Management des operationalen Risikos der Informationswirtschaft in Banken

Hermann Locarek-Junge, Lars Hengmith

Lehrstuhl für Finanzwirtschaft und Finanzdienstleistungen
Technische Universität Dresden
D-01062 Dresden
locarekj@finance.wiwi.tu-dresden.de
hengmith@finance.wiwi.tu-dresden.de

Abstract: Das operationale Risiko als Risiko direkter oder indirekter Verluste infolge unzulänglicher oder ausfallender interner Prozesse, Mitarbeiter und Systeme oder infolge von bankexternen Ereignissen ist in den Mittelpunkt des Interesses der Bankinformationswirtschaft gerückt. Die Quantifizierung des Risikos kann nur prozessorientiert erfolgen. Der Versuch Risiken zu identifizieren und zu messen trägt indirekt zu einer Verbesserung der Managementansätze bei.

1. Problemstellung

Risiken, insbesondere die zur Ertragserzielung eingegangenen Marktpreisrisiken und Risiken aus Kreditengagements, sind traditionell Betrachtungsgegenstand von Kreditinstituten (vgl. [BK00], S. 650). Ab Mitte der 90er Jahre wurde das Spektrum des Risikomanagements in Banken im Rahmen der Diskussion des Basel II-Prozesses zur Eigenkapitalunterlegung von Risiken um das Konzept der "operationalen Risiken" erweitert. Die Eigenkapitalunterlegung stellt eine Risikobegrenzungsnorm dar und hat als Bestandteil der Regulierung im Bankensystem eine Wahrung der Solvenz der Bank, sowie den Schutz der Gläubiger vor Vermögensverlusten zum Ziel (vgl. [HPW00], S. 328 ff.). Die Wahrung der Solvenz gewinnt mit der Sonderstellung von Kreditinstituten und den daraus resultierenden Quereffekten auf andere Wirtschaftsbereiche im Fall einer Insolvenz, sowie den traditionell niedrigen Eigenkapitalquoten der Banken in Deutschland zusätzlich an Bedeutung.

Während zunächst die Quantifizierung der Risiken im Mittelpunkt der Diskussion stand und versucht wurde, analog zu mathematischen Modellen des Markt- und Kreditrisikos einen „Value-at-Risk-Wert für operationale Risiken“ (vgl. [BK00], S. 650) zu ermitteln, ist in der weiteren Diskussion die Komplexität der IT-Systeme in Banken und die starke Abhängigkeit der betriebskritischen Prozesse in den Mittelpunkt des Interesses gerückt (Basler Komitee [Ba01b], [Ba01c], [Ba03], [BB01]), da ohne eine Analyse der Prozesse eine Abschätzung der Konsequenzen von fehlerhaften Prozessen nicht erfolgen kann.

In der vorliegenden Arbeit sollen Lösungen hierzu aus Prozessmanagement und Informatik-Sicherheitsmanagement aufgezeigt werden, die in bank– und finanzwirtschaftlichen Veröffentlichungen bisher kaum berücksichtigt wurden.

2. Risikodefinitionen

Das Basler Komitee für Bankenaufsicht definiert im zweiten Entwurf zu den neuen Eigenkapitalanforderungen operationales Risiko als "Risiko direkter oder indirekter Verluste infolge unzulänglicher oder ausfallender interner Prozesse, Mitarbeiter und Systeme oder infolge von bankexternen Ereignissen" (dt. Übers., [Ba01a], S. 2). Dieser nunmehr für alle Institute vorgegebenen Arbeitsgrundlage war eine rege Diskussion über die Natur und den Inhalt der operationalen Risiken vorausgegangen, die keineswegs in allen Instituten zu einem Ende gekommen ist.

Die Diskussion hält unter anderem deswegen noch an, weil die Basel II-Definition nicht als unfehlbar gesehen wird und daher auch keinen endgültigen Schlussstrich unter die Definitionsdebatte ziehen konnte. Dies zeigt sich deutlich in den Kommentaren, die während der Konsultationsfrist beim Komitee eingingen [Ba01a]. Der Zentrale Kreditausschuss (ZKA) fordert beispielsweise einen Ausschluss des Begriffes "Prozesse" aus der Definition, da nach Ansicht des ZKA diese aus der Interaktion von Menschen und Systemen entstehen und nicht als separater Risikotreiber betrachtet werden sollte (vgl. [ZKA01], S. 85). Zu den Komponenten des operationalen Risikos gehören nach Basel II die Verhaltensrisiken der Mitarbeiter (Fahrlässigkeit, Vorsatz, Unfälle), technisches Versagen (Systemausfälle), sowie Katastrophenereignisse (Sturm, Feuer, Terror). Die Definition des Basler Komitees umfasst weiterhin Rechtsrisiken, schließt aber das Reputationsrisiko, d.h. Image- und Glaubwürdigkeitsschäden, eindeutig aus (vgl. [BB00], S. 53).

Die deutschsprachige Literatur setzt vielfach Betriebsrisiken (von engl. "*operations risk*" vgl. [HPW00], S. 360 f.) mit operationalen Risiken (engl. "*operational risk*") gleich. Betriebsrisiken, d.h. Risiken, die dem laufenden Geschäftsbetrieb entspringen, bilden aber neben bankexogenen Risiken (z.B. Katastrophenrisiken) nur einen Teil des gesamten operationalen Risikos. Im deutschen Sprachraum werden Risiken weiterhin nach Entscheidungsebene und Fristigkeit in operative und strategische Risiken unterschieden. Operative Risiken, z.B. Kapazitätsfehlplanungen, betreffen das Tagesgeschäft und werden unmittelbar erfolgswirksam. Strategische Risiken, etwa das Investitionsrisiko in eine neue Technologie, wirken sich dagegen erst weit in der Zukunft auf die Ertragssituation der Bank aus. Der Begriff "operatives Risiko" ist in diesem Sinn im Deutschen bereits besetzt, so dass hier durchgehend von "operationalen Risiken" im Sinne von Basel II gesprochen werden soll.

3. Risikomanagement

3.1 Vorgehensmodell

Weitgehende Übereinstimmung besteht in der Literatur, den typischen Risikomanagement-Prozess in mehrere Phasen zu gliedern[1]. Ausgangspunkt eines wirksamen Risikomanagements stellt aus Sicht der Bank eine **Strategiedefinition** und die Aufstellung eines Zielsystems dar. Im nächsten Schritt müssen alle für die Informationsinfrastruktur und bankinternen Prozesse relevanten Risiken **identifiziert und analysiert** werden.

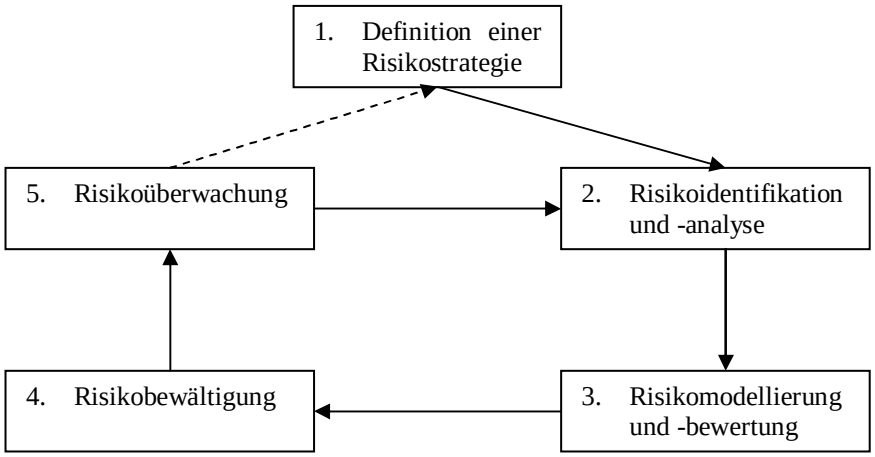

Abbildung 1: Der Risikomanagementprozess als Regelkreis

Diese ergeben sich aus vorhandenen Bedrohungen, wobei gleichzeitig Schwachstellen im Institut offengelegt werden. Kenntnisse der Risikoarten und deren Interdependenzen bilden die Grundlage für eine qualitative und quantitative **Risikobewertung**. Die erkannten und bewerteten Risiken müssen dann entsprechend **gesteuert** werden. In Umsetzung des Controlling-Gedankens sind im Rahmen einer **Risikoüberwachung** die getroffenen Maßnahmenentscheidungen auch hinsichtlich ihrer Wirksamkeit und Wirtschaftlichkeit kontinuierlich zu überprüfen. Der vorgestellte Managementprozess ist durch seinen generischen Charakter für alle typischen Bankrisiken (vgl. auch [Lü00], S. 1475), damit speziell auch für operationale Risiken anwendbar. Die permanente Entstehung neuer Risiken in einer sich schnell wandelnden Geschäftswelt muss eine Bank zu einer erhöhten Aufmerksamkeit veranlassen und zu wiederholten, d.h. zyklischen Prozessdurchläufen führen (vgl. [TS00], S. 20).

Die vorliegende Arbeit orientiert sich im weiteren Verlauf an diesem Phasenmodell und erläutert die einzelnen Schritte für operationale Risiken im Bereich der Informationsverarbeitung im Detail.

[1] Konrad stellt eine Reihe von Vorgehensmodellen näher vor (vgl. dazu [Ko98], S. 46 ff.; vgl. ebenso den Regelkreis nach [Lü00], S. 1475).

3.2 Strategiedefinition

Ausgehend von strategischen Zielen (z.B. ”Sicherste Bank im Online-Banking“) eines Instituts sind Sicherheitsziele für die Informationsinfrastruktur abzuleiten (vgl. [Ko98], S. 100). Dabei überwiegen bei der Betrachtung von Informationssystemen nicht nur in Kreditinstituten traditionell drei Sicherheitsziele[2]:

- Die Sicherung der **Verfügbarkeit** bedeutet, dass vorhandene Systeme und angebotene Dienste vor beabsichtigtem oder technischem Ausfall geschützt werden.

- Die inhaltliche Richtigkeit und (nachträgliche) Unveränderbarkeit von Informationen durch unbefugte Dritte beschreiben das Ziel der **Integrität**.

- **Vertraulichkeit** heißt, dass Informationen mit Schutzinteresse nur den adressierten Empfängern, z.B. den Kunden der Bank, zugänglich sind, und nicht durch Dritte gelesen werden können.

Diese Ziele werden ausgehend von der Gesamtbankebene hierarchisch für einzelne Geschäftsbereiche detailliert. Neben der Formulierung des eigentlichen Inhalts ist weiterhin ein Maßstab zu definieren, um so die Zielerreichung nachprüfen zu können. Zum Beispiel könnte die Verfügbarkeit eines Systems mit mindestens 99 % festgelegt werde, d.h. die maximale Stillstandszeit pro Jahr beträgt 3 Tage und 15 Stunden.

Die definierten Ziele müssen inklusive des Normengerüsts zum Umgang mit Sicherheitsfragen in umfassender Form schriftlich dargestellt werden. Die Bedeutung formulierter Strategien, Ziele und Richtlinien als Ausgangspunkt eines effektiven Managements wird nicht nur speziell für die Informationssicherheit, sondern darüber hinaus auch für operationale Risiken allgemein anerkannt. Sie sind z.B. integraler Bestandteil eines von der International Swaps and Derivatives Association (ISDA) vorgeschlagenen Frameworks zum Management operationaler Risiken (vgl. [ISD00], S. 21 f.).

3.3 Grundlagen der Risikoanalyse

Ziel einer Risikoidentifikation und -analyse ist eine möglichst vollständige Erfassung der relevanten Bedrohungen des Unternehmens bei gleichzeitiger Analyse potentieller Schwachstellen gegenüber diesen Bedrohungen (vgl. [Ko98], S. 23, ebenso [He99], S. 246). Die idealtypische Struktur einer Risikoanalyse ist bei [St02, S. 43 ff] beschrieben. Demnach besteht der erste Schritt darin, den **Analysebereich** abzugrenzen und zu beschreiben. Dabei sind auch die sicherheitsrelevanten Objekte zu identifizieren sowie die Beziehungen zwischen diesen Objekten zu beschreiben.

[2] Vgl. zum Beispiel [BSI00], S. 21 und [Ko98], S. 13 f.

Im Rahmen der **Risikoerkennung** werden dann die Risiken identifiziert und beschrieben. Das bedeutet, dass relevante Gefahren ermittelt und den sicherheitsrelevanten Objekten zugeordnet werden[3].

Im Folgenden werden mit der **Bedrohungsanalyse**, dem **Capability Maturity Modell** und der **Zertifizierung** drei Konzepte der Risikoidentifikation und –analyse vorgestellt.

3.4 Bedrohungsanalyse

Ziel der Bedrohungsanalyse ist, die systematische Feststellung, welche Unternehmensziele oder welche Komponenten der Informationsinfrastruktur durch welche Risiken gefährdet sind. Durch die Vielzahl von Bedrohungen in der heutigen Zeit ist es nicht möglich, diese vollständig aufzulisten[4]. Aus diesem Grund beschränken sich die folgenden Ausführungen auf die Darstellung einer allgemeinen Beschreibungsform für Bedrohungen, die Besonderheiten elektronischer Informationen und mögliche Angriffe auf die Informationsinfrastruktur.

a) Beschreibung von Bedrohungen

Nach den Common Criteria (CC) lassen sich Bedrohungen vollständig beschreiben durch (vgl. [BSI99], S. 24):

1. Quelle der Bedrohung (Urheber)
2. vermutete Angriffsmethode (Hergang des Zwischenfalls)
3. angriffsrelevante Schwachstelle (bedrohtes Objekt/Ziel)
4. Identifikation des angegriffenen Wertes (Konsequenz)

Die **Quelle der Bedrohung** kann aus Sicht der Bank sowohl endogen als auch exogen sein. Während Unfälle und Betrug durch Mitarbeiter oder technische Systemausfälle zu den internen Bedrohungen zählen, haben Hackerangriffe oder Naturkatastrophen ihren Ursprung außerhalb des Unternehmens. Es wird geschätzt, dass das größte Bedrohungspotential von internen Bedrohungen, und zwar speziell von den eigenen Mitarbeitern ausgeht. [Lü00], S. 1473 gibt den Anteil von deliktischen Handlungen, an denen unternehmensinterne Personen beteiligt sind, mit 60% an.

Die Frage nach dem **Hergang von Zwischenfällen** lässt sich durch technisches Versagen, höhere Gewalt, Unfälle, Fahrlässigkeit und Vorsatz beschreiben (vgl. [He99], S. 247 in Verbindung mit der Klassifizierung nach http://www.infosec.ch/faelle/). Zu den fahrlässigen Bedrohungen sind u.a. Bedienungsfehler, Fehler in Entwurf und Entwicklung genutzter Software zu rechnen. Zu den wichtigsten mit Vorsatz begangenen deliktischen Handlungen gehören Diebstahl, Sabotage und Betrug.

---

[3] Die nächsten Schritte der Risikoanalyse bei Stelzer sind die Risikobewertung und die Darstellung der Ergebnisse. Diese Punkte werden im Rahmen dieser Arbeit in einer separaten Phase (Risikobewertung) betrachtet.

[4] Zu einer umfassenden Darstellung der Bedrohungen der IT-Sicherheit von Banken aus technischer Sicht siehe [Ro02], S. 121 ff.; zur Darstellung von nicht-technischen Bedrohungen siehe [FBB02], S. 211 ff.

Die Common Criteria unterstellen in den verwendeten Beschreibungsmerkmalen (”vermutete Angriffsmethode“, ”angegriffener Wert“) vereinfachend, dass sämtliche Bedrohungen vorsätzlich herbeigeführt werden, da diese für die Sicherung der Informationsverarbeitung die bedeutendsten Anwendungsfälle darstellen (vgl. [BSI99], S. 15).

Nach [Ko98, S. 23] ist die **angriffsrelevante Schwachstelle** gleichzusetzen mit einem sicherheitsrelevanten Objekt. Diese bedrohten und damit zu schützenden Komponenten der Informationsinfrastruktur sind (erweitert nach [He99], S. 249):

- Gebäude
- Hardware
- Kommunikationsverbindungen
- Betriebssysteme
- Prozesse
- Anwendungsprogramme
- Daten

Daneben sind auch die im Abschnitt 3.2 diskutierten Sicherheitsziele Gegenstand der Bedrohung (vgl. insb. [He99], S. 247).

Bei der Bedrohungsanalyse muss weiterhin eine **Identifikation des angegriffenen Wertes** im Unternehmen, sowie möglicher direkter oder indirekter Konsequenzen vorgenommen werden (vgl. [TS00], S. 19), um so den Bedrohungen die richtige Bedeutung beimessen zu können (s.a. Kapitel 3.4: Risikobewertung).

b) Bedrohungspotenzial elektronischer Informationen

Für eine effiziente Identifikation der wesentlichen Risiken ist es unerlässlich, das Bedrohungspotenzial der kritischen Bereiche zu kennen. Die bankbetrieblichen Daten sind besonderen Bedrohungen ausgesetzt, da die Banken im deutschen Wirtschaftsgefüge eine Sonderstellung einnehmen. Dies liegt u.a. in den zahlreichen Verflechtungen und Einblicken der Banken in andere Bereiche der Wirtschaft im Rahmen von Kreditvergabe, als Hausbank oder Kapitaleigner begründet (vgl. [Ho97], S. 2). Banken befinden sich z.B. durch Vermögensdaten der Kunden oder durch Aufsichtsratsmandate erlangte Unternehmensinterna im Besitz hochsensibler Daten, die einem besonderen Geheimhaltungsinteresse unterliegen und die regelmäßig das Ziel von Angriffen sind[5].

Diese Daten werden größtenteils elektronisch verarbeitet und gespeichert. Gemäß Weck sind folgende Besonderheiten für elektronisch kodierte Informationen zu beachten (vgl. [We84], S. 14, ebenso bei [Bo95], S. 16 f.):

[5] Die luxemburgische Tochtergesellschaft der Commerzbank wurde im Jahr 1995 mit einer Liste von Vermögensinformationen über gutsituierte Kunden Opfer einer Erpressung (vgl. Der Spiegel 36/1995, S. 100 ff.). Der Erpresser drohte mit der Übermittlung der Daten an die deutschen Steuerbehörden. Ein ähnlicher Fall traf 1998 die Deutsche Bank (vgl. Der Spiegel 50/1998, S. 77).

- Sie sind mit Rechentechnik ohne Qualitätsverlust beliebig duplizierbar. Ein Duplikat ist genauso wertvoll wie das Original.
- Im Gegensatz zur Entwendung von physischen Gegenständen befindet sich der Eigentümer auch nach einem Informationsdiebstahl noch im Besitz der Information. Es ist damit schwer zu erkennen, ob man sich im alleinigen Besitz der Informationen befindet oder ob eine Entwendung stattgefunden hat. Eine Straftat ist schwer nachweisbar, wenn die entwendeten Informationen verarbeitet und in einen anderen Datenbestand integriert sind.
- Die Information ändert für den Besitzer den Wert durch eine Offenlegung und wird u.U. sogar wertlos, sobald er nicht mehr alleiniger Besitzer der Information ist.
- Einzelne, für sich allein wertlose Informationen, können den Informationsgehalt erhöhen, wenn sie (zeitlich oder gruppenmäßig) aggregiert betrachtet werden. Dieser Punkt ist zentrale Grundlage des Customer-Relationship-Managements oder von Data-Mining-Ansätzen, die aus vielen einzelnen Nutzungsdaten Kundenprofile erstellen. Insbesondere derartige Profildaten über Kunden stellen einen Wert für Angreifer dar.

c) Angriffe auf die Informationsinfrastruktur

Nicht nur die Frage, was bedroht ist, sondern auch die Fragen nach der Art der Bedrohung (=Wie) und dem Urheber (=Wer) sind von Interesse. Neben internen ”Angriffen“ wie Betrug oder Diebstahl, gewinnen von außen vorsätzlich begangene Delikte zunehmend an Bedeutung, was auf mehrere Faktoren zurückzuführen ist:

Nach Umfragen und fingierten Testangriffen wird geschätzt, dass 95% der Internet-Angriffe auf Unternehmen überhaupt nicht erkannt werden (vgl. Der Spiegel 20/2000, S. 77). Diese niedrigen Aufdeckungsquoten bei gleichzeitig mangelnder Abschreckung durch die Rechtslage und Rechtssprechung senken die Hemmschwellen potentieller Angreifer. Weiterhin werden durch den vernetzten Computereinsatz Angriffe ohne die physische Präsenz am Tatort möglich.

In jüngster Zeit kommt als weiterer Aspekt hinzu, dass durch ”fertige Angriffswerkzeuge“ im Internet auch durchschnittliche Computeranwender in die Lage versetzt werden, folgenschwere Angriffe zu starten (Viren, Würmer etc.[6]). Der vormals wenigen Spezialisten vorbehaltene technische Aspekt derartiger Angriffe tritt vollkommen in den Hintergrund (vgl. [Sch01], S. 98). Im Folgenden werden exemplarisch 2 typische Angriffsvarianten skizziert (vgl. [Fu00], S. 78 ff. und S. 94, sowie [HG97], Kap. 9.6).

Eine der am weitesten verbreiteten Angriffsformen ist die **Denial-of-Service (DoS)-Attacke**. Diese hat zum Ziel, bestimmte Komponenten der Informationsinfrastruktur an der Durchführung ihrer eigentlichen Arbeit zu hindern.

---

[6] Vgl. [Sch01], S. 98 ff. sowie [Sch00], S. 45. Ein Computervirus ist eine sich selbst reproduzierende und verbreitende Software mit destruktivem Charakter. Würmer beeinträchtigen dagegen ”nur“ die Rechenleistung infizierter Rechner.

Die augenscheinlichste, destruktive Variante überlastet z.B. einen Webserver mit einer Flut von Anfragen, so dass durch die Überlastung normale Anfragen nicht mehr bearbeitet werden können. Die Bedrohung beschränkt sich auf die Verfügbarkeit von Diensten. Angriffe werden so auch umgehend, d.h. zeitnah, an sehr langen Antwortzeiten oder völlig fehlender Verfügbarkeit des Dienstes erkannt. Zahlreiche Banken waren bereits Opfer dieser Angriffsform[7].

Die diffizilere Variante versucht dagegen, Sicherungsmaßnahmen außer Kraft zu setzen, indem z.B. eine *Firewall* durch andere Aufgaben daran gehindert wird, ihre bestimmte Sicherheitsfunktion zu erfüllen. DoS-Attacken dieser Art sind dann nur vorbereitende Aktionen zu weiteren Angriffen, etwa Datendiebstahl oder Betrug. Diese Variante ist schwieriger zu erkennen, wenn auf die Wirksamkeit der Sicherheitsmaßnahmen vertraut wird und diese nicht permanent kontrolliert werden.

Der **Man-in-the-middle-Angriff** hat zum Ziel, die Kommunikation von zwei Partnern (z.B. Bankkunde und Bank) abzuhören und gegebenenfalls zu manipulieren. Der Angreifer steht dabei zwischen beiden Kommunikationspartnern. Während beide Teilnehmer im Glauben sind, mit ihrem gewünschten Gegenüber zu kommunizieren, läuft sämtliche Kommunikation in Wirklichkeit über den Angreifer. Bei ungesichertem Homebanking kann er so in den Besitz der persönlichen Identifikationsnummer (PIN) und den Transaktionsnummern (TAN) des Opfers gelangen und diese zum Betrug nutzen.

Bedroht sind durch diese Angriffsart die Sicherheitsziele Vertraulichkeit, Integrität und Authentizität von Nachrichten, während das Ziel der Verfügbarkeit weitgehend unberührt bleibt.

3.5 Prozessrisikoanalyse mit Hilfe des Capability Maturity Modells

Risiken entstehen nicht nur aus den grundlegenden Bedrohungen, sondern auch aus der Gestaltung der Geschäftsprozesse der Bank. Die Betrachtung von Prozessrisiken ist somit im Rahmen einer umfassenden Risikoanalyse unabdinglich.

Im Folgenden wird mit dem *Capability Maturity Model* (CMM) beispielhaft ein Prozessreifemodell vorgestellt, welches eine Beurteilung der Entwicklungsstufe des Managements von Geschäftsprozessen und somit Aussagen über Schwachstellen und Risiken in diesen Prozessen ermöglicht. Hintergrund des für den Bereich der Softwareentwicklung entwickelten CMM ist die Annahme, dass die Steuerung/Beherrschbarkeit eines Geschäftsprozesses einen Entwicklungsprozess darstellt, den das CMM auf fünf Stufen misst. Das Software Engineering Institute (SEI) der Carnegie Mellon Universität hat mit dem CMM seit 1986 ein aus 5 Stufen bestehendes Modell zur Beurteilung von Softwareentwicklungs-Prozessen entwickelt (Version 1.0 in 1991/1992, vgl. [Pa93]). Ziel ist dabei nicht die Bewertung des Prozessoutputs (Softwareprodukt; im Sinne dieser Arbeit entsprechend der Bankleistung), sondern der Weg (=Prozess) zu dessen Erstellung.

---

[7] Zum Beispiel ConSors im März 2000 (vgl. http://www.golem.de/0003/6738.html).

Folgende Stufen werden durch das CMM definiert ([Pa93], S. 10 ff.):

1. Ausgangsstufe (Initial)

In einer Unternehmung auf Stufe 1 laufen die Prozesse vorwiegend improvisiert, d.h. ohne die Anwendung fundierter Managementpraktiken. Ein Prozessverantwortlicher wurde nicht eingesetzt und das Wissen um die Prozesse ist nicht dokumentiert. Der Output eines Prozesses hängt dann im Wesentlichen von den Fähigkeiten und vom Einsatz der beteiligten Personen ab. Für das Management stellt der gesamte Prozess eine große Black-Box dar, d.h. es ist völlig undurchsichtig, wer was warum macht oder wie lange Vorgänge dauern. Der Prozess ist somit aus Sicht des Managements nicht steuerbar, d.h. das Endergebnis kann bezüglich Zeit, Kosten und Qualitätseigenschaften praktisch nicht vorausgesagt werden. Das prozessimmanente operationale Risiko ist damit enorm.

2. Wiederholungsstufe (Repeated)

Befindet sich eine Organisation auf der Stufe 2, existieren unternehmenseigene Verfahrensweisen sowie erste Ansätze zur Planung und Kontrolle basierend auf Ergebnissen der Vergangenheit. Abläufe werden somit ohne Schlüsselpersonen wiederholbar. Ergebnisse werden für das Management an festgelegten Punkten des Prozesses sichtbar (z.B. *Meilensteine*), dazwischen dominiert aber weiterhin die Black-Box.

3. Definitionsstufe (Defined)

Eine Organisation befindet sich nach dem CMM auf der dritten Stufe, wenn die Prozesse und Verfahrensweisen unternehmensweit institutionalisiert, standardisiert und festgeschrieben sind. Die Dokumentation fördert ein besseres Verständnis für die internen Abläufe und entspricht der von Gaitanides geforderten Strukturtransparenz von Prozessen (vgl. [Ga94], S. 37 ff.). Eine Organisation auf dieser Stufe weiß, was sie tut, weiß aber nicht zwingend, wie gut sie dabei ist, da keine Messungen der Prozesse vorgenommen werden.

4. Managementstufe (Managed)

Die Managementstufe ist erreicht, wenn die definierten Prozesse auch qualitativ und quantitativ (hinsichtlich Zeit, Kosten oder anderer Parameter) überwacht werden. Über ein Prozesskennzahlenkonzept mit Performance Indikatoren lassen sich vom Management Aussagen über die Prozess- oder Ergebnisqualität schon in frühen Phasen des Prozesses treffen (z.B. mit Hilfe von Benchmarking oder dem Vergleich historischer Werte). Es wird damit z.B. transparent, wie gut ein Prozess der derzeitigen *"best practice"* entspricht, andererseits können Prozesse auf diese Weise auch frühzeitig gesteuert werden.

5. Optimierungsstufe (Optimized)

Das Hauptaugenmerk der Optimierungsstufe liegt auf der fortlaufenden Verbesserung der bestehenden Prozesse auf Grundlage der gewonnen Messwerte. Eine Organisation auf der höchsten Stufe im CMM ist eigenständig in der Lage, bestehende Prozesse, zum Beispiel durch Reengineering-Projekte, zu optimieren.

Obwohl die Softwareentwicklung sehr spezifische Eigenschaften aufweist (etwa die typische Projektorganisation mit Budgetvorgabe und Zeitrestriktionen), kann die Grundidee dennoch analog auch auf andere Domänen übertragen werden. Eine Übertragung des Konzepts auf das operationale Risikomanagement in Banken kann auf zwei Ebenen erfolgen:

1. Für jeden bankbetrieblichen Prozess kann der Reifegrad z.B. über ein Self-Assessment bestimmt werden. Prozesse auf niedrigen Stufen im Sinne des CMM stellen aus Sicht der Bank riskante, weil nicht steuerbare Abläufe dar. Gleichzeitig erlaubt das CMM die Identifikation von Schlüsselbereichen zur Verbesserung des betrachteten Prozesses.[8]

2. Gleichermaßen kann auf einer Metaebene der Prozess des Managements operationaler Risiken mit seinen dargestellten Phasen selbst Betrachtungsgegenstand des CMM sein. Mit anderen Worten befindet sich der Prozess des ORM selbst auf einem Entwicklungspfad. Mithin kann das CMM zu einer Einschätzung der Leistungsfähigkeit des Operational Risk Managements in Banken genutzt werden[9].

Bei der Anwendung des CMM muss zwischen den erwarteten und den tatsächlich realisierten Ergebnissen eines Prozesses unterschieden werden (Leistungsvermögen ex ante (”*capability*“) vs. Leistung ex post (”*performance*“), vgl. [Pa93], S. 4). Eine höhere Stufe nach CMM ist somit weder hinreichend noch notwendig für gute Prozessergebnisse oder die Verhinderung von operationalen Zwischenfällen. Nichtsdestotrotz bilden leistungsfähigere Prozesse auf einer höheren Stufe eine wichtige Voraussetzung für die Reduzierung operationaler Risiken.

Abschließend lässt sich feststellen, dass das CMM ein einfach gehaltenes Modell darstellt, um die Managementqualitäten und Risiken von Prozessen sowohl aus interner als auch aus externer Sichtweise (Bankenaufsicht) einschätzen zu können.

---

[8] Das CMM nennt diesen Anwendungsfall ”*process assessment*“ (vgl. [Pa93], S. 44).
[9] In der Sprache des CMM ist dieser Fall eine ”(*software*) *capability evaluation*“, d.h. eine Beurteilung des Leistungsvermögens (vgl. [Pa93], S. 44).

3.6 Zertifizierung und Auditierung von IT-Systemen

Zertifizierungen der IT-Systeme werden von anerkannten Zertifizierern auf Basis eines bestimmten Standards durchgeführt. Der vom British Standards Institute entwickelte BS 7799 erhebt den Anspruch, ein Wertungssystem für das Management der IT-Sicherheit zu bieten, und nicht zur Prüfung von Produkten oder Softwaresystemen ([Vo00], S. 63). Hierfür hat eine Gruppe von Praktikern in mehrjähriger Arbeit einen Fragenkatalog zur Einschätzung der Sicherheit von IT-Systemen entwickelt (vgl. [Vo02], S. 25). Als ISO 17799 wird der Standard auf internationaler Ebene weitergeführt. Neben der umfangreichen Erfahrung, welche bei der Entwicklung des Standards einfließt, sind vor allem die Objektivität des Prüfers und die effiziente Dokumentation der Sicherheit nach außen als Vorteile für das Unternehmen zu nennen (vgl. [Vo02], S. 24).

3.7 Risikobewertung

Um das Risiko sinnvoll steuern zu können, sowie um die Berechnung der Eigenkapitalunterlegung nach Basel II zu ermöglichen, ist eine Risikobewertung erforderlich. Gegenwärtig wird eine Vielzahl von Ansätzen zur Risikoquantifizierung diskutiert. Diese Ansätze können klassifiziert werden nach dem Betrachtungsobjekt (z.B. Betrachtung von Einzel-, Kumul- oder Extremschäden), nach der Ein- oder Mehrperiodigkeit des Ansatzes oder nach der Vorgehensweise (Top-Down/Bottom-Up). Der Value-at-Risk-Ansatz stellt zur Zeit das wirkungsvollste Instrument zur monetären Risikoquantifizierung dar (vgl. z.B. [JR02], S. 86). Dieses Konzept, welches ursprünglich zur Messung der Marktpreisrisiken in Banken entwickelt wurde, wird inzwischen auch zur monetären Bewertung anderer Risikoarten eingesetzt. Der Value-at-Risk beschreibt den maximalen Verlust, welcher bezüglich einer Risikoposition bzw. eines sicherheitsrelevanten Objekts im Betrachtungszeitraum mit einer vorgegebenen Wahrscheinlichkeit (entspricht dem Konfidenzniveau) nicht überschritten wird.

Im Bereich der Informationssicherheit hingegen wird das Risiko überwiegend qualitativ bestimmt, d.h. es erfolgt eine Einstufung auf einer bzw. auf mehreren Ordinalskalen[10]. Das liegt zum einen daran, dass Zusammenhänge zwischen Risikoeinflussfaktoren und der Risikoexposition zum derzeitigen Zeitpunkt meist nicht exakt bestimmt werden können und zum anderen reicht die verfügbare Datenbasis operationaler Verlustdaten i.d.R. nicht aus für die Schätzung von Modellparametern und damit für die Quantifizierung der Risiken. Die Schätzung von Eintrittswahrscheinlichkeiten und Schadenshöhen ist also nur mit großen Unsicherheiten möglich (vgl. auch [Ko98], S. 81).

Quantitative Risikobewertungen für operationale Risiken allgemein und speziell für IT-Risiken vermitteln somit den Eindruck von rechnerischer Objektivität, die in Wirklichkeit nicht vorhanden ist (vgl. dazu [Ha99], S. 104 und [BSI00], S. 44) und können daher nur als grobe Schätzwerte angesehen werden.

---

[10] Zur Vorgehensweise der qualitativen Risikoanalyse in der IT-Beratungspraxis siehe z.B. [BBL02], S. 55 ff.

Es wird auch immer – trotz Weiterentwicklung der Modelle und umfangreicher Datensammlungen – Bereiche des operationalen Risikos geben, für die eine Quantifizierung nicht sinnvoll ist. Zum Ableiten von Handlungsalternativen und zur Risikosteuerung und ist eine monetäre Aussage bezüglich der Risiken auch meist nicht notwendig.

3.8 Risikobewältigung

a) Unternehmensspezifische Maßnahmen

Aufbauend auf einer qualitativen oder quantitativen Risikobewertung müssen Maßnahmen zum Umgang mit den operationalen Risiken getroffen werden. Hierfür schlägt Gaulke eine Risikovermeidungstreppe vor, bei der folgende Instrumente eingesetzt werden (vgl. [Gau00], S.68): Risikovermeidung, Risikoverringerung, Risikoübertragung und Risikoübernahme.

Um den angemessenen und sinnvollen Einsatz dieser Instrumente sicherzustellen, müssen die wesentlichen Unternehmensprozesse einige Voraussetzungen erfüllen. Im Rahmen der Risikoidentifikation und –bewertung wird meist bereits deutlich, in welchen Kernbereichen Handlungsbedarf besteht und welche konkreten Maßnahmen zur Prozessverbesserung zu ergreifen sind. Dazu zählen neben dem Einsetzen eines Prozessverantwortlichen, der Dokumentation interner Abläufe, der Entwicklung eines Prozesskennzahlenkonzepts (z.B. Definition von Key Performance Indicators) mit anschließender Prozessmessung und der Einrichtung adäquater Kontrollmechanismen auch der Aufbau eines angemessenen Änderungsmanagements (Change Management), um der hohen Änderungsrate betrieblicher Prozesse Rechnung zu tragen.

b) Grundschutzmaßnahmen

Unabhängig von den Ergebnissen der Risikoidentifikation und –bewertung können in der Bank Grundschutzmaßnahmen durchgeführt werden. Beim Einsatz dieser Maßnahmen wird davon ausgegangen, dass Unternehmen in bestimmten Bereichen den gleichen Risiken ausgesetzt sind und diesen mit ähnlichen Sicherungsmaßnahmen begegnen können (vgl. [St02], S. 39). Als Quelle für die Auswahl der Sicherungsmaßnahmen dient z.B. das vom Bundesamt für Sicherheit in der Informationstechnik herausgegebene und in regelmäßigen Abständen aktualisierte Grundschutzhandbuch (Quelle). Grundschutzmaßnahmen sind somit geeignet, schnell und preiswert Sicherheitsmechanismen zu implementieren. Allerdings ist für neue Technologien, unternehmensspezifische Besonderheiten und kostenintensive Maßnahmen die Vorgehensweise über die Risikoidentifikation und –bewertung zu wählen, da hierfür der Grundschutz keine geeigneten Instrumente bietet, bzw. es wirtschaftlich sinnvoll ist, eine genaue Risikoanalyse durchzuführen.

3.9 Risikoüberwachung

Im Rahmen des Risikomanagements der Markt- und Kreditrisiken ist durch die Institution des Risikocontrollings eine Überwachung vorgesehen und wird auch erfolgreich angewendet (z.B. Backtesting der verwendeten Modelle auf Verträglichkeit mit den empirischen Beobachtungen und eventuelle Adaptation). Im Bereich der IT-Sicherheit ist dagegen ein Controlling-Gedanke in vielen Fällen unterentwickelt: Zum einen wird die Wirksamkeit der Maßnahmen vielfach nicht überprüft (vgl. z.B. [SH00], S. 138), zum anderen oft Sicherheit "um jeden Preis" gefordert (vgl. [BSI00], S. 198).

Die **Wirksamkeit** vorhandener Sicherungsmaßnahmen kann durch Konzeptionsfehler (d.h. die Idee ist ungeeignet) oder durch Implementierungsfehler (d.h. fehlerhafte Umsetzung der Idee) gemindert werden (vgl. auch [Fu00], S. 49f.). Ein Indikator für die Wirksamkeit des Risikomanagements ist z.B. das Verhältnis zwischen den aufgetretenen und den durch das System verhinderten Zwischenfällen.

Die **Wirtschaftlichkeit** der Maßnahmen wird durch das Verhältnis von Kosten zu Nutzen definiert. Der zentrale **Nutzen** sicherer Informationssysteme besteht neben der qualitativen Komponente der Erreichung der gesetzten Sicherheitsziele (wie Integrität, Verfügbarkeit und Vertraulichkeit) in der Abwendung realer Schäden (quantitativer Aspekt). Der Nutzen wird durch die Kosten bestimmt, die dem Unternehmen ohne Sicherungsmaßnahmen entstanden wären. Bei den **Kosten** der Sicherungsmaßnahmen fallen neben direkten Kosten (Anschaffungskosten; besser: "*Total Cost of Ownership*", TCO) auch nicht zu unterschätzende indirekte Kosten an (vgl. [We84], S. 55 f. und [NI96], S. 4). Diese umfassen u.a. die Kosten der nachlassenden Performance, z.B. durch den Einsatz von Verschlüsselungsverfahren, oder die Abnahme der Mitarbeitermotivation durch restriktive Sicherungsmaßnahmen und Beeinträchtigungen des Arbeitsablaufs (vgl. [NI96], S. 4). Die Angabe der indirekten Kosten erweist sich als schwierige Aufgabe. Daher werden in der Regel nur die direkten Kosten herangezogen.[11]

4. Fazit

Während der Bereich *Operational Risk* sich in den Diskussionen um Basel II eines hohen Interesses erfreut und diese Risikoquelle über die Kapitalunterlegung für Risiken bereits kurzfristig in die Regulierung der Bankenaufsicht integriert werden soll, wurde im Rahmen des Konsultationsprozesses und der wissenschaftlichen Beschäftigung mit dem Thema eines klar: Ziel sollte nicht nur die optimale Kapitalunterlegung der Risiken sein, sondern auch die Beherrschung der Risiken im Eigeninteresse der Institute, da die Quantifizierung der Risiken nicht immer möglich sein wird. Die Nutzung klassischer und alternativer Management-Instrumente zur Ermittlung und Steuerung des operationalen Risikos wird weiter zu entwickeln sein. Bestehende Ansätze wie CMM und ähnliche Beiträge aus der Informatik werden zu verbessern, anzupassen und zu integrieren sein. Der Basel II-Prozesses leistet zu dieser Erkenntnis einen wichtigen Beitrag.

---

[11] Für eine umfassende Aufführung aktueller Kosten für Sicherungsmaßnahmen siehe [BSI00], S. 46 ff.

Literaturverzeichnis

[Ba01a] Basler Komitee für Bankenaufsicht: Operational Risk Consultative Document. http://www.bis.org/publ/bcbsca07.pdf; 2001. [14.04.2003]

[Ba01b] Basler Komitee für Bankenaufsicht: Risk Management Principles for Electronic Banking, http://www.bis.org/publ/bcbs82.pdf ; 2001. [14.04.2003]

[Ba01c] Basler Komitee für Bankenaufsicht: Quantitative Impact Study (QIS) 2 Operational Risk Loss Data, http://www.bis.org/bcbs/qisoprisknote.pdf; 04.05.2001. [14.04.2003]

[Ba03] Basler Komitee für Bankenaufsicht: The 2002 Loss Data Collection Exercise for Operational Risk: Summary of the Data Collected, http://www.bis.org/bcbs/qis/ldce2002.pdf; März 2003. [14.04.2003]

[BB00] British Bankers' Association: BBA Launches World's First Operational Loss Database, http://www.bba.org.uk/asp/docshow.asp?docid=1569; 11.07.2000. [24.07.2001]

[BB01] British Bankers' Association: BBA Operational Risk Database Standard Data Fields, http://www.bba.org.uk/pdf/ORDbStdFields.doc; 2000. [24.07.2001]

[BK00] Beeck, H.; Kaiser, T.: Quantifizierung von Operational Risk mit Value-at-Risk, in : Johannig, L.; Rudolph, B. [Hrsg.]: Handbuch Risikomanagement Band 1: Risikomanagement für Markt-, Kredit- und operative Risiken, Uhlenbruch Verlag, Bad Soden, 2000, S. 633-653.

[Bo95] Bongard, S.: Outsourcing-Entscheidungen in der Informationsverarbeitung, Gabler Wiesbaden (zugl.: Bamberg, Univ., Diss., 1993), 1995.

[BSI99] Bundesamt für Sicherheit in der Informationstechnik (BSI): Common Criteria v.2.1 - Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, http://www.bsi.de/literat/doc/cct1_21.pdf; 1999. [25.05.2001]

[BSI00] Bundesamt für Sicherheit in der Informationstechnik (BSI): Kosten und Nutzen der IT-Sicherheit, SecuMedia Verlag Ingelsheim, 2000.

[BBL02] Bräuhäuser, M./Biltzinger, P./Lorenz, C.: Qualitative Risikoanalyse – Methodische Vorgehensweise in der IT-Beratungspraxis. In: Roßbach, P./Locarek-Junge, H. (Hrsg.): IT-Sicherheitsmanagement in Banken, Bankakademie-Verlag, Frankfurt/M. 2002.

[FBB02] Feil, S./Biltzinger, P./Bräuhäuser, M., Nicht-technische Bedrohungen und Angriffe auf die IT-Sicherheit. In: Roßbach, P./Locarek-Junge, H. (Hrsg.): IT-Sicherheitsmanagement in Banken, Bankakademie-Verlag, Frankfurt/M. 2002.

[Fu00] Fuhrberg, K.: Internet-Sicherheit, Carl Hanser Verlag München, Wien, 2. Aufl., 2000.

[Ga94] Gaitanides, M.; Scholz R.; Vrohlings, A.; Raster, M.: Prozessmanagement, Carl Hanser Verlag München, Wien, 1994.

[Gau00] Gaulke, M.: Risikomanagement bei IT-Projekten, in : Zeitschrift für Kommunikations- und EDV-Sicherheit, Heft 5, 2000, S. 66-68.

[HG97] Anonymous: Hacker's Guide (Elektronische Version), Verlag Markt+Technik München, 1997.

[Ha99] Hammer, V.: Die 2. Dimension der IT-Sicherheit, Vieweg Verlag Braunschweig, Wiesbaden (zugl.: Darmstadt, Univ., Diss., 1998), 1999.

[HPW00] Hartmann-Wendels, T.; Pfingsten, A.; Weber, M.: Bankbetriebslehre, Springer Verlag Berlin, Heidelberg, 2. Aufl., 2000.

[He99] Heinrich, L.: Informationsmanagement, Oldenbourg Verlag München, Wien, 6. Aufl., 1999.

[Ho97] Hoffmann, T.: Rechtliche Schranken interner Informationsflüsse in Kreditinstituten: vom internen Bankgeheimnis zu den "Chinese Walls" im Insiderrecht, Stuttgart, Univ., Diss., 1997.

[ISD00] International Swaps and Derivatives Association, Inc.: Operational Risk Regulatory Approach Discussion Paper, http://www.isda.org/press/pdf/orradp900.pdf ;2000. [09.04.2003]

[JR02] Jörg, M./Rossbach, P.: Messung und Bewertung operationeller Risiken. In: Roßbach, P./Locarek-Junge, H. (Hrsg.): IT-Sicherheitsmanagement in Banken, Bankakademie-Verlag, Frankfurt/M. 2002.

[Ko98] Konrad, P.: Geschäftsprozess-orientierte Simulation der Informationssicherheit, Josef Eul Verlag Lohmar (zugl.: Köln, Univ., Diss., 1998), 1998.

[Lü00] Lück, W.: Managementrisiken im Risikomanagementsystem, in : Der Betrieb, Heft 30, 2000, S. 1473-1477.

[NI96] National Institute of Standards and Technology (NIST): Generally accepted System Security Principles, http://csrc.nist.gov/publications/nistbul/csl96-10.txt ; 1996. [10.07.2001]

[Pa93] Paulk, M.C.; Curtis, B.; Chrissis, M.B.; Weber, C.V.: Capability Maturity Model for Software, Version 1.1, Software Engineering Institute, CMU/SEI-93-TR24, DTIC Number ADA263403, 1993.

[Ro02] Roßbach, P.: Bedrohungen der IT-Sicherheit aus technischer Sicht. In: Roßbach, P./Locarek-Junge, H. (Hrsg.): IT-Sicherheitsmanagement in Banken, Bankakademie-Verlag, Frankfurt/M. 2002.

[RL02] Roßbach, P./Locarek-Junge, H. (Hrsg.): IT-Sicherheitsmanagement in Banken, Bankakademie-Verlag, Frankfurt/M. 2002.

[Sch01] Schmidt, J.: Virenbasteln für Dummies, in : C't, Heft 13, 2001, S. 98-101.

[Sch00] Schmitz, W.: IT-Sicherheitskonzepte im E-Business, in : HMD 215 Praxis der Wirtschaftsinformatik, Heft 10, 2000, S. 43-48.

[SH00] Schulzki-Haddouti, Ch.: Sicherheitsökonomie, in : C't, Heft 4, 2000, S. 138-140.

[St02] Stelzer, D.: Risikoanalysen als Hilfsmittel zur Entwicklung von Sicherheitskonzepten in der Informationsverarbeitung, S. 37-54. In: Roßbach, P./Locarek-Junge, H. (Hrsg.): IT-Sicherheitsmanagement in Banken, Bankakademie-Verlag, Frankfurt/M. 2002.

[TS00] Teufel, S.; Schlienger, T.: Informationssicherheit Wege zur kontrollierten Unsicherheit, in : HMD 216 Praxis der Wirtschaftsinformatik : Security Management, 2000, S. 18-31.

[Vo00] Voßbein, R.: Aussagefähige IT-System-Zertifikate nach BS 7799, in : Zeitschrift für Kommunikations- und EDV-Sicherheit, Heft 5, 2000, S. 63-65.

[Vo02] Voßbein, R.: Auditierung und Zertifizierung der IT-Sicherheit. In: Roßbach, P./Locarek-Junge, H. (Hrsg.): IT-Sicherheitsmanagement in Banken, Bankakademie-Verlag, Frankfurt/M. 2002, S. 23-36.

[We84] Weck, G.: Datensicherheit, Teubner Stuttgart, 1984.

[ZKA01] Zentraler Kreditausschuss: Comments of the Zentraler Kreditausschuss on the Basel Committee's Consultative Document of 16 January 2001 on a New Capital Adequacy Framework for Banks ("Basel II"), http://www.bis.org/bcbs/ca/zentkred.pdf; 28.05.2001. [05.04.2003]