Universität Hamburg
Fakultät Wirtschafts- und Sozialwissenschaften
Department Wirtschaft und Politik
Masterstudiengang Daten- und Informationsmanagement

Master Thesis
zur Erlangung des Grades
Master of Arts/Daten- und Informationsmanagement

Geschäftsprozessmodell-basiertes Management operationeller Risiken am Beispiel der CONRAD HINRICH DONNER BANK AG

Erstprüfer:	Prof. Dr. Markus Nüttgens
Zweitprüfer:	Prof. Dr. Gerhard Brosius
Verfasser:	Hans-Christian Wegner
	Wietreie 45
	22359 Hamburg
	dimand@gmx.net
Matrikel-Nr.:	15760
Abgabe:	22.03.2006

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

AG	Aktiengesellschaft
AktG	Aktiengesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
CHD	CONRAD HINRICH DONNER BANK AG
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CRSA	Control & Risk Self Assesment
eEPK	erweiterte Ereignisgesteuerte Prozesskette
engl.	englisch
EPK	Ereignisgesteuerte Prozesskette
ETA	Event Tree Analysis
EU	Europäische Union
FMEA	Fehlermöglichkeits- und Einflussanalyse
FTA	Fault-Tree-Analysis
GoM	Grundsätze ordnungsmäßiger Modellierung
HAZOP	Hazard and Operability Study
HGB	Handelsgesetz
HTML	Hypertext Markup Language
i.e.S.	im engeren Sinne
IdW	Institut der Wirtschaftsprüfer in Deutschland
IT	Informationstechnologie
KCI	Key Control Indicator
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KPI	Key Performance Indicator
KRI	Key Risk Indicator
KWG	Kreditwesengesetz
LAN	Local Area Network
lat.	lateinisch
MaH	Mindestanforderungen an das Betreiben der Handelsgeschäfte
MaIR	Mindestanforderungen an die Ausgestaltung der Internen Revision
MaK	Mindestanforderungen an das Kreditgeschäft
MaRisk	Mindestanforderungen an das Risikomanagement
max.	maximal
Mio.	Million

Mrd.	Milliarde
PAAG	Prognose-Auffinden-Ausmerzen-Gegenmaßnahmen
PHEA	Predictive Human Error Analysis
PIF	Performance-influencing factor
REFA	Reichsausschuss für Arbeitszeitermittlung
SEC	Securities and Exchange Commission
SOX	Sarbanes-Oxley Act
WAN	Wide Area Network
WpHG	Wertpapierhandelsgesetz

1. Einleitung

1.1 Problemstellung und Zielsetzung

Banken sehen sich mit verschiedenen Herausforderungen konfrontiert. Zwei dieser Herausforderungen bilden den Ausgangspunkt der Problemstellung dieser Master Thesis. So sind Banken durch eine Vielzahl von Bestimmungen in zunehmendem Maße dazu verpflichtet, operationelle Risiken in ihr Risikomanagement einzubeziehen. Mögliche Ursachen für das operationelle Risiko sind die Unangemessenheit oder das Versagen von internen Verfahren, Menschen und Systemen sowie externe Ereignisse.[1]

Gleichzeitig verschärft sich der Konkurrenzdruck zwischen den Banken. Die Folge sind sinkende Gewinne. Diesen suchen Banken nach innen gerichtet durch Einsparungen und nach außen gerichtet durch eine stärkere Orientierung an den Bedürfnissen der Kunden zu begegnen. Als Organisationsform, mit der sich beide Richtungen vereinen lassen, gewinnt die Prozessorganisation mehr und mehr an Bedeutung.[2] Bei der Prozessorganisation steht der optimale Ablauf der Prozesse im Mittelpunkt der Strukturierung des Unternehmens. Basis der Prozessorganisation sind Geschäftsprozessmodelle, in denen Prozesse Software-gestützt graphisch abgebildet werden. In derartigen Modellen lassen sich auch die Abhängigkeiten der Prozesse von Menschen und Systemen visualisieren. Daher eignen sie sich ebenso als Basis einer Analyse der Prozesse auf operationelle Risiken.

Hintergrund dieser Arbeit ist ein Projekt, das in der CONRAD HINRICH DONNER BANK AG (CHD) durchgeführt wurde. In diesem Projekt wurde die Zielsetzung verfolgt, ein Konzept zu entwerfen und zu validieren, welches es der Bank erlaubt, ihre existenziellen Prozesse derart zu modellieren, dass die Prozessmodelle eine geeignete Basis für das Management operationeller Risiken darstellen. Kann ein existenzieller Prozess für einen bestimmten Zeitraum nicht durchgeführt werden, sind für die Bank existenzbedrohende Konsequenzen zu erwarten. Für Banken sind die Risiken, die sich aus der Nutzung von Informationstechnologie (IT) ergeben, der zentrale Bestandteil der operationellen Risiken.[3] Daher wurde sich in der entwickelten Lösung auf derartige Risiken konzentriert.

Entsprechend besteht die Zielsetzung der vorliegenden Arbeit darin, nach einer Einführung in die Thematik ein geeignetes Konzept für ein Geschäftsprozess-basiertes Mana-

[1] Vgl. Baseler Ausschuss (2004a), S.157.
[2] Vgl. Becker/Meise (2005), S.119 f.
[3] Vgl. Hirschmann/Romeike (2004).

gement operationeller Risiken zu finden bzw. zu entwerfen und das Ergebnis zu dokumentieren.
Es ist keine Zielsetzung der Arbeit, auf die Quantifizierung möglicher Verluste aus operationellen Risiken einzugehen. Auch wird es kein Gegenstand der Arbeit sein, anhand von Prozessmodellen Optimierungspotenziale in der betrachteten Bank aufzuzeigen. Gleichwohl sei an dieser Stelle auf die generelle Möglichkeit der Generierung von Synergieeffekten bei einer Verbindung eines prozessorientierten Ansatzes für das Management operationeller Risiken mit den Vorteilen der Prozessorganisation hingewiesen.

1.2 Gang der Untersuchung

Im zweiten Kapitel wird mit der Definition der Begriffe Risiko und operationelles Risiko für deren eindeutiges Verständnis gesorgt. Es wird beschrieben, worin die Ziele des Risikomanagements liegen und auf welche Art und Weise es diese Ziele verfolgt.
Im dritten Kapitel wird erörtert, was speziell für Banken die Gründe sind, operationelle Risiken zu managen. Die Gründe lassen sich in drei Gruppen unterteilen. Entsprechend werden im ersten Teil des Kapitels ausgewählte Verlustfälle aus dem Bankensektor beschrieben. Die Vielzahl spektakulärer Verlustfälle insbesondere im Bankensektor hat dazu geführt, dass in zahlreiche für Banken geltende Regelwerke mehr oder weniger ausdrücklich die Verpflichtung zum Management operationeller Risiken aufgenommen wurde. Um welche Regelwerke es sich dabei handelt und welche Bestimmungen in ihnen getroffen werden, wird im zweiten Teil des Kapitels untersucht. Im dritten Teil wird ein weiterer Beweggrund thematisiert, demzufolge die Verpflichtung zum Management operationeller Risiken Banken gleichzeitig die Chance eröffnet, die Vorteile der Prozessorganisation zu nutzen.
Im vierten Kapitel werden die Grundlagen der Prozessorganisation dargelegt. Dafür wird zunächst auf Unzulänglichkeiten der klassischen Organisationsgestaltung eingegangen, bevor die Begriffe Prozess und Geschäftsprozess definiert und die Idee sowie die Ziele der Prozessorganisation beschrieben werden. Welche Aktivitäten zu einem Prozess zusammengefasst werden, beruht z.T. auf der subjektiven Sichtweise des Organisationsgestalters. Um einen Eindruck zu vermitteln, welche Überlegungen hierbei eine Rolle spielen können, wird auf Ansätze zur Klassifizierung von Prozessen eingegangen. Nach der Beschreibung der Merkmale eines Prozesses wird geklärt, warum Prozessmo-

delle die geeigneteste Form der Darstellung eines Prozesses sind. Im letzten Teil des Kapitels werden Grundlagen der Geschäftsprozessmodellierung vermittelt.

Das fünfte Kapitel beschreibt mehrere in der Literatur diskutierte Ansätze für das Management operationeller Risiken auf der Basis von Geschäftsprozessen. Ausgangspunkt dieser Ansätze sind Geschäftsprozessmodelle, die für ein eindeutiges Verständnis der betrachteten Prozesse sorgen. Das ursprüngliche Einsatzgebiet dieser Ansätze ist nicht die Bankenbranche, weshalb für jeden Ansatz eine Bewertung hinsichtlich seiner Eignung für den Einsatz in Banken vorgenommen wird.

Kapitel sechs beschreibt den in der CONRAD HINRICH DONNER BANK AG verfolgten Ansatz. Zuerst wird die Ausgangssituation bei der Entwicklung des Ansatzes beschrieben. Als Muster für die Vorgehensweise bei dessen Entwicklung diente das IT-Grundschutzhandbuch, weshalb dessen hierfür relevante Inhalte im zweiten Teil des Kapitels kurz zusammengefasst werden. Im dritten Teil wird die Vorgehensweise bei der Entwicklung des Konzepts und dessen Aufbau erklärt. Der vierte Teil enthält die Ergebnisse einer Evaluation von Geschäftsprozessmodellierungswerkzeugen, in der deren Eignung für die Implementierung des Konzepts untersucht wurde.

Das siebte Kapitel fasst die Ergebnisse der Arbeit zusammen und zeigt Möglichkeiten zur Weiterentwicklung des Konzepts auf.

2. Definition Risiko, operationelles Risiko und Risikomanagement

Um operationelle Risiken managen zu können, ist es unerlässlich, über eine exakte Definition des operationellen Risikos zu verfügen. Nach einer allgemeinen Definition für den Begriff Risiko im ersten Unterkapitel soll diese Grundvoraussetzung im zweiten Teil des Kapitels geschaffen werden. Im dritten Teil wird skizziert, was die Ziele des Risikomanagements sind und es wird der Zyklus beschrieben, in dem das Risikomanagement agiert.

2.1 Definition Risiko

Bezüglich der Bedeutung des Begriffs Risiko selber existieren unterschiedliche Auffassungen, weshalb zunächst hier für ein einheitliches Verständnis gesorgt werden muss. Die in der Betriebswirtschaftslehre herrschenden Meinungen lassen sich auf zwei Grundrichtungen zurückführen, bei denen Risiko entweder aus einem ursachenbezogenen oder aus einem wirkungsbezogenen Blickwinkel heraus betrachtet wird. Da Ursachen und Wirkungen in einem direkten Zusammenhang stehen – Wirkungen resultieren aus Ursachen –, ergibt sich durch Verbindung der beiden Grundrichtungen die folgende, dieser Arbeit zugrunde liegende Risikodefinition:[4]

> *"Risiko resultiert ursachenbezogen aus der Unsicherheit zukünftiger Ereignisse – wobei dies regelmäßig mit einem unvollständigen Informationsstand einhergeht – und schlägt sich wirkungsbezogen in einer negativen Abweichung von einer festgelegten Zielgröße nieder."*[5]

Eine *festgelegte Zielgröße* kann sowohl ein erwarteter Gewinn, als auch ein erwarteter Verlust sein. Folglich handelt es sich bei der Realisation eines erwarteten Verlustes nicht um ein schlagend gewordenes Risiko. Hiervon ist erst die Rede, wenn der Verlust durch zufällige Abweichung vom Erwartungswert höher ausfällt, als ursprünglich erwartet. Ein Beispiel für erwartete Verluste ist die auf Erfahrungswerten basierende, prozentuale Ausfallrate am Kreditbestand einer Bank innerhalb eines Geschäftsjahres.[6] Die Tatsache, dass Erwartungen in Bezug auf die Höhe von Verlusten bestehen, impliziert,

[4] Vgl. Schulte/Horsch (2004), S.14 f.
[5] Schulte/Horsch (2004), S.15.
[6] Vgl. Büschgen (1998), S.866 f.

dass Verluste nicht nur einfach hingenommen werden, sondern dass sich bewusst mit ihnen auseinandergesetzt wird.[7] Dies geschieht im Rahmen des Risikomanagements.
Eine wesentliche Ursache für Risiko sind unvollständige Informationen bezüglich zukünftiger Ereignisse. Prognosen bezüglich externer Ereignisse lassen sich schwer anstellen. Aber es ist zumindest förderlich, sich interner Abläufe und möglicher Auswirkungen externer Ereignisse auf die innerbetriebliche Leistungserstellung bewusst zu sein. Auf dieser Basis können Szenarien entworfen werden, wie die Bank bestimmten Ereignissen ggf. antizipativ entgegentreten kann.

2.2 Definitionen für das operationelle Risiko

2.2.1 Residualdefinition für das operationelle Risiko

Einer gängigen Definition zur Folge werden unter operationellen Risiken diejenigen Risiken verstanden, die nicht Gegenpartei- oder Marktrisiken sind.[8] Ohne Kenntnis dessen, was Gegenpartei- und Marktrisiken sind, kann der Unwissende aus dieser Residualdefinition[9] lediglich schließen, dass Risiken in die drei Arten Gegenpartei-, Markt- und operationelle Risiken eingeteilt werden können.[10] Zum weiteren Verständnis müssen daher die beiden erstgenannten Risikoarten definiert werden.
Unter Gegenparteirisiken[11] werden diejenigen Risiken zusammengefasst, die mit der möglichen Zahlungsunfähigkeit eines Geschäftspartners verbunden sind, der in einem Kapitalüberlassungsverhältnis mit der Bank steht.[12] Derartigen Risiken sind Banken bei verschiedenen banktypischen Geschäften ausgesetzt, die es beinhalten, sie bewusst einzugehen. Vor allem im Kreditgeschäft ist dies der Fall, bei dem das Risiko des teilweisen oder vollständigen Ausfalls von Zins- und Tilgungszahlungen existiert (Kreditrisiko). Als weitere Ausprägungen der Gegenparteirisiken bestehen die Risiken, dass der Emittent einer Anleihe, die die Bank besitzt (Emittentenrisiko), oder der Kontrahent in einem Handelsgeschäft (Kontrahentenrisiko) im Verlaufe des Geschäfts zahlungsunfä-

[7] Vgl. Geiger/Piaz (2001), S.791.
[8] Vgl. Beeck/Kaiser (2000), S.637; vgl. Peter/Vogt/Kraß (2000), S.657; vgl. Geiger/Piaz (2001), S.791 f.
[9] Eine Residualdefinition sagt aus, wodurch das zu definierende Objekt *nicht* gekennzeichnet ist. Das zu definierende Objekt ist das Residuum, also der Rest. Das Gegenteil einer Residualdefinition ist eine Positivdefinition.
[10] Zu weiteren Klassifizierungsmöglichkeiten für Risiken vgl. Schierenbeck (2003), S.8.
[11] Vgl. Schierenbeck (2003), S.5. Eine andere gängige Bezeichnung ist *Ausfallrisiko*. Vgl. Schulte/Horsch (2004), S.27.
[12] Vgl. Schulte/Horsch (2004), S.27.

hig wird und seinen Verpflichtungen nicht nachkommt.[13] Die Gegenparteirisiken bilden mit geschätzten 50% den größten Anteil am Gesamtrisiko einer Bank.[14]
Marktrisiken[15] bestehen darin, dass sich Märkte, auf denen die Bank agiert, negativ für die Bank entwickeln können. Entsprechend kann es sich bei den Marktrisiken konkret um Aktienkurs-, Zinsänderungs-, Währungs-, Rohstoffpreis[16] und Derivatrisiken[17] handeln. Marktrisiken machen einen Anteil von ungefähr 10-30% des Gesamtrisikos aus. Die verbleibenden 20-40% des Gesamtrisikos einer Bank sind entsprechend dem operationellen Risiko zuzurechnen.[18]
Die Beschreibung der beiden nicht-operationellen Risikoarten war insoweit von Nutzen, als dass diese nun definiert sind. Für ein hinreichendes Verständnis für operationelle Risiken als Residualgröße konnten sie jedoch nicht sorgen, so dass hierfür Positivdefinitionen heranzuziehen sind.

2.2.2 Positivdefinition für das operationelle Risiko

Es existieren verschiedene Definitionen für das operationelle Risiko, die z.T. unterschiedliche Begriffe beinhalten. Weitere verwendete Bezeichnungen sind *betriebliche Risiken*, *Betriebsrisiken*, *Abwicklungsrisiken*, *operative Risiken* und *Operational Risk*[19], die nicht immer übereinstimmend verwendet werden. In dieser Arbeit wird ausschließlich der Terminus *operationelles Risiko* gebraucht.
Schulte/Horsch unterteilen die *operativen Risiken* in *Risiken im Finanzbereich* und *Risiken im Betriebsbereich*. Der Finanzbereich beinhaltet alle finanziellen Beziehungen einer Bank. Unter den Risiken im Betriebsbereich fassen Schulte/Horsch u.a. *Abwicklungs- bzw. Betriebsrisiken* zusammen, die aus Fehlern und Defiziten im technisch-organisatorischen und personellen Bereich herrühren. Diese Risiken setzen sie wiederum gleich mit dem *Operational Risk* gemäß der neuen Baseler Eigenkapitalvereinbarung (Basel II)[20], das laut der Übersetzung des Baseler Eigenkapitalakkords durch die Deutsche Bundesbank dem *operationellen Risiko* entspricht.[21]

[13] Vgl. Schulte/Horsch (2004), S.73.
[14] Vgl. Beeck/Kaiser (2000), S.650.
[15] Eine andere gängige Bezeichnung sind Preis- bzw. Preisänderungsrisiken, vgl. Schulte/Horsch (2004) S.27.
[16] Vgl. Schierenbeck (2003), S.5.
[17] Vgl. Geiger/Piaz (2001), S.794.
[18] Vgl. Beeck/Kaiser (2000), S.650.
[19] Vgl. Minz (2002), S.13.
[20] Vgl. Schulte/Horsch (2004), S.26 ff.
[21] Vgl. Basel (2004a), S.157; vgl. Basel (2004b), S.137.

Schierenbeck hingegen fasst unter den *operationellen Risiken* sowohl *operative* als auch *strategische Risiken* zusammen. Ihm zufolge lassen sich operative Risiken auf technische und auf verhaltensbedingte Ursachen zurückführen, wobei auch externe Ereignisse zu berücksichtigen sind, da sie die Ursache für technische Probleme sein können. Strategische Risiken bestehen aus dem Risiko fehlerhafter Managemententscheidungen und aus rechtlichen Risiken.[22]

In den Verlautbarungen des Baseler Ausschusses für Bankenaufsicht findet sich erstmals in dem im Januar 2001 veröffentlichten Konsultationspapier eine Definition für das operationelle Risiko.[23] Diese wurde im weiteren Verlauf der Konsultationen leicht modifiziert, so dass schließlich in der endgültigen Fassung der Neuen Baseler Eigenkapitalvereinbarung folgende Definition gegeben wird:

> *„Operationelles Risiko ist die Gefahr von Verlusten, die in Folge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder in Folge externer Ereignisse eintreten.“*[24]

Gemäß dem Baseler Ausschuss sind Rechtsrisiken zu den operationellen Risiken zu zählen, wohingegen strategische Risiken und Reputationsrisiken explizit nicht als solche betrachtet werden.[25]

Rechtsrisiken spielen für Banken eine wichtige Rolle, da es sich bei Bankleistungen um vertraglich fixierte, abstrakte Dienstleistungen handelt. Es kommt daher den den Leistungsbeziehungen zugrunde liegenden Verträgen eine weitaus wichtigere Rolle zu, als es bei sachlichen Leistungen der Fall wäre, deren Güte sich auch an den Sachen selber bemessen lässt. Es existieren zwei unterschiedliche Ausprägungen des Rechtsrisikos, die sich auf unterschiedliche Ursachen zurückführen lassen. Zum einen kann sich die Gesetzeslage ändern, was Folgen für bestehende, nunmehr auf veralteten rechtlichen Annahmen beruhenden, Verträge hätte. Zum anderen können Verträge fehlerhaft formuliert sein und damit gegen geltendes Recht verstoßen.[26]

Reputationsrisiken entstehen durch Vorfälle, die zu einer Verschlechterung der öffentlichen Meinung über die Bank führen. Sie können die Wirkung haben, dass entweder

[22] Vgl. Schierenbeck (2003), S.4.
[23] Vgl. Baseler Ausschuss (2001a), S.103.
[24] Baseler Ausschuss (2004a), S.157.
[25] Vgl. Baseler Ausschuss (2004a), S.157.
[26] Vgl. Büschgen (1998), S.890.

bestehende Kunden abwandern oder dass potentielle Neukunden es unterlassen, mit der Bank zu kontrahieren.

Die Baseler Definition für das operationelle Risiko ist ursachenbasiert. Es wurde eine derartige Definition gewählt, um den Banken das Herangehen an das Management operationeller Risiken zu erleichtern.[27] Aufgrund der Tatsache, dass sie bindenden Charakter für Banken hat, hat sie sich durchgesetzt[28] und wird als Definition für diese Arbeit herangezogen.

Zur Konkretisierung dieser für Banken neuen Risikoart werden vom Baseler Ausschuss mögliche Ursachen für auf operationelle Risiken zurückzuführende Schadensfälle genannt, die in die aus Abbildung 1 ersichtlichen sieben Kategorien unterteilt sind.

Kategorie	Beschreibung
Interner Betrug	Unbefugte oder kriminelle Handlungen von Mitarbeitern gegenüber der Bank
Externer Betrug	Handlungen mit betrügerischer Absicht von Dritten
Beschäftigungspraxis und Arbeitsplatzsicherheit	Verstöße gegen Beschäftigungs-, Gesundheits- oder Sicherheitsabkommen
Kunden, Produkte und Geschäftsgepflogenheiten	Unbeabsichtigte oder fahrlässige Nichterfüllung geschäftlicher Verpflichtungen gegenüber Kunden, mangelhafte Art oder Struktur eines Produktes
Sachschäden	Beschädigung oder Verlust von Sachvermögen
Geschäftsunterbrechungen und Systemausfälle	Ausfall von IT-Systemen oder Telekommunikation
Abwicklung, Vertrieb und Prozessmanagement	Fehler bei der Geschäftsabwicklung oder im Prozessmanagement

Abbildung 1: Unterteilung der Ursachen für operationelle Risiken in Kategorien
In Anlehnung an: Baseler Ausschuss für Bankenaufsicht (2004), Anhang 7, S.255 f.

Im Gegensatz zu den finanziellen Risikoarten Gegenpartei- und Marktrisiko, die mit den Finanzströmen einer Bank in Verbindung stehen, entstehen operationelle Risiken nicht im Wertebereich, sondern im Betriebsbereich einer Bank.[29] Eine wesentliche Ursache für Risiko im Allgemeinen ist gemäß der oben vorgestellten Risikodefinition ein unvollständiger Informationsstand bezüglich zukünftiger Ereignisse. Mit den Risikofaktoren interne Verfahren, Menschen und Systeme liegen die Ursachen operationeller Risiken in

[27] Vgl. Baseler Ausschuss (2001b), S.2.
[28] Vgl. Pillen/Kasprowicz/Knappstein (2004), S.564.
[29] Vgl. Schierenbeck (2001), S.4.

einem hohen Maße in Aspekten des internen Leistungsbereichs, womit diese Risikoart im Hinblick auf ihre drei möglichen internen Ursachen zumindest bis zu einem gewissen Grad von Banken selber gestaltet und beeinflusst werden kann. Eine so hohe Beeinflussbarkeit ist bei finanziellen Risiken nicht gegeben, da Banken hier von unternehmensexternen Ereignissen und Entwicklungen abhängig sind.[30]

Operationelle Risiken gehen zwangsläufig mit jeder wirtschaftlichen Aktivität einher und begleiten ein Unternehmen von dessen Gründung an.[31] Demzufolge werden sie nicht bewusst von der Bank eingegangen, um im Gegenzug eine Risikoprämie als Ertrag zu erwirtschaften, wie es sich bspw. bei dem Kreditrisiko und einer Kreditvergabe verhält. Da, ganz im Gegenteil, durch operationelle Risiken nur Verluste entstehen können, ist es das Ziel der meisten Banken, diese zu vermeiden oder auf Dritte zu transferieren.[32]

Innerhalb der operationellen Risiken ist zu unterscheiden zwischen „high-frequency – low-severity"-Risiken und „low-frequency – high-severity"-Risiken. Zur erstgenannten Kategorie sind bspw. Schäden zu zählen, die durch auf die Bank zurückzuführende Fehler bei der Ausführung von Überweisungsaufträgen entstehen. Sie treten in einer relativ hohen Frequenz auf, stellen jedoch in der Regel keine Existenzbedrohung für eine Bank dar. Dies ist dagegen bei den „low-frequency – high-severity"-Risiken der Fall, die relativ selten schlagend werden, dafür aber ein hohes Schadenspotential haben. Aufgrund ihrer Seltenheit ist es besonders schwer, mögliche Folgen zu quantifizieren, was die eigentliche Gefahr für die Bank darstellt.[33]

2.3 Risikomanagement

Wie oben bereits erwähnt, ist das Betreiben von Risikomanagement ein Ausdruck dessen, dass Risiken in einem Unternehmen nicht einfach hingenommen, sondern sich bewusst mit ihnen auseinandergesetzt wird. Dabei ist sicherzustellen, dass die Risiken, die eine Bank eingeht, tragbar sind. Dafür ist eine Gegenüberstellung der Risiken mit den Risikoträgern, also den Risikodeckungspotentialen, vorzunehmen. Aus dieser Gegenüberstellung ergibt sich mit dem Verhältnis zwischen Risiken und Risikodeckungspotentialen die so genannte Risikoposition einer Bank.[34]

[30] Vgl. Geiger/Piaz (2001), S.792.
[31] Vgl. Jovic/Piaz (2001), S.923.
[32] Vgl. Hartmann-Wendels/Pfingsten/Weber (2004), S.667 f.
[33] Vgl. Hartmann-Wendels/Pfingsten/Weber (2004), S.668.
[34] Vgl. Schulte/Horsch (2004), S.16.

Das Risikomanagement einer Bank „umfasst sämtliche Maßnahmen zur planmäßigen und zielgerichteten Analyse, Beeinflussung (Steuerung) und Kontrolle der Risikoposition“[35]. Die Verwendung des Adjektivs *planmäßig* soll deutlich machen, dass die Maßnahmen nicht nur sporadisch durchgeführt werden, sondern dass sie idealerweise fest im Managementprozess der Bank verankert sind. *Zielgerichtet* bedeutet, dass von Seiten der Unternehmensleitung Vorstellungen über eine Soll-Risikoposition bestehen, so dass aus dem Abgleich mit der Ist-Risikoposition ein eventueller Handlungsbedarf abgeleitet werden kann.
Das Risikomanagement besteht aus einem Zyklus, der aus den drei Phasen *Risikoanalyse*, *Risikosteuerung* und *Risikokontrolle* besteht.

<table>
<tr><th colspan="6">Risikomanagement</th></tr>
<tr><th colspan="2">Risikoanalyse</th><th colspan="2">Risikosteuerung</th><th colspan="2">Risikokontrolle</th></tr>
<tr><td>Risiko-bestimmung</td><td>Analyse i.e.S.</td><td>aktiv</td><td>passiv</td><td rowspan="2">Analyse-methoden</td><td>Genauigkeit</td></tr>
<tr><td>- Identifikation

- Klassi-fizierung</td><td>- Messung

- Beurteilung</td><td>- Risiko-vermeidung

- Risiko-verminderung

- Risiko-überwälzung

- Risiko-diversifikation</td><td rowspan="3">Risikoübernahme vor dem Hinter-grund der

- Risikotragfähig-keit der laufenden Geschäftstätigkeit

und der

- Risikovorsorge früherer Perioden</td><td>Aktualität</td></tr>
<tr><td rowspan="2">Steuerungs-instrumente</td><td>Kosten</td></tr>
<tr><td>Nutzen</td></tr>
<tr><td rowspan="2">organisator. Umsetzung</td><td>zentral</td></tr>
<tr><td>dezentral</td></tr>
</table>

Abbildung 2: Die drei Phasen des Risikomanagements
Quelle: Schulte (1994), S.57.

Am Beginn des Zyklus steht innerhalb der *Risikoanalyse* die Identifikation möglicher Risikoquellen. Nachdem Risiken identifiziert wurden, können sie den drei Risikoarten Gegenpartei-, Markt- oder operationelle Risiken zugeordnet werden. Dies ist wichtig, da unterschiedliche Risiken mit unterschiedlichen Instrumenten gesteuert werden. In der Analyse im engeren Sinne findet – wenn möglich und unter Kosten-/Nutzen-Gesichtspunkten sinnvoll – eine Quantifizierung der Risiken statt, die die anschließend stattfindende Bewertung der Tragfähigkeit der Risiken ermöglicht.
Die *Risikosteuerung* beinhaltet die Beeinflussung der Ist-Risikoposition, die sowohl auf aktive, wie auch auf passive Art und Weise vollzogen werden kann.

[35] Schulte/Horsch (2004), S.17.

Im Rahmen der aktiven Risikosteuerung können vier verschiedene Maßnahmen zum Einsatz kommen. Die *Risikovermeidung* führt dazu, dass risikobehaftete Geschäfte nicht oder nur in einem begrenzten Umfang getätigt werden. Die *Risikoverminderung* setzt entweder bei den Ursachen an, indem Eintrittswahrscheinlichkeiten für Schadensfälle verringert werden, oder sie begrenzt auf Seiten der Wirkungen das Ausmaß möglicher Schäden. Bei der *Risikoüberwälzung* werden Risiken durch Abschluss entsprechender Geschäfte auf Dritte übertragen. Die *Risikodiversifikation* bedient sich der Risikostreuung, um so für einen Ausgleich zwischen Risiken und Chancen auf Gesamtbankebene zu sorgen.

Unter passiver Risikosteuerung wird das bewusste Eingehen von Risiken unter der Voraussetzung einer hinreichenden Risikotragfähigkeit verstanden. Diese Risikotragfähigkeit kann sich aus den im laufenden Geschäft erwirtschafteten Risikoprämien oder aus der Risikovorsorge vorangegangener Perioden ergeben.

An die Risikosteuerung schließt sich die Phase der *Risikokontrolle* an. Hier werden die Ergebnisse der beiden vorangegangen Phasen auf ihre Wirksamkeit hin überprüft. Differenziert werden kann zwischen einer Kontrolle der angewandten Analysemethoden und Steuerungsmaßnahmen an sich und ihrer organisatorischen Umsetzung.[36] Abbildung 2 fasst die drei Phasen des Risikomanagements zusammen.

Im folgenden Kapitel wird dargelegt, warum operationellen Risiken in jüngster Zeit eine gesteigerte Beachtung im Bankensektor gefunden haben.

[36] Vgl. Schulte/Horsch (2004), S.15 ff.

3. Gründe für das Management operationeller Risiken in Banken

Ausgangspunkt der gestiegenen Bedeutung operationeller Risiken im Bankensektor ist eine Reihe von Verlustfällen, weshalb im ersten Teil dieses Kapitels ausgewählte Fälle beschrieben werden. Deren Folge war der Erlass bzw. die Verschärfung einiger rechtlicher Bestimmungen, die im zweiten Teil des Kapitels behandelt werden. Die dadurch gegebene Verpflichtung zum Management operationeller Risiken eröffnet Banken gleichzeitig die Möglichkeit, bei der Verfolgung prozessorientierter Ansätze Vorteile der Prozessorganisation zu nutzen. Dieser Aspekt wird im dritten Teil des Kapitels skizziert.

3.1 Verlustfälle im Bankensektor

Es existieren zahlreiche Verlustfälle im Bankensektor, die sich auf operationelle Risiken zurückführen lassen. Im Folgenden werden drei in Bezug auf Schadenshöhe, Ursachen und dem von ihnen erregten Aufsehen unterschiedliche Fälle beschrieben.

3.1.1 Barings Bank

1995 wurde mit der *Barings Bank* eines der ältesten Bankhäuser Englands insolvent. Die Ursache hierfür lag in Verlusten in Höhe von ca. 1,3 Mrd. US-Dollar, die von Nicholas Leeson, dem General Manager der Niederlassung in Singapur, im Rahmen von spekulativen Börsentermingeschäften angehäuft wurden[37], obwohl die Niederlassung zu derartigen Transaktionen seitens der Zentrale in London nicht legitimiert war.[38] Das eigentliche Kerngeschäft dieser Niederlassung wurde von der Zentrale als risikolos eingeschätzt und darin ist der Grund dafür zu sehen, dass ein nur geringer Informationsaustausch zwischen Singapur und London stattfand und dass Leeson gleichzeitig für den Handel sowie die Dokumentation und die Kontrolle seiner eigenen Handelsgeschäfte verantwortlich war. So war es ihm auch möglich, ein geheimes Konto einzurichten, auf dem er anfallende Verluste verbuchte und damit deren Existenz vertuschte.
Im Zeitraum von 1992 bis 1994 nahm der Saldo dieses Kontos stetig zu, während die Niederlassung gleichzeitig London gegenüber Gewinne bilanzierte, wobei sich bis zu diesem Zeitpunkt die Gewinne und die (vertuschten) Verluste in etwa deckten. Beweg-

[37] Vgl. Blattner (2003), S.19.
[38] Vgl. o.V. (2005).

grund für Leeson war, dass er über Boni an den Gewinnen beteiligt wurde und er folglich einen über den genannten Zeitraum hinweg ansteigenden Betrag an Boni erhielt, der im Jahre 1994 sein Grundgehalt um ein Vielfaches überstieg.[39]

Nach einem äußerst verlustreichen Geschäft Anfang 1995 flog der Betrug auf. Die Schadenssumme überstieg zu diesem Zeitpunkt das Eigenkapital der Barings Bank, so dass sie Insolvenz anmeldete. Weiterhin bemerkenswert ist, dass gemäß der Praxis der europäischen Bankenregulierung nur 25% Prozent des Eigenkapitals einer Bank in ein Geschäft hätte fließen dürfen. Zudem verfügte Leeson über keine Ausbildung, die ihn zu einer Tätigkeit im sehr komplexen Derivathandel angemessen qualifiziert hätte.[40]

Bei diesem Fall handelt es sich um ein klassisches „low-frequency – high-severity"-Risiko. Die Ursachen der Insolvenz der Barings Bank liegen gemäß der Baseler Definition des operationellen Risikos in den Faktoren *interne Verfahren*, *Systeme* und *Mensch*.

Als internes Verfahren erwies sich die interne Kontrolle als mangelhaft, da sie zuließ, dass Leeson seine eigenen Handelsaktivitäten kontrollierte. Die fehlende kritische Hinterfragung der hohen Gewinne von Seiten der Zentrale ist ebenfalls diesem Punkt zuzuordnen.[41]

Systemseitig hätte die Möglichkeit bestanden, eine Software einzusetzen, mit der ein Abgleich zwischen an Börsen getätigten Geschäften und den Posten in der Wertpapierabrechnung der Bank sowie zwischen den Kundenaufträgen und den tatsächlich getätigten Geschäften möglich gewesen wäre. So hätten Leesons Aktivitäten eher entdeckt werden können.[42]

Auf Seiten des Faktors Mensch ist die kriminelle Energie und die Geldgier von Leeson als eigentlicher Auslöser dieses Falls zu nennen, deren Entfaltung durch die anderen genannten Faktoren begünstigt wurde. Auch spielte Leesons mangelnde Qualifikation eine Rolle.

3.1.2 Bank of New York

Im November 1985 erlitt die *Bank of New York* geschätzte Verluste in Höhe von 4 Mio. US-Dollar als Folge eines Computerausfalls. Mit den betroffenen Systemen führte die Bank das Clearing amerikanischer Staatsanleihen für zahlreiche Banken und Händler durch, wofür sie zu jenem Zeitpunkt der größte Anbieter in den USA war. Als Folge des

[39] Vgl. Blattner (2003), S.19 f.
[40] Vgl. Blattner (2003), S.20.
[41] Vgl. Minz (2004), S.29.
[42] Vgl. King (2001), S.26 f.

Ausfalls konnte die Bank für einen Zeitraum von 28 Stunden keine Anleihen liefern und keine Zahlungen durchführen. Der Ausfall führte zudem zu kurzfristigen Verwerfungen auf Geld- und Warenmärkten.

Um ihren Zahlungsverpflichtungen für erhaltene Anleihen nachkommen zu können, nahm die Bank of New York für einen Tag den Betrag von 20 Mrd. US-Dollar von der amerikanischen Notenbank auf. Hierfür musste sie den oben genannten Betrag von 4 Mio. US-Dollar Zinsen zahlen. Dies war bis zu dem Zeitpunkt die höchste Summe, die in einem derartigen kurzfristigen Refinanzierungsgeschäft von der Notenbank ausgeliehen wurde.

Dadurch, dass die Bank gleichzeitig keine Zahlungen empfangen konnte, befanden sich für einen kurzen Zeitraum 20 Mrd. US-Dollar im Besitz von Banken, die gegenüber der Bank of New York Zahlungsverpflichtungen hatten. Hieraus resultierte eine gesunkene Nachfrage nach kurzfristigen Geldern am Interbankenmarkt, die wiederum dazu führte, dass hier der Zinssatz an dem betroffenen Tag von 8,375% auf 5,5% fiel.

Gleichzeitig führten Meldungen über die Probleme der Bank zu einem Anstieg der Preise für Platin um 3,7%, was als Ausdruck von Ängsten der Marktteilnehmer vor bevorstehenden Turbulenzen an den Kapitalmärkten gedeutet werden kann. An der *New York Mercantile Exchange* wurden an diesem Tag im Platin-Handel so viele Kontrakte abgeschlossen, wie an keinem anderen Tag in den 29 Jahren davor.[43]

Dieser Verlustfall ist der Ursache *Systeme* zuzuordnen, da er durch einen Systemausfall bedingt wurde. Die Auswirkungen von Ausfällen oder eingeschränkten Verfügbarkeiten von Systemen über gegebene Zeiträume auf bestimmte Prozesse der Bank lassen sich bis zu einem gewissen Grad kalkulieren. Die Analyse von Ausfallszenarien kann den Entscheidungsträgern in Banken wertvolle Erkenntnisse über die Angemessenheit von bestehenden Notfallplänen bzw. über die Notwendigkeit liefern, überhaupt solche Pläne aufzustellen. Der Notfallplan für ein System sollte der Wichtigkeit des Systems für die Prozesse der Bank entsprechen und damit den mit einem Ausfall verbundenen Schadenspotentialen angemessen sein. Besonderes Augenmerk ist den Systemen zuzuwenden, die an bankexistenziellen Prozessen beteiligt sind. Kann eine Bank einen solchen Prozess für einen bestimmten Zeitraum nicht durchführen, sind existenzbedrohende Folgen für die Bank zu erwarten.

[43] Vgl. Zweig/Sullivan (1985).

Gleichzeitig müssen die Entscheidungsträger jedoch nach Gesichtspunkten der Wirtschaftlichkeit handeln. Da Backup-Lösungen für Systeme teuer sein können, ist die Entscheidung über deren Einsatz wohlüberlegt zu treffen.[44]

3.1.3 Banque Paribas

Die französische *Banque Paribas* wurde im Frühjahr 1996 von der Rating-Agentur *Fitch* in Bezug auf ihre Kreditwürdigkeit kurzfristig abgewertet, wodurch sie nicht mehr das bestmögliche Rating innehatte. Begründet wurde dies zum einen mit Verlusten, die die Bank 1995 erwirtschaftet hatte, und zum anderen mit der Tatsache, dass das Risikomanagement der Bank nicht mehr dem breit gefächerten Geschäft der Bank angemessen gewesen sei. Eine derartige Abstufung des Ratings ist für eine Bank mit höheren Kosten bei der Refinanzierung verbunden, bei der die Bank ihren Gläubigern zur Kompensation ihrer verschlechterten Bonität höhere Zinssätze zahlen muss.[45]
In Bezug auf den Abstufungsgrund Risikomanagement handelt es sich damit um ein operationelles Risiko der Kategorie *interne Verfahren*, da die Rating-Agentur die im Risikomanagement zur Anwendung kommenden Verfahren für nicht angemessen gehalten hat.
In diesem Fall handelte es sich um das Management von Gegenpartei- und Marktrisiken[46], es ist aber auch denkbar, dass auf diesem Wege sich ein für nicht angemessen befundenes Management operationeller Risiken selbst als ein operationelles Risiko mit finanziellen Einbußen im Ergebnis einer Bank niederschlägt. Banken sollten daher ein Risikomanagement vorweisen können, das sowohl den Forderungen der Bankenaufsicht, als auch den Ansprüchen der Rating-Agenturen genügt.[47]
Um die Wahrscheinlichkeit des Auftretens derartiger Verlustfälle in der Zukunft zu verringern und um dafür zu sorgen, dass sie keine existenzbedrohenden Folgen für Banken haben, wurden entsprechende Regelungen erlassen.

3.2 Rechtliche Rahmenbedingungen

Was die rechtlichen Anforderungen an deutsche Banken hinsichtlich des Managements operationeller Risiken sind und in welchen Regelungen sie begründet sind, wird in die-

[44] Vgl. King (2001), S.30.
[45] Vgl. o.V. (1996).
[46] Vgl. o.V. (1996).
[47] Vgl. King (2001), S.30 f.; vgl. Book/Rudolph (2005), S.56.

sem Abschnitt der Arbeit untersucht. Dies geschieht aus zwei Gründen relativ ausführlich. Zum einen wurden mehrere Regelungen erst kürzlich erlassen bzw. verschärft, zum anderen sind einige Regelwerke dadurch gekennzeichnet, dass sie lediglich implizite Verweise auf das operationelle Risiko enthalten, die daher einer Interpretation bedürfen. In jedem der folgenden Unterkapitel wird eine Rechtsnorm allgemein beschrieben. Überdies werden die in ihr enthaltenen Verweise auf operationelle Risiken genannt und mit der oben gegebenen Definition für das operationelle Risiko in Verbindung gebracht.

3.2.1 Kreditwesengesetz (KWG)

Das Kreditwesengesetz (KWG) ist die bedeutendste gesetzliche Grundlage für die Bankenregulierung in der Bundesrepublik Deutschland.[48] Das Ziel des KWG besteht darin, „die Funktionsfähigkeit des Finanzsektors, der besonders vertrauensempfindlich ist, durch Gläubigerschutz zu sichern.“[49] Zur Verfolgung dieses Ziels werden den Banken qualitative und quantitative Rahmenbedingungen vorgegeben und sie werden verpflichtet, den Aufsichtsbehörden Einblick in ihre Bücher zu gewähren.[50] Diese Rahmenbedingungen grenzen die Möglichkeiten der Banken ein, Risiken einzugehen und damit ihre eigene Existenz und als Folge dessen die Einlagen ihrer Kunden zu gefährden.[51] Sie enthalten implizite Regelungen, die der Eingrenzung operationeller Risiken dienen.[52]
In §25a Abs.1 KWG wird Banken auferlegt, besondere Maßgaben bei der Gestaltung ihrer Organisation zu beachten, damit sie in der Lage sind, für sie geltende gesetzliche Bestimmungen umzusetzen. So sollen sie über eine angemessene Strategie verfügen, in der ausdrücklich die Risiken und das Eigenkapital der Bank berücksichtigt werden. Des Weiteren ist ein angemessenes internes Kontrollsystem einzurichten, dass sich insbesondere der Steuerung und Überwachung von Risiken widmet. Es ist dafür zu sorgen, dass jederzeit mit hinreichender Genauigkeit die finanzielle Lage der Bank festgestellt werden kann. Für den Einsatz elektronischer Datenverarbeitung sind angemessene Sicherheitsvorkehrungen zu treffen. Getätigte Geschäfte sind vollständig zu dokumentieren und je nach Art der Unterlagen sind diese für mindestens sechs Jahre für Überprüfungen der Aufsichtsbehörden aufzubewahren. Banken haben Sicherungssysteme für gegen sie gerichtete Betrugsfälle einzurichten. §25a Abs.2 KWG besagt, dass auch bei

[48] Vgl. Hartmann-Wendels/Pfingsten/Weber (2004), S.386.
[49] Deutsche Bundesbank (2005b).
[50] Vgl. Deutsche Bundesbank (2005b).
[51] Vgl. Hartmann-Wendels/Pfingsten/Weber (2004), S.386 f.
[52] Vgl. Minz (2004), S.42.

einer Auslagerung für das Bankgeschäft wesentlicher Bereiche auf andere Unternehmen sichergestellt sein muss, dass die Geschäfte ordnungsgemäß durchgeführt werden. Zudem muss für die Bank die Möglichkeit der Steuerung und Kontrolle sowie für die Aufsicht die Möglichkeit der Prüfung und Kontrolle bestehen. Gemäß §29 Abs.1 KWG wird die Einhaltung dieser Vorgaben bei der Prüfung des Jahresabschlusses vom Wirtschaftsprüfer kontrolliert.

Diese Regelungen zielen mit der Vielzahl der organisatorischen Vorgaben schwerpunktmäßig auf die Eindämmung der Risikoursache *interne Verfahren* ab. Ebenfalls adressiert wird die Ursache *Systeme*.

Dem §32 Abs.1 KWG kann entnommen werden, dass es für die Erteilung der Erlaubnis zum Betreiben von Bankgeschäften erforderlich ist, dass die Geschäftsleitung der Bank als zuverlässig erachtet werden kann und sie die nötige fachliche Eignung zur Führung einer Bank besitzt. Damit soll eine solide und umsichtige Führung der Bank sichergestellt werden. Außerdem ist es für die Erteilung der Erlaubnis notwendig, einen tragfähigen Geschäftsplan bei der Aufsichtsbehörde einzureichen, in dem die Art der geplanten Geschäfte, der organisatorische Aufbau und die internen Kontrollverfahren der Bank dargelegt werden.

Damit beziehen sich die Regelungen des §32 KWG ebenfalls auf die Risikoursachen *interne Verfahren* und *Systeme*. Zusätzlich wird hier im Vergleich zu §25a KWG auf die Ursache *Mensch* abgezielt.

3.2.2 Die Neue Baseler Eigenkapitalvereinbarung (Basel II)

Im Juni 2004 wurde die Neue Baseler Eigenkapitalvereinbarung (Basel II) verabschiedet, die bis Ende 2006 in nationales Recht umzuwandeln ist.[53] Mit der ersten Baseler Eigenkapitalvereinbarung (Basel I) von 1988 wurde die internationale Vereinheitlichung der bankenaufsichtlichen Eigenkapitalanforderungen erreicht. Ursprünglich war die Baseler Eigenkapitalvereinbarung nur an international tätige Banken gerichtet, sie hat sich jedoch faktisch als weltweiter Kapitalstandard für Banken etabliert.[54] Unter *Eigenkapitalanforderung* ist die Verpflichtung seitens der Banken zu verstehen, Risikodeckungspotential vorzuhalten, um auch in dem Fall solvent zu bleiben, in dem eine vorab errechnete Maximalbelastung aus schlagend werdenden Risiken eintritt. Die Be-

[53] Vgl. Deutsche Bundesbank (2005a).
[54] Vgl. Deutsche Bundesbank (2001), S.16.

rechnung dieses so genannten ökonomischen Kapitals bzw. Risikokapitals[55] berücksichtigt gemäß Basel I das Gegenpartei-, das Markt- sowie gemäß Basel II zusätzlich das operationelle Risiko. Basel II unterscheidet sich von den anderen vorgestellten Normen dadurch, dass es weniger auf das Vermeiden von Risiken abzielt, als vielmehr auf deren Hinterlegung mit Risikokapital. So soll verhindert werden, dass Risikoereignisse die Existenz von Banken bedrohen.

Das damit verfolgte Ziel, die Stabilität des Bankensystems noch besser abzusichern, soll durch Regelungen erreicht werden, die in drei Säulen gegliedert sind. Säule 1 enthält Mindestkapitalanforderungen an die Banken, Säule 2 regelt den Überprüfungsprozess durch die Bankenaufsicht und in Säule 3 finden sich Forderungen nach der erweiterten Offenlegung bestimmter Kerninformationen, die es den Marktteilnehmern erlauben sollen, sich ein Bild über die Angemessenheit der Kapitalunterlegung einer Bank zu machen. Insbesondere die ersten beiden Säulen enthalten im Hinblick auf das operationelle Risiko interessante Aussagen, weshalb sich die weiteren Ausführungen auf diese beschränken.

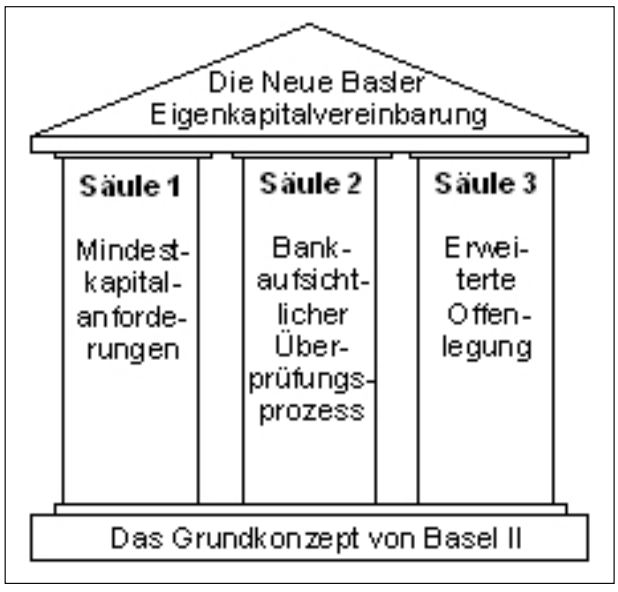


Abbildung 3: Die drei Säulen der Neuen Baseler Eigenkapitalvereinbarung
Quelle: Deutsche Bundesbank (2005a).

In Säule 1 wird die Berechnung der Mindest-Eigenkapitalanforderungen für die unterschiedlichen Risikoarten beschrieben.[56] Für das operationelle Risiko werden die Banken vor die Wahl gestellt, einen von drei Messansätzen zu nutzen. Diese Messansätze unter-

[55] Vgl. Schierenbeck (2003), S.21.
[56] Vgl. Baseler Ausschuss (2004a), S.14.

scheiden sich in ihrer Komplexität und folglich in ihrer Genauigkeit und in dem mit ihrer Umsetzung verbundenen Aufwand.[57]

Bei den beiden weniger komplexen Ansätzen *Basisindikatoransatz* und *Standardansatz* bzw. dem *alternativen Standardansatz* wird die Eigenkapitalanforderung auf Basis der Bruttoerträge der Bank der letzten drei Jahre ermittelt. Unter der Kategorie der *ambitionierten Messansätze* werden bankinterne Messsysteme verstanden, die bestimmte qualitative und quantitative Mindestanforderungen erfüllen und deren Einsatz zur Berechnung der Eigenkapitalanforderung gemäß Basel II daher von der Bankenaufsicht genehmigt wurde.[58] Die qualitativen Anforderungen betreffen im wesentlichen die organisatorische Stellung des Risikomanagements innerhalb der Bank und die Dokumentation der angewendeten Verfahren. Die quantitativen Anforderungen sollen die Genauigkeit der Berechnung der Eigenkapitalanforderung sicherstellen.[59]

Die zweite Säule von Basel II enthält Grundsätze für die qualitative Überprüfung des Risikomanagements durch die Bankenaufsicht. Das Überprüfungsverfahren soll gewährleisten, dass die Banken ausreichend Eigenkapital bereitstellen und soll sie in ihren Bemühungen bestärken, leistungsfähigere Risikomesssysteme zu entwickeln.[60] In Bezug auf operationelle Risiken zielen die Verlautbarungen der zweiten Säule darauf ab, dass diese genauso exakt gemessen werden wie andere bedeutende Risiken der Banken. Damit soll ihrem hohem Gefährdungspotential Rechnung getragen werden.[61]

3.2.3 Mindestanforderungen an das Risikomanagement (MaRisk)

Die Mindestanforderungen an das Risikomanagement (MaRisk) sollen Ende 2005 verabschiedet und für alle Banken in Deutschland verbindlich werden.[62] Mit den MaRisk werden die momentan gültigen Mindestanforderungen an das Kreditgeschäft (MaK), die Mindestanforderungen an das Betreiben der Handelsgeschäfte (MaH) und die Mindestanforderungen an die Ausgestaltung der Internen Revision (MaIR) in einem Regelwerk zusammengefasst. Die MaH haben die Zielsetzung, Risiken aus dem Handelsgeschäft der Banken frühzeitig zu erkennen und zu steuern. Die MaK verfolgen die gleiche Zielsetzung für das Kreditgeschäft der Banken. Die MaIR zielen darauf ab, Risiken auf-

[57] Vgl. Baseler Ausschuss (2004a), S.3.
[58] Vgl. Baseler Ausschuss (2004a), S.161 ff.
[59] Vgl. Baseler Ausschuss (2004a), S.163 ff.
[60] Vgl. Baseler Ausschuss (2004a), S.180.
[61] Vgl. Baseler Ausschuss (2004a), S.183 f.
[62] Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (2005a), AT 2.1.1.

grund unzureichender interner Kontrollen einzugrenzen. Das zusammengefasste Regelwerk soll eine ganzheitliche Betrachtung der Risiken der Banken erlauben.[63]

Es war eines der mit der Entwicklung der MaRisk verbundenen Ziele, einen qualitativen Standard für bis dahin nicht von der deutschen Bankenaufsicht explizit berücksichtigte Risikoarten zu schaffen.[64] Den operationellen Risiken kommt in den MaRisk dabei „ein zentraler – wenn nicht sogar überragender – Stellenwert"[65] zu, was auch eine logische Folge der Tatsache ist, dass die MaRisk auf Bestandteilen des §25a KWG basieren. Ausgangspunkt der MaRisk sind diejenigen Bestandteile des §25a KWG, in denen eine angemessene Geschäftsorganisation gefordert wird, was wiederum durch eine angemessene Strategie und ein angemessenes internes Kontrollverfahren umzusetzen sei. Gemäß den MaRisk setzt sich ein angemessenes internes Kontrollverfahren aus einer internen Revision und in einem internen Kontrollsystem zusammen. Das interne Kontrollsystem soll aufbau- und ablauforganisatorische Regelungen sowie ein Risikomanagement im Sinne der in Kapitel 2.3 gegebenen Beschreibung umfassen. Die MaRisk bewirken damit die Einrichtung angemessener Leitungs-, Steuerungs- und Kontrollprozesse innerhalb der Banken[66] und setzen Teile der zweiten Säule von Basel II in deutsches Recht um.[67]

Direkt angesprochen werden operationelle Risiken in den MaRisk in dem Abschnitt BTR 4, in dem allgemeine qualitative Anforderungen an das Management operationeller Risiken gestellt werden.[68]

Weitere Bestimmungen bezüglich operationeller Risiken existieren im gesamten Regelwerk, was ein Ausdruck ihrer übergreifenden Rolle ist.[69] So besteht die allgemeine Vorgabe, dass Tätigkeiten, die nicht miteinander vereinbar sind, von verschiedenen Personen durchzuführen sind.[70] Es wird damit den Risikoursachen *interne Verfahren* und *Mensch* Rechnung getragen, indem insbesondere internem Betrug und Fehleinschätzungen von Mitarbeitern entgegengewirkt wird.

[63] Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (2005b), S.1.
[64] Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (2005b), S.5.
[65] Bundesanstalt für Finanzdienstleistungsaufsicht (2005b), S.5.
[66] Vgl. Bundesverband Öffentlicher Banken Deutschlands e.V. (2005), S.1.
[67] Vgl. Bundesverband Öffentlicher Banken Deutschlands e.V. (2005), S.2.
[68] Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (2005a), BTR 4.
[69] Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (2005b), S.4.
[70] Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (2005a), AT 4.3.1 Ziffer 1.

Werden Teile der Revision an externe Prüfer übertragen, so ist sicherzustellen, dass der externe Prüfer über den notwendigen Sachverstand und die technischen Fachkenntnisse verfügt.[71] Hiermit wird die operationelle Risikoursache *Mensch* adressiert.

Im Risikomanagement sind die zur Anwendung kommenden Methoden durch einen fachlich geeigneten Mitarbeiter jährlich auf ihre Eignung zu überprüfen.[72] Die interne Revision ist ebenfalls für die Überprüfung des Risikomanagements verantwortlich,[73] wodurch der Risikoursache *interne Verfahren* entgegengewirkt wird.

Wird die Bank auf für sie neuen Märkten aktiv, so ist dies erst nach der Erarbeitung eines Konzeptes zulässig, das sich ausdrücklich mit dem Risikogehalt dieser Geschäfte auseinanderzusetzen hat. Auf diese Weise soll sichergestellt werden, dass die Bank auf Seiten des Personals, der Systeme und von organisatorischer Seite in der Lage ist, die Geschäfte durchzuführen.[74] Es werden also die Risikoursachen *Mensch*, *Systeme* und *interne Verfahren* adressiert.

Den möglichen Risikoursachen *Mensch* und *Systeme* werden jeweils ein Abschnitt der MaRisk gewidmet. Im Abschnitt *Personal* wird die Forderung nach einer qualitativ angemessenen Personalausstattung der Bank erhoben, mit der sichergestellt wird, dass die Mitarbeiter die erforderlichen Kenntnisse und Erfahrungen haben.[75] Der Abschnitt *Technisch-organisatorische Ausstattung* verlangt, dass die Systeme von ihrem Umfang und ihrer Qualität her den Geschäften der Bank angemessen sein sollen. Sie müssen eine hohe Verfügbarkeit und Stabilität gewährleisten und korrekt laufen. Die Eignung der Systeme und der IT-Prozesse ist regelmäßig zu überprüfen. Vor ihrem ersten Einsatz und nach jeder Änderung sind die Systeme zu testen und von technisch sowie von fachlich verantwortlichen Mitarbeitern abzunehmen.[76]

Für alle bankexistenziellen Aktivitäten und Prozesse sind Notfallpläne zu erstellen und regelmäßig auf ihre Angemessenheit zu überprüfen. Diese Notfallpläne müssen Pläne zur Geschäftsfortführung und zur Wiederaufnahme der Geschäfte beinhalten. Derartige Pläne sollen das Schadensausmaß in Notfallsituationen begrenzen.[77] Mögliche Ursachen für Notfälle sind *externe Ereignisse*, wie z.B. Feuer, Hochwasser, Terror und Stromausfall. Direkten Einfluss können solche externen Ereignisse auf die *Systeme* einer Bank haben, was deren Ausfall zur Folge haben kann. Ein Systemausfall kann wiederum be-

[71] Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (2005a), BT 2.4 Ziffer 3.
[72] Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (2005a), AT 4.1 Ziffer 4.
[73] Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (2005a), AT 4.4 Ziffer 3.
[74] Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (2005a), AT 8 Ziffer 1.
[75] Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (2005a), AT 7.1.
[76] Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (2005a), AT 7.2.
[77] Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (2005a), AT 7.3.

dingen, dass Geschäftsprozesse einer Bank nicht durchgeführt werden können, wodurch die Risikoursache *interne Verfahren* schlagend werden würde.

3.2.4 Wertpapierhandelsgesetz (WpHG)

Das Wertpapierhandelsgesetz (WpHG) ist Bestandteil des 2. Kapitalmarktförderungsgesetzes,[78] welches wiederum zum Ziel hat, vor dem Hintergrund der Zunahme des internationalen Wettbewerbs der Finanzplätze das Vertrauen der Anleger in den deutschen Kapitalmarkt zu stärken sowie dessen Leistungsfähigkeit zu erhöhen.[79] Es enthält indirekte Bezüge auf operationelle Risiken. Gültig ist das WpHG u.a. für alle Banken.
In §31 Abs.1 WpHG wird gefordert, dass Banken Wertpapierdienstleistungen und Wertpapiernebendienstleistungen mit der erforderlichen Sachkenntnis, Sorgfalt und Gewissenhaftigkeit auszuführen haben. Gemäß § 2 WpHG zählen zu diesen Dienstleistungen die Anschaffung und Veräußerung von Wertpapieren für Dritte und die Verwahrung von Wertpapieren. Bezogen auf das operationelle Risiko ist also dafür zu sorgen, dass bei diesen Geschäften der Risikofaktor *Mensch* die notwendige Beachtung findet.
Gemäß §33 WpHG sind Banken dazu verpflichtet, im Wertpapiergeschäft Verfahren und Mittel anzuwenden, die für dessen ordnungsgemäße Durchführung notwendig sind. Sie sollen über angemessene interne Kontrollverfahren verfügen, um Verstößen gegen Regelungen des WpHG entgegenwirken zu können. Auch wenn die Bank die Durchführung dieser Geschäfte an ein anderes Unternehmen überträgt, muss die Bank die ordnungsgemäße Durchführung der Geschäfte sicherstellen und sie in ihre internen Kontrollverfahren einbeziehen. Damit sind in §33 Regelungen formuliert, die hauptsächlich den Risikofaktor *interne Verfahren* ansprechen. Die Forderung nach Mitteln, die einer ordnungsgemäßen Durchführung dienlich sind, kann durch entsprechende *Systeme* erfüllt werden.

3.2.5 Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)

Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) wurde 1998 vor dem Hintergrund zahlreicher Unternehmenskrisen sowie eines steigenden internationalen Vergleichs zwischen den Finanzplätzen verabschiedet. Ziel des KonTraG

[78] Vgl. Büschgen (1998), S.266.
[79] Vgl. Büschgen (1998), S.200.

war es, durch eine Erweiterung der Auskunftspflichten und durch eine Stärkung der Kontrollmöglichkeiten bei Kapitalgesellschaften das Vertrauen der Anleger in den deutschen Kapitalmarkt zu erhöhen. Es enthält Bestimmungen, die für Kapitalgesellschaften Veränderungen bei der Führung und der Jahresabschlusserstellung zur Folge haben. Bewirkt wird dies nicht durch eigenständige Regelungen, sondern durch Änderungen und Ergänzungen anderer Gesetze, vorrangig dem Aktiengesetz (AktG) und dem Handelsgesetz (HGB).

Im Hinblick auf operationelle Risiken wurde gemäß Art.1 Abs.9 c) KonTraG der §91 Abs.2 AktG erschaffen, demzufolge der Vorstand einer Kapitalgesellschaft geeignete Maßnahmen zu treffen hat, die die Gesellschaft in die Lage versetzen, ihren Fortbestand gefährdende Entwicklungen früh erkennen zu können. Zu diesen Maßnahmen zählt insbesondere die Einrichtung eines Überwachungssystems. Da sich diese Regelung nur im AktG findet, gilt sie rein formell nur für diejenigen Banken, die sich in der Rechtsform der Aktiengesellschaft befinden. In der Gesetzesbegründung findet sich jedoch der Hinweis, dass davon ausgegangen wird, dass diese Regelung auch eine „Ausstrahlungswirkung auf den Pflichtenrahmen der Geschäftsführer auch anderer Gesellschaftsformen“[80] hat. Gemäß §317 Abs.4 HGB muss bei der Prüfung des Jahresabschlusses vom Wirtschaftsprüfer beurteilt werden, ob das Überwachungssystem seine Aufgaben erfüllen kann.

Dem Institut der Wirtschaftsprüfer in Deutschland (IdW) zufolge ergibt sich für Unternehmen aus §91 Abs.2 AktG die Verpflichtung, ein Risikomanagement einzurichten, das alle Prozesse und Funktionen eines Unternehmens auf ihnen eventuell innewohnende existenzgefährdende Risiken durchleuchtet. Dabei ist zu unterscheiden, ob die Risiken aus den Prozessen und Funktionen selbst resultieren, oder ob die Risiken durch externe Ereignisse hervorgerufen werden.[81] Der Begriff des operationellen Risikos wird im AktG und vom IdW zwar nicht explizit genannt, die Verweise des IdW deuten jedoch klar darauf hin, dass das operationelle Risiko gemeint ist.

3.2.6 Sarbanes-Oxley-Act (SOX)

Der Sarbanes-Oxley Act (SOX)[82] – benannt nach dem Senator Paul S. Sarbanes und dem Abgeordneten Michael Oxley – wurde im Juli 2002 in den USA als Reaktion auf aufsehenerregende Fälle von Bilanzbetrug von an dortigen Börsen notierten Unterneh-

[80] Bundesrat-Drucksache 872/97, S. 37.
[81] Vgl. Institut der Wirtschaftsprüfer (1999), S.352.
[82] Es sind zwei Abkürzungen gleichermaßen gebräuchlich: SOX und SOA. In dieser Arbeit wird die erstgenannte Variante verwendet.

men verabschiedet.[83] Ziel war es, das dadurch erschütterte Vertrauen der Anleger in die Kapitalmärkte schnellstmöglich wieder herzustellen. Dies ist insbesondere für die USA sehr wichtig, da nach dortigem Verständnis das Funktionieren der Kapitalmärkte in hohem Maße für Wachstum und Wohlstand verantwortlich ist.[84] Gegenstand des SOX sind Regelungen, die die Integrität der Rechnungslegung, der Finanzberichterstattung und der Geschäftspraktiken durch Publizitätspflichten der Unternehmen gewährleisten sollen. Somit dient der SOX der Stärkung des amerikanischen Corporate Governance Systems.[85] In einem starken Corporate Governance System[86] handeln Unternehmen nach „anerkannte[n] Standards guter und verantwortungsvoller Unternehmensführung“[87].

Die Vorschriften des SOX gelten für alle Unternehmen, die der US-amerikanischen Börsenaufsicht *Securities and Exchange Commission* (SEC) unterstehen. Dies sind Unternehmen, deren Wertpapiere entweder an Börsen oder auf andere Art und Weise in den USA öffentlich gehandelt werden. Auch Tochterunternehmen dieser Firmen, die ihren Sitz außerhalb der USA haben, sowie Wirtschaftsprüfungsgesellschaften, die entweder in den USA ansässig sind oder Jahresabschlüsse der SEC unterstehender Unternehmen prüfen, sind an die Bestimmungen des SOX gebunden.[88] In 2004 gab es 30 deutsche Unternehmen, die aufgrund dieser Regelungen an die SEC berichten mussten, darunter auch die Deutsche Bank AG.[89] Es wird erwartet, dass in absehbarer Zeit ähnliche Regelungen auf EU-Ebene verabschiedet werden oder dass sich der SOX de facto auch für solche Unternehmen als Standard etabliert, die ihm rein formell nicht unterliegen, wie es mit Basel I der Fall war.[90] Von daher sollten deutsche Banken dem SOX mit Blick auf die Zukunft Beachtung schenken.

Der SOX ist in elf Abschnitte unterteilt, die ihrerseits jeweils mehrere *Sections* enthalten. Die wesentlichsten Aussagen finden sich in Section 302 und 404.[91] Section 302 enthält u.a. die Forderung, dass der Vorstand und der Finanzvorstand für den Aufbau interner Kontrollsysteme verantwortlich sind, die sicherstellen, dass Quartals- und Jahresabschlüsse alle relevanten Informationen enthalten. Section 404 zufolge ist das Ma-

[83] Vgl. Diederichs (2005), S.301.
[84] Vgl. Kauffmann/Götzenberger (2003), S.150 f.
[85] Vgl. Diederichs (2005), S.301.
[86] Corporate Governance (engl.) = Unternehmensführung.
[87] Deutscher Corporate Governance Kodex (2005), S.1.
[88] Vgl. Diederichs (2005), S.301.
[89] Vgl. Grosse/Tsapanis/Stromberg (2004), S.105.
[90] Vgl. Kauffmann/Götzenberger (2003), S.155.
[91] Vgl. Grosse/Tsapanis/Stromberg (2004), S.105.

nagement zudem für die Einrichtung und Aufrechterhaltung angemessener Prozesse für die Finanzberichterstattung verantwortlich.

Operationelle Risiken werden im SOX nicht ausdrücklich erwähnt, aber ein Hinweis darauf, dass mit der Forderung nach dem Betreiben eines internen Kontrollsystems operationelle Risiken adressiert werden, ergibt sich aus der Tatsache, dass es zwar offen gelassen wird, wie ein Kontrollsystem konkret auszugestalten ist, die SEC aber verlautbaren ließ, dass ein dem COSO-Rahmenwerk entsprechendes Kontrollsystem die Anforderungen erfüllt.[92] Das amerikanische *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) hat das Ziel, die Qualität des Finanzberichtswesens zu verbessern. In seinem *Internal Control – Integrated Framework* heißt es, dass ein internes Kontrollsystem u.a. die Beurteilung von Risiken beinhalten soll, und zwar „risks from external and internal sources"[93]. Bei Risiken aus internen Quellen handelt es sich um operationelle Risiken.

Auch das Versagen von an der Finanzberichterstattung beteiligten *Systemen* kann dazu führen, dass dem SOX nicht entsprochen werden kann, weshalb Unternehmen ihre IT diesbezüglich einer kritischen Überprüfung unterziehen sollten.[94]

3.3 Operationelles Risiko und Prozessorganisation

Zahlreiche Regelungen verpflichten Banken zum Management operationeller Risiken. Den bei der Umsetzung der Bestimmungen anfallenden Kosten steht im ersten Moment nur eine Verringerung des operationellen Risikos gegenüber, dem eine Bank ausgesetzt ist. Auf welche Art und Weise Banken die Bestimmungen umsetzen, ist ihnen freigestellt.

Einen Ansatz zur Umsetzung der Bestimmungen stellt die geschäftsprozessorientierte Herangehensweise dar. Grundlage hierbei ist die Modellierung von Geschäftsprozessen. Auf Basis der Prozessmodelle können Verfahren angewendet werden, die die Geschäftsprozesse auf mögliche Fehlerquellen und deren Auswirkungen untersuchen oder die die Simulation von Risikoszenarien beinhalten. Diese Verfahren werden in Kapitel 5 beschrieben. Hierbei ergeben sich zwei wesentliche Vorteile.

Zum einen kann durch die Simulation der Einrichtung und des Aufhebens von Risikomaßnahmen die Wirtschaftlichkeit der Maßnahmen untersucht werden.[95] Zum anderen

[92] Vgl. Kauffmann/Götzenberger (2003), S.159; vgl. Färber/Wagner (2005), S.157.
[93] Vgl. COSO (1994).
[94] Vgl. Ostler (2005).

kann das Management operationeller Risiken mit der „proaktive[n] Erschließung von Benefits für die Prozessorganisation“[96] verbunden werden. Dabei geht es darum, Geschäftsprozesse frühzeitig nach dem Gesichtspunkt der Risikovermeidung zu gestalten. War die Bank vorher nicht nach Prozessgesichtspunkten organisiert, so bietet es sich an, die geschäftsprozessorientierte Herangehensweise an das Management operationeller Risiken dazu zu nutzen, weitere mit der Prozessorganisation verbundene Vorteile zu erschließen.

Um die Bedeutung dieses Aspektes zu verdeutlichen, werden im folgenden Kapitel die Grundlagen der Prozessorganisation behandelt.

[95] Vgl. Bergmann, M. (2005), S.15.
[96] Bergmann, M. (2005), S.14.

4. Grundlagen der Prozessorganisation

Um die Grundlagen der Prozessorganisation zu vermitteln, wird zunächst die klassische Herangehensweise an die Organisationsgestaltung beschrieben. Nach der Definition der Begriffe Prozess und Geschäftsprozess wird der Inhalt und die Zielsetzung der Prozessorganisation beschrieben und es wird auf deren Vorteile gegenüber dem klassischen Konzept eingegangen. Danach werden Kriterien genannt, nach denen Prozesse abgegrenzt werden können und es werden die möglichen Bestandteile eines Prozesses beschrieben. Nach der Diskussion unterschiedlicher Darstellungsmittel für Prozesse wird kurz auf Aspekte der Geschäftsprozessmodellierung eingegangen.

4.1 Klassische Organisationsgestaltung gemäß dem Analyse-Synthese-Konzept

Es existieren verschiedene Organisationskonzepte, die beschreiben, wie die Organisation eines Unternehmens gestaltet werden kann. Die klassische Organisationsgestaltung baut auf dem von Kosiol geprägten Analyse-Synthese-Konzept auf.
Unter Organisation wird in der Betriebwirtschaftslehre „sowohl das zielorientierte ganzheitliche Gestalten von Beziehungen in offenen sozialen Systemen als auch das Ergebnis dieser Tätigkeit“[97] verstanden. Mit der Organisationsgestaltung sollen also bestimmte Soll-Zustände in offenen sozialen Systemen erreicht werden. Ein offenes soziales System ist dadurch gekennzeichnet, dass Menschen in vielfältigen Wechselbeziehungen zu anderen Menschen innerhalb des Systems und mit der Umwelt stehen.[98]
Ausgangspunkt des Analyse-Synthese-Konzeptes ist die Gesamtaufgabe eines Unternehmens. Um diese operationalisieren zu können, wird sie im Rahmen der *Aufgabenanalyse* nach bestimmten Kriterien in Teilaufgaben zerlegt.[99] Nach der Aufgabenanalyse werden die so ermittelten Teilaufgaben innerhalb der *Aufgabensynthese* zu Aufgabenkomplexen zusammengefasst, so dass sie Aufgabenträgern zugewiesen werden können. Durch die Verteilung der Teilaufgaben entstehen Organisationseinheiten. Die personenbezogene Aufgabenbündelung führt zur Bildung einer Stelle, bei der Bündelung mehrerer Stellen entsteht eine Abteilung. Das Ergebnis ist die Aufbauorganisation eines

[97] Vahs (2005), S.13.
[98] Vgl. Vahs (2005), S.10 ff.
[99] Vgl. Kosiol (1962), S.45 ff.

Unternehmens, die regelt, welche Stellen und welche Abteilungen welche Teilaufgaben wahrnehmen.[100]

Im Anschluss an die Aufgabensynthese findet die *Arbeitsanalyse* statt. Hierbei werden die Teilaufgaben in Arbeitsteile zerlegt. Abgeschlossen wird das Analyse-Synthese-Konzept mit der *Arbeitssynthese*, in deren Rahmen Arbeitsprozesse gestaltet werden. Hier werden die Arbeitsteile nach drei Gesichtspunkten zusammengeführt. Bei der personalen Synthese wird der Hintergedanke verfolgt, die Arbeitsteile vom Umfang her einer Person übertragen zu können. Bei der temporalen Synthese sollen die Durchlaufzeiten der bearbeiteten Objekte optimiert werden. Hierzu müssen die Leistungen der beteiligten Personen aufeinander abgestimmt werden. Die lokale Synthese hat die Optimierung der Transportwege im Unternehmen zum Ziel, was durch eine gezielte räumliche Anordnung der unterschiedlich ausgestatteten Arbeitsplätze geschieht. Aus der Arbeitssynthese geht die Ablauforganisation eines Unternehmens hervor, die regelt, welche Stelle welchen Arbeitsteil wann und an welchem Ort ausführt.[101]

Beim Analyse-Synthese-Konzept wird davon ausgegangen, dass sich die im Rahmen der Ablauforganisation betrachteten Prozesse an die vorher festgelegte Aufbauorganisation anpassen. Hieraus ergibt sich der Hauptkritikpunkt an Kosiols Ansatz. Wird nämlich diesem gefolgt, beschränkt sich die Strukturierung eines Geschäftsprozesses auf eine Planung der Reihenfolge, in der die Aufgaben auszuführen sind. Dies mag bis zu einem gewissen Grad für Fertigungsprozesse ausreichend sein, da hier Stellen durch maschinelle Einrichtungen vorgegeben werden und auch die Reihenfolge der Aktivitäten oft vorgegeben ist. Bei Verwaltungsprozessen und weniger stark durch Technik bestimmte Prozesse ist die Aufgabenverteilung hingegen in größerem Umfang frei bestimmbar.[102] Die Stellen, die im Rahmen der Aufgabensynthese gebildet werden, weisen – abgesehen vom Arbeitssynthesemerkmal „Objekt“ – eine funktionale Spezialisierung auf. Geschäftsprozesse hingegen sind zumeist stellenübergreifend, was auf diesem Wege nicht berücksichtigt wird. So entstehen in einer funktionalen Aufbauorganisation z.T. abteilungsübergreifende Schnittstellen, die einen hohen Koordinations- und Kontrollaufwand erfordern, da andernfalls gleiche Teilaufgaben mehrfach ausgeführt werden.[103] Abbildung 4 zeigt die Prozessabwicklung in einer funktionalen Organisation.

[100] Vgl. Kosiol (1962), S.76 ff.
[101] Vgl. Kosiol (1962), S.192 ff.
[102] Vgl. Gaitanides (1983), S.61 f.
[103] Vgl. Schulte-Zurhausen (2002), S.45 f.; vgl. Kugeler/Vieting (2005), S.237.

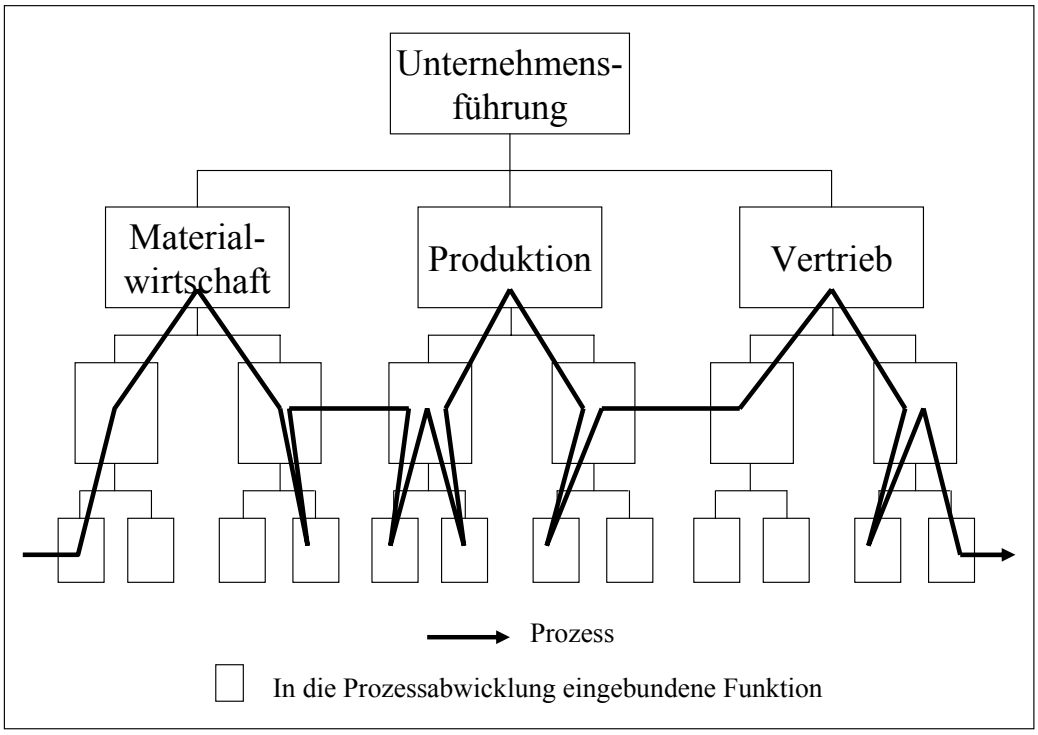


Abbildung 4: Prozessabwicklung in einer funktionalen Organisation
Quelle: Vahs (2005), S.204.

4.2 Definition Prozess und Geschäftsprozess

Wie sich bereits aus den obigen Ausführungen ableiten lässt, bestehen Prozesse aus der Aneinanderreihung von Teilaufgaben. Definiert werden kann ein Prozess als

> *„inhaltlich abgeschlossene, zeitliche und sachlogische Folge der Funktionen, die zur Bearbeitung eines betriebswirtschaftlich relevanten Objektes notwendig sind.“*[104]

Diese Abfolge von Funktionen wird durch ein bestimmtes Ereignis gestartet und hat einen bestimmten Input und Output.[105] Was dabei das Startereignis und was der Output eines Prozesses ist und was demzufolge inhaltlich als *ein* Prozess angesehen wird, lässt sich nicht allgemein bestimmen, da es stark von der subjektiven Sichtweise der Person abhängig ist, die den Prozess definiert. Die geforderte *inhaltliche Abgeschlossenheit* eines Prozesses ist dann als gegeben anzusehen, wenn in dem Prozess ein betriebswirtschaftlich relevantes Objekt bearbeitet wird und die Person, die den Prozess definiert,

[104] Becker/Schütte (1996), S.52 f.
[105] Vgl. Vahs (2005), S.209.

den Prozess separat von anderen Aktivitäten betrachten *möchte*.[106] Bei den betriebswirtschaftlichen Objekten wird unterschieden zwischen Informationsobjekten, also bspw. Rechnungen, und materialisierten Objekten, wie es z.B. Waren sind.
Der Begriff Geschäftsprozess wird häufig synonym mit dem des Prozesses verwendet, wenngleich es sich bei einem Geschäftsprozess eigentlich um eine spezielle Art eines Prozesses handelt,[107] die wie folgt definiert werden kann:

> *„Geschäftsprozesse repräsentieren die Geschäftsarten einer Unternehmung, ergeben sich aus den obersten Sachzielen und weisen zwingend Schnittstellen zu externen Marktpartnern auf."*[108]

In dieser Arbeit werden die beiden Begriffe Prozess und Geschäftsprozess synonym verwendet, da es im überwiegenden Teil der Arbeit nicht zweckmäßig oder nicht möglich wäre, zwischen Prozessen und Geschäftsprozessen zu differenzieren. Dies wäre in den meisten Fällen erst in Verbindung mit einem konkreten Unternehmen möglich bzw. sinnvoll.

4.3 Inhalt und Zielsetzung der Prozessorganisation

Unter Prozessorganisation soll in dieser Arbeit eine prozessorientierte Organisationsgestaltung verstanden werden, bei der im Gegensatz zum Analyse-Synthese-Konzept Abteilungen und „Stellen nicht nur nach Kriterien des Aufbaus, sondern auch nach Kriterien des Ablaufs gebildet werden."[109] Gaitanides gliedert die prozessorientierte Organisationsgestaltung analog zu Kosiols Vorgehen in drei Schritte.
Der erste Schritt beinhaltet eine Prozessanalyse. Hier müssen zunächst inhaltlich abgeschlossene Vorgänge identifiziert werden, die im weiteren Verlauf als Prozess betrachtet werden. Diese werden dann soweit in Teilprozesse zerlegt, bis einzelne Aktivitäten vorliegen. Darauf wird die zeitliche Bearbeitungsreihenfolge der Aktivitäten festgestellt. Aktivitäten können gegenüber anderen Aktivitäten vorrangig, gleichrangig oder nachrangig durchzuführen sein. Liegen all diese Informationen vor, können die Prozesse

[106] Vgl. Gaitanides (1983), S.65.
[107] Vgl. Becker/Schütte (1996), S.52.
[108] Becker/Schütte (1996), S.53.
[109] Gaitanides (1983), S.62.

dokumentiert werden. Als letzter Bestandteil der Prozessanalyse werden die Bearbeitungszeiten der einzelnen Aktivitäten ermittelt.[110]

Im zweiten Schritt werden die Aktivitäten Stellen zugeordnet. Dabei wird für verschiedene Varianten der Aufgabenverteilung untersucht, welche Kapazitäten sie zu verarbeiten in der Lage sind. Ergebnis ist eine bestimmte Anzahl an Stellen, mit der es in einem gegebenen Zeitraum möglich sein soll, einen erwarteten Leistungsumfang zu bewältigen.

Im dritten Schritt wird sich der Koordination von Prozessen gewidmet. Hier wird zunächst berücksichtigt, mit welchen organisatorischen Maßnahmen die Leistungsbereitschaft und Motivation der Stelleninhaber sichergestellt werden kann. Nachdem dies geklärt ist, werden Aspekte der Abstimmung zwischen Stelleninhabern innerhalb eines Prozesses geregelt. Dieser Abstimmungsbedarf resultiert aus der Arbeitsteiligkeit der meisten Prozesse. Abschließend werden Maßnahmen entwickelt, mit denen Abstimmungsproblemen zwischen verschiedenen Prozessen begegnet werden kann.[111]

Ein Vorteil der Prozessorganisation und der damit einhergehenden Integration von Funktionen liegt in der Verringerung der gegenseitigen Abhängigkeiten von Tätigkeiten und in einer Reduzierung der Schnittstellenproblematik. Folgen sind ein reduzierter Koordinationsaufwand, weniger Doppelarbeiten und weniger Fehler, die aus Interdependenzen und Schnittstellen herrühren.

Ein weiterer Vorzug ergibt sich aus der Vergabe von Verantwortung und Kompetenzen für abteilungsübergreifende Prozesse an einen oder mehrere Mitarbeiter, die damit die Rolle eines so genannten *Process Owner* einnehmen. Dies geht damit einher, dass die Hierarchie in den Hintergrund tritt. Damit tritt als alternativer Koordinationsmechanismus die Selbstabstimmung der Prozessbeteiligten in den Vordergrund, die wiederum zu höheren Freiräumen und damit einhergehend zu einer gesteigerten Motivation führt.

Die Prozessorganisation beinhaltet eine Orientierung am internen und externen Kunden. Dadurch entsteht die Neigung, überbetrieblich, und nicht nur aus der Sichtweise der eigenen Abteilung zu denken und zu handeln. Damit kann eine Unternehmenskultur geprägt werden, in der Abläufe im Unternehmen ständig hinterfragt und verbessert werden.[112]

Die Zielsetzung der Prozessorganisation besteht somit darin, eine Struktur zu schaffen, die einen in Bezug auf die Kriterien Zeit, Kosten und Qualität optimalen Ablauf von

[110] Vgl. Gaitanides (1983), S.63 ff.
[111] Vgl. Gaitanides (1983), S.159 ff.
[112] Vgl. Vahs (2005), S.206 f.

Geschäftsprozessen ermöglicht und die eine hohe Innovationsfähigkeit des Unternehmens sicherstellt.[113] Von der Erreichung diese Zielsetzung versprechen sich Unternehmen Vorteile gegenüber ihren Wettbewerbern.[114] Ergebnis der Prozessorganisation ist „eine Konzentration auf wertschöpfende Prozesse und eine erhöhte Transparenz der Abläufe im Unternehmen mit einer daraus resultierenden höheren Flexibilität und effizienterem Ressourceneinsatz."[115]

4.4 Ansätze zur Klassifizierung von Prozessen

Weiter oben wurde angeführt, dass es in hohem Maße auf subjektiven Sichtweisen beruht, welche Aktivitäten als ein Prozess betrachtet werden. Um Anhaltspunkte dafür zu geben, welche Überlegungen dabei eine Rolle spielen können, werden im Folgenden drei gängige Ansätze zur Klassifizierung von Prozessen beschrieben. Ihnen zur Folge lassen sich Prozesse nach ihrem Marktbezug, dem Prozessgegenstand oder der Art der in ihnen ausgeführten Tätigkeit unterscheiden.

4.4.1 Marktbezug

An das Wertkettenmodell von Porter angelehnt können Prozesse in *Kern-, Support- und Innovationsprozesse* unterteilt werden. Unterscheidungskriterium ist dabei ihr Bezug zum Markt.[116] Eine Wertkette ist ein analytisches Instrument, mit dem sich ein Unternehmen in seine strategisch relevanten Tätigkeiten zerlegen lässt. Mit dem Einsatz von Wertketten bezwecken Unternehmen, Quellen für Wettbewerbsvorteile zu ermitteln, sich Wettbewerbsvorteile zu verschaffen und sie zu behaupten.[117] Unter *Wert* wird in diesem Zusammenhang der Betrag verstanden, den die Abnehmer bereit sind, für die Leistung des Unternehmens zu bezahlen. Das Ziel des Unternehmens sollte es sein, einen Wert zu schaffen, der größer ist als die Kosten der Produktion, um eine *Gewinnspanne* zu erwirtschaften.

Die Tätigkeiten, die im Unternehmen durchgeführt werden und die für die Schaffung des Wertes verantwortlich sind, werden von Porter als Wertaktivitäten bezeichnet und in primäre und unterstützende Aktivitäten unterteilt. Im Rahmen der primären Aktivitäten

[113] Vgl. Vahs (2005), S.218 ff.
[114] Vgl. Schulte-Zurhausen (2002), S.45 f.; vgl. Becker/Vieting (2005), S.237.
[115] Helbig (2003), S.14.
[116] Vgl. Vahs (2005), S.216.
[117] Vgl. Porter (1999), S.63 ff.

wird das Produkt hergestellt, an den Abnehmer verkauft und übermittelt sowie der Kundendienst durchgeführt. Die unterstützenden Aktivitäten dienen der Aufrechterhaltung der primären Aktivitäten. Sie beinhalten den Kauf von Materialien, die Bereitstellung der technologischen Infrastruktur, das Personalwesen und weitere Funktionen, die der Bereitstellung und Aufrechterhaltung der Unternehmensinfrastruktur dienen.[118]

Aus dem Wertkettenmodell wurden die Begriffe *Kernprozess* als Entsprechung primärer Aktivitäten und *Supportprozess* für unterstützende Aktivitäten abgeleitet. Kernprozesse beziehen sich direkt auf die Produkte eines Unternehmens, Supportprozesse sind dagegen nicht an der Wertschöpfung beteiligt, aber für die Durchführung der Kernprozesse notwendig.[119] Als Ergänzung zu diesen beiden an das Wertkettenmodell angelehnten Prozesskategorien existiert die Kategorie der Innovationsprozesse, in deren Rahmen neue Produkte, Verfahren und Strukturen entwickelt und eingeführt werden.[120]

Abbildung 5 zeigt das Modell der Wertkette. Es enthält die Gewinnspanne und alle Kategorien von in Unternehmen vorhandenen Aktivitäten. Damit gibt es den Gesamtwert des Unternehmens wieder.[121]

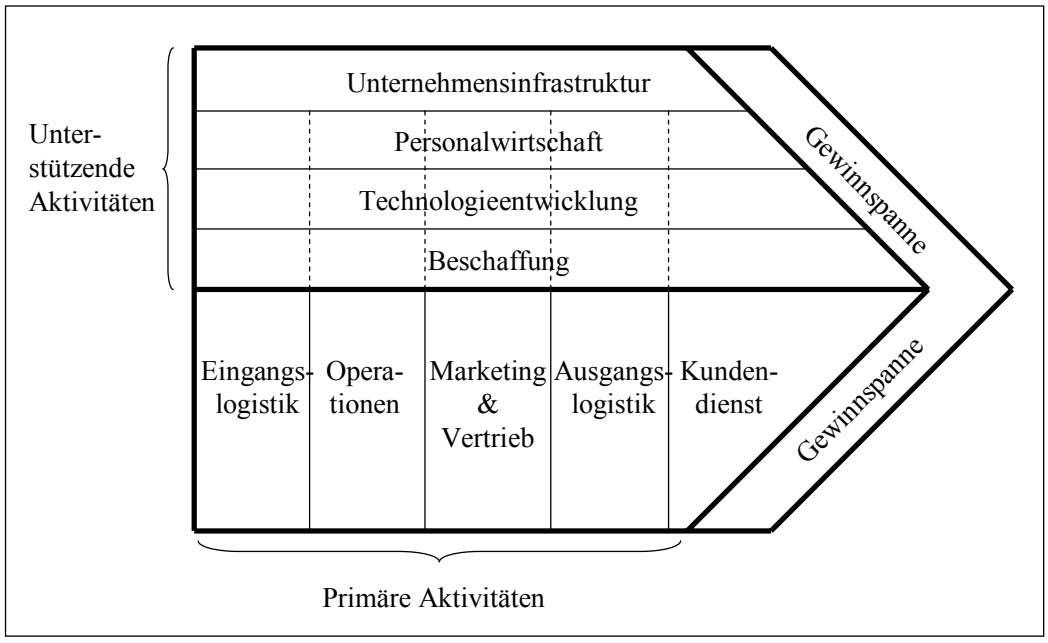


Abbildung 5: Wertkettenmodell von Porter
Quelle: Porter (1999), S.66.

[118] Vgl. Porter (1999), S.68 f.
[119] Vgl. Becker/Kahn (2005), S.7.
[120] Vgl. Vahs (2005), S.216; vgl. Schulte-Zurhausen (2002), S.53.
[121] Vgl. Porter (1999), S.68.

4.4.2 Prozessgegenstand

Grochla versteht Unternehmen als Systeme, deren Elemente sich in informationellen und materiellen Beziehungen untereinander und mit der Umwelt befinden.[122] Demzufolge lassen sich Prozesse anhand ihres Gegenstands in *informationelle* und *materielle Prozesse* unterscheiden.

Informationelle Prozesse – auch Informationsprozesse genannt – betreffen den Austausch und die Verarbeitung von Informationen. Auch der Umgang mit materiellen Informationsträgern wie Akten oder Disketten wird zu den informationellen Prozessen gezählt.[123] Charakterisieren lassen sich informationelle Prozesse dadurch, dass zu ihrem Start Informationen beschafft werden bzw. vorliegen müssen, die während des Prozesses transformiert und gespeichert und danach in transformierter Form übermittelt werden.[124] Der klassische Output eines informationellen Prozesses ist eine Entscheidung.[125]

Materielle Prozesse beinhalten dagegen den Austausch physischer Objekte zwischen den Einheiten innerhalb eines Unternehmens und dessen Umwelt sowie die Verarbeitung derartiger Objekte. Sie treten vorrangig innerhalb der Leistungserstellung eines Unternehmens auf und sind besonders stark bei Unternehmen ausgeprägt, deren Leistungserstellung materielle Objekte zum Gegenstand haben. Bei Dienstleistungsunternehmen können Informationsträger die Rolle materieller Objekte einnehmen, wie bspw. Banknoten und Münzgeld bei Banken. Ein materieller Prozess beginnt mit der Beschaffung der zu verarbeitenden Güter, beinhaltet deren Be- oder Verarbeitung und endet mit dem Absatz der erzeugten Produkte. Bei der Gestaltung materieller Prozesse stehen Aspekte der zeitlichen und vor allem der örtlichen Koordination stärker im Vordergrund, als es bei informationellen Prozessen der Fall ist, da Informationen in den meisten Fällen geringere Anforderungen an die Transportwege stellen.[126]

4.4.3 Art der Tätigkeit

Gemäß Hill/Fehlbaum/Ulrich können *operative Prozesse* und *Leitungsprozesse* unterschieden werden.[127] Unterscheidungskriterium ist in diesem Fall die Art der ausgeübten Tätigkeit. In operativen Prozessen findet die Leistungserstellung eines Unternehmens

[122] Vgl. Grochla (1883), S.76.
[123] Vgl. Schulte-Zurhausen (2002), S.52.
[124] Vgl. Grochla (1983), S.105.
[125] Vgl. Grochla (1983), S.76 ff.
[126] Vgl. Grochla (1983), S.120 f.
[127] Vgl. Hill/Fehlbaum/Ulrich (1994), S.26.

statt, weshalb sie auch *Leistungsprozesse* genannt werden. Sie haben einen materiellen oder immateriellen Output, der entweder an externe oder an interne Kunden gerichtet ist. Bei externen Kunden als Abnehmer wird von direkten Leistungsprozessen, bei internen Kunden entsprechend von indirekten Leistungsprozessen gesprochen. Diese Klassifizierung innerhalb der Leistungsprozesse entspricht der Differenzierung zwischen Kern- und Supportprozessen.

Im Rahmen von Leitungs- oder Managementprozessen werden die Unternehmensaktivitäten geplant, kontrolliert und gesteuert. Innerhalb der Leitungsprozesse wird unterschieden zwischen strategischen und operativen Managementprozessen. Die strategischen Managementprozesse haben zum Ziel, die langfristige Entwicklung des Unternehmens zu gestalten. In den operativen Managementprozessen werden Vorgaben aus dem strategischen Bereich umgesetzt und es werden die Leistungsprozesse gesteuert.[128] Abbildung 6 fasst die aufgeführten Prozessarten zusammen.

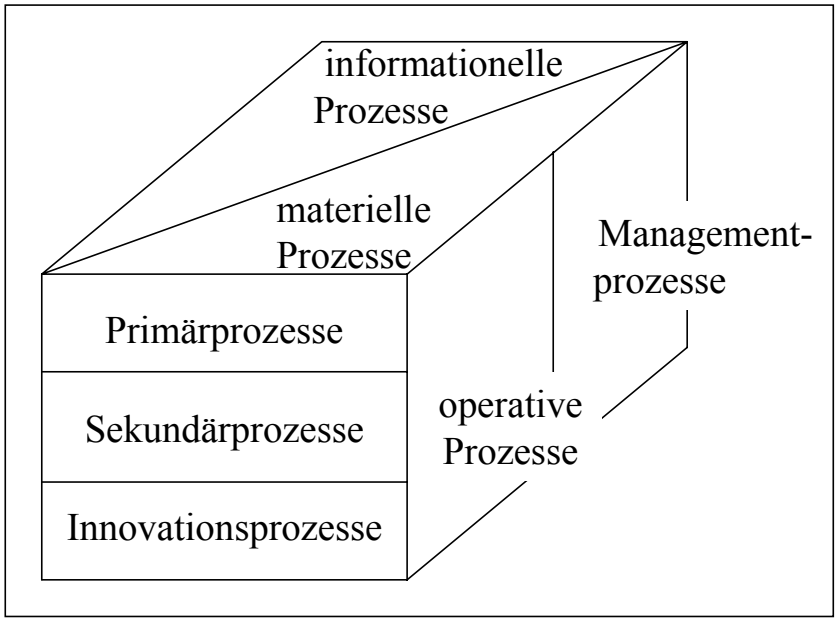


Abbildung 6: Klassifizierungsmöglichkeiten von Prozessen
Quelle: Schulte-Zurhausen (2002), S.52.

4.5 Merkmale von Prozessen

Bis zu dieser Stelle der Arbeit wurden als Merkmale von Prozessen der Input, die Aktivitäten innerhalb des Prozesses sowie der Output genannt. In diesem Kapitel werden

[128] Vgl. Vahs (2005), S.215 f.

weitere Bestandteile genannt, die ein Prozess aufweisen kann, sowie deren Zusammenhänge beschrieben.

Gegenstand eines jeden Prozesses ist eine bestimmte *Aufgabe*, deren Erfüllung das Ziel des Prozesses darstellt. Diese Aufgabe sollte mit einem Substantiv und einem Verb beschrieben werden, also bspw. „Order ausführen".[129] Die Abfolge aller Prozesse eines Unternehmens dient dem Zweck, betriebliche Leistungen zu erbringen und durch deren Verkauf am Markt eine Gewinnspanne zu erwirtschaften.[130]

Jeder Prozess hat einen *Input* bzw. Eingabe und einen *Output* bzw. Ausgabe.[131] Die Aufgabe des Prozesses kann nun unter Zuhilfenahme dieser beider Begriffe genauer beschrieben werden. Sie besteht darin, aus einem definierten Input einen definierten Output zu erzeugen. Input können Arbeitsgegenstände, Informationen und Energie sein, die im Prozess verändert oder verwendet werden. Der Output besteht aus im Sinne des Prozessziels veränderten, verwendeten oder neu erstellten Arbeitsgegenständen, Informationen oder Energie.[132]

Der Input stammt aus mindestens einer *Quelle*, also einem Sender oder Lieferanten. Der Output wird an mindestens eine *Senke*, also einem Empfänger oder Kunden, weitergereicht.[133] Bei einer Abfolge von Prozessen kann der Output eines Prozesses einem nachgelagerten Prozess als Input dienen.[134]

Ausgelöst wird ein Prozess durch ein *Ereignis*, also einer Zustandsänderung. Ein Ereignis kann externer oder zeitlicher Natur sein. Wird ein Prozess durch einen Input angestoßen, handelt es sich um ein Ereignis externer Natur. Bei einem Ereignis zeitlicher Natur beginnt der Prozess zu einem bestimmten Zeitpunkt.[135]

Um die Transformation des Input in einen bestimmten Output durchzuführen, finden im Verlaufe des Prozesses verschiedene *Aktivitäten*[136] bzw. Funktionen statt, die miteinander in einem zeitlichen und sachlogischen Zusammenhang stehen.[137]

Die Aktivitäten werden von *Menschen* und/oder *Betriebs- bzw. Arbeitsmitteln* – auch Sachmittel genannt - erledigt.[138] Menschen und Sachmittel werden in diesem Zusam-

[129] Vgl. REFA (1991), S.151.
[130] Vgl. Porter (1999), S.67 f.
[131] Vgl. Jackson/Ashton (1995), S.108; vgl. REFA (1991), S.152 f.
[132] Vgl. REFA (1991), S.152 f.
[133] Vgl. Schulte-Zurhausen (2002), S.50.
[134] Vgl. Wilhelm (2003), S.24.
[135] Vgl. Schulte-Zurhausen (2002), S.50.
[136] Vgl. Jackson/Ashton (1995), S.111.
[137] Vgl. Becker/Schütte (1996), S.52 f.
[138] Vgl. REFA (1991), S.151 f.

menhang als *Aktionsträger* bezeichnet[139], die für die Durchführung der Aktivitäten zu *Produktiveinheiten* zusammengefasst werden.[140] Bei den meisten Prozessen werden die Aktivitäten von Menschen unter Zuhilfenahme von Sachmitteln erledigt. Je nachdem, welche Aktivitäten zu einem Prozess zusammengefasst werden, kann ein Prozess auch ohne Beteiligung von Menschen, also vollautomatisch durchgeführt werden. Als Sachmittel dienen Anlagen, Einrichtungen, Maschinen, Werkzeuge und Organisationsmittel.[141]

Die Durchführung der Aktivitäten wird durch *Methoden* geregelt, die mehr oder weniger stark formalisiert sind. Eine Methode beschreibt die Art und Weise der Beteiligung eines Menschen an einem Prozess.

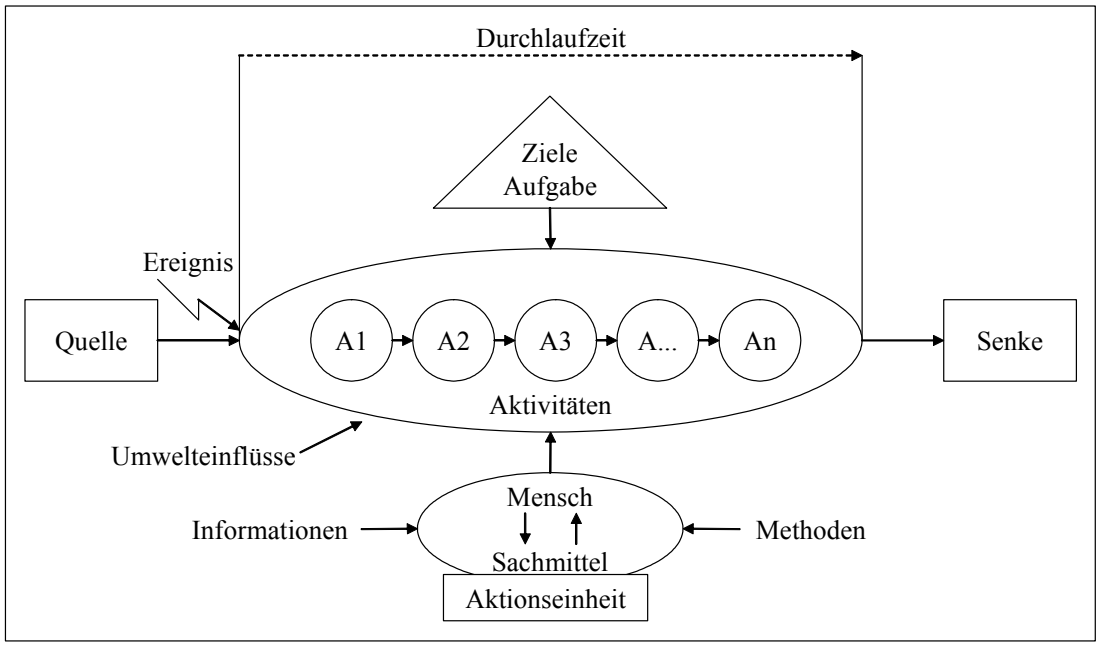


Abbildung 7: Merkmale eines Prozesses
Quelle: in Anlehnung an Schulte-Zurhausen (2002), S.50.

Um die Aktivitäten durchführen zu können, benötigen die Aktionsträger Wissen. Dieses Wissen kann in zwei Ausprägungen vorliegen, nämlich in der Kenntnis über Methoden – dem so genannten Methodenwissen – oder in anderweitigen *Informationen*, die zumeist in gespeicherter Form vorliegen.

[139] Vgl. Schulte-Zurhausen (2002), S.50.
[140] Vgl. Küpper (1982), S.13.
[141] Vgl. REFA (1991), S.151 f.

Ein Prozess hat eine bestimmte *Durchlaufzeit*, die sich von dem Moment, in dem die Aktionsträger erstmalig aktiv werden, bis zu dem Moment, in dem der vollständige und fehlerfreie Output an die Senke übergeben wird, erstreckt.[142]
Umwelteinflüsse können in Form von physikalischen, chemischen, biologischen, organisatorischen und sozialen Faktoren die Durchführung eines Prozesses beeinflussen. Sie wirken insbesondere auf Menschen und Sachmittel ein.[143]
In Abbildung 7 werden die Merkmale eines Prozesses zusammengefasst.

4.6 Darstellungsmittel für Prozesse

Eine Grundvoraussetzung der Prozessorganisation ist das Wissen über den Inhalt der Prozesse. In diesem Kapitel werden drei mögliche Mittel für die Darstellung von Prozessen beschrieben und begründet, welches Mittel hierfür am geeignetesten ist.

4.6.1 Beschreibung in Textform

Viele Sacherverhalte werden in Unternehmen in Textform dokumentiert. In den Anfängen der Prozessorganisation wurden auch Prozesse auf diese Art und Weise beschrieben. Schnell kristallisierten sich einige Nachteile dieser Beschreibungsform heraus.
So sind Texte nicht eindeutig und lassen dem Leser viele Interpretationsmöglichkeiten. Auf Basis von Texten lassen sich keine weitergehenden Analysen der Prozesse durchführen, in deren Rahmen bspw. der Prozess auf Brüche im Prozessablauf untersucht werden soll. Es lässt sich nur mühsam feststellen, ob der Prozess vollständig erfasst wurde. Zwischen den Beschreibungen verschiedener Prozesse lassen sich nur schwer Zusammenhänge ermitteln, was bspw. von Interesse wäre, um durch Identifizierung gleichartiger Tätigkeiten in verschiedenen Prozessen Rationalisierungspotentiale zu ermitteln. Die Aktualisierung von textualen Prozessbeschreibungen ist aufwändig, da es schwer erkennbar ist, auf welche Bestandteile eines Prozesses sich eine Änderung der betrieblichen Realität auswirkt. Folge sind Inkonsistenzen der Beschreibungen.
Die zahlreichen Nachteile haben dazu geführt, dass andere Mittel für die Prozessbeschreibung genutzt werden.[144]

[142] Vgl. Schulte-Zurhausen (2002), S.51.
[143] Vgl. REFA (1991), S.153.
[144] Vgl. Bergsmann/Grabek/Brenner (2005), S.54.

4.6.2 Prozessgitter

Eine andere Möglichkeit besteht darin, Prozesse mit Hilfe von Tabellenkalkulationsprogrammen wie Microsoft Excel zu beschreiben. Hier können einheitliche Vorlagen erstellt werden, mit denen übersichtlich die Abfolge der Aktivitäten, die beteiligten Aktionsträger sowie Inputs und Outputs abgebildet werden können. Abbildung 8 zeigt ein Beispiel für die Anwendung eines Prozessgitters. Durch die Übersichtlichkeit und die Möglichkeit, Prozesse unternehmensweit in einer einheitlichen Struktur zu erfassen, werden einige schwer wiegende Nachteile der Textbeschreibung eliminiert. Zudem erlauben Tabellenkalkulationsprogramme bis zu einem gewissen Grad Auswertungen, die sich durch die Möglichkeiten des Filterns, Sortierens und durch formelgestützte Berechnungen umsetzen lassen. Durch Makroprogrammierung lassen sich die genannten Funktionalitäten automatisieren, was den Komfort erhöhen und die für eine Auswertung benötigte Zeit verringern kann. Andere Nachteile der Textbeschreibung bleiben bestehen.

Prozessablauf			Abteilung				
Laufende Nr.	Teilprozess-Bezeichnung		a	b	c	d	e
01	Teilprozess 16	a					
02	Teilprozess 23	d					
03	Teilprozess 18	b					
04	Teilprozess 17	a					
05	Teilprozess 19	c					
06	Teilprozess 20	e					
07	Teilprozess 24	d					

Abbildung 8: Anwendung eines Prozessgitters
Quelle: Bergsmann/Grabek/Brenner (2005), S.55.

Die Umsetzung der genannten Auswertungsmöglichkeiten sowie die Pflege dieser so genannten Prozessgitter können sehr aufwändig sein, zudem unterliegen die Auswertungen gewissen Restriktionen. Eine Verteilung der einzelnen Prozessgitter auf verschiedene Tabellenblätter kann die Leichtigkeit der Auswertung und Änderung zusätz-

lich einschränken. Prozessgitter bedeuten damit einen Fortschritt zu den Textbeschreibungen, sind aber kein ideales Instrument zur Abbildung von Prozessen.[145]

4.6.3 Prozessmodell

Die Probleme der Prozessbeschreibung mittels Texten und Prozessgitter wurden durch das Zusammenwirken von drei Entwicklungen behoben, die innerhalb der letzten zehn Jahre stattfanden.

Die erste Entwicklung bestand darin, Prozesse graphisch abzubilden. Zumeist wurden hierfür Ablaufdiagramme genutzt. Derartige Prozessmodelle haben den Vorteil, dass Betrachter sie leicht lesen und den Inhalt schnell erfassen können. Das Problem der Eindeutigkeit der Modelle blieb jedoch vorerst bestehen, so dass Analysen nur eingeschränkt möglich waren und die Pflege sich weiterhin schwierig gestaltete.

Parallel wurden Modellierungssprachen entwickelt. Ihr Einsatz sorgte für eine Vereinheitlichung der Prozessdarstellung, so dass Modelle nunmehr eindeutig und klar waren. Viele dieser Modellierungssprachen erlauben eine in hohem Maße eindeutige Darstellung von Prozessen, sind dafür auf der anderen Seite aber sehr formal und folglich für Modelladressaten aus den Fachabteilungen schwer verständlich. Eine hohe Eindeutigkeit bedingt damit Defizite in der Lesbarkeit und Kommunizierbarkeit, was die Eignung derartiger Modellierungssprachen für die Darstellung von Geschäftsprozessen stark einschränkt. Ein Durchbruch in Bezug auf die Verbindung von hoher Genauigkeit und Verständlichkeit bedeutete daher die Entwicklung der Ereignisgesteuerten Prozesskette (EPK) von Scheer. Die Methode der EPK ist formal genug, um mit ihr Prozessmodelle zu erzeugen, die so exakt sind, dass sie weitergehende Analysen erlauben. Gleichzeitig ist sie so einfach, dass auch Mitarbeiter aus den Fachabteilungen sie in kurzer Zeit erlernen können.

Als drittes wurde Software entwickelt, die die graphische Modellgestaltung erleichtert und über eine integrierte Datenbank verfügt. In dieser Datenbank können zum einen die Regeln von Modellierungssprachen gespeichert werden, so dass das Modellierungswerkzeug den Modellierer bei der Einhaltung der Regeln der Sprache unterstützt. Zum anderen wird dafür gesorgt, dass Objekte, die z.B. einen bestimmten Aktionsträger oder eine Aktivität repräsentieren, nur einmal angelegt und anschließend in verschiedenen Modellen verwendet werden können. Je nach Ausstattungsumfang der einzelnen Model-

[145] Vgl. Bergsmann/Grabek/Brenner (2005), S.54 f.

lierungswerkzeuge bildet ein derartiges Repository die Basis für umfangreiche Möglichkeiten der Analyse und Simulation. Der Aufwand für die Pflege der Modelle wird verringert, da eine Änderung an einem zentral hinterlegten Objekt an allen Stellen wirkt, an denen das Objekt in den Modellen verwendet wird.[146]

4.7 Grundlagen der Geschäftsprozessmodellierung

4.7.1 Modellierungszweck und Modellgestaltung

Ein Modell kann verstanden werden „als ein immaterielles Abbild der Realwelt ... für Zwecke eines Subjekts“[147]. Aus dieser Definition kann geschlossen werden, dass der Verwendungszweck eines Modells bei der Modellierung zu beachten ist. Ein möglicher Verwendungszweck eines Prozessmodells ist das Risikomanagement. Die Gestaltung eines Prozessmodells vollzieht sich auf der syntaktischen und der semantischen Ebene. Auf syntaktischer Ebene gilt es, die Notation der verwendeten Modellierungssprache einzuhalten. Dies lässt sich relativ leicht umsetzen, zumal viele Modellierungswerkzeuge den Modellierer dabei unterstützen. Schwieriger ist es, ein Modell so zu gestalten, dass es seinen Zweck – oder genauer gesagt den Zweck des Modelladressaten – erfüllt. Dies vollzieht sich auf der semantischen, also der inhaltlichen Ebene.
Mit den Grundsätzen ordnungsmäßiger Modellierung (GoM) wurden Gestaltungsregeln aufgestellt, die eine bedarfsgerechte Modellgestaltung zum Ziel haben. Sie bestehen aus sechs Grundsätzen. Im Zusammenhang mit dem Zweck des Modells ist der Grundsatz der Relevanz hervorzuheben. In ihm wird die Forderung aufgestellt, im Vorwege die Ziele der Modellierung zu explizieren. Dies geschieht aus Sicht des Modelladressaten, wenn dieser mit dem Modellierer nicht identisch ist. Ein Prozessmodell erfüllt genau dann den Grundsatz der Relevanz, wenn das Entfernen von Informationen aus dem Modell einen verringerten Grad der Zielerreichung zur Folge hätte. Das Modell muss zudem denjenigen Teil der Realität abbilden, der der Zielerreichung dient, und es muss dies auf einem angemessenen Abstraktionsniveau tun.[148]

[146] Vgl. Bergsmann/Grabek/Brenner (2005), S.57 f.
[147] Becker/Rosemann/Schütte (1995), S.435.
[148] Vgl. Becker/Rosemann/Schütte (1995), S.438.

4.7.2 Erweiterte Ereignisgesteuerte Prozesskette (eEPK)

Es existieren unterschiedliche Modellierungssprachen, die für die Abbildung von Geschäftsprozessen geeignet sind. Im Rahmen dieser Arbeit soll nicht auf Unterschiede zwischen verschiedenen Sprachen eingegangen werden. Stattdessen soll kurz die Syntax der im deutschsprachigen Raum viel genutzten Modellierungssprache EPK beschrieben werden. Wie andere Modellierungssprachen auch, beinhaltet die EPK bestimmte Objekttypen, die eine bestimmte Semantik haben und die in den Modellen in bestimmten Beziehungen zueinander stehen dürfen. Diese Regelungen werden auch als das Metamodell einer Modellierungssprache bezeichnet. Jeder Objekttyp wird in der EPK durch ein bestimmtes graphisches Symbol repräsentiert. Objekttypen der EPK sind bspw. Funktionen und Ereignisse. In den Modellen werden Instanzen der Objekttypen verwendet. Instanzen der Objekttypen werden als Objekte bezeichnet. Ein Objekttyp kann als eine Klasse aufgefasst werden, die gewissermaßen einen Bauplan enthält, der aussagt, welche Eigenschaften ein von ihr abgeleitetes Objekt hat. Wird ein Objekt in einem Modell verwendet, entsteht dadurch eine Objektausprägung, die auf das Objekt verweist. Änderungen an einem Objekt wirken sich auf alle Ausprägungen des Objektes aus.[149]

Grundlegende Objekttypen der EPK sind Funktionen, Ereignisse und Verknüpfungsoperatoren. Funktionen beschreiben Aktivitäten und haben Entscheidungskompetenz für den weiteren Prozessverlauf. Sie werden durch Ereignisse ausgelöst und erzeugen Ereignisse. Ereignisse drücken eingetretene Zustände aus und sind damit eine passive Komponente der EPK.[150] Jede EPK beginnt mit einem oder mehreren (Start-) Ereignissen und endet mit einem oder mehreren (End-) Ereignissen. Eine EPK besteht aus einer wechselseitigen Abfolge von Ereignissen und Funktionen, was als bipartiter Graph bezeichnet wird.[151] Es existieren drei verschiedene Verknüpfungsoperatoren, mit denen Verzweigungen nicht-linearer Prozessketten modelliert werden können:

- Die konjunktive Verknüpfungen *AND* drückt den Sachverhalt „a und b“ aus.
- Die disjunktive Verknüpfung *XOR* drückt den Sachverhalt „a oder b“ aus. Sie wird auch als *exklusives ODER* bezeichnet.

[149] Vgl. Rosemann/Schwegmann/Delfmann (2005), S.61 ff.
[150] Vgl. Keller/Nüttgens/Scheer (1992), S.9 ff.
[151] Vgl. Rosemann/Schwegmann/Delfmann (2005), S.66 f.

- Die adjunktive Verknüpfung *OR* drückt den Sachverhalt „a oder b oder [a und b]“ aus. Sie wird auch als *inklusives ODER* bezeichnet.[152]

Aus der Eigenschaft des Ereignisses als passives Element der EPK folgt, dass ihm weder eine disjunktive noch eine adjunktive Verzweigung folgen darf, da es ansonsten unzulässigerweise über den weiteren Prozessverlauf entscheiden würde. Sofern eine Verzweigung der Prozesskette im weiteren Prozessverlauf wieder zusammengeführt wird, ist an der zusammenführenden Gabelung der gleiche Verknüpfungsoperatorentyp wie an der auseinanderführenden Gabelung der Prozesskette zu verwenden.
Je nach Bedarf können EPKs um weitere Informationen angereichert werden.[153] Dies ist von besonderer Relevanz, wenn EPKs als Grundlage für das Management operationeller Risiken dienen sollen. So können Organisationseinheiten, Stellen oder Personen mit Funktionen assoziiert werden. Eine Assoziation ist eine Beziehung zwischen Objekten gleichrangiger Klassen bzw. zwischen den Objekten innerhalb einer Klasse.[154] Durch die Modellierung der Verantwortlichkeiten für die Durchführung von Funktionen findet der Faktor *Mensch* Eingang in die Modelle. Als weitere Ergänzung der EPK können allgemeine Ressourcen und Anwendungssysteme abgebildet werden. Der letztgenannte Punkt spielt eine zentrale Rolle für die Modellierung der Abhängigkeit einer Funktion von Systemen. Eine um derartige semantische Beschreibungselemente ergänzte EPK wird als erweiterte Ereignisgesteuerte Prozesskette (eEPK) bezeichnet.[155]
Geschäftsprozessmodelle schaffen Transparenz hinsichtlich *interner Verfahren* und der für ihre reibungslose Durchführung benötigten *Menschen* und *Systeme*. Diese drei Faktoren wurden weiter oben als mögliche Ursachen für das operationelle Risiko vorgestellt. Auch können Prozessmodelle als Hilfestellung dabei dienen, Auswirkungen der vierten möglichen Risikoursache *externe Ereignisse* auf die drei genannten innerbetrieblichen Ursachen des operationellen Risikos abzuschätzen. Daher existieren verschiedene Geschäftsprozessmodell-basierte Ansätze für das Management operationeller Risiken.

[152] Vgl. Keller/Nüttgens/Scheer (1992), S.14; vgl. Rosemann/Schwegmann/Delfmann (2005), S.66.
[153] Vgl. Rosemann/Schwegmann/Delfmann (2005), S.66 f.
[154] Vgl. Scheer (2001), S.114.
[155] Vgl. Scheer/Nüttgens/Zimmermann (1997), S.5.

5. Geschäftsprozessmodell-basierte Ansätze für das Management operationeller Risiken

In diesem Kapitel werden Geschäftsprozessmodell-basierte Ansätze für die Identifikation und Bewertung operationeller Risiken beschrieben und hinsichtlich ihrer Eignung für den Einsatz in Banken untersucht. Die in den Ansätzen enthaltenen Bewertungen der Risiken verstehen sich als eine allgemeine Einschätzung der Auswirkungen des Eintretens eines Risikoereignisses auf einen Geschäftsprozess bzw. auf eine Funktion innerhalb eines Prozesses und nicht als Berechnung einer monetären Größe.

5.1 Risk Mapping

Risk Mapping ist ein vom Baseler Ausschuss vorgeschlagenes Verfahren für das Management operationeller Risiken. Es dient der Identifikation von Schwachstellen in Geschäftsprozessen und soll damit die Priorisierung von Verbesserungsmaßnahmen erleichtern.[156]

Produkt des Risk Mapping ist eine Risk Map. Es existiert keine einheitliche Auffassung darüber, wie genau eine solche „Risko-Landkarte“ auszusehen hat. In dieser Arbeit wird dem Ansatz gefolgt, demzufolge es sich bei einer Risk Map um ein Geschäftsprozessmodell handelt, das um Informationen über Risikofaktoren angereichert wurde. Ziel des Risk Mapping soll es sein, die Risiken möglichst vollständig abzubilden. Hierfür ist ein tief greifendes Verständnis der zugrunde liegenden Geschäftsprozesse notwendig.[157]

Aufgrund seiner engen Verbindung zur Geschäftsprozessmodellierung wird das Verfahren auch *Risk and Process Mapping* genannt.[158] Der Begriff Process Mapping kann mit dem der Geschäftsprozessmodellierung gleichgesetzt werden.

So beinhaltet der erste Schritt des Risk Mapping die Modellierung der Geschäftsprozesse einer Bank.

Aufbauend auf den Prozessmodellen werden die Risiko-Treiber analysiert. Risiko-Treiber sind alle für die Prozesse benötigten Personen, Systeme, Anlagen sowie externe Ereignisse, deren Eintreten Auswirkungen auf den Prozess haben kann. Dies sollte durch Mitarbeiter der unteren Führungsebene geschehen, da sie einen großen Einfluss zumindest auf die drei erstgenannten Faktoren haben. Dabei wird auch ermittelt, unter

[156] Vgl. Baseler Ausschuss (2003), S.8.
[157] Vgl. Scandizzo (2005), S.231 ff.
[158] Vgl. Doerig (2003), S.73.

welchen Umständen welche Ressourcen ausfallen können und welche Auswirkungen dies auf die Prozesse hätte.

Im Anschluss werden die Risiko-Faktoren der Ressourcen ermittelt, die auf die einzelnen Aktivitäten innerhalb der Prozesse wirken. Diese sind: Anzahl, Qualität, Relevanz[159] und Ausfall. Die Risiko-Faktoren geben die Dimension an, innerhalb der die Wichtigkeit einer Ressource für eine Aktivität gemessen werden kann.

Im Anschluss werden die Risiken identifiziert. Dafür wird der Frage nachgegangen, was die Auswirkungen des Auftretens kritischer Risiko-Faktoren auf den Geschäftsprozess wären. Hierbei kommt der Vorteil der prozessorientierten Analyse zur Geltung, da sie die direkten Auswirkungen einer Fehlfunktion auf nachgelagerte Instanzen entlang der Wertschöpfungskette der Bank zu Tage treten lässt. Eine isolierte Betrachtung einzelner organisatorischer Einheiten oder einzelner Funktionen würde diese Informationen nicht liefern und damit ein unzureichendes Bild der Risikosituation der Bank zeichnen. Der Schritt der Risikoidentifikation ist besonders gründlich zu vollziehen, um möglichst vollständig die Risken der Bank zu erfassen.

Auf Basis der identifizierten Risiken werden die potentiellen Verluste identifiziert und analysiert. Die Ergebnisse dieses Schrittes dienen einer späteren Priorisierung der Maßnahmen, die zur Verminderung der operationellen Risiken einzuleiten sind. Angaben über die Höhe von Verlusten werden in vielen Fällen zunächst auf Annahmen des Managements beruhen. Es sollte sichergestellt werden, dass diese Angaben mit Daten aus etwaigen nach Durchführung des Risk Mapping eintretenden Verlustfällen aktualisiert werden. Zur Unterstützung können externe Verlustdatenbanken herangezogen werden.

Damit ist das eigentliche Risk Mapping beendet. Einem Vorschlag von Scandizzo folgend können im Anschluss die dabei gewonnenen Erkenntnisse, nämlich die Risiko-Treiber, Risiko-Faktoren und potentielle Verluste, dazu genutzt werden, um Key Risk Indicators (KRI) zu definieren.[160]

KRI sind Indikatoren, die eine Prognosen über risikobehaftete Entwicklungen innerhalb der Bank erlauben. KRI bestehen aus einer bewusst getroffenen Auswahl an Key Performance Indicators (KPI) und Key Control Indicators (KCI). KCI treffen Aussagen über die Wirksamkeit der Kontrollmechanismen innerhalb der Bank.[161] KPI sollen Prognosen erlauben, wie wahrscheinlich eine Fehlfunktion innerhalb eines Prozesses ist.

---

[159] Das in der referenzierten englischsprachigen Quelle verwendete Wort *criticality* wurde mit *Relevanz* übersetzt.

[160] Vgl. Scandizzo (2005), S.237 ff.

[161] Vgl. Doerig (2003), S.72.

Sie sind häufig mit dem Output von Geschäftsprozessen und Problemen innerhalb der Prozesse verbunden. Beispiele für KPI sind die Anzahl an Fehlern bei der Abwicklung von Wertpapierordern oder Ausfallzeiten von Systemen.[162]

Vorteil des Risk Mapping ist, dass mit dem Verfahren die operativen Risiken einer Bank sehr detailliert analysiert werden können. Dies kann sich auf der anderen Seite jedoch auch nachteilig auswirken, da der Einsatz mit einem hohen Aufwand verbunden ist.

5.2 Control & Risk Self Assessment (CRSA)

Ursprünglich ist das Control & Risk Self Assesment (CRSA) eine Methode der internen Revision. Eine andere gängige Bezeichnung ist *Control Self Assessement*.[163]

Ziel des CRSA ist es, die Wirksamkeit interner Kontrollen zu beurteilen. Da die Unangemessenheit oder das Versagen interner Kontrollen ein operationelles Risiko darstellt, wie es auch der in Kapitel 3.1.1 geschilderte Fall der Barings Bank gezeigt hat, wird das CRSA mittlerweile nicht nur als ein Instrument der Revision, sondern auch als eines des Risikomanagements betrachtet.[164] Insbesondere die aus dem KonTraG und SOX folgenden Regelungen fokussieren auf die internen Kontrollsysteme, so dass es ein breites Anwendungsgebiet für diese Methode gibt. Ein wesentliches Element des CRSA ist dessen prozessorientierter Ansatz, dem der Gedanke zugrunde liegt, dass Kontrolle nicht losgelöst von den Geschäftsprozessen eines Unternehmens, sondern vielmehr in die Geschäftsprozesse integriert sein sollte.

Das Verfahren wird zumeist in Form eines strukturierten und moderierten Workshops durchgeführt. Vor Beginn des Workshops sollten die Geschäftsziele des Unternehmens fixiert sein. Im Rahmen des Workshops sollen aus mangelhaften Kontrollen resultierende Gefahren für die Zielerreichung des Unternehmens identifiziert und entsprechende Verbesserungen der Kontrollen entwickelt werden. Daher nehmen an ihm Mitarbeiter teil, die Interesse an der Erreichung der Ziele haben und die die Zielerreichung beeinflussen können.[165] Die Teilnehmer sollten ein tief greifendes Verständnis für die zu analysierenden Geschäftsprozesse haben. Idealerweise liegen Prozessmodelle vor, damit sichergestellt werden kann, dass das Verständnis auch übereinstimmend ist.[166]

---

[162] Vgl. Scandizzo (2005), S.239 f.
[163] Vgl. Jans (2003), S.27.
[164] Vgl. Barnes Marschdorf (1999), S.698.
[165] Vgl. Barnes Marschdorf (1999), S.694 ff.
[166] Vgl. Balfan/Gledhill/Haubenstock (2002).

Der erste Schritt des Workshops besteht darin, mögliche Gefahren für die Zielerreichung zu identifizieren und zu bewerten. Die Identifikation geschieht oft durch Brainstorming.[167] Zur Unterstützung kann an dieser Stelle eine Risk Map herangezogen werden.[168] Die Bewertung der Risiken beinhaltet die Abschätzung ihres relativen Gefährdungspotentials für die Zielerreichung und eine Bestimmung ihrer Eintrittswahrscheinlichkeiten.

Im nächsten Schritt werden bestehende Kontrollen identifiziert. Dabei wird ebenfalls durch Brainstorming die Wirksamkeit der Kontrollen bewertet. Sollten Kontrollen als ineffizient angesehen werden, so werden die Risiken, denen sie nunmehr nicht entgegenwirken, als unkontrollierte Risiken festgehalten. Nach Identifikation aller Kontrollen werden durch einen Abgleich mit den Risiken ggf. weitere unkontrollierte Risiken ermittelt. Eine andere Bezeichnung für ein unkontrolliertes Risiko ist *Residualrisiko*. Es ist kein Ziel des CRSA, alle Residualrisiken zu eliminieren, da Kontrollen Kosten verursachen und auch bei vorhandener Kontrolle nicht zwangsläufig alle Residualrisiken ausgeschaltet werden können. Etwaigen Gefährdungen der Schlüsselziele der Bank sollte jedoch besonderes Augenmerk gewidmet werden.

Im folgenden Schritt werden alle Residualrisiken analysiert. Dabei wird entschieden, welche Risiken eingegangen und welche beeinflusst werden sollen, da ihre möglichen Schadensausmaße inakzeptabel sind. Für die Kontrolle der letztgenannten Risiken werden Maßnahmen erarbeitet.

Darauf folgt eine Optimierung des Kontrollportfolios. Ziel ist es, erneut zu überprüfen, ob die Kontrollen vollständig sind. Zudem soll ermittelt werden, ob die Kontrollen ein gesundes und sinnvolles Maß nicht überschreiten und bestimmte Kontrollen mehrfach vorgenommen werden. Als letztes werden die Ergebnisse des Workshops kommuniziert.[169]

Vorteile des CRSA liegen darin, dass bei den Prozessverantwortlichen das Bewusstsein dafür geweckt bzw. bestätigt wird, dass sie für das Risikomanagement mit verantwortlich sind und dass Kontrollen einen Nutzen für die Bank haben. Dies kann zu einer erhöhten Akzeptanz von Kontrollen führen, da falsche Eindrücke über die Rolle der internen Revision beseitigt werden. Das Verständnis der Verbindungen zwischen den Geschäftsprozessen, Risiken und Unternehmenszielen wird verbessert.

[167] Vgl. Barnes Marschdorf (1999), S.697.
[168] Vgl. Jans (2003), S.28.
[169] Vgl. Barnes Marschdorf (1999), S.697 f.

Als Nachteil ist zu nennen, dass die Güte der Ergebnisse stark von den am CRSA beteiligten Personen abhängig ist. Zudem ist die Methode bei einer Anwendung auf alle Risiken zeitaufwändig und dadurch, dass Mitarbeiter der Managementebene an den Workshops beteiligt sind, personalkostenintensiv. Dem kann dadurch entgegengewirkt werden, dass die im ersten Schritt stattfindende Priorisierung der Risiken dazu genutzt wird, lediglich die größten Risiken einer weiteren Betrachtung zu unterziehen.[170]

5.3 Fehlermöglichkeits- und Einflussanalyse (FMEA)

Die Fehlermöglichkeits- und Einflussanalyse (FMEA), auch Failure Mode and Effect Analysis oder - weniger gebräuchlich - Ausfalleffektanalyse genannt, wurde ursprünglich für Projekte in der Luft- und Raumfahrt entwickelt.[171] Ziel der FMEA ist es, bereits in einem frühen Stadium der Entwicklungs- und Fertigungsprozesse mögliche Fehlerquellen und deren Auswirkungen zu entdecken und ihnen damit frühzeitig entgegenwirken zu können. Je eher Fehler erkannt werden, desto leichter und weniger kostspielig ist ihre Beseitigung.[172] Es soll also erreicht werden, Fehler in Entwicklung und Fertigung zu vermeiden, anstatt sie beheben zu müssen.[173] Eine weitere Option der FMEA besteht darin, im Unternehmen vorhandenes Wissen über Fehler und deren Auswirkungen auf die Qualität der Produkte zu sammeln und verfügbar zu machen.[174]

Es wird zwischen zwei FMEA-Arten unterschieden. Diese sind die *System-FMEA Produkt* und die *System-FMEA Prozess*. Die System-FMEA Produkt wird im Anschluss an die Fertigstellung des Entwurfs eines neuen Produktes durchgeführt. Mit ihrer Hilfe sollen mögliche Fehler des Entwurfs entdeckt, hinsichtlich ihrer Schwere bewertet und Maßnahmen zur Behebung der Fehler vorgeschlagen werden. Ihr Ziel liegt somit darin, mit einem möglichst einwandfreien Entwurf die Basis für ein fehlerfreies Produkt zu legen. Die System-FMEA Prozess setzt nach Erstellung der Fertigungspläne ein und hat die gleichen Aufgaben und Ziele wie die System-FMEA Produkt, jedoch bezogen auf die Fertigungsprozesse.[175]

Durchgeführt werden FMEAs durch interdisziplinäre Teams, die bei Bedarf von Mitarbeitern aus den Fachabteilungen unterstützt werden. Exemplarisch soll nun die Durch-

[170] Vgl. Jans (2003), S.28.
[171] Vgl. Pfeifer (2001a), S.395.
[172] Vgl. Ruta (1999). S.44.
[173] Vgl. Schubert (1993), S.5.
[174] Vgl. Pfeifer (2001a), S.394 f.
[175] Vgl. Pfeifer (2001a), S.397 f.

führung einer System-FMEA Prozess skizziert werden. Die Ergebnisse der Arbeitsschritte werden in FMEA-Formularen festgehalten.[176]

Die Durchführung beginnt damit, die Prozessschritte und ihre Inhalte zu erfassen. Aufbauend auf diesen Informationen können im Rahmen der Fehleranalyse alle potentiellen Fehlerarten der Prozessschritte sowie ihre möglichen Folgen aufgenommen werden. Die Folgen der Fehler werden von den Teammitgliedern aus Sicht des Kunden bewertet und es werden alle denkbaren Ursachen für die potentiellen Fehler festgehalten.

Die Risikobewertung wird durch das Sammeln von möglichen Prüfmaßnahmen eingeleitet, mit denen die Fehler nach ihrem Eintreten entdeckt oder mit denen sie von vornherein vermieden werden können. Somit liegen für jede potentielle Fehlerart mögliche Ursachen und Auswirkungen vor und es kann für jede Fehlerursache die Auftretenswahrscheinlichkeit *A* sowie für jeden Fehler die Entdeckungswahrscheinlichkeit *E* und die Schwere der Auswirkung *S* ermittelt werden. Die Multiplikation dieser drei Werte ergibt die Risikoprioritätszahl *RPZ*. Es gilt also:

$$RPZ = A * E * S$$

mit

RPZ = Risikoprioritätszahl

A = Auftretenswahrscheinlichkeit

E = Entdeckungswahrscheinlichkeit

S = Schwere der Auswirkung.

Die Faktoren *A*, *E* und *S* können jeweils einen Wert zwischen 1 und 10 annehmen, wobei höhere Werte eine höhere Auftretenswahrscheinlichkeit, eine niedrigere Entdeckungswahrscheinlichkeit bzw. einen höheren Schweregrad ausdrücken.

Der Höchstwert für eine Fehlerart beträgt 1.000, wobei in der Praxis oft eine *RPZ* = 125, also 5 * 5 * 5, als kritische Grenze angesehen wird. Abgesehen von Fehlerursachen mit einer hohen RPZ führen alle Einzelbewertungen für einen der drei Faktoren größer als 8 zu weiterführenden Untersuchungen, die in die Entwicklung von Verbesserungsmaßnahmen durch das FMEA-Team münden sollen. Hierbei kann dessen interdisziplinäre Zusammensetzung die Ergebnisse der kreativen Denkprozesse verbessern. Die entworfenen Maßnahmen sind anschließend sowohl auf ihre Auswirkungen auf die drei Bewertungsgrößen als auch unter Kostengesichtspunkten kritisch zu würdigen und im

[176] Vgl. dazu Witter (1995), S.15 ff.

Falle eines positiven Votums umzusetzen. Die RPZ-Werte nach Umsetzung der Maßnahmen sind als Ist-Werte festzuhalten. Es wird empfohlen, nach einer gewissen Zeit diese auf theoretischen Überlegungen basierenden Werte zu überprüfen.[177]

Banken bieten keine Produkte im eigentlichen Sinne, sondern vielmehr Dienstleistungen an. Diese werden jedoch auch gewissermaßen *konstruiert*, so dass die System-FMEA Produkt zur Lösung bestimmter Probleme bei Bankdienstleistungen eingesetzt werden kann. Die System-FMEA Prozess kann Banken bei der Verbesserung von Geschäftsprozessen unterstützen, die wiederkehrende und gleich bleibende Elemente beinhalten.[178]

Ein Vorteil der FMEA liegt darin, dass sie trotz der vorgegebenen Methodik ein relativ flexibles Instrument ist, da die Analyse operationeller Risiken aus unterschiedlichen Perspektiven stattfinden kann. Die in der Methodik verankerte, nachgelagerte Überprüfung der Ergebnisse erhöht den Druck auf die Teilnehmer, realistische Einschätzungen abzugeben und die gesetzten Ziele zu erreichen.[179]

Der Nachteil liegt in dem hohen Zeit- und Personalaufwand. Daher erscheint die FMEA nicht dazu geeignet, mit ihr die gesamten operationellen Risiken einer Bank zu erfassen. Stattdessen bietet sie sich für die gezielte Analyse bestimmter, besonders wichtiger Risiken an.[180] Unter Kosten-Nutzen-Aspekten sinnvolle Einsatzgebiete könnten die Einführung neuer Produkte, IT-Systeme oder Reorganisationsprojekte sein.[181]

5.4 Baumanalysen

Das Ziel der Baumanalysen ist es, qualitative Daten über Fehlermöglichkeiten in Prozessen zu gewinnen. Ihr ursprüngliches Einsatzgebiet ist die Entwicklung und Überprüfung von Sicherheitskonzepten technischer Anlagen. Sie eignen sich insbesondere zur Analyse stark standardisierter Prozesse. Es wird unterschieden zwischen der Fehlerbaumanalyse und der Störablaufanalyse.[182]

Bei der Fehlerbaumanalyse, auch Fault-Tree-Analysis (FTA) genannt, wird versucht, eine Aussage über das Verhalten eines Systems beim Auftreten eines bestimmten Fehlers zu machen und die aus dem Fehler resultierende Ausfallwahrscheinlichkeit zu er-

[177] Vgl. Witter (1995), S.19 ff.
[178] Vgl. Münchbach (2001), S.166 f.
[179] Vgl. Münchbach (2001), S.171.
[180] Vgl. Minz (2004), S.95.
[181] Vgl. Münchbach (2001), S.171.
[182] Vgl. Minz (2004), S.89.

mitteln.[183] Dazu werden die unmittelbaren Ursachen ermittelt, die anschließend ggf. wiederum in ihre Ursachen herunter gebrochen werden. Der eigentlichen Erstellung des Fehlerbaums, in dem die Beziehungen zwischen einem Fehler und dessen Ursachen graphisch dargestellt werden, gehen folgende Schritte voraus.[184]

Zuerst werden im Rahmen einer Analyse detaillierte Kenntnisse über den untersuchten Prozess gesammelt. Hierbei wird bestimmt, welche Funktionen im Rahmen des Prozesses ausgeführt werden, welche Menschen sowie internen und externen Hilfsmittel hierfür benötigt werden und wie der Prozess auf Ausfälle einzelner Hilfsmittel, ganzer Funktionen innerhalb des Prozesses und auf menschliche Fehler reagiert. Daraufhin wird das unerwünschte Ereignis und die Zuverlässigkeitskenngröße festgelegt, deren Reaktion auf das unerwünschte Ereignis analysiert werden soll. Eine Zuverlässigkeitskenngröße kann bspw. eine maximal zulässige Anzahl an Ausfällen pro Jahr sein. Der letzte Schritt vor dem Aufstellen des Fehlerbaums besteht darin, die Ausfallarten der am Prozess beteiligten Komponenten und die Auswirkungen derer Ausfälle zu bestimmen. An dieser Stelle empfiehlt es sich, die Ergebnisse einer FMEA zu berücksichtigen.

Auf Basis dieser Vorarbeiten wird der Fehlerbaum erstellt. Es existieren unterschiedliche Auffassungen darüber, mit welcher Bedeutung welche Symbole in einem Fehlerbaum verwendet werden.[185] Abbildung 9 zeigt ein Beispiel für einen Fehlerbaum gemäß Münchbach.

Der fertige Fehlerbaum wird zu Auswertungen genutzt, die Informationen dafür liefern, welche Ausfallkombinationen das unerwünschte Ereignis bedingen können, wie häufig das unerwünschte Ereignis eintritt und was die kleinste Kombination an Ausfällen ist, die das unerwünschte Ereignis zur Folge hat.[186]

[183] Vgl. Pfeifer (2001a), S.348.
[184] Vgl. Kenney (1993), S.176.
[185] Vgl. Kenney (1993), S.176 f.; vgl. Münchbach (2001), S.161 sowie die Bedeutungen der Shapes der Schablone *Shapes zur Fehlerstrukturanalyse* in Microsoft Visio 2003.
[186] Vgl. Pfeifer (2001a), S.349 ff.

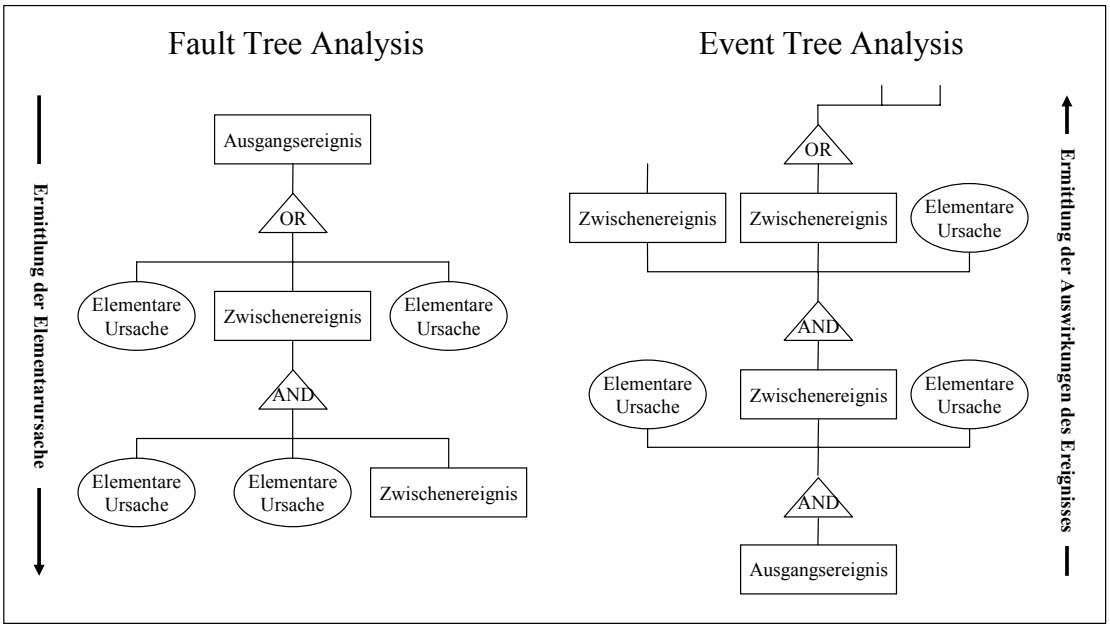


Abbildung 9: Fehlerbaum und Ereignisbaum gemäß Münchbach
Quelle: Münchbach (2001), S.162.

Die Störablaufanalyse, auch Event Tree Analysis (ETA), geht den umgekehrten Weg, indem von einem auslösenden Ereignis ausgehend dessen mögliche Auswirkungen auf nachgelagerte Schritte eines Prozesses ermittelt werden.[187] Sie ist genau genommen eine Variante der FMEA.[188] Resultat ist ein Ereignisbaum, der verschiedene Ereignisketten enthält, die zu bestimmten Auswirkungen führen, die wiederum an den Blättern, also den Endpunkten des Baumes, abgelesen werden können.

Störablaufanalysen sind insbesondere dazu geeignet, Ereignisse zu untersuchen, die viele verschiedene Auswirkungen haben können. Falls das auslösende Ereignis einer Störablaufanalyse direkt zu einem bestimmten Fehler im Prozess führt, ist es sinnvoller, die Gründe, die zu diesem Fehler führen können, in einer Fehlerbaumanalyse zu untersuchen. Die Quintessenz einer Störablaufanalyse kann der Auf- bzw. Ausbau von Sicherheitsmaßnahmen sein, die negative Auswirkungen von Risikoereignissen vermeiden sollen.[189]

Die Vorteile der Baumanalysen liegen in der methodisch analytischen Vorgehensweise,[190] die sich zur Analyse von Optimierungspotentialen eignet,[191] und der anschaulichen Darstellung. Der genormte Aufbau erlaubt den Software-gestützten Aufbau und Auswertung, was bei größeren Fehlerbäumen zur Vermeidung von Fehlern ausdrücklich

[187] Vgl. Kenney (1993), S.177 ff.
[188] Vgl. Kletz (1999), S.54.
[189] Vgl. Kenney (1993), S.177 ff.
[190] Vgl. Ruta (1999), S.43; vgl. Minz (2004), S.92.
[191] Vgl. Münchbach (2001), S.163.

zu empfehlen ist. Zudem können im Rahmen der Baumanalysen auch Kombinationen von Ereignissen berücksichtigt werden, was bei der FMEA nicht möglich ist.[192] Baumanalysen können das Bewusstsein der Mitarbeiter für Fehlerquellen und Zusammenhänge in Prozessen erhöhen.[193]

Als Nachteile sind die hohen inhaltlichen, zeitlichen und methodischen Anforderungen an die Teilnehmer zu nennen, die zunehmen, je komplexer die Bäume werden. Insbesondere die Abschätzung der Wahrscheinlichkeiten ist problematisch, zumal sie auf subjektiven Einschätzungen beruht.[194] In Bezug auf operationelle Risiken eignet sich die Anwendung von Baumanalysen nur für standardisierte Prozesse. Die Vielzahl der operationellen Risiken in Banken kann das Festlegen des unerwünschten Ereignisses erschweren.

Aufgrund der hohen Kosten bietet sich der Einsatz der Baumanalysen zur Analyse von Prozessen an, in denen besonders häufig Fehlerereignisse eintreten oder in denen Fehler besonders hohe Schadenssummen zur Folge haben können.[195]

5.5 Predictive Human Error Analysis (PHEA)

Die Predictive Human Error Analysis (PHEA) ist ein Verfahren, mit dem systematisch ermittelt werden kann, welche Fehler von Menschen in den einzelnen Schritten eines Prozesses verursacht werden können.

Für die Anwendung der PHEA wird vorausgesetzt, dass klar ist, was in einem Prozess geschieht und was die Rollen der an ihm beteiligten Personen sind. Dafür sollte idealerweise ein Prozessmodell vorliegen. Ist der gesamte Prozess in hohem Maße Risikokritisch, werden alle Prozessschritte einer PHEA unterzogen, ansonsten geschieht dies nur für kritische Prozessschritte.

Für jeden zu untersuchenden Prozessschritt wird ermittelt, ob in ihm Menschen Tätigkeiten durchführen, die zu Fehlern führen können. Dies geschieht anhand einer vorgegebenen Liste, die verschiedene mögliche Fehler beinhaltet, die in sechs Fehlerkategorien unterteilt sind. Diese Liste ist in Abbildung 10 ersichtlich. Die Bezeichnung jeder Kategorie impliziert eine bestimmte Tätigkeit, so dass in diesem Schritt der PHEA alle Prozessschritte zunächst auf das Vorhandensein einer der Tätigkeiten überprüft werden. Prozessschritte, die keine dieser letztlich Fehlerquellen repräsentierenden Tätigkeiten

[192] Vgl. Ruta (1999), S.43; vgl. Minz (2004), S.92.
[193] Vgl. Minz (2004), S.92.
[194] Vgl. Ruta (1999), S.43; vgl. Minz (2004), S.92.
[195] Vgl. Minz (2004), S.92.

enthalten, werden im weiteren Verlauf der PHEA nicht betrachtet. Wichtig ist es hierbei, dass die die PHEA durchführende Person so genannte *Performance-influencing factors* (PIF)[196] beachtet. PIFs können z.B. Zeitdruck oder schwierig zu bedienende Software sein. Danach wird hinterfragt, welche konkreten Fehler der zutreffenden Fehlerkategorien in den Prozessschritten auftreten können, welche Auswirkungen die Fehler haben können, anhand welcher Faktoren der Fehler erkannt werden kann, bevor dessen Auswirkungen zu Tage treten und mit welchen Strategien der Fehler vermieden werden kann.

Action Errors	
A1	Action too long/short
A2	Action mistimed
A3	Action in wrong direction
A4	Action too little/much
A5	Misalign
A6	Right action on wrong object
A7	Wrong action on right object
A8	Action omitted
A9	Action incomplete
A10	Wrong action on wrong object
Checking Errors	
C1	Checking omitted
C2	Check incomplete
C3	Right check on wrong object
C4	Wrong check on right object
C5	Check mistimed
C6	Wrong check on wrong object
Retrieval Errors	
R1	Information not obtained
R2	Wrong information obtained
R3	Information retrieval incomplete
Transmission Errors	
T1	Information not transmitted
T2	Wrong information transmitted
T3	Information transmission incomplete
Selection Errors	
S1	Selection omitted
S2	Wrong selection made
Plan Errors	
P1	Plan preconditions ignored
P2	Incorrect plan executed

Abbildung 10: Liste mit Fehlerkategorien und Fehlern zur Durchführung einer PHEA
Quelle: Center for Chemical Process Safety (1994), S.192.

[196] Performance-influencing factors (engl.) = leistungsbeeinflussende Faktoren.

Die Ergebnisse der PHEA werden auf geeigneten Formularen schriftlich festgehalten. Sie sollen den Verantwortlichen in den Unternehmen aufzeigen, welche Prozessschritte besonders schwerwiegende Risiken beinhalten, die in menschlichen Fehlern begründet sind, und damit den Impuls zu Gegenmaßnahmen geben. Diese Maßnahmen können Warnungen an die Mitarbeiter, eine Verbesserung der verwendeten Sachmittel oder eine besondere Würdigung bestimmter Aspekte im Rahmen der Ausbildung und Schulung der Mitarbeiter sein.

Von Vorteil ist, dass die Methode durch ihren systematischen Ansatz eine sehr gründliche Analyse schwerwiegender menschlicher Fehler erlaubt und dass sie vorbeugend wirkt.[197] Ihr liegt eine breite Auffassung der menschlichen Fehler zugrunde, so dass sie prinzipiell auch in Banken zur Analyse operationeller Risiken der Ursache *Mensch* genutzt werden kann.[198]

Nachteilig für den Einsatz dieser Methode in Banken dürfte es sein, dass keine öffentlich zugänglichen Quellen über ihren Einsatz in Banken vorliegen, und daher am Anfang eines Einsatzes das zeitaufwändige Unterfangen stünde, die Fehlerkategorien und Fehler der Liste an die Tätigkeiten in Banken anzupassen.[199]

5.6 Szenario-Analysen

Die What-If-Analyse („Was-Wäre-Wenn-Analyse“) ist die einfachste Variante einer Szenarioanalyse und findet in erster Linie Anwendung bei der Prävention von Katastrophenrisiken.[200] Sie kann sowohl bei bestehenden, als auch bei neuen Prozessen genutzt werden. Eine What-If-Analyse wird von einer meist zwei- bis dreiköpfigen Expertengruppe durchgeführt, die der Frage nachgeht, was die Folgen wären, wenn eine bestimmte Sache schief läuft oder nicht funktioniert. Die Beantwortung dieser Frage beruht sowohl auf ihrem eigenen Wissen, als auch auf Interviews, die mit an den Prozessen beteiligten Mitarbeitern geführt werden. Um mit dieser Methode eine möglichst vollständige Identifikation möglicher Risikoquellen zu erreichen, ist es wichtig, dass sie von erfahrenen Personen durchgeführt wird.

Ein Geschäftsprozess wird im Rahmen dieser Methode üblicherweise von seinem Startereignis ausgehend dem Prozessverlauf folgend untersucht. Die Expertengruppe befragt die für die Durchführung einzelner Funktionen im Prozess verantwortlichen Mitarbeiter,

[197] Vgl. Center for Chemical Process Safety (1994), S.190 ff.
[198] Vgl. Münchbach (2001), S.159.
[199] Vgl. Minz (2004), S.98.
[200] Vgl. Minz (2004), S.99.

was bei Eintritt eines bestimmten Ereignisses die Folgen wären und was unternommen werden könnte bzw. müsste, um unerwünschten Folgen zu begegnen. Alternativ kann in der Befragung auch untersucht werden, was die Auswirkungen bestimmter Maßnahmen sind, die z.B. der Sicherheit des Personals beim Eintritt von Risikoereignissen dienen sollen.[201]

Das Worst-Case-Szenario ist eine andere Ausprägung der Szenario-Analyse, die auch als Stress-Analyse bezeichnet wird.[202] Es zielt auf die Identifikation von „low-frequency – high-severity"-Risiken ab. Häufig sind diese Risikosituationen durch das Zusammentreffen mehrerer unerwünschter Ereignisse gekennzeichnet,[203] wohingegen die What-If-Analyse von einzelnen Ereignissen ausgeht.[204] Die zu untersuchenden Szenarien werden entweder selber entwickelt oder basieren auf Fällen, die sich bei anderen, insbesondere der gleichen Branche zugehörigen Unternehmen ereignet haben. Worst-Case-Szenarien werden häufig für die Überprüfung von Notfallplänen genutzt, die die Aufrechterhaltung des Geschäftsbetriebs sichern sollen. Bezogen auf die Bankenbranche ist eine denkbare im Rahmen einer solchen Analyse zu untersuchende Risikokonstellation ein lang andauernder Ausfall von Wertpapierhandelssystemen während turbulenter Zeiten an den Wertpapiermärkten.

Ein großer Vorteil der Szenarioanalysen liegt in ihrer hohen Freiheit, wodurch sie auch für die Identifikation nur qualitativ erfassbarer Risiken geeignet sind. Die an die Mitarbeiter gestellten Fragen können bereits zu einer Steigerung des Bewusstseins für Risiken führen. Zudem sind Szenarioanalysen die am leichtesten und schnellsten anwendbaren Verfahren zur Risikoidentifikation,[205] wie es auch vom Baseler Ausschuss konstatiert wird.[206]

Nachteile liegen darin, dass die Verfahren von Haus aus keine Strukturierung beinhalten und die Ergebnisse auf subjektiven Einschätzungen beruhen. Dem lässt sich bis zu einem gewissen Grad dadurch entgegentreten, dass erfahrene Personen mit der Analyse betraut werden. Die Erfahrungen dieser Personen können jedoch auf der anderen Seite dazu führen, dass deren Blickwinkel verengt ist und bei der Analyse bestimmte Aspekte außer acht gelassen werden.[207] Zudem ist der Zeitaufwand für diese Methode sehr hoch

[201] Vgl. Kenney (1993), S. 127.
[202] Vgl. Minz (2004), S.100.
[203] Vgl. Münchbach (2001), S.156.
[204] Vgl. Kenney (1993), S. 126.
[205] Vgl. Münchbach (2001), S.156 f.
[206] Vgl. Baseler Ausschuss (1994), S.15 f.
[207] Vgl. Münchbach (2001), S.156 f.

und es wird qualifiziertes internes wie auch externes Personal benötigt, wodurch hohe Kosten entstehen.[208]

5.7 Ursache-Wirkungsdiagramm

Während bei den Szenario-Analysen versucht wird, die Folgen bestimmter Ereignisse zu ermitteln, wird bei einem Ursache-Wirkungsdiagramm der entgegengesetzte Weg gegangen, indem Symptome auf mögliche Ereignisse zurückgeführt werden. Andere Bezeichnungen für dieses Verfahren sind in Anlehnung an den Namen seines Erfinders Ishikawa-Diagramm und in Anlehnung an sein Aussehen Fischgrätendiagramm. Im Gegensatz zur Szenario-Analyse wird bei der Erstellung eines Ursache-Wirkungsdiagramms eine strukturierte Vorgehensweise verfolgt. Ergebnis ist ein Diagramm, das von der Struktur her demjenigen in Abbildung 11 entspricht.

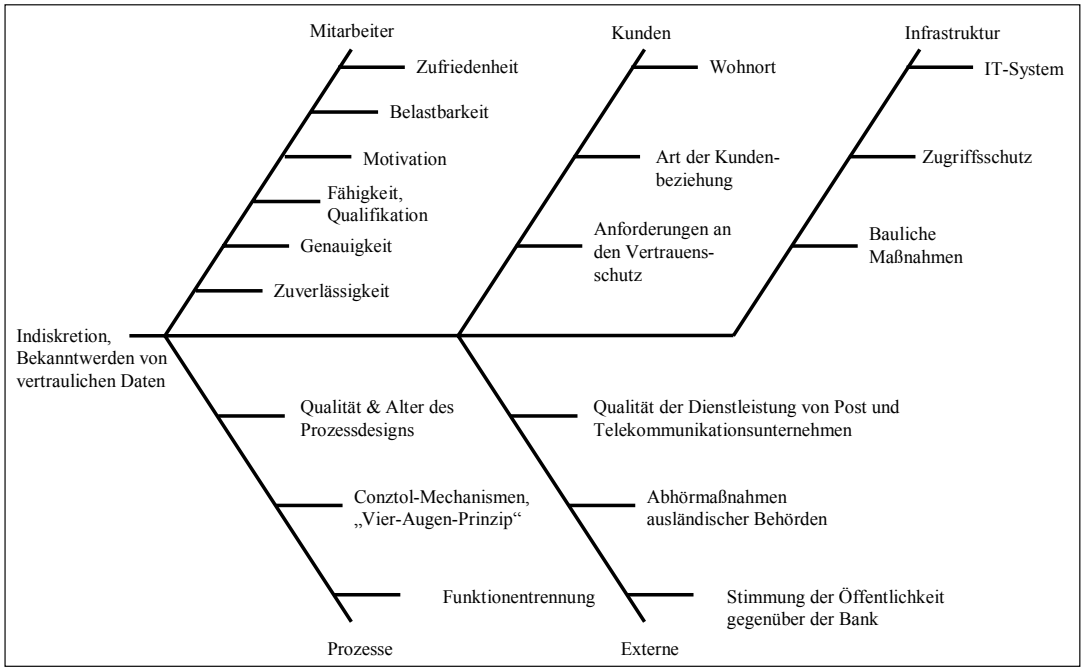


Abbildung 11: Ursache-Wirkungs-Diagramm
Quelle: Münchbach (2001). S.158.

An der Spitze des waagerechten Striches befindet sich die Auswirkung eines Fehlers. Durch Brainstorming werden mögliche Ursachen für diese Wirkung ermittelt, die in zwei Gruppen unterteilt werden. Die eine Gruppe enthält unabhängige Ursachen, die andere Einflussfaktoren, die andere Ursachen beeinflussen. Die unabhängigen Ursachen

[208] Vgl. Minz (2004), S.101.

finden sich im Diagramm an den Enden der schräg von oben und unten auf den waagerechten Strich zulaufenden Striche. Die Subfaktoren werden gewissermaßen als Gräten mit waagerechten Strichen an die zugehörigen Striche der übergeordneten Ursachen angehängt. Sollte das Brainstorming eine tiefere Untergliederung der Ursache zum Ergebnis haben, dann sollte die Hauptursache kritisch hinterfragt und das Diagramm ggf. in mehrere kleiner Diagramme unterteilt werden, da es ansonsten an Übersichtlichkeit verliert.[209] Die Ursachen korrespondieren in vielen Fällen mit der 7-M-Checkliste, die die Faktoren Mensch, Maschine, Material, Methode, Mitwelt, Management und Messung repräsentiert.[210]

Vorteile des Ursache-Wirkungsdiagramms liegen in der Einfachheit des Verfahrens und der Möglichkeit, Ursachen für operationelle Risiken weiter zu unterteilen. Diese detaillierte Sichtweise kann der Identifikation der eigentlichen Gründe der Risiken zuträglich sein.

Aus der Einfachheit ergeben sich jedoch auch die Nachteile des Verfahrens. So eignet es sich nicht zur Analyse komplexer Zusammenhänge und verknüpfter Risikoereignisse.[211] Aufgrund der Tatsache, dass es bei Symptomen ansetzt, eignet es sich nicht für eine vorbeugende Risikoanalyse. Die Diskussion der möglichen Ursachen und ihrer Verbindungen zueinander kann sehr aufwändig sein, was die Akzeptanz der Ergebnisse vermindern kann.[212]

5.8 Hazard and Operability Study (HAZOP)

Das Verfahren Hazard and Operability Study (HAZOP) wurde ursprünglich in der Chemieindustrie für die Identifikation und Analyse von Risiken technischer Systeme entwickelt.[213] Im deutschen Sprachraum ist es auch unter dem Begriff PAAG-Verfahren bekannt, wobei die Abkürzung PAAG für *Prognose-Auffinden-Ausmerzen-Gegenmaßnahmen* steht.[214] Eingesetzt werden kann die HAZOP sowohl in der Entwicklungsphase als auch bei bereits laufenden Systemen.[215] Genau betrachtet handelt es sich

[209] Vgl. Pfeifer (2001b), S.7 f.
[210] Vgl. Pfeifer (2001a), S.40.
[211] Vgl. Münchbach (2001), S.157 f.
[212] Vgl. Minz (2004), S.103.
[213] Vgl. Redmill/Chudleigh/Catmur (1999), S.1 f.
[214] Vgl. Minz (2004), S.104.
[215] Vgl. Redmill/Chudleigh/Catmur (1999), S.29.

bei diesem Verfahren um eine weiterentwickelte und stark formalisierte Szenarioanalyse.[216]

Ausgangspunkt einer HAZOP ist je nachdem, ob ein technisches System oder ein Prozess untersucht wird, ein graphisches Abbild des Systems oder ein Prozessmodell. Die folgenden Ausführungen beziehen sich auf die Risikoanalyse eines Prozesses. Mit Hilfe des Prozessmodells wird von den Mitgliedern des die HAZOP durchführenden Teams das Ziel eines jeden Prozessschrittes definiert. Das Konzept der HAZOP basiert auf der Annahme, dass jede Abweichung von dem Ziel eines Prozessschrittes ein Risiko für die fehlerfreie Durchführung des gesamten Prozesses darstellen kann. Daher beinhaltet das Konzept eine Liste von Schlüsselwörtern, die mögliche Abweichungen ausdrücken. Eine Auflistung von Schlüsselwörtern mitsamt ihrer Bedeutung findet sich in Abbildung 12. Aufgabe des HAZOP-Teams ist es, für jeden Prozessschritt Gründe sowie Auswirkungen für jede der möglichen Abweichungen vom Ziel des Prozessschritts zu finden. Dies geschieht durch Brainstorming und Diskussion. Die identifizierten Gründe und Auswirkungen jeder Abweichung werden beginnend mit ihrer schwersten Auswirkung und in der Reihenfolge derer Schweregrade aufgelistet. Danach werden auf demselben Wege mögliche Sicherheitsmaßnahmen und weitere Empfehlungen gesammelt.[217]

Schlüsselwort	*Bedeutung*	*Erklärung (Beispiel)*
No	Negation	Ein Folgeschritt in der Prozesskette tritt nicht ein (z.B. eine Unterschriftenkontrolle wird nicht durchgeführt und der Prozess blockiert, da der Transaktionsstatus nicht auf OK steht).
More	Quantitative Zunahme	Mehr Inputs, als zu bewältigen sind (z.B. Auftragseingänge)
Less	Quantitative Abnahme	Für einen Folgeschritt notwendige Eingaben fehlen (z.B. Formulare sind nicht vollständig ausgefüllt).
More than	Qualitative Zunahme	Eine Transaktion wird doppelt eingegeben, aber so dass es nicht als dieselbe Transaktion identifizierbar ist.
Part of	Qualitative Abnahme	Ein Input entspricht nicht der Qualität, die für einen Folgeschritt erforderlich ist (altes Formular verwendet, so dass dieses nicht elektronisch weiterverarbeitet werden kann).
Reverse	Logisches Gegenteil	Eine Transaktion wird genau entgegengesetzt ausgeführt (z.B. Verkauf statt Kauf).
Other than	Vollständige Substitution	Sonstige Ereignisse, die im Gegensatz zum normalen Prozessablauf eintreten können (z.B. plötzlicher IT-Systemausfall).

Abbildung 12: Schlüsselwörter der HAZOP
Quelle: Münchbach (2001), S.164.

Besonders interessant im Hinblick auf die Identifikation operationeller Risiken sind die der HAZOP zugrunde liegenden möglichen Gründe für Zielabweichungen der Prozess-

[216] Vgl. Münchbach (2001), S.163 f.
[217] Vgl. AcuTech, S.1.

schritte. Diese liegen in menschlichen Fehlern, Fehlern bei den verwendeten Gerätschaften und externen Ereignissen[218] und entsprechen damit möglichen Ursachen für operationelle Risiken.

Ein Vorteil der HAZOP ist es, dass der Versuch unternommen wird, alle Möglichkeiten der Zielabweichung und deren Auswirkungen systematisch zu erfassen.[219] Es können sowohl qualitative als auch quantitative Abweichungen formuliert werden, was für die Flexibilität der HAZOP spricht.

Nachteile des Verfahrens liegen darin, dass tendenziell die aus einer HAZOP resultierenden Sicherheitsmaßnahmen zu streng ausfallen. Die HAZOP ist für den Einsatz in einem statischen Umfeld konzipiert, daher sind die Ergebnisse nach Reorganisationsmaßnahmen ggf. hinfällig.[220] Die Ergebnisse sind stark von den Teammitgliedern und deren Zusammenarbeit abhängig.[221] Zudem ist das Verfahren sehr zeit- und personalintensiv, was es wenig dafür geeignet erscheinen lässt, alle Prozesse einer Bank zu analysieren.

Als Einsatzgebiet würde sich die gezielte Überprüfung der Plausibilität von Risikoindikatoren sowie der Auswirkungen von Nichterreichung festgelegter kritischer Werte bei Risikoindikatoren anbieten.[222] Risikoindikatoren sind Kenngrößen, die Rückschlüsse auf die Risikosituation einer Bank erlauben.[223]

Die Beschreibung Geschäftsprozessmodell-basierter Ansätze zum Management operationeller Risiken und deren Bewertung hinsichtlich ihrer grundsätzlichen Eignung für den Einsatz in Banken bildet die Basis für die Suche nach einer geeigneten Lösung für die CONRAD HINRICH DONNER BANK AG.

[218] Vgl. AcuTech, S.5 f., im englischen Originaltext werden die Kategorien *human failure*, *equipment failure* und *external events* genannt.
[219] Vgl. Minz (2004), S.105.
[220] Vgl. Münchbach (2001), S.165.
[221] Vgl. Minz (2004), S.106.
[222] Vgl. Münchbach (2001), S.165.
[223] Vgl. Baseler Ausschuss (2003), S.8 f.

6. Fallbeispiel CONRAD HINRICH DONNER BANK AG

Im ersten Teil dieses Kapitels wird die Ausgangssituation für das Projekt bei der CONRAD HINRICH DONNER BANK AG (CHD) beschrieben. Die Vorgehensweise orientierte sich an Aussagen des IT-Grundschutzhandbuches, die daher im zweiten Teil skizziert werden. Das Vorgehen bei der Entwicklung des Konzeptes wird im dritten Teil dokumentiert. Im letzten Teil werden Modellierungswerkzeuge daraufhin untersucht, ob sie sich für die Umsetzung des entwickelten Konzepts eignen.

6.1 Ausgangssituation

Die CHD ist als Bank mit Sitz in Deutschland gemäß den geltenden Vorschriften dazu verpflichtet, operationelle Risiken zu managen. Daher wurde in der CHD ein Projekt zu dieser Thematik durchgeführt. Aufgrund der zentralen Stellung der mit der Nutzung von IT verbundenen Risiken innerhalb der operationellen Risiken sollte in dem Projekt ein Tool entwickelt und validiert werden, das die Verantwortlichen der IT-Abteilung der CHD dabei unterstützt, mit dem Einsatz von IT verbundene operationelle Risiken zu identifizieren und zu steuern.

Es wurde von Seiten der CHD der Entschluss getroffen, einen Geschäftsprozessmodell-basierten Ansatz zu wählen, weil er die Erfüllung der von den Verantwortlichen geäußerten Wünsche versprach. Diese bestanden darin, die Auswirkungen des Ausfalls von IT-Ressourcen auf bankexistenzielle Prozesse möglichst transparent darzustellen. Zudem sollten Informationen über die Relevanz, die einzelne Ressourcen für die Prozesse haben, bei den Fachabteilungen in Verbindung mit der Darstellung der Prozesse erhoben und gespeichert werden können. Auf diese Art und Weise sollte eine möglichst vollständige Sammlung von Daten auf der Grundlage eines einheitlichen Verständnisses seitens der IT-Abteilung und der Fachabteilungen über den Inhalt der Geschäftsprozesse gewährleistet werden. Die Daten sollten für Auswertungen nutzbar sein, mit denen Informationen über Risiken verfügbar sein sollten.

Zur Validierung des Konzeptes sollten einige Prozesse gemäß dem zu entwickelnden Konzept modelliert werden. Dem Modellierungszweck *Risikomanagement* entsprechend sollte dabei ein hohes Abstraktionsniveau gewählt werden, das gleichzeitig so detailliert ist, dass es eine Abbildung aller für die Prozessdurchführung benötigter Ressourcen erlaubt. Eine gleichzeitige Nutzung der Modelle zum Erschließen von Vorteilen der Prozessorganisation war nicht beabsichtigt. Gegenstand der Betrachtung sollte aus-

schließlich die Verfügbarkeit der Systeme sein. Andere Fehlermöglichkeiten der IT, wie Vertraulichkeit und Integrität, sollten keine Berücksichtigung finden.
Die Verfügbarkeit ist in dem Fall, in dem sie nicht gegeben ist, die auffälligste Ausprägung einer IT-Fehlfunktion. Sie ist dadurch gekennzeichnet, dass Systeme nicht laufen, wodurch möglicherweise Prozesse stillstehen. Vertraulichkeit zielt darauf ab, dass Daten nicht von unbefugten Dritten eingesehen werden können. Integrität meint die Korrektheit der Daten. Inkorrekte Daten können zu vielerlei Fehlern und Problemen führen.[224]
Von den im fünften Kapitel beschriebenen Ansätzen versprach das Risk Mapping in Verbindung mit der Integration von KPI am interessantesten zu sein. Die übrigen Ansätze kamen im frühen Stadium des Projektes nicht in Frage, da sie das Vorhandensein von Prozessmodellen voraussetzen. Der mit dem Risk Mapping verbundene Nachteil des hohen Aufwands wird in der CHD nicht zum tragen kommen, da es nur auf bankexistenzielle Prozesse angewendet wird. Spezifische Aspekte der IT wurden in das Projekt integriert, indem sich die Vorgehensweise in Grundzügen an Aussagen des IT-Grundschutzhandbuches orientierte.

6.2 IT-Grundschutzhandbuch

Mit der Herausgabe des IT-Grundschutzhandbuches wurde von Seiten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) der hohen Abhängigkeit der heutigen Gesellschaft und insbesondere der Bankenbranche von der IT Rechnung getragen. Aus dieser hohen Abhängigkeit resultiert die Möglichkeit schwerwiegender Schäden bei Ausfällen der IT. Ziel des Grundschutzhandbuches ist es daher, die von der IT verarbeiteten Daten zu schützen und die Sicherheit der IT zu gewährleisten.[225] Im IT-Grundschutzhandbuch werden Empfehlungen zur Sicherung typischer IT-Systeme gegeben, die gleichzeitig die Basis für die Absicherung besonders schutzbedürftiger Systeme bilden. Typische Systeme sind dadurch gekennzeichnet, dass sie weit verbreitet eingesetzt werden, es sich bei ihnen also um keine individuellen Lösungen handelt. Sie weisen keinen sehr hohen Schutzbedarf hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit auf.[226]

[224] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2004), S.15.
[225] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2004), S.10.
[226] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2004), S.15.

Es werden Vorschläge unterbreitet, wie im Rahmen des IT-Sicherheitsmanagements vorzugehen sei. Die Kernaufgabe des IT-Sicherheitsmanagements besteht darin, ein Sicherheitskonzept für die IT zu entwerfen, das die Grundlage für die Umsetzung der Sicherheitsmaßnahmen bildet. Die Vorschläge sind in mehrere Schritte gegliedert, von denen die ersten beiden für die Herangehensweise an das Projekt genutzt wurden. Dieses sind die IT-Strukturanalyse und die Schutzbedarfsfeststellung.[227]

Im Rahmen der *IT-Strukturanalyse* werden zunächst die Bestandteile der IT eines Unternehmens in einem Netzplan erfasst. Ein Netzplan ist eine graphische Übersicht über die Systemkomponenten und ihre Vernetzung untereinander. Der Netzplan sollte laufend auf einem aktuellen Stand gehalten werden. Um seine Übersichtlichkeit zu erhöhen, sollten weniger relevante Informationen aus ihm entfernt werden. Hierzu sollte aus gleichartigen Komponenten jeweils eine Gruppe gebildet werden, so dass alle Bestandteile einer Gruppe im Netzplan durch *ein* Objekt dargestellt werden. Des Weiteren sind innerhalb der Strukturanalyse in Tabellenform alle Systeme aufzulisten, wobei im Gegensatz zum Netzplan auch geplante und nicht vernetzte Komponenten erfasst werden sollen. Neben den Systemkomponenten sollen ebenfalls Applikationen erfasst werden, an die besonders hohe Anforderungen bezüglich Vertraulichkeit, Integrität oder Verfügbarkeit bestehen.[228]

Die auf die Strukturanalyse folgende *Schutzbedarfsfeststellung* soll der Reihe nach den Schutzbedarf für Applikationen, Systeme, Kommunikationsverbindungen sowie für die IT benötigter Räumlichkeiten hinsichtlich ihrer Vertraulichkeit, Integrität und Verfügbarkeit ermitteln. Im Mittelpunkt der Betrachtung und damit am Anfang der Analyse stehen die Applikationen, da sie die Schnittstelle der IT zu den Geschäftsprozessen darstellen. Aus dem Schutzbedarf einer Applikation kann der Schutzbedarf der für den Betrieb der Applikation notwendigen Systeme, Kommunikationsverbindungen und Räumlichkeiten abgeleitet werden. Umgekehrt ergibt sich aus Sicht eines einzelnen Systems, Kommunikationsweges bzw. Raumes dessen Schutzbedarf aus der Gesamtheit der Folgen, die dessen Fehlfunktion auf Anwendungen hätte.

Im Grundschutzhandbuch wird vorgeschlagen, die Bestandteile der IT drei unterschiedlichen Schutzbedarfskategorien zuzuordnen: *niedrig bis mittel*, *hoch* oder *sehr hoch*. Die Einstufung soll für jede Anwendung separat für jede der möglichen Fehlfunktionen Vertraulichkeit, Integrität oder Verfügbarkeit vorgenommen werden. Zur Unterstützung

[227] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2004), S.37.
[228] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2004), S.38 ff.

dieser Einstufung wurde vom BSI ein Fragenkatalog aufgestellt. Die Antworten auf diese Fragen sind direkt bei den Anwendern zu erheben.

Um die Sichtweise der Anwender zu ergänzen, wird vorgeschlagen, den Schutzbedarf der Anwendungen zusätzlich aus der ganzheitlichen Sicht der Geschäftsprozesse heraus zu ermitteln, so dass eine Aussage darüber getroffen werden kann, wie wichtig eine Anwendung für die Durchführung eines Geschäftsprozesses ist. In vielen Unternehmen ist den Mitarbeitern ihre Rolle im Kontext der Geschäftsprozesse nicht bewusst und folglich kann von ihnen keine die Prozesssicht berücksichtigende Aussage über die Relevanz der von ihnen genutzten Anwendungen erwartet werden. Für diese Fälle wird empfohlen, derartige Einschätzungen von Personen aus der Managementebene einzuholen.

Der Schutzbedarf der Systeme ergibt sich aus dem Schutzbedarf der Anwendungen, für deren Betrieb die Systeme benötigt werden. Dem Maximum-Prinzip zur Folge ist der Schutzbedarf eines Systems so hoch wie der höchste Schutzbedarf der von ihm abhängigen Anwendungen.

Ist eine Anwendung auf den Output einer anderen Anwendung angewiesen und nutzen die Anwendungen unterschiedliche Systeme, so gilt hier das Maximum-Prinzip in Bezug auf die Schutzbedarfe der Systeme.

Nutzen mehrere Anwendungen ein System, so ist zu berücksichtigen, dass eine Fehlfunktion sich auf mehrere Anwendung auswirken kann, wodurch der Schutzbedarf des Systems erhöht werden kann. Dies führt zu einem Kumulationseffekt.

Andersherum können Verteilungseffekte vorliegen, wenn eine Anwendung auf mehrere Systeme zugreift, aber sich der Schutzbedarf der Anwendung nicht auf bestimmte Systeme überträgt, weil nur unwichtige Bestandteile der Anwendung auf bestimmte Systeme zugreifen.

Der Schutzbedarf für Kommunikationswege und Räume ist vom Schutzbedarf der Systeme abzuleiten, die die Verbindungen bzw. die Räumlichkeiten nutzen. Es sind sowohl die Räume zu erfassen, die ausschließlich dem Betrieb von Systemen dienen, als auch bspw. Büroräume, die teilweise für diesen Zweck genutzt werden. Bei von vielen Systemen genutzten Räumen, wie bspw. Serverräumen, sind mögliche Kumulationseffekte zu beachten.[229]

[229] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2004), S.44 ff.

6.3 Vorgehensweise

Aufgrund des Entschlusses, eine Geschäftsprozessmodell-basierte Herangehensweise zu wählen, wurde die Priorisierung des IT-Grundschutzhandbuches umgekehrt und zur Ermittlung des Schutzbedarfs die Prozesssicht gegenüber der Sichtweise der Anwender vorgezogen. Es muss die Möglichkeit bestehen, die Relevanz von Bestandteilen der IT-Landschaft für die Durchführung ganzer Prozesse, und nicht nur für einzelne Funktionen, zu ermitteln und transparent zu machen. Im Folgenden wird der Aufbau des entwickelten Konzepts beschrieben.

6.3.1 Abbildung der IT-Landschaft und Gruppierung ihrer Bestandteile

Zuerst wurde anhand von Sekundärquellen die IT-Landschaft der CHD abgebildet. Dies geschah entgegen dem Vorschlag des IT-Grundschutzhandbuches nicht in Form eines Netzplanes, sondern es wurde zunächst in dem genutzten Geschäftsprozessmodellierungswerkzeug für jede Anwendung und für jede Systemkomponente eine Instanz einer Klasse namens *Sachmittel* erzeugt. Diese Klasse sollte alle dinglichen Ressourcen beinhalten, die für die Durchführung der Geschäftsprozesse innerhalb der CHD benötigt werden. Die Abbildung von Abhängigkeiten zwischen Objekten wurde in einem späteren Schritt verwirklicht.

Dem Vorschlag des Grundschutzhandbuches, bei der Abbildung der IT-Landschaft soweit wie es sinnvoll ist, zu abstrahieren und gleichartige Komponenten mit einem Objekt abzubilden, wurde gefolgt. So wurden alle Clients, das LAN und alle WAN-Verbindungen jeweils mit einem Objekt abgebildet.

In Ergänzung zu dieser Gruppierung im Sinne einer Zusammenfassung mehrerer gleichartiger Komponenten zu einem Objekt wurde eine Gruppierung im Sinne einer Zusammenfassung mehrerer gleichartiger Objekte zu einer Gruppe vollzogen. Hierzu wurde für jede Gruppe eine Unterklasse der Klasse *Sachmittel* gebildet und die einzelnen Objekte in die entsprechenden Klassen verschoben. Dies hat den Vorteil, beim Modellieren eine höhere Übersicht über die verfügbaren Objekte zu haben. Die Gruppenbildung basierte auf der folgenden Überlegung.

Innerhalb einer IT-Landschaft existieren Beziehungen zwischen Anwendungen, Systemen, Netzwerkverbindungen und Räumlichkeiten. Zur Veranschaulichung seien die klassischen Beziehungen innerhalb einer Client-Server-Architektur skizziert. Derartige Anwendungen werden in der CHD eingesetzt. Die Struktur besteht darin, dass das Fron-

tend einer Anwendung auf einem Client läuft und der Client im LAN mit einem Server verbunden ist, auf dem eine zugehörige Serverapplikation läuft. Der Server ist wiederum über das LAN und über eine WAN-Strecke mit einem Backend bei einem externen Dienstleister verbunden. Gleichzeitig befinden sich sowohl der Client als auch der Server in bestimmten Räumen, die ihrerseits Bestandteile bestimmter Gebäude sind. Es sei angemerkt, dass dieses eine häufig anzutreffende, aber gewiss nicht die einzig existente Konstellation ist.
Diesen grundlegenden Zusammenhängen folgend wurden die Bestandteile der IT in den Klassen *Interner IT-Service*, *Server*, *Raum*, *Gebäude*, *Externer IT-Service*, *Netzwerk* und *Sonstiges* gruppiert. Von der Klasse *Netzwerk* wurden die beiden Instanzen *LAN* und *WAN* gebildet, von der Klasse *Sonstiges* die Instanzen *Client* und *Drucker*.

6.3.2 Verwendung von Assoziationen

Dem IT-Grundschutzhandbuch folgend standen die Anwendungen im Mittelpunkt der Betrachtung, da sie die Schnittstelle der IT mit den Geschäftsprozessen bilden. Die Ableitung der Schutzbedarfe der Systeme, Netzwerkverbindungen und Räumlichkeiten vom Schutzbedarf der die Systeme benötigenden Anwendungen wurde hingegen vereinfacht. So wird in dem Konzept nicht die Abhängigkeit der Anwendungen von den Systemen und die Abhängigkeit der Systeme wiederum von Netzwerkverbindungen und Räumlichkeiten betrachtet. Stattdessen werden direkt die Abhängigkeiten der Anwendungen von IT-Komponenten der drei anderen genannten Kategorien dargestellt. Umgesetzt wurde dies in den Prozessmodellen mit Assoziationen.
Dafür wurde in dem Metamodell definiert, dass alle Instanzen der Klasse *Sachmittel* untereinander Assoziationen eingehen dürfen. Anschließend wurden die konkreten Assoziationen auf Instanzebene festgelegt. Eine andere denkbare Vorgehensweise wäre es gewesen, nur Assoziationen zwischen Instanzen von Klassen zuzulassen, die gemäß der oben beschriebenen typischen Verbindungen in einer Client-Server-Architektur in Verbindung zueinander stehen. Diese Vorgehensweise wurde nicht verfolgt, weil dadurch das Metamodell Restriktionen enthalten hätte, die den Modellierer behindert hätten, wenn die Realität vom Regelfall abweicht.
Einen Sonderfall in Bezug auf die Art der verwendeten Assoziationen nehmen die Verbindungen der Server zu Räumen und die Verbindungen der Räume wiederum zu Gebäuden ein. Diese beiden Abhängigkeiten wurden mit so genannten transitiven Bezie-

hungen abgebildet. Das hat zur Folge, dass die Assoziation eines Raumes mit einem Gebäude sich zu einem Server, der mit dem Raum assoziiert ist, durchzieht bzw. auf ihn übergeht.[230] Damit muss nur der jeweils für den Betrieb einer Anwendung benötigte Server mit dieser assoziiert werden. Die Informationen, welcher Raum und welches Gebäude für den Serverbetrieb und damit letztlich für die Anwendung benötigt werden, ziehen sich automatisch zu der die Anwendung repräsentierenden Instanz durch und müssen folglich nicht für jede Anwendung einzeln im Modell gepflegt werden. Damit wird der Aufwand bei der Modellierung der Abhängigkeitsbeziehungen reduziert. Auch die Pflege der Modelle wird erleichtert, da eventuelle Änderungen der Standorte der Server nur pro Server, und nicht pro Anwendung geändert werden müssen.

Prinzipiell würden sich transitive Assoziationen auch dafür nutzen lassen, die Verkettung der Abhängigkeiten zwischen Bestandteilen der IT abzubilden, wie sie oben für die Client-Server-Architektur skizziert wurde. Im Projekt wurde nicht auf diese Weise verfahren. Stattdessen wurden einzelne Assoziationen zwischen jeder Anwendung und den jeweils von ihr benötigten Komponenten erzeugt. Der Grund hierfür liegt darin, dass für eine Umsetzung mit transitiven Assoziationen die Abbildung der IT-Landschaft auf eine weniger abstrakte Art und Weise hätte vollzogen werden müssen. Es wäre bspw. nicht möglich gewesen, das LAN der CHD mit einem einzigen Objekt abzubilden. Dieses eine LAN-Objekt trägt bei *mehreren* Frontends dazu bei, diese jeweils mit ihrem zugehörigen Backend zu verbinden. Aus Sicht eines *bestimmten* Frontends wäre es so jedoch nicht zuordenbar, mit welcher IT-Komponente sie über das LAN verbunden wird und andersherum, welche dem LAN nachgelagerten Komponenten von einem bestimmten Frontend benötigt werden. Stattdessen würden sich *alle* Assoziationen, die dem LAN nachgelagert sind, auf die Anwendung durchziehen. Gelöst werden könnte dieses Problem, wenn jede Anwendung in den Modellen ein eigenes LAN-Objekt zugeordnet bekäme. Dies würde jedoch nicht der Realität entsprechen und es würde die Modelle künstlich vergrößern, zumal auf die ebenfalls abstrakt in einem Objekt abgebildeten IT-Komponenten *Client* und *WAN* die gleiche Problematik zutrifft. Das Metamodell des Konzepts ist aus Anhang 1 ersichtlich.

Mit der Verwendung von Assoziationen wurden vier Intentionen verfolgt. Die erste Intention besteht darin, die Komplexität der später zu erzeugenden Prozessmodelle zu verringern. In diesen Modellen sollen alle IT-Ressourcen abgebildet werden, die für die Durchführung einzelner Funktionen benötigt werden. Bei Betrachtung der oben skiz-

[230] Transire (lat.) = übergehen, durchziehen.

zierten möglichen Abhängigkeiten eines Frontends wird deutlich, dass ein Prozessmodell bei einer expliziten graphischen Darstellung aller benötigter Sachmittel durch jeweils ein Objekt schnell an Übersichtlichkeit verlieren kann. Damit diente der beschriebene Weg der Komplexitätsreduktion, wobei trotzdem keine Informationen verloren gingen. Um zusätzlich zu der nicht expliziten Darstellung der nachgelagerten Systeme diese graphisch abzubilden, befindet sich hinter jedem Objekt, das ein Frontend repräsentiert, ein Modell, in dem die Abhängigkeitsbeziehungen des Frontends graphisch dargestellt werden. Anhang 2 enthält ein Beispiel hierfür. Zudem wird bei der Modellierung an jede Funktion ein Objekt angehängt, über das der Betrachter mittels einer Hinterlegung zu einem Modell gelangt, in dem alle weiteren Sachmittel graphisch durch jeweils ein Objekt repräsentiert werden. Um hier wiederum die Übersichtlichkeit zu wahren, werden die Objekte nach Klassen gegliedert. Ein derartiges Modell befindet sich in Anhang 3.

Die zweite Intention bestand darin, den Aufwand bei der Modellierung und der Pflege der Modelle zu verringern. Diese Aussage basiert auf der Prämisse, dass in der CHD Anwendungen existieren, die für mehrere Funktionen genutzt werden. Durch die Verwendung von Assoziationen muss nicht jedes Mal, wenn eine Anwendung für die Durchführung einer Funktion benötigt wird, diese mitsamt der von ihr benötigten Komponenten graphisch im Modell abgebildet werden, sondern es wird hierfür ein einziges Objekt ins Modell eingefügt. Entsprechend muss bei der Änderung einer Abhängigkeit diese nur einmal auf Ebene der die Anwendung repräsentierenden Instanz im Modell geändert werden.

Hieraus ergibt sich die dritte Intention, nämlich die Sicherung der Konsistenz der Daten, die dadurch erreicht wird, dass die Abhängigkeiten einer Anwendung jeweils für jede Anwendung an nur *einer* Stelle im Modell hinterlegt und gepflegt werden müssen.

Als viertes besteht bei der Verwendung von Assoziationen die Möglichkeit, Abfragen gegen Prozessmodelle auszuführen, sofern das verwendete Modellierungswerkzeug dies unterstützt. Bezogen auf das Ergebnis des Projektes wird der Anwender in die Lage versetzt, Auswertungen zu erstellen, die Auskunft über die Abhängigkeitsbeziehungen zwischen Anwendungen und Systemen sowie zwischen Funktionen und IT-Ressourcen geben. Die Auswertung dieser Abhängigkeitsbeziehungen zwischen IT und Funktionen bzw. Geschäftsprozessen bildet eine erste Basis für die Identifikation IT-bedingter operationeller Risiken.

6.3.3 Verwendung von Attributen

An dieser Stelle fließt mit der Anreicherung der Prozessmodelle um weitere risikorelevante Informationen ein Grundgedanke des Risk Mapping in das Konzept ein. Umgesetzt wurde dieser Gedanke darüber, den Instanzen von Funktionen und IT-Ressourcen Attribute zuzuordnen und somit Attributwerte in den Modellen speichern zu können. Zu diesem Behufe wurden die drei Attribute *maximale tolerierte Ausfallzeit*, *Prozess* und *zugesicherte maximale Ausfallzeit* definiert.

Die ersten beiden Attribute werden allen Funktionen zugeordnet. Das erste der beiden gibt an, wie lang die maximal tolerierte Ausfalldauer einer Funktion aus Sicht der Fachabteilung ist. Die Attributwerte werden jeweils bei der die Funktion ausführenden Fachabteilung erhoben. Das Attribut *Prozess* sorgt dafür, dass jede Funktion im Rahmen einer Abfrage einem Prozess zugeordnet werden kann, und wird bereits während des Modellierens vom Modellierer gepflegt.

Das letzte der drei Attribute wird allen Instanzen zugeordnet, die IT-Ressourcen repräsentieren, und gibt an, welche maximale Ausfalldauer der IT-Bereich der CHD den Nutzern bestimmter Anwendungen in den Fachabteilungen zusichert.

Die Daten werden nach der Modellierung von den Verantwortlichen des IT-Bereichs in die bestehenden Prozessmodelle eingepflegt. Im Sinne von Scandizzos Vorschlag zur Erweiterung des Risk Mapping um KRI handelt es sich bei den Attributen *max. tolerierte Ausfallzeit* und *zugesicherte max. Ausfallzeit* um Soll-Werte für den KPI *Ausfallzeit* jeweils aus Sicht der Fachabteilungen bzw. der IT-Abteilung. Das Konzept erlaubt damit den Verantwortlichen der CHD eine Steuerung des Kernrisikos *Systemausfall*.

Die Attribute müssen nicht bei jeder Funktion bzw. Ressource manuell definiert werden, sondern werden auf Ebene der übergeordneten Klasse definiert und vererben sich an deren Instanzen.[231]

Die Namen der Attribute und die Attributwerte können in den Objekten der Funktionen und Sachmittel ein- und ausgeblendet werden, so dass sie direkt im Modell ersichtlich sind.

6.3.4 Abfragen gegen Modelle

Auf Basis des beschriebenen Konzepts sollen alle bankexistenziellen Prozesse der CHD modelliert werden. Aufgrund der hohen Abhängigkeit des Bankgeschäfts von der IT ist

[231] Vgl. Scheer (2001), S.113.

davon auszugehen, dass ein Großteil der für diese Prozesse benötigten Anwendungen einen hohen Schutzbedarf hat.
Ein Beispiel für einen gemäß dem Konzept modellierten Prozess findet sich in Anhang 4. Im Anhang befindet sich nur die oberste Hierarchieebene des Prozessmodells. Eine weitere Detaillierung des Prozesses ist zwar möglich, zur Umsetzung der für das Management operationeller Risiken in der CHD verfolgten Interessen jedoch nicht zwingend notwendig.
Gegen die Modelle dieser Prozesse lassen sich Abfragen ausführen, die die Verantwortlichen der IT der CHD mit folgenden für das Management IT-bedingter operationeller Risiken essentiellen Informationen versorgen werden:

- Auflistung aller verwendeter IT-Komponenten und Abgleich, ob für eine Komponente eine geringere Ausfallzeit zugesichert wird, als es für nachgelagerte Komponenten der Fall ist,
- Überblick über die maximal tolerierte und die zugesicherte maximale Ausfallzeit auf Prozess-, Funktions- oder IT-Ressourcenebene,
- Exception-Reporting, wenn die maximal tolerierte Ausfallzeit einer Funktion IT-seitig nicht gewährleistet werden kann,
- Berücksichtigung der nachgelagerten Systeme inklusive derer zugesicherter maximaler Ausfallzeiten bei den beiden vorher genannten Punkten.

Die Abfragen werden mit dem in Anhang 5 befindlichem Code aus einer Excel-Arbeitsmappe heraus makrogesteuert gestartet. Die Ergebnisse werden in zwei HTML-Dateien geschrieben, auf die Webabfragen der Arbeitsmappe referenzieren. Über den in Anhang 6 befindlichen Code werden die Webabfragen aktualisiert und somit aktualisierte Daten aus den HTML-Dateien in die Arbeitsmappe übertragen. Diese beiden Makros werden aus dem Tabellenblatt *Wartung* heraus gestartet, in dem der Nutzer vor der Ausführung der Makros die Pfade zum Modell, zu den Abfragedateien und zu den Outputdateien angeben kann. Das Tabellenblatt *Wartung* ist in Anhang 7 ersichtlich. Innerhalb der Arbeitsmappe werden durch einige Formeln die Abfrageergebnisse für die gewünschten Auswertungen nutzbar gemacht und die Auswertungen letztlich über Excels AutoFilter und bedingte Formatierungen realisiert. Aus den Anhängen 8 und 9 ist der Aufbau der beiden Tabellenblätter mit den Analysen ersichtlich.

Neben den Abfragemöglichkeiten können die Modelle selber unterschiedliche Informationsbedürfnisse erfüllen. Je nach Wunsch des Betrachters können bestimmte Attributwerte im Modell angezeigt werden. Durch die Hierarchisierung der Modelle können Prozesse entweder auf einer übergeordneten abstrakten oder einer detaillierten Ebene betrachtet werden. Jede Funktion der obersten Hierarchieebene wird in einer darunter liegenden Verfeinerung detailliert dargestellt. Abhängigkeiten einer Funktion von Ressourcen werden sowohl mit Hilfe von Assoziationen als auch graphisch in eigenen Sachmitteldiagrammen dargestellt.
Die Umsetzung des Konzepts befindet sich auf der dieser Arbeit beigelegten CD-ROM.

6.4 Evaluation von Modellierungswerkzeugen hinsichtlich ihrer Eignung für die Umsetzung des Konzepts

Das Konzept wurde mit dem in der CHD verwendeten Modellierungswerkzeug *SemTalk 2.1* realisiert. In diesem Teil der Arbeit sollen zwei weitere Modellierungswerkzeuge darauf untersucht werden, ob sich eine derartige Lösung mit ihnen umsetzen ließe. Es handelt sich dabei um das *ARIS-Toolset 7.0* und *iGrafx Process 2005*.[232]
SemTalk basiert auf dem Graphikwerkzeug Microsoft Visio und erweitert dieses um einige für die Geschäftsprozessmodellierung wesentliche Funktionalitäten. Kern dieser Erweiterung ist die Anbindung an eine Datenbank, wodurch es ermöglicht wird, Ausprägungen des gleichen Objekttyps mehrfach in Modellen zu nutzen und sie dabei als einander zugehörig identifizieren zu können.
Beim ARIS-Toolset handelt es sich nach Angaben seines Herstellers IDS Scheer AG um das weltweit meist verkaufte Modellierungswerkzeug.[233] Neben der eEPK unterstützt es einige weitere Modellierungssprachen, die allerdings formaler und weniger leicht zu verstehen sind. Die für die CHD zu erstellenden Modelle sollen auch von Mitarbeitern der Fachabteilungen möglichst schnell verstanden werden, weshalb im Rahmen dieser Evaluation beim ARIS-Toolset lediglich die eEPK als Methode zur Modellierung der Prozesse untersucht wurde.
Das Werkzeug iGrafx bietet unterschiedliche Ausstattungsvarianten seiner Modellierungswerkzeuge an. Es wurde nicht die reichhaltigste und damit teuerste Ausstattungsvariante *iGrafx Process for Six Sigma 2005* evaluiert, da deren zusätzliche Features kei-

[232] Die exakten Versionsbezeichnungen der Tools lauten: SemTalk 2.1.0.5196, ARIS-Toolset 7.0.0.95269, iGrafx 10.0.4.582.
[233] Vgl. IDS Scheer (2005).

nen erweiterten Nutzen für die Umsetzung des Konzeptes versprachen.[234] Die Software von iGrafx beinhaltet eine eigenständige Sprache zur Modellierung von Geschäftsprozessen.

Für den Vergleich werden zunächst anhand der in SemTalk entwickelten Lösung Kriterien entwickelt, die ein Modellierungswerkzeug erfüllen muss, damit sich das Konzept in ihm abbilden lässt. Anschließend wird deren Erfüllung für die beiden anderen Tools überprüft. Die Ergebnisse werden verbal beschrieben und tabellarisch zusammengefasst.

6.4.1 Ableitung der Vergleichskriterien

Die nachfolgenden Kriterien wurden als relevant für die Umsetzung des Konzepts mit SemTalk identifiziert.

Hierarchisierungen: Mit Hierarchisierungen können Modelle in mehrere Hierarchieebenen unterteilt werden. Dies soll sowohl für Funktionen als auch für Sachmittel möglich sein. In SemTalk wird diese Funktionalität als *Verfeinerung* bezeichnet.

Assoziationen zwischen Funktionen und Sachmitteln: Die Abhängigkeit einer Funktion von Sachmitten wird über Assoziationen ausgedrückt.

Assoziationen zwischen Sachmitteln: Um die Abhängigkeit eines Sachmittels von anderen Sachmitteln abzubilden, werden ebenfalls Assoziationen genutzt. Da das Metamodell der genutzten Modellierungssprache eEPK dies nicht zulässt, wurde das Metamodell entsprechend angepasst.

Implizite Assoziationen: Um die Modelle nicht mit allen für das Betreiben eines Frontends benötigten nachgelagerten Systemen zu überfrachten, werden zwischen jeweils einem Frontend und den für seinen Betrieb benötigten weiteren Sachmitteln Assoziationen angelegt, ohne dies in dem Prozessmodell graphisch abzubilden. Diese Art der Assoziation wird im Folgenden als *implizite Assoziation* bezeichnet. Implizite Assoziationen können in SemTalk ebenso wie explizite Assoziationen über Abfragen ausgewertet werden.

Transitive Assoziationen: Für die Abhängigkeit der Server von Räumen und wiederum der Räume von Gebäuden werden transitive Assoziationen genutzt. So muss für jeden Server nur an einer Stelle im Modell dessen Standort gepflegt werden.

[234] Vgl. iGrafx (2004), S.5 ff.

Attribute: Es werden Attribute definiert, die Funktionen bzw. Sachmitteln zugeordnet werden. Zwei der Attribute enthalten Zeitangaben, die entsprechend im Zeitformat gepflegt werden können.
Attribute im Modell anzeigen: Auf Wunsch können die Attributnamen und Attributwerte in den Modellen ein- und ausgeblendet werden.
Export aller benötigter Daten: Mittels Abfragen werden Funktionen, explizit wie auch implizit assoziierte Sachmittel und Attributwerte aus dem Modell exportiert und in Excel ausgewertet.

In den folgenden beiden Kapiteln wird überprüft, inwieweit die beiden Modellierungswerkzeuge die Kriterien erfüllen.

6.4.2 Evaluation iGrafx Process 2005

Hierarchisierungen: Die in iGrafx Process 2005 angebotene Methode zur Prozessmodellierung ermöglicht es, Aktivitäten mit hierarchisch untergeordneten Prozessdiagrammen zu verknüpfen. Ressourcen sind kein nativer Bestandteil der angebotenen Modellierungsmethode. Es können zwar nachträglich Objekte in das Metamodell eingebunden werden, die Ressourcen repräsentieren. Diese können aber nicht mit anderen Diagrammen verknüpft werden.
Assoziationen zwischen Funktionen und Sachmitteln: In iGrafx können Ressourcen mit Aktivitäten assoziiert werden, allerdings nicht explizit im Modell, sondern ausschließlich implizit.
Assoziationen zwischen Sachmitteln: Assoziationen zwischen Ressourcen sind nicht möglich und das Metamodell lässt sich nicht dahingehend erweitern.
Implizite Assoziationen: Implizite Assoziationen zwischen Aktivitäten und Ressourcen sind möglich, nicht jedoch untereinander zwischen Ressourcen (siehe vorige beide Kriterien).
Transitive Assoziationen: Es besteht keine Möglichkeit, transitive Assoziationen zu definieren.
Attribute: Attribute können selber definiert und Aktivitäten hinterlegt werden. Es wurde jedoch keine Möglichkeit gefunden, Ressourcen selbst definierte Attributwerte zuzuweisen. Stattdessen werden jeder Ressource, egal ob systemseitig vordefiniert oder

selbst erstellt, bestimmte Attribute zugewiesen, die Angaben über Kosten aufnehmen können.

Zudem lassen sich Attribute nicht im Zeitformat speichern. Stattdessen kann das Format *Zahl* genutzt werden, wobei zur Umsetzung des Konzepts eine Konvention darüber getroffen werden müsste, in welcher Maßeinheit die Attributwerte gepflegt werden sollen.

Attribute im Modell anzeigen: Attributwerte und –namen können nicht in den Modellen eingeblendet werden.

Export aller benötigter Daten: Es können Abfragen erstellt werden, mit denen sich Daten aus dem Modell in Textdateien exportiert lassen. Es ist aber nicht möglich, Attributwerte der Ressourcen abzufragen. Dadurch können die Informationsbedürfnisse der Verantwortlichen der CHD mit den Abfragen nicht befriedigt werden.

Fazit: Das Tool iGrafx Process 2005 erfüllt die meisten Kriterien nicht. Am schwerwiegendsten ist, dass keine selbst definierten Attribute hinter Ressourcen gespeichert werden können und es zudem nicht möglich ist, Attributwerte der Ressourcen abzufragen. Daher eignet sich dieses Tool nicht dazu, das vorgestellte Konzept umzusetzen.

6.4.3 Evaluation ARIS-Toolset 7.0

Hierarchisierungen: Funktionen lassen sich im ARIS-Toolset über so genannte Hinterlegungen detaillierter darstellen. Bei Sachmitteln gestaltet sich das komplizierter. So finden sich im Metamodell der eEPK zwei Objekttypen, die semantisch dafür geeignet erscheinen, ein Frontend darzustellen, nämlich *Allgemeine Ressource* und *Anwendungssystem*.[235] Allgemeine Ressourcen lassen sich ausschließlich mit Modellen vom Typ *Casual Model* hinterlegen. Bei Anwendungssystemen stehen neben dem Casual Model weitere Modelltypen zur Auswahl, nämlich *Anwendungssystemdiagramm, Business Controls Diagram, Programmablaufplan (PA), SAP Integrationsprozess (XI)* und *Zugriffsdiagramm (physikalisch)*. Keines der letztgenannten Modelltypen eignet sich dazu, Abhängigkeiten zwischen Bestandteilen einer IT-Landschaft zu modellieren, so dass einzig das Casual Model eine Hinterlegung hinter den beiden Objekttypen erlaubt, die sinnvollerweise Frontends repräsentieren können. Dieser „zwanglose“ Modelltyp erlaubt es, zu modellieren, ohne dabei Regeln beachten zu müssen. Im Umkehrschluss gilt jedoch auch, dass beim Casual Model ein Metamodell nicht besteht und auch nicht

[235] Vgl. IDS Scheer (2005b), S.15-14 ff. Die Benennung der Seitenzahl folgt der Bezeichnung in der Quelle. S.15-14 bedeutet Kapitel 15 Seite 14.

selbst erzeugt werden kann. Folglich ist keine gezielte Auswertung der Assoziationen bestimmter Objekttypen möglich, und es würde im Sinne der Gesamtlösung keinen Nutzen bringen, das Casual Model zu verwenden. Daher wird als Ergebnis festgehalten, dass im ARIS-Toolset keine Hinterlegung von IT-Ressourcen möglich ist.

Assoziationen zwischen Funktionen und Sachmitteln: Das Metamodell der eEPK erlaubt Assoziationen zwischen Funktionen und Sachmitteln.

Assoziationen zwischen Sachmitteln: Assoziationen zwischen verschiedenen Sachmitteln innerhalb der eEPK sind nicht erlaubt und es besteht keine Möglichkeit, das Metamodell dahingehend anzupassen. Prinzipiell ist eine Modellierung der IT-Landschaft und damit verbunden von Assoziationen zwischen IT-Bestandteilen in Modellen vom Typ *Netzdiagramm* möglich.[236] Diese lassen sich allerdings nicht den Frontends hinterlegen. Zumindest ist es möglich, Ausprägungskopien, also dieselben Objekte, in den Netzdiagrammen und den eEPKs zu nutzen. Das Produkt des Konzeptes soll ein Gesamtmodell sein, durch das der Betrachter navigieren kann. Es soll nicht aus Einzelmodellen bestehen, die aus Sicht der Navigation isoliert nebeneinander existieren. Daher wird festgehalten, dass das ARIS-Toolset keine zur Umsetzung des Konzepts zufrieden stellende Möglichkeit bietet, Assoziationen zwischen Sachmitteln zu erzeugen.

Implizite Assoziationen: Assoziationen können im ARIS-Toolset zunächst nur explizit, also im Modell sichtbar, angelegt werden. Hierzu werden zwei Objekte mit einer Kante verbunden. Wird die Kante anschließend gelöscht, bleibt die so genannte *Beziehung* zwischen den Objekten bestehen, wodurch eine implizite Assoziation entsteht. Aufgrund des mangelnden Nutzens für die Umsetzung des Konzeptes (siehe Kriterium Assoziationen zwischen Sachmitteln) lautet das Urteil trotzdem, dass das ARIS-Toolset implizite Assoziationen nicht im notwendigen Ausmaße zulässt.

Nicht zu verwechseln ist die implizite Assoziation mit dem im ARIS-Toolset verwendeten Begriff *Implizite Beziehung*. Er bezieht sich nur auf Swimlane-Modelle, in denen bspw. alle von einer Organisationseinheit ausgeführten Funktionen in einer Zeile oder Spalte – der so genannten Swimlane – angeordnet werden und sie durch die Zuordnung zu so einer Swimlane implizit der Organisationseinheit zugeordnet werden.

Transitive Assoziationen: Es wurde keine Möglichkeit gefunden, transitive Assoziationen zu definieren.

Attribute: Es sind im ARIS-Toolset eine Vielzahl von Attributen vordefiniert, für die bei den verschiedenen Objekttypen Werte hinterlegt werden können. Die für die CHD

[236] Vgl. IDS Scheer (2005b), S.8-10.

benötigten Attribute werden jedoch nicht angeboten. Eigenständige Attribute lassen sich nur unter nichts sagenden Namen wie *Benutzerattribut Zeitdauer 1* oder *Benutzerattribut Text 2* nutzen. Hiermit ist es zwar prinzipiell möglich, Daten in Modellen zu speichern. Sie werden jedoch hinter Namen versteckt, die nicht sprechend sind. Dies verstößt gegen eine Grundidee der Prozessmodellierung, der zur Folge Prozessmodelle Sachverhalte möglichst eindeutig und unmissverständlich ausdrücken sollen. Die Attribute lassen die Speicherung von Werten im Zeitformat zu.

Attribute im Modell anzeigen: Attributwerte und deren Bezeichnungen können in Modellen angezeigt werden, wobei das Anzeigen nicht sprechender Namen wenig sinnvoll erscheint und dies auch dem Einblenden der Attributwerte seinen Reiz nimmt.

Export aller benötigter Daten: Daten aus ARIS-Modellen können mit Abfragen u.a. in Excel-Dateien exportiert werden. Dies kann sowohl mit vorgefertigten als auch mit selbst programmierten Reports vollzogen werden. Es lassen sich alle Funktionen, Ereignisse und mit ihnen verbundene Objekte mitsamt ihrer Attributwerte auswerten. Im Rahmen der zur Verfügung stehenden Zeit gelang es dem Verfasser der Arbeit nicht, eine Abfrage zu erstellen, die die für das Konzept benötigten Informationen aus Modellen extrahiert. Es wird jedoch davon ausgegangen, dass dies technisch gesehen möglich ist. So existiert der vorgefertigte Report *ModellInfo.rsm*, mit dem sich Daten aus den Modellen extrahieren lassen, die den gewünschten Informationen nahe kommen.[237]

Fazit: Das ARIS-Toolset liefert eine Vielzahl vorgefertigter Modelltypen, Attribute und Assoziationen. Allerdings lässt sich dieser reichhaltige Baukasten nur in engen Grenzen erweitern. Daher kann das Konzept mit diesem Modellierungswerkzeug zwar in groben Zügen, nicht jedoch zufrieden stellend realisiert werden.

In Abbildung 13 werden die Ergebnisse der Evaluation tabellarisch zusammengefasst.

[237] Mit dieser Abfrage können jeweils aus einem Modell alle hierin verwendeten Objekte, ihre gepflegten Attribute sowie Angaben darüber, zu welchen anderen Objekten sie in welcher Beziehung stehen in eine Excel-Tabelle geschrieben werden.

	ARIS-Toolset 7.0	iGrafx Process 2005	SemTalk 2.1
Hierarchisierungen von Funktionen	X	X	X
Hierarchisierungen von Sachmitteln			X
Assoziationen zwischen Funktionen und Sachmitteln	X		X
Assoziationen zwischen Sachmitteln			X
Implizite Assoziationen			X
Transitive Assoziationen			X
Selbst definierte Attribute für Funktionen	X	X	X
Selbst definierte Attribute für Sachmittel	X		X
Attribute im Modell anzeigen	X		X
Export aller benötigter Daten	X		X

Abbildung 13: Zusammenfassung der Ergebnisse der Evaluation

7. Fazit und Ausblick

Die Zielsetzung der Arbeit bestand darin, ein Konzept für das Geschäftsprozessmodell-basierte Management operationeller Risiken in der CHD zu finden. Aufgrund der zentralen Stellung, die die mit der Nutzung der IT verbundenen Risiken innerhalb der operationellen Risiken einer Bank einnehmen, sollte das Konzept speziell diese Risiken berücksichtigen. Nachdem die Grundlagen für das Verständnis der Thematik gelegt worden sind, wurden verschiedene in der Literatur diskutierte Geschäftsprozessmodell-basierte Ansätze auf ihre generelle Eignung für ihren Einsatz im Bankensektor untersucht. Bis zu einem gewissen Grad war diese Eignung bei allen Ansätzen gegeben.

Auf Basis des Ansatzes des Risk Mapping sowie Aussagen des IT-Grundschutzhandbuches wurde ein Konzept entwickelt, mit dem Geschäftsprozesse unter spezieller Berücksichtigung der für deren Durchführung benötigten IT-Ressourcen modelliert werden können, und exemplarisch umgesetzt. Dieses Konzept erlaubt eine Anreicherung der Prozessmodelle mit Informationen, die Hinweise auf risikobehaftete Konstellationen geben, sowie eine abfragegestützte Auswertung der Modelle, die eine Analyse der Informationen erlaubt. Gleichzeitig sorgen die Prozessmodelle für ein einheitliches Verständnis der betrachteten Prozesse in Gesprächen mit Fachabteilungen, die mit ihrem Wissen über die von ihnen in den Prozessen ausgeführten Funktionen einen wichtigen Teil zu der Gewinnung der notwendigen Informationen beitragen.

Eine Möglichkeit zur Erweiterung des Konzepts bestünde darin, die gesamte IT-Landschaft der CHD zu modellieren. Auf diesem Wege ließe sich ermitteln, welche IT-Komponenten *keinen* hohen Schutzbedarf aufweisen und ob deren Absicherung unter dem Aspekt der Wirtschaftlichkeit gerechtfertigt ist.

Als weiterer Schritt könnte über ein Attribut die Dauer gespeichert werden, die ein Prozess von seinem Startereignis aus gesehen benötigt, bis dessen einzelne Funktionen aktiviert werden. Hierdurch würde die Information vorliegen, bis wann ein System aus Sicht des Prozesses spätestens wieder funktionstüchtig sein müsste. Als Einwand gegen diesen Vorschlag lässt sich vorbringen, dass viele Prozesse in einer so hohen Frequenz angestoßen werden, dass die beteiligten Systeme praktisch permanent benötigt werden. Daher würde diese Erweiterung nur für selten durchgeführte Prozesse mit keiner allzu kurzen Durchführungsdauer der einzelnen Funktionen einen Sinn machen.

Der Faktor Mensch könnte in die Modelle einbezogen werden, indem gespeichert wird, ob eine Funktion manuell, automatisch-interaktiv oder vollautomatisch durchgeführt

wird.[238] Bei automatisch-interaktiven Funktionen sind Eingaben eines Mitarbeiters an einem System notwendig. Hierbei besteht die Möglichkeit von Fehleingaben. Hier ließe sich zusätzlich zu der Prozesssicht die Sicht der Anwender einbeziehen, indem diese um ein konstruktives Feedback hinsichtlich der Bedienbarkeit der Systeme gebeten werden. Ein für eine Funktion in einem bankexistenziellen Prozess benötigtes System sollte einfach zu bedienen und wohl dokumentiert sein, um die Wahrscheinlichkeit von Fehleingaben zu vermindern. Bei manuell durchzuführenden Funktionen könnten die Modelle dazu genutzt werden, das Vorhandensein von Wissensmonopolen zu identifizieren, die eine Gefahr im Falle einer Krankheit oder des Ausscheidens des Mitarbeiters aus der Bank darstellen würden. Diese Erweiterung bezieht Aspekte der Predictive Human Error Analysis in das Konzept ein.

Das in der CHD verwendete Werkzeug SemTalk erlaubt die Umsetzung des Konzepts und ist aufgrund seiner hohen Flexibilität auch dazu in der Lage, die CHD erfolgreich bei der Umsetzung von etwaigen Erweiterungen zu begleiten.

[238] Vgl. Kahl/Kupsch (2005), S.65.

QUELLENVERZEICHNIS

AcuTech: The HAZOP (Hazard and Operability) Method. (http://www.acusafe.com/Hazard_Analysis/HAZOP_Technique.pdf, abgerufen am 22.12.05)

AktG: Aktiengesetz vom 01.01.1966.

Balfan, M./Gledhill, P./Haubenstock, M. (2002): Self Assessment of Operational Risk, in: The RMA Journal 02/2002, S.65-69. (http://www.findarticles.com/p/articles/mi_m0ITW/is_5_84/ai_n14897063#, abgerufen am 22.12.05)

Barnes Marschdorf, K. (1999): Control Self Assessment: Eine Methode des Risikomanagements, in: Der Schweizer Treuhänder 08/99, S.693-700. (http://www.treuhaender.ch/pdf/artikel/a99_0693.pdf, abgerufen am 22.12.05)

Baseler Ausschuss (1994): Risk Management Guidelines for Derivatives, Basel 1994. (http://www.bis.org/publ/bcbsc211.pdf, abgerufen am 22.12.05)

Baseler Ausschuss (2001a): Konsultationspapier - Die Neue Baseler Eigenkapitalvereinbarung, Basel 2001. (http://www.bundesbank.de/download/bankenaufsicht/pdf/rules_translation.pdf, abgerufen am 22.12.05)

Baseler Ausschuss (2001b): Working Paper on the Regulatory Treatment of Operational Risk, Basel 2001. (http://www.bis.org/publ/bcbs_wp8.pdf, abgerufen am 22.12.05)

Baseler Ausschuss (2003): Sound Practices for the Management and Supervision of Operational Risk, Basel 2003. (http://www.bis.org/publ/bcbs96.pdf, abgerufen am 22.12.05)

Baseler Ausschuss (2004a): Internationale Konvergenz der Kapitalmessung und Eigenkapitalanforderungen - Überarbeitete Rahmenvereinbarung, Basel 2004.

(http://www.bis.org/publ/bcbs107ger.pdf, abgerufen am 22.12.05)

Baseler Ausschuss (2004b): International Convergence of Capital Measurement and Capital Standards – A Revised Framework, Basel 2004. (http://www.bis.org/publ/bcbs107.pdf, abgerufen am 22.12.05)

Becker, J./Kahn, D. (2005): Der Prozess im Fokus, in: Becker, J./Kugeler, M./ Rosemann, M.: Prozessmanagement: Ein Leitfaden zur prozessorientierten Organisationsgestaltung, 5.Aufl., Berlin/Heidelberg/New York 2005, S.3-16.

Becker, J./Meise, V. (2005): Strategie und Ordnungsrahmen, in: Becker, J./Kugeler, M./ Rosemann, M.: Prozessmanagement: Ein Leitfaden zur prozessorientierten Organisationsgestaltung, 5.Aufl., Berlin/Heidelberg/New York 2005, S.105-154.

Becker, J./Rosemann, M./Schütte, R. (1995): Grundsätze ordnungsmäßiger Modellierung, in: Wirtschaftinformatik 05/1995, S.435 – 445.

Becker, J./Schütte, R. (1996): Handelsinformationssysteme, Landsberg/Lech 1996.

Beeck, H./Kaiser, T. (2000): Quantifizierung von Operational Risk mit Value-at-Risk, in: Johanning, L./Rudolph, B.: Handbuch Risikomanagement: Band 1. Risikomanagement für Markt-, Kredit- und operative Risiken, Bad Soden 2000, S.633-653.

Bergsmann, S./Grabek, A./Brenner, M. (2005): Transparenz durch Prozessanalyse und –modellierung, in: Horváth & Partners (Hrsg.): Prozessmanagement umsetzen: Durch nachhaltige Prozessperformance Umsatz steigern und Kosten senken, Stuttgart 2005.

Bergmann, M. (2005): „Risikoarme, schlanke Prozesse gestalten“: Ein Interview mit Prof. Dr. Erhard Petzel über das intelligente Management Operationeller Risiken und die Optimierung von Unternehmensprozessen, in: Pass Age, 01/2005 S.14-15. (http://www.pass-fs.com/download/passage_01_2005_print.pdf, abgerufen am 22.12.05)

Blattner, P. (2003): Globales Risikomanagement für Banken, München/Wien 2003.

Book, N./Rudolph, D. (2005): IT Risk Management – Sarbanes-Oxley & Co. als Motor der IT-Sicherheit?, in: Information Management & Consulting 02/2005, S.55-60.

Bundesamt für Sicherheit in der Informationstechnik (2004): IT-Grundschutzhandbuch 2004, Bonn 2004. (http://www.bsi.de/gshb/deutsch/download/GSHB2004.pdf, abgerufen am 22.12.05)

Bundesanstalt für Finanzdienstleistungsaufsicht (2005a): Konsultation 07/05: Zweiter Entwurf der Mindestanforderungen an das Risikomanagement (MaRisk) vom 22.09.2005, Frankfurt 2005. (http://www.bundesbank.de/download/bankenaufsicht/pdf/marisk/marisk2_entwurf.pdf, abgerufen am 22.12.05)

Bundesanstalt für Finanzdienstleistungsaufsicht (2005b): Anschreiben vom 02.02.05, Frankfurt 2005. (http://www.bundesbank.de/download/bankenaufsicht/pdf/marisk/20050202_anschreiben.pdf, abgerufen am 22.12.05)

Bundesrat-Drucksache 872/97 (http://www.parlamentsspiegel.de/portal/WWW/Webmaster/GB_I/I.4/Dokumentenarchiv/dokument.php?pl=BB&part=D&pnr=872/97&quelle=parla, abgerufen am 22.12.05)

Bundesverband Öffentlicher Banken Deutschlands e.V. (2005): Vergleich zwischen 1. und 2. Entwurf der MaRisk. (http://www.voeb.de/content_frame/downloads/marisk_synopse.pdf, abgerufen am 21.10.05)

Büschgen, H.E. (1998): Bankbetriebslehre: Bankgeschäfte und Bankmanagement, 5.Aufl., Wiesbaden 1998.

Center for Chemical Process Safety (1994): Guidelines for Preventing Human Error in Process Safety, New York 1994.

COSO (1994): Internal Control - Integrated Framework Executive Summary. (http://www.coso.org/publications/executive_summary_integrated_framework.htm, abgerufen am 22.12.05)

Deutsche Bundesbank (2001): Monatsbericht April 2001. (http://www.bundesbank.de/download/volkswirtschaft/monatsberichte/2001/200104mb.pdf, abgerufen am 22.12.05)

Deutsche Bundesbank (2005a): Basel II - Die neue Baseler Eigenkapitalvereinbarung. (http://www.bundesbank.de/bankenaufsicht/bankenaufsicht_basel.php, abgerufen am 22.12.05)

Deutsche Bundesbank (2005b): Motive und Ziele (http://www.bundesbank.de/bankenaufsicht/bankenaufsicht_motive.php, abgerufen am 22.12.05)

Deutscher Corporate Governance Kodex (http://www.corporate-governance-code.de/ger/download/D_CorGov_Endfassung2005.pdf , abgerufen am 22.12.05)

Diederichs, M. (2005): Sarbanes-Oxley-Act, in: Controlling 04-05/2005, S.301-303.

Doerig, H.-U. (2003): Operational Risks in Financial Services: An Old Challenge in a New Environment. (http://www.credit-suisse.com/en/csgn/operational_risk.pdf, abgerufen am 22.12.05)

Färber, N./Wagner, T.M. (2005): Adaption des internen Kontrollsystems an die Anforderungen des Sarbanes-Oxley-Act, in: Controlling 03/2005, S.155-161.

Gaitanides, M. (1983): Prozessorganisation: Entwicklung, Ansätze und Programme prozessorientierter Organisationsgestaltung, München 1983.

Geiger, H./Piaz, J.-M. (2001): Identifikation und Bewertung operationeller Risiken, in: Schierenbeck, H./Rolfes, B./Schüller, S. (Hrsg.): Handbuch Bankcontrolling, 2.Aufl., Wiesbaden 2001, S.789-802.

Grochla, E. (1983): Unternehmensorganisation: neue Ansätze und Konzeptionen, 9.Aufl., Opladen 1983.

Grosse, S./Tsapanis, E./Stromberg, M.O. (2004): Geschäftsprozessorientierter Ansatz zur Einhaltung der Corporate Governance-Erklärung und des Sarbanes-Oxley-Gestzes, in: Innovation durch Geschäftsprozessmanagement: Jahrbuch Business Process Excellence 2004/2005, Berlin/Heidelberg 2004, S.103-117.

HGB: Handelsgesetzbuch vom 10.05.1897.

Hartmann-Wendels, T./Pfingsten, A./Weber, M. (2004): Bankbetriebslehre, 3.Aufl., Berlin 2004.

Helbig, R. (2003): Prozessorientierte Unternehmensführung: Eine Konzeption mit Konsequenzen für Unternehmen und Branchen dargestellt an Beispielen aus Dienstleistung und Handel, Heidelberg 2003.

Hill, W./Fehlbaum, R./Ulrich, P. (1994): Organisationslehre 1. Ziele, Instrumente und Bedingungen, 5.Aufl., Bern/Stuttgart/Wien 1994.

Hirschmann, S./Romeike, F. (2004): IT-Sicherheit als Ratingfaktor, in: Rating aktuell, 01/2004, S. 12-17.
(http://www.basel-ii.info/modules.php?name=News&file=article&sid=76, abgerufen am 22.12.05)

IDS Scheer (2005a)
(http://www.ids-scheer.de/, abgerufen am 22.12.05)

IDS Scheer (2005b): Methode ARIS 7.0, Saarbrücken 2005.

iGrafx (2004): iGrafx Process 2005 for Six Sigma Benutzerhandbuch, Ottawa 2004.

Institut der Wirtschaftsprüfer (1999): IDW Prüfungsstandard: Die Prüfung des Risikofrühwarnsystems nach § 317 Absatz 4 HGB (IDW PS 340), in: IdW-Fachnachrichten 08/1999, S.350–357.

Jackson, P./Ashton, D. (1995): ISO 9000: Der Weg zur Zertifizierung, 2.Aufl., Landsberg/Lech 1995.

Jans, V. (2003): Erfahrungen mit Control & Risk Self Assessment: Die interne Revision als Katalysator für ein aktives Risikomanagement, in: Der Schweizer Treuhänder 1-2/2003, S.27-32.

Jovic, D./Piaz, J-M. (2001): „Operational Risk Management" als kritischer Erfolgsfaktor für Banken, in: Der Schweizer Treuhänder 10/2001, S.923-930.

Kahl, T./Kupsch, F. (2005): Transformation und Mapping von Prozessmodellen in verteilten Umgebungen mit der ereignisgesteuerten Prozesskette, in: Nüttgens, M./Rump, F.J.: EPK 2005 - Geschäftsprozessmanagement mit Ereignisgesteuerten Prozessketten, Proceedings des 4. Workshops der Gesellschaft für Informatik e.V. (GI) und Treffens ihres Arbeitskreises, Hamburg 2005, S.54-73.

Kauffmann, H./Götzenberger, G. (2003): Aufbau eines effektiven Internal Control Systems nach Section 404 des Sarbanes-Oxley-Acts, in: Horváth, P. (Hrsg.): Performancesteigerung und Kostenoptimierung: Neue Wege und erfolgreiche Praxislösungen, Stuttgart 2003, S.149-166.

Keller, G./Nüttgens, M./Scheer, A.-W. (1992): Semantische Prozessmodellierung auf der Grundlage „Ereignisgesteuerter Prozessketten (EPK)", in: Scheer, A.-W. (Hrsg.): Veröffentlichungen des Instituts für Wirtschaftsinformatik, Heft 89, Saarbrücken 1992. (http://www.iwi.uni-sb.de/nuettgens/Veroef/Artikel/heft089/heft089.pdf, abgerufen am 22.12.05)

Kenney, W.F. (1993): Process Risk Management Systems, New York/Weinheim/Cambridge 1993.

Kessler, B. (2000): Ein heuristisches Verfahren zur Prävention von operativen Unternehmensrisiken – angewendet am Beispiel der St. Gallischen Kantonalbank, Freiburg i. Ue. 2000.

King, J.L. (2001): Operational Risk: Measurement and Modelling, Chichester 2001.

Kletz, T. (1999): HAZOP and HAZAN: Identifying and Assessing Process Industry Hazards, 4.Aufl., Philadelphia 1999.

Kosiol, E. (1962): Organisation der Unternehmung, Wiesbaden 1962.

Kugeler, M./Vieting, M. (2005): Gestaltung einer prozessorientierten Aufbauorganisation, in: Becker, J./Kugeler, M./Rosemann, M.: Prozessmanagement: Ein Leitfaden zur prozessorientierten Organisationsgestaltung, 5.Aufl., Berlin/Heidelberg/New York 2005, S.221-267.

Küpper, H.-U. (1982): Ablauforganisation, Stuttgart/New York 1982.

KWG: Gesetz über das Kreditwesen (Kreditwesengesetz) in der Neufassung der Bekanntmachung vom 09.09.1998.

Minz, K.-A. (2004): Operationelle Risiken in Kreditinstituten, Frankfurt 2004.

Münchbach, D. (2001): Management der operationellen Risiken des Private Banking: Gestaltungsempfehlungen für ein System zum Management der operationellen Risiken des Private Banking, Bamberg 2001.

o.V. (1996): Banque Paribas Transactions Rating Downgraded to ‘F-1’ by Fitch, London 1996.
(http://www.prnewswire.de/cgi/release?id=10376, abgerufen am 22.12.05)

o.V. (2005): Nick Leeson und der Konkurs der Barings-Bank 1995. (http://www.zeitenwende.ch/page/index.cfm?SelNavID=1258, abgerufen am 22.12.05)

Ostler, U. (2005): Gut gemeint und teuer: SOX in IT und Organisation. (http://www.silicon.de/cpo/hgr-wipo/detail.php?nr=18773, abgerufen am 22.12.05)

Peter, A./Vogt, H.J./Kraß, V. (2000): Management operationeller Risiken bei Finanzdienstleistern, in: Johanning, L./Rudolph, B.: Handbuch Risikomanagement: Band 1. Risikomanagement für Markt-, Kredit- und operative Risiken, Bad Soden 2000, S.655-677.

Pfeifer, T. (2001a): Qualitätsmanagement: Strategien, Methoden, Techniken, 3.Aufl., München/Wien 2001.

Pfeifer, T. (2001b): Praxisbuch Qualitätsmanagement: Aufgaben, Lösungswege, Ergebnisse, 2.Aufl., München/Wien 2001.

Pillen, G./Kasprowicz, T.J./Knappstein, M. (2004): IT zur Umsetzung von Basel II: Operationelle Risiken, in: Moormann, J./Fischer, T.: Handbuch Informationstechnologie für Banken, Wiesbaden 2004, S.561-577.

Porter, M.E. (1999): Wettbewerbsvorteile: Spitzenleistungen erreichen und behaupten, 5.Aufl., Frankfurt/New York 1999.

Redmill, F./Chudleigh, M./Catmur, J. (1999): System Safety: HAZOP and Software HAZOP, Chichester 1999.

REFA, Verband für Arbeitsstudien und Betriebsorganisation (1984): Methodenlehre des Arbeitsstudiums, 7.Aufl., München 1984.

Rosemann, M./Schwegmann, A./Delfmann, P. (2005): Vorbereitung der Prozessmodellierung, in: Becker, J./Kugeler, M./Rosemann, M.: Prozessmanagement: Ein Leitfaden zur prozessorientierten Organisationsgestaltung, 5.Aufl., Berlin/Heidelberg/New York 2005, S.45-103.

Ruta, A. (1999): Fehlermöglichkeits- und Einflussanalyse FMEA für die Produktionslogistik, Düsseldorf 1999.

Scandizzo, S. (2005): Risk Mapping and Key Risk Indicators in Operational Risk Management, in: Economic Notes, 02/2005, S.231-256.

Scheer, A.-W./Nüttgens, M./Zimmermann, V. (1997): Objektorientierte Ereignisgesteuerte Prozesskette (oEPK) – Methode und Anwendung, in: Scheer, A.-W. (Hrsg.): Veröffentlichungen des Instituts für Wirtschaftsinformatik (IWi), Universität des Saarlandes, Heft 141, Saarbrücken 1997.
(http://www.iwi.uni-sb.de/Download/iwihefte/heft141.pdf, abgerufen am 22.12.05)

Scheer, A.-W. (2001): ARIS – Modellierungsmethoden, Metamodelle, Anwendungen, 4.Aufl., Berlin 2001.

Schierenbeck, H. (2003): Ertragsorientiertes Bankmanagement Band 2: Risiko-Controlling und integrierte Rendite-/Risikosteuerung, 8.Aufl., Wiesbaden 2003.

Schubert, M. (1993): FMEA - Fehlermöglichkeits- und Einflussanalyse: Leitfaden, Berlin 1993.

Schulte, M. (1994): Integration der Betriebskosten in das Risikomanagement von Kreditinstituten, Wiesbaden 1994.

Schulte, M./Horsch, A. (2004): Wertorientierte Banksteuerung II: Risikomanagement, 3.Aufl., Frankfurt 2004.

Schulte-Zurhausen, M. (2002): Organisation, 3.Aufl., München 2002.

Schütte, R. (1998): Grundsätze ordnungsmäßiger Referenzmodellierung: Konstruktion konfigurations- und anpassungsorientierter Modelle, Wiesbaden 1998.

Vahs, D. (2005): Organisation: Einführung in die Organisationstheorie und –praxis, 5.Aufl., Stuttgart.

Wilhelm, R. (2003): Prozessorganisation, München 2003.

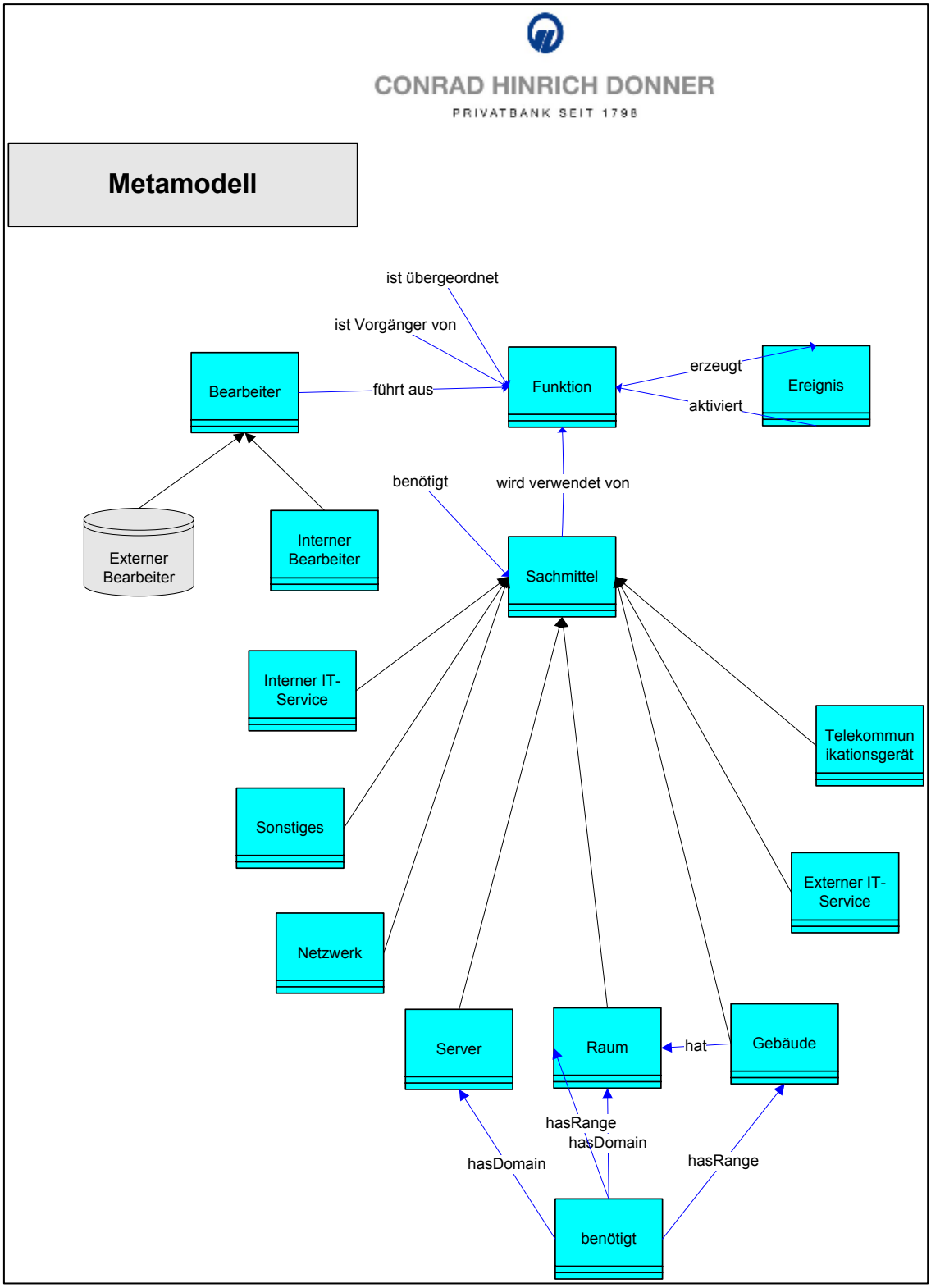
Witter, A. (1995): Entwicklung eines Modells zur optimierten Nutzung des Wissenspotentials einer Prozess-FMEA, Düsseldorf 1995.

WpHG: Gesetz über den Wertpapierhandel (Wertpapierhandelsgesetz) in der Neufassung der Bekanntmachung vom 09.09.1998.

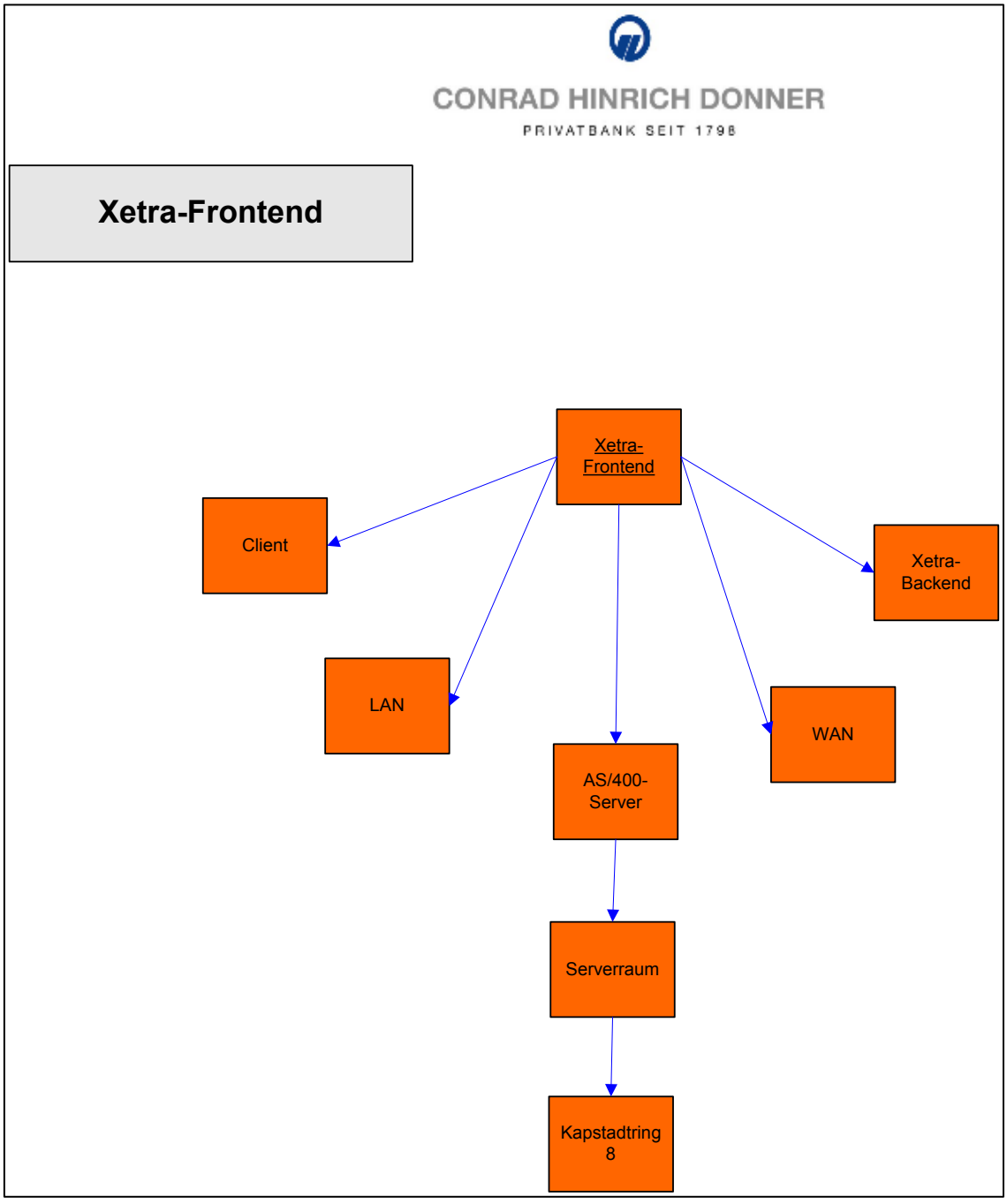
Zweig, P.L./Sullivan, A. (1985): A Computer Snafu Snarls the Handling of Treasury Issues, in: Wall Street Journal, 25.11.1985.

Anhang

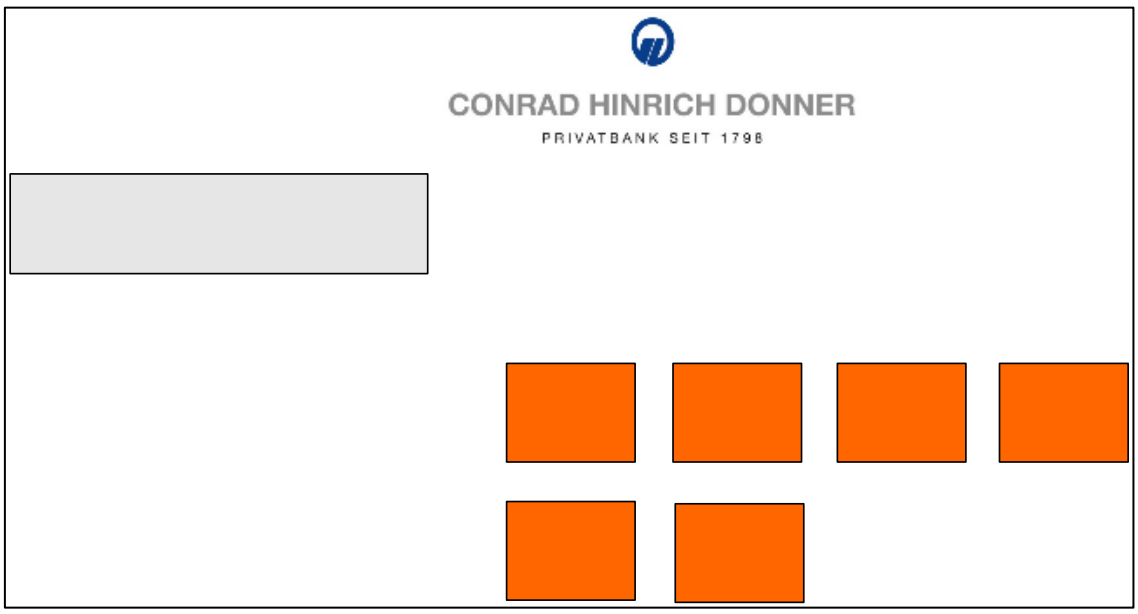
Anhang 1: Metamodell des Konzepts



Anhang 2: Graphische Darstellung der Abhängigkeitsbeziehungen eines Frontends



Anhang 3: Graphische Darstellung sonstiger für die Durchführung einer Funktion benötigter Sachmittel



Weitere Sachmittel Order entgegennehmen

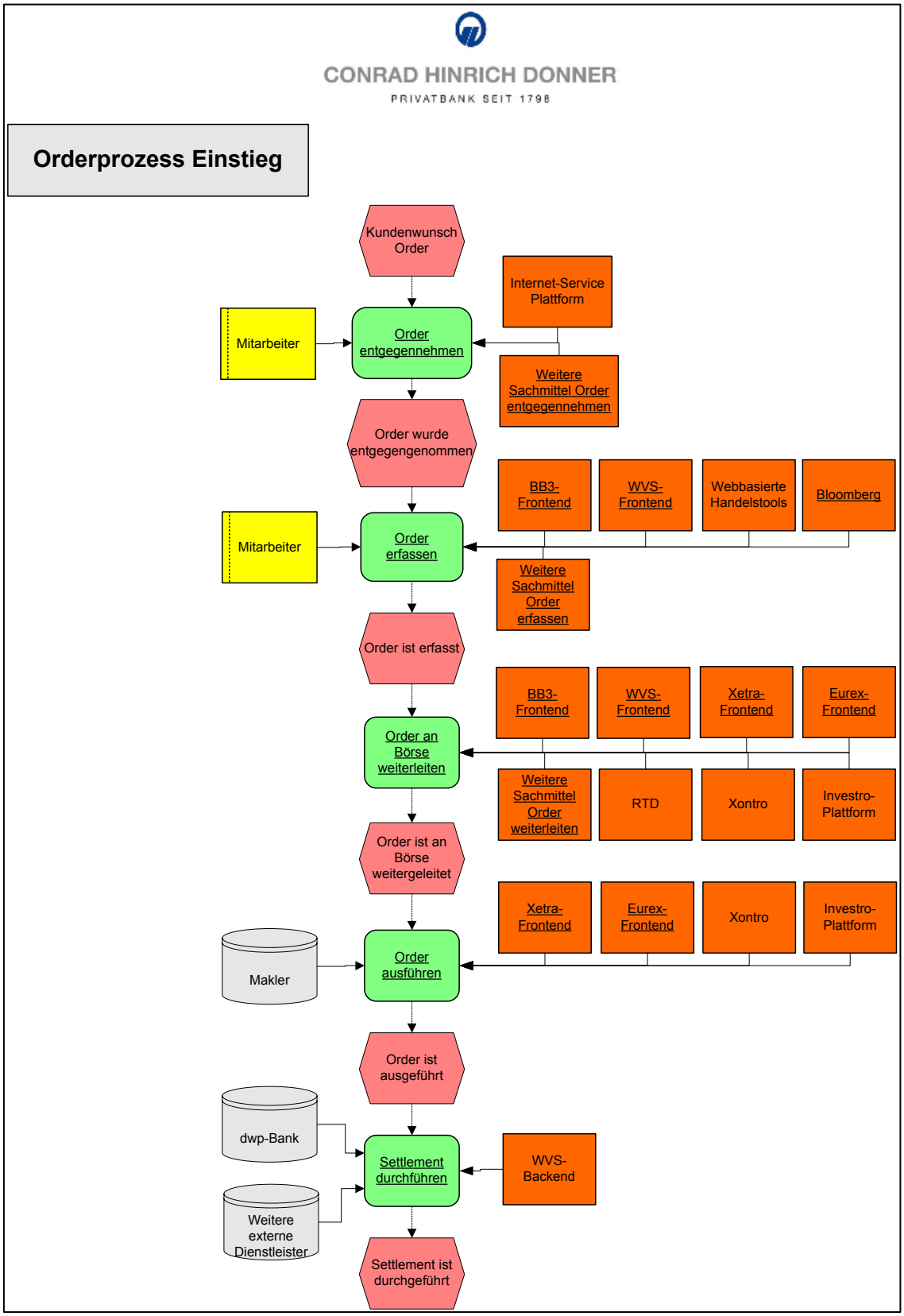
Räumlichkeiten

Vertrie
ste

Telekommunikation

Tele

Anhang 4: Beispiel für einen gemäß dem Konzept modellierten Prozess



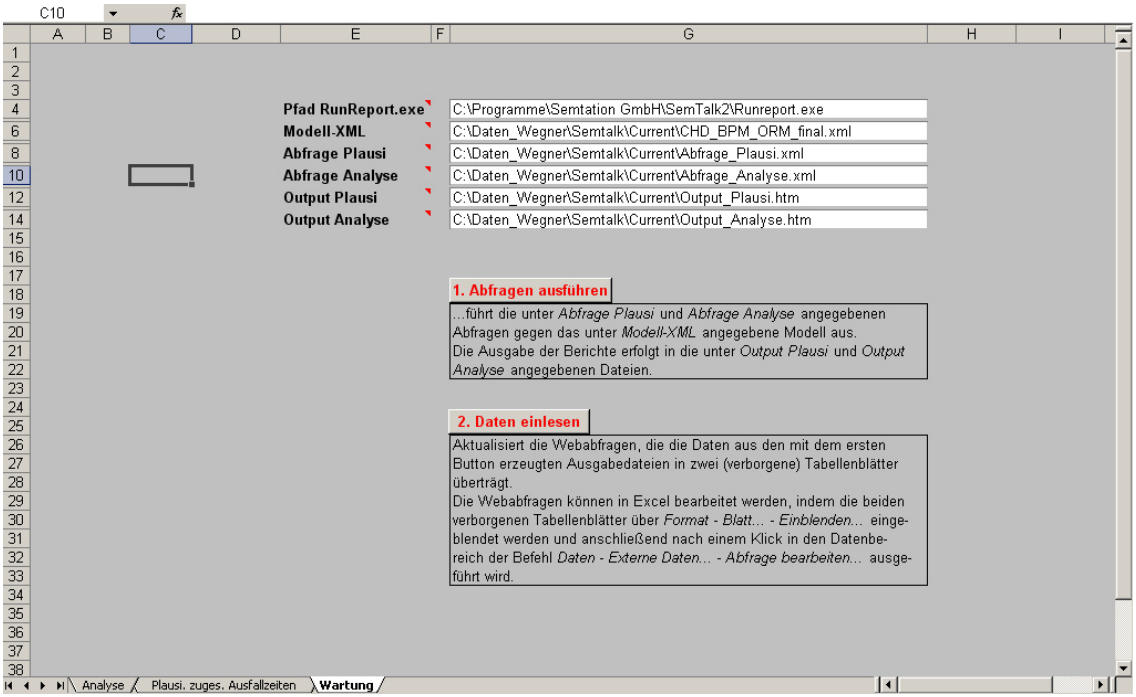
Anhang 5: Code zum Ausführen von Abfragen gegen ein Modell

```
Sub AbfrageAusfuehren()
    Dim STProg As String
    Dim STDatei As String
    Dim STReport1 As String
    Dim STReport5 As String
    Dim STReportOutput1 As String
    Dim STReportOutput5 As String

    STProg = Range("G4").Value
    STDatei = Range("G6").Value
    STReport1 = Range("G8").Value
    STReport5 = Range("G10").Value
    STReportOutput1 = Range("G12").Value
    STReportOutput5 = Range("G14").Value

    Shell "" & STProg & "   " & STDatei & "   " & STReport1 & "   " &
STReportOutput1 & "", 2
    Shell "" & STProg & "   " & STDatei & "   " & STReport5 & "   " &
STReportOutput5 & "", 2
End Sub
```

Anhang 6: Code zum Aktualisieren der Webabfragen in Excel

```
Sub ExtDatenAktualisieren()
    ActiveWorkbook.RefreshAll
End Sub
```

Anhang 7: Tabellenblatt *Wartung*



Anhang 8: Tabellenblatt mit Auswertung der Plausibilität der zugesicherten maximalen Ausfallzeiten

A2 =WENN(UND(ISTLEER(__imp_Plausi!A2);(__imp_Plausi!C2<>""));A1;WENN(ISTLEER(__imp_Plausi!A2);"";__imp_Plausi!A2))

	A	B	C	D	E	F	G
1	**Sachmittel...**	**...mit zugesicherter max. Ausfallzeit...**	**...benötigt Sachmittel...**	**...mit zugesicherter max. Ausfallzeit.**	**Differenz der beiden Ausfallzeiten**		
2	AS/400-Server	0	Serverraum	0	0		
3	Ballindamm 27	0					
4	BB3-Backend	0					
5	BB3-Frontend	0	Client	0	0		
6	BB3-Frontend	0	LAN	0	0		
7	BB3-Frontend	0	BB3-Server	0	0		
8	BB3-Frontend	0	WAN	0	0		
9	BB3-Frontend	0	BB3-Backend	0	0		
10	BB3-Server	0	Serverraum	0	0		
11	Bloomberg	0	Client	0	0		
12	Bloomberg	0	LAN	0	0		
13	Bloomberg	0	WAN	0	0		
14	Client	0					
15	Drucker	0					
16	Eurex-Backend	0					
17	Eurex-Frontend	0	Client	0	0		
18	Eurex-Frontend	0	LAN	0	0		
19	Eurex-Frontend	0	AS/400-Server	0	0		
20	Eurex-Frontend	0	WAN	0	0		
21	Eurex-Frontend	0	Eurex-Backend	0	0		
22	Fax-Gerät	0					
23	Händlerraum	0					
24	Internet-Service Plattform	0	WAN	0	0		
25	Investro-Plattform	0					
26	Kapstadtring 8	0					
27	KSC	0					
28	LAN	0					
29	Raum Institutionelle Sales	0					
30	RTD	0	Client	0	0		
31	RTD	0	LAN	0	0		
32	RTD	0	AS/400-Server	0	0		
33	RTD	0	WAN	0	0		

Analyse | **Plausi. zuges. Ausfallzeiten** | Wartung

Anhang 9: Tabellenblatt mit Analyse der Abhängigkeitsbeziehungen und der Attributwerte

A2 =WENN(UND(ISTLEER(__imp_AnalyseIC2);(ODER(__imp_AnalyseID2<>"";__imp_AnalyseIF2<>""")));A1;WENN(ISTLEER(__imp_AnalyseIC2);"";__imp_AnalyseIC2))

	A							
1	Prozess	Funktion	max. zulässige Ausfallzeit	Sachmittel verwendet für	zugesicherte max. Ausfallze	Sachmittel benötigt für Sachmittel	zugesicherte max. Ausfallze	zulässig ./. zugesiche
2	Orderprozess	Börsenkürzel überprüfen.	0	WVS-Backend	0			0
3	Orderprozess	Maklerzettel ausdrucken.	0	WAN	0			0
4	Orderprozess	Maklerzettel ausdrucken.	0	Händlerraum	0			0
5	Orderprozess	Maklerzettel ausdrucken.	0	LAN	0			0
6	Orderprozess	Maklerzettel ausdrucken.	0	Serverraum	0	Kapstadtring 8	0	0
7	Orderprozess	Maklerzettel ausdrucken.	0	WVS-Backend	0			0
8	Orderprozess	Maklerzettel ausdrucken.	0	AS/400-Server	0	Serverraum	0	0
9	Orderprozess	Maklerzettel ausdrucken.	0	Drucker	0			0
10	Orderprozess	Maklerzettel ausdrucken.	0	WVS-Frontend	0	Client	0	0
11	Orderprozess	Maklerzettel ausdrucken.	0	WVS-Frontend	0	LAN	0	0
12	Orderprozess	Maklerzettel ausdrucken.	0	WVS-Frontend	0	WAN	0	0
13	Orderprozess	Maklerzettel ausdrucken.	0	WVS-Frontend	0	WVS-Backend	0	0
14	Orderprozess	Order an Backend der Ba	0	WAN	0			0
15	Orderprozess	Order an Backend der Ba	0	Serverraum	0	Kapstadtring 8	0	0
16	Orderprozess	Order an Backend der Ba	0	LAN	0			0
17	Orderprozess	Order an Backend der Ba	0	BB3-Backend	0			0
18	Orderprozess	Order an Backend der Ba	0	BB3-Server	0	Serverraum	0	0
19	Orderprozess	Order an Backend der Ba	0	BB3-Frontend	0	Client	0	0
20	Orderprozess	Order an Backend der Ba	0	BB3-Frontend	0	LAN	0	0
21	Orderprozess	Order an Backend der Ba	0	BB3-Frontend	0	BB3-Server	0	0
22	Orderprozess	Order an Backend der Ba	0	BB3-Frontend	0	WAN	0	0
23	Orderprozess	Order an Backend der Ba	0	BB3-Frontend	0	BB3-Backend	0	0
24	Orderprozess	Order an Backend des W	0	WAN	0			0
25	Orderprozess	Order an Backend des W	0	WVS-Backend	0			0
26	Orderprozess	Order an Backend des W	0	LAN	0			0
27	Orderprozess	Order an Backend des W	0	WVS-Frontend	0	Client	0	0
28	Orderprozess	Order an Backend des W	0	WVS-Frontend	0	LAN	0	0
29	Orderprozess	Order an Backend des W	0	WVS-Frontend	0	WAN	0	0
30	Orderprozess	Order an Backend des W	0	WVS-Frontend	0	WVS-Backend	0	0
31	Orderprozess	Order an Börse weiterleit	0	Weitere Sachmittel Order	0			0

Analyse | Plausi. zuges. Ausfallzeiten | Wartung

Anhang 10: Inhalt der beigefügten CD-ROM

Die beigefügte CD-ROM enthält die beiden Ordner *Internet-Quellen* und *Konzept* und *Master Thesis*.

In dieser Arbeit wurden Internet-Quellen genutzt. Um der Flüchtigkeit des Mediums *Internet* zu begegnen, sind im Ordner *Internet-Quellen* alle verwendeten Quellen gespeichert, die über das Internet verfügbar sind. Dieses sind gleichzeitig alle Quellen, zu denen im Quellenverzeichnis ein Hyperlink angegeben wurde. Die Dateinamen entsprechen der Zitierweise in den Fußnoten dieser Arbeit.

Im Ordner *Konzept* befindet sich die im sechsten Kapitel vorgestellte Lösung sowie die Datei *Installation.pdf*, der entnommen werden kann, wie die Lösung genutzt werden kann. Voraussetzung hierfür ist eine vorhandene Installation von *SemTalk 2.1.0.5196* (oder neuere Version) und *Excel 2000*.

Der Ordner *Master Thesis* enthält diese Arbeit in Form einer PDF-Datei.

Eidesstattliche Versicherung

Hiermit versichere ich an Eides statt, dass ich die vorliegende Arbeit selbständig und ohne die Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Alle wörtlich oder sinngemäß den Schriften anderer Autoren entnommene Stellen habe ich kenntlich gemacht.

Hans-Christian Wegner