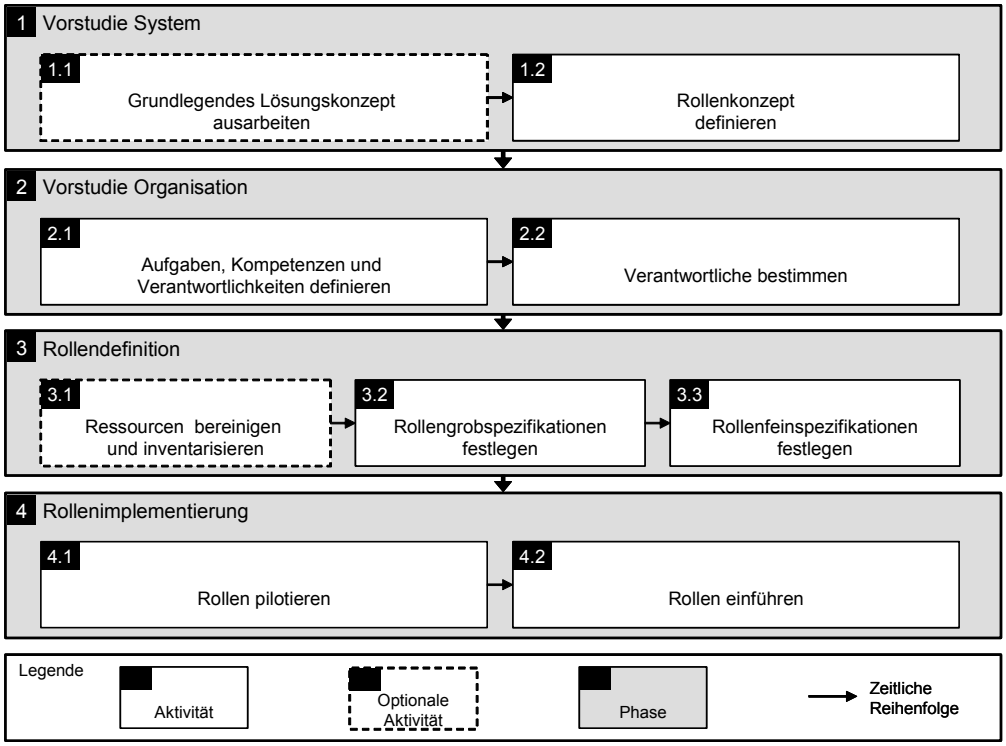

Abbildung 63: Vorgehensmodell „Integration der Autorisierung“

Phase 1: Vorstudie System

Ziel der Phase „Vorstudie System“ ist es, grundlegende Lösungskonzepte für die Entwicklung und Implementierung der systemübergreifenden Rollen zu entwickeln. Zum einen müssen Möglichkeiten aufgezeigt werden, wie die Organisation eines Unternehmens mittels technischer Strukturen abgebildet werden kann (Aktivität 1.1). Darüber hinaus gilt es, Rollenklassen sowie deren Beziehungen festzulegen (Aktivität 1.2). Die abgeleiteten Rollenklassen strukturieren im weiteren Vorgehen den Rollendefinitions- und -implementierungsprozess.

Phase 2: Vorstudie Organisation

In der Phase „Vorstudie Organisation“ werden die Aufgaben, Kompetenzen und Verantwortlichkeiten bei der Definition und Pflege der Berechtigungen zu Administrationsrollen gebündelt (Aktivität 2.1). Hierbei müssen insbesondere auch regulatorische Anforderungen berücksichtigt werden. Abschliessend werden die Administrationsrollen mit geeigneten Mitarbeitern besetzt (Aktivität 2.2).

607 Vgl. im Folgenden auch Kapitel 6.3.3.
608 Vgl. im Folgenden auch Kapitel 6.3.3.

Phase 3: Rollendefinition

Ziel der Phase „Rollendefinition“ ist es, eine Spezifikation der zu implementierenden Rollen festzulegen. Vor der eigentlichen Definition der Rollen müssen ggf. die Ressourcen, die zu Rollen zu bündeln sind, inventarisiert und bereinigt werden (Aktivität 3.1). Die eigentliche Spezifikation der Rolle beginnt mit der Grobspezifikation der Rollen (Aktivität 3.2). Hierzu wird für jede Rolle festgelegt, welche Mitarbeiter mit der Rolle arbeiten. Darüber hinaus gilt es, die wesentlichen Ressourcen, die eine Rolle umfasst, vorläufig festzulegen. Anschliessend wird die ermittelte Grobspezifikation verfeinert und abgeschlossen (Aktivität 3.3). Bei der Feinspezifikation muss insbesondere überprüft werden, ob die Mitarbeiter, die einer Rolle zugeordnet sind, tatsächlich auf alle Ressourcen der Rolle zugreifen dürfen.

Phase 4: Rollenimplementierung

In der Phase „Rollenimplementierung“ werden die definierten Rollen getestet und implementiert. Vor der Implementierung der Rollen empfiehlt es sich, diese zu pilotieren (Aktivität 4.1). Im Rahmen der eigentlichen Rollenimplementierung erfolgt die Einführung der entwickelten Rollen in die Produktion (Aktivität 4.2). Um die Administration weitestgehend zu automatisieren, bietet sich die Spezifikation von Regeln an, welche die automatisierte Pflege der Berechtigungen unterstützen.

7.3.4 Bewertung des konsolidierten Vorgehensmodells

Das aus den vorangegangenen Abschnitten resultierende Vorgehensmodell erhebt Anspruch auf Allgemeingültigkeit und strebt darüber hinaus Empfehlungscharakter an.[609] Im Folgenden wird dargelegt, inwiefern das zu detaillierende Vorgehensmodell diesen beiden Aspekten gerecht wird.

Die Identifikation von Strukturanalogien bildet wiederum die Grundlage, um der Forderung nach *Allgemeingültigkeit* gerecht zu werden.[610] Beide Fallstudien weisen zahlreiche Gemeinsamkeiten auf. Sie umfassen neben den Aktivitäten zur Definition und Implementierung der Rollen elementare Aktivitäten z.B. zur Bestimmung von Verantwortlichkeiten oder zur initialen Strukturierung des Entwicklungsprozesses. Das in den Fallstudien gewählte Vorgehen ergibt sich zwangsläufig bzw. unterliegt logischer Stringenz: Vor der eigentlichen Implementierung der Rollen müssen diese spezifiziert werden. Vor der Spezifikation gilt es, grundlegende Aspekte wie Verantwortlichkeiten und elementare Lösungsansätze für die eigentliche Rollendefinition und -implementierung festzulegen. Die Gemeinsamkeiten der Fallstudien lassen

609 Zum Anspruch der Arbeit vgl. Kapitel 5.1.2.
610 Vgl. Schütte 1998, S. 237f; Kapitel 5.1.2.

sich demzufolge inhaltlich erklären. Damit liegen semantikbehaftete Strukturanalogien vor, die den Anspruch der konsolidierten Vorgehensweise auf Allgemeingültigkeit rechtfertigen.[611]

Der *Empfehlungscharakter* des zu detaillierenden Methodenbausteins kann nur eingeschränkt sichergestellt und nachgewiesen werden.[612] Die hierzu ermittelten Anforderungen[613] werden durch das induktiv abgeleitete Vorgehensmodell wie folgt adressiert:

- Einbezug existierender Leitlinien und Vorgaben: Im Rahmen des abgeleiteten Vorgehensmodells werden existierende Leitlinien und Vorgaben durch die Aktivität „Rollenfeinspezifikationen festlegen“ innerhalb der Rollendefinition berücksichtigt. Auch bei der Definition der Administrationsrollen innerhalb der Phase „Vorstudie Organisation“ werden existierende Regelungen beachtet.

- Durchführung einer Risikoanalyse: Die Identifikation und Bewertung von Risiken ist Gegenstand der Risikoanalyse.[614] Das induzierte Vorgehensmodell greift diese Aspekte innerhalb der Aktivität „Rollenfeinspezifikationen festlegen“ durch eine entsprechende Schwachstellenanalyse auf. Diese stellt fest, ob die Mitarbeiter, die einer Rolle zugewiesen sind, unter Berücksichtigung des bestimmten Schutzbedarfs auf die der Rolle zugeordneten Berechtigungen zugreifen dürfen.

- Ableitung angemessener Massnahmen: Schwachstellen müssen entsprechend ihres Risikos adressiert werden.[615] Die Aktivitäten der Phase „Rollendefinition“ berücksichtigen diese Anforderung: Berechtigungen, mit denen keine oder lediglich geringe Risiken einhergehen, können freizügig zugewiesen werden. Berechtigungen, die erhebliche Risiken bergen, werden restriktiv auf der Basis der Schwachstellenanalyse vergeben.

- Definition von Leitlinien: Diese optionale Anforderung[616] ist insbesondere im Rahmen der Spezifikation der Administrationsrollen von Bedeutung. Die Festlegung von Aufgaben, Kompetenzen und Verantwortlichkeiten innerhalb der Phase „Vorstudie Organisation“, die das Handlungsumfeld der beteiligten Administratoren bestimmen, entspricht dieser Anforderung.

Das induzierte Vorgehensmodell adressiert folglich die erarbeiteten Anforderungen. Eine angemessene Berücksichtigung der Anforderung innerhalb der Entwicklung der einzelnen Aktivitäten stellt den Empfehlungscharakter der Vorgehensweise sicher.

611 Vgl. Kapitel 5.1.2.
612 Vgl. im Folgenden Kapitel 5.1.2.
613 Vgl. Kapitel 5.2.
614 Vgl. Kapitel 2.4.
615 Vgl. Kapitel 2.4.
616 Vgl. Kapitel 5.2.

7.4 Aktivitäten

Im Folgenden wird das Vorgehen zur Erstellung der Ergebnisse detaillierter dargestellt. Das Vorgehen wird dabei analog zum Methodenbaustein „Autorisierungsarchitektur“ in Aktivitäten und nicht in Techniken zerlegt. Diese Entscheidung lässt sich wiederum auf die Wahl des geeigneten Abstraktionsgrades zurückführen.[617]

7.4.1 Aktivitäten der Phase „Vorstudie System“

7.4.1.1 Grundlegendes Lösungskonzept ausarbeiten

Ziel dieser Aktivität ist es, grundlegende Lösungskonzepte zu erarbeiten, die aufzeigen, wie die Organisation eines Unternehmens mittels technischer Strukturen abgebildet werden kann. Typisches Ergebnis dieser Aktivität sind Modelle, die die Zusammenhänge zwischen Aufbau- und Ablauforganisation auf der einen und den Berechtigungen auf Daten und Funktionen der Applikationen und Systeme auf der anderen Seite darstellen.[618] Mit dieser Aktivität geht die Definition von Begrifflichkeiten zur Schaffung eines einheitlichen Sprachverständnisses einher.

In einem ersten Schritt müssen die wesentlichen Elemente der Aufbauorganisation erfasst werden. Entitäten wie z.B. Person, Stelle und Organisationseinheit sind analog zum entwickelten Metamodell „Aufbauorganisation“[619] zu identifizieren, zu definieren und in Beziehung zu setzen. Von besonderer Bedeutung ist hierbei die Unterscheidung zwischen primären, dauerhaften Organisationseinheiten und sekundären Organisationseinheiten der Projektorganisation, da sich die Verwaltung der primären und sekundären Organisationseinheiten stark unterscheidet. Während die primären Organisationseinheiten mit ihren Mitarbeitern in der Regel zentral in den HR-Systemen gepflegt werden, erfolgt die Administration der Projekte mit ihren Projektmitgliedern in speziell hierfür vorgesehenen Werkzeugen eher dezentral, teilweise ohne explizit hierfür vorgesehene Systeme.[620]

In einem zweiten Schritt müssen die Ablauforganisation und ihre Beziehungen zur Aufbauorganisation analog zum Metamodell „Ablauforganisation“ [621] dargestellt werden. Zentrale Herausforderung ist es, die Entitäten der Ablauforganisation von den Entitäten der Aufbauorganisation abzugrenzen. Während die Zerlegung der Ablauforganisation in die zentralen Entitäten Prozess und Aktivität noch auf der Hand liegt, ist insbesondere die definitorische Abgrenzung von Prozessrolle und Stelle von zentraler Bedeutung. In den Fallstudien wurden beide Begriffe zum Teil synonym verwendet, was zu Missverständnissen führte. Beide Begriffe bezeich-

617 Vgl. Kapitel 6.4.
618 Vgl. hierzu insbesondere Fallstudie GENERALI, Kapitel 4.4.
619 Vgl. Kapitel 5.3.2.
620 Diese Aussage basiert auf den erhobenen Fallstudien, vgl. Kapitel 4.
621 Vgl. Kapitel 5.3.3.

nen eine Bündelung von Aktivitäten. Der Begriff „Stelle“ betont jedoch die aufbauorganisatorische Bündelung von Aktivitäten: „Eine Stelle [wie z.B. „Sachbearbeiter Schaden“] bezeichnet eine Zusammenfassung von Aufgaben, die eine derartige Kapazitätsnachfrage bilden, dass sie einer Person übertragen werden können und diese dauerhaft bei definierter, im Regelfall kontinuierlicher Arbeitszeit auslasten.“[622] Eine Prozessrolle wie z.B. „Verantwortlicher Schaden Lebensversicherung“ stellt hingegen eine ablauforganisatorische Bündelung von Aktivitäten dar.[623]

Abschliessend gilt es, die erstellten Modelle analog zum Metamodell „Integration der Autorisierung“[624] in Zusammenhang zu den Daten und Funktionen der Applikationen und Systeme zu bringen. Um die wesentlichen Elemente der Applikationen und Systeme, die im Kontext der Vergabe von Berechtigungen relevant sind, abzubilden und zu definieren, bietet sich die Berücksichtigung etablierter Standards wie RBAC und ERBAC an.[625] Diese definieren Entitäten wie Nutzer, Rolle, Recht und deren Beziehungen. Einen direkten Bezug zur Ablauforganisation stellen diese Standards jedoch nicht her. Problematisch ist auch der Begriff „Rolle“. Im Gegensatz zur Prozessrolle der Ablauforganisation stellt eine Rolle im Kontext der erwähnten Standards eine Bündelung von Berechtigungen dar. Um Missverständnisse zu vermeiden, sollten durch die Verwendung unterschiedlicher, klar definierter Begrifflichkeiten wie z.B. „Prozessrolle“ und „Rolle“ Synonyme vermieden werden.

7.4.1.2 Rollenkonzept definieren

Ziel der Aktivität „Rollenkonzept definieren“ ist es, so genannte Rollenklassen zu identifizieren. Durch die Definition der Rollenklassen erfolgt eine Strukturierung des Rollendefinitions- und -implementierungsprozesses. Jede zu definierende Rolle muss genau einer Rollenklasse entsprechen. In der Praxis werden die Rollenklassen synonym auch als Rollenkategorien oder Rollentypen bezeichnet. Abschliessend werden grundlegende Beziehungen zwischen den Rollen der unterschiedlichen Klassen definiert.

Bei der Zusammenfassung von Berechtigungen zu Rollen wird grundsätzlich zwischen Rollen für interne und für externe Mitarbeiter unterschieden.[626] Im Rahmen der Fallstudien zeigt sich darüber hinaus eine weitere Unterteilung der Rollen, die an interne Mitarbeiter vergeben werden: Unterschieden werden die Rollen, die die Berechtigungen der primären, dauerhaften Organisation strukturieren und jene Rollen, die die Berechtigungen der Projektorganisation umfassen. Die Rollen, die die primäre Organisation adressieren, orientieren sich an „natürlichen“ Organisationsstrukturen wie z.B. Kostenstellen, Abteilungen oder auch Standorten.[627] Die

622 Vgl. Rosemann/zur Mühlen 1997, S. 101.
623 Vgl. Rosemann/zur Mühlen 1997, S. 101.
624 Vgl. Kapitel 7.2.
625 Vgl. Kapitel 2.3.
626 Vgl. im Folgenden insbesondere Fallstudie GENERALI, Kapitel 4.4.
627 Vgl. im Folgenden Kern et al. 2002, S. 48.

Rollen, die die sekundäre Organisation adressieren, entsprechen den einzelnen Projekten eines Unternehmens.

Um die Rollen, die die primäre Organisation adressieren, zu definieren, empfiehlt es sich, Organisationsstrukturen als Grundlage zu wählen, die relativ konstant sind.[628] Strukturen, die sich z.B. durch eine Reorganisation fundamental verändern, ziehen einen erhöhten Pflegeaufwand nach sich. Tabelle 48 fasst in der Praxis verwendete Rollenklassen für die primäre Organisation zusammen.

Unternehmen	Rollenklasse	Beschreibung
Basler Versicherung[629]	Default-Rollen	„Default-Rollen" enthalten grundlegende Rechte für alle Mitarbeiter.
	Abteilungs-Rollen	„Abteilungs-Rollen" enthalten die elementaren Berechtigungen für alle Mitarbeiter einer Abteilung.
	Standard-Rollen	„Standard-Rollen" enthalten die Berechtigungen, die ausgewählte Mitarbeiter einer Abteilung benötigen.
	Spezial-Rollen	„Spezial-Rollen" enthalten ausgewählte, besonders kritische Berechtigungen.
GENERALI[630]	Beginner	Rollen der Klasse „Beginner" enthalten die grundlegenden Berechtigungen eines Bereiches.
	Intermediate	Rollen der Klasse „Intermediate" umfassen im Vergleich zu einer Rolle der Klasse „Beginner" zusätzliche Berechtigungen.
	Experte	Spezialisten eines Bereiches bekommen eine „Expert"-Rolle zugewiesen.
	Manager	Leitenden Mitarbeitern wird eine Rolle der Klasse „Manager" zugeordnet.
Siemens[631]	Basisrollen	„Basisrollen" enthalten grundlegende Berechtigungen für interne und externe Mitarbeiter.
	Organisatorische Rollen	„Organisatorische Rollen" orientieren sich an den Abteilungen des Unternehmens.
	Hierarchische Rollen	„Hierarchische Rollen" berücksichtigen die hierarchischen Strukturen im Unternehmen.
	Funktionale Rollen	„Funktionale Rollen" orientieren sich an den durchzuführenden Tätigkeiten der Mitarbeiter.

Tabelle 48: Rollenklassen in der Praxis

Neben den Rollenklassen müssen auch die grundlegenden Beziehungen zwischen den Rollen der Klassen festgelegt werden. Grundsätzlich erlauben Autorisierungsstandards die Vererbung von Berechtigungen.[632] Die Vererbung verspricht einen reduzierten Administrationsaufwand, so dass beispielsweise die GENERALI von diesem Konzept Gebrauch macht.[633] Ein Nachteil stellt hingegen die Komplexität dar, die mit wachsenden Vererbungshierarchien einhergeht. Im Rahmen der Aktivität ist somit festzulegen, ob eine Vererbung von Berechtigungen praktiziert werden soll. Je nach definierten Rollenklassen ist dann festzulegen, wie viele Verer-

628 Vgl. im Folgenden Kern et al. 2002, S. 48.
629 Vgl. Fallstudie Basler Versicherungen, Kapitel 4.3.
630 Vgl. Fallstudie Basler GENERALI, Kapitel 4.4.
631 Vgl. Roeckle et al. 2000, S. 105f.
632 Vgl. Kapitel 2.3.
633 Vgl. Fallstudie GENERALI, Kapitel 4.4.

bungsstufen erwünscht sind und wie die Rollen der unterschiedlichen Klassen miteinander in Beziehung stehen.[634]

7.4.2 Aktivitäten der Phase „Vorstudie Organisation“

7.4.2.1 Aufgaben, Kompetenzen und Verantwortlichkeiten definieren

Ziel dieser Aktivität ist es, die Aufgaben, Kompetenzen und Verantwortlichkeiten bei der Definition und Pflege der Berechtigungen zu Administrationsrollen zusammenzufassen. Hierzu müssen zuerst die notwendigen Aufgaben identifiziert werden, die im Rahmen von Definition und Pflege durchzuführen sind. Schliesslich müssen die Aufgaben zu Administrationsrollen gebündelt und mit Kompetenzen und Verantwortlichkeiten versehen werden. Hierbei ist die Berücksichtigung regulatorischer Anforderungen besonders wichtig.

Die Identifikation der Aufgaben beinhaltet die Definition der wesentlichen Aufgabenkomplexe, die im Rahmen der Administrationsprozesse durchzuführen sind. Um eine vollständige Identifikation zu gewährleisten, bietet sich das Metamodell „Integration der Autorisierung“[635] mit seinen Kernentitäten „Benutzerkonto“, „Rolle“ und „Ressource“ als Ausgangspunkt und Strukturierungsraster an. Folgende Aufgabenkomplexe können auf der Basis des Metamodells identifiziert werden:

- Definition und Pflege der Ressourcen: Die Definition und Pflege der Ressourcen umfassen das Anlegen, Löschen sowie die Modifikation von Ressourcen. Das Anlegen und die Modifikation von Ressourcen beinhalten die Bündelung von feingranularen Berechtigungen zu Ressourcen.

- Definition und Pflege der Rollen: Die Definition und Pflege der Rollen umfassen das Anlegen, Löschen sowie die Modifikation von Rollen. Das Anlegen und die Modifikation von Rollen beinhaltet einerseits die Zusammenfassung von Ressourcen zu Rollen. Andererseits muss festgelegt werden, welche Mitarbeiter einer Rolle zugewiesen werden.

- Definition und Pflege der Benutzerkonten: Die Definition und Pflege der Benutzerkonten umfassen das Anlegen, Löschen sowie die Modifikation von Nutzerinformationen. Von besonderer Bedeutung ist hierbei die Zuweisung der Benutzerkonten zu Rollen, die entsprechend der Rollendefinitionen erfolgen muss.

Die Bündelung der einzelnen Aktivitäten zu Administrationsrollen und auch die Zuweisung der Administrationsrollen zu Mitarbeitern können nicht beliebig gestaltet werden. Interne und externe Anforderungen müssen bei der Zusammenstellung identifiziert und ggf. gewichtet

634 Vgl. hierzu auch Fallstudie GENERALI, Kapitel 4.4.
635 Vgl. Kapitel 7.2.

werden.[636] Hierbei spielen wiederum existierende Sicherheitsstandards eine massgebliche Rolle.[637] Auf der Basis der vorgestellten Sicherheitsstandards lassen sich u.a. folgende wesentliche Anforderungen ermitteln:

- Schaffung klarer Verantwortlichkeiten:[638] Für die einzelnen Ressourcen, Rollen und Nutzer gilt es, Verantwortliche zu definieren. In der Fallstudie Basler Versicherungen ist beispielsweise jede Ressource und Rolle einem „Ressource Owner“ bzw. „Rollen Owner“ zugeordnet. Diese sind für die korrekte Spezifikation und Pflege der Ressourcen und Rollen verantwortlich und entscheiden darüber hinaus über deren Verwendung.

- Einbezug des Fachbereiches:[639] Die Zugriffsberechtigungen müssen den Mitarbeitern entsprechend ihrer geschäftlichen Tätigkeit zugeordnet werden. Daher hat es sich bewährt, Vertreter aus den jeweiligen Fachabteilungen als Rollen- und Ressourcenverantwortliche zu ernennen, die die mit der Rolle bzw. Ressource verknüpften Teilprozesse genau kennen.[640]

- Einbezug der Systemverantwortlichen:[641] Bei der Vergabe der Berechtigungen ist sicherzustellen, dass die Systemverantwortlichen in den Prozess involviert sind. Im Rahmen der Fallstudie Basler Versicherungen ist ein „Ressourcen Owner“ beispielsweise ein Systemverantwortlicher des Fachbereiches, der die Ressourcen „seiner“ Systeme betreut.[642] Dadurch, dass er bei der Zuweisung von Ressourcen zu Rollen seine Zustimmung erteilen muss, kann er den Zugriff auf „seine“ Systeme steuern.

- Aufgabentrennung:[643] Um den Missbrauch von Befugnissen zu vermeiden, ist auch bei der Administration von Berechtigungen eine angemessene Trennung von Kompetenzen und Aufgaben sicherzustellen. Insbesondere muss verhindert werden, dass das Anlegen von Ressourcen und Rollen sowie die Zuweisung von Rollen zu Nutzern lediglich von einer einzigen Person durchgeführt wird.[644]

Unter der Berücksichtigung der Anforderungen sind die Aufgaben zu Administrationsrollen zu bündeln. Mit der Zuweisung von Kompetenzen und Verantwortlichkeiten wird die Administrationsrollendefinition abgeschlossen. Tabelle 8 zeigt beispielhaft eine Administrationsrollendefinition,[645] wie sie in der Fallstudie Basler Versicherungen zu finden ist.

636 Vgl. hierzu auch Kapitel 6.4.1.3.
637 Vgl. Kapitel 5.2
638 Vgl. ISO 2000a, Kapitel 5.
639 Vgl. ISO 2000a, Kapitel 9.1.
640 Vgl. Hartje et al. 2003, S. 176; Fallstudie Basler Versicherungen, Kapitel 4.3.
641 Vgl. ISO 2000a, Kapitel 9.2.
642 Vgl. Fallstudie Basler Versicherungen, Kapitel 4.3.
643 Vgl. ISO 2000a, Kapitel 9.2.
644 Vgl. Hartje et al. 2003, S. 208ff.
645 Vgl. Fallstudie Basler Versicherungen, Kapitel 4.3.

7.4.2.2 Verantwortliche bestimmen

Zielsetzung der Aktivität „Verantwortliche bestimmen“ ist es, die Administrationsrollen mit geeigneten Mitarbeitern zu besetzen. Dabei muss ggf. eine Schulung der Mitarbeiter stattfinden, um eine adäquate Wahrnehmung der Administrationsrollen sicherzustellen. Bei der Besetzung der Rollen kommt der Herkunft der Mitarbeiter eine besondere Bedeutung zu. Es ist zu entscheiden, inwieweit die Definition und Pflege der Rollen und Ressourcen eigenständig durch die Mitarbeiter des Fachbereiches durchgeführt werden soll.

Bei der Einbindung des Fachbereiches in die Administration können zwei unterschiedliche Ansätze unterschieden werden. Eine starke Einbindung des Fachbereiches umfasst die Besetzung der Administrationsrollen zur Definition und Pflege von Rollen und Ressourcen mit Mitarbeitern des Fachbereiches. In der Fallstudie Basler Versicherungen werden beispielsweise die Rollen durch Vertreter der einzelnen Fachbereichsabteilungen definiert:[646] Nicht eine zentrale IT-Abteilung definiert die unterschiedlichen Rollen, sondern eine Vielzahl ausgewählter Fachvertreter führt diese Aktivität für ihren Verantwortungsbereich aus. Der IT kommt somit lediglich eine unterstützende Funktion bei der Definition und Pflege der Rollen zu.

Starke Einbindung des Fachbereiches
Anwendungsbereiche
• Fachbereich besitzt die Bereitschaft, sich an der Administration massgeblich zu beteiligen • Fachbereich besitzt das technische Basiswissen zur Pflege von Rollen und Ressourcen
Vorteile
• Mitarbeiter des Fachbereiches kennen die Geschäftsprozesse und die Mitarbeiter, die diese durchführen • Bessere Akzeptanz und kontiunierliche Pflege der Rollen und Ressourcen seitens der Mitarbeiter
Nachteile
• Mitarbeitern des Fachbereiches fehlt ggf. das technische Basiswissen • Mitarbeiter des Fachbereiches erkennen nicht die Bedeutung der Definition und Pflege der Rollen und Ressourcen

Tabelle 49: Administration bei starker Einbindung des Fachbereiches

Die Vorteile der starken Einbindung des Fachbereiches liegen vor allem im Wissen der Mitarbeiter des Fachbereiches um die Geschäftsprozesse und die daran beteiligten Akteure. Darüber hinaus sind durch die starke Einbindung des Fachbereiches die Akzeptanz und die kontinuierliche Pflege der Rollen und Ressourcen in wesentlich höherem Masse gewährleistet, als wenn die Administration ausschliesslich von der IT verantwortet wird. Nachteilig ist jedoch, dass die Mitarbeiter des Fachbereiches ggf. nicht über das technische Basiswissen verfügen, das zur Administration der Systeme notwendig ist. Darüber hinaus müssen sie über die Be-

646 Vgl. Fallstudie Basler Versicherungen, Kapitel 4.3.

reitschaft verfügen, sich mit derart technischen Tätigkeiten auseinanderzusetzen. Eine starke Einbindung des Fachbereiches in die Administration bietet sich daher insbesondere dann an, wenn die Bereitschaft des Fachbereiches für derartige Tätigkeiten und das notwenige technische Grundverständnis vorhanden sind. Tabelle 49 fasst Anwendungsbereiche sowie Vor- und Nachteile des diskutierten Ansatzes zusammen.

Geringe Einbindung des Fachbereiches
Anwendungsbereiche
• Fachbereich besitzt nicht die Bereitschaft sich an der Administration massgeblich zu beteiligen • Fachbereich besitzt nicht das technische Basiswissen oder die konzeptionellen Fähigkeiten zur Definition und Pflege von Rollen und Ressourcen
Vorteile
• Mitarbeiter der IT kennen die Systeme • Mitarbeiter der IT sind in konzeptionellen Tätigkeiten wie der Spezifikation von Berechtigungen geschult
Nachteile
• Mitarbeiter der IT haben geringeres Wissen über die Geschäftsprozesse als die Mitarbeiter des Fachbereiches • Geringe Akzeptanz der entwickelten Rollen bei den Mitarbeitern des Fachbereiches • Kontinuierliche Pflege der Rollen und Ressourcen ist lediglich eingeschränkt gegeben

Tabelle 50: Administration bei geringer Einbindung des Fachbereiches

Die Vorteile des Ansatzes, der dem Fachbereich lediglich eine unterstützende Funktion bei der Administration zuordnet, liegen insbesondere darin, dass die Mitarbeiter der IT in konzeptionellen Tätigkeiten wie der Spezifikation von Rollen und Ressourcen geschult sind und über ein fundiertes technisches Wissen über die zu administrierenden Systeme verfügen. Die Mitarbeiter der IT verfügen jedoch über ein geringeres Geschäftsprozesswissen als ihre Kollegen im Fachbereich. Darüber hinaus zeigt sich durch die erhobenen Fallstudien, dass bei geringer Beteiligung des Fachbereiches die kontinuierliche Pflege der Berechtigungen nur eingeschränkt durchgeführt wird.[647] Tabelle 50 fasst überblicksartig die Eigenschaften des diskutierten Ansatzes zusammen.

Insbesondere die Mitarbeiter des Fachbereiches, die mit Administrationsaufgaben betraut werden und über keinerlei Erfahrungen in diesem Umfeld verfügen, sind angemessen zu schulen. Die Mitarbeiter müssen die Bedeutung der Administration für die Sicherheit der Informationssysteme verstehen und ihre persönliche Verantwortung erkennen und annehmen.[648] Darüber hinaus müssen sie über das notwendige Wissen verfügen, um eine adäquate, risikogesteuerte Vergabe von Berechtigungen zu gewährleisten.

647 Vgl. hierzu insbesondere Kapitel 4.3 und 4.4.
648 Vgl. im Folgenden Petruch 2002, S. 284.

7.4.3 Aktivitäten der Phase „Rollendefinition“

7.4.3.1 Ressourcen bereinigen und inventarisieren

Diese Aktivität hat zum Ziel, die Qualität der bestehenden Ressourcen sicherzustellen sowie diese in einem zentralen Repository zu dokumentieren. Aufgrund der Vielzahl der Ressourcen bietet sich die Verwendung eines speziellen Werkzeuges zur Inventarisierung an. Dies kann eine ausdrücklich hierfür entwickelte Anwendung (vgl. Fallstudie Basler Versicherungen[649]) oder ein auf dem Markt verfügbares Werkzeug sein (vgl. Fallstudie GENERALI[650]).

Um die Qualität der vergebenen Ressourcen zu sichern, sind in Anlehnung an HELFERT folgende Aspekte zu berücksichtigen:[651]

- Glaubwürdigkeit: Die Ressourcen sind in Absprache mit dem Fachbereich auf ihre Korrektheit hin zu prüfen. Für die jeweiligen Ressourcen sind darüber hinaus die Verantwortlichkeiten zu definieren. Es ist ferner darauf zu achten, dass die Ressourcen entsprechend den anzuwendenden Berechtigungsschemata spezifiziert sind.

- Zeitlicher Bezug: Die Ressourcen müssen auf das aktuelle Tätigkeitsumfeld der Mitarbeiter abgestimmt sein. In Abhängigkeit rechtlicher und interner Anforderungen ist sicherzustellen, dass eine Historie über die vergebenen Ressourcen geführt wird.

- Nützlichkeit: Es ist zu überprüfen, inwieweit die spezifizierten Ressourcen tatsächlich notwendig sind. Entsprechend der Ansätze des Sicherheitsmanagements sind Berechtigungen und damit auch Ressourcen ein Mittel zur Risikobewältigung, das aus Gründen der Wirtschaftlichkeit nur dann eingesetzt werden sollte, wenn ein entsprechendes Risiko vorliegt.[652]

- Verfügbarkeit: Die Zugriffsrechte zur Administration der Berechtigungen und Ressourcen sind ebenfalls in die Analyse einzubeziehen, um auch ihre kontinuierliche Pflege sicherzustellen. Darüber hinaus ist die Systemverfügbarkeit der Autorisierungskomponenten zu gewährleisten.

In den Fallstudien hat sich insbesondere die Auszeichnung der Ressourcen mit einem Kurztext und einer sprechenden Bezeichnung bewährt.[653] Einzelne, feingranulare Berechtigungen, die den Mitarbeitern nicht direkt zugewiesen sind, wurden aus Wirtschaftlichkeitsgründen im Rahmen der erhobenen Fallstudien nicht weiter dokumentiert. Tabelle 51 zeigt exemplarisch eine dokumentierte Ressource.

---

649 Vgl. Fallstudie Basler Versicherungen, Kapitel 4.3.
650 Vgl. Fallstudie GENERALI, Kapitel 4.4.
651 Vgl. Helfert 2002, S. 84.
652 Vgl. Kapitel 2.4.4.
653 Vgl. im Folgenden insbesondere Fallstudie Basler Versicherungen, Kapitel 4.3.

Attribut	Wert
ID	SchadenVollSG
Kurztext	Vollzugriff Schaden Agentur St. Gallen
System	Schadenmanagement
Owner	Herr Müller, Abteilung Schaden
Bezeichnung	Zugriff auf die Schäden der Agentur St. Gallen. …

Tabelle 51: Dokumentierte Ressource (Beispiel)

7.4.3.2 Rollengrobspezifikationen festlegen

Ziel der Aktivität ist es, eine Grobspezifikation der zu implementierenden Rollen zu ermitteln. Hierzu wird für jede Rolle festgelegt, welche Mitarbeiter mit der Rolle arbeiten. Darüber hinaus werden die wesentlichen Ressourcen, die eine Rolle umfasst, erhoben. Die Definition der Rollen erfolgt auf Basis der Top-Down- oder Bottom-Up-Vorgehensweise.

Bei der Top-Down-Vorgehensweise bilden Organisation und Prozesse den Ausgangspunkt der Rollendefinition.[654] Für jede Organisationseinheit müssen in einem ersten Schritt die Aktivitäten identifiziert werden, die durch Informationssysteme unterstützt werden. Die Aktivitäten sind zu Komplexen zu bündeln, die von einer Gruppe von Personen ausgeführt werden. Hierzu können existierende Prozessdefinitionen oder Stellenbeschreibungen herangezogen werden. Die Berechtigungen, die im Rahmen der Aktivitätskomplexe von den Mitarbeitern benötigt werden, werden dann zu Rollen zusammengefasst.

In den Fallstudien zeigt sich, dass die Definition von Rollen nur sehr eingeschränkt auf aufbauorganisatorischen Elementen wie z.B. Stellen basiert.[655] In den einzelnen Organisationseinheiten existieren vielmehr eine Vielzahl von informellen, nicht dokumentierten Stellvertretungen und ablauforganisatorischen Aufgaben- und Kompetenzverteilungen, die zu berücksichtigen sind.

Die Vorteile der Top-Down-Rollendefinition liegen in der strukturierten, zielgerichteten Vorgehensweise, die die Rollen entsprechend der Prozesse und der Organisation festlegt. Falls im Ableitungsprozess Sicherheitsanforderungen und -risiken berücksichtigt werden, so wird die Definition den Ansprüchen des Sicherheitsmanagements[656] gerecht. Die Top-Down-Vorgehensweise ist jedoch sehr zeitaufwendig und damit sehr kostenintensiv.[657] Zudem existieren in einer Unternehmung in der Regel bereits Berechtigungen, die als Ausgangspunkt zur Rollendefinition verwendet werden können. Ist die Qualität der existierenden Berechtigungen mangelhaft, so bildet die Top-Down-Rollendefinition die einzige Möglichkeit, adäquate Rol-

654 Vgl. im Folgenden Roeckle et al. 2000, S. 107.
655 Vgl. im Folgenden Kapitel 4.3 und 4.4.
656 Vgl. Kapitel 5.2.
657 Vgl. im Folgenden Kuhlmann et al. 2003, S. 185.

lendefinitionen zu ermitteln. Tabelle 52 fasst Anwendungsbereiche sowie Vor- und Nachteile der Top-Down-Vorgehensweise zusammen.

Top-Down-Rollendefinition
Anwendungsbereiche
• Geringe Qualität der vergebenen Berechtigungen • Zugriffsberechtigungen sollen mit den Prozessen und der Organisation im Einklang stehen
Vorteile
• Zugriffsberechtigungen sind im Einklang mit Organisationsstrukturen und Prozessen • Zugriffsberechtigungen sind im Einklang mit Sicherheitsanforderungen und -risiken
Nachteile
• Keine direkte Berücksichtigung bereits vorhandener Berechtigungen • Zeit- und kostenintensive Vorgehensweise zur Rollendefinition

Tabelle 52: Charakteristika der Top-Down-Rollendefinition

Die Bottom-Up-Rollendefinition stellt eine Alternative zur Top-Down-Vorgehensweise dar. Hier bilden vorhandene Rechtedefinitionen den Ausgangspunkt der Definition. Durch die Suche nach Mustern in den vorhandenen Zugriffskontrolldaten werden Berechtigungen zu Rollen zusammengefasst.

Bottom-Up-Rollendefinition
Anwendungsbereiche
• Hohe Qualität der existierenden Berechtigungen • Erstellung von vorläufigen Rollendefinitionen, die im Anschluss validiert und angepasst werden
Vorteile
• Bestehende Berechtigungen dienen als Ausgangspunkt der Rollendefinition • Zeitaufwand zur Ableitung der Rollen gering • Kostengünstige Vorgehensweise zur Rollendefinition
Nachteile
• Qualität der abgeleiteten Rollen hängt von der Qualität der bereits vergebenen Berechtigungen ab • Keine unmittelbare Berücksichtigung von Organisationsstrukturen und Prozessen • Keine unmittelbare Berücksichtigung von Sicherheitsanforderungen und -risiken

Tabelle 53: Charakteristika der Bottom-Up-Rollendefinition

Der Vorteil dieses Ansatzes liegt in der Nutzung bereits bestehender Daten zur automatisierten Ableitung von Rollen.[658] Dies kann den Rollendefinitionsprozess erheblich beschleunigen. Bei mangelnder Qualität der existierenden Berechtigungen ist jedoch eine automatisierte Bündelung der Berechtigungen zu Rollen nicht sinnvoll. Da von den existierenden Berechtigungen ausgegangen wird, stellt das Ergebnis der Bottom-Up-Rollendefinition eine Konsoli-

658 Vgl. im Folgenden Kuhlmann et al. 2003, S. 184f.

dierung der Ist-Situation dar. Ob die ermittelten Rollen im Einklang mit den Organisationsstrukturen und Prozessen sowie den Sicherheitsanforderungen und -risiken stehen, gilt es im weiteren Verlauf der Rollendefinition erst zu klären. Tabelle 53 zeigt Anwendungsbereiche sowie Vor- und Nachteile der Bottom-Up-Vorgehensweise im Überblick.

Idealerweise sollte die Ableitung der Rollen sowohl Bottom-Up als auch Top-Down durchgeführt werden.[659] Im Rahmen der Fallstudien stellen Organisation und Prozesse den Ausgangspunkt der Rollendefinition dar. Eine Überarbeitung und Anpassung der initialen Rollendefinitionen erfolgt anschliessend auf der Basis existierender Berechtigungen.

Tabelle 54 zeigt exemplarisch die Grobspezifikation einer Rolle. Zu den Basisinformationen, die für eine Rolle festzuhalten sind, gehören u.a. die technische Bezeichnung, der Einsatzbereich, die textuelle Beschreibung der Rolle sowie der für die Rolle verantwortliche Mitarbeiter. Ebenfalls zu spezifizieren sind die Mitarbeiter, denen die Rolle im Betrieb zugewiesen wird. Abschliessend ist festzuhalten, welche wesentlichen Ressourcen eine Rolle umfasst. Die entsprechenden Ressourcen können mit ihrem technischen Bezeichner referenziert oder textuell beschrieben werden.

Rolle: Mitarbeiter Schaden			
Basisdaten			
Technische ID:	MSchaden		
Einsatzbereich:	Abteilung Schaden		
Beschreibung:	Die Rolle enthält die Berechtigungen, die jeder Mitarbeiter der Abteilung Schaden benötigt.		
Owner:	Hans Müller		
Zuordnung Mitarbeiter			
Relevant für:	Alle Mitarbeiter der Abteilung Schaden		
Ausschluss:	-		
Vorläufige Zuordnung Ressourcen			
Applikation	System	Ressource	Bemerkung
Applikation A	System 1	AGDWXXWS	Modell
	System 2	LLNV AGD	Kompetenz
Applikation B	System 3	PADU 0001	Profil
…	…	…	…

Tabelle 54: Grobspezifikation einer Rolle (Beispiel)

7.4.3.3 Rollenfeinspezifikationen festlegen

Die Aktivität „Rollenfeinspezifikationen festlegen“ hat zum Ziel, den Rollen die notwendigen Ressourcen zuzuordnen und somit die bereits ermittelte Grobspezifikation zu verfeinern und

[659] Vgl. Kern et al. 2002, S. 48.

abzuschliessen. Im Rahmen der Spezifikation muss überprüft werden, ob die Mitarbeiter, die einer Rolle zugeordnet sind, tatsächlich auf alle Ressourcen einer Rolle zugreifen dürfen.

Die Zuweisung von Ressourcen zu Rollen wird durch den Einbezug entsprechender Wissensträger abgeschlossen. Zu berücksichtigen sind hierbei insbesondere die Mitarbeiter der zentralen Benutzerverwaltung und die entsprechenden Systemverantwortlichen, die über ein umfangreiches Wissen über die Ressourcen verfügen. Bei der Zuweisung von Ressourcen zu Rollen kommt der Berücksichtigung von Sicherheits- und Datenschutzaspekten eine besondere Bedeutung zu: Im Rahmen der Zuweisung der Ressourcen zu Rollen ist der Schutzbedarf der Ressourcen unter Berücksichtigung existierender Leitlinien und Vorgaben zu bestimmen (vgl. Tabelle 55). Im Anschluss hieran ist zu prüfen, ob die Mitarbeiter einer Rolle unter Berücksichtigung des bestimmten Schutzbedarfs auf die der Rolle zugeordneten Ressourcen zugreifen dürfen.

System A		
Ressource	**Schutzbedarf**	**Begründung**
AGDWXXWS	Hoch	Ressource ermöglicht Zugriff auf Adressinformationen.
AGDWXXAK	Sehr Hoch	Ressource ermöglicht Zugriff auf Krankheitsdaten.
AGDWXXRL	Hoch	Ressource ermöglicht Zugriff auf Schäden.
…	…	…

Tabelle 55: Schutzbedarfsbestimmung der Ressourcen (Beispiel)

Da der Schutzbedarf meist nicht quantifizierbar ist, beschränkt man sich in der Praxis auf eine qualitative Aussage. Das IT-Grundschutzhandbuch unterteilt den Schutzbedarf beispielsweise in die drei Kategorien:[660]

- Niedrig bis mittel: Die Schadensauswirkungen sind begrenzt und überschaubar.
- Hoch: Die Schadensauswirkungen können beträchtlich sein.
- Sehr hoch: Die Schadensauswirkungen können ein für das Unternehmen existentiell bedrohliches, katastrophales Ausmass erreichen.

Bei der Angabe der Schutzbedarfskategorien ist es hilfreich, Schadensszenarien einzubeziehen. Die Autorisierung widmet sich primär den Sicherheitszielen Vertraulichkeit und Integrität[661] und kann daher beispielsweise auf der Basis des „Standard of Good Practice for Information Security“ anhand der folgenden Schadensszenarien beurteilt werden:[662]

660 Vgl. BSI 2004, Kapitel 2.2.
661 Vgl. Kapitel 2.3.
662 Vgl. ISF 2003, CB 1.1 und CB 1.2

Schadensszenarien	
Vertraulichkeit	Beeinträchtigung der Mitarbeitermotivation (z.B. durch mangelnde Datenqualität)
	Beeinträchtigung der Vertraulichkeit, der Marke oder der Reputation gegenüber Shareholdern oder Kunden
	Entstehung zusätzlicher Kosten (z.B. durch die Notwendigkeit Vorfälle zu untersuchen und die aufgetretenen Schäden zu beheben)
	Missbrauch von Informationen
	Verlust von Marktanteilen
	Verlust von Wettbewerbsvorteilen
	Verstoss gegen gesetzliche oder vertragliche Bestimmungen
Integrität	Behinderung von Geschäftsaktivitäten
	Verlust durch falsche (Management-) Entscheidungen

Tabelle 56: Schadensszenarien Vertraulichkeit und Integrität

Bei der Bestimmung des Schutzbedarfes sind Aspekte des Datenschutzes ebenfalls zu berücksichtigen. Schadensszenarien, die zur Bestimmung des Schutzbedarfs herangezogen werden, sind z.B. die unbefugte Weitergabe personenbezogener Daten oder die unzulässige Erhebung personenbezogener Daten.[663]

Ein weiterer wichtiger Aspekt, der bei der Definition der Rollen beachtet werden muss, ist die Funktionstrennung.[664] Die Funktionstrennung legt fest, welche Funktionen nicht miteinander vereinbar sind, also auch nicht von einer Person gleichzeitig wahrgenommen werden dürfen. Im Kontext der Rolledefinition ist somit zu prüfen, ob die Ressourcen einer Rolle auch in ihrer Gesamtheit einem Mitarbeiter zugeordnet werden dürfen.

7.4.4 Aktivitäten der Phase „Rollenimplementierung“

7.4.4.1 Rollen pilotieren

Ziel der Aktivität „Rolle pilotieren“ ist es, die definierten Rollen zu implementieren und zu testen. Dazu empfiehlt es sich, jeweils einem repräsentativen Mitarbeiter einer zu implementierenden Rolle die Ressourcen der entsprechenden Rolle zuzuteilen.[665] Treten im Test Probleme auf, muss die Rolle entsprechend modifiziert und erneut im Betrieb getestet werden.

Im Rahmen der übergeordneten Qualitätssicherung müssen Tests und Überprüfungen systematisch durchgeführt und dokumentiert werden.[666] Der Testprozess sollte in Anlehnung an

663 Vgl. BSI 2004, Kapitel 2.2.
664 Vgl. BSI 2004, M 2.5.
665 Vgl. Fallstudie Basler Versicherungen, Kapitel 4.3.
666 Vgl. Balzert 1998, S. 547.

allgemeine Konzepte aus dem Software Engineering mindestens aus drei Schritten bestehen:[667]

- Testplanung: Die Testplanung umfasst die Ermittlung der zeitlichen Testaufwände und personellen Testressourcen. Für den Test der spezifizierten Rollen muss pro Rolle wenigstens ein repräsentativer Mitarbeiter ausgewählt werden. Die jeweiligen Mitarbeiter sollten im täglichen Betrieb den Berechtigungsumfang der Rolle möglichst vollständig ausschöpfen, so dass auch im Rahmen der Tests eine ganzheitliche Überprüfung der Rolle unter alltäglichen Bedingungen gewährleistet ist. Darüber hinaus sollten die ausgewählten Tester über die Zeit und die Bereitschaft verfügen, bei der Feinabstimmung der Rollen mitzuwirken.

- Testdurchführung: In einem ersten Schritt müssen den Testern alle existierenden Berechtigungen entzogen werden, um ihnen dann die Ressourcen zuzuordnen, die ihnen aufgrund ihrer Rollenzugehörigkeiten zustehen. In den Fallstudien erfolgte der Test insbesondere durch die Ausführung alltäglicher Tätigkeiten. Spezielle Testfälle wurden nur eingeschränkt entwickelt und durchgeführt.

- Testkontrolle: Im Rahmen der Tests ist bei etwaigen Zugriffsproblemen eine schnelle Anpassung der Rollen sicherzustellen, um den störungsfreien Betrieb möglichst durchgängig zu gewährleisten. Somit ist sicherzustellen, dass die Personen, die an der Definition und Implementierung einer zu testenden Rolle beteiligt sind, während der Tests für eventuelle Rücksprachen und Eingriffe verfügbar sind.

Nach dem Abschluss der Tests beginnt die eigentliche Einführung der systemübergreifenden Rollen.

7.4.4.2 Rollen einführen

Ziel der Aktivität „Rollen einführen“ ist es, die Berechtigungen aller Mitarbeiter auf der Basis der erarbeiteten Rollen effizient zu administrieren. Hierzu müssen entsprechende Autorisierungskomponenten integriert und eine maximale Automatisierung der Administration durch die Spezifikation von Regeln realisiert werden.

Die Aktivität umfasst die Einführung der entwickelten Rollen in die Produktion. Die Einführung umfasst u.a. folgende wesentliche Tätigkeiten:[668]

- Installation der Lösung: Die Installation der Lösung beinhaltet die Einrichtung des Produktes in dessen Zielumgebung zum Zwecke des Betriebs.[669] Für die Administration der entwickelten Rollen empfiehlt sich die Verwendung von Werkzeugen, die speziell für die

667 Vgl. Balzert 1998, S. 548.
668 Vgl. Balzert 2000, S. 1088.
669 Vgl. Balzert 2000, S. 1088.

systemübergreifende Administration von Berechtigungen entwickelt wurden.[670] Zunächst müssen diese, falls noch nicht geschehen, an die zu administrierenden Systeme angebunden werden. Um eine Automatisierung der Administration zu ermöglichen, müssen darüber hinaus Quellsysteme wie z.B. Personalverwaltungssysteme an das systemübergreifende Administrationswerkzeug angeschlossen werden. Im Werkzeug selbst müssen ausserdem alle Rollen angelegt und mit den Ressourcen der zu administrierenden Systeme verknüpft werden. Ebenfalls sind die Mitarbeiter den Rollen im System zuzuordnen.

- Inbetriebnahme der Lösung: Die eigentliche Inbetriebnahme kann auf drei Arten erfolgen.[671] Bei der direkten Umstellung wird unmittelbar von der alten auf die neue Lösung übergegangen. Dagegen werden beim Parallellauf alte und neue Lösung solange redundant betrieben, bis sichergestellt ist, dass die neue Lösung den gestellten Anforderungen entspricht. Im Unterschied zur ersteren Variante sieht der Ansatz der Versuchsläufe die stufenweise Erprobung und Einführung eines Systems vor. Im Rahmen der Fallstudien wurde ausnahmslos die stufenweise Einführung der neuen Administrationslösungen praktiziert. Sukzessive wurden die Rollen für alle Mitarbeiter implementiert und in den Betrieb übernommen.

Um die Administration weitestgehend zu automatisieren, empfiehlt sich die Spezifikation von Regeln. Folgende werkzeugspezifische Tätigkeiten sind u.a. hierfür notwendig:[672]

- Spezifikation von Regeln zur Rollenzuordnung:[673] Unterschiedliche Attribute beschreiben die Organisationseinheit, die Stelle oder auch den Standort eines Benutzers. Diese Daten können zur Automatisierung der Administration herangezogen werden. Durch die Änderung von Benutzerattributen, z.B. im Personalverwaltungssystem, können die Rollen, die einem Benutzer zusätzlich zugewiesen oder entzogen werden, automatisch durch hinterlegte Regeln bestimmt werden.

- Spezifikation von Regeln zur Ressourcenzuordnung:[674] In der Regel determinieren unterschiedliche Aspekte die Berechtigungen, die ein Benutzer für seine Arbeit benötigt. Ein typisches Beispiel hierfür ist die Abhängigkeit der Zugriffsberechtigungen eines Mitarbeiters von dessen Standort und Stelle. Würden beide Dimensionen bei der Definition der Rollen berücksichtigt, so würde eine Vielzahl von zu administrierenden Rollen entstehen. Um dieses Problem zu umgehen, basieren Rollen in der Regel auf lediglich einer Dimension. Um dennoch weitere Dimensionen einzubeziehen, werden wiederum Regeln verwendet, die auf der Basis vorhandener Benutzerattribute die Ressourcen einer Rolle bestimmen. Die durchgängige Verwendung von Namenskonventionen ist hierfür eine grundlegende Voraussetzung.

---

670 Vgl. hierzu auch die Fallstudien Basler Versicherungen und GENERALI, Kapitel 4.3 und 4.4.
671 Vgl. im Folgenden Balzert 2000, S. 1088.
672 Vgl. Kern 2002, S. 7ff.
673 Vgl. Kern 2002, S. 7f.
674 Vgl. Kern 2002, S. 8f.

- Spezifikation von Regeln zur Parameterbestimmung:[675] Zahlreiche Applikationen schränken den Zugriff auf ihre Daten und Funktionen auf der Basis von benutzerspezifischen Parametern ein. Beispielsweise wird die Vergabe von Krediten typischerweise durch entsprechende Limiten begrenzt. Für die Anwender müssen somit die entsprechenden Parameter auf der Basis existierender Benutzerattribute bestimmt und an die entsprechenden Systeme propagiert werden. Der Propagation liegen wiederum Regeln zugrunde, die sowohl einfache Wertübergaben als auch komplexe Transformationen durchführen können.

Mit der Spezifikation der Regeln ist die initiale Einführung der Rollen abgeschlossen.

7.5 Dokumentationsmodell

Tabelle 57 zeigt das Dokumentationsmodell „Integration der Autorisierung“, das die Ergebnisse und die zeitlichen und inhaltlichen Beziehungen zwischen den Ergebnissen dieses Methodenbausteins darstellt. Die Darstellung erfolgt überblicksartig und unter besonderer Berücksichtigung der Beziehungen der Ergebnisse, da die Ergebnisse bereits im Zusammenhang der Ableitung sowie innerhalb der einzelnen Aktivitäten beschrieben wurden. Im Rahmen der Aktivitäten werden auch Ergebnisse erarbeitet, bei denen nicht die Dokumentation, sondern die unmittelbare informationstechnische Umsetzung im Vordergrund steht. Das Dokumentationsmodell kann daher treffender als Ergebnismodell bezeichnet werden.

A basiert auf B	**Ergebnis B**			
Ergebnis A	**I Vorstudie System**	**II Vorstudie Organisation**	**III Rollen-definition**	**IV Rollenimple-mentierung**
1 Vorstudie System				
1.1 Metamodell				
1.2 Rollenkonzept	1.1			
2 Vorstudie Organisation				
2.1 Administrationsrollen	1.1, *1.2*			
2.2 Administratoren	1.1, *1.2*	*2.1*		
3 Rollendefinition				
3.1 Ressourceninventar	1.1			
3.2 Rollengrobspezifikationen	1.1, *1.2*		3.1	
3.3 Rollenfeinspezifikationen	1.1, 1.2		3.1, *3.2*	
4 Rollenimplementierung				
4.1 Rollenpiloten	1.1, 1.2		3.1, *3.3*	
4.2 Implementierte Rollen	1.1, 1.2		3.1, 3.3	*4.1*

Legende: Essentielle Ergebnisabhängigkeiten sind kursiv dargestellt

Tabelle 57: Dokumentationsmodell „Integration der Autorisierung“

675 Vgl. Kern 2002, S. 9.

Die in der Phase *„Vorstudie System“* entwickelten Ergebnisse gehen in fast jede folgende Aktivität und somit auch in deren Ergebnisse ein. Das erarbeitete Metamodell wird im Rahmen der folgenden Aktivitäten insbesondere zur Vereinheitlichung der Sprache und damit als Kommunikationsbasis eingesetzt. Auch das erarbeitete Rollenkonzept, das wesentliche Rollenklassen definiert, prägt den weiteren Entwicklungsprozess massgeblich. Sowohl die zu definierenden Administrationsrollen als auch die Entwicklung der Rollen selbst werden von den Rollenklassen beeinflusst. Die in der Phase *„Vorstudie Organisation“* bestimmten Administratoren realisieren die eigentliche Rollendefinition und -implementierung, so dass die entwickelten Administrationsrollen und die entsprechenden Besetzungen im weiteren Verlauf des Vorgehens durchgehende Verwendung finden. Die dokumentierten Ergebnisse dieser Phase fliessen jedoch nicht unmittelbar in die Ergebnisse der folgenden Phasen ein. In der Phase *„Rollendefinition“* erfolgt zuerst die Grobspezifikation der Rollen. Diese Grobspezifikation bildet die Grundlage für die Feinspezifikation der Rollen, welche wiederum Ausgangspunkt der Implementierung ist. Die systematische Aufnahme und Dokumentation der Ressourcen in ein Ressourceninventar kann der Ausgangspunkt aller folgenden Aktivitäten sein. Die *Implementierung der Rollen* beginnt mit der Realisierung von Rollenpiloten, die die Basis für die eigentliche Implementierung der Rollen darstellen.

7.6 Rollenmodell

Die Entwicklung und Implementierung der systemübergreifenden Rollen erfolgte im Rahmen der Fallstudien durch speziell hierfür initiierte Projekte. Diese Projekte wurden von entsprechenden Arbeitsgruppen durchgeführt. Zu Beginn der Projekte stand die gemeinsame Erarbeitung von Grundlagen im Mittelpunkt. Im Projektverlauf wurden dann die Verantwortlichkeiten für die Rollendefinition, -pflege und -implementierung, die über die verantwortlichen Projektmitglieder hinausgingen, unternehmensspezifisch festgelegt. Die beschriebenen Aktivitäten „Administrationsrollen definieren“ und „Administratoren definieren“ thematisieren dieses Vorgehen zur Festlegung der Verantwortlichkeiten.[676] In den Arbeitsgruppen waren folgende Unternehmensvertreter präsent:

- Vertreter Management: Um eine flächendeckende Einführung der systemübergreifenden Rollen sicherzustellen, ist die Mitwirkung zahlreicher Mitarbeiter aus dem Fachbereich und der IT vonnöten. Es ist Aufgabe des Managements, die hierfür erforderlichen Ressourcen bereitzustellen. Da sich das Projekt über unterschiedliche Verantwortungsbereiche erstreckt, muss darüber hinaus die bereichsübergreifende Projektunterstützung sichergestellt werden. Im Rahmen der analysierten Fallstudien übernahm jeweils das Topmanagement der IT die Rolle „Projektsponsor“, um die dargestellten Erfordernisse angemessen umzusetzen.

[676] Vgl. Kapitel 7.4.2.1.

- Vertreter Fachbereich: Die Mitarbeiter des Fachbereichs kennen die Geschäftsprozesse und die mit diesen einhergehenden Verantwortlichkeiten. Um die fachlichen Anforderungen angemessen und ausreichend zu berücksichtigen, ist ihre Projektbeteiligung unabdingbar.

- Vertreter Entwicklung: Die Vertreter der Entwicklung verfügen über Erfahrungen bei der Entwicklung systemspezifischer Berechtigungskonzepte. Diese Erfahrungen können sie bei der Einführung der systemübergreifenden Rollen einbringen.

- Vertreter Betrieb: Aus dem Bereich Betrieb ist insbesondere die zentrale Benutzeradministration in das Projekt einzubeziehen, da sie als zentrale Organisationseinheit für die Pflege der Berechtigungen verantwortlich ist.

- Vertreter Revision, Risiko- und Sicherheitsmanagement: Bei der Entwicklung der systemübergreifenden Administrationslösung müssen existierende Weisungen und verwendete Sicherheitsstandards Berücksichtigung finden.[677] Die Einbeziehung von Mitarbeitern der verantwortlichen Abteilungen wie Revision, Risiko- oder Sicherheitsmanagement ist daher unabdingbar.

Auf der Basis der Fallstudien lassen sich analog zum Methodenbaustein „Autorisierungsarchitektur“ die Projektrollen Projektsponsor, Projektleiter und Projektmitarbeiter identifizieren.[678] Im Rahmen der Fallstudien übernahm das Topmanagement der IT die Rolle des Projektsponsors.[679] Die Projektleitung wurde von einem Vertreter der zentralen Benutzerverwaltung bzw. durch einen Mitarbeiter der Revision durchgeführt. Die Projektmitarbeiter rekrutierten sich aus den Vertretern der dargestellten Unternehmensbereiche. Im Verlauf des Projektes erfolgte, wie in den Ausführungen dargelegt,[680] die Definition weiterer unternehmensspezifischer Administrationsrollen.

677 Vgl. Kapitel 5.2.
678 Vgl. Kapitel 6.6.
679 Vgl. im Folgenden Kapitel 4.3 und 4.4.
680 Vgl. Kapitel 7.4.2.1.

8 Kritische Würdigung und Ausblick

Das abschliessende Kapitel dient der kritischen Reflexion der erarbeiteten Ergebnisse. Hierzu werden in Abschnitt 8.1 zunächst die wesentlichen Ergebnisse der Arbeit zusammengefasst und diese anschliessend in Abschnitt 8.2 gewürdigt. Abschliessend wird in Abschnitt 8.3 ein Ausblick auf weitere Forschungsthemen gegeben, die in unmittelbarem Zusammenhang mit den Ergebnissen der Arbeit stehen.

8.1 Zusammenfassung der Arbeit

Das primäre Gestaltungsziel der Arbeit ist die Entwicklung einer Methode für die effektive und effiziente Autorisierung. Gegenstand der Methode sind, bedingt durch das Entstehungsumfeld der Arbeit, die Themenbereiche „Autorisierungsarchitektur“ und „Integration der Autorisierung“. Die Erhebung und Analyse aktueller Grundlagen und Methoden der Autorisierung in Praxis und Forschung stellt das primäre Erkenntnisziel der Arbeit und die Grundlage der Methodenentwicklung dar.

Die Entwicklung der Methode beginnt mit der Aufarbeitung elementarer Grundlagen und der Abgrenzung der Thematik (Kapitel 2). Zunächst wird das Business Engineering vorgestellt, das den Forschungsrahmen der Arbeit bildet. Zur Abgrenzung der Autorisierung wird sodann die Sicherheit von Informationssystemen thematisiert. Da sich in der unternehmerischen Praxis die rollenbasierte Autorisierung als dominierendes Konzept etabliert hat, stehen ausgewählte Standards zur rollenbasierten Autorisierung im Fokus der weiteren Ausführungen. Anschliessend erfolgt eine Darstellung des Risikomanagements im Kontext der Autorisierung: Autorisierung als Verwaltung und Kontrolle von Berechtigungen wird implementiert, um potenzielle Schäden zu vermeiden und sich gegen Risiken zu schützen. Autorisierung ist somit ein Element der Risikobewältigung und Teil des Risikomanagements. Aus den vorgenannten Grundlagen werden abschliessend Konsequenzen für die weitere Vorgehensweise der Methodenentwicklung abgeleitet.

Im Anschluss an die Aufarbeitung der Grundlagen erfolgt die Untersuchung methodischer Ansätze, die sich mit dem Thema Autorisierung befassen (Kapitel 3). Dabei werden insbesondere solche Ansätze berücksichtigt, die hinsichtlich ihres Abstraktionsgrades eine hinreichend konkrete Diskussion erlauben und umsetzungsorientiert sind oder bereits in der Praxis eingesetzt wurden. Die diskutierten Ansätze gehen über eine rein technische Betrachtung des Themas Sicherheit hinaus. Den aktuellen Erkenntnissen in Forschung und Praxis entsprechend baut der Grossteil der Ansätze auf der rollenbasierten Autorisierung auf. Dabei werden nur in eingeschränktem Masse risikoorientierte Vorgehensweisen berücksichtigt: Sehr umfangreiche Sicherheitsmassnahmen sind nur durch einen entsprechend hohen Einsatz von Ressourcen umzusetzen. Geringe Vorkehrungen bergen die Gefahr, dass es zu erheblichen Schäden infolge mangelnder Sicherheit kommt. Lediglich die Arbeit von HARTJE ET AL. umfasst überhaupt durchgängig detaillierte, methodische Elemente, ohne sich dabei allerdings

vertieft den Themenschwerpunkten dieser Arbeit zu widmen. Vor diesem Hintergrund war ein eigener Methodenvorschlag zu erarbeiten.

Da die untersuchten Ansätze zur Autorisierung keine umfassende, methodische Sichtweise auf die gewählten Schwerpunkte der Dissertation bieten, werden im Folgenden (Kapitel 4) Praxisprojekte in Form von Fallstudien dokumentiert, die im weiteren Verlauf der Arbeit als Ausgangspunkt des Methodenentwurfes dienen. Jeweils zwei Fallstudien widmen sich dabei genau einem der beiden Themenschwerpunkte der Arbeit. Da die beiden Methodenbausteine „Autorisierungsarchitektur“ und „Integration der Autorisierung“ nicht aus Versatzstücken unterschiedlicher Herkunft zusammengesetzt werden sollen, stehen die Identifikation von Gemeinsamkeiten und das Prinzip der Induktion im Vordergrund der Methodenkonstruktion. Jede Fallstudie wird daher bei der Methodenentwicklung gleichermassen berücksichtigt und deckt jeweils den ganzen Betrachtungsgegenstand eines Themenschwerpunktes ab.

Vor der eigentlichen Ableitung der Methode erfolgt die Festlegung wesentlicher Methodengrundlagen (Kapitel 5). Dazu werden zunächst die grundlegenden Elemente der zu entwickelnden Methode auf Basis des Methoden-Engineering definiert. Im Business Engineering stellt das Methoden-Engineering nach GUTZWILLER die Grundlage der Methodenentwicklung dar. Obwohl damit ein Metamodell sowie entsprechende Ausführungen vorliegen, kommt es bei dem Entwurf von Methoden im Kontext des St. Galler Business Engineering zu einer unterschiedlichen Verwendung der Methodenelemente. Das Metamodell des Methoden-Engineering wird daher präzisiert und erweitert, um so die Methodenelemente und ihr Zusammenwirken verbindlich und präzise für die vorliegende Arbeit zu definieren. Um den Anspruch und den Charakter der zu entwickelnden Methode festzulegen, wird ihr Profil anhand ausgewählter Merkmale des Methoden-Engineering und der Referenzprozessmodellierung verdeutlicht. Dabei wird u.a. dargelegt, inwiefern die Methode den Kriterien „Allgemeingültigkeit“ und „Empfehlungscharakter“ entspricht. Um den Empfehlungscharakter der Methode sicherzustellen, werden sodann Anforderungen an die Methode abgeleitet. Ausgangspunkt der Ableitung bilden international etablierte Sicherheitsstandards, die die situationsgerechte Operationalisierung von Effizienz- und Effektivitätszielen zum Gegenstand haben. Die Festlegung wesentlicher Methodengrundlagen endet mit der Beschreibung eines grundlegenden Metamodells, das wesentliche Entitätstypen der Domäne Autorisierung in Bezug zueinander setzt.

Auf Basis der beschriebenen Fallstudien und der analysierten Literatur wird anschliessend ein Vorgehens-, Meta-, Dokumentations- und Rollenmodell für die Entwicklung einer Autorisierungsarchitektur abgeleitet (Kapitel 6). Im Rahmen der durchzuführenden Aktivitäten gilt es, zunächst die wesentlichen Grundlagen zur Entwicklung der Autorisierungsarchitektur zu legen. Neben der Abgrenzung und Untergliederung der zu entwickelnden Architektur sind Anforderungen an die Autorisierung zu erheben und zu dokumentieren. In der anschliessenden Analyse der Ist-Situation erfolgt die Ermittlung von Schwachstellen, die als Ausgangspunkt der Architekturentwicklung dienen. Ziel der folgenden Aktivitäten ist, wesentliche Gestaltungsoptionen und Handlungsanweisungen zur Lösung bzw. Regelung der identifizierten

Schwachstellen zu erarbeiten. Abschliessend erfolgt die Identifikation von Massnahmenkomplexen zur Umsetzung der erarbeiteten Lösungsansätze. Hierzu müssen Massnahmen abgeleitet und unter Berücksichtigung inhaltlicher Verflechtungen zu Massnahmenkomplexen gebündelt werden.

Abschliessend wird – ebenfalls auf der Grundlage der beschriebenen Fallstudien und der analysierten Literatur – ein Vorgehens-, Meta-, Dokumentations- und Rollenmodell für die Integration der Autorisierung abgeleitet (Kapitel 7). Die Ableitung knüpft an die Ausführungen zur Autorisierungsarchitektur (Kapitel 6) an, die u.a. unterschiedliche Gestaltungsoptionen der Autorisierung umfassen und hierdurch die Integration von systemspezifischen Berechtigungskonzepten als Lösungsansatz identifizieren, der massgeblich zu einer effektiven und effizienten Autorisierung beiträgt. In Entsprechung zum entwickelten Vorgehensmodell gilt es zunächst, grundlegende Lösungskonzepte für die Entwicklung und Implementierung systemübergreifender Rollen z.B. in Form von Metamodellen zu entwickeln und zu spezifizieren. Um internationalen Sicherheitsstandards gerecht zu werden, sind die Aufgaben, Kompetenzen und Verantwortlichkeiten bei der Definition und Pflege der Berechtigungen zu Administrationsrollen zu bündeln und diese mit geeigneten Mitarbeitern zu besetzen. Anschliessend erfolgt die eigentliche Spezifikation der systemübergreifenden Rollen. Hierzu wird für jede Rolle festgelegt, welche Mitarbeiter mit der Rolle arbeiten. Darüber hinaus sind die Berechtigungen, die eine Rolle umfasst, festzulegen. Im Rahmen der Rollenimplementierung werden die definierten Rollen schliesslich informationstechnisch umgesetzt, getestet und in den Betrieb überführt.

8.2 Kritische Würdigung

Im Rahmen der Methodenentwicklung wurde bereits eine kritische Diskussion der erarbeiteten Ergebnisse anhand der Kriterien „Allgemeingültigkeit“ und „Empfehlungscharakter“ geführt.[681] Diese Diskussion soll im Folgenden anhand ausgewählter Kriterien ausgeweitet werden. Da dem Dissertationsvorhaben das Design-Science-Paradigma zugrunde liegt, werden der Würdigung die Design-Science-Richtlinien von HEVNER ET AL. zugrunde gelegt, die wesentliche Anforderungen an eine Forschungsarbeit formulieren.[682]

Ergebnis eines Design-Science-Forschungsprozesses ist ein *anwendbares Artefakt* in der Form eines Konstruktes, eines Modells, einer Methode oder einer Instanz:[683] Das Ergebnis dieser Arbeit ist eine Methode, die induktiv abgeleitet wird. Dadurch, dass die Methodenbausteine nicht aus Versatzstücken unterschiedlicher Fallstudien zusammengesetzt werden, sondern auf der Verallgemeinerung und der Identifikation von Gemeinsamkeiten basieren, ist das

681 Zur Definition der Kriterien vgl. Kapitel 5.1.2; zur Bewertung vgl. Kapitel 6.3.4 und 7.3.4.
682 Vgl. Hevner et al. 2004, S. 82ff.
683 Vgl. Hevner et al. 2004, S. 82f.

entwickelte Artefakt anwendbar: Die einzelnen Fallstudien stellen Instanzen der entwickelten Methode dar und zeigen auf diese Weise deren potenzielle Anwendbarkeit.

Das Ziel eines Design-Science-Forschungsprozesses ist die Entwicklung von *Lösungen für wichtige und relevante Probleme*:[684] Die Bedeutung der Autorisierung als Grundfunktion der Sicherheit ist unumstritten.[685] Trotz zahlreicher Lösungsansätze steht den Verantwortlichen in den Unternehmen kein umfassendes methodisches Vorgehen für die mittel- und langfristige, unternehmensweite Gestaltung der Autorisierungsinfrastruktur (im Sinne einer Autorisierungsarchitektur) sowie für die systemübergreifende Integration von Berechtigungen zur Verfügung.[686] Die Arbeit adressiert diese Lücke durch die Entwicklung einer entsprechenden Methode.

Der *Nutzen*, die *Qualität* und die *Wirksamkeit eines Artefaktes* muss bewertet bzw. demonstriert werden:[687] Die Arbeit setzt sich explizit mit der Bewertbarkeit von Artefakten auseinander. Unter dem Kriterium „Empfehlungscharakter" wird insbesondere die Abhängigkeit der Bewertung von subjekt-, sach- und umfeldbedingten Gegebenheiten thematisiert.[688] Die Qualität der zu entwickelnden Methode wird durch die Ableitung und Berücksichtigung von Anforderungen sichergestellt, die auf der Basis etablierter Sicherheitsstandards ermittelt werden. Diese Vorgehensweise kann dabei nur in begrenztem Umfang die Qualität der Methode sicherstellen. Ein absoluter Qualitätsnachweis kann, der konstruktivistischen Perspektive folgend, nicht erbracht werden.[689]

Design-Science muss einen *klaren und nachprüfbaren Forschungsbeitrag erzeugen*, der in der Schaffung eines Artefaktes oder der Erweiterung der Wissensbasis liegt:[690] Die vorliegende Arbeit entwickelt zum einen ein Artefakt in Form einer Methode. Darüber hinaus setzt sich die Arbeit mit der adäquaten Spezifikation und Entwicklung von Methoden auseinander.[691] Auf diese Weise trägt sie zur fundamentalen Wissensbasis bei.

Design-Science beruht auf der Anwendung stringenter Vorgehensweisen.[692] Die *Stringenz der Forschung* wird dabei durch die effektive Nutzung der Wissensbasis sichergestellt: Die vorliegende Arbeit greift auf unterschiedliche Art und Weise auf die existierende Wissensbasis zurück: Insbesondere im Rahmen der Grundlagen und der Diskussion vorhandener, methodischer Ansätze wird explizit auf die Wissensbasis Bezug genommen. Auch der eigentliche Vorgang der Methodenkonstruktion baut auf wissenschaftlichen Arbeiten auf, die sich mit der

684 Vgl. Hevner et al. 2004, S. 84f.
685 Vgl. Kapitel 2.2.3.
686 Vgl. Kapitel 3.2.6.
687 Vgl. Hevner et al. 2004, S. 85f.
688 Vgl. Kapitel 5.1.2.
689 Vgl. hierzu auch Kapitel 5.1.2.
690 Vgl. Hevner et al. 2004, S. 87.
691 Vgl. Kapitel 5.1.
692 Vgl. im Folgenden Hevner et al. 2004, S. 87f.

Methodenkonstruktion und den zu spezifizierenden Methodenelementen auseinandersetzen und somit ebenfalls der Wissensbasis zuzurechnen sind.

Design-Science ist durch eine iterative Vorgehensweise gekennzeichnet.[693] Optimale Lösungen können dabei im Umfeld des „Information Systems Research" in der Regel nicht bestimmt werden. Die *Entwicklung von Artefakten* ist daher letztlich ein heuristischer *Suchprozess*: Im Rahmen der Arbeit dienen vor allem Fallstudien als Ausgangspunkt der Methodenerstellung. Infolge dessen hängt die Qualität der Methode massgeblich von der Qualität der Fallstudien ab. Alle erhobenen Vorgehensweisen haben sich in der Praxis bewährt und basieren auf dem langjährigen Erfahrungswissen der entsprechenden Unternehmen.[694] Im Sinne des Design-Science sind sie das Ergebnis eines heuristischen Suchprozesses, das massgeblich durch die Erfahrung, Kreativität und Problemlösungsfähigkeit der verantwortlichen Mitarbeiter beeinflusst wird.

Design-Science-Forschungsergebnisse sind angemessen zu *kommunizieren* und sowohl für Fach- als auch für Führungskräfte aufzubereiten:[695] Im Rahmen der Methodenkonstruktion werden die Methodenelemente detailliert spezifiziert, so dass Fachkräfte die Methode in der Praxis anwenden können. Gegenstand und Motivation der Methode werden zu Beginn der Arbeit so dargestellt, dass auch Führungskräfte den Anwendungsbereich und den Innovationsgehalt der Methode einschätzen können.

8.3 Ausblick

Die vorliegende Arbeit versteht sich als Ausgangspunkt für weitere wissenschaftliche Aktivitäten und Umsetzungen in der Praxis. Folgende Themen stellen Ansatzpunkte zur Weiterentwicklung dar:

- Integration ins Architekturmanagement: Die entwickelten Aktivitäten zur Ermittlung einer Autorisierungsarchitektur könnten in bestehende Ansätze des Architekturmanagements integriert werden. Dabei ist zu beachten, dass das Architekturmanagement je nach Definition sowohl durch dauerhaft implementierte Prozesse (z.B. Architekturführung) als auch durch temporäre Transformationsprozesse (z.B. initiale Erarbeitung oder grundlegende Überarbeitung einer Architektur) gekennzeichnet ist. Während erstere im Rahmen des St. Galler Business Engineering vor allem durch die Entwicklung von Referenzprozessmodellen adressiert werden, sind letztere Gegenstand der Methodenentwicklung. Eine klar definierte Schnittstelle zwischen den dauerhaft implementierten Prozessen und den temporären Transformationsprozessen ist notwendig, um die entwickelten Architekturaktivitäten als Transformationsaktivitäten in einen Architekturmanagementansatz eingliedern zu können.

693 Vgl. im Folgenden Hevner et al. 2004, S. 88f.
694 Vgl. hierzu auch Kapitel 4.
695 Vgl. Hevner et al. 2004, S. 90.

- Referenzprozesse der Autorisierung: Die entwickelte Methode adressiert Transformationsprozesse im Umfeld der Autorisierung. Um auch die dauerhaft implementierten Autorisierungsprozesse, die durch die primäre Organisation abgewickelt werden, zu thematisieren, bietet sich die Erstellung eines entsprechenden Referenzmodells für die unternehmensweite Verwaltung von Zugriffsberechtigungen an.

- Entwicklung von systemspezifischen Berechtigungskonzepten: Mit der Entwicklung eines Vorgehensmodells für die Einführung systemübergreifender Berechtigungskonzepte thematisiert die Arbeit die Integration der Autorisierung. Weitere Forschungsarbeiten könnten die Entwicklung systemspezifischer Berechtigungskonzepte unter Berücksichtigung systemübergreifender Rollen thematisieren.

- Anwendung der entwickelten Methode: Wünschenswert wäre darüber hinaus eine Anwendung der entwickelten Methode in der Praxis. Die gemachten Erfahrungen könnten in die Weiterentwicklung der Methode einfliessen und würden diese auf eine breitere Fallstudienbasis stellen.

- Metamodell Methoden-Engineering: Das in der Arbeit erweiterte Metamodell des Methoden-Engineering könnte im Zuge folgender Forschungsarbeiten kritisch diskutiert und weiterentwickelt werden. Im Fokus dieser Arbeiten könnte insbesondere das Verhältnis zwischen Aktivitäten und Techniken stehen. Die Beziehung der Notation zu den Metaentitätstypen „Ergebnis“, „Technik“ und „Dokumentationsmodell“ erscheint ebenfalls diskussionswürdig.

- Methoden-Engineering und Referenzprozessmodellierung: In der Arbeit werden Vorgehensweisen und Überlegungen der Referenzprozessmodellierung auf das Methoden-Engineering übertragen. Aspekte wie z.B. die Methodenkonfiguration, die in der vorliegenden Arbeit lediglich ansatzweise thematisiert werden, können im Rahmen weiterer Arbeiten aufgegriffen, kritisch reflektiert und weiterentwickelt werden.

- Ermittlung von Erfolgsfaktoren: Zentrale Erfolgsfaktoren, die es bei der Autorisierung im Allgemeinen und bei der Methodenanwendung im Besonderen zu beachten gilt, könnten in weiteren, quantitativen Forschungsarbeiten ermittelt werden.

Der beispielhafte Überblick zeigt, dass die Arbeit als Ausgangspunkt für unterschiedliche Forschungsarbeiten genutzt werden kann. Da die Anforderungen an die Vollständigkeit und Wirksamkeit der Sicherheitsmechanismen immer weiter wachsen,[696] wird der Autorisierung auch in Zukunft eine hohe Aufmerksamkeit zuteil werden.

[696] Vgl. Hartje et al. 2003, S. 13.

Anhang: Ansprechpartner zu den Fallstudien

Die Fallstudien wurden auf Basis von Interviews und Dokumentenanalysen zusammengestellt. Die Befragung der Unternehmensvertreter erfolgte am Dienstsitz der Interviewpartner. Vertiefende Nachbesprechungen der Interviews wurden telefonisch durchgeführt. Folgende Ansprechpartner waren an der Erhebung der Fallstudien beteiligt:

Fallstudie Basler Versicherungen

Ghislaine Ackermann Pfluger
Zentrale Benutzerverwaltung
Basler Versicherungen
Aeschengraben 21
CH-4002 Basel
Experteninterview am 24.06.2005

Fallstudie Credit Suisse

Gritta Wolf
IT Security Architecture
Credit Suisse
Lessingstrasse 3
CH-8070 Zürich
Experteninterview am 04.07.2005

Fallstudie GENERALI Gruppe Schweiz

Jürgen Lorek
Internal Audit Services
GENERALI (Schweiz) Holding
Soodmattenstr. 10
CH-8134 Adliswil
Experteninterview am 23.06.2005

Fallstudie Winterthur Group

Bruno Honegger, Thomas Fuhrer
IT Architecture
Winterthur Group
General Guisan-Strasse 40
CH-8401 Winterthur
Experteninterview am 31.05.2005

Literaturverzeichnis

Amann/Atzmüller 1992
Amann, E., Atzmüller, H.: IT-Sicherheit – Was ist das?, in: Datenschutz und Datensicherung, 16(1992)6, S. 286-292.

Bâloise-Holding 2005
Bâloise-Holding: Geschäftsbericht 2004, Basel, 2005.

Balzert 1998
Balzert, H.: Lehrbuch der Software-Technik, Band 2, Software-Management, Software-Qualitätssicherung, Unternehmensmodellierung, Spektrum Akademischer Verlag, Heidelberg, 1998.

Balzert 2000
Balzert, H.: Lehrbuch der Software-Technik, Band 1, Software-Entwicklung, 2. Auflage, Spektrum Akademischer Verlag, Heidelberg, 2000.

Basler Ausschuss für Bankenaufsicht 2004
Basler Ausschuss für Bankenaufsicht: Internationale Konvergenz der Eigenkapitalmessung und der Eigenkapitalanforderungen, Bank für Internationalen Zahlungsausgleich, Basel, 2004.

Becker 1995
Becker, J.: Strukturanalogien in Informationsmodellen – Ihre Definition, ihr Nutzen und ihr Einfluss auf die Bildung von Grundsätzen ordnungsmässiger Modellierung (GOM), in: König, W. (Hrsg.): Wirtschaftsinformatik '95, Physica, Heidelberg, 1995, S. 133-150.

Becker et al. 2002
Becker, J., Algermissen, L., Delfmann, P., Knackstedt, R.: Referenzmodellierung, in: Das Wirtschaftsstudium, 30(2002)11, S. 1392-1395.

Birkhölzer/Vaupel 2003
Birkhölzer, T., Vaupel, J.: IT-Architekturen – Planung, Integration, Wartung, VDE, Berlin, 2003.

BITKOM 2005a
BITKOM: Kompass der IT-Sicherheitsstandards, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., 2005, http://www.bitkom.org/files/documents/BITKOM_Broschuere_Sicherheitsstandard_V1.01f.pdf (15.07.2005).

BITKOM 2005b
BITKOM: Matrix der Haftungsrisiken, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., 2005, http://www.bitkom.org/files/documents/Bitkom-Leitfaden_Matrix-Haftungsrisiken_V0.1.0f.pdf (10.07.2005).

Blümle 1975
Blümle, E.-B.: Stellvertretung, in: Gaugler, E. (Hrsg.): Handwörterbuch des Personalwesens, C.E. Poeschel, Stuttgart, 1975, S. 1887-1893.

Brauhäuser et al. 2003
Brauhäuser, M., Biltzinger, P., Lorenz, C.: Qualitative Risikoanalyse – Methodische Vorgehensweise in der IT-Beratungspraxis, in: Rossbach, P., Locarek-Junge, H. (Hrsg.): IT-Sicherheitsmanagement in Banken, Bankakademie, Frankfurt am Main, 2003, S. 55-70.

Braun et al. 2004
Braun, C., Hafner, M., Wortmann, F.: Methodenkonstruktion als wissenschaftlicher Erkenntnisansatz, Arbeitsbericht, Institut für Wirtschaftsinformatik, Universität St. Gallen, 2004.

Braun et al. 2005
Braun, C., Wortmann, F., Hafner, M., Winter, R.: Method Construction – A Core Approach to Organizational Engineering, in: Proceedings of the 2005 ACM Symposium on Applied Computing, Santa Fe, 2005, S. 1295-1299.

Brenner et al. 2003
Brenner, W., Zarnekow, R., Pörtig, F.: Entwicklungstendenzen im Informationsmanagement, in: Österle, H., Winter, R. (Hrsg.): Business Engineering – Auf dem Weg zum Unternehmen des Informationszeitalters, 2. Auflage, Springer, Berlin, 2003, S. 147-168.

British Standards Institution 2002
British Standards Institution: BS 7799-2 – Information Security Management Systems – Specification with Guidance for Use, 2002, http://www.bsonline.bsi-global.com (03.07.2005).

Brockhaus 2005
Brockhaus: Suchergebnis für »Klasse«, Bibliographisches Institut & F. A. Brockhaus AG, 2005, http://www.brockhaus.de/suche/index.php?begriff=Klasse&bereich=mixed&x=0&y=0 (10.09.2005).

BSI 1992
BSI: BSI 7105 – IT-Sicherheitshandbuch, Bundesamt für Sicherheit in der Informationstechnik, Bonn, 1992.

BSI 1998
BSI: IT-Sicherheitskriterien, Bundesamt für Sicherheit in der Informationstechnik, 1998, http://www.bsi.bund.de/zertifiz/itkrit/itgruend.pdf (25.03.2002).

BSI 2004
BSI: IT-Grundschutzhandbuch, Bundesamt für Sicherheit in der Informationstechnik, 2004, http://www.bsi.de/gshb/deutsch/menue.htm (17.02.2005).

BSI 2005
BSI: BSI Schulung IT-Grundschutz – Glossar, Bundesamt für Sicherheit in der Informationstechnik, 2005, https://ncc.uni-mannheim.de/bsi-webkurs/gsschul/gskurs/seiten/glossar/gloss_ah.htm (19.09.2005).

Büllesbach 1999
Büllesbach, A.: Datenschutz als prozessorientierter Wettbewerbsbestandteil, in: Praxis der Informationsverarbeitung und Kommunikation, 22(1999)3, S. 162-169.

Bundesaufsichtsamt für das Kreditwesen 1996
Bundesaufsichtsamt für das Kreditwesen: Mindestanforderungen an das Betreiben von Handelsgeschäften der Kreditinstitute, in: Scharf, P., Luz, G. (Hrsg.): Risikomanagement, Bilanzierung und Aufsicht von Finanzderivaten, Schäffer, Stuttgart, 1996, S. 655-675.

BVerfGe 1983
BVerfGe: BVerfGe 65, 1 – Volkszählung – Urteil des ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden, 1983, http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm (12.07.2004).

Cazemier 1999
Cazemier, J.: ITIL Security Management, The Stationery Office Books, London, 1999.

Chalmers 1989
Chalmers, A. F.: Wege der Wissenschaft, Springer, Berlin, 1989.

Chandramouli/Sandhu 1998
Chandramouli, R., Sandhu, R.: Role-Based Access Control Features in Commercial Database Management Systems, in: Proceedings of the 21th NIST-NSA National Computer Security Conference, Crystal City (VA), 1998, S. 503-511.

Credit Suisse Group 2005
Credit Suisse Group: Geschäftsbericht 2004, Zürich, 2005.

Dangelmaier et al. 2002
Dangelmaier, W., Lessing, H., Pape, U., Rüther, M.: Klassifikation von EAI-Systemen, in: HMD – Praxis der Wirtschaftsinformatik, 38(2002)225, S. 61-71.

Dern 2003
Dern, G.: Management von IT-Architekturen – Informationssysteme im Fokus von Architekturplanung und -entwicklung, Vieweg, Braunschweig, 2003.

DIN 1988
DIN: DIN 44300 – Teil I – Informationsverarbeitung, Allgemeine Begriffe, Deutsches Institut für Normung, Berlin, 1988.

Eckert 2003
Eckert, C.: IT-Sicherheit – Konzepte, Verfahren, Protokolle, 2. Auflage, Oldenbourg, München, 2003.

Endrei et al. 2004
Endrei, M., Ang, J., Arsanjani, A., Chua, S., Comte, P., Krogdahl, P., Luo, M., Newling, T.: Patterns – Service-Oriented Architecture and Web Services, 2004, http://www.redbooks.ibm.com/redbooks/pdfs/sg246303.pdf (01.10.2005).

Federrath/Pfitzmann 2000
Federrath, H., Pfitzmann, A.: Gliederung und Systematisierung von Schutzzielen in IT-Systemen, in: Datenschutz und Datensicherheit, 24(2000)12, S. 704-710.

Ferraiolo et al. 2001
Ferraiolo, D., Sandhu, R., Gavrila, S., Kuhn, R. D., Chandramouli, R.: Proposed NIST Standard for Role-Based Access Control, in: ACM Transactions on Information and System Security, 4(2001)3, S. 224-274.

Ferstl/Sinz 1998
Ferstl, O., Sinz, E. J.: Grundlagen der Wirtschaftsinformatik, 3. Auflage, Oldenbourg, München, 1998.

Fettke/Loos 2002
Fettke, P., Loos, P.: Methoden zur Wiederverwendung von Referenzmodellen – Übersicht und Taxonomie, in: Becker, J., Knackstedt, R. (Hrsg.): Referenzmodellierung 2002, Arbeitsbericht Nr. 90, Institut für Wirtschaftsinformatik, Universität Münster, 2002, S. 9-33.

Fischer-Hübner 2001
Fischer-Hübner, S.: IT-Security and Privacy, Springer, Berlin, 2001.

Frank et al. 1999
Frank, U., Klein, S., Krcmar, H., Teubner, A.: Aktionsforschung in der WI – Einsatzvoraussetzungen und -gelegenheiten, in: Schütte, R., Siedentopf, J., Zelewski, S. (Hrsg.): Wirtschaftsinformatik und Wissenschaftstheorie – Grundpositionen und Theoriekerne, Arbeitsbericht Nr. 4, Institut für Produktion und Industrielles Informationsmanagement, Universität GH Essen, 1999, S. 71-90.

Fürer 1990
Fürer, G.: Risk Management im internationalen Bankgeschäft, Haupt, Bern, 1990.

Gamma et al. 1996
Gamma, E., Helm, R., Johnson, R., Vlissides, J.: Entwurfsmuster – Elemente wiederverwendbarer objektorientierter Software, Addison-Wesley, München, 1996.

Garlan 1995
Garlan, P.: Introduction to the Special Issue on Software Architecture, in: IEEE Transactions on Software Engineering, 21(1995)4, S. 269-274.

GENERALI (Schweiz) Holding 2005
GENERALI (Schweiz) Holding: Geschäftsbericht 2004, Adliswil, 2005.

Greiffenberg 2004
Greiffenberg, S.: Methodenentwicklung in Wirtschaft und Verwaltung, Verlag Dr. Kovac, Hamburg, 2004.

Gross/Knippschild 1996
Gross, H., Knippschild, M.: Instrumente und Organisation der Risikosteuerung von Handelsaktivitäten, in: Krummnow, J. (Hrsg.): Schriften zur Unternehmensführung, Gabler, Wiesbaden, 1996, S. 97-113.

Gutzwiller 1994
Gutzwiller, T.: Das CC RIM-Referenzmodell für den Entwurf von betrieblichen, transaktionsorientierten Informationssystemen, Physica, Heidelberg, 1994.

Hafner 2002
Hafner, M.: Datenschutz im Data Warehousing, Arbeitsbericht, Institut für Wirtschaftsinformatik, Universität St. Gallen, 2002.

Hafner 2005
Hafner, M.: Entwicklung einer Methode für das Management der Informationssystemarchitektur im Unternehmen, Dissertation, Universität St. Gallen, 2005.

Hafner/Winter 2005
Hafner, M., Winter, R.: Vorgehensmodell für das Management der unternehmensweiten Applikationsarchitektur, in: Ferstl, O.K., Sinz, E.J., Eckert, S., Isselhorts, T. (Hrsg.): Wirtschaftsinformatik 2005, Physica, Heidelberg, 2005, S. 627-646.

Haller 1986
Haller, M.: Risiko-Mangement – Eckpunkte eines integrierten Konzepts, in: Jacob, H. (Hrsg.): Schriften zur Unternehmensführung, Gabler, Wiesbaden, 1986, S. 7-43.

Hartje et al. 2003
Hartje, H., Probst, U., Jäck, K., Hessler, M.: SAP Berechtigungswesen – Design und Realisierung von Berechtigungskonzepten für SAP R/3 und SAP Enterprise Portal, Galileo Press, Bonn, 2003.

Helfert 2002
Helfert, M.: Planung und Messung der Datenqualität in Data-Warehouse-Systemen, Difo-Druck, Bamberg, 2002.

Herrmann 2006
Herrmann, C.: Referenzprozesse für die Wartung von Data-Warehouse-Systemen, Dissertation, Universität St. Gallen, 2006 (in Planung).

Herrmann et al. 2004
Herrmann, C., Schwinn, A., Zellner, G.: Referenzprozessmodellierung, Arbeitsbericht, Institut für Wirtschaftsinformatik, Universität St. Gallen, 2004.

Herwig/Schlabitz 2004
Herwig, V., Schlabitz, L.: Unternehmensweites Berechtigungsmanagement, in: Wirtschaftsinformatik, 46(2004)4, S. 289-294.

Heuer/Saake 2000
Heuer, A., Saake, G.: Datenbanken – Konzepte und Sprachen, mitp, Bonn, 2000.

Hevner et al. 2004
Hevner, A. R., March, S. T., Park, J.: Design Science in Information Systems Research, in: MIS Quarterly, 28(2004)1, S. 75-105.

Heym 1993
Heym, M.: Methoden-Engineering – Spezifikation und Integration von Entwicklungsmethoden für Informationssysteme, Dissertation, Universität St. Gallen, 1993.

Hochstein/Hunziker 2003
Hochstein, A., Hunziker, A.: Serviceorientierte Referenzmodelle des IT-Managements, in: HMD – Praxis der Wirtschaftsinformatik, 39(2003)232, S. 46-56.

Holznagel et al. 2003
Holznagel, B., Dietze, L., Kussel, S., Sonntag, M.: Recht der IT-Sicherheit, Beck, München, 2003.

Hoppe/Priess 2003
Hoppe, G., Priess, A.: Sicherheit von Informationssystemen – Gefahren, Massnahmen und Management im IT-Bereich, NWB, Herne, 2003.

IEEE 2000
IEEE: IEEE 1471-2000 – IEEE Recommended Practice for Architectural Description of Software Intensive Systems, Institute of Electrical and Electronical Engineers, 2000, http://www.idi.ntnu.no/~letizia/swarchi/IEEE1471.pdf (10.09.2005).

Imboden 1983
Imboden, C.: Risikohandhabung – Ein entscheidungsbezogenes Verfahren, Haupt, Bern, 1983.

IMG 1996
IMG: Promet PSI – Methodenhandbuch für die Prozess- und Systemintegration, Version 1.0, Information Management Group, St. Gallen, 1996.

IMG 1997
IMG: Promet BPR – Methodenhandbuch für den Entwurf von Geschäftsprozessen, Version 2.0, Information Management Group, St. Gallen, 1997.

IMG 2001
IMG: Promet STP – Methodenhandbuch für die System- und Technologieplanung, Version 1.1, Information Management Group, St. Gallen, 2001.

Initiative D21 2001
Initiative D21: IT-Sicherheitskriterien im Vergleich, 2001, http://www.initiatived21.de/druck/news/publikationen2002/doc/22_1053502380.pdf (17.02.2005).

ISACA 2000
ISACA: Control Objectives for Information and Related Technology (CobiT) Audit Guidelines, Information Systems Audit Control Association, 2000, http://www.isaca.org/cobit.htm (17.02.2005).

ISACA Switzerland Chapter 2001
ISACA Switzerland Chapter: Cobit – Der international annerkannte Standard für IT-Governance, Information Systems Audit and Control Association, Switzerland Chapter, 2001, http://www.isaca.ch/files/CobitBroschuere.pdf (15.07.2005).

ISF 2003
ISF: The Standard of Good Practice for Information Security, The Information Security Forum, 2003, http://www.isfsecuritystandard.com (01.05.2005).

ISO 1996a
ISO: ISO/IEC 10181-1 – Security Frameworks for Open Systems – Overview, International Organization for Standardization, 1996, http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=24404&ICS1=35&ICS2=100&ICS3=1 (12.06.2005).

ISO 1996b
ISO: ISO/IEC 10181-3 – Security Frameworks for Open Systems – Access Control Framework, International Organization for Standardization, 1996, http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=18199&ICS1=35&ICS2=100&ICS3=1 (30.09.2005).

ISO 1997
ISO: ISO/IEC TR 13335-2 – Guidelines for the Management of IT Security – Managing and Planning IT Security, International Organization for Standardization, 1997, http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=21755&ICS1=35&ICS2=40&ICS3=&scopelist= (12.08.2005).

ISO 1998
ISO: ISO/IEC TR 13335-3 – Guidelines for the Management of IT Security – Techniques for the Management of IT Security, International Organization for Standardization, 1998, http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=21756&scopelist= (30.09.2005).

ISO 2000a
ISO: ISO/IEC 17799 – Code of Practice for Information Security Management, geschützte Originalfassung, International Organization for Standardization, 2000, http://www.iso.ch/iso/en/prods-services/popstds/.../fr/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441&ICS1=35 (01.03.2004).

ISO 2000b
ISO: ISO/IEC 17799 – Code of Practice for Information Security Management, International Organization for Standardization, 2000, http://www.educationwarwick.com/SIMUInformation/Data%20Protection_BS%207799_2000.pdf (01.04.2004).

ISO 2004
ISO: ISO/IEC Directives – Part 2 – Rules for the Structure and Drafting of International Standards, International Organization for Standardization, 2004, http://isotc.iso.org/livelink/livelink/3656851/ISO_IEC_Directives__Part_2Rules_for_the_structure_and_drafting_of_International_Standards__2004__5th_edition___pdf_format_.pdf?func=doc.Fetch&nodeid=3656851 (01.09.2005).

IT Governance Institute 2004
IT Governance Institute: IT Control Objectives for Sarbanes-Oxley, 2004, http://www.isaca.org/Content/ContentGroups/Research1/Deliverables/IT_Control_Objectives_for_Sarbanes-Oxley_7july04.pdf (20.07.2005).

Jonscher/Dittrich 1994
Jonscher, D., Dittrich, K.: Realisierung von Sicherheitsstrategien mit Hilfe flexibler Zugriffskontrollmechanismen, in: Bauknecht, K., Dittrich, K. (Hrsg.): Sicherheit in Informationssystemen, vdf, Zürich, 1994, S. 23-52.

Jörg/Rossbach 2002
Jörg, M., Rossbach, P.: Messung und Bewertung operationeller Risiken, in: Rossbach, P., Locarek-Junge, H. (Hrsg.): IT-Sicherheitsmanagement in Banken, Bankakademie, Frankfurt am Main, 2002, S. 71-94.

Kaib 2002
Kaib, M.: Enterprise Application Integration – Grundlagen, Integrationsprodukte, Anwendungsbeispiele, Deutscher Universitäts-Verlag, Wiesbaden, 2002.

Keil et al. 1998
Keil, M., Cule, P. E., Lyytinen, K., Schmidt, R. C.: A Framework for Identifying Software Project Risks, in: Communications of the ACM, 41(1998)11, S. 76-83.

Kern 2002
Kern, A.: Advanced Features for Enterprise-Wide Role-Based Access Control, in: Proceedings of the 18th Annual Computer Security Applications Conference, Las Vegas, 2002, S. 333-343.

Kern et al. 2004a
Kern, A., Kuhlmann, M., Kuropka, R., Ruthert, A.: Ein Modell für die effiziente Administration applikatorischer Sicherheit, Arbeitskonferenz "Elektronische Geschäftsprozesse", Universität Klagenfurt, 2004, http://www.betasystems.de/g_beta.nsf/pdf/gdownload_presse04/$file/Artikel_EGP2004_BetaSystems.pdf (30.09.2005).

Kern et al. 2004b
Kern, A., Kuhlmann, M., Kuropka, R., Ruthert, A.: A Meta Model for Authorisations in Application Security Systems and Their Integration into RBAC Administration, in: Proceedings of the 9th ACM Symposium on Access Control Models and Technologies, Yorktown Heights, 2004, S. 87-96.

Kern et al. 2002
Kern, A., Kuhlmann, M., Schaad, A., Moffett, J. D.: Observations on the Role Life-Cycle in the Context of Enterprise Security Management, in: Proceedings of the 7th ACM Symposium on Access Control Models and Technologies, Monterey, 2002, S. 43-51.

Kersten 1995
Kersten, H.: Sicherheit in der Informationstechnik – Einführung in Probleme, Konzepte und Lösungen, 2. Auflage, Oldenbourg, München, 1995.

Klesse/Wortmann 2004
Klesse, M., Wortmann, F.: Erfolgsfaktoren der Applikationsintegration – Ergebnisse einer empirischen Studie, Arbeitsbericht, Institut für Wirtschaftsinformatik, Universität St. Gallen, 2004.

König et al. 1996
König, W., Heinzl, A., Rumpf, M., von Poblotzki, A.: Zur Entwicklung der Forschungsmethoden und Theoriekerne der Wirtschaftsinformatik in den nächsten zehn Jahren – Eine kombinierte Delphi- und AHP-Untersuchung, in: Heilmann, H., Heinrich, L.J., Roithmayer, F. (Hrsg.): Information Engineering, München, 1996, S. 36-65.

Konrad 1998
Konrad, P.: Geschäftsprozess-orientierte Simulation der Informationssicherheit – Entwicklung und empirische Evaluation eines Systems zur Unterstützung des Sicherheitsmanagements, Dissertation, Universität zu Köln, 1998.

Krallmann 2003
Krallmann, H.: Transformation einer industriell geprägten Unternehmensstruktur zur einer service-orientierten Organisation, Symposium "Herausforderungen der Wirtschaftsinformatik in der Informationsgesellschaft", Institut für Wirtschaftsinformatik, Universität Leipzig, 2003, http://www.iwi.uni-leipzig.de/d/institut/symposium/Krallmann-Leipzig-040203.pdf (30.09.2005).

Krasna et al. 1998
Krasna, M., Rozman, I., Stiglic, B.: How to Improve the Quality of Software Engineering Project Management, in: ACM SIGSOFT Software Engineering Notes, 23(1998)3, S. 120-125.

Kremer 2004
Kremer, S.: Information Retrieval in Portalen – Gestaltungselemente, Praxisbeispiele und Methodenvorschlag, Dissertation, Universität St. Gallen, 2004.

Kuhlmann 2005
Kuhlmann, M.: Geschäftsorientiertes Provisioning mit Regeln und Rollen, Identity Management Day 2005, Frankfurt am Main, 2005, http://www.uspmarcom.de/itverlag/IdM05/documents/BetaSystemsProvisioningmitRegelnundRollen_MartinKuhlmann.pdf (12.09.2005).

Kuhlmann et al. 2003
Kuhlmann, M., Shohat, D., Schimpf, G.: Role Mining – Revealing Business Roles for Security Administration Using Data Mining Technology, in: Proceedings of the 8th ACM Symposium on Access Control Models and Technologies, Como, 2003, S. 179-186.

Laing/Forzi 2003
Laing, P., Forzi, T.: IT-Risikomanagement in dynamischen und flexiblen Wertschöpfungsnetzwerken, in: Uhr, W., Esswein, W., Schoop, E. (Hrsg.): Wirtschaftsinformatik 2003, Band 1, Physica, Heidelberg, 2003, S. 101-123.

Lange 2004
Lange, J.: Sicherheit als notwendige Eigenschaft computergestützter Informationssysteme – Betrachtungsgegenstand und Grundlagen, Arbeitsbericht, Lehrstuhl für Wirtschaftsinformatik, Ruhr-Universität Bochum, 2004.

Lau/Gerhardt 1994
Lau, B., Gerhardt, W.: Ein rollenbasiertes unternehmensbezogenes Rechteverwaltungs-Paradigma, in: Bauknecht, K., Teufel, S. (Hrsg.): Sicherheit in Informationssystemen, vdf, Zürich, 1994, S. 53-89.

Lichter et al. 1993
Lichter, H., Schneider-Hufschmidt, M., Züllighoven, H.: Prototyping in Industrial Software Projects – Bridging the Gap between Theory and Practice, in: Proceedings of the 15th International Conference on Software Engineering, Baltimore, 1993, S. 221-229.

Lippold 1992
Lippold, H.: Informationssicherheit, in: Frese, E. (Hrsg.): Handwörterbuch der Organisation, 3. Auflage, Poeschel, Stuttgart, 1992, S. 912-922.

Lorek 2003
Lorek, J.: GENERALI-Identity-Management mit Siemens DirXmetaRole, GENERALI (Schweiz) Holding, Adliswil, 2003.

Lorek 2004
Lorek, J.: GENERALI-Identity-Management mit Siemens DirXmetaRole, JUSTSAVE Management Club, München, 2004.

Marent 1995
Marent, C.: Branchenspezifische Referenzmodelle für betriebswirtschaftliche IV-Anwendungsbereiche, in: Wirtschaftsinformatik, 37(1995)3, S. 303-313.

NIST 2002
NIST: Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology, 2002, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (12.07.2004).

NSW GCIO 2003a
NSW GCIO: Information Security Guideline for NSW Government – Part 1 – Information Security Risk Management, New South Wales Government Chief Information Office, 2003, http://www.oit.nsw.gov.au/pdf/4.4.16.IS1.pdf (19.09.2005).

NSW GCIO 2003b
NSW GCIO: Information Security Guidelines for NSW Government, New South Wales Government Chief Information Office, 2003, http://www.oict.nsw.gov.au/content/2.3.a.guidelines.asp (19.09.2005).

NSW GCIO 2003c
NSW GCIO: Return on Investment for Information Security, New South Wales Government Chief Information Office, 2003, http://www.oict.nsw.gov.au/content/7.1.15.ROSI.asp (19.09.2005).

Oppliger 1997
Oppliger, R.: IT-Sicherheit – Grundlagen und Umsetzung in der Praxis, Vieweg, Braunschweig, 1997.

Ortner 1997
Ortner, E.: Methodenneutraler Fachentwurf – Zu den Grundlagen anwendungsorientierter Informatik, B.G. Teubner Verlagsgesellschaft, Stuttgart, 1997.

Österle/Blessing 2003
Österle, H., Blessing, D.: Business Engineering Modell, in: Österle, H., Winter, R. (Hrsg.): Business Engineering – Auf dem Weg zum Unternehmen des Informationszeitalters, 2. Auflage, Springer, Berlin, 2003, S. 65-86.

Österle/Winter 2003
Österle, H., Winter, R.: Business Engineering, in: Österle, H., Winter, R. (Hrsg.): Business Engineering – Auf dem Weg zum Unternehmen des Informationszeitalters, 2. Auflage, Springer, Berlin, 2003, S. 3-20.

Pernul 1995
Pernul, G.: Information Systems Security – Scope, State-of-the-art and Evaluation of Techniques, in: International Journal of Information Management, 15(1995)3, S. 239-255.

Petruch 2002
Petruch, K.: IT-Sicherheit – Definitiv mehr als nur Technik, in: Rossbach, P., Locarek-Junge, H. (Hrsg.): IT-Sicherheitsmangement in Banken, Bankakademie, Frankfurt am Main, 2002, S. 277-292.

Phillipp 1976
Phillipp, F.: Risiko und Risikopolitik, in: Grochla, E., Wittmann, W. (Hrsg.): Handwörterbuch der Betriebswirtschaft, Schäffer-Poschel, Stuttgart, 1976, S. 3453-3460.

Pipkin 2000
Pipkin, D. L.: Information Security – Protecting the Global Enterprise, Prentice Hall PTR, Upper Saddle River, 2000.

Pohl/Weck 1993
Pohl, H., Weck, G.: Stand und Zukunft der Informationssicherheit, in: Datenschutz und Datensicherung, 17(1993)1, S. 18-22.

Raepple 2001
Raepple, M.: Sicherheitskonzepte für das Internet – Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, 2. Auflage, dpunkt, Heidelberg, 2001.

Reichmann/Lachnit 1976
Reichmann, T., Lachnit, L.: Planung, Steuerung und Kontrolle mit Hilfe von Kennzahlen, in: Zeitschrift für betriebswirtschaftliche Forschung, 28(1976)5, S. 705-723.

Roeckle 1999
Roeckle, H.: Rollenbasierter Zugriffsschutz – Automatisierte Bildung der Rollen im Unternehmen auf der Basis eines prozessorientierten Vorgehensmodells, in: IT-Sicherheit, 5(1999)1, S. 25-34.

Roeckle et al. 2000
Roeckle, H., Schimpf, G., Weidinger, R.: Process-Oriented Approach for Role-Finding to Implement Role-Based Security Administration in a Large Industrial Organization, in: Proceedings of the 5th ACM Workshop on Role-Based Access Control, Berlin, 2000, S. 103-110.

Röhm 2000
Röhm, A. W.: Sicherheit offener Elektronischer Märkte – Modellbildung und Realisierungskonzept, Dissertation, Universität Essen, 2000.

Rolf 1998
Rolf, A.: Grundlagen der Organisations- und Wirtschaftsinformatik, Springer, Berlin, 1998.

Rosemann/zur Mühlen 1997
Rosemann, M., zur Mühlen, M.: Modellierung der Aufbauorganisation in Workflow-Management-Systemen – Kritische Bestandsaufnahme und Gestaltungsvorschläge, in: Proceedings EMISA-Fachgruppentreffen 1997, Darmstadt, 1997, S. 100-118.

Rosenberg 1992
Rosenberg, R. S.: The Social Impact of Computers, Academic Press, San Diego, 1992.

Rupprecht 2002
Rupprecht, J.: Datensicherheit im Data Warehousing – Grundlagen, Zugriffskontrolle, Fallbeispiele, Arbeitsbericht, Institut für Wirtschaftsinformatik, Universität St. Gallen, 2002.

Samarati/de Capitani di Vimercati 2002
Samarati, P., de Capitani di Vimercati, S.: Access Control – Policies, Models and Mechanisms, in: Focardi, R., Gorrieri, R. (Hrsg.): Foundations of Security Analysis and Design – Tutorial Lectures, Springer, Berlin, 2002, S. 137-196.

Sandhu 1996
Sandhu, R.: Roles versus Groups, in: Proceedings of the 1st ACM Workshop on Role-Based Access Control, Gaithersburg, 1996, S. 25-27.

Sandhu/Samarati 1994
Sandhu, R., Samarati, P.: Access Control – Principles and Practice, in: IEEE Communications Magazine, 32(1994)9, S. 40-48.

Schätzle et al. 2002
Schätzle, R., Seifert, T., Kleine-Gung, J.: Enterprise Java Beans – Kritische Betrachtungen zu einer modernen Software-Architektur, in: Wirtschaftsinformatik, 44(2002)3, S. 217-244.

Schelp 2003
Schelp, J.: Proposal Kompetenzzentrum Integration Factory, Institut für Wirtschaftsinformatik, Universität St. Gallen, 2003.

Schneider 2000
Schneider, J.: Sicherheit von Anwendungssystemen im Intranet und Internet, in: HMD – Praxis der Wirtschaftsinformatik, 37(2000)216, S. 92-100.

Schulte 1997
Schulte, M.: Bank-Controlling II – Risikopolitik in Kreditinstituten, Bankakademie, Frankfurt am Main, 1997.

Schulte-Zurhausen 1999
Schulte-Zurhausen, M.: Organisation, 2. Auflage, Vahlen, München, 1999.

Schütte 1998
Schütte, R.: Grundsätze ordnungsmässiger Referenzmodellierung, Gabler, Wiesbaden, 1998.

Schwegmann 1999
Schwegmann, A.: Objektorientierte Referenzmodellierung – Theoretische Grundlagen und praktische Anwendung, Gabler, Wiesbaden, 1999.

Schweizer 1999
Schweizer, A.: Data Mining, Data Warehousing – Datenschutzrechtliche Orientierungshilfen für Privatunternehmen, Orell Füssli, Zürich, 1999.

Schwinn 2005
Schwinn, A.: Entwicklung einer Methode zur Applikationsintegration in heterogenen Informationssystemen, Dissertation, Universität St. Gallen, 2005 (in Vorbereitung).

Schwinn/Hagen 2006
Schwinn, A., Hagen, C.: Measured Integration – Metriken für die Integrationsarchitektur, in: Schelp, J., Winter, R. (Hrsg.): Integrationsmanagement, Springer, Berlin, 2006, S. 267-292.

Senger/Österle 2004
Senger, E., Österle, H.: Promet Business Engineering Case Studies (BECS), Version 2.0, Arbeitsbericht, Institut für Wirtschaftsinformatik, Universität St. Gallen, 2004.

Seufert 2001
Seufert, S.: Die Zugriffskontrolle, Dissertation, Otto-Friedrich-Universität Bamberg, 2001.

Seufert 2002
Seufert, S.: Der Entwurf strukturierter rollenbasierter Zugriffskontrollmodelle, in: Informatik – Forschung und Entwicklung, 17(2002)1, S. 1-11.

Siegrist 2003
Siegrist, E.: Architekturmanagement in der Credit Suisse, 12. St. Galler Anwenderforum, St. Gallen, 2003, http://forum.iwi.unisg.ch/downloads/forum/12/7_Siegrist.zip (1.12.2004).

Sinz 1999
Sinz, E. J.: Architektur von Informationssystemen, in: Rechenberg, P., Pomberger, G. (Hrsg.): Informatik-Handbuch, 2. Auflage, Hanser, München, 1999, S. 1035-1046.

Stahlknecht/Hasenkamp 1999
Stahlknecht, P., Hasenkamp, U.: Einführung in die Wirtschaftsinformatik, Springer, Berlin, 1999.

Stelzer 1990
Stelzer, D.: Kritik des Sicherheitsbegriffs im IT-Sicherheitsrahmenkonzept, in: Datenschutz und Datensicherung, 14(1990)10, S. 501-506.

Teubner 1997
Teubner, A.: Organisations- und Informationssystemgestaltung – Theoretische Grundlagen und integrierte Methoden, Gabler, Wiesbaden, 1997.

Theil 1995
Theil, M.: Risikomanagement für Informationssysteme, Dissertation, Wirtschaftsuniversität Wien, 1995.

Turowski 2001
Turowski, K.: Spezifikation und Standardisierung von Fachkomponenten, in: Wirtschaftsinformatik, 43(2001)3, S. 269-281.

Ulrich 1984
Ulrich, H.: Management, Haupt, Bern, 1984.

Vieting/Kumpf 2002
Vieting, M., Kumpf, J.: Prozessbasierte Gestaltung von (Aufbau-)Organisation und Berechtigungskonzept am Beispiel SAP R/3, in: Becker, J., Kugeler, M., Rosemann, M. (Hrsg.): Prozessmanagement, 3. Auflage, Springer, Berlin, 2002, S. 411-435.

vom Brocke 2003
vom Brocke, J.: Referenzmodellierung – Gestaltung und Verteilung von Konstruktionsprozessen, Logos, Berlin, 2003.

von Rössing 2005
von Rössing, R.: Betriebliches Kontinuitätsmanagement, mitp, Bonn, 2005.

Vossbein 2002
Vossbein, R.: Auditierung und Zertifizierung – Ein Weg zu sicheren Systemen, in: Rossbach, P., Locarek-Junge, H. (Hrsg.): IT-Sicherheitsmanagement in Banken, Bankakademie, Frankfurt am Main, 2002, S. 23-36.

Winter et al. 2003
Winter, M., Herrmann, C., Helfert, M.: Datenqualitätsmanagement für Data-Warehouse-Systeme – Technische und organisatorische Realisierung am Beispiel der Credit Suisse, in: von Maur, E., Winter, R. (Hrsg.): Data Warehouse Management, Springer, Heidelberg, 2003, S. 221-240.

Winter 2002
Winter, R.: Informationsmanagement, in: Dubs, R., Euler, D., Rüegg-Stürm, J. (Hrsg.): Einführung in die Managementlehre, Pilotversion, Haupt, Bern, 2002, S. 929-969.

Winter 2003a
Winter, R.: An Architecture Model for Supporting Application Integration Decisions, Proceedings of the 11th European Conference on Information Systems, Neapel, 2003, http://web.iwi.unisg.ch/org/iwi/iwi_pub.nsf/wwwPublAuthorGer/E0B96DE31441FF22C1256D09004D73A1/$file/ecis2003.pdf (12.11.2005).

Winter 2003b
Winter, R.: Modelle, Techniken und Werkzeuge im Business Engineering, in: Österle, H., Winter, R. (Hrsg.): Business Engineering – Auf dem Weg zum Unternehmen des Informationszeitalters, 2. Auflage, Springer, Berlin, 2003, S. 87-118.

Winter 2004a
Winter, R.: Ein Modell zur Visualisierung der Anwendungslandschaft als Grundlage der Informationssystem-Architekturplanung, Arbeitspapier, Institut für Wirtschaftsinformatik, Universität St. Gallen, 2004.

Winter 2004b
Winter, R.: Unternehmensarchitektur und Integrationsmanagement für Finanzdienstleister, Arbeitspapier, Institut für Wirtschaftsinformatik, Universität St. Gallen, 2004.

Winter/Schelp 2005
Winter, R., Schelp, J.: Dienstorientierung im Business Engineering, in: HMD – Praxis der Wirtschaftsinformatik, 41(2005)241, S. 45-55.

Winterthur Group 2005
Winterthur Group: Geschäftsbericht 2005, Winterthur, 2005.

Wolf/Runzheimer 2000
Wolf, K., Runzheimer, B.: Risikomanagement und KonTraG, 2. Auflage, Gabler, Wiesbaden, 2000.

Wolf/Runzheimer 2003
Wolf, K., Runzheimer, B.: Risikomanagement und KonTraG, 4. Auflage, Gabler, Wiesbaden, 2003.

Wortmann 2004
Wortmann, F.: Integrationsinfrastrukturen in der Finanzdienstleistungsbranche – Rahmenbedingungen und Entwicklungen, Arbeitsbericht, Institut für Wirtschaftsinformatik, Universität St. Gallen, 2004.

Zarnekow et al. 2004
Zarnekow, R., Brenner, W., Grohmann, H.: Informationsmanagement – Konzepte und Strategien für die Praxis, dpunkt, Heidelberg, 2004.

Zentrum für sichere Informationstechnologie – Austria 2004
Zentrum für sichere Informationstechnologie – Austria: Österreichisches IT-Sicherheitshandbuch – IT-Sicherheitsmanagement, 2004, http://www.a-sit.at/unterstuetzung/sicherheitshdb/OE-IT-SIHB_Teil1.pdf (17.02.2005).

Lebenslauf

Persönliche Angaben

Vorname, Name	Felix Wortmann
Geburtsdatum	18. Februar 1977
Geburtsort	Münster (Deutschland)

Schulische und universitäre Ausbildung

09/1983-06/1987	Ludgeri-Grundschule, Lüdinghausen
08/1987-06/1996	St. Antonius Gymnasium, Lüdinghausen
10/1997-03/2002	Wirtschaftsinformatikstudium an der Westfälischen Wilhelms-Universität Münster
08/1999-12/1999	University of Alabama, Tuscaloosa Al, USA
05/2002-11/2005	Doktorandenstudium an der Universität St. Gallen, Institut für Wirtschaftsinformatik

Berufliche Tätigkeiten

08/1996-08/1997	Zivildienst am Ruderverein Münster von 1882
1996-2000	Diverse Tätigkeiten im Bereich Beratung und Softwareentwicklung
05/2002-11/2005	Wissenschaftlicher Mitarbeiter am Institut für Wirtschaftsinformatik der Universität St. Gallen, Lehrstuhl Prof. Dr. Robert Winter