February 2005

Ein Steuerungsmodell für das Management von IV-Sicherheitsrisiken bei Kreditinstituten

Christian Locher
Universität Regensburg

In: Ferstl, Otto K, u.a. (Hg) 2005. *Wirtschaftsinformatik 2005: eEconomy, eGovernment, eSociety*; 7. Internationale Tagung Wirtschaftsinformatik 2005. Heidelberg: Physica-Verlag

ISBN: 3-7908-1574-8

Ein Steuerungsmodell für das Management von IV-Sicherheitsrisiken bei Kreditinstituten

Christian Locher
Universität Regensburg

Zusammenfassung: Die IV-Sicherheit wird in vielen Unternehmen nicht effizient genug gesteuert. Oft wird nur ein pauschaler Anteil des IT-Budgets für die Absicherung der Systeme investiert. Dies liegt daran, dass noch keine anerkannten Methoden zur Evaluation des Nutzens von Investitionen in die IV-Sicherheit entwickelt wurden. Sie werden zu pauschal und unstrukturiert behandelt. Die vorliegende Arbeit stellt einen Lösungsansatz für die Finanzwirtschaft vor. Da IV-Sicherheitsrisiken Teil des operationellen Risikos bei Kreditinstituten sind, lassen sie sich auch mit den dort gebräuchlichen Methoden bearbeiten. Basierend auf einer Systematisierung von IV-Sicherheitsinvestitionen wird ein Integrationsansatz in eine risikoorientierte Performance-Messmethode vorgestellt, die zur Beurteilung der risiko- und monetären Wirkungen von IV-Sicherheitsinvestitionen dient.

Schlüsselworte: Operationelle Risiken, Steuerung, IV-Sicherheitsrisiken, ROSI, RAPM

1 Einführung

Die in der IV-Sicherheit eingesetzten Produkte unterliegen einer stetigen technischen Verbesserung. Eine Umsetzung in ein höheres Sicherheitsniveau ist aber meist nicht festzustellen. Eine repräsentative Umfrage des BSI[1] ergab, dass 20% der deutschen IT-Sicherheitsexperten glauben, ihre Organisation wäre wegen unzureichender Sicherheitsmaßnahmen verwundbar. Die jährliche Sicherheitsstudie des CSI (Computer Security Institute)[2] ergab, dass die durchgeführten Gegenmaßnahmen oft nicht ausreichten, um auf die veränderte Bedrohungslage zu reagieren. Obwohl die Finanzwirtschaft in IV-Sicherheitsfragen sehr sensibel ist, sind die bekannt gewordenen Vorfälle der letzten Jahre erschreckend[3].

---

1 Repräsentative Telefonumfrage (N=500) im Jahr 2003, siehe http://www.bsi.de

2 Umfrage (N=494) im Jahr 2004, siehe [Gord+04]

3 z. B. Sicherheitslücke in Homebanking-Applikation (Deutsche Bank 24, 2000); Möglichkeit des Diebstahls geheimer Kundendaten (Deutsche Kreditbank, 2003); Wurm

Diese Vorfälle können sich auf mehrere Ursachen zurückführen lassen:

- Die Budgets für Informationssicherheit sind zu niedrig. Notwendige Investitionen werden deshalb nicht durchgeführt. Die durchgeführten Investitionen dienen primär der Technologieanpassung oder der Realisierung von Einsparpotenzialen.
- Die Budgets sind ausreichend, aber die Kreditinstitute haben keine mit der IV-Strategie korrespondierende Investitionsstrategie für IV-Sicherheitsmaßnahmen. Deshalb wird vorhandenes Kapital nicht zielgerichtet investiert und die Organisation wird leichter verwundbar.

Beide Gründe korrespondieren mit der Nutzenbewertung von IV-Sicherheitsinvestitionen sowie der Bereitstellung und zielgerichteten Verwendung des IV-Sicherheitsbudgets.

IV-Sicherheitsinvestitionen haben oftmals keinen über die Erhöhung des Sicherheitsniveaus hinausgehenden betriebswirtschaftlichen Nutzen. Weil die Vorteilhaftigkeit der Investition schwer zu zeigen ist, sehen sich IV-Sicherheitsabteilungen mit der Anforderung einer Quantifizierung des Nutzens konfrontiert. Das IV-Controlling muss diese Anforderungen aufnehmen und Rahmenwerke für die Bewertung von IV-Investitionen, insbesondere von IV-Sicherheitsinvestitionen entwickeln.

Neuere Ansätze der Sicherheitsökonomie identifizierten den Faktor Risiko als einen wesentlichen Faktor in der Nutzenberechnung. Diese Ansätze sind aber nach einhelliger Meinung in der Wissenschaft noch am Anfang des Reifezyklus. Viele der Modelle (u. a. der „Return on Security Investment“) nutzen überwiegend qualitative Faktoren, sollen aber monetäre Ergebnisse liefern. Vor allem aber berücksichtigen die bestehenden Ansätze nicht die offensichtliche Beziehung zu den im betriebswirtschaftlichen Controlling bzw. im Risikocontrolling genutzten Methoden. Diese bauen auf rein quantitativen Größen auf. Nur eine Integration der Kennzahlen in die dort verwendeten Methoden ermöglicht aber ein durchgängiges Controlling-Konzept im Unternehmen. Seit der Veröffentlichung von Basel II muss die IV-Sicherheit zudem in einem größeren Rahmen des operationellen Risikos eines Kreditinstituts gesehen werden.

Unter diesem Aspekt untersucht die vorliegende Arbeit bestehende Methoden zur Bewertung und Steuerung von IV-Sicherheitsinvestitionen und stellt als Lösungsansatz ein Gesamtkonzept vor.

Die Arbeit geht zunächst auf die Evaluation von IV-Investitionen ein. In diesem Kontext wird der Bezug zum Faktor Risiko bei Banken hergestellt und Methoden zur Performance-Messung, die den Faktor Risiko berücksichtigen, vorgestellt.

'Code Red' legt Geldautomaten lahm (Bank of America, 2003); Nimda Wurm legt interne Netzwerke lahm (Deutsche Bank, National Australia Bank, 2001)

Danach wird auf die IV-Sicherheit und deren Auswirkungen auf das operationelle Risiko nach Basel II eingegangen. Bestehende Ansätze zur Bewertung und Steuerung von IV-Sicherheitsmaßnahmen werden dargestellt und auf Eignung für die Integration in das operationelle Risikomanagement untersucht. Als Lösungsansatz wird ein Modell vorgestellt, das die Bewertung von IV-Sicherheitsrisiken und die Maßnahmenplanung im Kontext des operationellen Risikomanagements unterstützt. Der Beitrag schließt mit einem Ausblick auf die Integrationsmöglichkeiten in bestehende risikoadjustierte Kennzahlensysteme bei Kreditinstituten.

2 Evaluation von Investitionen

Das Sachziel des finanziellen Controllings ist die Effizienz in Form von Einnahmen, Rentabilität, Produktivität oder Liquidität eines bestimmten Projekts, einer Organisationseinheit oder einer Investition [Reic01]. Dies gilt auch für IV-Investitionen. Der Nutzen von IV-Investitionen kann aber durch weitere Kriterien, wie Qualität, Funktionalität oder Unterstützung der Unternehmensstrategie, ausgedrückt werden. Deshalb können IV-Investitionen nicht auf rein monetärer Basis bewertet werden [Krcm03].

2.1 Bewertungsmodelle für IV-Investitionen

Für eine umfassende Bewertung einer IV-Investition sind deshalb qualitative und quantitative Methoden notwendig. In der Praxis bewerten die Unternehmen Investitionsalternativen vor allem mit finanziellen Kriterien (z. B. NKW), Management-Kriterien (z. B. Unterstützung von Geschäftsmodellen) und Entwicklungs-Kriterien (z. B. Einführung einer neuen Technologie, Wahrscheinlichkeit der erfolgreichen Beendigung des Projekts) [Baco94].

Die Auswahl der Methode zur Investitionsanalyse basiert auf der Art des Projekts, der Tragweite der Auswirkungen sowie auf dem Investitionsvolumen [Olfe01], [Mile72]. Zur Bewertung der Management- und Entwicklungs-Kriterien werden qualitative Methoden genutzt [CoJa94], [Hoch94], [WiMa94]. Hierbei werden ausgewählte Kriterien ordinal bewertet und in einem Punktbewertungsmodell gewichtet und aggregiert. Anschließend wird eine Rangfolge der Investitionsalternativen festgelegt. Eine finanzielle Betrachtung der Investition muss in der Regel isoliert durchgeführt werden. Sie dominiert in der Investitionsentscheidung, wenn kein Nutzen im Sinne der Unterstützung von Geschäftsmodellen gezeigt werden kann [Baco94]. Dies gilt regelmäßig für IV-Sicherheitsinvestitionen. Nachfolgend wird deshalb insbesondere auf die finanziellen Methoden eingegangen.

2.2 Messung der finanziellen Performance von IV-Investitionen

Finanzielle Aspekte von IV-Investitionen werden mit bereits im Unternehmenscontrolling bekannten Methoden bewertet. Einige dienen eher der einmaligen Investitionsbewertung zur Entscheidungsunterstützung, andere der Unterstützung der unterjährigen Steuerung. Die Performance-Messmethoden werden grob in risikosensitive und nicht risikosensitive Ansätze unterschieden. Weiterhin kann in statische und dynamische Methoden unterschieden werden [Nage88], [Reich01].

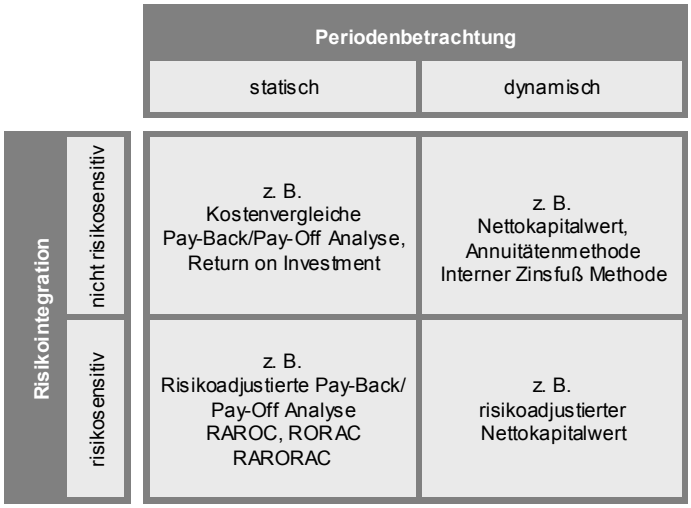

Abbildung 1: Einordnung quantitativer Methoden zur Performance-Messung

Beide Konzepte können nochmals in Residualkonzepte und Rentabilitätskonzepte unterteilt werden. Im Rahmen der Arbeit wird als statisches Konzept der Return on Investment (ROI) mit seinen abgeleiteten risikosensitiven Ansätzen und als dynamisches Konzept der Nettokapitalwert (NKW) vorgestellt. Der NKW wurde nach [Baco94] bei 75% der untersuchten IV-Projekte zur Bewertung verwendet. Die CSI Studie ergab, dass 55% der Unternehmen den ROI und 25% den NKW anwendeten [Gord+04].

Der ROI ist ein statisches Rentabilitätskonzept. Er stellt eine Beziehung zwischen den Cash-Flows und dem gebundenen Kapital her:

$$ROI = \frac{Einzahlungen - Auszahlungen}{Kapital} \tag{1}$$

Die Risikoorientierung bei der Entscheidungsfindung ist eine wesentliche Forderung von Basel II. Um diese Anforderung in den Performance-Messmethoden umzusetzen, wurden in der Kreditwirtschaft statische, risikosensitive Modelle entwickelt, die hauptsächlich auf dem Konzept des ROI basieren (z. B. *Risk adjusted return on capital* (RAROC), *Return on risk adjusted capital* (RORAC), vgl. [Brin01], [Chor04]). Allen gemeinsam ist, dass sie eine Verbindung zwischen den Cash-Flows und dem Risiko von Projekten herzustellen versuchen. Der RAROC z. B. wird wie folgt definiert[4]:

$$\text{RAROC} = \frac{\text{Einzahlungen} - \text{Auszahlungen} - \text{Erwarteter Verlust}}{\text{Regulatorisches Kapital}} \tag{2}$$

Bei den statischen Methoden zur Performance-Messung sind operationelle Risiken erst teilweise integriert. Unter der Annahme, dass operationelle Risiken mit dem Value-at-Risk (VaR)[5] gemessen werden, können diese – entsprechende Datenqualität vorausgesetzt – aber methodisch integriert werden. Der RAROC allein reicht aber nicht aus, um die Rentabilität von Investitionen zu zeigen. Hierfür muss der RAROC mit den Kapitalkosten verglichen werden: Eine Investition ist dann sinnvoll, wenn der RAROC mindestens dem Kapitalkostensatz entspricht.

Stellvertretend für die dynamischen Ansätze wird der NKW vorgestellt. Er erlaubt die Berücksichtigung von verschiedenen Cash-Flows während der ökonomischen Lebensdauer n der Investition. Alle durch das Projekt verursachten Ein- und Auszahlungen sollen hierbei berücksichtigt werden. Mit E_t als Einzahlungen und A_t als Auszahlungen in der Periode t sowie i als internem Zinsfuß, wird der Nettokapitalwert K_0 der Investition wie folgt bestimmt [Olfe01]:

$$K_0 = \sum_{t=0}^{n} (E_t - A_t) \frac{1}{(1+i)^t} \tag{3}$$

Die mit dem Projekt direkt verbundenen Risiken werden durch die Justierung des internen Zinsfußes berücksichtigt. Weitere Risiken aus dem Betrieb werden nicht im Modell abgebildet.

---

4 Die erwarteten Verluste sind als der Erwartungswert der Verluste in einer Periode definiert. Das regulatorische Kapital wird als Begriff in Abschnitt 3.2 eingeführt.

5 Der VaR ist die Verlusthöhe, die mit einem bestimmten Konfidenzniveau innerhalb einer gegebenen Periode nicht überschritten wird.

Für positive K_0 sind die Rückflüsse aus dem gebundenen Kapital höher als bei einer alternativen Investition. Die Investition wird als profitabel angesehen und sollte durchgeführt werden. Dynamische risikosensitive Methoden in der Art des NKW sind noch nicht verfügbar.

3 Management von Investitionen in die IV-Sicherheit

3.1 Begriffsverständnis und Zielsystem der IV-Sicherheit

Das deutsche BSI definiert Sicherheit als den Zustand eines IT-Systems, in dem die Risiken, die bei dessen Einsatz aufgrund von Bedrohungen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß beschränkt sind. Der Sicherheitsbegriff wird verstärkt auf Informationen als schützenswertes Gut bezogen: „Information security is intended to safeguard information. Security is the means of achieving an acceptable level of residual risks. The value of the information has to be protected." [Caze+03].

Das notwendige Sicherheitsniveau wird in einer IV-Sicherheitsstrategie festgelegt. Diese hat vier Ziele: Vorgabe fundamentaler IV-Sicherheitsziele, Definition von Ressourcen (z. B. monetär, personell), Definition einer IV-Sicherheitspolitik und Vorgabe von Verantwortlichkeiten und Organisationsstrukturen [Stel93].

Die Sachziele des IV-Sicherheitsmanagements sind die Sicherstellung von Vertraulichkeit, Integrität und Verfügbarkeit. Diese Sachziele müssen unter Berücksichtigung von bestehenden Gesetzen, Effizienz, Effektivität und Adäquatheit der Maßnahmen als Formalziele verwirklicht werden. Zur Sicherstellung eines (auch aus ökonomischen Gesichtspunkten) optimalen Investitionsportfolios muss eine Investitionsstrategie für die IV-Sicherheit formuliert werden. Fehlt diese, dann werden IV-Sicherheitsinvestitionen mehr oder weniger zufällig, auf jeden Fall aber ohne Berücksichtigung bestehender Interdependenzen, durchgeführt werden. Dabei könnten sie im schlimmsten Falle sogar entgegengesetzte Wirkungen entfalten. Die Integration möglichst vieler dieser Zielkriterien in einem Kennzahlensystem ist eines der herausragenden Probleme des IV-Sicherheitsmanagements. Die Umsetzung der IV-Sicherheit fand bisher weitgehend isoliert von unternehmerischen Gesichtspunkten statt. Der Kontext der Unternehmenssteuerung und die Integration in das operationelle Risikomanagement sind bei Kreditinstituten aber wesentliche Gestaltungsparameter. Deshalb wird im nächsten Punkt Basel II als wesentliche gesetzliche Rahmenbedingung vorgestellt.

3.2 IV-Sicherheitsrisiken im Kontext Basel II

Bankgeschäfte werden zu großen Teilen mit Fremdkapital getätigt. Weil die meisten Bankgeschäfte mit Risiken verbunden sind, müssen die Kreditinstitute diese zu einem bestimmten Prozentsatz mit Eigenkapital absichern [Base04]. Durch die Addition der Verluste aus operationellen Risiken zu den Verlusten aus Markt- und Kreditrisiken, haben Banken zusätzlich die operationellen Risiken mit Eigenkapital abzusichern [Base04]. Dabei folgen sie unten stehender Formel:

$$C_{Basel} = \frac{BIS / KWG - Kapital}{\text{Risikoaktiva Kreditrisiko} + 12{,}5 * (\text{Marktrisiko} + \text{Operationelles Risiko})} \geq 0{,}08 \quad (4)$$

Hohe operationelle Risiken werden nach Inkrafttreten von Basel II in 2007 negative Einflüsse auf das regulatorische Eigenkapital haben. Banken können dann weniger Kapital in profitable, aber risikobehaftete Geschäfte investieren. Weil das regulatorische Eigenkapital das tatsächlich vorhandene Risikokapital nicht übersteigen kann, muss es von den Kreditinstituten effizient genutzt werden: Auf der einen Seite beschränkt es die Höhe des Kapitals, das in Geschäften verbraucht werden darf. Auf der anderen Seite sollte die Summe des ungenutzten Kapitals so niedrig wie möglich sein um die Eigenkapitalrentabilität nicht zu weit zu senken.

Obwohl Basel II Banken auch die Anwendung von einfacheren, indikatorbasierten Risikomodellen (mit dem Bruttoertrag als Indikator) gestatten wird, zwingt es größere und international aktive Banken zur Anwendung von anspruchsvolleren Modellen (z. B. den in Abschnitt 4.2.3 vorgestellten Verlustverteilungsansatz). Die Kapitalallokation soll aber nicht nur auf Gesamtbankebene, sondern auch auf Geschäftsbereichsebene zur Steuerung verwendet werden [Base04]. Die Geschäftsbereiche müssen die operationellen Risiken eigenständig steuern, um das in ihrer Verantwortlichkeit liegende operationelle Risiko auf ein sinnvolles Niveau zu verringern. Risikosensitive interne Steuerungssysteme unterstützen dieses Vorgehen [Brin01].

Nach Basel II können operationelle Verluste durch Technologie, Prozesse, Menschen oder externe Ereignisse verursacht werden. Das mit dem Betrieb von IT-Systemen verbundene Risiko ist deshalb Teil des operationellen Risikos in Banken. Versuche, IV-Sicherheitsrisiken in das Management operationeller Risiken zu integrieren, sind aber noch am Anfang. Dies wird zusätzlich dadurch erschwert, dass die IV-Sicherheitsrisiken nicht explizit in einer Risikokategorie berücksichtigt werden, sondern über verschiedene Kategorien (z. B. Systemsicherheit in der Kategorie „Externer Betrug“, Kategorie „Geschäftsunterbrechungen und Systemausfälle“) verteilt sind. Dies ist z. T. unverständlich, da Banken großteils immaterielle Produkte herstellen und verarbeiten, deren Verarbeitung mittels IT stattfindet. Demzufolge haben Risiken, die mit der IT zusammenhängen, bei Banken einen sehr hohen Stellenwert. Die Herausforderung für das IV-Sicherheitsmanage-

ment liegt nun darin, entsprechende Steuerungsmethoden zu implementieren. Die damit verbundenen Schwierigkeiten werden nachfolgend diskutiert.

3.3 Bestehende Ansätze zur Steuerung von IV-Sicherheitsinvestitionen

Der Nutzen von IV-Sicherheitsinvestitionen kann nur schwer gemessen werden, da sie oft weder finanzielle Rückflüsse noch Kosteneinsparungen verursachen. Die bereits in Abschnitt 2.1 angesprochene Problematik gilt insbesondere hier: Der ökonomische Wert von IV-Sicherheitsinvestitionen (zumindest derer, die keine positiven Cash-Flows verursachen) kann nicht objektiv gezeigt werden [Voss00].[6] Sie dienen in der Regel auch nicht der Ausschöpfung von strategischen Vorteilen, sondern der Technologieanpassung („State-of-the-art“) oder der Verwirklichung eines Grundschutzes.

Das IV-Sicherheitsmanagement steht somit vor einem Dilemma: Einerseits müssen Kosten quantifiziert werden, andererseits kann nur ein qualitativer Nutzen gezeigt werden. Diese Problematik ist aber keinesfalls unabhängig vom verwendeten Vorgehensmodell zur Realisierung der IV-Sicherheit im Unternehmen. Der vom BSI favorisierte Grundschutzansatz unterstützt beispielsweise eine Kosten-Nutzen-orientierte Betrachtung nicht, weil nur Maßnahmen, die sich aus Gefährdungskatalogen ergeben, berücksichtigt werden. Eine monetäre Betrachtung der Maßnahmen erfolgt nicht.

Deshalb werden Entscheidungsmodelle gefordert, die eine zentrale Steuerung und Priorisierung von Maßnahmen unterstützen. Als zusätzliche Anforderung muss im Kontext Basel II formuliert werden, dass die verwendete Methodik zumindest in die im operationellen Risikomanagement üblichen Methoden integrierbar sein muss.

Die erste Anforderung kann durch detaillierte Risikoanalysen überwunden werden [PfPf03], [AnSh94], [Stel02]. Die Risikoanalyse wird als Methode im IV-Sicherheitsmanagement oft kritisiert [Pfle97], [Voss00]. Sie ermöglicht durch ein kardinales Bewertungsprinzip aber die Verwendung monetärer Größen [Stel02]. Einfachere Ansätze der quantitativen Risikoanalyse gehen von der Definition des Risikos als Erwartungswert eines Schadens aus (Risiko = Schaden x Eintrittswahrscheinlichkeit). Durch diese Darstellung kann es zu einer gefährlichen Gleichbehandlung unterschiedlich schwerer Schäden kommen, weshalb die Ableitung von Maßnahmen hieraus nicht zu empfehlen ist [Voss00].

---

6 Besonders der Umstand, dass nach [Gord+04] mehr als die Hälfte aller Unternehmen bereits nicht risikosensitive Performance-Messmethoden zur Evaluation von IV-Sicherheitsinvestitionen nutzten, verwundert hier.

Auf Basis der Risikoanalyse wurden Modelle entwickelt, die die Investitionsentscheidung unterstützen sollen. Der Nutzen einer IV-Sicherheitsinvestition wird z. B. durch den Risikominderungseffekt gezeigt [PfPf03]:

$$\text{Nutzen} = \text{Monetäre Risikoverminderung} - \text{Kosten für Sicherheitsmaßnahme} \quad (5)$$

Eine Sicherheitsinvestition ist dann profitabel, wenn der Risikominderungseffekt größer als die Kosten der Investition ist. Die Methodik kann über die oben angeführte Kritik hinaus kritisiert werden. Sie unterstützt die Entscheidung bei einer Investition, hilft aber nicht bei der Priorisierung verschiedener Alternativen. Es bleibt Ermessenssache des Entscheiders, wie hoch sein individueller Grenzpreis für IV-Sicherheitsinvestitionen ist (d. h. wie viel ihm z. B. ein Euro Risikoverminderung an Investitionskosten wert ist) – deshalb kann es nicht als objektives Kriterium gewertet werden. Weil traditionelle Performance-Messmethoden nicht auf den Faktor „Risiko“ eingehen, ist es nicht möglich, die Ergebnisse dieser Methode dort zu nutzen. In den risikosensitiven Methoden ist die Anwendung aber ebenso nicht möglich, da der Erwartungswert eines Risikos nur einen Teil der notwendigen Informationen ausmacht. Die zweite Anforderung lässt sich innerhalb dieses Modells deshalb nicht erfüllen. Die vorgestellte Methodik wurde in einer breiten Palette von ROSI-Konzepten weiterentwickelt. Viele ziehen neben den quantitativen Daten auch qualitative Daten zur Bewertung heran. Eine Erweiterung durch Variablen wie *criticality factor*, *exposure factor*, *vulnerability factor* (vgl. [Micr03]) scheint ebenso wenig sinnvoll. Die Kriterien sind nicht mehr orthogonal zu einander und der Vorteil der Quantifizierung wird durch qualitative Kriterien aufgeweicht.

[Cavu+04] stellen eine spieltheoretische Lösung des Problems vor. Sie argumentieren, dass IV-Sicherheit mit dem Verhalten von Angreifern und Verteidigern (also dem IV-Sicherheitsmanagement) zu tun habe. Also müssten Ansätze zur Maßnahmenplanung verwendet werden, die die Ziel- und Wertesysteme der beteiligten Parteien berücksichtigen. Allgemein muss an dem Ansatz kritisiert werden, dass er von einem intentionalen Angreifer ausgeht. Es ist fraglich, wie der Ansatz z. B. auf Wurmattacken der letzten Zeit anzuwenden wäre. Der Ansatz geht auch nur auf einen sehr engen Sicherheitsbegriff im Sinne des Angriffs auf bestimmte IT-Systeme ein. Die Aufstellung der Auszahlungsmatrix baut wie die oben genannten Modelle auf quantitative Risikoanalysen auf. Der Ansatz kann eine zentrale Entscheidungsunterstützung für einen begrenzten Anwendungsbereich bieten. Die zweite Forderung kann dieser Ansatz ebenfalls nicht erfüllen.

Eine andere Herangehensweise ist, die im operationellen Risikomanagement entwickelten Methoden auf Anwendbarkeit zu überprüfen. Schließlich sind IV-Sicherheitsrisiken, wie in Abschnitt 3.2 gezeigt, ein Bestandteil der operationellen Risiken. Von einem solchen Ansatz geht der in Kapitel 4 gezeigte Lösungsansatz aus. Er wendet den meistverwendeten fortgeschrittenen Ansatz, den Verlustverteilungsansatz, auf die IV-Sicherheit an. Die Datenversorgung geschieht wie in den

anderen Ansätzen durch quantitative Risikoanalysen. Diesen liegt aber ein anderes Risikoverständnis zu Grunde: Das Risiko wird als Zufallsvariable verstanden, die einer spezifischen Verteilung unterliegt. Die Verwendung von statistischen Verteilungen ist dem Erwartungswert vorzuziehen, weil im späteren Verlauf auch unerwartete Verluste (d. h. Verluste, die zwischen dem Erwartungswert und dem VaR liegen) mit in der Berechnung berücksichtigt werden sollen. Gerade diese sind für die Eigenkapitalunterlegung nach Basel II interessant. Die erste Anforderung kann bei einer hinreichend großen Verlusthistorie in Verbindung mit Expertenmeinungen durch Risikoanalysen hergestellt werden. Zusätzliche Informationen zu Risikoereignissen, z. B. der durchschnittliche und maximale Schaden können in den Risikoanalysen mit aufgenommen werden. Die zwei Forderungen können auf diesem Weg erfüllt werden. Der Ansatz weicht nicht unerheblich von den bisherigen Ansätzen zur Umsetzung der IV-Sicherheit ab. Ein Nutzen entsteht aber nur dann, wenn der Ansatz richtig im Unternehmen angewendet wird. Dies wird im nachfolgenden Kapitel beschrieben.

4 Ein Steuerungsmodell für IV-Sicherheitsinvestitionen

Das vorhergehende Kapitel zeigte, dass bestehende Methoden das IV-Sicherheitsmanagement nur unvollständig unterstützen: Qualitativen Methoden mangelt es an Transparenz und Objektivität, während quantitative Modelle auf Basis von nicht risikosensitiven Methoden nicht in der Lage sind, die Erhöhung des Sicherheitsniveaus als betriebswirtschaftlichen Nutzen auszudrücken. Der hier vorgestellte Ansatz bietet die Möglichkeit, verschiedenartige IV-Sicherheitsinvestitionen quantitativ zu bewerten und Empfehlungen für die Investitionsentscheidung auszusprechen. Hierfür müssen die IV-Sicherheitsinvestitionen in sinnvolle Gruppen unterteilt und eine Investitionsstrategie formuliert werden.

4.1 Systematisierung von IV-Sicherheitsinvestitionen

Alle Investitionen, deren Gegenstand die IV-Sicherheitsinfrastruktur eines Unternehmens ist, werden nachfolgend als IV-Sicherheitsinvestition bezeichnet. Damit wird dem Umstand Rechnung getragen, dass IV-Sicherheitsinvestitionen nicht zwingend nur das Sicherheitsniveau erhöhen. Eine Systematisierung in den Dimensionen *Motivation* der Investition und deren *Auswirkung* erscheint deshalb sinnvoll.

Eine Investition kann entweder durch eine sicherheitstechnische Notwendigkeit (z. B. verursacht durch Release-Wechsel und Einstellung des Kundensupports

durch den Hersteller, Grundschutz, aktuelle Bedrohungen) oder durch ein Kosten-Nutzen-Kalkül motiviert sein.

Die Auswirkungen der Investition sind davon unabhängig. Im Wesentlichen können drei Auswirkungs-Typen identifiziert werden:

1. Durch die Investition wird lediglich eine neue Technologie im Unternehmen eingeführt. Es gibt neben den Anschaffungskosten keine Auswirkungen auf die Kostenstruktur bzw. auf das Sicherheitsniveau.
2. Die Investition kann – durch Nutzung von Synergieeffekten oder durch Prozessverbesserungen – Rationalisierungspotenziale freisetzen. Dies ist durch Kosteneinsparungen messbar. Beispiele sind Enterprise Access Management Software, Nutzung von VPN (Virtual Private Networks) an statt RAS (Remote Access Service) Servern, Passwort-Synchronisation (oder Single-Sign-On) oder die Nutzung von Managed Services. Diese Auswirkungen können mit herkömmlichen Methoden zur Investitionsanalyse erfasst werden.
3. Durch eine Erhöhung des Sicherheitsniveaus kann ein geringeres Risiko erreicht werden. Das heißt, ein IT-System wird davor bewahrt, unter das geforderte Sicherheitsniveau zu fallen. Mit den traditionellen Methoden kann dieser Nutzen nicht gezeigt werden. Die Risikoanalyse ist die Ausgangsmethode zur Quantifizierung der Auswirkungen.

4.2 Methodik zur Bewertung von IV-Sicherheitsinvestitionen

Basierend auf der Segmentierung von IV-Sicherheitsinvestitionen wird eine Investitionsstrategie für die IV-Sicherheit formuliert. Anhand der Strategie wird gezeigt, wie IV-Sicherheitsinvestitionen strukturiert evaluiert werden können. Die Investitionsstrategie geht auf die in Abschnitt 2.2 eingeführten Methoden zur Performance-Messung ein. Im Verlauf wird gezeigt werden, dass es durch Einsatz von risikosensitiven Performance-Messmethoden möglich ist, die Investition innerhalb einer geschlossenen Methodik zu bewerten.

4.2.1 Definition einer Investitionsstrategie für das IV-Sicherheitsmanagement

Aus der Systematik für IV-Sicherheitsinvestitionen kann eine Investitionsstrategie abgeleitet werden. Folgende Investitionen sollen durchgeführt werden:

1. Alle sicherheitstechnisch notwendigen Investitionen, egal ob sie Auswirkungen auf Risiko- oder Kostenstrukturen der IV-Sicherheit haben.
2. Alle Investitionen, die Kostensenkungen nach sich ziehen, sodass der NKW der Investition größer oder gleich Null ist. Wenn mehr als eine mögliche Al-

ternative für die Investition bestehen, dann sollte die mit dem höchsten ROI ausgeführt werden.

3. Alle Investitionen, die ausreichende Risikoverminderungen nach sich ziehen. Weil es schwer möglich ist, die gewollten Effekte von den Nebeneffekten (z. B. durch Änderung der Umgebung) zu trennen, sollte das Risiko als konstant während der betrachteten Periode angenommen werden. Der Nutzen wird mit einem Opportunitätszinssatz berechnet:

$$Nutzen = \Delta\text{regulatorisches Kapital x Eigenkapitalrentabilität} \quad (6)$$

Die unter Punkt 1 genannten Investitionen müssen im Modell nicht zwingend einer Kosten-Nutzen-Betrachtung unterzogen werden. Nachfolgend werden die Auswirkungen 2 und 3 aus Abschnitt 4.1 untersucht. Anschließend werden die Aspekte in Abschnitt 4.3 in ein Gesamtmodell zur Steuerung von IV-Sicherheitsinvestitionen basierend auf dem RAROC zusammengefasst.

4.2.2 Bestimmung der Kostenwirkung

Weil die Einzahlungen E_t für Sicherheitsinvestitionen schwierig zu bestimmen sind, werden bei der Investitionsentscheidung nur die Auszahlungen A_t betrachtet. Im Folgenden werden beispielhaft alle Komponenten des Investitionsvorhabens „Ablösung eines RAS-Dienstes durch VPN“ betrachtet (vgl. [Cisc01]).

Veränderung der variablen Kosten (A_t) = ΔKommunikationskosten + +ΔInfrastrukturkosten + ΔWartungskosten + ΔUser-Supportkosten + Δandere variable Kosten (7)

Anschaffungskosten (A_0) = Hardwarekosten + Softwarekosten + Installationskosten + Training des Betriebspersonals + Training der Anwender + andere Kosten (8)

Der NKW der VPN-Investition in einer angenommenen 5-Jahres-Periode ist dann[7]:

$$K_0 = -A_0 + \sum_{t=1}^{5} A_t \frac{1}{(1+i)^t} \quad (9)$$

Bei $K_0 \geq 0$ ist die Investition profitabel und sollte durchgeführt werden.

[7] In diesem Fall ist A_t positiv für Kosteneinsparungen

4.2.3 Bestimmung der Risikowirkung

Investitionen, für die $K_0<0$ gilt, die aber eine Erhöhung des Sicherheitsniveaus verursachen, sind für den IV-Sicherheitsleiter schwerer zu begründen. In diesem Fall ist es sinnvoll, die Risikowirkung zu untersuchen, die – wie in Abschnitt 3.3 gezeigt – bei Kreditinstituten in eine Kostengröße transformiert werden kann. Die Aufnahme und Quantifizierung der Risiken durch Expertenmeinungen sowie interne und externe Schadensdatenbanken sind bereits Bestandteil des Managements operationeller Risiken nach Basel II. Der vorgestellte Ansatz basiert auf einem fortgeschrittenen Quantifizierungsansatz, dem Verlustverteilungsansatz[8]. Er kann institutsindividuell ausgestaltet werden, vorgegeben sind nur eine Risikokategorisierung und eine Schablone für die Geschäftsfelder der Bank sowie weitere qualitative und quantitative Vorgaben. [Base03]

Im ersten Schritt der Integration ist zu bestimmen, in wie fern IV-Sicherheitsrisiken in das operationelle Risiko der Bank einfließen. Hierfür müssen die wesentlichen Geschäftsprozesse und die wesentlichen IV-Prozesse des Kreditinstituts evaluiert werden. Die Quantifizierung ist zukunftsorientiert, d. h. sie hat in Szenarien mit und ohne Durchführung der geplanten Gegenmaßnahmen zu erfolgen. In einer Matrix werden die Verbindungen zwischen den Prozessen und den IT-Systemen dargestellt. Für jedes Wertepaar müssen – unter Berücksichtigung der Schadenshistorie – mögliche Schadensszenarien entwickelt werden. Die Geschäftseinheiten quantifizieren in der Risikoanalyse die Verluste für mögliche Szenarien (z. B. Ausfall eines IT-Systems). Die IV-Sicherheit beziffert die Verlusthäufigkeiten. Wenn die IV-Sicherheitsrisiken den Geschäftsprozessen zugeordnet sind, kann die Risikomatrix mit IV-Sicherheitsrisiken für die Gesamtbank erstellt werden (vgl. Abb. 2). Gleichartige Risiken werden hierbei in Risikokategorien zusammengefasst.

---

[8] Die Risikoquantifizierung im Verlustverteilungsansatz basiert auf einem versicherungsmathematischen Ansatz. Für jede Risikokategorie werden die identifizierten Risiken mit statistischen Verteilungen für Verlusthöhe und –häufigkeit approximiert. Basierend hierauf wird eine Monte-Carlo-Simulation für einen bestimmten Zeitraum durchgeführt. Interessant ist, ob sich für IV-Sicherheitsrisiken – ebenso wie für bereits bestehende Risikokategorien – charakterisierende Verteilungen finden lassen.

Geschäfts-prozess/ Risikokategorie	GP_1	GP_2	GP_3	…	GP_n	∑ RK
RK_1	L_{11}	L_{12}	L_{13}	...	L_{1n}	L(RK1)
RK_2	L_{21}	L_{22}	L_{23}	…	L_{2n}	L(RK2)
RK_3	L_{31}	L_{32}				L(RK3)
…	…	…	…	…	…	L(RK4)
RK_m	L_{m1}	L_{m2}	L_{m3}	…	L_{mn}	L(Rk5)
	$L(GP_1)$	$L(GP_2)$	$L(GP_3)$	….	$L(GP_n)$	∑IV-Sicherheits risiken

$L_{22}=\{l_{21},l_{22},l_{23},l_{24},\ldots,l_{2i}\}$

RK Risikokategorie
GP Geschäftsprozess
L_{mn} Aggregierte prognostizierte Verluste in RK_m des GP_n
l_{2i} i-tes Einzelrisiko für GP_2

Abbildung 2: Risikomatrix für IV-Sicherheitsrisiken

Das Gesamtrisiko L_{mn} steht für die Menge der Einzelrisiken einer Risikokategorie und eines Geschäftsprozesses. Diese Einzelrisiken werden durch Verteilungen für Verlusthöhe und Verlustwahrscheinlichkeit approxomiert. Als Maß für das Risiko kann z. B. der VaR angewendet werden (vgl. Abb. 3) [Chor04]. Die Verteilungsannahme bedingt eine gewisse Menge von Daten für jedes L_{mn}. Die Genauigkeit der Aussagen steigt mit der Anzahl der Daten. Ein Problem stellt die noch mangelnde Praxis zur Quantifizierung von Schäden der IV-Sicherheit dar. Hier helfen nur langfristige Programme für die Quantifizierung und Sammlung der Verluste, um die Genauigkeit der Methode zu steigern. Die Quantifizierung des Risikoprofils wird später in einer Monte-Carlo-Simulation in Normal- und Worst-Case-Szenarien durchgeführt, sodass ausreichendes Kapital zu diesen Risiken zugeordnet werden kann [Ande02], [Haub02]. Während in anderen Branchen zumindest derzeit keine weiteren Aussagen gemacht werden können, hilft die Formel zur Eigenkapitalunterlegung aus Abschnitt 3.2, das Risiko zur Berechnung des Nutzens zu verwenden.

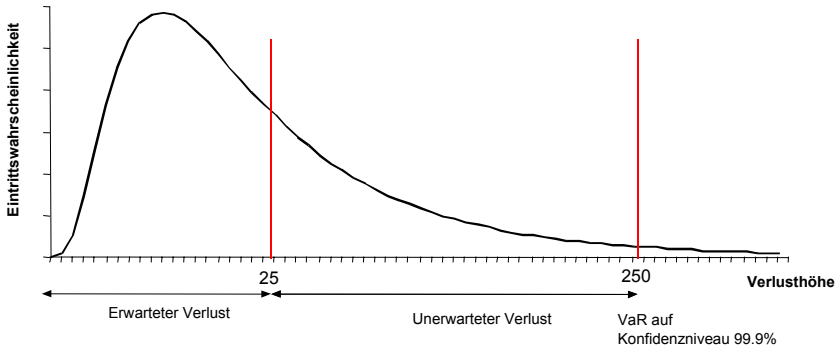

Abbildung 3: Verlustverteilung in einer Risikokategorie

In einer angenommenen 5-Jahres-Periode[9] der Investition kann dann die Rentabilität analog zu Formel 6 wie folgt ausgedrückt werden[10]:

$$K_0 = \sum_{t=0}^{5} \Delta\text{regulatorisches Kapital}_t * i_{ROE,t} \frac{1}{(1+i)^t} \tag{10}$$

Der Nutzen K_0 der Investition ist dann das auf t=0 abdiskontierte freigewordene Eigenkapital multipliziert mit der durchschnittlichen Eigenkapitalrentabilität. Die Risikowirkung wird somit ebenfalls monetär ausgedrückt und kann mit den Kosteneffekten verrechnet werden:

$$K_{o,gesamt} = -A_0 + \sum_{t=0}^{n} (A_t + \Delta\text{regulatorisches Kapital}_t * i_{ROE,t}) \frac{1}{(1+i)^t} \tag{11}$$

4.3 Integration in das RAPM eines Kreditinstituts

Die Integration in eine risikoadjustierte Performance-Messung eines Kreditinstituts komplettiert die Steuerungsinstrumente für die IV-Sicherheit. Da die Geschäftseinheiten die Kosten ihres verursachten Risikos (durch den „Kauf" von Eigenkapital) selbst tragen müssen, sind Anreize zu Investitionen in Maßnahmen zur Senkung des operationellen Risikos gegeben. Als Beispiel dient der bereits in Kapitel 2.2 vorgestellte RAROC. Weil der RAROC ein statischer Ansatz ist, müssen Cash-Flows und Risikoeffekte aus den Abschnitten 4.2.2 und 4.2.3 periodisiert werden. Die Integrationsmethodik ist dann offensichtlich (siehe Formel 2):

---

9 Tatsächlich sollte der Betrachtungszeitraum für jede Investition dynamisch gewählt werden, da diese verschiedene Charakteristiken aufweisen können.

10 Analog zum Verfahren beim Nettokapitalwert wird der Wert diskontiert.

- Die Kosteneffekte wirken sich im Zähler aus
- Die Risikoeffekte wirken sich im Zähler und im Nenner aus

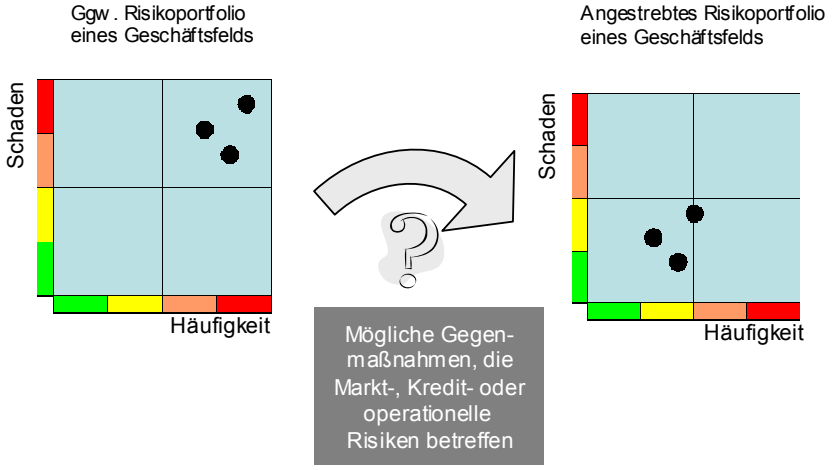

Abbildung 4: Maßnahmenplanung basierend auf Risikodaten

Alle IV-Sicherheitsrisiken sind Bestandteil des RAROC einer Geschäftseinheit. Weil operationelle Risiken keine Einnahmen generieren können, werden die Geschäftseinheiten risikoavers handeln. Wenn der RAROC der Organisationseinheit unter den Ziel-RAROC fällt (d. h. sie benötigt mehr Kapital als zuerst angenommen), könnte sie versuchen durch bestimmte Gegenmaßnahmen mindestens in einer Risikoart (d. h. Kredit-, Markt- oder operationelle Risiken) die Risiken zu senken (vgl. Abb. 4). Die Auswahl der Maßnahmen erfolgt dann rein nach Kosten-Nutzen-Gesichtspunkten. Deshalb werden nur effektive und effiziente Gegenmaßnahmen durchgeführt. Zusätzlich wird die Gefahr eines Monopolverhaltens des Anbieters der Gegenmaßnahme vermindert. Technische und organisatorische Maßnahmen sind zudem gleich berechtigt.

5 Zusammenfassung

Die vorliegende Arbeit zeigt die Schwächen bestehender Methoden bei der Bewertung und Steuerung von IV-Sicherheitsinvestitionen auf. Der Lösungsweg basiert auf bereits in den Kreditinstituten gemachten Anstrengungen. Er zeigt aber auch, dass es ohne risikosensitive Controllinginstrumente schwer ist, den Nutzen von IV-Sicherheitsinvestitionen zu zeigen. Eine Berechnung des Nutzens der Investition auf Basis der Eigenkapitalhinterlegung wurde in Abschnitt 4.2 vorgestellt. Dieses Instrument ist ideal zu Entscheidungsunterstützung vor Durchfüh-

rung der Investition. Die unterjährige Steuerung kann mit dem in Abschnitt 4.3 gezeigten Konzept besser unterstützt werden. Offensichtlich ist deshalb auch, dass nicht nur effiziente Kostenverrechnungssysteme (z. B. zur Transformation der IV-Sicherheit in ein Profit Center), sondern auch effiziente Risikoverrechnungssysteme (d. h. Transformation der IV-Sicherheit in einen Lösungsanbieter zur Risikoreduktion) gebraucht werden. Die Kreditinstitute haben bisher sehr viel Kapital in die Risikomanagementsysteme für operationelle Risiken investiert. Bisher haben sie aber vergleichsweise wenig Nutzen daraus gezogen. IV-Sicherheitsmanager könnten helfen, diesen Aufwand in Nutzen zu transformieren, indem sie eine Integrationsstrategie für die IV-Sicherheit in das Management der operationellen Risiken erarbeiten. Dies wird zwar weitere Kosten verursachen, doch würden diese durch die Vorteile aufgewogen werden. Das erfordert aber auch ein Umdenken seitens der IV-Sicherheit: Die IV-Sicherheitsrisiken sind ein Teil der operationellen Risiken. Eine Einbindung in ein Gesamtkonzept zur Steuerung operationeller Risiken erfordert die Anwendung neuer Methoden und Instrumente in der IV-Sicherheit. Nicht alle der Instrumente, z. B. die Quantifizierungsmethodik, können in der IV-Sicherheit einfach angewendet werden. Insbesondere fehlen Daten. Diese müssen verstärkt gesammelt und Methoden zur strukturierten Aufnahme der IV-Sicherheitsrisiken entwickelt werden. Die Vorteile des Vorgehens liegen dann auf der Hand: Bessere Informationen über IV-Sicherheitsrisiken, bessere Datenqualität für die Quantifizierung der operationellen Risiken, bessere Einbindung des IV-Sicherheitsmanagements in die Unternehmenssteuerung und ein besseres Verständnis über die Vorzüge einer gut gemanagten IV-Sicherheit.

Literatur

[Ande02] Anders, U.: The path to operational risk economic capital. In: Alexander, C. (Hrsg.): Operational Risk - Regulation, Analysis and Management. Prentice Hall: Upper Saddle River, 2002: S. 215-226.

[AnSh94] Anderson, A.; Shain, M.: Risk Management. In: Caelli, W.; Longley,D.; Shain, M. (Hrsg.): Information Security Handbook. MacMillan: Basingstoke, 1994: S. 75-128.

[Baco94] Bacon, J. C.: Why companies invest in information technology. In: Willcocks, L. (Hrsg.): Information Management - The evaluation of information systems investments. Chapmann & Hall, London et al., 1994: S. 31-47

[Base03] Basel Committee on Banking Supervision: Sound Practices for the Management und Supervision of Operational Risk. Bank for International Settlements: Basel, 2003.

[Base04] Basel Committee on Banking Supervision: International Convergence of Capital Measurement and Capital Standards. Bank for International Settlements: Basel, 2004.

[Brin01] Brink, G. J. van den: Operational Risk - Wie Banken das Betriebsrisiko beherrschen. Schäffer-Poeschel: Stuttgart, 2001.

[Cavu+04] Cavusoglu, H.; Cavusoglu, H.; Raghunathan, S.: Economics of IT security management: Four improvements to current security practices. Communications of the Association for Information Systems: (2002) 14, S. 65-75

[Chor04] Chorafas, D. N.: Operational Risk Control with Basel II. Elsevier: Oxford, 2004.

[Cisc01] Cisco Systems: VPN Benefits Study. http://www.cisco.com/warp/pulic/cc/soneso/vpn/vpne/cosui_br.pdf, 2001, Abruf am 2004-04-19

[CoJa94] Coleman, T.; Jamieson, M.: Beyond return on investment. In: Willcocks, L. (Hrsg.): Information Management - The evaluation of information systems investments. Chapmann & Hall: London et al., 1994.

[Caze+03] Cazemier, J. A.; Overbeek, P. L.; Peters, L. M.: IT Infrastructure Library - Security management. Stationary Office, CCTA: London, 2003.

[Gord+04] Gordon, L. A.; Loeb, M. P.; Lucyshyn, W.; Richardson, R.: 2004 CSI/FBI Computer Crime and Security Survey. San Francisco: Computer Security Institute, 2004.

[Haub02] Haubenstock, M.:The operational risk management framework. In: Alexander, C.: Operational Risk - Regulation, Analysis and Management. Prentice Hall: Upper Saddle River, 2002.

[Hoch94] Hochstrasser, B.: Justifying IT investments. In: Willcocks, L.: Information Management - The evaluation of information systems investments. Chapmann & Hall: London et al., 1994.

[King01] King, Jack L.: Operational Risk - Measurement and Modeling. Wiley: Chichester et al., 2001.

[Krcm03] Krcmar, H.: Informationsmanagement. Springer: Berlin et al., 2003.

[Loca02] Locarek-Junge, H.: IT-Risikomanagement in Banken. In: Rossbach, P.; Locarek-Junge, H. (Hrsg.): IT-Sicherheitsmanagement in Banken. Bankakademie Verlag: Frankfurt, 2002.

[Micr03] Microsoft Corporation: Securing Windows 2000 Server. http://www.microsoft.com/downloads/details.aspx?FamilyId=9964CF42-E236-4D73-AEF4-7B4FDC0A25F6&displaylang=en, 2003. Abruf am 2004-04-08.

[Mile72] Miles, L. D.: Techniques of Value Analysis and Engineering. Wiley: New York, 1972.

[Nage88] Nagel, K.: Nutzen der Informationsverarbeitung: Methoden zur Bewertung von strategischen Wettbewerbsvorteilen. Oldenbourg: München/Wien, 1988.

[OCG02] OCG: IT-Infrastructure Library - ICT Infrastructure Management. TSO: Norwich, 2002.

[Olfe01] Olfert, K.: Investition. Kiehl: Ludwigshafen (Rhein), 2001.

[Pfle97] Pfleeger, C. P.: Security in Computing. Prentice Hall: Upper Saddle River, 1997.

[PfPf03] Pfleeger, C. P.; Pfleeger, S. L.: Security in Computing. Prentice Hall: Upper Saddle River, NJ, 2003.

[Reic01] Reichmann, T.: Controlling mit Kennzahlen und Managementberichten: Grundlagen einer systemgestützten Controlling-Konzeption. München: Vahlen, 2001.

[Stel93] Stelzer, D.: Sicherheitsstrategien in der Informationsverarbeitung: ein wissensbasiertes objektorientiertes System für die Risikoanalyse. Deutscher Universitätsverlag: Köln, 1993.

[Stel02] Stelzer, D.: Risikoanalysen als Hilfsmittel zur Entwicklung von Sicherheitskonzepten in der Informationsverarbeitung. In: Rossbach, P.; Locarek-Junge, H. (Hrsg.): IT-Sicherheitsmanagement in Banken. Bankakademie Verlag: Frankfurt, 2002.

[Voss00] Vossbein, :Kosten und Nutzen der IT-Sicherheit. Studie des BSI zur Technikfolgenabschätzung. SecuMedia: Ingelheim, 2000.

[WiMa94] Willcocks, L.; Margetts, H.: Risk and information systems: developing the analysis. In: Willcocks, L. (Hrsg.): Information Management - The evaluation of information systems investments. Chapmann & Hall: London et al., 1994.