Anja Hechenblaikner

Operational Risk in Banken

GABLER EDITION WISSENSCHAFT

Bank- und Finanzwirtschaft

Herausgegeben von
Professor Dr. Hermann Meyer zu Selhausen

Weitreichende Veränderungen auf den Finanzmärkten bringen große Herausforderungen für Theorie und Praxis mit sich. Die Schriftenreihe „Bank- und Finanzwirtschaft" greift Entwicklungen und Probleme aus diesem Fachgebiet auf. Sie bietet ein Forum für wissenschaftliche Beiträge und stellt Lösungsansätze und Forschungsergebnisse zu aktuellen Problemen der Bank- und Finanzwirtschaft zur Diskussion.

Anja Hechenblaikner

Operational Risk in Banken

Eine methodenkritische Analyse der Messung von IT-Risiken

Mit einem Geleitwort von
Prof. Dr. Hermann Meyer zu Selhausen

Deutscher Universitäts-Verlag

Bibliografische Information Der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

Dissertation Universität München, 2006

1. Auflage Juni 2006

Lektorat: Brigitte Siegel / Stefanie Loyal

Der Deutsche Universitäts-Verlag ist ein Unternehmen von Springer Science+Business Media.
www.duv.de

Umschlaggestaltung: Regine Zimmer, Dipl.-Designerin, Frankfurt/Main
Druck und Buchbinder: Rosch-Buch, Scheßlitz
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier
Printed in Germany

ISBN-10 3-8350-0424-7
ISBN-13 978-3-8350-0424-5

Geleitwort

Im Rahmen der Neuen Basler Eigenkapitalvereinbarung (Basel II) hat der Basler Ausschuss für Bankenaufsicht für die Messung des Operational Risk drei Ansätze vorgeschlagen, den Basisindikatoransatz, den Standardansatz und den institutsindividuellen fortgeschrittenen Ansatz. Sowohl der Basisindikator- als auch der Standardansatz sind so grob und geradezu primitiv, dass die großen Institute bestrebt sind, eigene Ansätze zur Risikomessung zu entwickeln und von der Bankenaufsicht anerkennen zu lassen, um eine vergleichsweise niedrigere Eigenkapitalunterlegung des Operational Risk zu erreichen. Die Entwicklung fortgeschrittener Ansätze ist schon seit Jahren in Gang, und daran wird auch nach der Umsetzung von Basel II weiter gearbeitet werden. Eine wissenschaftliche Begleitung dieser Entwicklungen ist auch weiterhin wünschenswert.

Mit den von ihm vorgeschlagenen Ansätzen hat sich der Basler Ausschuss zum Treiber einer Entwicklung gemacht, die durchaus auch ungute Züge trägt: Einige Institute fühlen sich geradezu unter Druck, eigene Ansätze zu entwickeln und anerkennen zu lassen. Parallel hierzu kam bei vielen Bank-Risikomanagern der dringende Wunsch auf, nach den Markt- und Kreditrisiken nun auch noch die Operationellen Risiken nach dem Konzept des Value-at-Risk zu messen und in die gesamtbankbezogene Risk-Return-Steuerung zu integrieren. Das alles hat dazu geführt, dass in konzeptioneller und auch methodischer Hinsicht teilweise sehr fragwürdige Kompromisse gemacht werden, nicht nur von Praktikern des Risikomanagements. Aus diesen Gründen ist es sehr zu begrüßen, dass die Verfasserin der vorliegenden Schrift es sich zur Aufgabe gemacht hat, die Entwicklung der Modelle und Methoden für die Messung von Operational Risk und speziell IT-Risiken aus wissenschaftlicher Sicht distanziert und methodenkritisch aufzuarbeiten und zu begleiten.

Bevor die verschiedenen Ansätze zur Messung von IT-Risiken analysiert werden können, entwickelt die Verfasserin die folgenden methodenbezogenen Beurteilungskriterien: Datenverfügbarkeit und Datenqualität, Verwendbarkeit der Messergebnisse insbesondere im Risikomanagement, Kausalzusammenhang zwischen Messgröße und IT-Risiko, Berücksichtigung von Abhängigkeiten zwischen Risikofaktoren, Berücksichtigung der aktuellen Risikosituation einer Bank und Validierbarkeit des einzelnen Ansatzes. Das Kriterium „Datenverfügbarkeit und Datenqualität" ist für die Messung von Operational Risk offensichtlich von grundlegender Bedeutung. Um die ganze Tiefe dieser Problematik sichtbar zu machen, erörtert die Verfasserin sehr detailliert, welche Verzerrungen bei der Erhebung von Schadendaten auftreten können, wie leichtfertig historische Daten mit „synthetischen" Daten vermischt werden, wie eingeschränkt die Aussagekraft der Daten aus externen Datenpools ist etc. Wenn

Chief Risk Manager diese Probleme zur Kenntnis nähmen, könnten sie die Verlässlichkeit der Risikomessergebnisse, die man ihnen in der Praxis vorlegt, und die sie zur Grundlage der Risikosteuerung machen, sehr viel besser einschätzen.

Im Hauptteil der Arbeit werden die verschiedenen Ansätze jeweils kurz dargestellt, bevor die Beurteilungskriterien speziell auf Indikatoransätze und statistische / versicherungsmathematische Ansätze angewandt werden. Es zeigt sich, dass für den Basisindikatoransatz und den Standardansatz des Basler Ausschusses, die zu den Financial Risk Indicator-Ansätzen gehören, der unterstellte Kausalzusammenhang zwischen Risikoindikator (Risikoursache) und Risikowirkung empirisch nicht nachgewiesen werden kann. Die Non-Financial Risk Indicator-Ansätze stellen jeweils einen Zusammenhang her zwischen einem oder mehreren nicht-finanziellen Risikoindikatoren einerseits und der Risikowirkung andererseits, beispielsweise in Form eines Regressionsmodells. Beim IT-Risiko kommen zumeist technische Indikatoren in Betracht. Die IT-Risikowirkung wird durch Schadensummen erfasst, die sich nach der Realisierung von IT-Risiken ergeben haben. Die Verfasserin beurteilt diese Ansätze anhand ihrer Kriterien und kommt zu dem Ergebnis, dass sie durchaus ein beachtliches Potential aufweisen. Problematisch sind aber auch hier die Datenverfügbarkeit, der Nachweis von Kausalzusammenhängen, die Erfassung der Abhängigkeiten der Risikoindikatoren untereinander und die Validierung.

Von strukturell ganz anderer Art sind die statistischen / versicherungsmathematischen Ansätze. Sie beruhen empirisch auf einer Schadenanzahl- und einer Schadenhöhenverteilung, die durch theoretische Verteilungen approximiert werden. Aus diesen Verteilungen wird dann, z. B. mit der Monte-Carlo-Technik, eine Gesamtverlustverteilung gebildet, aus der die Risikomanager dann den Operational Value-at-Risk ablesen möchten. Dies Konzept ist für Risikomanager attraktiv, weil sie den Operational Value-at-Risk gern in die Risk-Return-Steuerung für die Gesamtbank integrieren möchten. So verständlich dieser Wunsch ist, so kompromisslos wird in der Praxis häufig Druck auf die Modellentwickler ausgeübt, methodische Bedenken zurückzustellen und derartige Modelle unbedingt in der Bank zu implementieren. Bei der Beurteilung dieser Ansätze anhand ihrer Kriterien zeigt die Verfasserin, dass das Problem der Datenverfügbarkeit, verglichen mit den Indikator-Ansätzen, nur in anderem Gewande auftritt: Gerade für die so bedeutenden Großschäden, die sehr selten vorkommen, gibt es nur extrem wenige Beobachtungen. Das hat die Modellentwickler dazu bewogen, die Gesamtverlustverteilung durch eine theoretische Verteilung zu approximieren, die im rechten Tail eine plausible Wahrscheinlichkeitsmasse aufweist, wenn man für die Approximation nur den „richtigen" Verteilungstyp wählt. Im Prinzip beruht dieses Vorgehen auf der Annahme, dass die empirisch nicht verfügbare Information über das Großschadensrisiko im rechten Tail der empirisch nicht validier-

baren theoretischen Verteilung für den Gesamtverlust steckt und daraus nur „deduziert" werden muss. Die Fragwürdigkeit dieses Vorgehens ist offenkundig.

Die methodenkritische Beurteilung von Ansätzen zur Messung des IT-Risikos in Banken stellt eine große Herausforderung dar. Die Problemstellung ist sehr schwer fassbar und strukturierbar, die Erfassung der relevanten empirischen Phänomene durch Datenerhebung ist nur ganz eingeschränkt möglich, und bei den in der Literatur dokumentierten Modellentwicklungen ist in methodischer Hinsicht eine geradezu provozierende Leichtfertigkeit der beteiligten Modellentwickler festzustellen, wie sie bisher nur bei Kreditportfoliorisikomodellen sichtbar geworden ist. Mit den Kriterien, die die Verfasserin für die Beurteilung der verschiedenen Ansätze entwickelt hat, gelingt ihr eine tiefgehend methodenkritische, transparente und auch Vergleiche ermöglichende Durchdringung der derzeit bekanntesten Ansätze für die Messung von IT-Risiken.

Die vorliegende Arbeit richtet sich gleichermaßen an Forscher und Praktiker des bankbetrieblichen Risikomanagements. Ich wünsche ihr, dass sie die Betroffenen zu einer kritischen Reflexion des bisherigen Vorgehens anregt und sie auch dazu bewegt, vermehrt methodenkritische Überlegungen in die Weiterentwicklung von Risikomodellen einzubringen.

Prof. Dr. Hermann Meyer zu Selhausen

Vorwort

Diese Arbeit entstand während meiner Tätigkeit als wissenschaftliche Mitarbeiterin am Seminar für Bankwirtschaft der Ludwig-Maximilians-Universität München und wurde vom Promotionsausschuss der Fakultät für Betriebswirtschaft im Wintersemester 2005/2006 als Dissertation angenommen. Obwohl man eine Dissertation letztlich immer alleine schreibt, gibt es dennoch einige Menschen, die mich bei der Erstellung wesentlich unterstützt haben und denen ich deshalb an dieser Stelle herzlich danken möchte.

An erster Stelle bedanke ich mich bei meinem Doktorvater Prof. Dr. Hermann Meyer zu Selhausen, der mir die Promotion nicht nur ermöglicht, sondern diese auch geduldig begleitet hat. Insbesondere seine intensive Auseinandersetzung mit meiner Arbeit gegen Ende der Bearbeitungszeit hat einen großen Beitrag zur Qualität der Arbeit geleistet! Prof. Dr. Elmar Helten danke ich für die engagierte Übernahme des Koreferats. Auch er hatte einen starken fachlichen Einfluss auf meine Arbeit.

Große Unterstützung habe ich durch meine Kolleginnen und Kollegen des Seminars für Bankwirtschaft erhalten, denen ich dafür herzlich danke. Hervorzuheben aus dieser mir sehr wichtigen Gemeinschaft sind Dr. Karin Stenke, Dr. Oliver Krautwurst und Dr. Stefan Decker. Die ganze Zeit über stand mir Dr. Karin Stenke mit ihrem fachlichen Rat aber auch mit großer persönlicher Unterstützung beiseite. Sie „quälte" sich durch alle meine wissenschaftlichen Ergüsse und behielt immer den Durchblick. Dr. Oliver Krautwurst war mir ein sehr wichtiger Diskussionspartner, mit dem man sich die Bälle nicht nur fachlich wunderbar hin und her spielen konnte. Von ihm habe ich viel gelernt. Ganz besonders herzlich danken möchte ich Dr. Stefan Decker. Er entwickelte sich vom Lieblingskollegen zum Mann fürs Leben. Den Weg der Dissertation mit ihm gemeinsam gehen zu können, hat diesen deutlich freundlicher werden lassen. Er war immer für mich da und hat damit maßgeblich zum Erfolg dieser Arbeit beigetragen.

Neben dieser fachlichen und persönlichen Unterstützung durch meine Kollegen erhielt ich wichtige „operative" Hilfe durch unsere wissenschaftlichen Hilfskräfte. Danke an Torsten Lorenz, Felix Noth, Sylvia Schürger und die anderen fleißigen Helfer! Ohne Euch hätte ich insbesondere die Berge an Literatur nicht Händeln können.

Ein wichtiger Schritt in der Entstehungsgeschichte dieser Promotion war das postgraduale Studium der „Betriebswirtschaftlichen Forschung". Hier lernte ich, neben einigen wissenschaftstheoretischen und methodischen Erkenntnissen, auch einige „Leidensgenossen" fachlich und persönlich kennen. Ich danke den „Freunden der

betriebswirtschaftlichen Forschung" des Jahrgangs Sommersemester 2001 für die Wegbegleitung.

Großen fachlichen Support zu meiner Arbeit erhielt ich von Dr. Thomas Hartung. Er war immer für eine Diskussion zu haben und hat mir damit nicht nur über den „Copula-Berg" geholfen. Darüber hinaus haben mich die Diskussionen mit Christian Jegg im Rahmen seiner Diplomarbeit weitergebracht. Danke dafür!

Gerade in den letzten Zügen meiner Dissertation bin ich ganz in die Tiefen des Operational Risk abgetaucht und habe meine Freunde vernachlässigt – danke an alle, die mir die Treue gehalten haben!

Zum Abschluss danke ich meiner Familie für Ihre liebevolle Unterstützung! Insbesondere meine Eltern Marita und Bernd Hechenblaikner sind immer für mich da und unterstützen mich in allen Lebenslagen. Sie haben mich persönlich geformt und mir meinen beruflichen Werdegang und diese Promotion ermöglicht – deshalb widme ich ihnen diese Arbeit!

Sollte ich jemanden vergessen haben, so ist dies wohl als ein klassisches Operational Risk – menschliches Versagen – anzusehen. Ein großes „Sorry" dafür.

Dem Leser dieser Arbeit wünsche ich, dass er eine genau so große Begeisterung für das spannende Thema Operational Risk und insbesondere dessen Messung entwickelt, wie ich es in den letzten Jahren getan habe! Durch seine Komplexität und bisweilen schwierige Greifbarkeit treibt einen das Operational Risk zwar manchmal zur Verzweiflung – bleibt damit aber auch interessant und Wert, seine Zeit damit zu verbringen.

Anja Hechenblaikner

Inhaltsverzeichnis

MAK	Mindestanforderungen an das Kreditgeschäft der Kreditinstitute
MDA	Maximum Domain of Attraction
ÖBA	Österreichisches Bankarchiv (Zeitschrift)
OECD	Organisation for Economic Co-operation and Development
ORX	Operational Riskdata eXchange Association
PHEA	Predictive Human Error Analysis
POT	Peaks over Threshold
QIS	Quantitative Impact Study
RMA	Risk Management Association
SAS	Software and Services Institute Inc.
STA	Standardised Approach / Standardansatz
VaR	Value-at-Risk
WiSt	Wirtschaftswissenschaftliches Studium (Zeitschrift)
ZBB	Zeitschrift für Bankrecht und Bankwirtschaft
ZfgK	Zeitschrift für das gesamte Kreditwesen
ZKA	Zentraler Kreditausschuss

Abkürzungsverzeichnis

AMA	Advanced Measurement Approaches / fortgeschrittene Ansätze
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
Basel II	Die neue Basler Eigenkapitalvereinbarung
BIA	Basis Indicator Approach / Basisindikatoransatz
BIS	Bank for International Settlements
BIT	Banking and Information Technology (Zeitschrift)
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz)
c.d.f.	cumulative distribution function / kumulative Verteilungsfunktion
CPU	Central Processing Unit / Prozessor
CVaR	Conditional Value-at-Risk
DAX	Deutscher Aktienindex
DIN	Deutsches Institut für Normung e.V.
DIT	Deutscher Investment-Trust Gesellschaft für Wertpapieranlage mbH
EU	Europäische Union
GuV	Gewinn- und Verlustrechnung
EVT	Extreme Value Theory / Extremwerttheorie
FIRST	Financial Institutions Risk Scenario Trend Database
FMEA	Failure Mode and Effect Analysis / Fehlermöglichkeits- und –einflussanalyse
HAZOP	Hazard and Operability Study
IAS	International Accounting Standards
IEC	International Electrotechnical Commission
IFRS	International Financial Reporting Standards
ISDA	International Swaps and Derivatives Association Inc.
ISO	International Organization for Standardization
IT	Informationstechnik / Informationstechnologie / Information Technology
KCI	Key Control Indicator
KPI	Key Performance Indicator
KRI	Key Risk Indicator
MAH	Mindestanforderungen an das Betreiben von Handelsgeschäften

Abbildungsverzeichnis

Anhangsverzeichnis

1. Einleitung

1.1 Problemstellung

Der wesentliche Einfluss der Informationstechnologie (IT) auf Kreditinstitute ist in der Literatur unumstritten.[1] Viel diskutiert ist der Einsatz der IT vor allem im Zusammenhang mit Rentabilität und strategischen Wettbewerbsvorteilen.[2] Ein sehr wesentlicher Gesichtspunkt für Banken ist aber auch das Risiko, das aus dem Einsatz von IT resultiert. Es kann davon ausgegangen werden, dass ein Ausfall wesentlicher IT-Systeme über einen längeren Zeitraum zu hohen Schäden und im Extremfall sogar zur Insolvenz einer Bank führen kann.[3]

An großer Bedeutung gewonnen hat die Betrachtung des IT-Risikos in letzter Zeit vor allen Dingen auch dadurch, dass das IT-Risiko ein Teilaspekt des Operational Risk ist.[4] Durch zahlreiche spektakuläre Verlustfälle[5] in den letzten Jahren wurde die Öffentlichkeit für diese Risikokategorie sensibilisiert. Auch die Bankenaufsicht wurde durch die, teilweise dramatischen, Verlustfälle auf diese Risikokategorie aufmerksam und hat im Rahmen der Neuen Basler Eigenkapitalvereinbarung (Basel II) im Januar 2001[6] erstmals explizite Regelungen zur aufsichtsrechtlichen Behandlung von operationellen Risiken getroffen.[7] In den derzeitig in Deutschland geltenden aufsichtsrechtlichen Vorschriften des Grundsatz I über die Eigenmittel der Institute[8] werden operationelle Risiken nur implizit über eine „Überschätzung" des Kreditrisikos abgedeckt.[9]

---

[1] Vgl. bspw. Meyer zu Selhausen, H. (Bank-Informationssysteme, 2000), S. 5; Moormann, J. (Digitalisierung, 2000), S. 5ff.; Wings, H. (Digital Business, 1999), S. 10.

[2] Vgl. bspw. Hanow, G.A. (Produktivität, 1999), S. 18f.; Moormann, J. (Umbruch, 1999), S. 5ff.

[3] Vgl. Bartl, D. R. (Sicherheitsanforderungen, 2003), S. 112; Petruch, K. (Technik, 2002), S. 278. Untersuchungen deuten darauf hin, dass bei einem vollständigen Ausfall der EDV selbst die elementarsten bankbetrieblichen Funktionen nicht länger als eine Woche aufrechterhalten werden könnten. Vgl. Büschgen, H. E. (Prüfstein, 1992), S. 84. Eine Untersuchung von Hammer, V. ((Technikgestaltung, 1999), S. 161) ermittelt als unternehmensgefährdende IT-Ausfallzeit für Banken einen Wert von 2 Tagen.

[4] Vgl. Basel Committee on Banking Supervision (Capital Accord, 2003), Punkt 607 und siehe Kap. 2.1.1.2, S. 11.

[5] Einen Überblick über zahlreiche Fälle gibt z. B. Peachey, A. (Finanzdesaster, 2002), S. 327ff. oder Brandner et al. (Finanzdienstleistungsunternehmen, 2002), S. 347ff.

[6] Vgl. Basel Committee on Banking Supervision (Capital Accord, 2001).

[7] Vgl. Höfer, S. / Schrott, A. (Blick, 2003), S. 158. Bereits 1998 veröffentlichte der Basler Ausschuss für Bankenaufsicht ein kurzes Arbeitspapier zum Thema „Operational Risk Management" (Vgl. Basel Committee on Banking Supervision (Operational Risk Management, 1998)). Dieses enthält allerdings weder konkrete Regelungen zu Operational Risk noch eine Definition, sondern stellt dar, dass Operational Risk ein wichtiges Thema für Banken sei, mit dem sich nun auch die Bankenaufsicht in Zukunft beschäftigen wolle.

[8] Vgl. BaFin (Grundsatz I, 1997).

[9] Vgl. Basel Committee on Banking Supervision (Operational Risk, 2001), S. 1 und Deutsche Bundesbank (Monatsbericht April, 2001), S. 28.

Auch in den Verlautbarungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) wie den „Mindestanforderungen an das Betreiben von Handelsgeschäften" (MAH) und den „Mindestanforderungen an das Kreditgeschäft der Kreditinstitute"[10] (MAK) werden zwar Aspekte des operationellen Risikos angesprochen, allerdings wird dies nicht explizit genannt.

Nun wird im Rahmen von Basel II vom Basler Ausschuss für Bankenaufsicht eine Unterlegung des Operational Risk mit Eigenkapital gefordert, wie dies bereits für Marktpreis- und Kreditrisiken geregelt ist.[11] Begründung hierfür ist, dass durch die verbesserte und damit risikosensitivere Messung der Kreditrisiken nach Basel II nun ein kleinerer „Eigenkapitalpuffer" für „andere Risiken", wie das Operational Risk, bei der Eigenmittelunterlegung der Kreditrisiken entsteht.[12] Zum anderen hat die Aufsicht erkannt, dass das Operational Risk aufgrund zahlreicher Entwicklungen in der Bankpraxis immer mehr an Bedeutung gewinnt. Dazu zählen insbesondere eine wachsende IT-Abhängigkeit der Bankgeschäfte und eine hohe Komplexität der Geschäftstätigkeit der Banken aufgrund von Entwicklungen wie Konzentrationsprozessen in der Kreditwirtschaft, Outsourcing, Entwicklung komplexer Finanzprodukte etc.[13] Im Rahmen der Forderung nach einer Eigenkapitalunterlegung der Operational Risk erfolgt daher durch den Basler Ausschuss eine Definition von Operational Risk und die Darstellung unterschiedlicher Ansätze zur Ermittlung der notwendigen Eigenkapitalunterlegung und damit implizit zur Messung von Operational Risk.

Allerdings haben sich im Risikomanagement der Banken noch keine Standards zur Messung von Operational Risk etabliert.[14] Es existiert eine Vielzahl an unterschiedlichsten Ansätzen zur Quantifizierung von operationellen Risiken, die sich in ihrer Vorgehensweise und der benötigten Datengrundlage teilweise erheblich unterscheiden.[15] Vom Basler Ausschuss werden grundsätzlich drei Ansätze zur Ermittlung der Eigenmittelunterlegung vorgeschlagen.[16] Diese sind so gestaltet, dass sie ein Spektrum mit zunehmender Sophistizierung und Risikosensitivität bilden, auf dem sich die Banken von einfacheren zu fortgeschritteneren Ansätzen bewegen können. Dabei

---

[10] Vgl. BaFin (MAK, 2002).

[11] Vgl. Basel Committee on Banking Supervision (Capital Accord, 2001), S. 94ff.

[12] Vgl. Basel Committee on Banking Supervision (Operational Risk, 2001), S. 1.

[13] Vgl. Basel Committee on Banking Supervision (Operational Risk, 2001), S. 1 und Deutsche Bundesbank (Monatsbericht April, 2001), S. 28.

[14] Vgl. Haas, M. / Kaiser, T. (Insufficiency, 2004), S. 13; Faisst, U. / Kovacs, M. (Methodenvergleich, 2003), S. 342; Schierenbeck, H. (Bankmanagement, 2003), S. 483.

[15] Vgl. Faisst, U. / Kovacs, M. (Methodenvergleich, 2003), S. 342.

[16] Vgl. hierzu und im folgenden Basle Committee on Banking Supervision (Convergence, 2004), S. 137. Die drei Ansätze sind der Basic Indicator Approach, der Standardised Approach und die Advanced Measurement Approaches, die unter bestimmten Voraussetzungen den Einsatz bankinterner Modelle erlauben.

enthalten die ersten beiden Ansätze ganz konkrete Vorgaben, wie die Messung zu erfolgen hat, während im Rahmen des dritten Ansatzes die Banken die Möglichkeit haben, eigene Ansätze zur Messung durch die Bankenaufsicht anerkennen zu lassen. Durch die Regelungen des Basler Ausschusses zur Eigenmittelunterlegung der Operational Risk entsteht deshalb für die Kreditinstitute ein Ansporn, eigene Ansätze zur Messung zu entwickeln.[17] Durch den vorhandenen Zeitdruck[18] ist es dabei aber vor allem wichtig, zu überprüfen, ob diese Ansätze auch methodischen Ansprüchen genügen und als valide[19] einzustufen sind.[20]

Unstrittig ist in der aktuellen Diskussion, die seit Veröffentlichung des zweiten Entwurfs zur Änderung der Eigenkapitalvereinbarung von 1988 im Januar 2001[21] den entscheidenden Antrieb bekommen hat[22] und seitdem auch laufend an Intensität zunimmt, dass das Operational Risk und damit auch das IT-Risiko eine hohe Bedeutung für Banken hat.[23] Geeinigt hat man sich derzeit auch auf eine weitgehend akzeptierte Definition des Operational Risk[24], die allerdings in dieser Form für ein sinnvolles Management dieser Risiken noch viel zu allgemein ist[25] und einer genaueren Konkretisierung, insbesondere auch in speziellen Teilbereichen wie dem IT-Risiko mit allen seinen Besonderheiten, bedarf. Forschungsbedarf gibt es vor allem noch im

---

[17] Vgl. Röckle, S. (Schadensdatenbanken, 2002), S. 35.

[18] Es ist vorgesehen, dass der Basler Akkord Ende 2006 in nationales Recht umgesetzt werden soll. Für die fortgeschritteneren Ansätze ist Ende 2007 als Startzeitpunkt geplant. Siehe Basel Committee on Banking Supervision (Convergence, 2004), Punkt 2, S. 1.

[19] Der Basler Ausschuss fordert bspw. zur Anerkennung eines fortgeschrittenen Ansatzes, dass dieser validiert werden kann. Vgl. Basle Committee on Banking Supervision (Convergence, 2004), Punkt 666 und 668, S. 144.

[20] Schon bei Kreditportfoliorisikomodellen, wie bspw. Credit Metrics oder CreditRisk+, hat sich gezeigt, dass eine schnelle Forcierung der Entwicklung solcher Modelle teilweise auf Kosten der methodischen Gründlichkeit und Absicherung dieser Modelle geht. Vgl. hierzu ausführlich Meyer zu Selhausen, H. (Validierung, 2004).

[21] Vgl. Basel Committee on Banking Supervision (Capital Accord, 2001). Der erste Entwurf der Änderung des Kapitalakkords im Juni 1999 (Basel Committee on Banking Supervision (Framework, 1999), S. 50f., Punkt 82-87) enthält bereits Hinweise darauf, dass operationelle Risiken bei der Eigenkapitalunterlegung berücksichtigt werden sollen, explizite Eigenkapitalanforderungen werden aber erst im Entwurf vom Januar 2001 konkretisiert und erläutert.

[22] Vgl. Locarek-Junge, H. (IT-Risikomanagement, 2002), S. 3.

[23] Insbesondere die Tatsache, dass Operational Risk nach Inkrafttreten des neuen Basler Eigenkapitalakkords mit Eigenkapital unterlegt werden müssen, hat diese Erkenntnis stark forciert. Vgl. hierzu bspw. Dowd, V. (Basel approach, 2003), S. 31; Cap Gemini Ernst & Young (Trends, 2002), S. 10. In dieser Studie zu operationellen Risiken in Kreditinstituten gaben die befragten Kreditinstitute als wichtigste Motivation zum Aufbau eines Operational Risk-Controllings die regulatorischen Anforderungen an.

[24] Vgl. hierzu ausführlich Kap. 2.1.1.1, S. 8ff.

[25] Vgl. Piaz, J.-M. (Banken, 2002), S. 4.

Bereich der Identifikations-[26] und Messmethoden für diese Risiken. Zwar existiert für beide Fragestellungen bereits eine Vielzahl von Methoden, die häufig aus anderen Teilbereichen des Risikomanagements[27] oder auch aus anderen Forschungsbereichen und Branchen übernommen wurden. Allerdings hat sich noch kein Standard herausgebildet und es fehlt vor allem an Tests, die die Korrektheit und die Leistungsfähigkeit dieser Methoden zeigen. Vielmehr täuschen die Messmethoden, die im Ergebnis einen möglichen Verlustbetrag in Euro ausweisen, derzeit eher eine Exaktheit vor, die zum jetzigen Stand aber noch nicht gegeben ist und somit das Bankmanagement zu falschen Schlussfolgerungen verleiten kann.[28] Eine schlüssige und methodisch gesicherte Messung des IT-Risikos ist eine unabdingbare Voraussetzung für eine sinnvolle Steuerung dieses Risikos[29] und auch für eine adäquate aufsichtsrechtliche Eigenkapitalunterlegung.

Obwohl die aufsichtsrechtlichen Vorschriften als „Treiber" der Entwicklung im Bereich des Managements von Operational Risk und damit auch der IT-Risiken zu sehen sind, ist es aber für Banken auch wichtig zu erkennen, dass IT-Risiken schon aus betriebswirtschaftlichen Gesichtspunkten eines fundierten und gezielten Managements bedürfen. Im Bereich der IT ist deshalb die IT-Sicherheit – als komplementärer Begriff zum IT-Risiko[30] – längst ein Thema und es gibt zahlreiche Bestrebungen, die IT-Sicherheit zu erhöhen. Dazu gehören bspw. das IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik[31] oder der ISO/IEC 17799:2000 „Information Technology – Code of Practice for Information Security Management"[32], ein Standard der „International Organization for Standardization". Dieses bereits vorhandene Wissen im Bereich der IT-Sicherheit wird allerdings selten in die eher finanzwirtschaftlich orientierte Diskussion um das „Operational Risk" eingebracht.[33]

In der Literatur existieren also Schwerpunkte im Bereich des technischen IT-Sicherheitsmanagements, die finanzwirtschaftliche Perspektive des Risikomanage-

---

[26] Auf eine nähere Analyse der Identifikationsmethoden wird in dieser Arbeit verzichtet. Eine umfangreiche Beschäftigung mit möglichen Identifikationsmethoden hat ergeben, dass Aussagen zu Vor- oder Nachteilen einzelner Verfahren nur sehr vage möglich sind und regelmäßig sehr stark vom einzelnen Kreditinstitut abhängen. Ein Überblick über mögliche Identifikationsmethoden wird im Kap. 2.2.2, S. 25ff. gegeben.

[27] Vgl. ähnlich Buzziol, S. (Systematik, 2004), S. 19.

[28] Vgl. Jörg, M. / Roßbach, P. (Messung, 2002), S. 92.

[29] Vgl. ähnlich Romeike, F. (Risikokategorien, 2003), S. 165.

[30] Vgl. Locarek-Junge, H. (IT-Risikomanagement, 2002), S. 5.

[31] Vgl. Bundesamt für Sicherheit in der Informationstechnik (IT-Grundschutzhandbuch, 1999).

[32] Vgl. hierzu bspw. Voßbein, R. (Zertifizierung, 2002), S. 25ff.

[33] Vgl. Locarek-Junge, H. (IT-Risikomanagement, 2002), S. 4.

ments wird aber häufig vernachlässigt.[34] Für die Messung des Operational Risk finden sich zwischenzeitlich Ausführungen in zahlreichen Veröffentlichungen. Allerdings enthalten diese entweder nur einen groben Überblick über Ansätze zur Messung des Operational Risk, ohne diese methodisch näher zu beleuchten und die Anwendbarkeit der Ansätze zu hinterfragen.[35] Zu den statistischen / versicherungsmathematischen Ansätzen existieren hingegen zahlreiche Aufsätze, die schon sehr tief in methodische Feinheiten der Ansätze gehen, ohne dass die Anwendungsvoraussetzungen kritisch diskutiert werden.[36] Bei Indikatoransätzen beschränkt sich die Literatur größtenteils auf die Basler Ansätze sowie auf den Einsatz von Indikatoren zur Risikosteuerung.[37]

---

[34] Eine Ausnahme stellt hier bspw. der Sammelband von Roßbach, P. / Locarek-Junge, H. (IT-Sicherheitsmanagement, 2002), dar, in dem neben der rein technischen Sichtweise auch andere Perspektiven eingenommen werden.

[35] Vgl. bspw. Piaz, J.-M. (Banken, 2002); Jörg, M. (Herausforderungen, 2002); Minz, K.-A. (Operationelle Risiken, 2004).

[36] Vgl. bspw. Frachot, A. et al. (Operational Risk, 2001); Frachot, A. et al. (Loss Distribution Approach, 2003); Leippold, M. / Vanini, P. (Quantification, 2003).

[37] Vgl. bspw. Brink, G. J. van den (Risiko-Indikatoren, 2004); Taylor, D. / Hofmann, D. G. (Signal Failure, 1999).

1.2 Ziel und Gang der Untersuchung

In der vorliegenden Arbeit wird der Fokus auf ein Teilgebiet der operationellen Risiken gelegt, und zwar wie bereits angedeutet auf die Risiken, die aus dem Einsatz von IT-Systemen resultieren. Dies ist sinnvoll, da IT-Risiken aufgrund der hohen Abhängigkeit der Kreditinstitute vom IT-Einsatz eine besondere Bedeutung erlangen.[38] Dabei werden bereits vorhandene Kenntnisse aus dem Bereich der IT-Sicherheit mit der finanzwirtschaftlichen Sichtweise, die in Basel II gefordert wird, verbunden.

Ziel dieser Arbeit ist es nun im speziellen, eine sinnvolle Definition als Basis für ein Management von IT-Risiken zu erarbeiten, sowie ausgewählte Methoden zur Messung von IT-Risiken in Kreditinstituten darzustellen und kritisch zu beurteilen. Es wurden zwei grundlegende Klassen von Ansätzen ausgewählt: Indikatoransätze und statistische / versicherungsmathematische Ansätze. Diese werden detailliert dargestellt und in Bezug auf die Anwendbarkeit, aber insbesondere auch auf die Validität und Einhaltung methodischer Ansprüche beleuchtet.

Als Grundlage für diese Arbeit werden zunächst die wesentlichen Begriffe geklärt und Risikokategorien gebildet, ohne die ein sinnvolles Management für IT-Risiken nicht möglich ist. Dazu werden in **Kap. 2** die wesentlichen Begriffe „Operational Risk" (Kap. 2.1.1) und „IT-Risiko" (Kap. 2.1.2) definiert und kategorisiert. Darauf aufbauend wird in Kap. 2.2 der IT-Risikomanagementprozess in seinen Grundlagen beleuchtet. Dabei wird auf die Notwendigkeit eines IT-Risikomanagements eingegangen und die einzelnen Phasen des Prozesses, d. h. Identifikation, Messung, Steuerung und Kontrolle, werden kurz erläutert.

In **Kap. 3** erfolgen eine Darstellung wesentlicher Grundlagen zur Messung von IT-Risiken sowie eine Entwicklung methodenbezogener Beurteilungskriterien. Dabei wird zunächst in Kap. 3.1 ein Überblick über Ansätze zur Messung von IT-Risiken gegeben und eine Einordnung der Ansätze in Klassen vorgenommen. In dieser Arbeit nicht weiter verfolgte Klassen von Ansätzen werden kurz beschrieben und ihr Ausschluss begründet. In Kap. 3.2 werden die im Kap. 4 heranzuziehenden methodenbezogenen Beurteilungskriterien entwickelt. Anschließend werden im Kap. 3.3 wesentliche Grundlagen für das Beurteilungskriterium „Datenverfügbarkeit und Datenqualität" beleuchtet. Wegen der besonderen Bedeutung der Daten und um Redundanzen in den beurteilenden Kapiteln zu vermeiden, wird an dieser Stelle auf verschiedene Arten von Daten, mögliche Datenquellen und Probleme im Zusammenhang mit den Daten und dem Datensammlungsprozess eingegangen.

In **Kap. 4** erfolgt eine Darstellung und methodenkritische Beurteilung von Indikatoransätzen und statistischen / versicherungsmathematischen Ansätzen. Dabei werden

---

[38] Vgl. Moormann, J. (Umbruch, 1999), S. 5f.

zunächst in Kap. 4.1 Indikatoransätze, getrennt nach Ansätzen, die auf Financial Risk Indicators (Kap. 4.1.2) bzw. auf Nonfinancial Risk Indicators (Kap. 4.1.3) aufbauen, dargestellt und anhand der in Kap. 3.2 entwickelten Kriterien beurteilt. Der Fokus bei den Ansätzen auf Basis von Financial Risk Indicators liegt auf dem Basisindikator- und dem Standardansatz des Basler Ausschusses. Die Ausführungen zu den Nonfinancial Risk Indicators bringen neue Ideen zu Indikatoren, die im Zusammenhang mit der Messung von IT-Risiken vielversprechend sind. Abschließend zu Kap. 4.1 werden darüber hinaus Kombinationen von Risikoindikatoren zur Messung analysiert (Kap. 4.1.4). In Kap. 4.2 werden statistische / versicherungsmathematische Ansätze zur Messung des IT-Risikos detailliert dargestellt (Kap. 4.2.1) und ebenfalls anhand der ausgewählten Kriterien beurteilt (Kap. 4.2.2). Am Ende des Kap. 4 steht eine zusammenfassende Beurteilung der betrachteten Messansätze (Kap. 4.3). Zusätzlich werden Einsatzempfehlungen für Indikatoransätze und statistische / versicherungsmathematische Ansätze abgeleitet.

Die Arbeit schließt in **Kap. 5** damit, Parallelen zwischen der IT-Risikomessung und der Messung anderer Risikoarten in Banken aufzuzeigen. Zudem wird in **Kap. 6** ein kurzer Ausblick auf bevorstehende Entwicklungen gegeben.

2. Grundlagen zu IT-Risiken und zum IT-Risikomanagementprozess

2.1 Definition und Kategorisierung von IT-Risiken als Teil des Operational Risk

2.1.1 Operational Risk

2.1.1.1 Definition des Operational Risk

Schon in der Umgangssprache finden sich vielfältige Bedeutungen für den Begriff „Risiko".[39] Auch in der betriebswirtschaftlichen Literatur gibt es eine Vielzahl unterschiedlicher Definitionen.[40] Die vorhandenen Risikodefinitionen lassen sich bspw. in drei Gruppen einteilen[41], wobei eine Unterscheidung nach Ursache und Wirkung des Risikos vorgenommen wird:

Die erste Gruppe zielt dabei auf die ökonomische Wirkung des Risikos ab und definiert Risiko „...als Möglichkeit der Planverfehlung, als Gefahr einer Fehlentscheidung, als Verlustgefahr und als Gefahr einer Zielabweichung."[42]

Die zweite Gruppe stellt die Ursache des Risikos in den Vordergrund und versucht Risiko über ein vorhandenes Informationsdefizit zu erklären. Dabei geht sie von einer Entscheidungssituation aus, in der keine Sicherheit bezüglich der Konsequenz einer Entscheidung herrscht, aber dennoch entweder objektive und / oder subjektive Wahrscheinlichkeitsverteilungen für die eintretenden Konsequenzen vorliegen, durch die das Risiko beschrieben wird.[43]

Die dritte Gruppe führt die beiden oben genannten Komponenten zusammen und definiert Risiko als eine Kombination von möglicher Zielverfehlung und einem Informationsdefizit. So sieht Helten den Risikobegriff „...immer in Zusammenhang mit unvollständiger und unvollkommener Information über die Wirkungszusammenhänge der Realität und den daraus resultierenden Ziel- und Planabweichungen, die möglicherweise zu Schäden und Verlusten führen können..."[44]. Ziel- und Planabweichungen, die zu einem positiven Ergebnis führen, können hingegen als „Chance" bezeichnet werden.[45]

---

[39] Vgl. Helten, E. (Messung, 1994), S. 1f.

[40] Vgl. Härterich, S. (Produktrisiken, 1987), S. 3.

[41] Zu dieser Dreiteilung der Risikodefinitionen siehe Braun, H. (Risikomanagement, 1984), S. 22ff. und vgl. zu den folgenden Ausführungen Härterich, S. (Produktrisiken, 1987), S. 5ff.

[42] Härterich, S. (Produktrisiken, 1987), S. 6.

[43] Vgl. z. B. Knight, F. H. (Risk, 1921), S. 197ff. oder Bamberg, G. / Coenenberg, A. G. (Entscheidungslehre, 1996), S. 66ff.

[44] Helten, E. (Messung, 1994), S. 2.

[45] Vgl. Büschgen, H. E. (Bankbetriebslehre, 1998), S. 865.

Diese Definition von Helten berücksichtigt sowohl Ursachen als auch Wirkungen des Risikos und scheint damit insbesondere als Hintergrund für eine Definition des Operational Risk und als Basis für ein Management dieser Risiken geeignet.

Ursachen für Operational Risk[46] sind im bankinternen Bereich zu finden, dort wo die spezifischen Charakteristika eines Kreditinstituts liegen.[47] Folglich müssten eigentlich so viele Definitionen für das operationelle Risiko existieren, wie es Banken gibt, um die institutsspezifischen Besonderheiten jeder einzelnen Bank widerzuspiegeln.[48] Dies wird auch von der Aufsicht erkannt. So gesteht der Basler Ausschuss den Kreditinstituten zu, eigene Definitionen anzuwenden. Voraussetzung ist, dass die Definitionen die Operational Risk klar abgrenzen und dass alle wesentlichen Risiken sowie deren Ursachen erfasst werden.[49]

Da in der vorliegenden Arbeit nicht auf Besonderheiten einzelner Kreditinstitute eingegangen werden kann, ist es sinnvoll, hier die am weitesten verbreitete und auch weitgehend akzeptierte Operational Risk-Definition des Basler Ausschusses heranzuziehen:[50]

„Operational Risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk."[51]

Diese Definition enthält sowohl Ursachen von Operational Risk als auch deren Wirkungen. Dabei werden die Ursachen zunächst in externe und interne Ursachen getrennt. Externe Ursachen wirken von außen auf das Unternehmen ein und können von diesem nicht beeinflusst werden, wie bspw. Naturkatastrophen. Interne Ursachen liegen im Bereich von Prozessen, Menschen und Systemen.[52] Betrachtet wer-

---

[46] Begrifflich werden hier die angelsächsische Originalbezeichnung „Operational Risk" sowie deren offizielle Übersetzung (vgl. Übersetzung der Deutschen Bundesbank: Basler Ausschuss für Bankenaufsicht (Eigenkapitalvereinbarung, 2001)) „operationelles Risiko" verwendet. Verzichtet wird auf Begriffe wie „Betriebsrisiko", „operatives Risiko" oder „operationales Risiko", da es hierbei zu sprachlichen Differenzen kommen kann. Bspw. wird unter Betriebsrisiko teilweise nur das Risiko der direkten Geschäftsabwicklung verstanden, also ein Teilbereich der Operational Risk. Der Begriff „operatives Risiko" könnte als Gegenstück zum „strategischen Risiko" gesehen werden, was dem Operational Risk aber ebenfalls nicht vollumfänglich gerecht wird. Vgl. bspw. Beeck, H. / Kaiser, T. (Value-at-Risk, 2000), S. 636f.

[47] Vgl. Röckle, S. (Schadensdatenbanken, 2002), S. 19.

[48] Einen Überblick über unterschiedliche Definitionen gibt Piaz, J.-M. (Banken, 2002). S. 58ff.

[49] Vgl. Basel Committee on Banking Supervision (Sound Practices 2003), S. 2.

[50] Vgl. Geiger, H. / Piaz, J.-M. (Bewertung, 2001), S. 792. Ursprünglich resultiert diese Definition aus einer Studie der British Bankers`Association (BBA), der International Swaps and Derivates Association (ISDA) und der Robert Morris Association (RMA) in Zusammenarbeit mit Pricewaterhouse-Coopers (PwC), vgl. BBA et al. (Frontier, 1999), S. 3.

[51] Vgl. Basel Committee on Banking Supervision (Convergence, 2004), Punkt 644, S. 137.

[52] Eine Betrachtung der Ursachen für Operational Risk findet in Kap 2.1.1.2, S. 11ff. statt.

den darüber hinaus auch Risiken, die rechtlicher Natur sind. Explizit ausgeschlossen werden hingegen Risiken, die der Bank aus strategischen Entscheidungen oder im Zusammenhang mit der Reputation entstehen. Als Wirkungen von operationellen Risiken werden Verluste definiert.[53]

Keine weitere Beachtung findet in dieser Arbeit die ebenfalls weit verbreite indirekte Definition, die unter Operational Risk alle Risiken, die nicht eindeutig dem Marktpreis- oder dem Kreditrisiko zugeordnet werden können, fasst.[54] Dies ist zwar leicht verständlich, kann aber im wissenschaftstheoretischen Sinne kaum als Definition betrachtet werden und ist in keiner Weise als Basis für ein Risikomanagement von Operational Risk geeignet, da die Vielfalt des Operational Risk nicht ansatzweise konkretisiert wird.

Die durch diese Negativdefinition implizierte Einordnung des Operational Risk in das Risikospektrum der Bank als ein Erfolgsrisiko[55] kann jedoch als sinnvoll erachtet werden, da eine Auswirkung des Operational Risk auf den finanziellen Erfolg des Kreditinstituts zu bejahen ist.[56] Im Gegensatz zu Marktpreisrisiken und Kreditrisiken, die als Erfolgsrisiken des liquiditätsmäßig-finanziellen Bereichs gesehen werden können, ist das Operational Risk ein Erfolgsrisiko des technisch-organisatorischen Bereichs.[57] Von den aus der Geschäftstätigkeit einer Bank resultierenden Erfolgs- und Liquiditätsrisiken sind noch auf einer höheren Ebene die strategischen Risiken abzugrenzen, die nicht aus Einzelgeschäften, sondern aus langfristig wirkenden Entscheidungen auf der Ebene der Gesamtbank oder einzelner strategischer Geschäftsfelder resultieren.[58] Oftmals wird das strategische Risiko den operationellen Risiken

---

[53] In der ersten Version von Basel II wurde noch zwischen direkten und indirekten Verlusten unterschieden (vgl. Basel Committee on Banking Supervision (Capital Accord 2001), S. 94). Direkte Verluste sind Verluste, die sich im Falle des Eintretens eines Risikoereignisses direkt in der Gewinn- und Verlustrechnung niederschlagen, während indirekte Verluste durch einen Potentialverlust für die Zukunft, bspw. durch Verlust eines Kunden oder von Know-how eines Mitarbeiters, gekennzeichnet sind (vgl. Münchbach, D. (Private Banking, 2001), S. 18ff.). Indirekte Verluste sind nur sehr schwer zu erfassen. Ferner stehen sie oft in einem direkten Zusammenhang mit der Reputation des Kreditinstituts. Das Reputationsrisiko wurde aber gezielt aus der Definition des Operational Risk ausgeschlossen. Ferner sieht es der Basler Ausschuss nicht als sinnvoll, die indirekten Verluste mit Eigenkapital zu unterlegen, sodass diese aus der Definition ausgeschlossen wurden und nun nur noch allgemein von Verlusten gesprochen wird, wobei mögliche Verlustereignisse durch das Konsultationspapier vorgegeben werden (vgl. Basel Committee on Banking Supervision (Working Paper, 2001), S. 2).

[54] Vgl. u. a. Beeck, H. / Kaiser, T. (Value-at-Risk, 2000), S. 637; Piaz, J.-M. (Banken, 2002), S. 59.

[55] Basis dieser Definition ist die Annahme, dass Schwankungen im Ertrag des Kreditinstituts aus Marktpreis-, Kredit- und operationellen Risiken resultieren, woraus sich schließen lässt, dass diese drei Risikoarten zu den Erfolgrisiken zu zählen sind. Vgl. Münchbach, D. (Private Banking, 2001), S. 16f.

[56] Zu einer ähnlichen Systematisierung wie der in dieser Arbeit getroffenen siehe Hofmann, M. (Steuerung, 2002), S. 12ff.

[57] Vgl. zu dieser Einteilung der Bereiche Büschgen, H. E. (Bankbetriebslehre, 1998), S. 869f.

[58] Vgl. Büschgen, H. E. (Bankbetriebslehre, 1998), S. 880f.