Thema:

IT-Risikomanagement: Komponenten, Prozesse und Methoden eines IT-Risikomanagementsystems

Diplomarbeit

Arbeitsgruppe Wirtschaftsinformatik III
Managementinformationssysteme

Themensteller: Prof. Hans-Knud Arndt
Betreuer: Prof. Hans-Knud Arndt

vorgelegt von: Florian Fricke

Abgabetermin: 26. September 2010

„Die Klugheit ist sehr geeignet zu bewahren, was man besitzt,
doch allein die Kühnheit versteht zu erwerben.“

(Friedrich der Große, † 1786)

Inhaltsverzeichnis

Verzeichnis der Abkürzungen und Akronyme

AktG	Aktiengesetz
Basel II	Neue Baseler Eigenkapitalvereinbarung
BIA	Business Impact Analysis
BSI	Bundesamt für Sicherheit in der Informationstechnik
GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GoBS	Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme
ISACA	Information Systems Audit and Control Association
ISM	Information Security Management
ISO	International Organization for Standardization
IT	Informationstechnologie
ITIL	Information Technology Infrastructure Library
ITSCM	IT Service Continuity Management
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
OGC	Office of Government Commerce
ROSI	Return on Security Investment
SOA	Sarbanes-Oxley Act
TCO	Total Cost of Ownership
VaR	Value at Risk

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung und Überblick

1.1 Motivation und Ziel der Arbeit

Informationstechnologien sind in der heutigen Unternehmenslandschaft nicht mehr wegzudenken. Der Einsatz dieser Technologien ermöglicht es den Unternehmen, flexibel, schnell und angemessen auf das Marktumfeld zu reagieren und so Marktanteile und Marktposition zu festigen oder auszubauen. Daher ist insbesondere der Einsatz von Computern in Unternehmen als Indikator für den Einsatz von Informationstechnologien zu sehen. Wie eine Auswertung der Genesis – Datenbank des Statistischen Bundesamtes zeigt, nutzen im Schnitt 84% aller Unternehmen Computer. Es lässt sich darüber hinaus auch ableiten: je größer ein Unternehmen, desto unerlässlicher scheint die Nutzung von Computern.

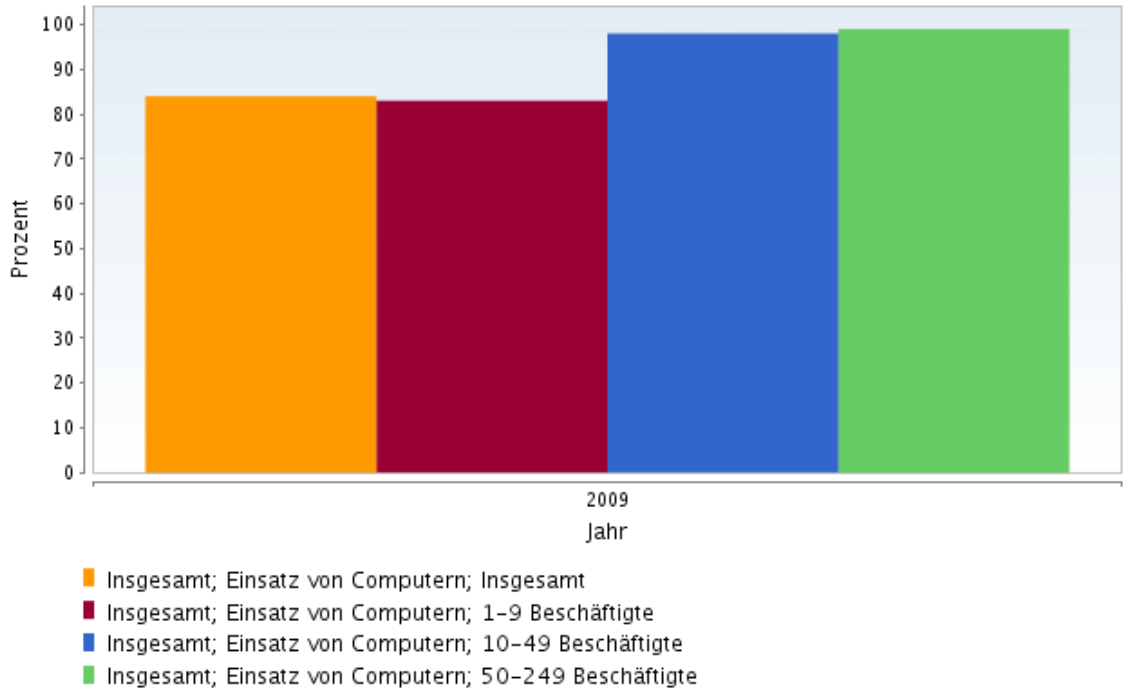

Abbildung 1: Computernutzung in Unternehmen

Quelle: Statistisches Bundesamt, Genesis - Online Datenbank

Gestaffelt nach Firmengröße ergeben sich folgende Werte für das Jahr 2009:

Beschäftigte in Unternehmen	Computereinsatz aller Unternehmen in %
1 - 9	83
10 - 49	98
50 - 249	99
250 und mehr	100
Insgesamt	84

Tabelle 1: Computernutzung in Unternehmen

Quelle: Statistisches Bundesamt, Genesis - Online Datenbank

Anfänglich als reine Datenverarbeitungssysteme ausgelegt, entwickelten sich die Informationstechnologien zu einem operativen Bereich im Unternehmen, was sowohl Chancen als auch Risiken eröffnet. Unternehmen sind heutzutage mehr denn je Abhängig von Verfügbarkeit, Zuverlässigkeit und Vertraulichkeit der eingesetzten Systeme bzw. deren Informationen.[1] Den Gefahren durch Störung der Systeme oder den Verlust von Informationen wird heute mit einem ganzheitlichen Ansatz entgegengewirkt. Durch die Einführung eines IT-Risikomanagementsystems werden wirtschaftliche Aspekte ebenso beachtet wie Sicherheitsaspekte.[2] Die Forderung nach einem Risikomanagementsystem ergibt sich aber auch aus der Tatsache der steigenden Komplexität in Unternehmen und der Abhängigkeit von Prozessen sowie der gesetzlichen Vorgabe nach einem Risikomanagement (KonTraG[3]) für bestimmte Unternehmen.

Das Ziel vorliegender Arbeit ist es, den Aufbau und die Durchführung eines IT-Risikomanagements zu beschreiben. Dabei werden Voraussetzungen erläutert, die organisatorische Struktur erklärt und die rechtlichen sowie regulatorischen Anforderungen analysiert. Anhand von „Best – Practice“ - Ansätzen wird untersucht, inwieweit diese eine Hilfestellung zur Ein- und auch Durchführung eines IT-Risikomanagements bieten. Es wird also versucht ein ganzheitliches Modell zu entwickeln, das dem geneigten Leser

[1] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2009), S. 13f
[2] Vgl. Junginger (2005), S. 179
[3] Vgl. Kapitel 3.2

einen möglichst breiten und vollständigen Überblick über Rahmenbedingungen, Komponenten, Prozesse und Methoden eines IT-Risikomanagementsystems gibt.

1.2 Abgrenzung des Themengebietes

Im Verlauf vorliegender Arbeit ergibt sich eine Vielzahl von Berührungspunkten mit anderen Wissenschaftsbereichen. Das Risikomanagement als Teil der Wirtschaftswissenschaften, im speziellen der Entscheidungstheorie und Finanzierungstheorie, bildet die Grundlage des IT-Risikomanagements. Die Untersuchung der Komponenten und Prozesse lehnt sich eng an das betriebliche Risikomanagement an und ergänzt es für die spezifischen Charakteristika des IT-Risikomanagements. Die Ausgestaltung des strategischen IT-Risikomanagementprozesses lehnt sich an die Organisation- und Unternehmensführung an. Des Weiteren werden im Verlauf der Arbeit rechtliche Aspekte betrachtet, die den Rechtswissenschaften zuzuordnen sind. Für einige Methoden des operativen IT-Risikomanagementprozesses werden mathematische Verfahren benutzt, die der Finanzierungslehre entnommen sind. Die Rahmenwerke, die in dieser Arbeit untersucht werden, stammen aus der Informationstechnik.

Durch die Vielzahl an Verflechtungen mit anderen Wissenschaftsbereichen ist es durch den begrenzten Umfang dieser Arbeit nicht möglich, sämtliche Inhalte mit der nötigen Intensität zu untersuchen.

1.3 Aufbau der Arbeit

Die Arbeit gliedert sich in acht Kapitel. Nach dem einführenden Kapitel eins, folgt das Fundament der Arbeit. In Kapitel zwei werden grundlegende Begrifflichkeiten definiert und als Basis für die weitere Betrachtung analysiert. In Kapitel drei werden rechtliche Anforderungen an das Risikomanagement im Allgemeinen und für das IT-Risikomanagement im Speziellen betrachtet. Mit Hilfe des Kapitels vier wird versucht, aus bestehenden Standards und „Best-Practice“ – Ansätzen eine Vorgabe für den Aufbau und den Ablauf eines IT-Risikomanagements zu erhalten. Die Kapitel fünf bis sieben widmen sich in aller Ausführlichkeit dem Prozess des IT-Risikomanagements. Dort werden Methoden und Verfahren zur Identifikation, Analyse und Steuerung von Risiken vorgestellt und bewertet. Den Abschluss bildet Kapitel acht mit der Zusammenfassung der Ergebnisse und der Ableitung von Erkenntnissen daraus.

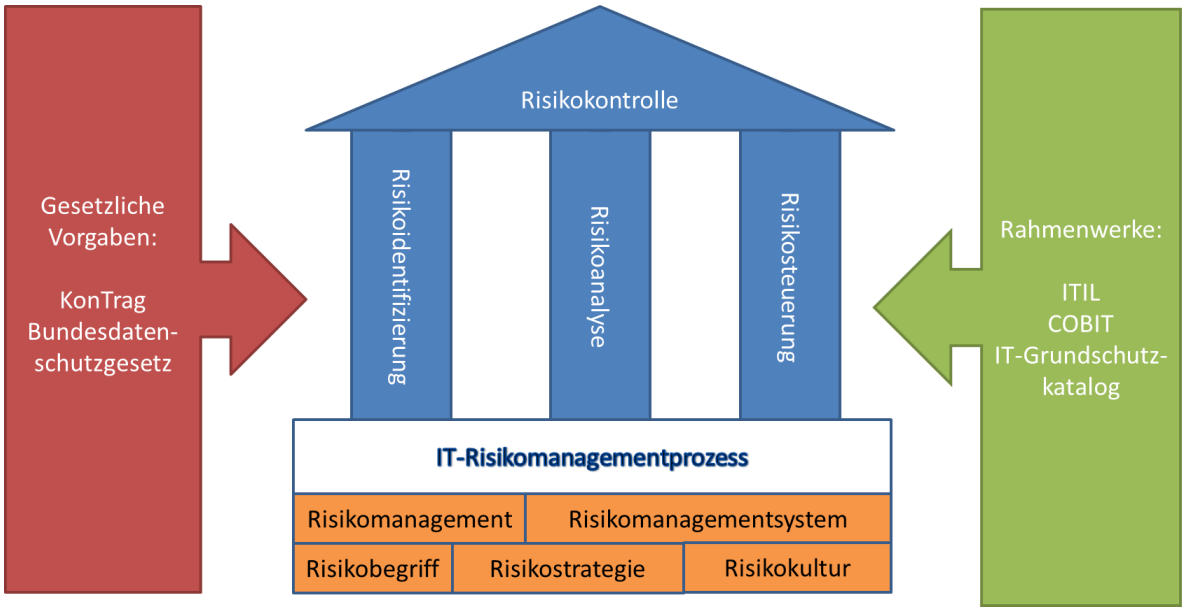

Abbildung 2: Aufbau der Arbeit

Quelle: eigene Darstellung

2 Grundlagen

2.1 Überblick

Im folgenden Kapitel werden die Grundlagen erläutert und wichtige Begriffe definiert. Es wird aufgezeigt, dass für ein IT-Risikomanagement eine Risikostrategie benötigt wird. Diese Strategie etabliert die Ausrichtung des Unternehmens bezüglich der Wahrnehmung und Behandlung von Risiken. Desgleichen wird beschrieben, dass eine Risikokultur notwendig ist, um ein Risikobewusstsein im Unternehmen zu schaffen. Die Aspekte der Kommunikation werden dabei ebenso berücksichtigt wie die Ausgestaltung der Risikoorganisation. Den Abschluss bildet der IT-Risikomanagementprozess. Dieser bildet den Auftakt für die folgenden Kapitel.

2.2 Risikobegriff

Es gibt eine Vielzahl von Definitionen für den Risikobegriff. Ursprünglich wird unter dem Wort „Risiko“ eine negative Abweichung vom erwarteten Zielzustand verstanden.[4] Sprachlich lässt sich der Begriff „Risiko“ auch auf diesen negativen Aspekt zurückführen, als er im 16. Jahrhundert in die deutsche Sprache Einzug gehalten hat. Er ist etymologisch sowohl dem italienischen Wort *„ris(i)co“* entlehnt, welches so viel wie *„Die Klippe, die es zu umschiffen gilt“* bedeutet, als auch dem griechischen *„riza“*, das sich wiederum sinnbildlich in *„Die Wurzel, über die man stolpern kann“* übersetzen lässt[5].

Vielen Risiken steht eine Chance gegenüber[6]. Ein bekanntes Beispiel sind Spekulationen am Aktienmarkt. Der Chance auf Gewinne steht dort das Risiko eines Verlustes gegenüber. Eine Chance wird allgemein als positive Abweichung einer Zielsetzung definiert.[7] Chancen und deren Realisierungsmöglichkeiten werden im Rahmen dieser Arbeit nicht näher betrachtet.

Neben dieser einfachen Begriffsbestimmung gibt es noch eine Vielzahl weiterer Definitionen für den Risikobegriff. Im Folgenden werden einige Beispieldefinitionen genannt, ohne dass diese Aufzählung den Anspruch auf Vollständigkeit erhebt.

[4] Vgl. Müller-Reichhart (1994), S. 9ff.; Brink; Romeike (2005), S. 58; Wagner (2000), S. 7f
[5] Vgl. Duden, Herkunftswörterbuch (2006), o.S.
[6] Vgl. Königs (2006), S. 10
[7] Vgl. Fiege (2006), S. 43f

***Entscheidungstheoretischer Risikobegriff*:**

„In der Entscheidungstheorie wird der Begriff des Risikos in Zusammenhang mit Risikosituationen gebraucht. Risikosituationen sind dadurch gekennzeichnet, dass der Entscheider den vorliegenden möglichen Umweltzustanden subjektive oder objektive Eintrittswahrscheinlichkeiten zuordnen kann bzw. diese vorliegen.“[8]

***Informationsorientierter Risikobegriff*:**

„*Der informationsorientierte Ansatz definiert das Risiko nicht als Gefahr, sondern als eine spezifische, sich durch Unsicherheit auszeichnende, Informationsstruktur, welche den Entscheidungen zugrunde liegt.*“[9]

***Alter betriebswirtschaftlicher Risikobegriff*:**

„*Das von der frühen BWL vertretene extensive Verständnis sah das Risiko als Begleiterscheinung jeder wirtschaftlichen Tätigkeit, die sich als Misserfolg in Form eines Kapital- oder Vermögensverlustes oder auch entgangenen Gewinns ausdrückt. Charakteristisch für diese Phase ist die Auffassung vom Risiko als eine schicksalhafte Erfolgsbedrohung, so dass die Risikoursachen oder Beeinflussungsmöglichkeiten seitens der Unternehmer gar nicht thematisiert wurden.*“[10]

Ausfallorientierter Risikobegriff:

Beim ausfallorientierten Risikobegriff wird „Risiko“ als Gefahr einer negativen Abweichung des tatsächlich realisierten Ergebnisses vom geplanten bzw. erwarteten Ergebniswert verstanden.[11] Bei dieser Definition steht dem Risiko die Chance als positive Abweichung vom Erwartungswert gegenüber. Die Chance bleibt aber bei der ausfallorientierten Risikomessung unberücksichtigt. Die bekannteste Kennzahl beim ausfallorientierten Risikobegriff ist der „Value-at-Risk“. Der „Value-at-Risk“ definiert den maximal geschätzten Wertverlust einer Einzelposition oder eines Portfolios, der unter üblichen

[8] Vgl. Wack (2007), S 22
[9] Vgl. Filipiuk (2008), S. 13
[10] Vgl. ebd., S. 12
[11] Vgl. Eisele (2004), S. 12

Marktbedingungen innerhalb eines abgegrenzten Zeitraums mit einer festgelegten Wahrscheinlichkeit nicht überschritten wird.[12]

Bei IT-Risiken handelt es sich ausschließlich um Verlustereignisse; das heißt, das Risiko wird als negative Abweichung vom Erwartungswert aufgefasst. Daher findet in dieser Arbeit ausschließlich die Definition des „ausfallorientiertes Risikos“ Anwendung.

2.3 Risikokategorien und IT-Risiken

Unternehmen können sich mit einer mit Vielzahl unterschiedlicher Arten von Risiken konfrontiert sehen. Diese Risiken kann man in zwei Kategorien unterteilen: in Finanzrisiken und operationelle Risiken.

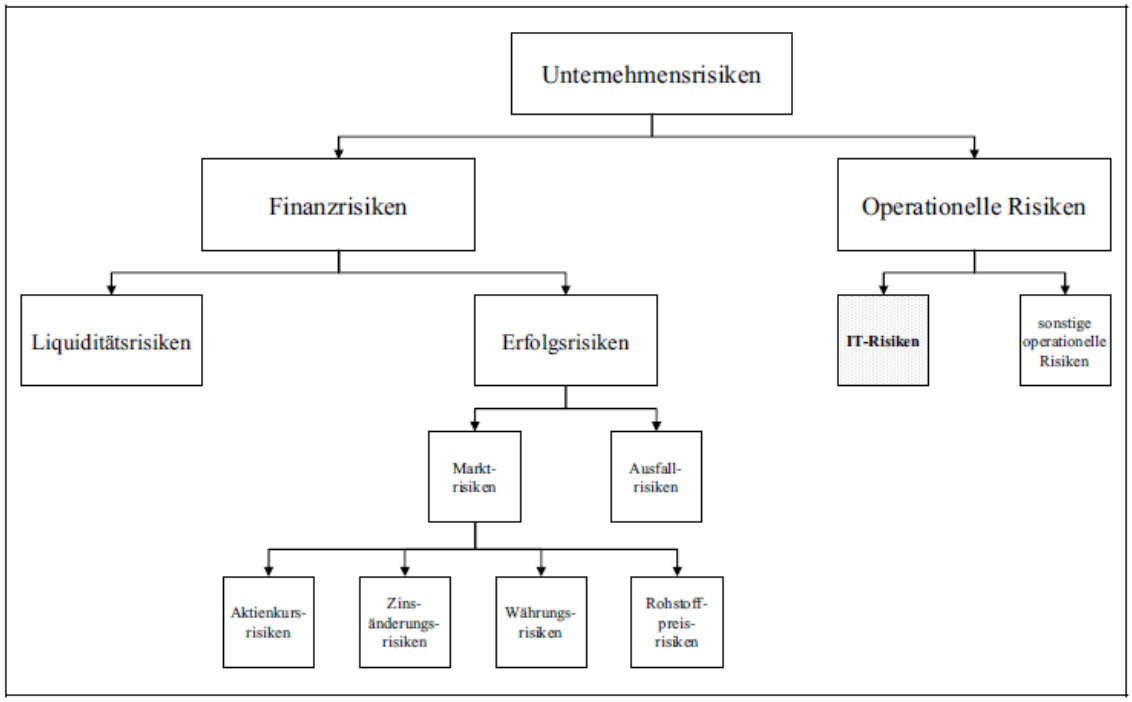

Abbildung 3: Risikokategorien

Quelle: Prokein (2008), S.10

Mit dem Begriff „Operationelle Risiken“ bezeichnet man alle betrieblichen Risiken. Dabei kann die Definition direkt oder indirekt erfolgen.[13] Sämtliche Risiken, die nicht

[12] Vgl. Schierenbeck (2001), S. 17
[13] Vgl. Prokein (2008), S.10

den Markt- oder Kreditrisiken zugeordnet sind, werden als operationelle Risiken aufgefasst. Die direkte Definition erfolgt am Beispiel der Definition des *Basler Ausschusses für Bankenaufsicht*; demnach bezeichnen operationelle Risiken *„ […] die Gefahr von Verlusten, die infolge einer Unzulänglichkeit oder des Versagens von internen Verfahren, Menschen oder Systemen oder infolge externer Ereignisse eintreten. Diese Definition schließt Rechtsrisiken ein, nicht jedoch strategische Risiken.“*[14]

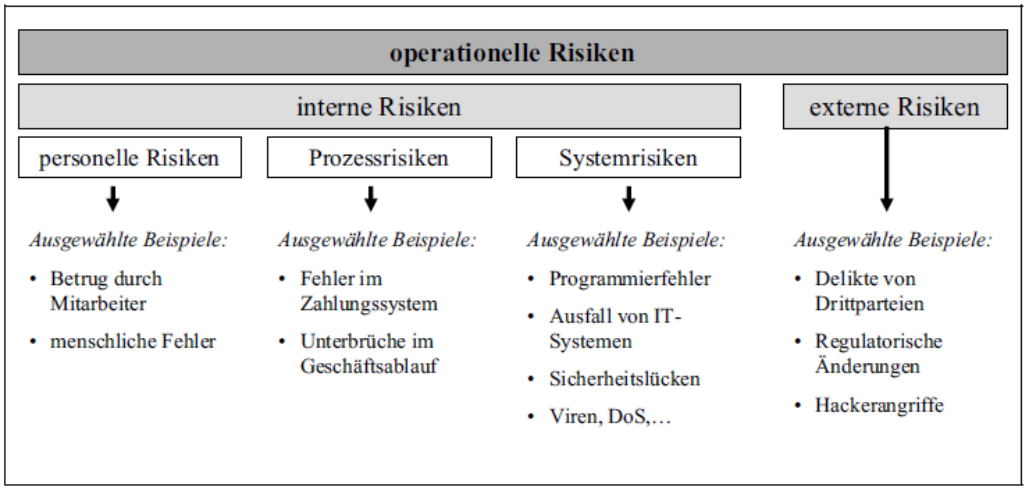

Abbildung 4: Kategorisierung operationeller Risiken nach ihren Ursachen

Quelle: Prokein (2008), S.10

Aus der direkten Definition der operationellen Risiken und aus Abbildung 4 geht hervor, dass Risiken wie „Ausfall von IT-System“ sowie „Hackerangriffe“ den operationellen Risiken zuzuordnen sind. IT-Risiken stellen daher eine Teilmenge des operationellen Risikos dar.

Finanzrisiken, welche sich auf die Finanzströme eines Unternehmens beziehen, werden in Liquiditätsrisiken und Erfolgsrisiken unterteilt.[15] Liquiditätsrisiken bezeichnen dabei Risiken, bei denen Zahlungsverpflichtungen nicht fristgerecht nachgekommen werden kann. Erfolgsrisiken mindern den Erfolg eines Unternehmens und können sogar zu einem Verlust führen. Dieses Risiko wird auch als „Verlustrisiko“ bezeichnet.[16] Es lässt sich ebenfalls in zwei Unterkategorien einteilen: in Ausfallrisiken und Marktrisiken. Ausfallrisiken drücken die Gefahr einer Nichterfüllung von vertraglichen Verpflichtun-

[14] Vgl. Basler Ausschuss für Bankenaufsicht (2004), S. 157
[15] Vgl. Eisele (2004), S. 24
[16] Vgl. Ahrendts; Marton (2008), S. 12

gen durch einen Vertragspartner aus.[17] Der Onlinevertrieb von Produkten und die damit einhergehende Zahlungsverpflichtung des Kunden ist ein Beispiel für ein Ausfallrisiko. Gibt es dabei eine negative Abweichung vom Erwartungswert (Kunde zahlt seine Rechnung) in der Form einer verspäteten Zahlung beziehungsweise eines Zahlungsausfalls, kann diese Abweichung zu großen Problemen führen.[18] Unter Marktrisiken versteht man die Gefahr einer negativen Entwicklung des Marktumfelds, in dem das Unternehmen agiert. Diese Art von Risiken kann nochmals in vier Unterkategorien aufgeteilt werden: in Aktienkursrisiken, Zinsänderungsrisiken, Währungsrisiken und Rohstoffpreisrisiken.[19]

2.4 Risikostrategie und Risikokultur

Noch vor dem Beginn des IT-Risikomanagement-Prozesses wird vom Unternehmen zunächst die IT-Risikostrategie festgelegt. Angelehnt an die Vorgaben des betrieblichen Risikomanagements, bildet diese die Rahmenbedingungen für das weitere Vorgehen. Die Risikostrategie gibt Aufschluss über die gewünschte oder erwartete Risikoneigung des Unternehmens, die sich an den Unternehmenszielen ausrichtet. Die Sicherung und Weiterführung des Unternehmens ist dabei als primäres Ziel anzunehmen.[20] Die sich aus dieser Maxime ableitenden Ziele sind Gewinnmaximierung und Senkung von Kosten auf der einen Seite, aber auch Datenschutz und der Schutz der Reputation auf der anderen Seite.[21] In der folgenden Abbildung wurden mittelständische deutsche Firmen nach ihren Risikoneigungen befragt.

	risiko-freudig	risiko-bereit	risiko-neutral	risiko-avers	risiko-scheu
Verarb. Gew.	6,7	38,3	37,9	7,8	7,7
Bau	9,2	23,4	38,7	11,0	15,4
Handel	7,7	36,5	36,8	7,7	6,8
Dienstleistungen	7,8	34,2	34,8	7,5	13,0
Gesamt	7,8	34,0	36,5	8,2	10,8

Angaben in %, Rest o. A.

Abbildung 5: Risikoneigung bei unternehmerischen Entscheidungen[22]

Quelle: Creditreform (2007), S. 24

[17] Vgl. Eisele (2004), S. 26
[18] Vgl. Raab, Siegl (2007), S. 35
[19] Vgl. Eisele (2004), S. 27
[20] Vgl. Krcmar (2005), S. 444 f
[21] Vgl. Romeike, Finke (2003), S. 151
[22] Die Kategorien der Risikoneigung werden in der Zeitschrift nicht näher erläutert.

In der Literatur[23] finden sich typischerweise drei Ausprägungen der Risikoneigung. Dazu ein Beispiel: Eine Person kann an einer Lotterie teilnehmen und muss für die Teilnahme 10€ bezahlen. Mit einer Wahrscheinlichkeit von 50% erhält diese Person eine Auszahlung von 0 €. Demgegenüber steht eine mögliche Auszahlung von 50€ mit einer Wahrscheinlichkeit von ebenfalls 50%. Risikofreudige Personen wählen die Chance auf 50€, obwohl das Risiko des Verlustes ebenso groß ist. Eine risikoneutrale Person ist indifferent bezüglich einer Entscheidung, bei der Lotterie mitzuspielen. Risikoaverse Personen hingegen werden die Teilnahme an der Lotterie vermeiden.

Aus obiger Abbildung ist zu entnehmen, dass ein Großteil der befragten Unternehmen eine risikoneutrale bis risikobereite Einstellung vertreten. Diese Einstellung wird vom Management des Unternehmens festgelegt und regelt, wie und in welchem Verhältnis sich das Unternehmen bezüglich Chancen und Risiken verhält.[24] Dabei wird außerdem die maximale Schadenshöhe bzw. die maximale Verlustgrenze für einzelne Unternehmensteile oder das gesamte Unternehmen festgelegt.

Bei der Etablierung, Ausrichtung und Kommunikation der Risikostrategie ist es unerlässlich, im Unternehmen eine Risikokultur zu schaffen. Letztlich sind die Mitarbeiter für den Erfolg eines Unternehmens ausschlaggebend.[25] In der Risikokultur geht es um die Schaffung einer Atmosphäre, bei der Sorgen, Probleme und Ängste offen ausgesprochen werden können. Nur durch diesen Umstand ist es möglich Risiken, die das Unternehmen gefährden können, einzugrenzen und entsprechend zu handeln. Risikostrategie und Risikokultur sind dabei keinesfalls fixiert und sollten fortwährend angepasst werden.[26]

2.5 Risikomanagement

Der Begriff Risikomanagement stammt aus dem amerikanischen Sprachraum und ist in den 50er Jahren bekannt geworden.[27] Dieses frühe Risikomanagement beschäftigte sich mit der Frage, wie man Versicherungen möglichst kostengünstig abschließen oder wie man auf Versicherungen gänzlich verzichten kann. Jedoch wurden in diesem frühen Risikomanagement ausschließlich Verluste betrachtet, die extern verursacht wurden. Dies führte dazu, dass Risiken, wie etwa Brände oder Diebstahl, berücksichtigt wurden,

[23] Vgl. Holler (2008), S. 36ff; Vgl. Laux (2003), S. 2116ff
[24] Vgl. Rosenkranz; Missler-Behr (2005), S. 41
[25] Vgl. Ahrendts; Marton (2008), S. 17
[26] Vgl. Rosenkranz; Missler-Behr (2005), S. 41
[27] Vgl. Fiege (2006), S. 51f

aber Risiken, die durch Entscheidungen des Managements entstanden, unberücksichtigt blieben. Mit der Zeit entwickelte sich das Risikomanagement weiter und es wurden neue Unternehmensbereiche abgedeckt.[28] Auch wurden durch Weiterentwicklung entscheidungsabhängige Risiken in die Entwicklung eingebracht, so dass heute ein ganzheitlicher Ansatz des Risikomanagements ermöglicht wird.

Das Risikomanagement ist eine Funktion der Unternehmensführung.[29] Aufgabe des Risikomanagements ist die systematische Identifikation, Analyse, Steuerung und Überwachung von Risiken, die den Fortbestand des Unternehmens bedrohen. Um Risiken mithilfe eines Risikomanagementsystems zu erkennen und daraufhin Maßnahmen zur Reduzierung dieser Risiken einzuleiten, wird ein Prozess benötigt. Dieser Risikomanagementprozess ist mitarbeitergetrieben und muss durch das Management unterstützt und getragen werden.[30] Das Ziel des Prozesses ist es, den Fortbestand des Unternehmens zu sichern.

2.6 Risikomanagementsystem

Unter einem Risikomanagementsystem versteht man *„…aufbau- und ablauforganisatorische Regelungen hinsichtlich der Behandlung von Risiken, sowie als eine eindeutige Verantwortungszuweisungsstruktur…*“.[31] Die Ausgestaltung des Risikomanagementsystems ist dabei von Größe, Struktur und Komplexität des Unternehmens abhängig.[32] Um das IT-Risikomanagement in ein bestehendes Unternehmen einzugliedern, sind eine Zuweisung der Verantwortungen und die Definition von Rollen notwendig. Rollen sind dabei fest definierte Verantwortlichkeitsbereiche, die in der Firmenhierarchie verankert sind. Einer Person können dabei mehrere Verantwortungsbereiche und damit verschiedene Rollen zugeordnet werden.[33]

Gibt es mehr als einen IT- Bereich im Unternehmen, stellt sich außerdem die Frage, inwieweit das IT-Risikomanagement eingliedert werden soll. Unterschieden werden dabei das zentrale IT-Risikomanagement und das dezentrale IT-Risikomanagement. Beim zentralen IT-Risikomanagement werden sämtliche IT-Bereiche durch eine Orga-

[28] Vgl. Exner-Merkelt (2008), o.S.
[29] Vgl. Filipiuk (2009), S. 16f
[30] Vgl. Wildemann (2006), S. 28 f
[31] Vgl. Filipiuk (2008), S. 65f
[32] Vgl. Burger; Buchhart (2002), S. 261
[33] Vgl. Seibold (2005), S. 136

nisationseinheit betreut. Diese Form der Institutionalisierung wird *Separation* genannt.[34] Dabei wird eine zentrale Stelle geschaffen, die die Aufgaben des IT-Risikomanagements wahrnimmt. Vorteilhaft bei dieser Form der Institutionalisierung ist eine Konzentration von Wissen über Risiken und Methoden innerhalb der Stabsstelle. Dadurch ist eine höchstmögliche objektive Bewertung der Risiken gewährleistet. Die Nachteile dieser Methode sind jedoch der fehlende operative Bezug und die fehlende Prozesskenntnis.[35]

Das Gegenteil dazu ist die Integration des IT-Risikomanagements in bestehende IT-Bereiche. Dabei werden Aufgaben des IT-Risikomanagements direkt den Entscheidungsträgern zugewiesen. Der Vorteil bei dieser direkten Ansiedlung im IT-Bereich ist die hohe Fachkenntnis hinsichtlich der möglichen Risiken und die enge Verknüpfung im operativen Bereich. Weniger Vorteilhaft ist die isolierte Betrachtung der Risiken, die diesen IT-Bereich betreffen. Dadurch können Wechselwirkungen von Risiken unberücksichtigt bleiben und somit ein umfassendes IT-Risikomanagement verhindert werden.

Die Kombination aus beiden Konzepten hat sich in der betrieblichen Praxis durchgesetzt.[36] Durch Zuweisung der Risikoverantwortung auf operative Entscheidungsträger, die Risiken identifizieren und vorgegebene Maßnahmen umsetzen, wird dem Aspekt der Integration Rechnung getragen. Zentral verwaltet werden hingegen die Risikobewertung und die Überwachung dieser Risiken. Auch die Festlegung der Maßnahmen und dadurch der Steuerung dieser Risiken wird in der Stabsstelle durchgeführt. Durch diese Verteilung der Aufgaben ist ein ganzheitlicher Ansatz des IT-Risikomanagements gegeben. Sämtliche Mitarbeiter sind in diesen Prozess eingebunden. Dies führt zur Erhöhung des Risikobewusstseins und damit zur Verbesserung des IT-Risikomanagementprozesses.[37]

Für die einzelnen Rollen schlägt Seibold folgende Aufteilung vor:

[34] Vgl. Wolke (2008), S. 241
[35] Vgl. Junginger (2005), S. 207
[36] Vgl. Wolke (2008), S. 242
[37] Vgl. Junginger (2005), S. 207

Rolle	Beschreibung
IT-Risikomanager	Der IT-Risikomanager ist verantwortlich für die Durchführung des IT-Risikomanagements. Er führt Maßnahmen zur Identifizierung und Bewertung von Risiken und Risikoreduzierungsmaßnahmen durch, wobei er auf die jeweiligen Experten zugreifen kann. Der IT-Risikomanager überwacht die entscheidenden Maßnahmen. Er fungiert als Stabsstelle für den oder die Entscheider.
IT-Risikoentscheider	Der Risikoentscheider verantwortet, ob als Einzelperson oder als Gremium, letztlich die vorhandene Risikosituation. Er entscheidet über die präferierte Vorgehensweise, die in der IT-Risk-Policy dokumentiert wird. Der Risikoentscheider legt die IT-Risikostrategie fest. Er entscheidet über IT-Reduzierungsmaßnahmen, deren Kosten und über die verbleibenden und zu akzeptierenden Restrisiken.
IT-Risikoverantwortliche	IT-Risikoverantwortliche sind grundsätzlich Mitarbeiter, die für *die* Aufgaben verantwortlich sind, die Risiken beinhalten. In der Regel sind dies alle Mitarbeiter. Ihre Verantwortlichkeit wird über die Risikokultur kommuniziert und gelebt. Als Ansprechpartner in einzelnen Themengebieten können ausgewiesene IT-Verantwortliche benannt werden. Sofern keine gesonderte Nennung erfolgt, sind die jeweiligen Führungskräfte für die in ihrem Aufgabengebiet vorherrschenden IT-Risiken verantwortlich. IT-Risikoverantwortliche haben regelmäßig zu prüfen, ob die Risiken in dem angenommenen Maße noch vorhanden bzw. ob weitere Risiken hinzugekommen sind. Ferner setzen sie die Reduzierungsmaßnahmen um. Bei Eintritt eines Risikos veranlassen sie Schadensreduzierungsmaßnahmen.
IT-Risikoträger	IT-Risikoträger sind Personen, die bei einem schlagend gewordenen Risiko den Schaden tragen oder mit zu tragen haben. Dies können Mitarbeiter im Fachbereich oder innerhalb des IT-Bereichs sein.

Tabelle 2: Rollen des IT-Risikomanagements

Quelle: Seibold (2005), S. 137

2.7 Prozesse des IT-Risikomanagementsystems

Für das allgemeine Risikomanagement wird in der Literatur[38] eine vierphasige Vorgehensweise vorgeschlagen.

Die einzelnen Phasen lauten:

(1) Identifikation

(2) Bewertung[39]

(3) Steuerung

(4) Kontrolle

[38] Vgl. Hechenblaikne (2006), S. 25ff; Vgl. Scherpereel (2006), S. 16ff; Vgl. Prokein (2008), S. 15ff

[39] In der Literatur wird in Bezug auf diese Phase auch oft von Risikoquantifizierung oder Risikoanalyse gesprochen.

Da diese vier Phasen weitläufig gefasst sind, werden sie auch für das IT-Risikomanagementsystem herangezogen.[40] Die folgende Abbildung verdeutlicht ihr Zusammenwirken.

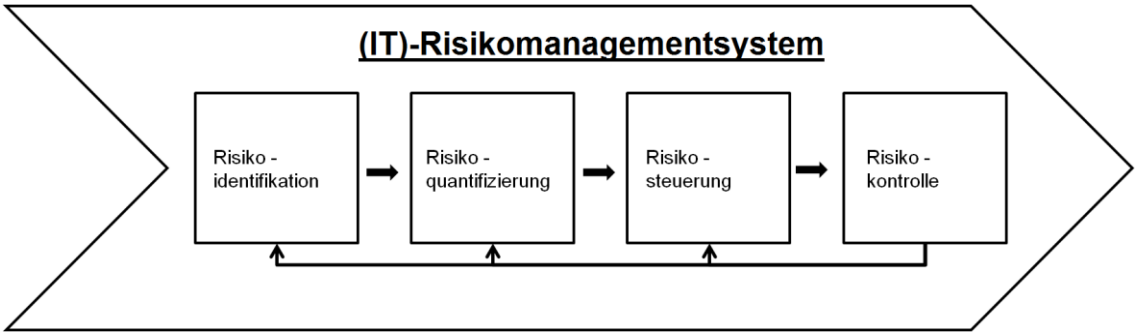

Abbildung 6: Risikomanagementsystem

Quelle: eigene Darstellung

Phase I (Risikoidentifikation):

Die erste Phase beschäftigt sich mit der Definition von IT-Risiken, der Kategorisierung von existierenden Bedrohungen sowie zukünftig eintretenden Bedrohungen. Genauer beschrieben wird diese Phase in Kapitel vier und fünf. Dort wird anhand der Standardwerke eine geeignete Abbildung der Standardrisiken für die erste Phase dargelegt. Anschließend werden in Kapitel fünf Methoden der Risikoidentifikation vorgestellt und bewertet.

Entscheidend bei der Risikoidentifikation ist die Qualität, mit der sie durchgeführt wird. Alle nicht identifizierten Risiken können, soweit sie unternehmensrelevante Bedrohungen darstellen, nicht vorhersehbare Verluste mit sich bringen. Die Wichtigkeit der Risikoidentifikation wird umso deutlicher, als dass es sich bei der ersten Phase um eine ex-ante Betrachtung handelt.

[40] Vgl. Prokein (2008), S. 16ff

Phase II (Risikobewertung):

Ziel dieser Phase ist es, identifizierte Risiken einzuschätzen, um Aussagen darüber treffen zu können, inwieweit und in welchem Maße die Risiken den Unternehmenszielen gefährlich werden können. Um die Höhe des Risikos bestimmen zu können, werden bei der Risikoquantifizierung vor allem die beiden Größen *Eintrittswahrscheinlichkeit* und *Verlusthöhe* bestimmt. Bei der Risikoquantifizierung ist ein starker Zukunftsbezug anzunehmen, da Annahmen über mögliche Eintritte bzw. über mögliche Verluste getroffen werden müssen. Eine Vorhersage aufgrund von historischen Daten gestaltet sich wegen der unvollkommenen Informationen zu beiden Größen als schwierig. Daher werden in Kapitel 5 Methoden vorgestellt, die diesem Umstand Rechnung tragen.

Phase III (Risikosteuerung):

Auf den Erkenntnissen der Risikobewertung basierend, werden in dieser Phase Entscheidungen über den Umgang mit diesen Risiken getroffen. In Kapitel 7 werden Methoden zum Umgang mit Risiken vorgestellt. Dabei wird auch die wirtschaftliche Betrachtung der Methoden nicht vernachlässigt.

Phase IV (Risikokontrolle):

Abgeschlossen wird der Prozess des IT-Risikomanagementsystems mit der Risikokontrolle. Es handelt sich hierbei um eine Betrachtung, die nach Eintritt eventueller Risiken stattfindet. So untersucht man in der Risikokontrolle, inwieweit die getroffenen Annahmen aus Phase I und II eingetreten sind. Ferner wird untersucht, ob die Methoden aus Phase III im Verhältnis zu erzieltem Nutzen aus diesen Methoden standen. Weiterhin wird hinterfragt, ob diese Methoden generell einen Einfluss auf die Eintrittswahrscheinlichkeit bzw. die Verlusthöhe hatten.

Zu den weiteren Aufgaben der Risikokontrolle gehört die Übermittlung der Ergebnisse. Dazu werden den Anspruchsgruppen[41] und dem Management im Unternehmen Bericht erstattet.

[41] Vgl. Kapitel 3.1

Zusammenfassend lässt sich festhalten, die Phasen I – III sind ex-ante Betrachtungen der Risiken. Erst in der IV. Phase wird auch das wirklich Geschehene betrachtet. Daraus folgt, dass die Einschätzungen und Steuerungen aus den ersten drei Phasen einen großen Einfluss auf den Eintritt bzw. auf die Erfassung von allen unternehmensbedrohenden Risiken darstellen.

Weiterhin festzuhalten ist, dass die einzelnen Prozesse als solche nicht nach einmaligem Durchlauf beendet sind. Vielmehr geht aus der Abbildung 6 hervor, dass diese Prozesse kontinuierlich durchlaufen werden. Dies ist wichtig, um optimal auf neue Bedrohungen zu reagieren.

3 Rechtliche und regulatorische Anforderungen

3.1 Anspruchsgruppen (Stakeholder) im IT-Risikomanagement

In der Definition des „ausfallorientierten Risikos“ wird das Risiko als eine negative Abweichung vom Erwartungswert multipliziert mit einer bestimmten Wahrscheinlichkeit definiert. Dieser Erwartungswert respektive dieses Ziel werden wiederum von verschiedenen Anspruchsgruppen definiert. Eine Folge davon ist, dass sich Ziele mit einem Wechsel der Anspruchsgruppen verändern können und damit auch das Risiko an sich. Dieser Zusammenhang wird in der folgenden Grafik dargestellt.

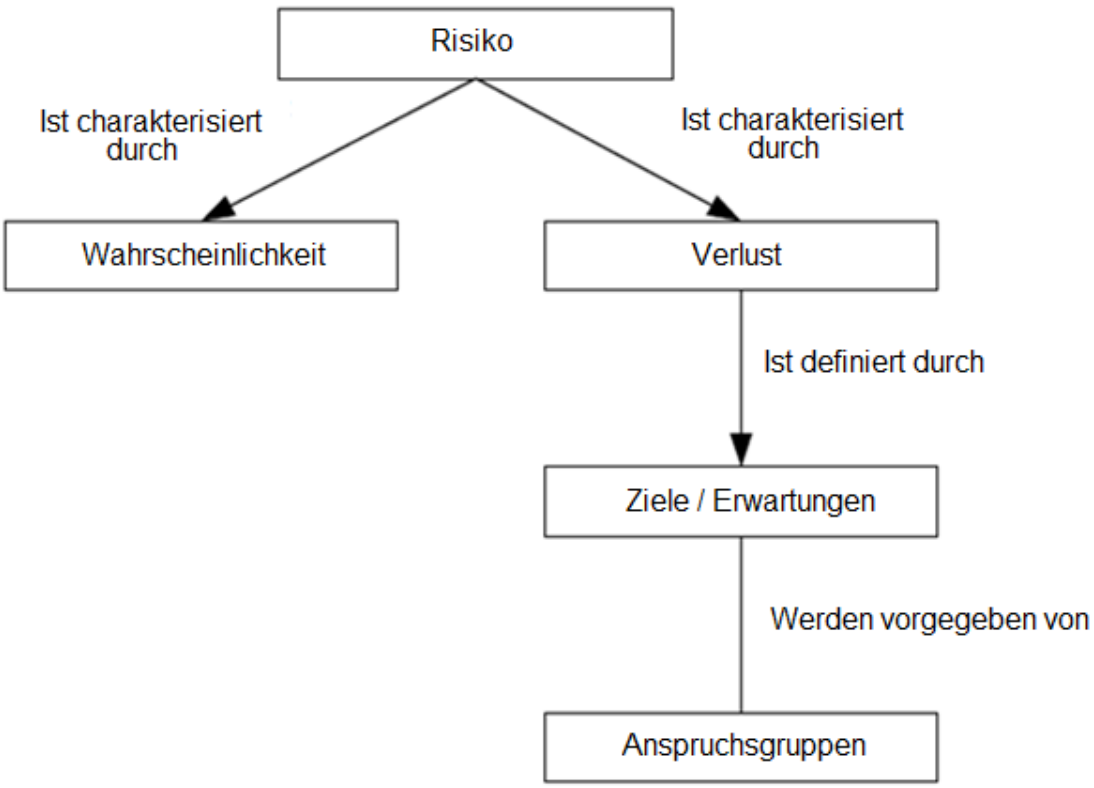

Abbildung 7: Erweiterte Risikodefinition

Quelle: in Anlehnung an Kontio (2000), S.7

Risiken für ein Unternehmen lassen sich nur genau *dann* als zufriedenstellend identifizieren, wenn die Ziele und Erwartungen bekannt sind.

Eine mögliche Methode, um die Ziele der verschiedenen Anspruchsträger zu identifizieren, ist die „Anspruchsgruppen-Ziel Prioritätstabelle“[42].

	Anspruchsgruppe A Priorität: 1	**Anspruchsgruppe B Priorität: 1**	**...**	**Anspruchsgruppe X Priorität: 2**
Ziel 1	1	4	...	4
Ziel 2	3	1	...	1
...	...	...	...	...
Ziel n			...	

Tabelle 3: „Anspruchsgruppe-Ziel Prioritätstabelle“

Quelle: in Anlehnung an Kontio (2000), S.21

So könnte man zum Beispiel für Ziel 1 annehmen, dass es die Minimierung der Kosten darstellt. Ziel 2 würde indes die Gewinnmaximierung beinhalten. Anspruchsgruppe A soll den Kunden darstellen und Anspruchsgruppe B den Projektmanager. In diesem Beispiel würde der Kunde also seine Priorität auf die Kostenminimierung legen und ist nicht an der Gewinnmaximierung des Projektmanagers interessiert. Aus diesem Tabellenbeispiel lassen sich auch Konflikte ableiten. Anspruchsgruppe A und B haben die gleiche Priorität, sind aber an entgegen gesetzten Zielen interessiert.

Festzuhalten bleibt, die Anspruchsgruppe ist für die Definition eines konkreten Risikos unerlässlich und die Bedürfnisse und Ziele dieser Anspruchsgruppe müssen so genau wie möglich erfasst und umgesetzt werden.

[42] Vgl. Kontio (2000), S.19 ff

3.2 Gesetz zur Kontrolle und Transparenz von Unternehmen (KonTraG)

Am 01.05.1998 ist das *Gesetz zur Kontrolle und Transparenz von Unternehmen* (KonTraG) in Kraft getreten. Es brachte vorrangig Neuerungen für an der Börse gehandelte Aktienunternehmen. Das *KonTraG* fasst eine Vielzahl von Einzelgesetzen zusammen, so z.B. das Aktiengesetz und das Handelsgesetz.[43] Ziel des Gesetzes ist es, die Arbeit des Aufsichtsrates zu verbessern, eine erhöhte Transparenz zu ermöglichen, stärkere Kontrolle durch den Aufsichtsrat zuzulassen sowie die Qualität der Abschlussprüfung zu verbessern.

Dem § 91 im AktG wurde folgender Absatz hinzugefügt: *„Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden."* Durch diesen Absatz wird deutlich, dass der Vorstand einer Aktiengesellschaft für ein angemessenes Risikomanagement und eine angemessene interne Revision zu sorgen hat. Die konkrete Ausgestaltung dieser gesetzlichen Forderung ist abhängig von Faktoren wie Größe, Branche oder Struktur des Unternehmens. Festzuhalten bleibt, dass der Gesetzgeber in Deutschland durch Einführung dieses Gesetzes ein Risikomanagementsystem fordert, um bestehende und zukünftige Risiken frühzeitig zu identifizieren, zu analysieren, zu bewerten und zu steuern. Das *KonTraG* bildet somit die gesetzliche Grundlage zur Einführung eines Risikomanagements.

3.3 Anforderungen an die interne Revision

Die interne Revision in einem Unternehmen ist eine Institution, die sämtliche Aktivitäten und Systeme dieses Unternehmens überwacht.[44] Dabei wird diese Aufgabe von speziellen, unternehmensinternen und unbefangenen Personen durchgeführt, die zudem keiner anderen Abteilung zugeteilt sind. Dadurch, dass diese Personen nicht in den täglichen Arbeitsablauf eingebunden sind und keinerlei Berührungspunkte zu den Ergebnissen der zu überwachenden Prozesse haben, ist eine neutrale und möglichst objektive Prüfung gewährleistet.[45] Die Aufgaben der internen Revision sind dabei wie folgt zu sehen:

- Fehlerbeseitigungsfunktion
- Entscheidungsfunktion

[43] Vgl. Fiege (2006), S. 18 f
[44] Vgl. Fiege (2006), S. 83
[45] Vgl. ebd., S. 83f

- Verhaltenssteuerungsfunktion

Durch aufgedeckte Mängel oder Abweichungen ist eine Korrektur dieser Prozesse möglich. Das Aufdecken dieser Fehler ermöglicht bei ähnlichen Prozessen, Entscheidungen effizienter und fehlerfreier zu treffen. Die Existenz einer internen Revision mit ihrer Überwachungsfunktion regt Mitarbeiter an, sich konform nach den Richtlinien des Unternehmens zu verhalten.

Über das „Management Auditing“ werden sowohl die Leistungen des Managements als auch die Ablauf- und Aufbauorganisation überprüft. In diesen operativen Bereich fällt auch die Prüfung des Risikomanagementsystems. Das Ziel der Prüfung dieses Systems ist es, die Qualität und Funktionsfähigkeit der eingesetzten Maßnahmen, Methoden und Instrumente sicherzustellen. Die interne Revision kann beim Aufbau eines Risikomanagementsystems in begrenztem Maße beratend behilflich sein. Dabei muss aber sichergestellt sein, dass die Aufgaben der internen Revision trotz des zusätzlichen Ressourcenbedarfs für die Beratung gewährleistet sind. Ebenfalls muss sichergestellt sein, dass durch die Beteiligung der internen Revision in beratender Funktion kein Interessenskonflikt entsteht, der das Prüfergebnis des Risikomanagementsystems negativ beeinflusst.[46]

Fiege definiert in folgender Abbildung die Anforderungen, die an eine moderne Interne Revision gestellt werden:

[46] Vgl. Fiege (2006), S. 84

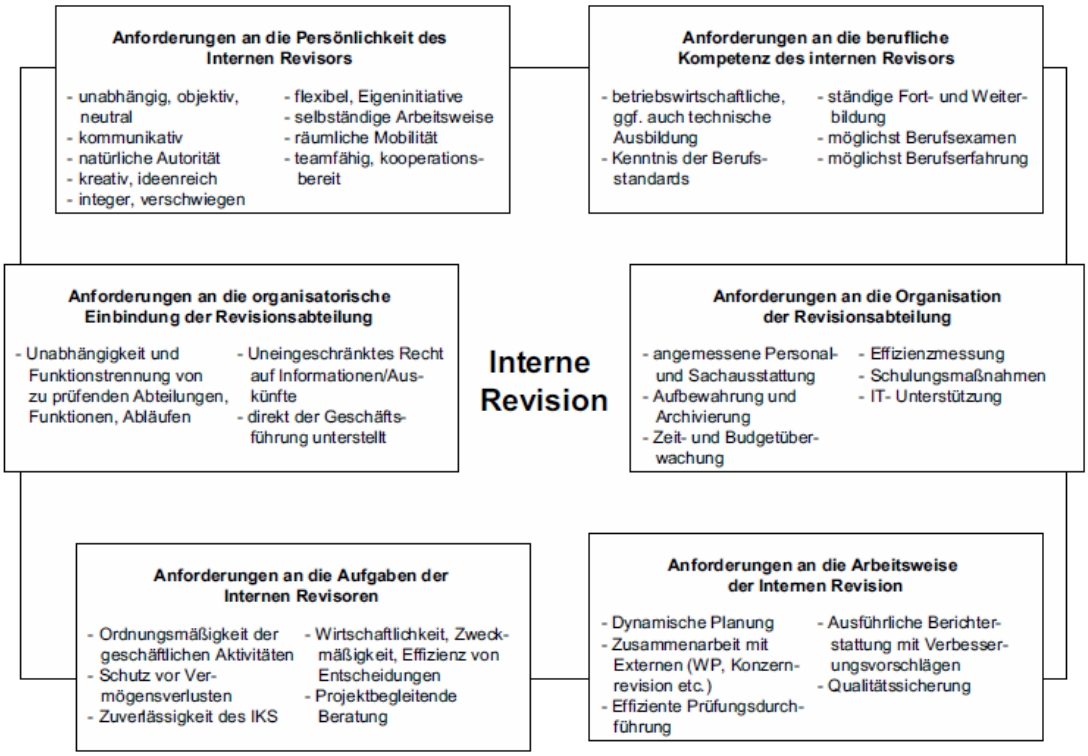

Abbildung 8: Anforderungen an eine moderne Interne Revision

Quelle: Fiege (2006), S. 86

3.4 Weitere Gesetze und regulatorische Anforderungen

National und international gibt es eine Reihe von weiteren Gesetzen und Anforderungen zum Risikomanagement. Sind Unternehmen an der US-Börse notiert oder handelt es sich um US-Unternehmen, so unterliegen diese Unternehmen dem US-Bundesgesetz „Sarbanes-Oxley Act“ (SOA). Wesentliche Gründe zur Einführung dieses Gesetzes waren zahlreiche Finanzskandale in den USA[47]. Das Gesetz wurde mit dem Ziel der Stärkung des Vertrauens der Anleger in die Unternehmen und Kapitalmärkte verabschiedet. Die Zielsetzung ähnelt daher der des *KonTraG*. - Auch beim *SOA* gibt es Anforderungen zum internen Kontrollsystem. Als Bezug nehmend auf das Risikomanagement gelten dort vor allem die *Sections 302* und *404*. Inhaltlich verpflichten sie zur Implementierung eines internen Kontrollsystems sowie sowohl zu einer schriftlichen Bestätigung

[47] Die bekanntesten Firmen waren *Enron* (ein Energiekonzern) und *Worldcom* (eine Telefongesellschaft), die jeweils mit Bilanzfälschungen Milliarden Dollar zu viel ausgewiesen haben.

der Wirksamkeit als auch der Effizienz dieser Kontrollen durch die Unternehmensleitung.[48]

Eine weitere Aufgabe des Risikomanagements ist es, die Einhaltung der insbesondere für die IT geltenden gesetzlichen Anforderungen zu kontrollieren. Hierunter fallen zum Beispiel die Regelungen der Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) und auch die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS). Eine Nichtbeachtung dieser Regelungen führt sowohl zu straf- und zivilrechtlicher als auch zu persönlicher Haftung der Unternehmensorgane (z.B. Vorstand, Geschäftsführung) und wird als grob-fahrlässig angesehen[49]

[48] Vgl. Junginger (2005), S. 118
[49] Vgl. AktG (2008), § 93; GmbHG (2008), § 43

4 Rahmenwerke, Best Practice und Standards für das IT-Risikomanagement

4.1 Überblick

Die vielfältigen Aufgaben, die durch eine schnelle Entwicklung im Bereich der Informationstechnologie immer komplexer werden, bedürfen einer Anlehnung an bestehende Standards und „Best Practice“ – Ansätze, um diesem Umstand Rechnung zu tragen. Diese Standards und Ansätze geben eine Vorgehensweise vor, damit das IT-Management für bestehende Probleme möglichst praktikable Lösungsmodelle entwickeln kann. Durch den „Best Practice“ - Ansatz ist eine Erhöhung der Effizienz beim Umsetzen dieser Modelle gegeben. Durch Zertifizierung können sich ein Unternehmen, eine Abteilung oder ein bestimmter Mitarbeiter bestätigen lassen, dass die IT-Prozesse konform zu diesem Standard umgesetzt wurden.

Die Vorteile einer solchen Anlehnung an den Standard sind wie folgt zu sehen:

- Einheitliche Terminologie im gesamten Unternehmen
- Ganzheitliche Betrachtung der verschiedenen IT-Bereiche
- Übersicht der Prozesse und Funktionen
- Durchführung von standardisierten Audits

Für die Untersuchung der Standards bzw. „Best-Practice“-Ansätze im Rahmen vorliegender Arbeit werden konkret zwei Bewertungskriterien herangezogen:

1. Inwieweit bietet der Standard eine aufbau- und ablauforientierte Vorgehensweise für den Betrieb bzw. für die Einführung eines IT-Risikomanagements?
2. Werden alle Phasen des in Kapitel 2.7 vorgestellten IT-Risikomanagementprozesses aufgegriffen und erfolgt eine auf die Praxis bezogene Empfehlung der Umsetzung?

Diese Kriterien werden herangezogen, um einen möglichen Ansatz zu finden, der die Einführung und Durchführung eines IT-Risikomanagements ermöglicht. Dazu werden im Folgenden die prozessorientierten Standards bzw. „Best-Practice“-Ansätze „CobiT“ und „ITIL“ (auf internationaler Ebene) und (auf nationaler Ebene) die „IT-Grundschutz-Kataloge“ und die „BSI – Standards“ vorgestellt und betrachtet.

4.2 BSI – Standards und IT-Grundschutz-Kataloge

Regelmäßig veröffentlicht das *Bundesamt für Sicherheit in der Informationstechnik* (BSI)[50] die IT-Grundschutzkataloge. Zusätzlich dazu wird ein eigener IT-Grundschutz Standard publiziert. Beide Veröffentlichungen werden in unregelmäßigen Abständen aktualisiert[51] und den aktuellen Bedürfnissen angepasst. Inhalt der Publikationen sind Methoden und Beschreibungen um Sicherheitsmaßnahmen für Geschäftsprozesse, Anwendungen und IT-System zu identifizieren und umzusetzen.[52]
Mit dem Ziel, ein vertretbares Maß an IT-Grundschutz für das Unternehmen zu schaffen, das dem aktuellen Stand der Technik entspricht, werden die Informations- und Kommunikationssysteme hinsichtlich so genannter Schutzziele überprüft. Schutzziele sind dabei Verfügbarkeit, Vertraulichkeit und Integrität.[53] Neben der Überprüfung der Systeme wird eine Ermittlung des Bedrohungspotentials durchgeführt.

Die Publikationen sind unterteilt in Gefährdungskataloge, IT-Grundschutz-Bausteine und Maßnahmenkataloge. Die IT-Grundschutzkataloge geben dabei Möglichkeiten vor, Sicherheitsmaßnahmen auf technischer, organisatorischer, personeller und infrastruktureller Basis mit dem Grundschutzbedarf eines Unternehmens abzugleichen. Dieses Vorgehen kann nach DIN ISO/IEC 27001 zertifiziert werden und kann damit in einen international anerkannten Standard überführt werden.[54] Ein eigenständiges IT-Risikomanagement ist in der betrachteten 11. Auflage der IT-Grundschutzkataloge nicht beschrieben. Es wird jedoch auf die Notwendigkeit eines Risikomanagements hingewiesen, das operationale Risiken abdecken soll.[55]

Die folgende Abbildung gibt einen Überblick über die vom BSI frei erhältlichen Veröffentlichungen.

[50] Siehe hierzu: www.bsi.bund.de
[51] In dieser Arbeit wird die 11.Auflage der IT-Grundschutz-Kataloge verwendet.
[52] Vgl. Bundesamt für Sicherheit in der Informationstechnik (o.J.), o.S.
[53] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2009), S. 13f
[54] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2009), S. 28
[55] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2009), S. 1938

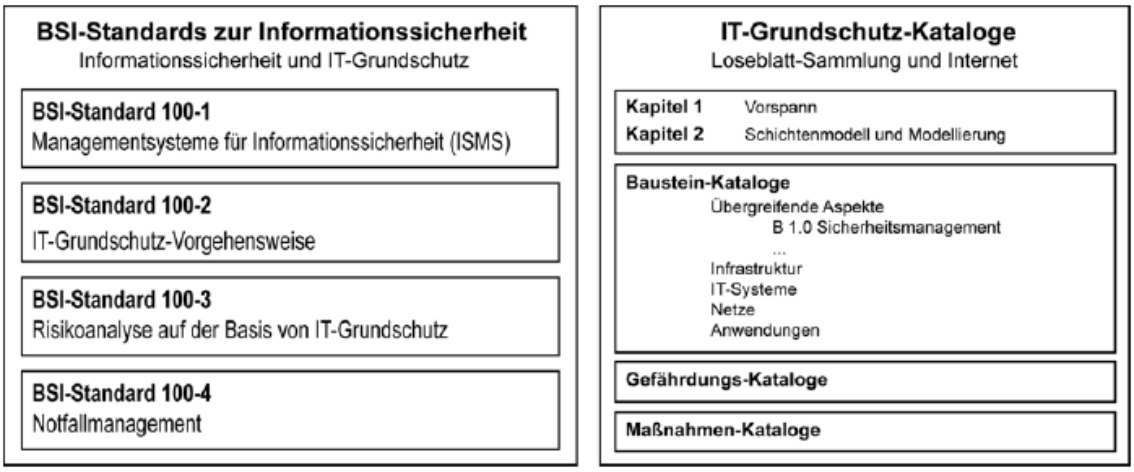

Abbildung 9: Übersicht über BSI-Publikationen zum Sicherheitsmanagement

Quelle: Bundesamt für Sicherheit in der Informationstechnik (2008-1), S. 10

Im Folgenden werden die Publikationen des BSI hinsichtlich der in Kapitel 4.1 postulierten Fragestellungen untersucht.

Der Organisationsbaustein beschreibt organisatorische Maßnahmen innerhalb der IT-Grundschutz-Kataloge und verweist darin auf die jeweiligen Gefährdungen und Maßnahmen.[56] Im Maßnahmenkatalog existiert mit der Maßnahme M2.337 eine Forderung nach einem Risikomanagement. Es wird darauf verwiesen, dass ein solches Risikomanagement in größeren Unternehmen bereits existiert und dass sich spezifische IT-Risiken mithilfe des etablierten Risikomanagements behandeln lassen.[57] Weiterhin wird auf die ergänzenden Standards des BSI verwiesen. In dem BSI Standard „IT-Grundschutz-Vorgehensweise“ wird ein möglicher Aufbau des Prozesses gestaffelt nach Firmengröße aufgezeigt.[58] Außerdem wird in der Maßnahme M3.45 „Planung von Schulungsinhalten zur Informationssicherheit“ in Modul 5 darauf hingewiesen, dass alle Mitarbeiter im Bereich des Risikomanagements geschult werden sollten.[59]

[56] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2009), S. 62
[57] Vgl. ebd., S. 1938
[58] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2008-2), S. 24ff
[59] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2009), S. 2377ff

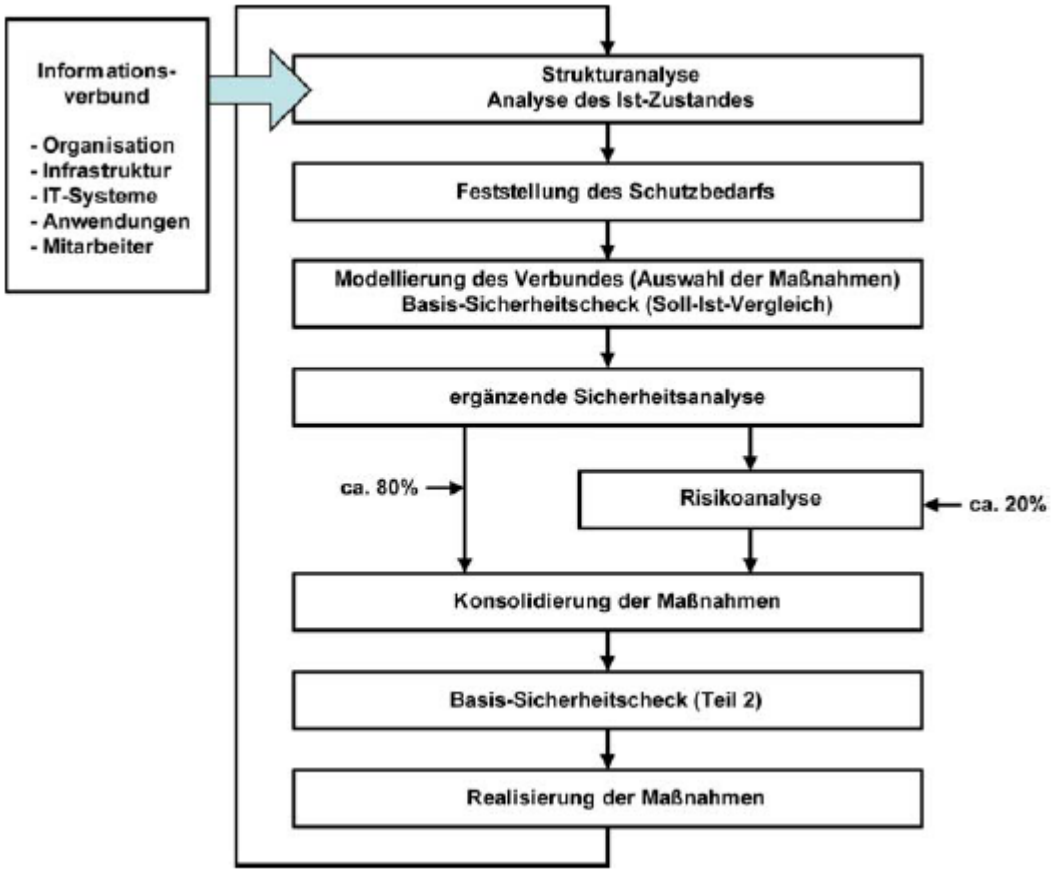

Abbildung 10: Sicherheitskonzeption nach IT-Grundschutz

Quelle: Bundesamt für Sicherheit in der Informationstechnik (2008-2), S. 36

Der Risikomanagementprozess kann anhand von Abbildung 9 teilweise verfolgt werden. Er beginnt beim BSI mit einer Strukturanalyse, bei der unter anderem entscheidende Geschäftsprozesse, organisatorische und personelle Rahmenbedingungen sowie die vorhandene Infrastruktur analysiert werden. Die Feststellung des Schutzbedarfs kategorisiert die erkannten Schwachstellen und teilt diese in Schutzbedarfskategorien ein.[60] Die Einteilung basiert dabei auf den zu erwartenden Schäden, die eine Verletzung der Schutzziele mit sich bringt. Die Behandlung der Risiken wird im BSI Standard „Risikoanalyse auf der Basis von IT-Grundschutz“[61] näher erläutert. Vorgeschlagen werden mehrere Strategien zum Umgang mit Risiken. Konkret genannt werden:

- Risikoreduktion
- Risikovermeidung
- Risikoübernahme

[60] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2008-2), S. 37f
[61] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2008-3), S. 17f

- Risikotransfer

Risiken, die zum Zeitpunkt der Betrachtung als akzeptabel eingestuft werden, später aber gefährlich werden können, werden gesondert dokumentiert. Die folgende Abbildung zeigt die Integration der Risikoanalyse in den Sicherheitsprozess.

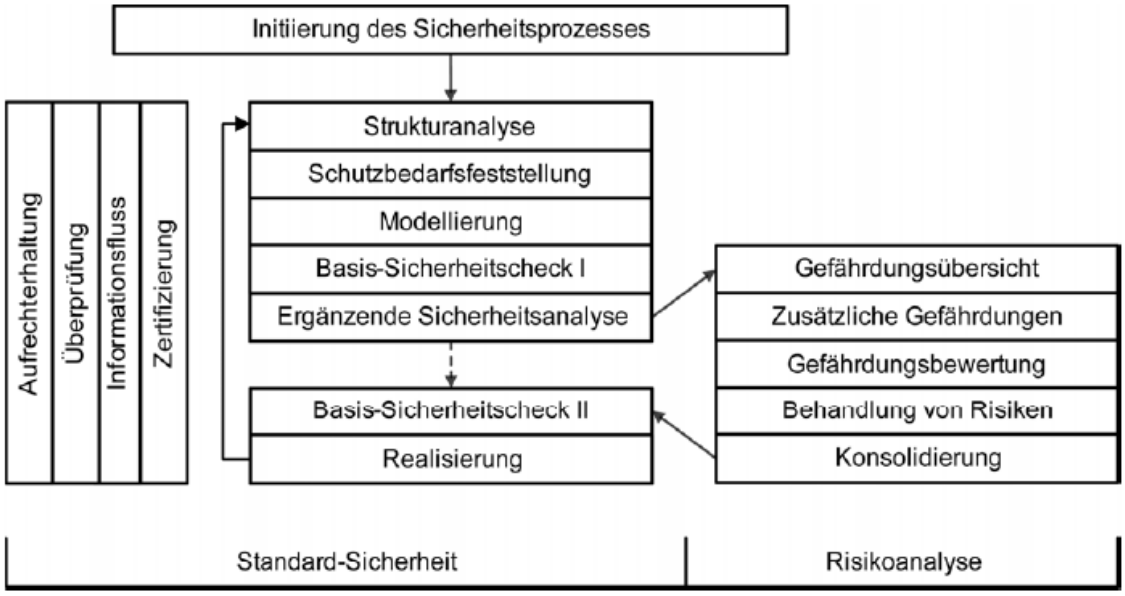

Abbildung 11: Integration der Risikoanalyse in den Sicherheitsprozess

Quelle: Bundesamt für Sicherheit in der Informationstechnik (2008-3), S. 5

Durch Überprüfung der erhaltenen Ergebnisse endet der Sicherheitsprozess. Er kann und soll jedoch auch nach Bedarf neu durchlaufen werden können.

Die IT-Grundschutz-Kataloge und die BSI – Standards bieten dem Anwender einen guten Einstieg in das Risikomanagement. Sie bilden den IT-Risikomanagementprozess vollständig ab und bieten für eine Vielzahl von Anwendungsfällen konkrete Risiken und Maßnahmen. Kritisch zu sehen ist, dass es keine aktive Komponente im Risikomanagement gibt. Die Forderung nach einer aktiven Suche nach neuen und übergeordneten Risiken wird unzureichend behandelt.

4.3 ITIL (Information Technology Infrastructure Library)

Die Information Technology Infrastructure Library (ITIL) in der Version 3 stellt ein prozessorientiertes Regelwerk[62] von „Best Practice"-Ansätzen dar, mit denen sich IT-Prozesse kontinuierlich überprüfen und optimieren lassen. Das britische „Office of Government Commerce" (OGC) veröffentlicht dieses Regelwerk. Die Orientierung folgt dem IT-Service-Management-Gedanken, der die IT als Lieferant von Dienstleistungen, welche sich an den Geschäftsprozessen orientieren, beschreibt.

ITIL besteht aus über 20 unterschiedlichen Prozessen, die einen Weg aufzeigen, um ein effektives IT-Service-Management durchführen zu können.[63] Das gesamte Werk ist in fünf Bücher (Service Strategy, Service Design, Service Transition, Service Operation und Continual Service Improvement) gegliedert, die sich mit den jeweiligen IT-Prozessen auseinandersetzen.

Die folgende Abbildung verdeutlicht die den Umfang und die Abdeckung durch ITIL:

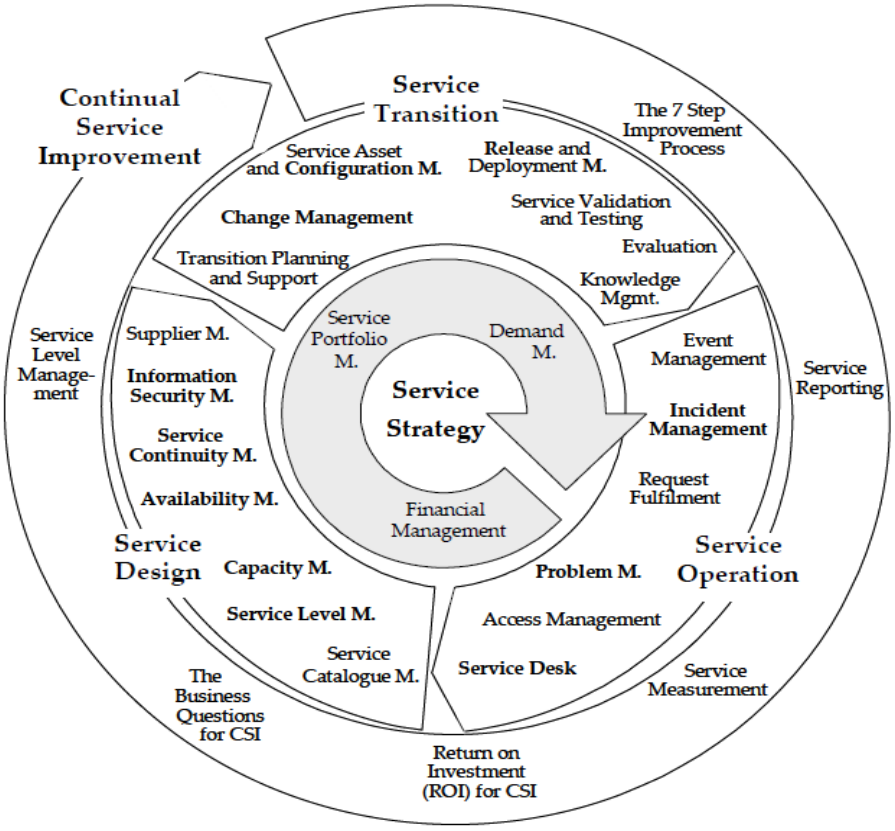

Abbildung 12: Übersicht über ITIL, die fünf Phasen samt Prozessen

Quelle: Buchsein; Victor; Günther; Machmeier, S. 54

[62] Vgl. Köhler (2005), S. 28
[63] Vgl. ebd., S. 24

ITIL stellt laut OGC den am besten akzeptierten Standard bezüglich des IT-Service-Managements dar. Zertifizierungen, nach ITIL auf der Homepage[64] des OGC, belegen diese Aussage. Als Adressaten von ITIL werden IT-Dienstleister, Berater, Anwender und das Management angeführt.[65]

Berührungspunkte zum Risikomanagement sind nicht in allen Bereichen von ITIL zu finden. Es finden sich Ansätze zum Risikomanagement in folgenden Prozessen: „IT Service Continuity Management" (ITSCM), „Information Security Management" (ISM) sowie „Availability Management" (AM).[66] Es gibt keinen Prozess bei ITIL, der sich ausschließlich dem Risikomanagement widmet. Vielmehr wird darauf verwiesen, dass ein Risikomanagement im Unternehmen implementiert sein sollte und dieses auch IT-Risiken abdecken muss.[67]

Nachfolgend soll der ITIL – Ansatz anhand der in Kapitel 4.1 vermerkten Fragestellungen untersucht werden.

Da es bei ITIL keinen eigenen Risikomanagementprozess gibt, kann es auch keine Hinweise bezüglich einer aufbau- und ablauforientierten Vorgehensweise für den Betrieb oder die Einführung eines Risikomanagements abliefern. Es setzt vielmehr ein bestehendes Risikomanagementsystem voraus und bietet somit für die organisatorische Sicht keine Hilfestellung an.

Im Buch „Service Design" wird in den Prozessen AM, ITSCM und ISM auf Risiken eingegangen, die dort behandelt werden. Die jeweiligen Prozesse beschäftigen sich mit IT-Risiken und ihren Auswirkungen. Der Fokus beim AM[68] ist die Sicherstellung der Verfügbarkeit für alle IT-Services. Die wirtschaftliche Betrachtung wird dabei ebenfalls nicht vernachlässigt. Um die Verfügbarkeit sicherzustellen, wird innerhalb des AM mit reaktiven und proaktiven Aktivitäten gearbeitet. Reaktive Aktivitäten beschäftigen sich mit dem Messen und Überwachen von IT-Komponenten, während bei den proaktiven Aktivitäten das Management der Risiken im Vordergrund steht. Um mögliche Risiken zu identifizieren, wird dabei die „Business Impact Analysis" (BIA) eingesetzt. Ziel dieser Methode ist es, Funktionen eines Geschäftsprozesses zu identifizieren, welche für den Erfolg eines Unternehmens entscheidend sind. Die Ergebnisse dieser Analyse werden dann als Input für den Bereich „Service Design" übernommen, um die Prozesse entsprechend anzupassen. Das ITSCM beschäftigt sich mit der Wiederherstellung von IT-Prozessen, nachdem ein Störfall oder ein Ausfall aufgetreten ist. Ausgangspunkt

[64] Vgl. http://www.itil-officialsite.com/ITILEISCRSQuery.asp
[65] Vgl. http://www.ogc.gov.uk/guidance_itil_4672.asp
[66] Vgl. Beims (2009), S.43
[67] Vgl. Ebel (2008), S. 70
[68] Vgl. Buchsein; Victor; Günther; Machmeier (2008), S. 66f

dieses Prozesses ist die bereits beschriebene BIA. Beim ITSCM wird allerdings die BIA unter der Annahme durchgeführt, dass der betrachtete IT-Service nicht zur Verfügung gestellt werden kann. Aus dieser Analyse und der weiteren Analyse der Risiken, die aus dem Ergebnis der BIA abgeleitet werden können, entsteht so eine Strategie, um den Prozess ITSCM zu optimieren und um Risiken darin zu minimieren. Innerhalb des Prozesses des ISM, der den effektiven Einsatz der Informationssicherheit gewährleisten soll, wird ausführlich auf die Risikosteuerung eingegangen. Diese Maßnahmen orientieren sich an der Art der Bedrohung, des Vorfalls oder des Schadens.

Zusammenfassend ist der „Best-Practice" – Ansatz ITIL in der hier betrachteten dritten Version nicht geeignet, um alle Phasen des Risikomanagementprozesses abzudecken. Er ist vielmehr eine Sammlung von Prozessen und beschreibt für die jeweiligen Prozesse spezifische IT-Risiken und Methoden, um diese zu analysieren und zu steuern. Eine übergeordnete Betrachtung der Risiken bezüglich Wechselwirkungen findet nicht statt. Es wird jedoch auf die Notwendigkeit eines im Unternehmen implementierten Risikomanagements verwiesen.

4.4 CObIT (Control Objectives for Information and Related Technology)

Der „Best Practice" – Ansatz „CObIT" beschreibt ein Prozessmodell zur Kontrolle der gesamten IT. Er wurde ursprünglich von der *ISACF* (Information Systems Audit and Control Foundation) als eine Methode der Auditierung entwickelt. Daher adressierte dieser Ansatz zunächst nur Auditoren, Endanwender und das Management. Die Entwicklung begann im Jahr 1994, 1996 wurde „CObIT" in der ersten Version veröffentlicht. Der aktuellste Stand der Entwicklung ist die Version 4.1, die in dieser Arbeit untersucht wird.

„CObIT" besteht aus Kontrollzielen und der Struktur für deren Klassifizierung. Dabei gibt es drei Ebenen für das Management der IT-Ressourcen. Die unterste Ebene ist dabei die Aktivitätsebene. Diese Aktivitäten werden benötigt, um ein vorgegebenes Ziel zu erreichen. Die nächst höhere Ebene ist die Ebene der Prozesse. Dabei werden Aktivitäten zu „natürlichen Gruppen"[69] zusammengefasst, die spezifische Kontrollen ermöglichen. Auf der obersten Ebene werden Prozesse konsolidiert und zu Domänen zusammengefasst. Diese Domänen entsprechen häufig den Organisationsanforderungen von IT-Bereichen in Unternehmen.[70]

[69] Vgl. Goltsche (2006), S. 25f
[70] Vgl. Goltsche (2006), S. 25

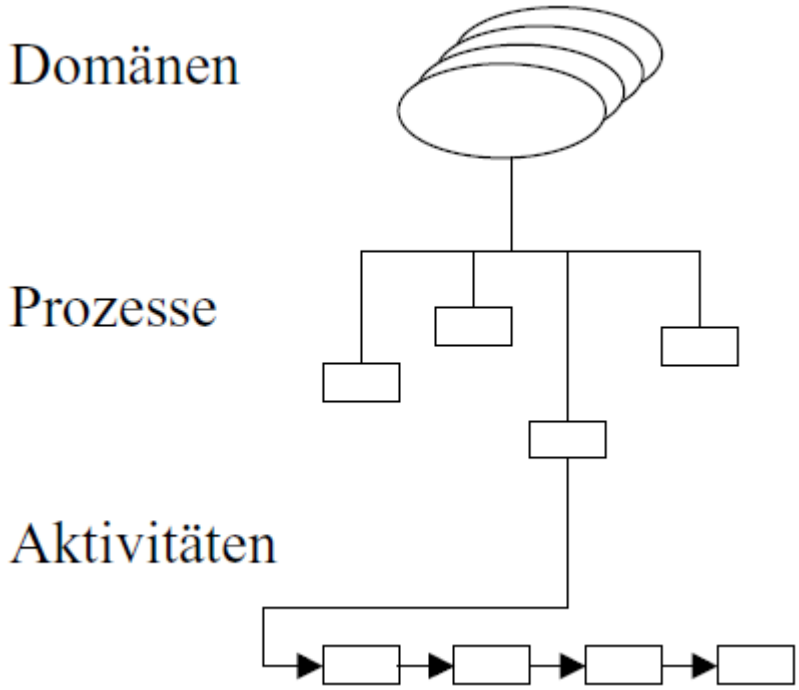

Abbildung 13: Hierarchie von „CObIT“

Quelle: Goltsche (2006), S. 25

Das „CObIT“ – Rahmenwerk erweitert diese Struktur um zwei Dimensionen, IT-Ressourcen und Geschäftsanforderungen. IT-Ressourcen sind bei „CObIT“ Menschen, Anwendungssysteme, Daten und Infrastruktur. Die Geschäftsanforderungen werden in folgende sieben Kategorien eingeteilt: Effektivität, Effizienz, Vertraulichkeit, Integrität, Verfügbarkeit, Compliance (Einhaltung rechtlicher Erfordernisse) und Zuverlässigkeit. Sie dienen als Kriterien für die Festlegung der Kontrollziele.

Stellt man diese Dimensionen grafisch dar, erhält man den sogenannten „CObIT“ – Würfel.

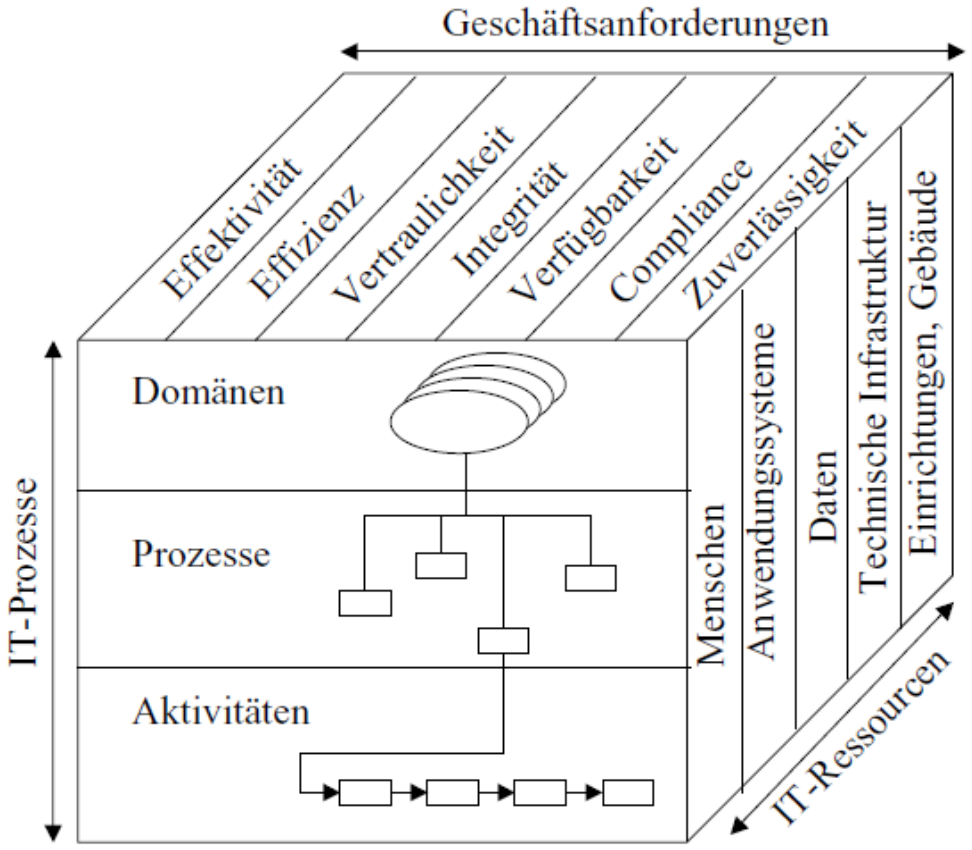

Abbildung 14: „CObIT“ - Würfel[71]

Quelle: Goltsche (2006), S. 26

Insgesamt beinhaltet „CObIT“ 34 kritische Prozesse mit 210 Aktivitäten. Diese Prozesse sind in vier Domänen eingeteilt.

Diese vier Domänen lauten:

- Planung und Organisation („Plan and organize“; PO)

  Diese Domäne beschäftigt sich primär mit der Strategie der IT. Ziel ist es herauszufinden, wie die IT am besten bei der Verwirklichung der Geschäftsziele eingesetzt werden kann. Diese Strategie muss dabei geplant, kommuniziert und durchgesetzt werden.[72] Darüber hinaus muss durch diese Phase auch eine geeignete Organisation und technische Infrastruktur bereitgestellt werden.

[71] Ab Version 4 des „CObIT“ – Rahmenwerkes werden die IT-Ressourcen „Technische Infrastruktur“ und „Einrichtungen, Gebäude“ unter „Infrastruktur“ zusammengefasst.
[72] Vgl. Goltsche (2006), S. 28f

- Beschaffen und implementieren („Acquire and implement“; AI)

  Innerhalb dieser Domäne werden Themen, wie das Identifizieren von geeigneten IT-Lösungen, Erwerb und Entwicklung dieser IT-Lösungen, aber auch Wartung und Anpassung („Change Management“) dieser Lösungen umgesetzt.[73]

- Bereitstellen und unterstützen („Deliver and support“; DS)

  Diese Domäne ist der Bereitstellung von Services gewidmet. Dabei werden Themen, wie Bereitstellung von Dienstleistungen, Sicherheit und die Durchführung von Schulungen, aufgeführt durch entsprechende Prozesse umgesetzt. [74]

- Überwachen und bewerten („Monitor and evaluate“; ME)

  Die letzte Domäne beinhaltet Kontrollprozesse, die auf die Einhaltung von zugrunde gelegten Standards und definierten Qualitätskriterien sowie den Kontrollzielen abzielen. Mit ihnen werden sämtliche Prozesse der vier Domänen gemessen.[75]

Zu jeder dieser vier Domänen gibt es definierte Prozesse, welche in folgender Abbildung ersichtlich sind:

Planung & Organisation		Delivery & Support	
PO1	Definieren eines strategischen IT-Plans	DS1	Service Level Management
PO2	Definieren der Informationsarchitektur	DS2	Lieferanten-Management
PO3	Definieren der technischen Ausrichtung	DS3	Performance und Kapazitätsmanagement
PO4	Definition der IT-Org. & ihrer Bezieh.	DS4	Continuity Management
PO5	IT-Investitionsmanagement	DS5	Sytem Security Management
PO6	Kommunizieren der Management Ziele und Strategien	DS6	Kostenmanagement
PO7	IT-Personalführungsmanagement	DS7	Anwenderschulung und Training
PO8	Managen der Qualität	DS8	Anwenderunterstützung
PO9	Risikomanagement	DS9	Konfigurationsmanagement
PO10	Projektmanagement	DS10	Problem Management
Akquisition & Implementierung		DS11	Data Management
AI1	Identifizierung automatisier Lösungen	DS12	Facility Management
AI2	Erwerb und Pflege von Applikations-SW	DS13	Operationsmanagement
AI3	Erwerb und Pflege der technischen IS	Monitoring und Evaluierung	
AI4	Befähigen des Betriebes	ME1	Überwachen und evaluieren IT Performance
AI5	Zur Verfügungstellung von IT-Ressourcen	ME2	Überwachen und evaluieren interner Kontrollen
AI6	Change Management	ME3	Sicherstellung der Einhaltung gesetzlicher Vorschriften
AI7	Installieren und Abnehmen von Systemen und Änderungen	ME4	Sorgen für IT-Governance

Abbildung 15: Prozesse der einzelnen Domänen

Quelle: Goltsche (2006), S. 28

[73] Vgl. Goltsche (2006), S. 30
[74] Vgl. ebd., S. 31
[75] Vgl. ebd., S. 33

Aus den Domänen und sonstigen „CObIT“ – Elementen lässt sich folgendes Referenzmodell erstellen:

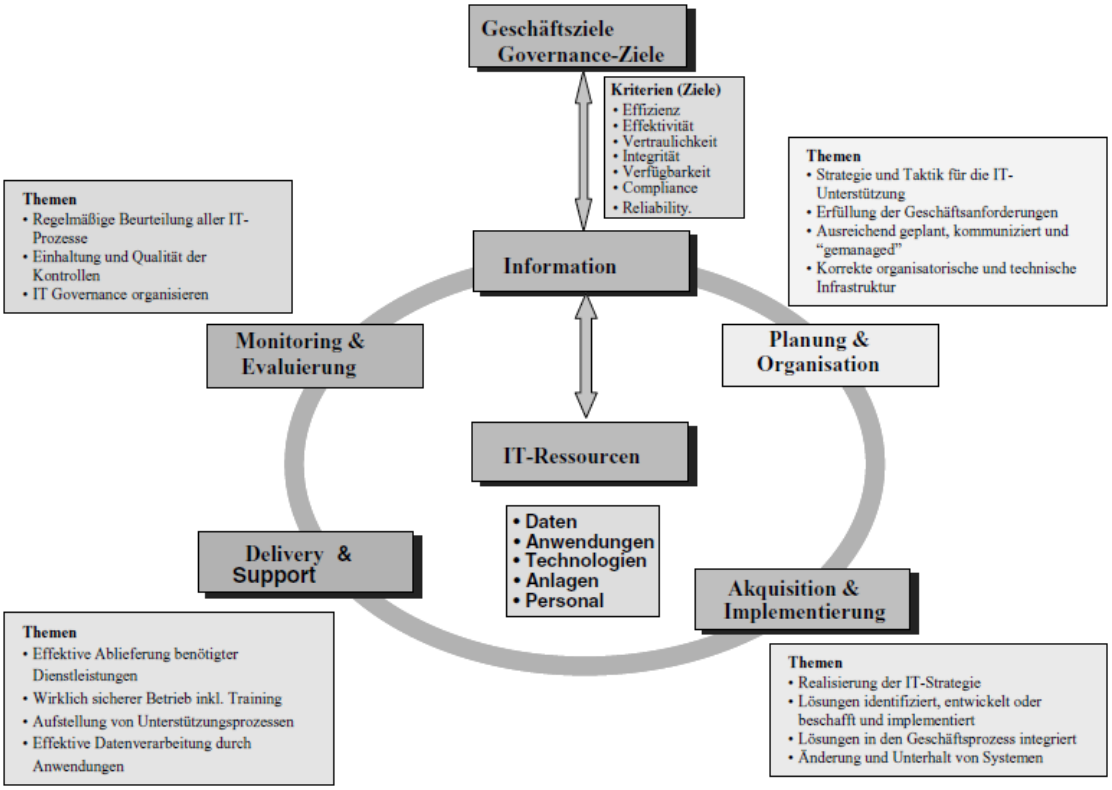

Abbildung 16: „CObIT“ - Referenzmodell

Quelle: Goltsche (2006), S. 43

Nachfolgend soll der „CObIT“ – Ansatz anhand der in Kapitel 4.1 vermerkten Fragestellungen untersucht werden.

Im Prozess PO9 der Domäne „Planung und Organisation“ wird detailliert dargestellt, wie der Aufbau und die Durchführung eines IT-Risikomanagementsystems ablaufen sollten. Dabei werden einzelne Aktivitäten bestimmten Personen oder Abteilungen der IT zugewiesen. Darüber hinaus gibt es im „CObIT“ – Rahmenwerk keine weiteren Ansätze, wie ein IT-Risikomanagementsystem einzuführen bzw. aufzubauen ist. Es gibt

jedoch zusätzlich zu „CObIT“ das „Risk IT“ – Rahmenwerk[76], welches ablauforientierte Prozesse für die einzelnen IT-Bereiche festlegt.

Sämtliche Phasen des in Kapitel 2.7 vorgestellten Risikomanagementsystems werden durch den Prozess PO9 abgedeckt. Die folgende Abbildung erläutert das Zusammenspiel der einzelnen Aktivitäten im Prozess PO9:

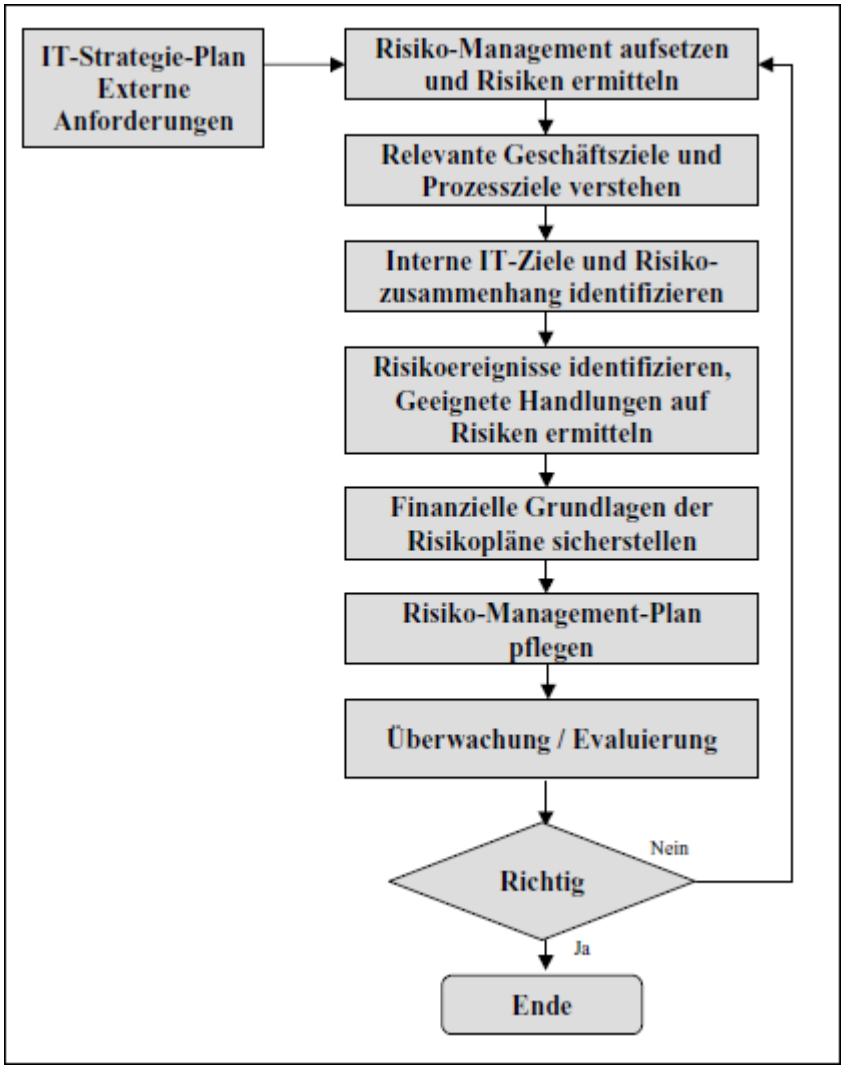

Abbildung 17: Flowchart - Risikomanagement

Quelle: Goltsche (2006), S. 77

Der Prozess der *Risikoidentifikation* findet sich in der Aktivität „Risiko-Management aufsetzen und Risiken ermitteln“ wieder. Die *Risikoanalyse* wird sowohl durch die Aktivität „Interne IT-Ziele und Risikozusammenhang identifizieren“ als auch durch die Aktivität „Risikoereignisse identifizieren“ abgedeckt. Das Steuern von Risiken (*Risikosteuerung*) wird durch die Aktivität „Geeignete Handlungen auf Risiken ermitteln“

[76] Es ist jedoch nicht Teil des hier betrachteten „CObIT“ – Rahmenwerks.

erfasst und umgesetzt. Die *Risikokontrolle* wird durch die Aktivität „Überwachung / Evaluierung“ durchgeführt.

Zusammenfassend enthält das Rahmenwerk „CObIT“ eine sehr detaillierte Vorstellung darüber, wie ein IT-Risikomanagementsystem aufzubauen ist und was es leisten muss. Einzig die fehlenden ablauforientierten Prozesse für die einzelnen Bereiche fehlen diesem Rahmenwerk. Diese sind jedoch, wie schon erwähnt, als Ergänzung zum „CObIT“ – Rahmenwerk im „Risk IT“ – Rahmenwerk enthalten.

4.5 Zusammenfassung

Alle erwähnten Ansätze enthalten Hilfestellungen bezüglich des Umgangs mit Risiken. Bezugnehmend auf die Kriterien, die in Kapitel 4.1 definiert wurden, ist die Abdeckung zur Ein- und Durchführung eines IT-Risikomanagementsystems am besten durch die „IT-Grundschutz-Kataloge“ und den dazugehörigen „BSI-Standards“ gegeben. Auch werden sämtliche Prozesse eines IT-Risikomanagementsystems erwähnt und beschrieben. Im „CObIT“ – Ansatz findet sich ebenfalls eine vollständige Abdeckung aller Prozesse des IT-Risikomanagementsystem. Diesem Ansatz fehlt jedoch eine Empfehlung zur praktischen Durchführung dieser Prozesse. „ITIL“ hingegen tangiert das Risikomanagement lediglich und fordert das Vorhandensein eines solchen Systems. Auch werden dabei die einzelnen Prozesse unzureichend angesprochen.

Ein vollständiges Vorgehensmodell zur Ein- und Durchführung eines IT-Risikomanagementsystems wird durch keinen Ansatz dargestellt. Vielmehr wird für bestimmte Teilbereiche des IT-Risikomanagementsystems aufgezeigt, wie dieses umgesetzt werden kann. Dabei beziehen sich diese Empfehlungen auf die strategische Komponente im IT-Risikomanagementsystem und bieten für die Ausgestaltung im operativen Rahmen keinerlei Hilfe an.

„CObIT“ und die „IT-Grundschutz-Kataloge“ bzw. „BSI-Standards“ als Rahmenwerke sind kostenlos zu beziehen wohingegen „ITIL“ als Rahmenwerk kostenpflichtig ist.

Die vorgestellten Ansätze sind nicht als direkte Konkurrenten anzusehen. Vielmehr ergänzen sich diese und decken gemeinsam bestimmte Themengebiete ab.[77]

[77] Vgl. Zhang (2010), S. 49ff

5 Methoden und Techniken zur Risikoidentifikation

5.1 Aufgaben und Elemente der Risikoidentifikation

Das Sprichwort *„Gefahr erkannt, Gefahr gebannt“* verdeutlicht sehr gut die Notwendigkeit, möglichst alle Risiken im IT-Bereich zu erkennen. Die Erkenntnisse der Risikoidentifikation lassen sich in einer Liste mit folgenden Informationen zusammenfassen: Kurzbeschreibung, Daten zur Risikoart und Angaben zu Ursachen des Risikos.[78]

Um nun diese Liste zu erstellen, werden in der Literatur[79] verschiedene Methoden angeboten. Diese Methoden unterscheiden sich in drei Bereiche: Analytische Methoden, Kreativitätsmethoden und Kollektionsmethoden[80]. Kollektionsmethoden sammeln risikospezifische Daten und eigenen sich daher überwiegend zur Identifikation von bekannten IT-Risiken. Diese Methoden betrachten Risiken ex-post. Kreativitäts- und Analytische Methoden haben dagegen das Potenzial auch zukünftige und unbekannte IT-Risiken aufzudecken. Kreativitätsmethoden sind gekennzeichnet durch ungewöhnliche Denkprozesse, bei Analytische Methoden hingegen versucht man, anhand der bestehenden Systeme und ihrer Eigenschaften aktiv nach Schwachstellen und unternehmensbedrohenden IT-Risiken zu suchen.

Im Folgenden werden gängige Methoden zur Identifikation von IT-Risiken dargestellt. Dabei werden exemplarisch aus allen drei Bereichen, drei Methoden näher vorgestellt und diese anhand ihrer Komplexität und Risikoabdeckung untersucht. Dieser Methoden wurden aufgrund ihrer Bedeutung in der praktischen Durchführung ausgewählt.

Analytische Methoden	Kreativitäts-methoden	Kollektions-methoden
Fehlerbaumanalyse	Brainstorming	Checkliste
Fehlermöglichkeits- und Einflussanalyse	Syntetik	Experten-befragung
Fragenkatalog	Delphi - Methode	Schadensfall - Datenbank
...	...	...

Abbildung 18: Überblick über die Methoden zur Risikoidentifikation

Quelle: eigene Darstellung

[78] Vgl. Ahrendts; Marton (2008), S. 15f
[79] Vgl. Zellmer (1990), S. 32ff
[80] Vgl. Piaz (2002), S. 75ff

5.2 Analytische Methoden

5.2.1 Fehlerbaumanalyse

Die Fehlerbaumanalyse ist eine Top-Down Methode. Dabei wird ein Ereignis vorgegeben, das nicht erwünscht ist. In Form einer Baumstruktur werden nun alle Möglichkeiten untersucht, die zu diesem primären Störereignis führen können. Es werden dabei alle sekundären Störereignisse aufgeführt. Dieser Prozess wird wiederholt und dabei werden alle sekundären Störereignisse als primäre Störereignisse aufgefasst und es erfolgt eine weitergehende Zerlegung. Aus dieser Modellierung entsteht eine grafische Abbildung der Störereignisse, die zur Top-Störung führen. Das Verfahren wird solange wiederholt, bis sich keine weitere Differenzierung bezüglich neuer Störereignisse möglich ist. Die Herausforderung bei dieser Methode besteht in der korrekten Wahl des initialen Störereignisses. Ist dieses zu allgemein gehalten, kann die Fehlerbaumanalyse schnell sehr komplex werden. Wird das Ereignis hingegen zu speziell gewählt, können wichtige Fehlerquellen übersehen werden.

Die Realisierung dieser Methode kann innerhalb der IT-Abteilung vollzogen werden. Aufgrund des in der IT-Abteilung vorhandenen Fachwissens ist die Zerlegung von IT-spezifischen Störereignissen durchführbar.

5.2.2 Fehlermöglichkeits- und Einflussanalyse (FMEA)

Die FMEA geht von einem intakten und störungsfreien System aus, um mögliche Fehler in Produkten und Prozessen schon vor ihrem Auftreten zu erkennen.[81] Entwickelt wurde diese Methode von der amerikanischen Raumfahrtbehörde „NASA“, um Fehler bei physikalischen Gütern oder Prozessen zu entdecken. Heute wird sie auch zur Identifikation von Schwachstellen und unternehmensrelevanten Bedrohungen bei IT-Systemen eingesetzt.

Zu Beginn wird das IT-System in einzelne Komponenten zerlegt, die anschließend auf mögliche Störungszustände analysiert werden. Aufgrund der Einzelaussagen wird dann ein Rückschluss über die Auswirkungen auf das Gesamtsystem vollzogen. Es handelt sich bei der FMEA also um einen „Bottom-Up-Ansatz“. Dieser wird durch Formblätter, welche zahlreiche Vorgaben zur Fehlerursache, Fehlerwirkung und bedrohtem Objekt beinhalten, unterstützt. Diese Formblätter beinhalten außer der Identifikation auch die

[81] Vgl. Prokein (2008), S.25f

Phasen der Analyse/Bewertung und Steuerung von Risiken. Für das Risikomanagement kommt dieser Methode jedoch die Hauptaufgabe der Identifikation zu.[82]

Die konkrete Formalisierung der Untersuchung und Erfassung der Ergebnisse bietet eine breite Grundlage für Detailanalysen. Diese können vor allem im Zusammenhang mit der Konzeption von speziellen, hochkritischen System genutzt werden. Jedoch eignet sich diese Methode, aufgrund ihrer hohen Komplexität und des hohen Aufwandes zur Durchführung, nicht zur breiten Identifikation aller Risiken im Unternehmen.[83] Ferner können durch die Detaillierung und dem daraus resultierenden Abstraktionsgrad für das Gesamtsystem keine Rückschlüsse über Abhängigkeiten oder Gemeinsamkeiten bezüglich anderer Systeme oder Prozesse zueinander identifiziert werden.[84]

Die Anwendung der FMEA in einer IT-Abteilung ist aufgrund der beschränkten Methodenkenntnis nicht zu realisieren. Die Durchführung sollte mit Hilfe externer Berater vollzogen oder durch das IT-Management angeordnet werden.

5.2.3 Fragenkatalog

Durch die Anwendung der Methode des Fragenkatalogs werden IT-Risiken mithilfe detaillierter Fragen, deren Antworten Hinweise auf mögliche Schwachstellen bzw. Bedrohungen geben, aufgedeckt. Das *Bundesministerium für Sicherheit in der Informationstechnologie* hat entsprechende standardisierte Fragebögen zur Identifikation von IT-Risiken ausgearbeitet.

Problematisch bei standardisierten Fragebögen ist der Fakt, dass unternehmensspezifische Faktoren unberücksichtigt bleiben. Zudem können solche Fragebögen nur entwickelt werden, wenn potentielle Angriffe bekannt sind. Daher basieren Fragebögen auf andere Methoden der Risikoidentifizierung.[85]

Die folgende Abbildung verdeutlicht den Aufbau eines solchen Fragebogens.

[82] Vgl. Piaz (2002), S. 90
[83] Vgl. Seibold (2006), S. 98
[84] Vgl. Prokein (2008), S. 26
[85] Vgl. Piaz (2002), S. 90

M 2.13	Wie werden schützenswerte Betriebsmittel entsorgt?		
	Werden Datenträger		
	- formatiert,	☐	☐
	- physikalisch gelöscht,	☐	☐
	- physikalisch zerstört,	☐	☐
	- entmagnetisiert?	☐	☐
	Wird Papier		
	- eigenhändig geschreddert,	☐	☐
	- anderen Personen zur Vernichtung übergeben (wenn ja, wem?), ...	☐	☐
	- sonstiges:	☐	☐

Abbildung 19: Auszug aus einem Fragebogen des BSI

Quelle: https://www.bsi.bund.de/cae/servlet/contentblob/474910/publicationFile/31054/04pc_f_pdf.pdf

5.2.4 Bewertung der vorgestellten Analytischen Methoden

Fragebögen, FMEA und Fehlerbaumanalysen sind geeignete Methoden zur Identifikation. Da in vielen Unternehmen eine standardisierte IT-Systemlandschaft vorzufinden ist, eignen sich besonders Fragebögen, um einen Überblick über die meist verbreiteten IT-Risiken zu erhalten. Außerdem stellen Fragebögen eine sehr kostengünstige Form der Identifizierung von Standardrisiken dar. Für die Unterstützung von hochkritischen Systemen eignet sich die FMEA. Durch die exakte Detaillierung werden bei einem solchen System möglichst viele Risiken aufgedeckt.

Zusammenfassend bleibt festzuhalten, dass eine Kombination der vorgestellten Methoden einen möglichst umfangreichen Einblick in die bestehenden Risiken gewährleistet. Die folgende Abbildung gibt eine Bewertung hinsichtlich des Aufwands, der Kosten sowie der Abdeckung des Risikospektrums und der Durchführung ab.

Methode	Aufwand / Komplexität	Kosten	Abdeckung des Risikospektrums	Durchführung
Fehlerbaumanalyse	durchschnittlich	gering	Prozess oder System	intern
FMEA	hoch	durchschnittlich	Prozess oder System	extern (intern)
Fragenkatalog	gering	gering	breite Abdeckung*	intern

* Bei Standardrisiken.

Abbildung 20: Bewertung der Analytischen Methoden

Quelle: eigene Darstellung

5.3 Kreativitätsmethoden

5.3.1 Brainstorming

Die „Brainstorming-Technik“ ist die älteste und bekannteste Technik zur Ideenfindung im Team.[86] Diese Technik wird in den unterschiedlichsten Situationen angewendet und eignet sich ebenfalls zum Identifizieren von Risiken. Die Idee beim „Brainstorming“ ist, dass die Teilnehmer dieser Technik in kurzer Zeit unterschiedliche Ideen sammeln. Dabei wird von einer direkten Bewertung der einzelnen Ideen beim Brainstorming selbst abgesehen. Auch Kritik ist in der Durchführungsphase des „Brainstormings“ verboten, um den kreativen Prozess so wenig wie möglich zu stören. Entscheidend bei der Methode des Brainstormings ist die Auswahl der Probanden wie auch des Moderators, der durch das „Brainstorming“ führt. An einem „Brainstorming“ sollten idealer Weise fünf bis sieben Probanden teilnehmen.[87] Der Prozess selbst verläuft in sogenannten Wellen[88]. Eine typische erste Welle dauert in der Regel fünf bis zehn Minuten. Danach kann es durchaus zu einer zweiten und sogar dritten Welle kommen. Die Ideen der zweiten und dritten Welle sind nicht mehr so zahlreich wie in der ersten, aber in der Regel origineller. Am Ende des Prozesses sollten die gesammelten Ideen strukturiert werden, um ein konsolidiertes Ergebnis zu erhalten. Die Durchführung dieser Methode verlangt, bis auf den beschriebenen Ablauf, keine Methodenkenntnis und kann daher Abteilungsintern durchgeführt werden. Dabei ist darauf zu achten, dass die Teilnehmer aus unterschiedli-

[86] Vgl. Arendts; Marton (2008), S.121
[87] Vgl. Prokein (2008), S.23
[88] Vgl. Arendts; Marton (2008), S.122

chen IT-Abteilungen ausgewählt werden, dabei aber keine großen Sprünge in der Hierarchie der Personen im Unternehmen vorhanden sind.[89] Dies fördert die für diese Methode unabdingbare Eigendynamik und Spontaneität.

5.3.2 Synektik

Bei der „Synektik“ handelt es sich um eine unkonventionelle Methode zur Risikoidentifizierung. Es werden scheinbar zusammenhangslose und irrelevante Elemente in den Prozess eingebracht. Die Methode der „Synektik“ versucht nun aus diesen gegebenen Elementen, durch Kombination und Reorganisation neue Muster zu entwickeln.[90] Die Teilnehmeranzahl sollte dabei sechs Personen nicht unterscheiden und diese Personen sollten von einem erfahrenen Moderator geführt werden. Der Ablauf kann in die folgenden Abschnitte unterteilt werden.[91]

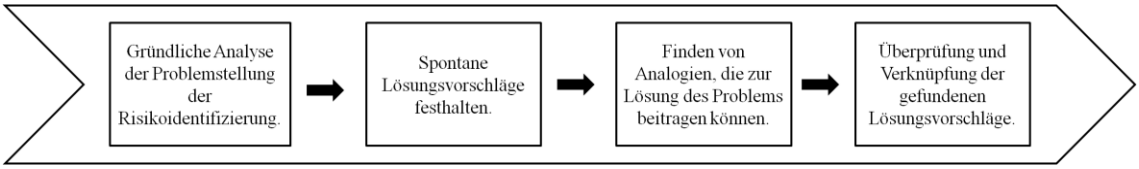

Abbildung 21: Ablauf der Synektik

Quelle: eigene Darstellung, in Anlehnung an Jung (2003), S. 340

Im ersten Schritt wird das Problem definiert und analysiert. Im Anschluss erfolgt die Eruierung von spontanen Lösungsvorschlägen. Mithilfe dieser Lösungsvorschläge werden Analogien gebildet. Diese können direkter, persönlicher oder symbolischer Art sein. Ist dieser Abschnitt abgeschlossen, werden die gefundenen Analogien auf das Problem übertragen und im letzten Schritt werden Lösungsansätze entwickelt.[92]

Die „Synektik“ ist gekennzeichnet durch einen erheblichen Zeitaufwand und durch einen hohen Anspruch an die Teilnehmer. Ebenfalls hoch ist der Anspruch an die Erfahrung des Moderators.[93] Diese Methode erlaubt es, sich unkonventionell mit der Identifizierung von IT-Risiken zu beschäftigen und kann dadurch auch auf vollkommen neue, vorher nicht beachtete Risiken schlussfolgern. Darüber hinaus eröffnet diese Methode eine Möglichkeit, die Risikoidentifizierung aus einer völlig anderen Perspektive zu betrachten.

[89] Vgl. Junginger (2005), S. 232 f
[90] Vgl. Prokein (2008), S. 24
[91] Vgl. Jung (2003), S. 340
[92] Vgl. Klempt (2007), S. 63
[93] Vgl. ebd., S. 63f

5.3.3 Delphi-Methode

Bei der „Delphi-Methode“ handelt es sich um eine Variation der Expertenbefragung[94]. Dazu existieren festgelegte Fragebögen, die die Teilnehmer beantworten müssen. Die Auswertung dieser Fragebögen erfolgt mit Hilfe von statistischen Verfahren. Ziel dieser Methode ist es, durch mehrmaliges Ausfüllen, Überdenken und Modifizieren des Fragebogens eine gemeinsame, einheitliche Tendenz abzuleiten. Die Methode ermöglicht eine indirekte Kommunikation zwischen verschiedenen IT-Abteilungen, die nicht an bestimmte Zeiten oder Orte gebunden ist, und betrachtet daher den vollständigen IT-Bereich. Im Ergebnis führt diese Methode zur Aufdeckung von IT-Risiken und unternehmensrelevanten Bedrohungen.

Die Eignung dieser Methode innerhalb der IT kann als gegeben angenommen werden. Dabei ist aber eine genügend große Anzahl von Experten der IT-Abteilungen unabdingbar. Zudem kann der Aufwand bei vielen Iterationen der Methode schnell ansteigen und zu Ermüdungseffekten bei den Probanden führen.[95]

5.3.4 Bewertung der vorgestellten Kreativitätsmethoden

Aus dem Fundus der Kreativitätsmethoden ist besonders das „Brainstorming“ hervorzuheben. Es ermöglicht eine kostengünstige und schnelle Identifikation von bestehenden Risiken. Diese Methode liefert außerdem verwertbare Informationen für andere Methoden, die auf kreatives Denken angewiesen sind.[96]

Der Aufwand bei der „Synektik“ ist aufgrund der Komplexität dieser Methode hoch. Durch den hohen Anteil an Kreativität eignet sich aber auch diese Methode im Speziellen zur Identifikation von bisher unberücksichtigten Risiken, aber weniger zu einer vollständigen Identifikation aller IT-Risiken.

Durch die Ermöglichung einer indirekten Kommunikation zwischen verschiedenen Abteilungen können bei der Delphi-Methode unternehmensrelevante Bedrohungen entdeckt werden. Der Nachteil bei dieser Methode ist aber, dass bei vielen Iterationen ein hoher Aufwand entstehen kann und der Fokus der Methode über den einzelnen IT-Abteilungen liegt.

Die folgende Abbildung gibt eine Bewertung hinsichtlich des Aufwands, der Kosten sowie der Abdeckung des Risikospektrums und der Durchführung ab.

---

[94] Vgl. Fiege (2006), S. 144
[95] Vgl. Prokein (2008), S. 25
[96] Vgl. 5.2.2 FMEA

Methode	Aufwand / Komplexität	Kosten	Abdeckung des Risikospektrums	Durchführung
Brainstorming	gering	gering	breite Abdeckung	intern
Synektik	hoch	hoch	mittlere Abdeckung	intern*
Delphi-Methode	hoch	hoch	mittlere Abdeckung	intern**

* Genaue Methodenkenntnis unabdingbar.** Erst ab einer gewissen Unternehmensgröße sinnvoll.

Abbildung 22: Bewertung der vorgestellten Kreativitätsmethoden

Quelle: eigene Darstellung

5.4 Kollektionsmethoden

5.4.1 Checkliste

Erfahrungen aus der Vergangenheit können helfen, zukünftig ähnlich geartete Risiken zu identifizieren. Aus diesem Grund werden Checklisten auf Basis vergangener Ereignisse erstellt. Daraus entsteht eine Liste mit Punkten, die eine Identifikation zukünftiger IT-Risiken vereinfacht bzw. in Ansätzen ermöglicht. Diese Liste wird dabei Punkt für Punkt abgearbeitet und hinsichtlich aktueller Bedrohungen untersucht. Fertige Checklisten bietet beispielsweise das *Bundesamt für Sicherheit in der Informationstechnologie* auf seiner Homepage an.[97]

Versicherungs-Check IT

	Potentielles Risiko	Mögliche Schadenhöhe	Derzeitige Deckung	Versicherungs-möglichkeit	Notizen
A Drittschaden (Haftpflicht)					
Personenschäden					
01	**Personenschäden** z.B. bei betrieblicher Tätigkeit bei Kunden, Unfall von Besuchern			Personenschadendeckung im Rahmen der Betriebshaftpflicht	
Sachschäden					
02	Schäden an fremden Sachen, wie z.B. Servern des Kunden, inklusive der möglicherweise daraus folgenden Betriebsunterbrechung des Kunden			Sachschadendeckung im Rahmen der Betriebshaftpflicht, sofern die beschädigte Sache nicht unmittelbar Gegenstand der Bearbeitung war.	
03	Schäden am gemieteten Gebäude z. B. durch Brand			Mietsachschaden im Rahmen der Betriebshaftpflicht	

Abbildung 23: Checkliste

Quelle: http://www.bsi.bund.de/gshb/deutsch/hilfmi/check.htm

[97] http://www.bsi.bund.de/gshb/deutsch/hilfmi/check.htm

Problematisch an Checklisten ist, dass diese entweder aus einer geringen Anzahl an hoch aggregierten Risiken[98] besteht oder aus einer Vielzahl an kaum aggregierten[99] Risiken. Bei einer hohen Aggregation kann es vorkommen, dass Wechselwirkungen zwischen Einzelrisiken teilweise oder komplett ignoriert werden. Eine niedrige Aggregation hat den Nachteil, dass eine vollständige Identifizierung aller Bedrohungen nicht gegeben ist.[100] Checklisten sollten daher nur als Einstieg in die Risikoidentifizierung benutzt und ergänzend zu anderen Methoden angewendet werden.

Durch die einfache und schnelle Durchführung innerhalb von IT-Abteilungen stellen Checklisten in der Praxis eine sehr häufig eingesetzte Methode der Risikoidentifizierung dar.[101]

5.4.2 Expertenbefragung

Der Grundgedanke bei einer Expertenbefragung besteht darin, Schwachstellen und Bedrohungen zu ermitteln. Dazu wird das Wissen von internen und externen Experten herangezogen. Bei internen Experten, also Mitarbeitern im Unternehmen, stehen vor allem Ereignisse im Mittelpunkt, die nicht schriftlich festgehalten wurden, aber auch Vorgehensweisen, bei einem eingetretenen Risiko. Diese Gespräche können strukturiert oder formlos durchgeführt werden. Besonders formlose Gespräche haben den Vorteil, dass eventuelle „Beinahevorfälle“, die der befragenden Person zu diesem Zeitpunkt unbekannt waren, aber noch keine finanziellen Auswirkungen hatten, aufgedeckt werden.[102]

Bei der Befragung von externen Experten profitiert man von der Erfahrung, die diese Experten in anderen Unternehmen gemacht haben. Dabei werden speziell Verlustereignisse, Schwachstellen und Angriffe bei ähnlichen Unternehmen betrachtet und somit für das eigene Unternehmen adaptiert.[103]

Durch die Befragung von externen Experten erhöhen sich Kosten und Aufwand bei dieser Methode, trotzdem kann eine breite Abdeckung der möglichen Risiken durch gezielte Auswahl der Experten erreicht werden. Die Durchführung kann sowohl intern als auch extern stattfinden.

---

[98] „Hoch aggregiert“ bedeutete in diesem Zusammenhang, dass viele Einzelrisiken, in einer bestimmten Position der Checkliste zusammengefasst sind.
[99] „Kaum aggregiert“ bezieht sich in diesem Fall auf Einzelrisiken.
[100] Vgl. Hölscher (2006), S. 359.
[101] Vgl. Prokein (2008), S.20
[102] Vgl. Prokein (2008), S.21
[103] Vgl. Piaz (2002), S. 83.

5.4.3 Schadensfall-Datenbank

Eine Identifizierung von Risiken mit Hilfe von vergangenheitsorientierter Auswertung von Daten bietet die Schadensfall-Datenbank. Innerhalb der Finanzbranche ist der Aufbau einer solchen Datenbank für Kreditinstitute vorgeschrieben.[104] Festgehalten werden alle auftretenden operationellen Ereignisse, die sich negativ auf das Unternehmen ausgewirkt haben.

In der betrieblichen Praxis, von oben genannten Kreditinstituten einmal abgesehen, ist der Aufbau einer solchen Datenbank nicht verbreitet. Jedoch kann mit Hilfe von Informationen der internen Revision, des Rechnungswesens der Rechtsabteilung und des Qualitätsmanagements eine ähnliche Sammlung der Daten geschaffen werden. Speziell in der IT existieren eine Unzahl an Datenbanken, Log-Dateien und Berichten, aus denen sich eine solche Datenbank bilden lässt. Kritisch dabei ist allerdings der Umstand, dass sich bei der IT die Rahmenbedingungen in sehr kurzen Zeitabständen ändern.[105] Somit können unter Umständen keine Rückschlüsse auf zukünftige Ereignisse gezogen werden.

Der Aufbau, die Nutzung und die Analyse dieser Datenbank obliegen der IT-Abteilung. Die Erkenntnis über frühere Verlustereignisse sollte monetär bewertet und an Verantwortliche weitergeleitet werden. Damit wird ein Risikobewusstsein geschaffen und diese Methode gewinnt dadurch an Bedeutung.

Der Aufwand dieser Methode kann bei einer Vielzahl von Quellsystemen sehr hoch sein. Durch den Implementierungsaufwand für nötige Schnittstellen in eine geeignete Datenbank können auch die Kosten sehr schnell ansteigen. Der Nutzen insbesondere im IT-Umfeld ist aufgrund der schnellen Entwicklungszeit und der fragwürdigen Vergleichbarkeit mit vergangenen Ereignissen als eher gering einzuschätzen.

5.4.4 Bewertung der vorgestellten Kollektionsmethoden

Checklisten eigenen sich aufgrund der beschriebenen Aggregationsproblematik nicht für eine vollständige Risikoidentifikation und sollten nur in Verbindung mit anderen Methoden angewendet werden.[106] Wie dargelegt, eignet sich diese Methode weder zum Identifizieren von Existenz bedrohenden IT-Risiken noch wird eine vollständige Identifizierung erreicht. Positiv bei dieser Methode sind der geringe Aufwand und die damit verbundenen geringen Kosten.

---

[104] Vgl. Baseler Ausschuss für Bankenaufsicht (2004), Tz. 663, 673.
[105] Vgl. Junginger M. (2005), S. 248.
[106] Vgl. Hölscher (2006), S. 359.

Die Befragung von Experten führt in der Regel zur Identifikation von Existenz bedrohenden Risiken.[107] Eine vollständige Identifizierung ermöglicht aber auch diese Methode nicht. Der Aufwand ist sowohl bei der internen als auch externen Befragung von Experten als eher gering einzuschätzen. Die Kosten im Mittel (in- und externe Experten) sind als durchschnittlich einzustufen.

Der hohe Aufwand und der fragwürdige Nutzen bei hohen Kosten lassen die Schadensfall – Datenbank als eine schlechte Methode erscheinen.

Die folgende Abbildung gibt eine Bewertung hinsichtlich des Aufwands, der Kosten sowie der Abdeckung des Risikospektrums und der Durchführung ab.

Methode	Aufwand / Komplexität	Kosten	Abdeckung des Risikospektrums	Durchführung
Checkliste	gering	gering	breite Abdeckung	intern
Expertenbefragung	niedrig	durchschnittlich	mittlere Abdeckung	intern/extern
Schadensfall - Datenbank	hoch	hoch	mittlere Abdeckung*	intern

* Abdeckung basiert auf Vergangenheitserfahrungen.

Abbildung 24: Bewertung der vorgestellten Kollektionsmethoden

Quelle: eigene Darstellung

5.5 Zusammenfassung

Die vorgestellten Methoden ermöglichen es, verschiedene Risiken zu erfassen. Dabei ist jedoch zu beachten, dass nicht jede Methode für jedes Unternehmen anzuwenden ist. Einige dieser Methoden verursachen durch Einsatz externer Personen hohe Kosten. Andere Methoden entfalten ihr Potential erst bei einem genügend großen Unternehmen. Ferner erhebt diese Zusammenstellung der Methoden keinesfalls Anspruch auf Vollständigkeit. Vielmehr soll durch das vierte Kapitel eine Einführung in die Methoden und Techniken der Risikoidentifizierung ermöglicht werden. Die abschließende Bewertung nach jedem Unterkapitel gibt einen Überblick hinsichtlich Aufwand, Kosten, Abdeckung des Risikospektrums und Durchführungsart.

[107] Vgl. Prokein (2008), S. 32

6 Methoden zur Risikobewertung

6.1 Überblick und Aufbau einer Risikobewertung

Aufgabe einer Risikobewertung ist es, die in der vorausgegangen Phase der Risikoidentifikation entdeckten Risiken zu beurteilen und bewerten. Das Ergebnis der Risikobewertung steht im Hinblick auf Qualität und Verfügbarkeit in direktem Zusammenhang zu der Risikoidentifikationsphase.[108] Die Notwendigkeit einer Risikobewertung ergibt sich aus der Notwendigkeit, Risiken den Bestand gefährdende und andere Risiken einzuteilen. Kernpunkte der Risikobewertung sind:

- Eintrittswahrscheinlichkeit
- Schadenshöhe bei Eintritt des Risikos
- Schadenshäufigkeit

Die Schadenshäufigkeit bestimmt wie oft ein Risiko in einem bestimmten Zeitraum auftritt. Abhängigkeiten bestehen zwischen den Punkten *Eintrittswahrscheinlichkeit* und *Schadenshäufigkeit* sowie zwischen der *Eintrittswahrscheinlichkeit* und der *Schadenshöhe*. Die identifizierten Risiken werden im Verlauf der Risikobewertung mehrfach gefiltert und in ein Risikoportfolio eingeordnet. Unterscheiden kann man die Risikobewertung in zwei Bewertungsmöglichkeiten. Der qualitative Ansatz ermöglicht eine schnelle Ordnung der Risiken in einen Kontext. Dabei auftretende, den Bestand gefährdende Risiken können im Anschluss der wesentlich detaillierteren quantitativen Bewertung zugeführt werden. Erläutert werden in diesem Kapitel Methoden der qualitativen sowie quantitativen Bewertung. Anschließend wird aufgezeigt, wie die Ergebnisse in einem Risikoportfolio weiter verwendet werden können. Geschlossen wird mit der Erläuterung der „Value at Risk“ – Methode.

6.2 Qualitative Bewertungsansätze

Qualitative Bewertungsansätze beschäftigen sich mit Risiken, die sich nicht mit Erwartungswerten und Eintrittswahrscheinlichkeiten beschreiben lassen. Damit ist auch die Schadenshöhe und somit das gesamte Schadenpotential für diese Art von Risiken nicht ermittelbar. Zu nennen wären beispielsweise der Fortgang von wichtigen Personen im Unternehmen und der damit verbundene Wissensverlust, mögliche Imageschäden für

[108] Vgl. Fiege (2006), S. 159ff

das Unternehmen oder Naturkatastrophen.[109] Um diese Risiken dennoch zu bewerten, ist es notwendig, dass subjektive Eintrittswahrscheinlichkeiten gebildet werden, um so eine Quantifizierung zu ermöglichen.

Annualisierung[110]

Bei der Annualisierung handelt es sich um ein stark vereinfachendes, mathematisches Modell zur Bewertung von Risiken. Um Eintrittswahrscheinlichkeiten zu bestimmen, wird bei dieser Methode die Frage nach der Häufigkeit des Schadeneintritts gestellt. Dabei werden verschiedene Zeiträume betrachtet. Beispielsweise wird dabei erfragt, wie oft das Risiko in den nächsten zwei, drei oder fünf Jahren eintritt. Wird dabei mit einem Eintritt alle fünf Jahre gerechnet, so ergibt sich rechnerisch ein Risiko von 20% für den Risikoeintritt im kommenden Jahr. Es lassen sich durch diese Methode aber nicht nur Eintrittswahrscheinlichkeiten ermitteln, sondern auch erwartete Schadenshöhen. So wird die Frage nach der Schadenserwartung in den nächsten fünf Jahren beispielsweise mit zehn Millionen Geldeinheiten beantwortet. Daraus ergibt sich eine Schadenserwartung für das kommende Jahr von zwei Millionen Geldeinheiten. Diese Methode eignet sich, um für kommende Perioden durchschnittliche Erwartungswerte abzuleiten. Die Nachteile bei dieser Methode sind zum einen, dass wechselseitige Abhängigkeiten der Risiken untereinander nicht berücksichtigt werden. Ebenso vermischen sich bei einer solchen Betrachtung Risiken, die den Bestand gefährden, mit harmlosen Risiken, die dafür häufiger, aber in weitaus geringerer Maße Schaden verursachen.

Als Schlussfolgerung kann man festhalten, dass diese qualitative Methodik ausschließlich einen groben Anhaltspunkt für die Risikobewertung liefern kann. Durch starke Vereinfachung der Eintritts- wie auch der Schadenswahrscheinlichkeiten auf mathematischer Ebene können bei Eintritt falsche Schadensausmaße eintreten.

Klassifikation

Eine weitere qualitative Bewertungsmöglichkeit besteht darin, Risiken in Klassen einzuteilen. Die einzelnen Klassen reichen dabei von unbedeutenden/geringen Risiken bis hin zu den Bestand gefährdenden / existenzbedrohenden Risiken. Die folgenden zwei Abbildungen verdeutlichen verschiedene Klassifikationsansätze.

[109] Vgl. Fiege (2006), S. 81f
[110] Vgl. ebd., S. 82f

Relevanz-klasse	Grad der Einflussnahme	Erläuterung
1	Unbedeutendes Risiko	Unbedeutende Risiken, die weder den Jahresüberschuss noch den Unternehmenswert spürbar beeinflussen.
2	Mittleres Risiko	Mittlere Risiken, die eine spürbare Beeinträchtigung des Jahresüberschusses bewirken.
3	Bedeutendes Risiko	Bedeutende Risiken, die den Jahresüberschuss stark beeinflussen oder zu einer spürbaren Reduzierung des Unternehmenswertes führen.
4	Schwerwiegendes Risiko	Schwerwiegende Risiken, die zu einem Jahresfehlbetrag führen und den Unternehmenswert erheblich reduzieren.
5	Bestandsgefährdendes Risiko	Bestandsgefährdende Risiken, die mit einer wesentlichen Wahrscheinlichkeit den Fortbestand des Unternehmens gefährden.

Abbildung 25: Risiko-Relevanzskala nach Gleißner

Quelle: Gleißner (2008), S. 104

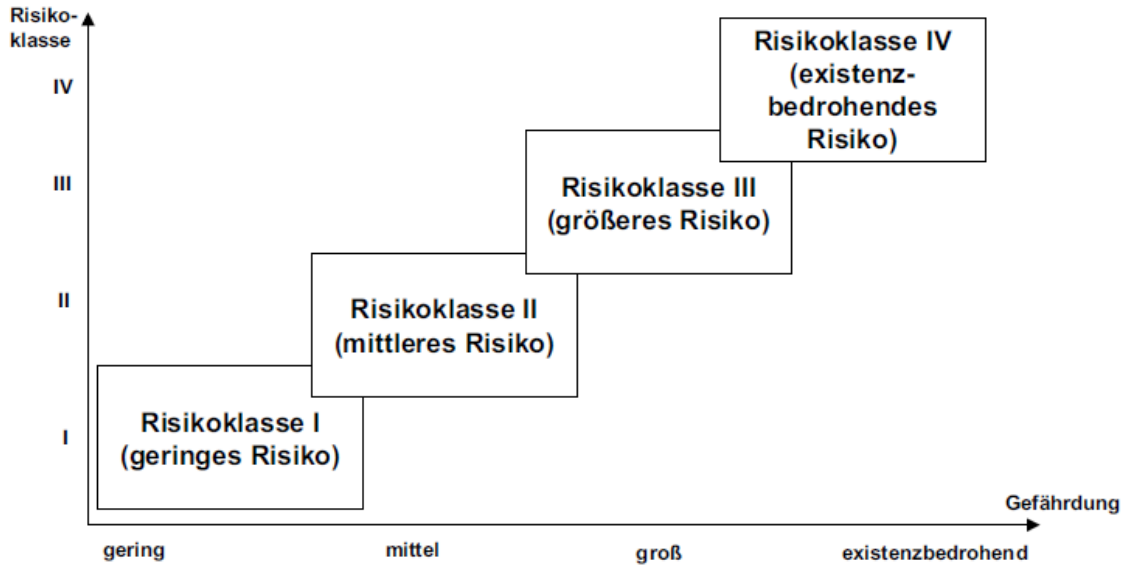

Abbildung 26: Risikoklassen

Quelle: Fiege (2006), S. 178

Je nach Risikoneigung und Unternehmensgröße können diese Einteilungen unterschiedlich ausgeprägt sein. In beiden Abbildungen wurde die Klassifikation anhand des Kriteriums „Unternehmensgefährdung“ vorgenommen. Durch die Benutzung einer Klassifikation wird klar, in welchen Bereichen Risiken einer genaueren Betrachtung unterzogen

werden müssen. Jedoch ist diese Methode, wie auch die Annualisierung, stark vereinfachend. Darüber hinaus sind die Merkmale für die einzelnen Kategorien subjektiv und können je nach befragter Person deutlich abweichen. Durch externe Berater oder mehrere interne Experten kann die Einteilung jedoch objektiver gestaltet werden. Gezielte Schulungen und Weiterqualifizierungen erhöhen diesen Effekt weiter, so dass eine Erhöhung der Genauigkeit bei der Klassifikation erreicht werden kann.[111]

Risikoportfolio

Eine andere Bewertungstechnik ist die Portfolio-Technik. Bei dieser Methode werden zunächst die identifizierten Risiken mit zusätzlichen Informationen wie Schadenshöhe und Eintrittswahrscheinlichkeit erweitert.[112] Es erfolgt dabei eine Verknüpfung von qualitativen und quantitativen Werten. Die folgende Abbildung zeigt ein Verwendungsbeispiel der Portfolio-Technik anhand eines Risikoportfolios.

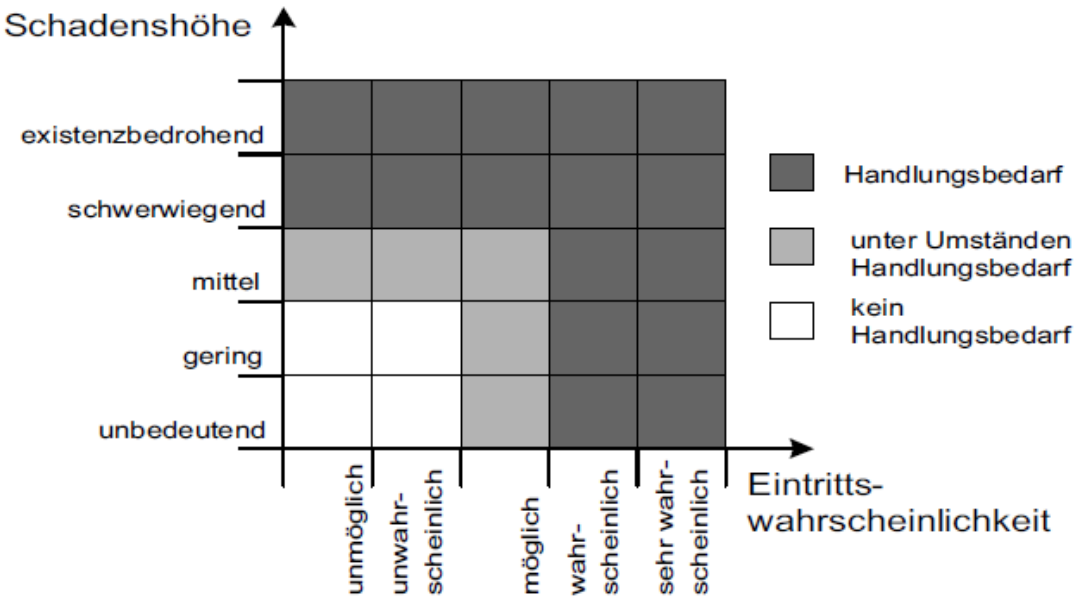

Abbildung 27: Risikoklassen

Quelle: Fiege (2006), S. 180

Der Vorteil bei einer solchen Darstellung der Risiken besteht darin, dass daraus ein direkter Handlungsbedarf abzuleiten ist. Relevant für die Betrachtung sind vor allem Risiken, die innerhalb der Schadenshöhe auf dem mittleren und schwerwiegenden Niveau eingeordnet sind. Diese können, ungeachtet der Eintrittswahrscheinlichkeit, erheblich den Betrieb einer Unternehmung bis hin zu Bestandsgefährdung beeinflussen.

[111] Vgl. Fiege (2006), S. 178f
[112] Vgl. Gleißner (2008), S. 117.

Mit Hilfe dieser Technik lassen sich Risiken in einfacher Form darstellen. Durch Einordnung der Risiken in einem Risikoportfolio lassen sich die Verteilung und eventuell auch die Konzentration der Risiken feststellen. Durch diese Methode erhält das Management eine Grundlage, um Risiken zu steuern. Durch die starke Vereinfachung und durch das Fehlen eines chronologischen Kriteriums wird auch bei dieser Technik nur ein unvollständiges Bild über die Risiken abgegeben. Es handelt sich, wie bei allen vorgestellten Methoden, um eine Momentaufnahme der Risiken und diese Risiken können sich in einem aktiven Marktumfeld jederzeit ändern.

Scoring

Das „Scoring" bietet eine Möglichkeit, verschiedene Risiken vergleichbar zu machen. Dabei werden den Risiken Bewertungskriterien zugewiesen (Eintrittswahrscheinlichkeit, Schadenshäufigkeit, Schadenshöhe und andere). Für die Erfüllung eines Kriteriums werden risikospezifische Punkte vergeben. Die einzelnen Kriterien erhalten eine Gewichtung. Durch Multiplikation von Gewichtung und Punkten ist es möglich, vergleichbare Risikowerte zu ermitteln.

Die Vorteile dieser Methode liegen in der Vergleichbarkeit von Risiken anhand des erzielten Wertes. Dies ist für Einzelrisiken ebenso anwendbar, wie für die Aggregation aller Einzelrisiken zu einem Gesamtrisiko. Nachteil auch dieser Methode ist es, dass Risiken nach subjektiven Kriterien eingeteilt werden. Wechselwirkungen zwischen den Einzelrisiken bleiben ebenso unberücksichtigt.

6.3 Quantitative Bewertungsansätze

Um quantitative Aussagen über Risiken treffen zu können, müssen diese zuvor bestimmten Zielen zugeordnet werden. Diese Ziele müssen nach Inhalt, Ausmaß und Zeitbezug festgelegt sein.[113] Nur so kann in einer Gegenüberstellung von Soll- und Ist-Zustand eine Aussage über die Abweichung und den damit erzielten Verlust getroffen werden. Da sich Kredit gebende Institute und Versicherungen verstärkt mit quantifizierbaren Risiken beschäftigen, stammen auch viele quantitative Bewertungsmethoden aus diesem Bereich.

Value-at-Risk

Lassen sich objektive Aussagen über die Eintrittswahrscheinlichkeit von Risiken treffen, kann der „Value-at-Risk" – Ansatz (VaR) verwendet werden. Der VaR trifft im Ergebnis eine Aussage über einen bestimmten Verlust, der innerhalb eines vorgegebe-

[113] Vgl. Fiege (2006), S. 165ff

nen Zeitraums mit einer bestimmten Wahrscheinlichkeit eintritt. Es gibt dabei verschiedene Möglichkeiten, den VaR zu berechnen, so zum Beispiel etwa die Monte-Carlo-Simulation oder die historische Simulation. Im Folgenden wird der Ablauf dieses Ansatzes anhand der Monte-Carlo-Simulation näher betrachtet.

Ausgangspunkt sind die Verteilungsfunktionen der Verlusthäufigkeit und -höhe, aus denen eine Gesamtverlustverteilung erstellt wird.[114] IT-Risiken haben die Eigenschaft, dass es sich entweder um sehr hohe Schäden mit geringer Wahrscheinlichkeit, oder um kleine Schäden mit hoher Wahrscheinlichkeit handelt.[115] Die Poisson-Verteilung beschreibt diese Eigenschaften am besten und wird somit für die Häufigkeitsverteilung herangezogen[116]. Für die Ermittlung der Schadenshöhe eignet sich die logarithmische Normalverteilung, die Ereignisse mit niedriger Wahrscheinlichkeit und hohen Werten (die stets positiv sind) darstellt.[117] Die Monte-Carlo-Methode drückt ein zweistufiges Vorgehen aus, das die Anzahl der Schadensfälle einer Periode und die entsprechenden Schadenshöhen bestimmt. Beide Werte werden multipliziert und als Gesamtschadensverteilung dargestellt. Um eine stabile Verlustverteilung zu erhalten, muss dieses zweistufige Vorgehen sehr oft wiederholt werden. Voraussetzung für die Bildung einer Gesamtverteilung ist die Unabhängigkeit der beiden Funktionen.[118]

Die Vorteile des VaR-Verfahrens liegen in der einfachen Kommunikation der Werte und in der Weiterverwendung der Ergebnisse innerhalb des betrieblichen Risikomanagements. Der hohe Aufwand für die Berechnung und die komplexe Erarbeitung stellen einen Nachteil dar. Zudem können nicht alle IT-Risiken durch den operationalen VaR-Ansatz abgebildet werden, da eine entsprechende Häufigkeit und Kategoriebildung der IT-Risiken gegeben sein muss. Nach Junginger ist die Berechnung für IT-Betriebsrisiken, wie z.B. Hardware-, Software- oder auch Benutzerfehler, durch den vorgestellten operationalen VaR-Ansatz durchführbar.[119]

Sensitivitätsanalyse

Sind keine Informationen über die Wahrscheinlichkeitsverteilung der Risikofaktoren vorhanden, kann die Sensitivitätsanalyse angewendet werden. Bei dieser Methode werden alle bis Risikofaktoren bis auf einen fixiert und der verbleibende Risikofaktor wird dann variiert. Die Analyse erfolgt dabei mit einer möglichst geringen Änderung des

[114] Vgl. Prokein (2008), S. 53
[115] Vgl. Königs (2006), S. 36
[116] Vgl. Junginger (2005), S. 258f
[117] Vgl. Hechenblaikner (2006), S. 179
[118] Vgl. ebd., S. 191f
[119] Vgl. Junginger (2005), S. 263

Risikofaktors. Nach Fiege[120] können mit Hilfe der Sensitivitätsanalyse zwei unterschiedliche Fragestellungen untersucht werden: zum einen die Ermittlung von kritischen Werten und zum anderen bei der Bandbreitenanalyse.

Bei der Ermittlung von kritischen Werten wird beobachtet, wann sich eine Handlungsalternative durch Variation der Ausgangsdaten in Bezug auf eine andere Handlungsalternative ändert. Es wird also der Wert gesucht, bei dem sich eine gegebene Handlungsalternative als schlechter herausstellt als eine andere.

Die Bandbreitenanalyse untersucht den absoluten Erfolg einer Handlungsalternative bei Variation der Ausgangsdaten. Dabei werden die Parameter so gewählt, dass die Handlungsalternative mit der günstigsten Ausgangsdatenlage betrachtet wird. Verglichen werden diese Ergebnisse dann mit der schlechtesten möglichen Ausgangsdatenlage. Durch die Betrachtung des schlechtesten Ausgangs einer Handlungsalternative mit dem bestmöglichen Ausgang für ebendiese erhält man eine Bandbreite an Informationen. Mit Hilfe dieser Informationen kann man abschätzen, ob sich bei der gegebenen Handlungsalternative Bereiche identifizieren lassen, die sich bestandsgefährdend im Unternehmen auswirken können.

Die Sensitivitätsanalyse kann besonders dann angewendet werden, wenn verschiedene Parameter relativ genau bekannt sind und wenn man einen starken Einflussparameter identifiziert hat, dessen Einfluss geschätzt werden soll. Da bei dieser Analyse Vereinfachungen und die Wechselwirkungen zwischen Risiken vernachlässigt werden, eignet sie sich als nur unterstützende Methode zur Bewertung von Risiken.

6.4 Zusammenfassung

Um Verluste aus IT-Risiken abzuschätzen gibt es keine Methode, weder qualitativ noch quantitativ, die eine allumfassende Risikobewertung ermöglicht. Auf den ersten Blick scheint die Risikobewertung nach der einfachen Formel „Eintrittswahrscheinlichkeit x erwartete Schadenshöhe“ eine simple und problemlos lösbare Aufgabe zu sein. Wie jedoch durch die verschiedenen Methoden der Risikobewertung dargestellt, ist es nahezu unmöglich, ohne eine entsprechende Datenbasis Aussagen über Risiken zu treffen. Bei unzureichender Basis müssen vielmehr Annahmen über Auswirkung, Eintrittswahrscheinlichkeit und Schadenshöhe getroffen werden, um überhaupt eine Aussage bezüglich der Risikobewertung treffen zu können. Daher ist es für IT-Risiken essentiell, eine entsprechende Datenbasis aufzubauen und die Methoden der Risikobewertung stets an veränderte Rahmenbedingungen anzupassen. Da die Risiken bei diesen Methoden iso-

[120] Vgl. Fiege (2006), S. 173f

liert betrachtet werden, besteht die Gefahr, dass die Wechselwirkungen zwischen den Risiken unberücksichtigt bleiben.

Die qualitativen Bewertungsmethoden ermöglichen eine schnelle Einordnung von Risiken in bestimmte Schadenshöchstklassen. Um Aussagen über Risiken zu treffen, die den Fortbestand des Unternehmens bedrohen, eignen sich diese Methoden. Auch ist durch die Einteilung von Risiken in Klassen eine Aussage über die minimale und maximale zu erwartende Schadenshöhe sowie die Eintrittswahrscheinlichkeit möglich. Ein direkter Handlungsbedarf lässt sich mit Hilfe der qualitativen Bewertungsansätze ableiten.

Für quantitative Methoden wie die Sensitivitätsanalyse ist eine genaue Kenntnis aller Parameter zwingend notwendig. Nur so können Aussagen bei veränderter Ausgangslage getroffen werden. Sind objektive Daten für die Eintrittswahrscheinlichkeit eines IT-Risikos bekannt, lässt sich mit Hilfe des „Value-at-Risk“ – Verfahrens feststellen, mit welcher Wahrscheinlichkeit ein bestimmter Verlust innerhalb eines gegebenen Zeitraums eintreten kann.

Die vorgestellten Möglichkeiten zur Risikobewertung stellen nur einen Ausschnitt aus der Methodenvielfalt der Risikobewertung dar. Die Kosten für die Durchführung können bei allen Methoden, bis auf den „Value-at-Risk“ – Ansatz, vernachlässigt werden. Dem hohen Implementierungsaufwand des „Value-at-Risk“ – Ansatzes steht eine schnelle und kostengünstige Aussage über finanzielle Risiken gegenüber.

7 Strategien zur Steuerung von IT-Risiken und Risikokontrolle

7.1 Risikosteuerung

Nachdem ein Risiko identifiziert und bewertet wurde, stellt sich die Frage nach dem Umgang mit dem Risiko. Die Risikosteuerung hat das Ziel, Risiken aktiv und gezielt zu beeinflussen. [121] Risiken wurden in der Risikobewertung mit einem bestimmten monetären Verlust bewertet. Dieser Verlust kann durch die Steuerungsmaßnahmen reduziert werden. Im Ergebnis sollen die Risiken auf ein in der Risikopolitik definiertes Sicherheitsniveau verringert werden.

Mögliche Angriffspunkte ergeben sich dabei aus der Betrachtung der Eintrittswahrscheinlichkeiten und der Schadenshöhe. Diese beiden Faktoren werden der in der Risikostrategie definierten maximalen Schadenshöhe gegenübergestellt und werden, sofern nötig, auf ein für das Unternehmen akzeptables Maß reduziert. Um eine Reduzierung der Schadenshöhe oder der Eintrittswahrscheinlichkeit zu erreichen, werden Maßnahmenpakete erforderlich, die sich wiederum monetär auswirken. Mit anderen Worten hat die Reduzierung von Schadenshöhe bzw. Eintrittswahrscheinlichkeit finanzielle Folgen, die abgewogen werden müssen. Eine Maßnahme sollte nicht mehr kosten, als für die Reduzierung eines IT-Risikos eingespart wird. In Kapitel 7.3 erfolgt eine gesonderte Wirtschaftlichkeitsbetrachtung dieser Schutzmaßnahmen.

Die Risikosteuerung wird dabei in zwei Abschnitte unterteilt. Auf der einen Seite stehen aktive und ursachenbezogene Maßnahmen, welche auf eine Beseitigung bzw. Reduzierung der Ursachen abzielen oder diese Ursachen vermindern sollen. Die andere Seite versucht die Auswirkungen eines Risikoeintritts zu beeinflussen. Dabei wird der Eintritt des Risikos bewusst akzeptiert. Vielmehr zielen Maßnahmen der passiven Risikosteuerung auf eine Veränderung der entstehenden Schadenshöhe ab.[122]

In der folgenden Abbildung werden die Optionen zur Risikosteuerung vorgestellt:

[121] Vgl. Klempt (2007), S. 82
[122] Vgl. Wiedemann (2008), S. 25

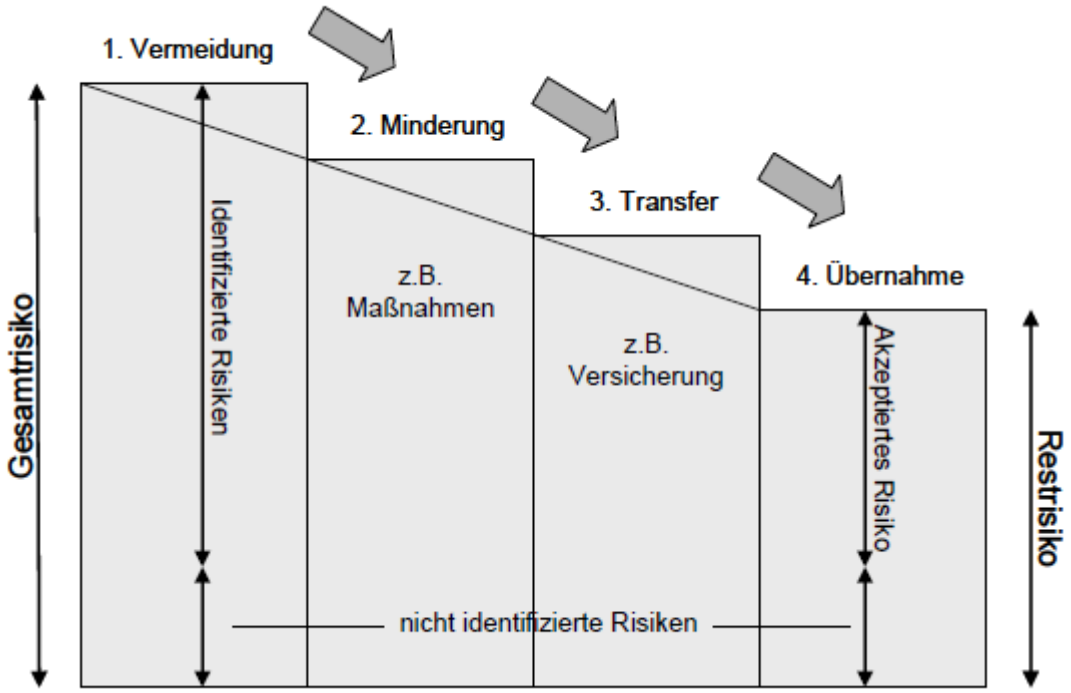

Abbildung 28: Risikoklassen

Quelle: Klempt (2007), S. 83

Die Strategien Vermeidung und Verminderung gehören zur aktiven Seite der Risikosteuerung. Transfer und Übernahme gehören zur passiven Seite. Im Gesamtrisiko sind auch immer nicht identifizierte Risiken enthalten, die sich durch keine der vier Risikostrategien steuern lassen.

7.2 Risikostrategien: Vermeiden, Vermindern, Transfer, Übernahme

7.2.1 Vermeiden

Die Vermeidung von Risiken stellt die erste Risikostrategie dar. Mit Hilfe dieser Strategie werden Eintrittswahrscheinlichkeit und/oder Schadenshöhe auf Null gesetzt.[123] Jedoch steht dem völligen Ausschließen von Risiken auch der vollkommene Verzicht auf Chancen gegenüber. Diese Strategie wird immer dann gewählt, wenn Risiken signifikante wirtschaftliche Schäden nach sich ziehen würden und somit über dem in der Risikostrategie definierten, maximalen Schadensmaß liegen würden. Andere Methoden, wie

[123] Vgl. Prokein (2008), S. 89

Transfer oder Verminderung, sind bei dieser Strategiewahl entweder nicht möglich, oder wären mit hohen Kosten verbunden.[124]

Folgende Abbildung verdeutlicht die Risikovermeidung:

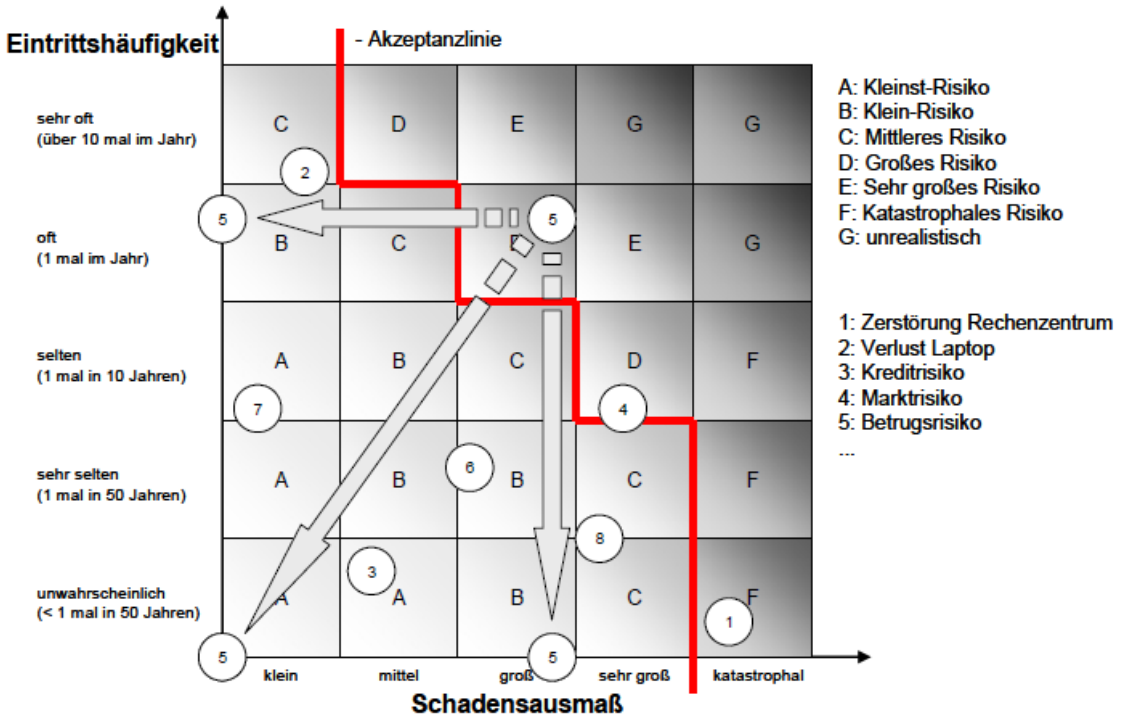

Abbildung 29: Risikovermeidung

Quelle: Klempt (2007), S. 84

In dieser Abbildung liegt das Risiko fünf außerhalb der Akzeptanzlinie. Da eine Verminderung nicht möglich ist, werden die Eintrittshäufigkeit und/oder das Schadensausmaß auf null reduziert. Beispielsweise bietet eine Bank solange kein Onlinebanking an, bis die Bank ihren Kunden und sich selbst eine höhere Sicherheit gewähren kann.[125]

7.2.2 Vermindern

Bei der Strategie der Risikoverminderung wird versucht, auf die Schadenshöhe bzw. Eintrittswahrscheinlichkeit Einfluss zu nehmen und diese zu reduzieren. Das Chancenpotential bleibt dabei bestehen.[126] Um diese Reduzierung zu erreichen, werden im IT-Umfeld überwiegend technische Sicherheitsmaßnahmen angewendet, die proaktiv und wirkungsbezogen eingesetzt werden. Die dabei eingesetzten Maßnahmen sind dabei

[124] Vgl. Klempt (2007), S. 83
[125] Vgl. ebd., S. 84
[126] Vgl. Rosenkranz, Missler-Behr (2005), S. 45

beispielsweise Virenscanner und Datensicherungssoftware, aber auch Hochverfügbarkeitslösungen für IT-Systeme oder Verschlüsselungstechniken.[127] Diese Beispiele verdeutlichen die vielfältigen Möglichkeiten im IT-Bereich, um Risiken zu vermindern. Die Möglichkeiten unterscheiden sich nach Komplexität und laufenden Kosten. Gerade durch komplexe Maßnahmen können neue, wie auch immer geartete Risiken entstehen. Es wäre denkbar, dass ein Unternehmen ein neues Datenbanksystem einführt, durch mangelnde Anwenderschulung aber Bedienungsfehler verursacht werden, die wiederum mit monetären Verlusten einhergehen.

Bei der Risikoverminderung gibt es zwei Ansätze.[128] Diese sollen an folgendem Beispiel verdeutlicht werden: Ein Unternehmen hat als Risiko eine mögliche Feuergefahr in einem Lager ausgemacht. Würde das Lager brennen, entstünden hohe Kosten und die Produktion würde sich verlangsamen. Eine Möglichkeit, mit dieser Situation umzugehen, ist es, die Lagerhalle mit Rauchmeldern auszustatten. Diesen Ansatz nennt man direkte Risikoverminderung. Es ist aber ebenso möglich, das Risiko zu verteilen, indem bestimmte Produkte auf andere Lager verteilt werden. Bei einem möglichen Feuer wäre so nur noch ein bestimmter Anteil der Produkte betroffen und das Risiko so verteilt. Diesen Ansatz der Risikominderung nennt man Risikodiversifikation. Die folgenden Abbildungen zeigen die direkte Risikominderung und die Risikodiversifikation:

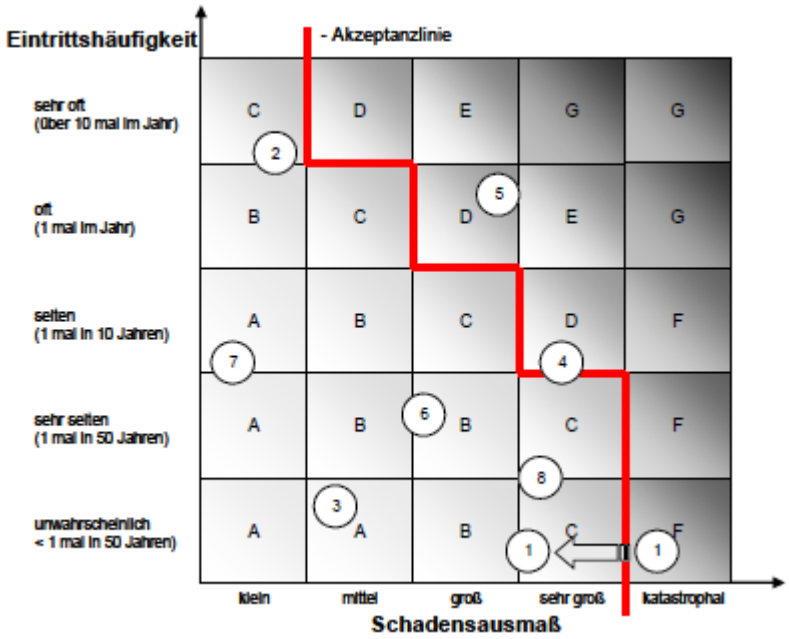

Abbildung 30: Risikoverminderung

Quelle: Klempt (2007), S. 85

[127] Vgl. Prokein (2008), S. 79
[128] Vgl. Klempt (2007), S. 85f

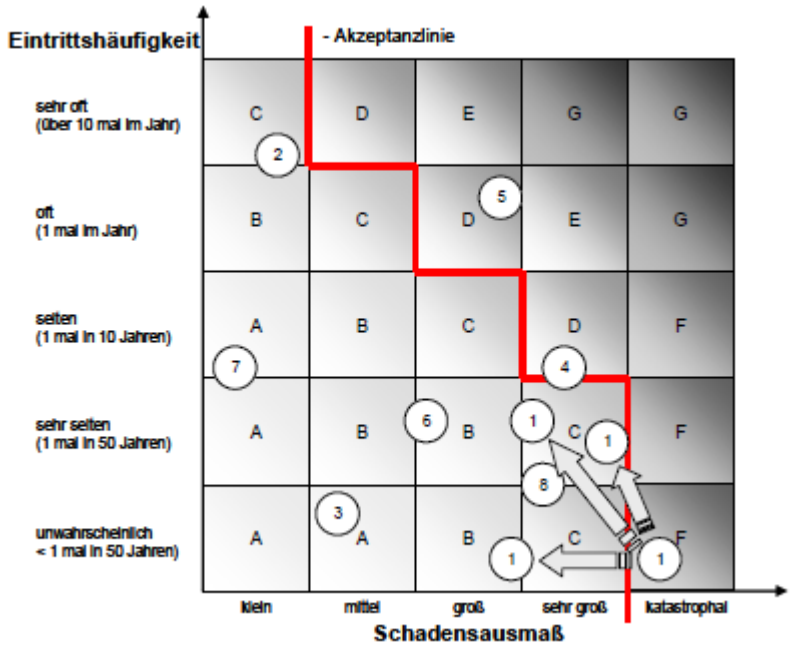

Abbildung 31: Risikodiversifikation

Quelle: Klempt (2007), S. 85

In Abbildung 30 ist zu erkennen, dass durch eine geeignete Maßnahme das Risiko eins in der Schadenshöhe vermindert wurde. Es wurde so von einer katastrophalen Schadenshöhe auf eine sehr große Schadenshöhe vermindert, welche innerhalb der Akzeptanz des Unternehmens liegt. Abbildung 31 zeigt die Verteilung des Risikos. Gemäß dem oben angesprochenen Beispiel würde das bedeuten, dass durch die Verteilung auf mehrere Lager die Schadenshöhe im Einzelfall sinken wird.

7.2.3 Transfer

Im Fall der Risikostrategie „Transfer“ besteht das Ziel nicht in einer Reduktion der Schadenshöhe bzw. der Eintrittswahrscheinlichkeit, sondern vielmehr wird der Eintritt des Risikos bewusst akzeptiert. Die Auswirkungen beim Eintritt eines Risikos werden dabei durch entsprechende Risikovorsorge vermindert oder vermieden.[129] Dazu werden die negativen Folgen eines Risikos vor dessen Eintritt von einer Vertragspartei übernommen. Die Grundbedingung für einen Risikotransfer ist also die Existenz einer Vertragspartei, die die Auswirkungen bei einem Risikoeintritt trägt, so dass die negativen Folgen nicht vom Unternehmen selbst getragen werden müssen.

[129] Vgl. Klempt (2007), S. 86f

Vertragspartner, die die Auswirkungen bei Risikoeintritt übernehmen, sind Versicherungen. Klassische Sachversicherungen übernehmen dabei gegen eine Prämie zum Beispiel Schäden aus Feuer oder Einbrüchen. Daneben transferieren Unternehmen vor allem Risiken, die ihre eigene Finanzkraft übersteigen könnten.[130] Neben den Versicherungen gibt es noch andere Möglichkeiten eines Risikotransfers. Beispielsweise ist der Abschluss eines Wartungsvertrages für Soft- oder Hardware ein solcher Transfer.[131] Die Vertragsparteien vereinbaren dabei, gewisse Zeiten bei einer Fehlerbehebung einzuhalten. Kommt es zu einem Fehler in der Soft- oder Hardware, greift der Wartungsvertrag und es kommt zu einer Fehlerbehebung innerhalb einer definierten Zeit. Das Unternehmen, das den Vertrag abschließt, kann somit also die maximale Zeit bis zur Problemlösung abschätzen und somit die Folgen bei Risikoeintritt gegen Zahlung einer Vertragsprämie vermindern. Kommt es nicht zu einer Behebung des Fehlers in der vertraglich vereinbarten Zeit, kann das Unternehmen, welches den Vertrag abgeschlossen hat, Schadensansprüche geltend machen.

Vorteile bei einem Risikotransfer sind die genaue Kenntnis der zu zahlenden Prämien und der eintreffenden Zahlungen bei Risikoeintritt. Alle Risiken mithilfe dieser Strategie auf einen Vertragspartner zu transferieren, ist wirtschaftlich jedoch nicht sinnvoll. Zunächst kostet jede Versicherung eines Risikos Geld. Darüber hinaus gibt es bestimmte Risiken, die nicht durch eine Versicherung abgedeckt werden können. So zum Beispiel ein Imageverlust infolge einer von Trojanern befallenen Software. Folgen aus so einem Risiko sind auf keine Versicherung übertragbar.[132] Ebenfalls sind die fortlaufenden Kosten für Versicherungen ein wirtschaftlich nicht zu unterschätzender Faktor.

7.2.4 Übernahme

Risiken, deren Schadensausmaß und Eintrittswahrscheinlich als gering einzustufen ist, werden mit Hilfe der Risikoübernahme gesteuert.[133] Bei diesen Risiken ist eine andere Steuerungsstrategie oft unwirtschaftlich in Bezug auf die aufgewendeten Ressourcen. Die Übernahme von Risiken setzt jedoch voraus, dass diese hinreichend analysiert, bewertet und dokumentiert sind. Ebenfalls muss die Entscheidung einer Übernahme mit der Geschäftsleitung abgesprochen sein oder aber von dieser initiiert werden. Wiedemann führt an, dass die Risikoübernahme als Steuerungsstrategie im Sinne der gesetzlichen Vorgaben als vollwertiges Steuerungsmittel anzusehen ist.[134] Jedoch müssen diese

[130] Vgl. Klempt (2007), S. 86
[131] Vgl. Junginger (2005), S. 281
[132] Vgl. Klempt (2007), S. 87
[133] Vgl. ebd., S. 89
[134] Vgl. Wiedemann (2008), S. 175f

Risiken beobachtet und überwacht werden, um bei Änderungen reagieren zu können. Dazu sind finanzielle Rücklagen zu bilden, um diese Risiken bei Eintritt bewältigen zu können.[135] Ebenfalls denkbar ist die Anwendung (implizit) bei Risiken, die in der Phase der Identifikation entweder nicht erkannt oder unzureichend analysiert wurden.[136]

7.3 Wirtschaftlichkeitsbetrachtungen von IT-Schutzmaßnahmen

Das Problem bei der Risikosteuerung ist, dass Risiken nur sehr schwer quantifizierbar sind.[137] Diese Ausgangslage beschreibt eine Art Dilemma, bei dem die Kosten für eine Steuerungsstrategie sofort sichtbar werden, der Nutzen aber nur geschätzt und nur im Falle eines Risikoeintritts ersichtlich ist.[138] Folgende Grafik verdeutlicht den Zusammenhang zwischen den Kosten, die Sicherheitsmaßnahmen verursachen, und den Kosten, die Folge eines Risikoeintritts sind.

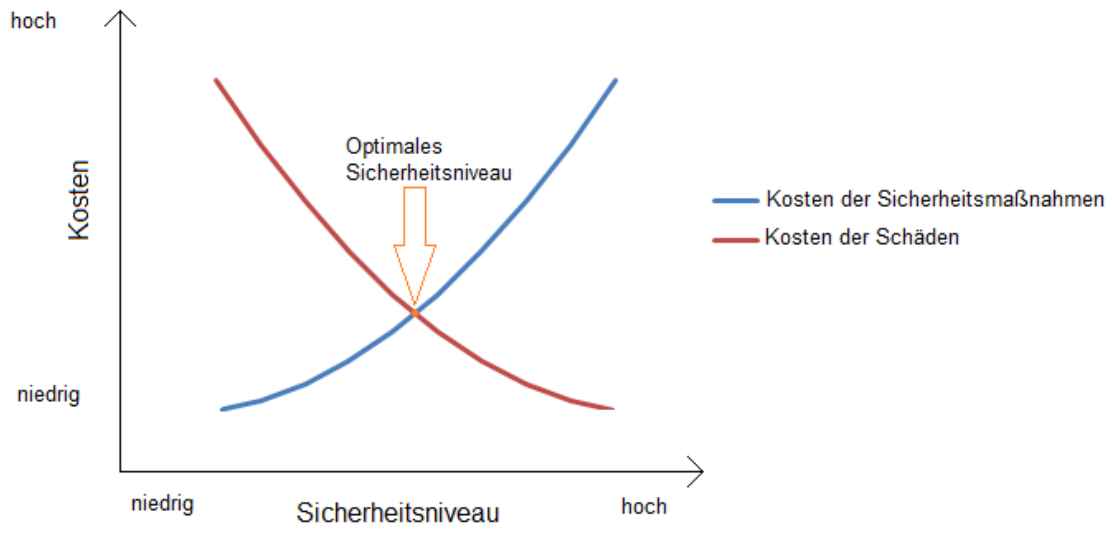

Abbildung 32: Kosten der Risiken / Kosten der Sicherheitsmaßnahmen

Quelle: In Anlehnung an Junginger (2005), S. 285

Anhand dieser Grafik wird ersichtlich, dass mit steigendem Sicherheitsniveau die Kosten für zusätzliche Sicherheit exponentiell höher werden. Das optimale Sicherheitsni-

[135] Vgl. Junginger (2005), S. 282
[136] Vgl. Klempt (2007), S. 89
[137] Vgl. Kapitel 6
[138] Vgl. Krcmar (2005), S. 448

veau liegt dabei im Schnittpunkt der zwei Kurven und es wird dabei der Grenznutzen den Grenzkosten gleichgesetzt.[139] Es gibt verschiedene Ansätze in der Wissenschaft, um die Wirtschaftlichkeit von Steuerungsmaßnahmen zu berechnen. Allerdings ermöglicht keine dieser Methoden eine exakte Berechnung.[140]

Eine verbreitete Methode, um die Wirtschaftlichkeit zu berechnen, ist der „Return on Security Investment" – Ansatz (ROSI). Inhalt dieser Methode ist die Gegenüberstellung von Kosten für die Maßnahme(n) und dem Nutzen daraus. Die Kosten werden dabei durch den „Total Cost of Ownership" – Ansatz (TCO) berechnet. Bei diesem Ansatz werden sämtliche Kosten der Maßnahme(n) berechnet. Die Kosten setzen sich unter anderem aus Anschaffungskosten, Schulungskosten für Mitarbeiter, Installationskosten sowie Kosten für Betrieb und Wartung zusammen. Der Nutzen auf der anderen Seite wird durch die Reduktion des Risikoschadens bei Eintritt der Maßnahme(n) und durch die Nutzung von Chancen bei Wahrnehmung des Risikos berechnet. Die Chancen fließen dabei als mögliche Umsatzsteigerungen bzw. Kostenminimierungen in die Berechnung ein. Die Differenz von Nutzen und Kosten ergibt dann die Kennzahl des ROSI. Dabei sind gewisse Konventionen, wie die Betrachtung einer Zeitperiode und Abschätzungen aufgrund fehlender Daten, einzuhalten.[141] Diese Kennzahl ermöglicht es der Unternehmensleitung, die Maßnahmen bewerten zu können, auch wenn diese wie erwähnt durch Abschätzung und fehlende Daten niemals genau sein kann.

7.4 Risikokontrolle

Die Aufgabe der Risikoüberwachung ist zu überprüfen, ob die aktuelle Risikolage mit der angestrebten Risikosituation übereinstimmt. Überprüft werden dabei sowohl operative als auch strategische Prozesse.[142] Dabei stehen die vorangegangenen Aktivitäten des Risikomanagements, die Risikodokumentation und das Aufspüren von Abweichungen im Mittelpunkt.[143] Der Prozess der Risikoüberwachung stellt dabei den letzten Schritt im IT-Risikomanagementsystem dar. Gleichzeitig dient dieser auch als Ausgangspunkt, um den kompletten Zyklus von der Identifikation bis hin zur erneuten Kontrolle kontinuierlich zu durchlaufen. Das Umfeld der Informationstechnologien ist geprägt durch eine hohe Entwicklungsgeschwindigkeit und durch einen kurzen Lebenszyklus dieser Technologien. Daher sind Kontrollen zeitnah und permanent durchzuführen.[144]

---

[139] Vgl. Junginger (2005), S. 284f
[140] Vgl. Prokein (2008), S. 126
[141] Vgl. Junginger (2005), S. 286
[142] Vgl. Klempt (2007), S. 90
[143] Vgl. Wiedemann (2008), S. 28
[144] Vgl. Krcmar (2005), S. 448f

Durchgeführt wird die operative Kontrolle durch Abweichungsanalysen. Dabei wird der vorgegebene Soll – Zustand mit dem erreichten Ist – Zustand verglichen. Betrachtet dabei werden jeweils die Einzelrisiken.[145] Werden dabei Abweichungen festgestellt, so ist zu überprüfen, inwieweit die ausgewählten Steuerungsmaßnahmen geeignet sind, um das Risiko entsprechend der Strategie zu behandeln. Falls es nötig wird, muss eine Korrektur dieser Maßnahmen stattfinden. Es werden aber nicht nur die Steuerungsmaßnahmen überprüft, sondern auch die Risikoidentifikation und die Risikobewertung. Sollten dabei nicht identifizierte Risiken entdeckt werden oder erweist sich eine Bewertung als fehlerhaft, so wird dieser Umstand durch die Risikokontrolle aufgedeckt und entsprechend kommuniziert. Die Überprüfung sämtlicher Bereiche des IT-Risikomanagementsystems ermöglicht es den Verantwortlichen, einen umfassenden Blick auf die Risikolage im Unternehmen bzw. im Unternehmensbereich zu geben. Die gewonnenen Rückschlüsse fließen dabei in die Risikopolitik ein und ermöglichen so, angemessen und schnell auf riskante Entwicklungen zu reagieren.[146]

Auf strategischer Ebene findet eine Überwachung und Anpassung des IT-Risikomanagementsystems und dessen Prozessen statt. Aufgedeckt werden sollen mögliche Defizite in der Organisation bzw. im Ablauf der Prozesse. Die Risikostrategie wird dahingehend überprüft, ob die definierten Maßnahmen und Zielvorgaben angemessen und wirksam sind.[147] Lassen sich Mängel bezüglich der definierten Verlustgrenzen feststellen, so ist die Risikostrategie entsprechend zu modifizieren.

Neben der prüfenden Funktion hat die Risikokontrolle auch eine dokumentierende Funktion. Dabei werden aus sämtlichen vorausgegangenen Arbeitsschritten Erkenntnisse formuliert und in Form eines Berichts an die beteiligten Personen kommuniziert. Diese Berichterstattung sollte dabei regelmäßig in monatlichem oder vierteljährlichem Abstand erfolgen, um eine angemessene Reaktionszeit zu ermöglichen.[148] Wird durch die Risikokontrolle ein nicht identifiziertes Risiko entdeckt, muss ein Sonderbericht erstellt werden, der außerhalb des oben angegebenen Zeitraums kommuniziert werden muss.[149] Generell sollte sich der Bericht auf das Wesentliche beschränken, das einzelne Risiko und die getroffenen Maßnahmen aber in aller Ausführlichkeit behandeln.[150]

---

[145] Vgl. Klempt (2007), S. 90f
[146] Vgl. ebd., S. 90
[147] Vgl. ebd., S. 91
[148] Vgl. Junginger (2005), S. 299
[149] Vgl. Wildemann H. (2006), S. 62
[150] Vgl. ebd., S. 60f

7.5 Zusammenfassung

Um Risiken effizient zu steuern, sind Vorgaben aus der Risikostrategie und die Ergebnisse der Risikoidentifizierung sowie Risikobewertung zu berücksichtigen. Im siebten Kapitel wurden die Strategieoptionen der Risikosteuerung vorgestellt und verdeutlicht Ebenfalls wurde auf eine besondere Bedeutung der Wirtschaftlichkeit von Steuerungsmaßnahmen hingewiesen. Den Abschluss bildete die Risikokontrolle, welche sowohl die operative als auch die strategische Prozessebene betrachtete. Daneben wurde auf eine gesonderte Bedeutung der Dokumentation verwiesen.

8 Zusammenfassung und Ausblick

In dieser Arbeit wurden zunächst die Grundlagen des Risikomanagements betrachtet. Dabei wurden wichtige Begrifflichkeiten erläutert und definiert. Dann wurde aufgezeigt, wie die Prozesse eines Risikomanagementsystems aussehen und diese einführend erklärt. Im Anschluss wurden regulatorische und rechtliche Anforderungen an die Durchführung erläuterte. Das Kapitel vier widmete sich der Frage, ob es Ansätze gibt, die einem Unternehmen bei der Ein- und Durchführung eines IT-Risikomanagementsystems Hilfestellungen aufzeigen können und dieses bei allen Phasen des IT-Risikomanagements unterstützt. Mit dem Kapitel vier wurde der strategische Teil des IT-Risikomanagements abgeschlossen. Anschließend erfolgte die operative Ausgestaltung der einzelnen Prozesse und es wurden Methoden und Ansätze zur Identifikation, Bewertung und Steuerung sowie Kontrolle aufgezeigt.

Aufgrund der Schnelllebigkeit innerhalb des IT-Umfeldes, ist eine gesonderte Betrachtung der Risiken aus diesem Bereich gerechtfertigt. Der Rahmen, in dem ein IT-Risikomanagement eingeführt werden soll, konnte sowohl strategisch als auch operativ aufgezeigt werden. Dabei ist jedoch zu beachten, dass die vorgeschlagenen Ansätze und Methoden lediglich als Hilfestellung für ein unternehmensindividuelles IT-Risikomanagementsystem zu sehen sind. Es wurde versucht, das IT-Risikomanagement in der Gesamtheit zu betrachten und es konnte anhand dieser Betrachtungsweise kein allgemeingültiges Modell entwickelt werden. Auch gibt es an einigen Stellen Schwierigkeiten bei der Umsetzung. Bei der Identifikation von IT-Risiken kann nicht sichergestellt werden, dass alle für das Unternehmen relevanten Risiken erfasst werden. Ebenfalls kann die Verflechtung der Risiken untereinander und im Unternehmen nicht definiert werden. In der Risikobewertung ist, aufgrund unzureichender oder fehlender Daten, nicht sichergestellt, dass jedes Risiko adäquat bewertet wird.

Die Aufgabe des IT-Risikomanagements ist es, die Risikostrategie mit Hilfe geeigneter Maßnahmen umzusetzen, nach außen zu Kommunizieren und eine Reduzierung der Risiken, bei gleichzeitiger Chancenwahrung, durchzusetzen. Durch die Chancenwahrung ist es ebenfalls Teil der Wertschöpfungskette im Unternehmen.

Im Lagebericht zur IT-Sicherheit in Deutschland[151] werden bestimmte Entwicklungen thematisiert, die die Aufgaben eines IT-Risikomanagementsystems in Zukunft tangieren könnten. Dabei werden im speziellen Hypervernetzung und Umweltschutz im IT-Umfeld gesehen. Beide Aspekte bergen Risiken, die es zu erfassen gilt aber auch gewaltige Chancen für Unternehmen. Ebenfalls sieht das BSI Unsicherheiten bezüglich tech-

[151] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2009), S. 47ff

nischer Trends wie Sicherheit in drahtlosen Sensornetzwerken und rechtlichen Trends wie künftig stärkerer gesetzlicher Regulierung.

All diese Unsicherheiten und Chancen stellen für das Risikomanagement im Allgemeinen und das IT-Risikomanagement im Speziellen, eine große Herausforderung für die Zukunft dar. Das betrifft sowohl national agierende wie auch global agierende Unternehmen.

Literaturverzeichnis

Ahrendts, Fibian; Marton Anita (2008): IT-Risikomanagement leben! Springer-Verlag: Berlin 2008

Baseler Ausschuss für Bankenaufsicht, Internationale Konvergenz der Kapitalmessung und Eigenkapitalanforderungen: Juni 2004: http://www.bundesbank.de/download/bankenaufsicht/pdf/eigenkapitalempfehlung_de.pdf, Aufgerufen am 03.07.2010

Beims, Martin (2009): IT-Service Management in der Praxis mit ITIL 3. Hanser Fachbuch: München 2009

Brink, Gerriet Jan van den; Romeike, Frank (2005): Corporate Governance und Risikomanagement im Finanzdienstleistungsbereich. Schäffer-Poeschel: Stuttgart 2005

Buchsein, Ralf; Victor Frank; Günther Holger; Machmeier Volker (2008): IT-Management mit ITIL® V3. Vieweg+Teubner: Wiesbaden 2008

Bundesamt für Sicherheit in der Informationstechnik (2008-1): BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS). Version 1.5, Bonn 2008

Bundesamt für Sicherheit in der Informationstechnik (2008-2): BSI-Standard 100-2: IT-Grundschutz Vorgehensweise. Version 2.0, Bonn 2008

Bundesamt für Sicherheit in der Informationstechnik (2008-3): BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz. Version 2.5, Bonn 2008

Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz: https://www.bsi.bund.de/cln_165/DE/Themen/ITGrundschutz/StartseiteITGrundschutz/startseiteitgrundschutz_node.html, Aufgerufen am 03.05.2010

Bundesamt für Sicherheit in der Informationstechnik (2009): IT-Grundschutz-Kataloge. 11 Ergänzungslieferung, Bonn 2009

Bundesamt für Sicherheit in der Informationstechnik (2009): Die Lage der IT-Sicherheit in Deutschland 2009, Bonn 2009

Bundesministerium der Justiz: Aktiengesetz: http://www.gesetze-im-internet.de/aktg/__91.html, Aufgerufen am 07.06.2010

Burger Anton, Buchhart Anton (2002): Risiko-Controlling. Oldenbourg: München 2002

CobiT Mapping: Overview of International IT Guidance: http://www.sox-expert.com/uploads/files/COBIT%20Mapping%202nd%20Edition.pdf, Aufgerufen am 13.07.2010

Creditreform: Wirtschaftslage und Finanzierung im Mittelstand Frühjahr 2007: http://www.creditreform.de/Deutsch/Creditreform/Presse/Archiv/Wirtschaftslage_Mittelstand_DE/2007-04/2007-04-04_Wirtschaftslage_Mittelstand_DE.pdf, Aufgerufen am 20.06.2010

Ebel, Nadin (2008): ITIL V3 Basis-Zertifizierung. Addison-Wesley: München 2008

Eisele, Burkhard (2004): Value-at-Risk-basiertes Risikomanagement in Banken. Deutscher Universitätsverlag: Wiesbaden 2004

Exner-Merkelt, Karin: Die historische Entwicklung des Risikomanagements: http://www.oeci.at/wissensportal/die-historische-entwicklung-des-risikomanagements-53/, Aufgerufen am 07.06.2010

Fiege, Stefanie (2006): Risikomanagement- und Überwachungssystem nach KonTraG. Deutscher Universitäts-Verlag: Wiesbaden 2006

Filipiuk, Bogna (2008): Transparenz der Risikoberichterstattung. Gabler Verlag: Wiesbaden 2008

Gleißner Werner (2008): Grundlagen des Risikomanagements. Vahlen Verlag: München 2008

Hechenblaikner, Anja (2006): Operational Risk in Banken. Deutscher Universitäts-Verlag: Wiesbaden 2006

Holler, Manfred (2008): Einführung in die Spieltheorie. Springer-Verlag: Berlin 2008

Junginger Markus (2005): Wertorientierte Steuerung von Risiken im Informationsmanagement. Deutscher Universitäts-Verlag: Wiesbaden 2005

Klempt, Peter (2007): Effiziente Reduktion von IT-Risiken im Rahmen des Risikomanagementprozesses. Institut für Sicherheit im E-Business (IESB): Bochum 2007

Köhler, Peter T. (2005): ITIL. Springer-Verlag: Berlin 2005

Kontio, Jyrki.: The Riskit Method for Software Risk: http://www.soberit.hut.fi/~jkontio/riskittr.pdf, Aufgerufen am 03.05.2010

Königs, Hans-Peter (2006): IT-Risiko-Management mit System. Vieweg+Teubner Verlag: Wiesbaden 2006

Krcmar, Helmut (2005): Informationsmanagement. Springer Verlag: Berlin 2005

Laux, Helmut (2003): Entscheidungstheorie. Springer Verlag: Berlin 2003

Müller-Reichhart, Matthias (1994): Empirische und theoretische Fundierung eines innovativen Risikoberatungskonzepts. Versicherungswirtschaft: Karlsruhe 1994

Piaz, Jean-Marc (2002): Operational Risk Management bei Banken. Versus: Zürich, 2002.

Prokein, Oliver (2008): IT-Risikomanagement: Identifikation, Quantifizierung und wirtschaftliche Steuerung. Gabler Verlag: Wiesbaden 2008

Rosenkranz, Friedrich; Missler-Behr Magdalena (2005): Unternehmensrisiken erkennen und managen. Springer Verlag: Berlin 2005

Raab, Peter; Siegl, Marcus (2006): Nutzung von Kundendaten zur Minimierung des Forderungsausfallrisikos im Distanzhandel. Erschienen in: Wirtschaftsinformatik, Volume 49 Number 1, S. 34-41, 2007

Romeike Frank, Finke Robert (2003): Erfolgsfaktor Risiko-Management, Wiesbaden 2003

Scherpereel, Peter (2006): Risikokapitalallokation in dezentral organisierten Unternehmen. Deutscher Universitäts-Verlag: Wiesbaden 2006

Schierenbeck, Henner (2001): Ertragsorientiertes Bankmanagement - Band 2. Gabler Verlag: Wiesbaden 2001

Seibold Holger (2006): IT-Risikomanagement. Oldenbourg: München 2006

Statistisches Bundesamt: Genesis-Online : https://www-genesis.destatis.de/genesis/online, Aufgerufen am 01.09.2010

Wack, Jessica (2007): Risikomanagement für IT-Projekte. Deutscher Universitäts-Verlag: Wiesbaden 2007

Wagner, Fred (2000): Risk Management im Erstversicherungsunternehmen: Modelle, Strategien. Versicherungswirtschaft: Karlsruhe 2000

Wiedemann Jochen (2008): IT-Notfallvorsorge im betrieblichen Risikomanagement: Entwicklung eines Gestaltungsmodells unter Berücksichtigung ökonomischer Aspekte am Beispiel einer TK-Unternehmung, Diss., Bochum 2008

Wildemann Horst (2006): Risikomanagement und Rating. TCW Transfer-Centrum GmbH & Co. KG: München 2006

Wolke Thomas (2008): Risikomanagement, 2. Auflage. Oldenbourg: München 2008

Zarnekow, Rüdiger; Hochstein, Axel; Brenner, Walter (2005): Serviceorientiertes IT-Management. Springer-Verlag: Berlin 2005

Zellmer, Gernot (1990)**:** Risiko-Management. Verlag Wirtschaft: Berlin 1990

Zhang, Ying (2010): Information Security Governance : http://bauhaus.cs.uni-magdeburg.de/cms/index/PID/19/EID/428C3A66AAE6195FC125768E00762C42, Aufgerufen am 02.08.2010

Abschließende Erklärung

Ich versichere hiermit, dass ich die vorliegende Diplomarbeit selbständig, ohne unzulässige Hilfe Dritter und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht.

Magdeburg, den 24. September 2010