VERWALTUNGS- UND WIRTSCHAFTSAKADEMIE
UND BERUFSAKADEMIE GÖTTINGEN
Frau Professor Dr. Antje Britta Mörstedt

Analyse des IT-Risikomanagements im Hinblick auf Wirtschaftlichkeitsaspekte

Thesis

Guido Helbich
Zielhecke 13
37339 Worbis

BW11.W.049

13. Mai 2014

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

AG	Aktiengesellschaft
AktG	Aktiengesetz
Basel II/III	Regelwerk des Basler Ausschuss für Bankenaufsicht
BDSG	Bundesdatenschutzgesetz
BSC	Balance Score Card
BSI	Bundesamt für Sicherheit in der Informationstechnik
CEO	Chief Exekutive Officer (Geschäftsführer)
CISO	Chief Information Security Officer (Informationssicherheitsbeauftragter)
CobiT	Internationales Framework für die IT-Governance
CSF	Critical Sucess Factor Kennzahl des CobiT-Framework
DV	Datenverarbeitung
E- Commerce	Elektronische Mark- und Handelsplätze
E- Shops	Elektronische Handelsplätze
ETA	Event Tee Analysis- Ereignisbaumanalyse
EU	Europäische Union
EuroSOX	Europäische Norm des SOX
FMEA	Fehlermöglichkeits- und Einflussanalyse
GdPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GmbH	Gesellschaft mit beschränkter Haftung
GoBS	Gesetz ordnungsgemäßer DV-gestützter Buchführungssysteme
HGB	Handelsgesetzbuch
IKS	Internes Kontrollsystem
IM	Informationsmanagement
ISMS	Informationssicherheits- Managementsystem
ISO/IEC	Normen der Internationalen Organisation für Normungen
IT	Informationstechnik/ -technologie
Jh.	Jahrhundert
KGI	Key Global Indikator Kennzahl des CobiT-Framework
KonTraG	Gesetz zur Kontrolle und Transparenz in Unternehmen
KPI	Key Performance Indikator Kennzahl des CobiT-Framework
Mrd.	Milliarde
n.Chr.	nach Christi
PC	Personal Computer
RiskIT	Bestandteil des CobiT-Framework

RM	Risikomanagement
ROI	Return on Investment
ROSI	Return on Security Investment-Kennzahl
RPZ	Risikoprioritätszahl
SLA	Service Level Agreement
SOX	Sarbanes Oxley Act
SÜG	Sicherheitsüberprüfungsgesetz
TBO	Total Benefit of Ownership
TCO	Total Cost of Ownership
TDDSG	Teledienstedatenschutzgesetz
UN	Unternehmen
UrhG	Urheberrechtsgesetz
ValIT	Bestandteil des CobiT-Framework
VaR	Value at Risk-Kennzahl
VPN	Virtual Privat Network- Netzwerkschnittstelle die eine sichere Datenverschlüsselung erlaubt

1 Einleitung

1.1 Ausgangssituation und Problemstellung

Die Informationstechnologien nehmen einen hohen Stellenwert in unserem Alltag und Umfeld ein.[1] Die anfängliche recht einseitige Funktion einer reinen Datenverarbeitung in den Unternehmen, vorrangig zu buchhalterischen Zwecken, ist in der heutigen Zeit umfangreichen und komplexen Einsatzmöglichkeiten der IT gewichen.[2] Für eine Vielzahl von Unternehmen prägt der Einsatz von IT-Systemen das gesamte Geschäftsfeld und ist damit ein wesentliches Element im wirtschaftlichen Wettbewerb. Darüber hinaus ist die Globalisierung der Märkte eine größer werdende Herausforderung für die Unternehmen.[3] In der Hinsicht kann die Informationstechnologie in den Unternehmen eine effektivere, effizientere und schnellere Reaktion auf sich global verändernde Marktsituationen ermöglichen.[4] Der stetige Zuwachs der Nutzung von Computertechnik in Unternehmen, der zurzeit bei 88% liegt, untermauert die Aussage einer weiten Verbreitung von IT-Systemen. Das zeigt die Auswertung der Statistica Datenbank des Statistischen Bundesamtes.[5]

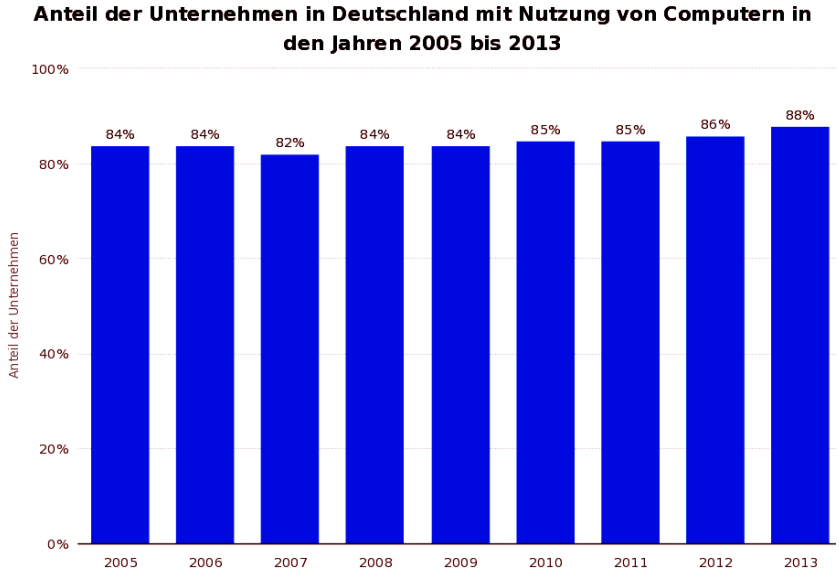

Abbildung 1: Computernutzung in deutschen Unternehmen von 2005- 2013
Quelle: Statistisches Bundesamt, S.1.

[1] Vgl. Eckert: IT, S.3.
[2] Vgl. Gadatsch: Masterkurs, S. 35.
[3] Vgl. Knoll: Praxisorientiertes, S V.
[4] Vgl. Tiemeyer: IT, S.1.
[5] Vgl. Statistisches Bundesamt: Anteil, S.1.

So ergeben sich aus der Nutzung der Informationstechnologien mehr Chancen im Wettbewerb, aber auch ein höheres Risiko. Insbesondere die zunehmende Vernetzung und die dadurch steigende Verwundbarkeit der Datensysteme, führen zu einer schnell variierenden Risikolandschaft. Die Datenverarbeitung hängt im hohen Maße von der Verfügbarkeit, Zuverlässigkeit und Vertraulichkeit, der eingesetzten IT-Systeme ab.[6] Darin erkennen auch die Unternehmen ein hohes IT-Risikopontential, was durch eine 2010 veröffentlichte Studie des TÜV Süd und der Hochschule Deggendorf bekräftigt wird. Hierin bewerten 528 Unternehmer des Mittelstandes die IT-Risiken mit 45%. Zu den wesentlichen Risiken zählen nach Meinung der Befragten Betriebsstörungen der IT-Systeme, Datenverluste, Datenmissbrauch durch Mitarbeiter oder fremde Personen, mangelhafte Datenverschlüsselung und Datensicherung sowie Schadsoftware.[7]

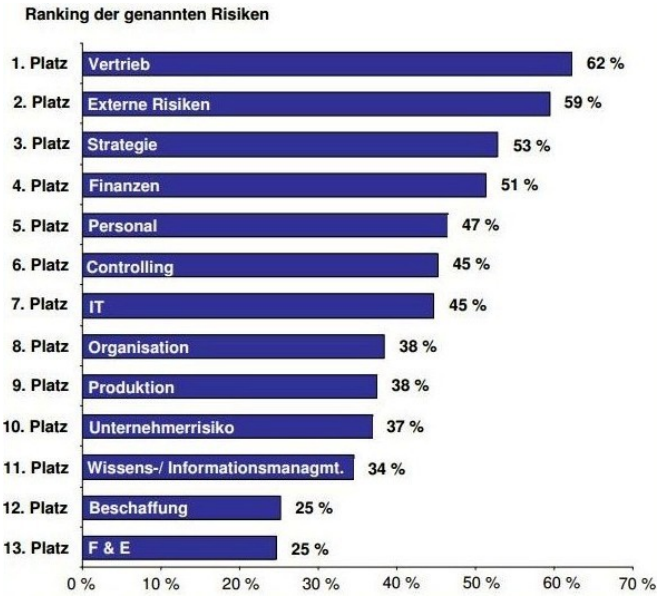

Abbildung 2: RCM Studie des TÜV-Süd und der Hochschule Deggendorf
Quelle: TÜV-Süd: Studie RCM Mittelstand, S.13.

Die IT-Systeme und deren Prozesse stellen darüber hinaus in vielen Unternehmen einen erheblichen Kostenfaktor dar.[8] Die Risiken sollten damit in diesem Bereich auf ein vertretbares Maß reduziert werden. Die Umsetzung dieses Zieles kann mit Hilfe eines ganzheitlichen wertorientierten IT-Risikomanagement ermöglicht werden.[9]

[6] Vgl. BSI: IT, S.15f.
[7] Vgl. TÜV-Süd: Studie, S.13.
[8] Vgl. FH-Kiel: Studie, S.6.
[9] Vgl. Junginger: Werteorientierte; S.3.

Die Komplexität der Informationstechnologie und deren Prozesse, gesetzliche Normen (z.B. KonTraG) und zu realisierende Standards fordern entsprechende Risikomanagementsysteme. Die Ausgestaltung, Betreibung und Verbesserung des Risikomanagements ist die Aufgabe der jeweiligen Entscheidungsträger eines Unternehmens.[10]

Die hier als Ausgangspunkt geschilderten Sachverhalte und Probleme, werfen die folgende Fragestellung auf.

Wie gestalten sich der Aufbau und die Prozesse eines modernen wertorientierten IT-Risikomanagements, das wesentlichen Zielsetzungen eines Unternehmens, wie Kostensenkung, Gewinnmaximierung und einem professionellen Risikomanagement gerecht wird?

1.2 Ziel der Arbeit

Um die zuvor hergeleitete Fragestellung beantworten zu können, verfolgt die Arbeit zwei wesentliche Aufgaben. Das erste Ziel soll die detaillierte Darstellung des IT-Risikomanagements und seiner Prozesse sein. Dazu nutzt diese Arbeit eine zielführende Struktur, um dem Leser eine bessere Übersicht zu verschaffen. So werden zunächst wesentliche Begriffe und Grundlagen erörtert, die für jedes Risikomanagement gelten. Der daraus gewonnene Erkenntnisstand bildet die Basis, um die Besonderheiten des Aufbaus und die Umsetzung eines IT-Risikomanagementsystems darzustellen. Dazu werden bedeutende Elemente und Bedingungen für ein spezifisches IT-Risikomanagement und dessen Prozess erläutert. Des Weiteren beschreibt die Arbeit mögliche organisatorische und personelle Strukturen und geht auf wesentliche rechtliche und regulatorische Anforderungen ein. Die Implementierung, Weiterführung, Ausbau und Verbesserung des IT-Risikomanagements soll anhand wesentlicher Standards und Regelwerke erläutert werden. Dabei werden diese Best-Practice- Methoden auf ihren Nutzen bei einer Installierung und Weiterführung eines IT-Risikomanagements untersucht. Im weiteren Verlauf soll der geneigte Leser durch eine vertiefende Beschreibung des IT-Risikomanagementprozesses für dessen Bedeutung sensibilisiert werden. Der IT-Risikomanagementprozess ist in vier Prozessabschnitte selektiert, die der Identifikation, Bewertung, Steuerung und Kontrolle von Risiken dienen. So werden sukzessive die einzelnen Prozessabschnitte analysiert und wesentliche Merkmale, Bedingungen, Methoden und Ziele erläutert.

[10] Vgl. Ebert: Risikomanagement, S.92f.

Die zweite wesentliche Zielsetzung der Arbeit ist eine kritische Betrachtung von wirtschaftlichen Aspekten und die Thematisierung eines ökonomischen Handelns. Dazu zählt sowohl eine Kosten-Nutzen-Betrachtung des IT-Risikomanagements an sich, als auch die an den UN-Zielen orientierte ökonomische Bewirtschaftung (Steuerung) der Risiken. Dafür werden wesentliche Methoden und Verfahren auf ihre Merkmale, Einsatzmöglichkeiten und Nutzen analysiert. Eine genaue Erläuterung von bedeutenden Kennzahlen dient dabei einer tiefgründigen Analyse der wirtschaftlichen Aspekte. Am Beispiel des Outsourcings wird kritisch eine moderne Methode der Kostenregulierung und Risikosteuerrung erörtert.

1.3 Aufbau der Arbeit

Die Arbeit ist in sechs Kapitel strukturiert. Dem ersten Kapitel, der Einleitung, folgt im Kapitel zwei die Definition und Beschreibung wesentlicher Begriffe des allgemeinen Risikomanagementsystems. Diese dienen als Grundlage, um im weiteren Verlauf des zweiten Kapitels, bedeutende Begrifflichkeiten des IT-Risikomanagements gezielt zu analysieren und zu definieren. Das dritte Kapitel befasst sich mit wesentlichen Anforderungen an das IT-Risikomanagements. Dazu zählen insbesondere bedeutende rechtliche Normen und wesentliche Regelwerke und Standards. Dafür werden sowohl für alle Risikomanagements bedeutende Rechtsnormen betrachtet, als auch für das IT-Risikomanagement spezifische Regelungen. Im Rahmen des vierten Kapitels werden wesentliche Methoden des IT-Risikomanagements erörtert. Dazu werden die einzelnen Stufen des IT-Risikomanagementprozesses analysiert, mit dem Ziel die Methoden und Aufgaben der Identifizierung, Bewertung, Steuerung und Kontrolle von Risiken detailliert zu beschreiben und zu bewerten. Das fünfte Kapitel befasst sich mit der wirtschaftlichen Betrachtung des IT-Risikomanagements. Dabei wird sowohl das IT-Risikomanagement selbst, als auch die Steuerung der Risiken unter dem ökonomischen Blickwinkel betrachtet und bewertet. Ein Resümee und die daraus hergeleiteten Erkenntnisse bilden im sechsten Kapitel den Abschluss der Arbeit.

2 Grundlagen

2.1 Definition vom IT-Risikomanagement

Der Begriff des Risikos wird in den Bereichen Wirtschaft, Politik, Wissenschaft und Gesellschaft unterschiedlich definiert. Es gibt jedoch eine mehrfache Übereinstimmung, „Risiko“ bedeutet eine negative Abweichung von einem zu erwartenden Ziel.[11] Das Risiko lässt sich etymologisch sowohl auf das griechische „rhiza“ als auch auf das vulgärlateinische „resecum“ zurückführen, beide Wörter beschreiben damit die „Klippe“,[12] die empfehlenswerter Weise zu umfahren ist.

Einer Vielzahl von Risiken stehen auch immer gewisse Chancen gegenüber, als fassliches Beispiel wären Spekulationen an der Börse bzw. das Glücksspiel zu nennen. Die Chance ist als positive Abweichung von einem bestimmten Ziel zu sehen.[13] Der Aufbau von Chancen soll hier jedoch nicht weiter erörtert werden. Im Folgenden soll anhand von ausgewählten Definitionen der Risikobegriff weiter erläutert werden. Darüber hinaus bietet die Literatur weitere Ansätze zur Bestimmung des Risikobergriffs.

Die extensiv orientierte Definition sieht das Risiko in den Begleitumständen, die sich aus dem wirtschaftlichen Handeln eines jeden Unternehmens ergeben, z.B. in Form von Kapital- oder Vermögensverlusten oder entgangener Gewinne. Das Risiko liegt hier in der Gefahr eines Misserfolgs und wird umgangssprachlich als unternehmerisches Risiko beschrieben.[14]

Der informationsorientierte Risikobegriff bezieht sich auf das Entstehen eines Risikos durch den Mangel an Informationen. Dabei spielen Unsicherheit, Ungenauigkeit und Unvollständigkeit an Informationen die entscheidende Rolle.[15]

In der entscheidungsorientierten Auffassung werden die Ursache und der Umfang einer Risikosituation betrachtet. Es wird auf die Fähigkeit der handelnden Akteure gesetzt, vorliegenden oder zukünftigen Umweltsituationen, Eintrittswahrscheinlichkeiten zuzuordnen.[16]

---

[11] Vgl. Diederichs: Risikomanagement, S.8; Dransfeld: Risiken, S.6; Hohrath: Analyse, S.102.
[12] Vgl. Köbler: Deutsches, S.344.
[13] Vgl. Königs: IT, S.10.
[14] Vgl. Siepermann: Risikokostenrechnung, S.13.
[15] Vgl. Nguyen: Handbuch, S.7.
[16] Vgl. Wolke: Risikomanagement, S.1.

Der ausfallorientierte Risikobegriff sieht ein Risiko in der Gefahr einer negativen Abweichung eines existierenden Ergebnisses von dem gesetzten bzw. prognostizierten Ergebniswert.[17] Die möglichen Chancen bleiben bei der ausfallorientierten Risikomessung unbeachtet. Das Ausfallrisiko zählt zu den Finanzrisiken eines Unternehmens. Eine Kennzahl von großer Bedeutung ist der „Value at Risk". Er beschreibt den Schaden, der unter üblichen Bedingungen innerhalb einer Periode mit einer gegebenen Wahrscheinlichkeit nicht überschritten wird.[18] IT-Risiken werden in der Literatur teilweise diesem Risikobegriff unterstellt (z.B. bei E-Commerce UN)[19] primär aber den operationellen Risiken zugeordnet.[20]

Mit dem Risiko ist in der heutigen Zeit häufig auch der Begriff des Risikomanagements eng verknüpft. Das erweckt den Eindruck es handele sich um ein neuzeitliches Phänomen. Im weitesten Sinne reicht der Begriff des Risikomanagement jedoch bis in die Antike zurück. Die Menschen versuchten ihr Schicksal gegenüber den Göttern durch gezielte Opfergaben positiv zu beeinflussen. Mit der Verbreitung des arabischen Zahlensystems um 1000 n.Chr. wich das Schicksalhafte immer mehr der Logik. Später entwickelte Luca Pacioli 1494 in seinem Werk „ Summa de arithmetic, geometrica et proportionalica" erstmals die Quantifizierung der Risiken beim Glücksspiel und erfand darüber hinaus die doppelte Buchführung. Am Ende des 19. Jh. führten Francis Galton und Karl Pearson mit der Korrelation und der Regression zwei statische Maße ein, die heute bei der Risikoanalyse eine wichtige Rolle spielen und somit eine große Bedeutung für das Risikomanagement besitzen.[21] In der Mitte des 20. Jh. wurde der Begriff des Risikomanagement häufig im Zusammenhang mit Versicherungen genannt. Dabei ging es im Wesentlichen darum, Versicherungen kostenmoderat abzuschließen oder gänzlich auf sie verzichten zu können. Es stand primär im Vordergrund äußerliche Risiken des Unternehmens abzusichern, intern entstandene Risiken, bedingt durch Fehlentscheidungen des Managements blieben mehrfach unberücksichtigt.[22] Infolgedessen entwickelte sich die Erkenntnis auch unternehmensinterne Risiken zu quantifizieren und qualifizieren und entscheidungsabhängige Risiken mit einzubeziehen, wodurch das Risikomanagement

[17] Vgl. Wolke: Risikomanagement, S.156f.
[18] Vgl. Königs: IT, S.31.
[19] Vgl. Knoll: IT, S.15.
[20] Vgl. Kersten/ Reuter/ Schröder: IT, S.5; Prokein: IT, S.10; Seibold: IT, S.10.
[21] Vgl. Stiefl: Risikomanagement, S.13.
[22] Vgl. Hartmann: Einkaufsmanagement, S.21.

eine stetige Entwicklung vollzog. Mit der Konsequenz, dass in den Unternehmen heute ein umfassendes Risikomanagement, welches viele Unternehmensbereiche abdeckt, inkludiert ist. Die Grundstruktur des Risikomanagements setzt sich aus einem strategischen Bereich und einem operativen Bereich zusammen. Der Inhalt der strategischen Ebene ist die Konzeption der Risikopolitik und Risikostrategie im Bezug auf die Unternehmensziele. Im operativen Segment findet die Bearbeitung der Risiken auf der Basis risikostrategischer Vorgaben gemäß dem Risikomanagementprozess statt.[23] Damit ist das Risikomanagement funktional in die Unternehmensleitung integriert und realisiert das systematische Erkennen, Analysieren, Lenken, Überwachen und Beseitigen von Risiken, die die Existenz der Unternehmung bedrohen. Um diese komplexe Aufgabenstellung zu realisieren, bedarf es einen durch die Mitarbeiter getragenen und durch das Management unterstützenden Prozesses. Dieser Risikomanagementprozess ist an das Ziel gekoppelt, den Fortbestand des Unternehmens zu sichern.[24]

2.2 Wesentliche Bedingungen zur Implementierung des IT-Risikomanagement

Eine wichtige Vorrausetzung für ein funktionierendes, ganzheitliches Risikomanagement ist die Ausgestaltung durch ein Risikomanagementsystem. Es beinhaltet die aufbau- sowie ablauforganisatorischen und technischen Richtlinien im Bezug auf den Umgang mit Risiken und darüber hinaus klare Kompetenzstrukturen. Das Risikomanagementsystem unterscheidet sich in seiner Steuerungs- und Führungsfunktion von der Umsetzungsfunktion des Risikomanagementprozesses. Die Bestimmung von Zielen und Geltungsbereichen, das systematische Umsetzen von Vorgaben, die Kontrolle des Systems und dessen Wirksamkeit sowie das Einleiten von Verbesserungen sind Bestandteile der Führungsfunktion.[25] Der Umfang und Ausbau des Risikomanagementsystems ist in einem erheblichen Maß von der Unternehmensgröße und -struktur, deren Komplexität und Risikobereitschaft sowie gesetzlichen Vorgaben abhängig.[26]

[23] Vgl. Königs: IT, S.109.
[24] Vgl. Strohmeier: Ganzheitliches, S.45- 47.
[25] Vgl. Wiederkehr/Züger: Risikomanagementsystem, S.17.
[26] Vgl. Buchhard/Burger: Risiko, S.260.

Die Informationstechnologie ist ein allgegenwärtiger Bestandteil des gesellschaftlichen, politischen und wirtschaftlichen Umfelds.[27] Demzufolge werden auch in den Unternehmen wichtige Prozesse durch die IT unterstützt, dazu zählen z.B. Beschaffung, Absatz, Finanzierung, Produktion und Verwaltung. Die IT-Systeme sind darüber hinaus oft sehr komplex und kostenintensiv und bedürfen in ihrer Anwendung einer großen Fachkompetenz.[28] Darüber hinaus erfordern die wesentlichen Schutzziele der IT, wie Vertraulichkeit, Integrität, Verfügbarkeit und Zurechenbarkeit, das Höchstmaß an Risikominimierung.[29] Darum gilt es, mit Hilfe eines gezielt abgestimmten Risikomanagements die Funktion von IT-Systemen und der IT-Sicherheit in einem Unternehmen sicher zustellen. Um dieses Ziel zu erreichen, sollte ein integratives IT-Risikomanagement in das gesamte Betriebsmanagementsystem eingegliedert werden. Unternehmen die dem IT-Risikomanagement eine hohe Beachtung schenken und dessen Prozesse kontinuierlich restrukturieren, sind wirtschaftlicher als UN die nur in Krisenzeiten reagieren. Das IT-Risikomanagement wird dabei von anderen Managementsystemen, wie zum Beispiel dem Qualitätsmanagement, dem Informationssicherheits-Management und dem klassischen Risikomanagement flankiert. Viele Unternehmensbereiche besitzen oft eine hohe Abhängigkeit von den IT-Systemen, daher entsteht für das IT-Risikomanagement eine wichtige Rolle im gesamten Managementsystem.[30]

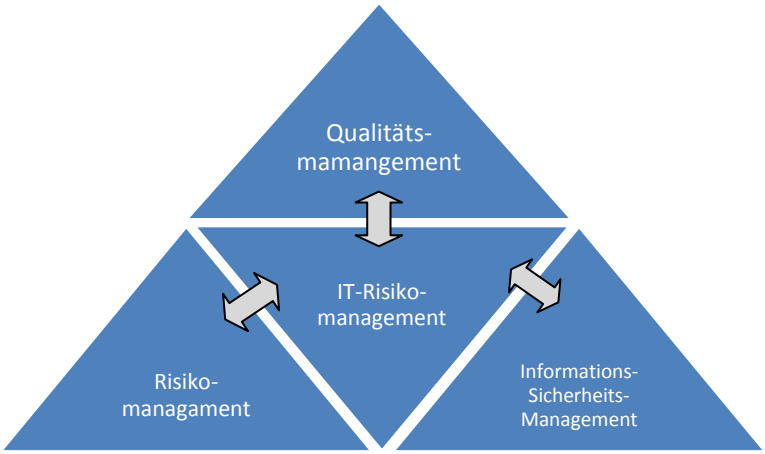

Abbildung 3: Beispiel für eine Managementsystem-Struktur

Eigene Darstellung

[27] Vgl. Eckert IT, S.3.
[28] Vgl. Tiemeyer: IT-Controlling, S.7.
[29] Vgl. Knoll: IT, S.18f.
[30] Vgl. Lenges: Framework, S.3f.

Um ein IT-Risikomanagement erfolgreich in ein UN einzugliedern, ist es notwendig, primär die Führungsaspekte und Führungsrollen zu definieren.[31] Daraus entstehen klar strukturierte Verantwortlichkeitsbereiche. Eine weitere wichtige Voraussetzung ist es, die IT-Strategie in Übereinstimmung mit den Zielen und Strategien des ganzen UN zu bringen. Daraus wird eine IT-Governance festgelegt. Dabei ist das IT-Risikomanagement eine mittelbare Schnittstelle zwischen der Risiko-Governance des UN und der IT-Governace. Für das IT-Risikomanagement gilt es die erforderliche IT-Risikotransparenz herzustellen, Vorrausetzung hierfür ist, neben der Sensibilisierung der Mitarbeiter, das IT-Krisenmanagement, die IT-Risikosteuerung, sowie die IT-Risikokultur.[32] Durch das Erkennen und Dokumentieren von Ursache- Wirkungs-Beziehungen ergibt sich die benötigte Risikotransparenz. In einigen Fällen lässt sich die Transparenz leider erst erstellen, wenn das Risiko eingetreten ist.[33]

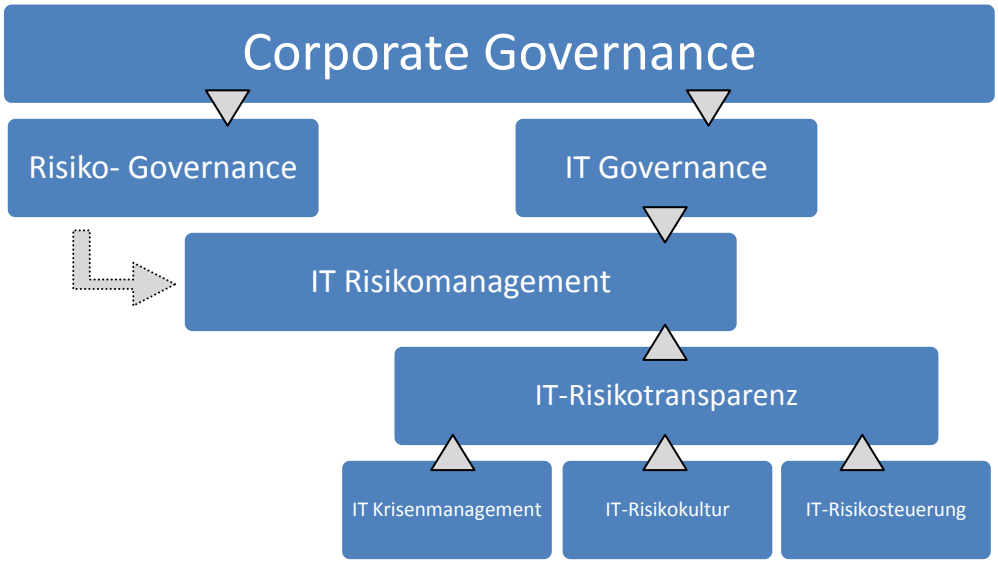

Abbildung 4: Integration des IT-Risikomanagement
Eigene Darstellung

Der Schaden ist ein wichtiger Begriff im Zusammenhang mit dem Risikomanagement im Allgemeinen und dem IT-Risikomanagement im Speziellen. Um ein Risiko einschätzen zu können, ist es wichtig die Eintrittswahrscheinlichkeit sowie die Tragweite eines Schadens zu bestimmen. Damit lässt sich für ein Risiko der Risikofaktor bestimmen, der das Produkt aus der Eintrittswahrscheinlichkeit und dem jeweiligen Schadensausmaß ist.[34] In den Kapiteln 4 und 5 dieser Arbeit wird darauf

[31] Vgl. Königs: IT, S.155.
[32] Vgl. Seibold: IT-Risikomanagement, S.7.
[33] Vgl. Knoll: IT, S.32.
[34] Vgl. Strohmeier: Ganzheitliches, S.20.

weiter ausführlich eingegangen. Beachtenswerter Weise muss der Schaden sich nicht unmittelbar in Euro und Cent niederschlagen. Es kann sich zunächst um einen sogenannten Reputationsschaden handeln, der sich eventuell erst später monetär auswirkt.[35] Daher gilt für das IT-Risikomanagement im Rahmen der Funktionssicherheit (safty), der Informationssicherheit (security), der Datensicherheit (protection) und des Datenschutzes (privacy) die Risiken auf ein vertretbares Maß zu reduzieren.[36]

Der Aufbau und die Steuerung des IT-Risikomanagement erfolgt durch definierte Führungsinstrumente, die wiederum bestimmten Führungs- und Kontrollinstanzen zugeordnet werden. Die Struktur bzw. Organisation kann dabei in Abhängigkeit von der Konstellation des UN variieren, elementar ist aber immer die eindeutige Zuordnung von Rollen und Verantwortlichkeiten.[37] So kann beispielsweise die Anzahl von IT-Bereichen die Fragestellung aufwerfen, eine zentrale oder dezentrale Gliederung des IT-Risikomanagement vorzunehmen.[38] Für ein zentrales IT-Risikomanagement spricht die hohe objektive Beurteilung von Risiken, nachteilig wirken sich eine mangelhafte operative Beziehung und die lückenhafte Prozesskenntnis aus. Eine dezentrale Organisationsform in die einzelnen IT-Bereiche hinein sorgt für eine hohe Fachkompetenz und exzellente operative Anbindung, aber durch die isolierte Risikoanalyse fehlt es an dem Erkennen von Wechselwirkungen. Eine Kombination aus beidem ist daher sinnvoll für das IT-Risikomanagement.[39] Der nachfolgend beschriebene RM-Aufbau orientiert sich am ISO/IEC 27001 Standard. Die oberste Ebene bildet die Risiko- und Sicherheitspolitik des gesamten UN und ist z.B. dem Aufsichtsrat zugeordnet oder einer anderen Form der UN-Leitung. In der Ebene der Informationssicherheitspolitik wird Wesentliches des IT-Sicherheits- und Risikomanagement in die Risiko- und Sicherheitspolitik mit einbezogen, um daraus Grundsätze, Ziele und die notwendigen Verantwortlichkeiten zu bilden. Diesem Bereich ist der Führungsinstanz des Geschäftsführers(CEO) zugeordnet. Die sich anschließende Ebene wird durch den Informationssicherheitsverantwortlichen(CISO) gelenkt bzw. kontrolliert und wird durch die Informationssicherheits- Management- Politik, die Informationssicherheits- Weisungs- und Ausführungsbestimmungen, sowie die IT-Sicherheits- Architektur und Standards ausgefüllt. Die IT-Sicherheitskonzepte dienen

[35] Vgl. Kersten/Reuter/Schröder: IT, S.213.
[36] Vgl. Eckert: IT, S.6.
[37] Vgl. Knoll: Praxisorientiertes, S.87.
[38] Vgl. Wolke: Risikomanagement, S.241f.
[39] Vgl. Junginger: Werteorientierte, S.206f.

Systemplattformen, Anwendungen und Prozessen und werden in dieser Ebene durch Systeminhaber und interne Audits kontrolliert.[40] Ein möglicher Organisationsaufbau der Verantwortlichkeiten ist in der folgenden Abbildung dargestellt. In Abhängigkeit vom Umfang und der Bedeutung der IT und der Unternehmensgröße, können einem Verantwortungsträger auch mehrere Rollen zugewiesen werden.[41]

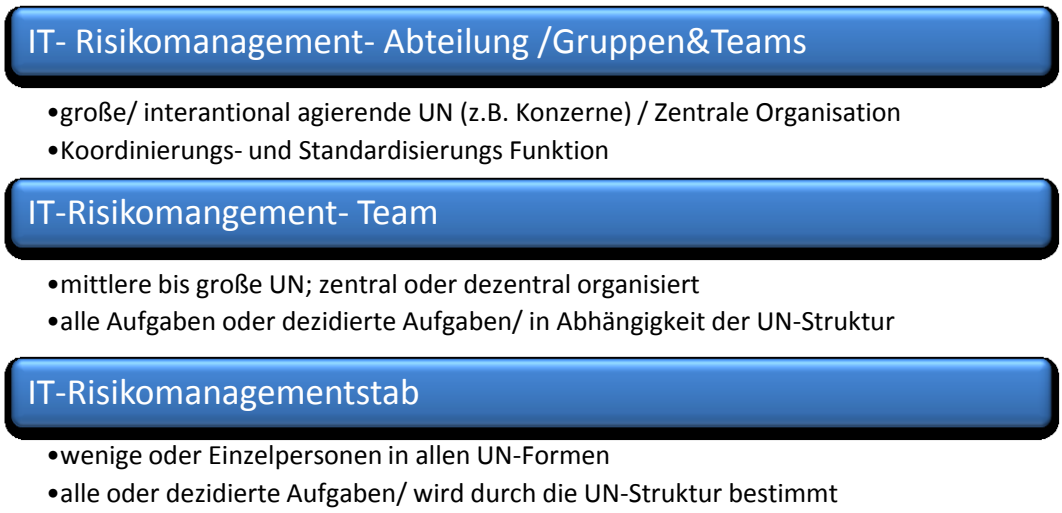

Abbildung 5: IT-Risikomanagement: mögliche Rollenverteilung
Eigene Darstellung (in Anlehnung an Knoll: Praxisorientiertes, S.88.)

Das IT-Risikomanagement adaptiert den bewährten vierphasigen Prozess des allgemeinen Risikomanagement.[42] Dazu gehören der Reihe nach die Identifikation, die Bewertung, die Steuerung und die Kontrolle von Risiken.[43] Ist die erste Phase der IT-Risikoidentifizierung, die gezielt im Kapitel 4.1 betrachtet wird, abgeschlossen, erfolgt in der zweiten Phase anhand von quantitativen und qualitativen Analysen eine Risikobewertung. Auf dazu genutzte Verfahren und Methoden wird in dieser Arbeit im Kapitel 4.2 detailliert eingegangen. Die gewonnen Daten aus der zweiten Phase, werden in der dritten Phase, der Risikosteuerrung, zur Einteilung der Instrumente genutzt. Dies wird im Kapitel 4.3 weiter vertieft, vereinfacht gesagt, geht es bei dieser Einteilung um: Vermeidung, Verminderung, Übertragung und Tolerierung von IT-Risiken. In der vierten und letzten Phase, wird der gesamte Prozess per Soll-Ist-Vergleiche kontrolliert.[44] Hierzu werden organisatorische Fragen und angewandte

[40] Vgl. Königs: IT, S.184.
[41] Vgl. Seibold: IT, S.137.
[42] Vgl. Prokein: IT, S.15.
[43] Vgl. Knoll: Praxisorientiertes, S.123- 152; Ebert: Risikomanagement, S.6- 7.
[44] Vgl. Stiefl: Risikomanagement, S.124.

Messmethoden erörtert, kontrolliert und anhand bestimmter Kennzahlen wirtschaftliche Aspekte beleuchtet. Die ökonomischen Hintergründe sollen ausführlich im 5. Kapitel thematisiert werden.

Dieser beschriebene vierphasige Prozess vollzieht sich in einem Kreislauf.[45] Restrisiken, formale Änderungen oder Neueinschätzungen führen zu einer erneuten Zirkulation, um das bestehende Risiko weiter zu minimieren. Der dargestellte Prozess bildet das Fundament des operativen Risikomanagement, da zeitnah und explizit Ergebnisse verfügbar sind. In der Summe entsteht eine Risikoliste bzw. ein Risikokatalog, wo sämtliche identifizierte Risiken aufgeführt werden.[46]

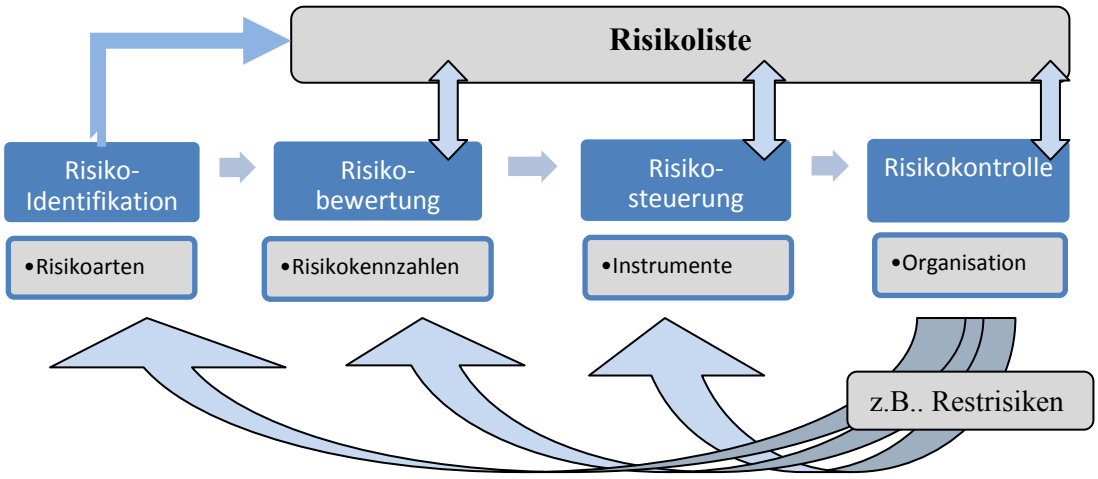

Abbildung 6: (IT)-Risikomanagementprozess
Eigene Darstellung

2.3 Abgrenzung wesentlicher Risikokategorien

Aus den im Kapitel 2.1 dargestellten Risikobegriffen geht hervor, dass sich ein Unternehmen vielen Risiken aussetzt. Sie können z.B. durch Fehlentscheidungen oder einfach aus dem unternehmerischen Handeln entstehen.[47] Diese Mechanismen sind jedoch Grundlage für die Geschäftstätigkeit eines jeden Unternehmens, da risikolos eine Gewinnerwirtschaftung langfristig als unrealistisch erscheint.[48] Ein Misserfolg resultiert jedoch oft aus zu spät erkannten Risiken, die unbeachtet bleiben

[45] Vgl. Wolke: Risikomanagement, S.4f.
[46] Vgl. Ebert: Risikomanagement, S.14.
[47] Vgl. Siepermann: Risikokostenrechnung, S.13.
[48] Vgl. Nguyen: Handbuch, S.5.

oder nicht analysiert werden. Daher wird in den UN ein effizientes Risikomanagement zunehmend thematisiert.[49]

Die Risikokategorien lassen sich unterteilen in: Finanzrisiken, deren Inhalt Liquiditätsrisiken und Erfolgsrisiken sind, sowie operationelle Risiken, zu denen auch IT-Risiken gezählt werden. Den sonstigen operationalen Risiken werden beispielsweise personelle, organisatorische und vor allem externe Risiken unterstellt.[50] Die folgende Grafik zeigt die Struktur von Risikokategorien.

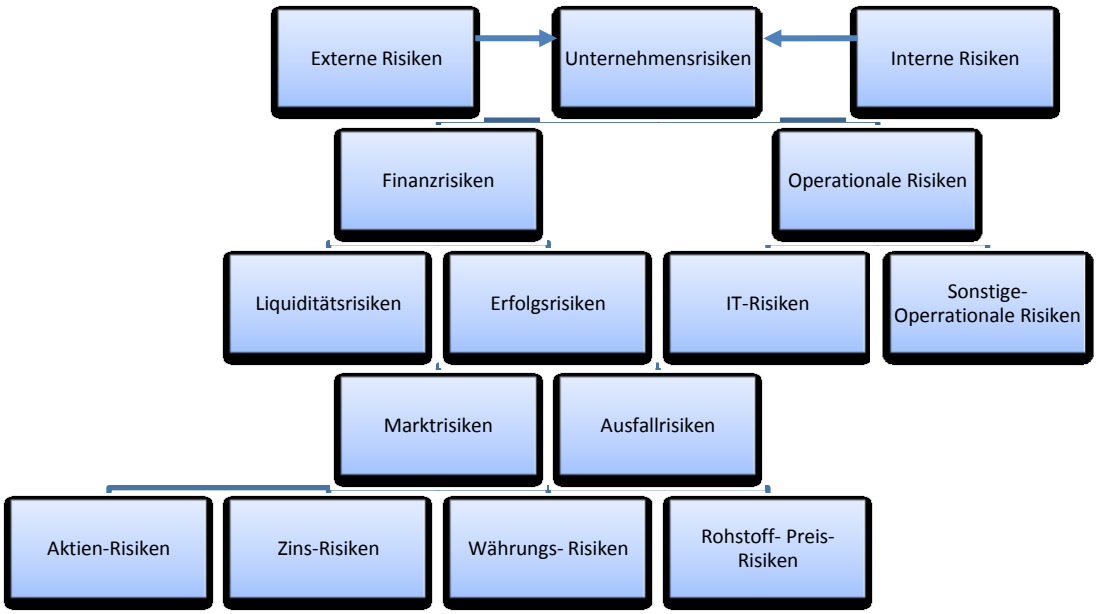

Abbildung 7: Risikokategorien
Eigene Darstellung

Die Abbildung verdeutlicht, die IT-Risiken werden im Bereich der operationalen Risiken eingeordnet. Diese Zuordnung der IT-Risiken entspricht auch dem Regelwerk Basel II/III des Baseler Ausschuss für Bankenaufsicht.[51] Darin wir das operationale Risiko als die Gefahr von Verlusten interpretiert, die auf unangemessene oder versagende interne Prozesse, Menschen, Systeme oder externe Ereignisse zurück zu führen sind. Dabei werden Rechtsrisiken mit eingeschlossen, jedoch Strategische- bzw. Reputationsrisiken ausgeklammert.[52] Eine differenziertere Unterteilung der Risiken ermöglicht eine genaue Zuordnung von Risikoursachen. So ergibt sich eine Unterscheidung in externe und interne Risiken. Den externen Risiken werden z.B. formelle Änderungen, Naturgewalten oder Schäden durch Dritte zu- geschrieben.

[49] Vgl. Wanner: Risikomanagement, S.26.
[50] Vgl. Seibold: IT, S.9f.
[51] Vgl. Kersten/Reuter/Schröder: IT, S.5.
[52] Vgl. Königs: IT, S.85.

Zu den internen Risiken zählen: personelle Risiken (z.B. Missbrauch durch Mitarbeiter oder Bedienungsfehler), Prozessrisiken (z.B. Fehler in System- oder Geschäftsabläufen) sowie Systemrisiken (z.B. Programmfehler, IT-Ausfälle, Trojaner, Viren oder Maleware).[53]

Die Liquiditätsrisiken, die ein Teil der Finanzrisiken darstellen, resultieren aus Zahlungsverpflichtungen, die möglicherweise nicht fristgerecht geleistet werden. Dies führt zu einer Erfolgsminderung des Unternehmens und endet eventuell in einem Verlust. Damit ist häufig auch die Rede von einem Verlustrisiko.[54] Das Ausfallrisiko, welches den Erfolgsrisiken untergeordnet ist, legt die Gefahr einer Nichterfüllung seitens der Vertragspartner zugrunde. Ein Beispiel wäre die Zahlungsverpflichtung von Kunden. Marktrisiken, ebenfalls den Erfolgsrisiken unterstellt, lassen sich ihrerseits in Aktienkursrisiken, Zinsrisiken, Marktpreisrisiken, Währungsrisiken und Rohstoffpreisrisiken aufteilen. Das IT-Risikomanagement in UN weist eher einen geringen Zusammenhang zu den in diesem Absatz genannten Risiken auf. Dies gilt jedoch nicht, wenn die IT als Unternehmen an sich auftritt.[55]

2.4 Wesentliches zum Inhalt der IT- Risikostrategie

Um das IT-Risikomanagement zu gestalten, ist eine IT-Risikostrategie erforderlich. Die Konzeption erfolgt auf der Basis der risikopolitischen Ausrichtung des gesamten Unternehmens sowie der Informationsmanagement-Strategie. Dazu ist es erforderlich, die Sicherheitsziele des Informationsmanagement in der Unternehmensstrategie zu fixieren. Die dadurch entstehenden Grundsätze bilden den Rahmen für die weiteren Maßnahmen und Planungen. Der informelle Inhalt der Risikostrategie gibt Auskunft über die gewollte bzw. prognostizierte Risikobereitschaft des Unternehmens, im Hinblick auf die angestrebten Unternehmensziele. Sowohl exakte Mengenwerte, die in Form von Geldeinheiten den höchsten Erwartungswert des Risikos repräsentieren, als auch qualitative Merkmale, wie Gewinnmaximierung und Kostensenkung ohne den Datenschutz oder die Reputation zu gefährden, können als Sicherheitsziel formuliert werden.[56]

[53] Vgl. Prokein: IT, S.10.
[54] Vgl. Siepermann: Risikokostenrechnung, S.85f.
[55] Vgl. Seibold: IT, S.10.
[56] Vgl. Junginger: Werteorientierte, S.199.

Die Zielformulierungen sind keine statischen Vorgaben, sondern werden vielmehr in Abhängigkeit der Unternehmensgröße skaliert, d.h. sie sind auch in Klein- und Mittelstandsunternehmen umsetzbar. Insbesondere die wertorientierte Unternehmensphilosophie definiert Rentabilität, Wachstum und Risiko als die entscheidenden Zielkomplexe, um ganzheitlich den Fortbestand des Unternehmens zu sichern.[57] Unter dem Gesichtspunkt eines wertorientierten Informationsmanagements lassen sich wesentliche Anteile einer Risikostrategie formulieren: 1.Bestimmung der Risikoneigung, sowie des Risikotragfähigkeitspotenzials (wie hoch darf der maximal zu erwartende quantitative Schaden sein); 2. Aufteilung von Risikoressourcen und Festlegung der IT-Risikomanagementorganisation; 3. konkrete Ziele für Risikoposition und Kontrollmechanismen; 4. Regelung von Kompetenzen und Verantwortlichkeiten und 5. konkrete Mess- und Bewertungsmethoden. Im Bezug auf den Lebenszyklus des Informationsmanagements und den damit verbundenen Risikoarten, sind durch die Risikostrategie Aussagen zu Auswahlentscheidungen (Prozesse, Techniken), Projektrisiken (Kosten, Qualität) sowie Betriebsrisiken (besonders zu schützende Bereiche) zu formulieren.[58] Der in 2.1 beschriebene Risikomanagementprozess ist das Fundament des operativen Risikomanagement und wird im Zuge der Risikostrategie durch eine strategische Komponente erweitert. Oft bilden operativ einzelne identifizierte Risiken in der Summe ein strategisches Risiko. Zudem wird empfohlen, Einflussfaktoren zyklisch in einem Portfolio zu bewerten und Zielvorgaben mittels einer BSC zu dokumentieren.[59]

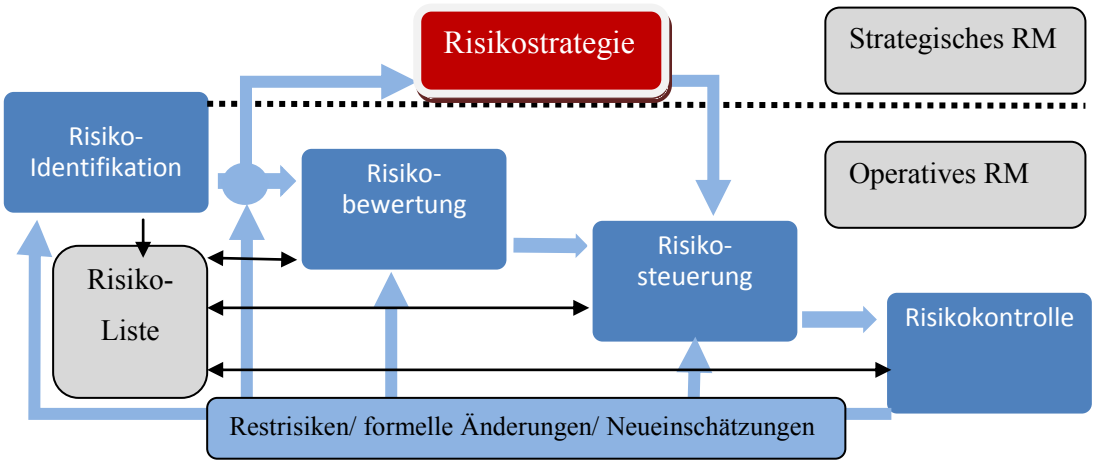

Abbildung 8: Risikostrategie im Risikomanagementprozess

Eigene Darstellung (in Anlehnung an Ebert: Risikomanagement, S.15)

[57] Vgl. Lister/Schierenbeck: Value, S.12.
[58] Vgl. Junginger: Wertorientierte, S.200.
[59] Vgl. Ebert: Risikomanagement, S.83.

Eine konkrete Zuordnung des IT-Leistungsvermögens in Unternehmen ist teilweise kompliziert, es sei denn, die Informationstechnologie an sich bildet den Geschäftszweig des Unternehmens (z.B. IT-Dienstleister). Das bedeutet trotz zahlreicher im IT-Controlling eingesetzter Kennzahlen, wie z.B. TCO, Netzwerkanalysen, Lebenszyklusmodellen und ROSI, lassen sich nicht immer genau Kosten und Nutzen der IT bestimmen.[60] Diese Problemstellung bildet ausführlich die Diskussion in Kapitel 5. Für ein wertorientiertes IM hat sich die Kombination von klassischen Kennzahlen und einer BSC bewährt, so können UN-Ziele sowie wesentliche Elemente aus entsprechenden Rahmenwerken (z.B. CobiT und BSI) kombiniert werden. In einer BSC können sowohl finanzielle als auch nichtfinanzielle Ziele aufgenommen und strategische und operative Aufgabenstellungen miteinander verknüpft werden. In einem Unternehmen sind mehrere BSC möglich, sie können immer feiner auf die einzelnen Bereiche abgestimmt werden, so auch für das IT-Risikomanagement.[61]

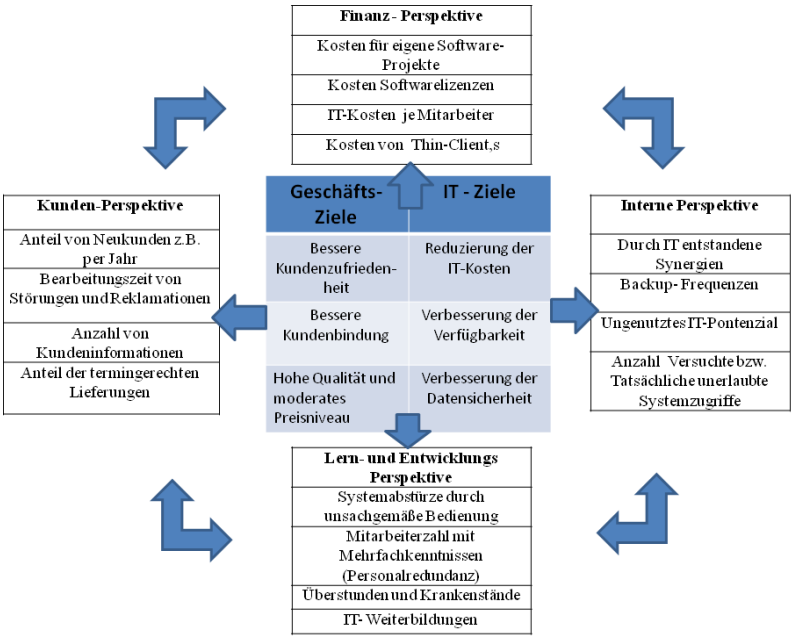

Abbildung 9: Bsp. BSC des IM-Management und IT-Risikomanagement
Eigene Darstellung

Die IT-Risikostrategie sollte letztlich sorgfältig geplant und dokumentiert werden. Dabei spielen Grundlagen, wie Verhinderung, Reduzierung, Übertragung, Vorbeugung und Tolerierung von Risiken die entscheidende Rolle. Außerdem ist allen Anspruchsgruppen gegenüber die Risikostrategie klar zu formulieren und im Unternehmen konsequent zu leben.[62]

[60] Vgl. Tiemeyer: IT, S.132f.
[61] Vgl. Junginger: Wertorientierte, S.96- 99; Königs: IT, S.124.
[62] Vgl. Knoll: Praxisorientiertes, S.63.

In an Betracht der IT-Risiken praktizieren die Unternehmen eine differenzierte Risikokultur. Nicht immer wird diese genau definiert, sondern ergibt sich im Lauf der Zeit aus den Anforderungen an das IT-System. Die IT-Risikokultur gibt den Umgang mit IT-Risiken auf der Grundlage eines gemeinschaftlichen Werteverständnisses des UN, einer IT-Risikokommunikation und einem geeigneten Managementstils, wieder. Inhaltlich geht es darum, wie mit IT-Risiken umzugehen ist, wer sie zu melden hat und zu welcher Konsequenz gemeldete IT-Risiken führen. Für eine konstruktive IT-Risikokultur ist es erforderlich, offen oder über anonymisierte Wege mit Entscheidungsträgern kommunizieren zu können. Ein wertorientierter Führungsstil ermöglicht IT-Risiken offen, vorbehaltlos und wertneutral darlegen zu können. Häufig führen betriebliche Engpässe und eingeschränkte Kapazitäten zu verzögerten Bearbeitungen von gemeldeten IT-Risiken, hier können Service Level Agreements (SLA) Abhilfe schaffen. Damit werden die Form und die Zeit der zur Bearbeitung gemeldeten IT-Risiken festgelegt.[63]

In der Beurteilung von IT-Risiken nehmen die UN eine unterschiedliche Haltung ein, die abhängig von dem IT-Risikowissen, den Erfahrungen und der Kontrollorientierung variiert.[64] Daraus resultiert eine individuelle IT-Risikoneigung, die durch einen risikoaversen, risikoneutralen oder risikoaffinen Charakter geprägt sein kann. Eine risikoaffine Ausrichtung wird als kritisch betrachtet, da hohe IT-Risiken zu Verletzungen von gesetzlichen Vorgaben führen können und mit zivil- oder strafrechtlichen Konsequenzen gerechnet werden muss.[65]

Generell gilt für Risiken, sie lassen sich vermeiden, reduzieren, übertragen, umwandeln oder akzeptieren. Im Rahmen der Risikostrategie gilt es die Risikoakzeptanz festzulegen. Die IT-Risikoakzeptanz ist abhängig von der IT-Risikoneigung und der IT-Risikotragfähigkeit (finanzielle Möglichkeiten), mit der Maßgabe in welcher maximalen Höhe ein IT-Risiko akzeptiert wird. Die Risikoakzeptanz ist das letzte strategische Mittel, wenn z.B. Risikovermeidung, -übertragung oder -umwandlung nicht den gewünschten Erfolg gezeigt haben.[66] Für strategische Entscheidungen werden Policies und Pläne umgesetzt. Dabei bilden die risikopolitischen Grundsätze des Unternehmens die Basis, woraus die IT-Risikopolitik abgeleitet wird.[67]

[63] Vgl. Disterer/Witteck: IT, S.17.
[64] Vgl. Fiege: Risikomanagementsystem, S.99.
[65] Vgl. Schneck: Risikomanagement, S.71.
[66] Vgl. Seibold: IT, S.33.
[67] Vgl. Königs: IT, S.138.

3 Wesentliche Anforderungen an das IT-Risikomanagement

3.1 Wesentliche rechtliche Normen

3.1.1 Wesentliche Anforderungen aus dem KonTraG

In den letzten Jahren führten in Deutschland einige bemerkenswerte Unternehmenskrisen und -zusammenbrüche, vordergründig, die von Kapitalgesellschaften, zu politischen und wirtschaftlichen Diskussionen. Im Mittelpunkt stand dabei die in den Gesellschaften praktizierte Corporate Governance. Hierin werden die Beziehungen zwischen dem Management (Geschäftsleitung) eines Unternehmens, seinem Aufsichtsrat, seinen Anteilseignern (Shareholder) und weiteren Anspruchsgruppen (Stakeholder) festgelegt und formuliert. Darüber hinaus werden Rahmenbedingungen sowie Mittel und Wege zu deren Umsetzung festgelegt. Im Hinblick auf das Risikomanagement gelten für die Geschäftsleitung folgende Aufgaben, konsequent im Sinne des Unternehmens zu handeln und dessen Fortbestand zu sichern, Transparenz herzustellen sowie eine effektive Überwachung zu ermöglichen.[68] Insbesondere für die beiden letztgenannten Aufgaben sah die deutsche Bundesregierung Handlungsbedarf. Aktiengesellschaften sollten zur Integration eines Risikomanagement verpflichtet werden.[69] Dazu wurde am 01.Mai 1998 das Gesetz zur Kontrolle und Transparenz von Unternehmen (KonTraG) verabschiedet. Es verpflichtet Vorstände börsennotierter UN zur Implementierung geeigneter Überwachungssysteme, um Risiken rechtzeitig zu identifizieren. Dem trägt auch der § 91 II AktG Rechnung, wonach der Vorstand geeignete Maßnahmen zu treffen hat und ein Überwachungssystem zu installieren ist, so dass gefahrvolle Entwicklungen zeitnah für die AG identifiziert werden können.[70] Dies gilt auch für die Form einer GmbH (sog. Ausstrahlungseffekt).[71] Zu den Risiken, die mit solchen Frühwarnsystemen erkannt werden sollen, gehören auch Schadensabläufe oder Systemfehler der IT und der Informationssicherheit (z.B. Datenverlust und -missbrauch und Angriffe auf IT-Ressourcen). Um die für die IT gültigen Anforderungen an das KonTraG zu erfüllen, empfiehlt sich die Konformität zu entsprechenden ISO- Normen.[72] Das KonTraG ist ein Artikelgesetz, welches das Kontroll- und Überwachungssystem verbessern soll.[73]

[68] Vgl. Junginger: Wertorientierte, S.116.
[69] Vgl. Ebert: Risikomanagement, S. 92.
[70] Vgl. Finke/Romeike: Erfolgsfaktor, 477.
[71] Vgl. Kirsch: Datenschutz, S.8.
[72] Vgl. Kersten/Reuter/Schröder: IT, S.296.
[73] Vgl. Fiege: Risikomanagement, S.8.

Die Änderungen durch das KonTraG wirken sich in erster Linie auf das HGB sowie das AktG aus. Es sind darüber hinaus weitere Gesetze betroffen, wie z.B. Puplizitätsgesetz, Genossenschaftsgesetz oder Wertpapierhandelsgesetz. An das KonTraG werden bestimmte Zielsetzungen geknüpft: effiziente Rahmenbedingungen für die Aufsichtsratsarbeit, Steigerung der Transparenz und Aufwertung der Kontrollfunktion der Hauptversammlung, moderne Finanzierungsformen, verbesserte Qualität der Abschlussprüfung und sehr gute Zusammenarbeit von Abschlussprüfer und Aufsichtsrat. In Deutschland sind im Hinblick auf die Corporate Governance spürbare Verbesserungen erreicht worden. An der Unternehmensüberwachung sind hier sowohl interne als auch externe Verantwortungsträger beteiligt.[74] Damit wird die Obhutpflicht des Managements gegenüber dem Unternehmen gestärkt und eine Offenlegung der Risiken im Lagebericht erforderlich.

Das KonTraG hatte auch gezielte Änderungen im Handelsgesetz zur Folge. So sind z.B. nach dem §315 HGB, im Konzernlagebericht wesentliche Kriterien des Risikomanagement aufzuführen. Dazu gehören im einzelnen Risikomanagementziele und dafür angewandte Methoden, Preisänderungs-, Ausfall- und Liquiditätsrisiken sowie die Bilanzierung von Sicherungsgeschäften.[75] Das Risikomanagement hat dadurch eine große Aufwertung erfahren und an Bedeutung gewonnen. Was dazu führte, dass indirekt das KonTraG auch auf andere UN wirkt, die keine Aktiengesellschaften sind, aber das Ziel verfolgen, durch ein modernes und integratives Risikomanagement die Existenz des UN zu sichern. Weiter lässt sich feststellen, der Gesetzgeber möchte die anvisierten Ziele nicht erzwingen, sondern gibt es als Aufgabe verantwortungsvoll in die Hände der Unternehmen. Diese gewinnen dadurch an Flexibilität und sind in der Lage sich autonom zu organisieren. Die Einrichtung eines Risikomanagements und die Offenlegungspflicht von Risiken werden durch die meisten UN als positiv bewertet. Gleichzeitig entsteht aus der verbesserten Zusammenarbeit zwischen Abschlussprüfer und Aufsichtsrat ein vorausschauendes Krisenmanagement.[76] Mit der Überlassung der Verantwortlichkeit obliegt den Unternehmen die Ausgestaltung des Risikomanagementsystems. Es werden für die IT das Aufstellen eines Sicherheitskonzeptes mit einer entsprechenden Strategie und speziell abgestimmten Kontrollmaßnahmen empfohlen.[77]

[74] Vgl. Fiege: Risikomanagement, S.9.
[75] Vgl. Wolke: Risikomanagement, S.258.
[76] Vgl. Runzheimer/Wolf: Risikomanagement, S.21f.
[77] Vgl. Eckert: IT, S.196.

3.1.2 Wesentliche Anforderungen aus weiteren Normen und Richtlinien

3.1.2.1 Anforderungen an interne Revisionen

Die interne Revision, als Einrichtung in einem UN, überwacht sämtliche Vorgänge, Verfahren und Maßnahmen, die durch den Aufsichtsrat, die Geschäftsführung oder andere Verantwortungsträger festgelegt wurden. Zum einen gilt es, die vorliegenden Ergebnisse auf ihre Vollständigkeit und Richtigkeit zu überprüfen, aber auch das unternehmerische Handeln und die Fehlerfreiheit von Systemen zu kontrollieren.[78] Die Grundvorrausetzung einer solchen Revision ist, die mit dieser Aufgabe betrauten Personen sollten in den zu kontrollierenden Systemen in keiner Funktion tätig sein. Damit soll die Neutralität gewährleistet und eventuelle Befangenheiten ausgeklammert werden. Im Folgenden soll eine Auswahl für die IT in Frage kommenden Revisionsprüfungen dargelegt werden:

- Überprüfen der Widerspruchsfreiheit von Datenbanken
- Überprüfen der Wirksamkeit von Redundanzen und Backupsystemen
- Betriebsschutzanlagen-Test (Feuerlöschsysteme, Klimaanlagen)
- Penetrationstest, um externe und interne Angriffsschwellen zu ermitteln

Die anvisierten Überprüfungen sind genau zu planen, da hier mit Systemausfällen und Prozessunterbrechungen im Rahmen der Testabläufe zu rechnen ist. Idealer Weise sind hier betriebsschwache Zeiträume auszuwählen.[79] Nach dem KonTraG ist die Geschäftsführung zur Sorgfaltspflicht gegenüber dem Unternehmen angehalten, die (bezogen auf Sorgfaltspflicht) durch ein effizientes internes Kontrollsystem (IKS) ermöglicht werden soll.[80] Die Kontrolle und Überwachung des UN ist eine unverzichtbare Aufgabe der Unternehmensleitung. Die interne Revision kann dabei wiederum die Geschäftsführung unterstützen, um ein erfolgreiches IKS zu führen.[81] So können wichtige Aufgaben zur Fehlerbeseitigung, Entscheidungsfindung und Verhaltensteuerung erfüllt werden. Die erkannten Defizite bzw. Abweichungen ermöglichen eine notwendige Prozesskorrektur und bei vergleichbaren Prozessen schneller zielführender Entscheidungen treffen zu können. Interne Revisionen erzeugen eine hohe Mitarbeitermotivation, sich konform an die Vorgaben des UN zu halten.[82]

---

[78] Vgl. Königs: IT, S.81, 91.
[79] Vgl. Kersten/Reuter/Schröder: IT, S.274.
[80] Vgl. Kirsch: Datenschutz, S.20.
[81] Vgl. Klinger/Klinger: Das Interne, S.7.
[82] Vgl. Fiege: Risikomanagement, S. 84.

Die interne Revision hat sich zu einem funktionalen Bestandteil des Managementsystems entwickelt. Sie ist als zentrale Abteilung in zahlreichen Unternehmen direkt deren Leitung unterstellt. Eine wesentliche Revisionsaufgabe ist, unter dem Aspekt der Vermögenserhaltung, durch konstruktive Arbeit gute Systemverbesserungsvorschläge vorzulegen. Die Qualität der internen Revision lässt sich anhand der entwickelten Vorschläge messen.[83] Mangelhafte interne Revisionen bzw. Fehler der ausführenden Personen können, insbesondere bei der Kontrolle des Risikomanagement, große Probleme hervorrufen. Im gravierendsten Fall können Fehler bzw. Risiken im Risikomanagementsystem selbst auftreten, auch bekannt als Überwachungsrisiko. Ein Risikomanagement in einem UN allein garantiert keine Sicherheit, sondern sollte selbst auf seine Funktionalität sorgfältig und regelmäßig überprüft werden.[84]

3.1.2.2 Wesentliche Anforderungen aus Basel II/III

Zunächst wurde mit diesem Werk die qualitative Risikobetrachtung bei der Kreditvergabe durch Geldinstitute eingeführt, d.h. die Bewertung von Ausfall-, Liquiditäts- und Marktpreisrisiken. Um Betriebsrisiken, die im täglichen Ablauf entstehen, mit einzubeziehen, wurde dann die Komponente der operationellen Risiken integriert. In der Folge sind Banken gezwungen ein ganzheitliches Risikomanagement zu führen, welches sowohl die klassischen Risiken bewirtschaftet als auch Strategien für operationale Risiken entwickelt. Zu den operationalen Risiken zählen auch Risiken der IT.[85] Operationelle Risikoereignisse werden in Basel II/III durch Beispiele aus dem Bereich der IT manifestiert. Schäden durch Hacker Angriffe, Verletzung von Datenschutzbestimmungen, Ausfall von Hardware, Software oder Telekommunikation oder Fehler bei der Bewirtschaftung von Datenbanken sollen auszugsweise hier als Beispiel genannt sein.[86] Diese Risiken treffen sowohl die Banken selbst als auch die zu bedienenden Unternehmen. Somit sind die Kreditinstitute auch bei ihren Kunden und Partnern an einem professionellen Risikomanagement interessiert. Demzufolge kann das Eigenkapital der Bank zur Risikoabsicherung geringer ausfallen und die Kosten für das angeforderte Kapital der Unternehmen können sinken.[87]

---

[83] Vgl. Horváth: Controlling S.699- 704.
[84] Vgl. Junginger: Wertorientierte, S.140.
[85] Vgl. Seibold: IT, S.2, S.227.
[86] Vgl. Königs: IT, S.89
[87] Vgl. Knoll: Praxisorientiertes, S.72.

Obwohl in Basel II/III Risiken von Banken im Mittelpunkt stehen, werden durch die operationale Komponente, Risiken nichtfinanzwirtschaftlicher Unternehmen mit einbezogen. Sinngemäß werden operationale Risiken als die Gefahr von Verlusten definiert, die durch Unangemessenheit oder Versagen von internen Personen, Prozessen und Systemen oder externen Einflüssen eintreten. Rechtliche Risiken werden hier mit eingeschlossen, Strategische- und Reputationsrisiken jedoch ausgeklammert. Um hier wirksam entgegenzusteuern, erlangen Risikomanagements, auch im Bereich der IT, in einer Vielzahl von UN generell an Bedeutung.[88]

3.1.2.3 Wesentliche Anforderungen aus Datenschutznormen

Ein Unternehmen ist verpflichtet, eine Vielzahl von gesetzlichen Verboten und Geboten einzuhalten. Die dazu erforderlichen Maßnahmen werden unter dem Begriff „Compliance“ zusammengefasst. Sie dienen dem Unternehmen und seinen Mitarbeitern, gesetzeskonform zu handeln und vorausschauend mögliche Gesetzesverstöße zu erkennen.[89] Die große Bandbreite und gestiegene Verwundbarkeit der Informationstechnologien in UN erfordern stetige gesetzliche und regulatorische Anpassungen. Diese professionell umzusetzen, setzt hohe Fachkompetenz und eine spezifische IT-Compliance voraus.[90]

Das BDSG fordert mit dem §1 Abs.1, jeder einzelne hat selbst über die Freigabe und weitere Verwendung seiner persönlichen Daten zu entscheiden. Einschränkungen über die „informelle Selbstbestimmung“ sind nur möglich, solange sie verfassungsrechtlich konform sind und der Normenklarheit und der Verhältnismäßigkeit entsprechen. Die Verletzung des Persönlichkeitsrechts ist durch organisatorische und verfahrensrechtliche Maßnahmen zu verhindern. In einigen Unternehmen (z.B. LIDL) wurde gegen das Persönlichkeitsrecht eklatant verstoßen. Das führte zur Erhebung von Bußgeldern in Millionenhöhe und einem enormen Imageverlust. Auf Grund solcher Verstöße sah sich der Gesetzgeber veranlasst, mit den Novellen I-III das BDSG zu reformieren. Für die Unternehmen leitet sich die Verpflichtung zur Einrichtung eines ISMS aus dem §9 BDSG und seiner Anlagen ab, wonach die persönlichen Daten mit geeigneten Systemen zu schützen sind. Ein IT-Risikomanagement trägt wesentlich zur Erfüllung dieser Vorgaben bei.[91]

---

[88] Vgl. Wolke: Risikomangement, S.201f.
[89] Vgl. Kirsch: Datenschutz, S.18.
[90] Vgl. Lenges: Framework, S.3.
[91] Vgl. Kersten/Reuter/Schröder: IT, S.6.

Nach dem § 4f Abs.1 BDSG soll durch einen Datenschutzbeauftragten, sowohl in öffentlichen als auch nichtöffentlichen Institutionen, der Datenschutz sichergestellt werden. Die große Zahl an verfügbaren Daten kann Unternehmen dazu verleiten, sie zu eigenen Marketingzwecken zu missbrauchen oder an Dritte weiter zu veräußern. Der daraus kurzfristig erzielte wirtschaftliche Nutzen kann aber zu Imageverlusten, Bußgeldern oder strafrechtliche Konsequenzen führen, die möglicherweise den Fortbestand des UN gefährden.[92] Die Allgemeine Datenschutzrichtlinie der EU sagt aus, dass es die Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten zu schützen gilt. Eine einheitliche weltweite Übereinstimmung zu dem Begriff des Datenschutzes gibt es jedoch nicht.[93] Die zuvor genannten gesetzlichen Grundlagen zum Datenschutz beziehen sich nur auf Forderungen der Informationsverarbeitung. Es werden keine Aussagen zu Maßnahmen der Datensicherheit getroffen, die steht jedoch im kausalen Zusammenhang zum Datenschutz. Unter der Datensicherheit ist der Schutz vor Zerstörung, Verlust oder Missbrauch von Informationen zu verstehen. Dazu sind geeignete bauliche, technische sowie organisatorische Maßnahmen erforderlich. Die UN haben Vorkehrungen zu treffen, um die Sicherheit, Verfügbarkeit sowie Zuverlässigkeit von IT-Systemen zu gewährleisten. Es lässt sich feststellen, eine mangelhafte Datensicherheit bewirkt einen unzureichenden Datenschutz.[94]

Auch die Grundsätze, zum Datenabruf und der Prüfung digitaler Unterlagen (GdPdU) und ordnungsgemäßer DV gestützter Buchführungssysteme (GoBS), verpflichten zum Schutz vor Datenmissbrauch, gemäß den §§ 146 und 147 der Abgabenordnung. Hiermit werden die Zugriffsrechte der Finanzbehörden geregelt und den UN im Umgang mit den gespeicherten Daten eine entsprechende Sorgfaltspflicht auferlegt. Es wird darüber hinaus die Implementierung eines IKS gefordert. Das IKS und ein ISMS ermöglichen durch Kontrollen und daraus resultierenden Maßnahmen den Schutz des Vermögens und der Informationen.[95]

Für die Informationstechnologien gibt es auf Grund ihrer großen Verbreitung enorm viele Berührungspunkte mit Gesetzen und Normen. Auf alle infrage kommenden Regelungen an dieser Stelle einzugehen, ist leider nicht möglich. Im Folgenden

[92] Vgl. Kirsch: Datenschutz, S.24.
[93] Vgl. Königs: IT, S.96.
[94] Vgl. Junginger: Wertorientierte, S.129.
[95] Vgl. Kersten/Reuter/Schröder: IT, S.2f.

sollen einige Beispiele für Vorschriften, die in ihrer Auslegung ein ISMS fordern, genannt werden. [96]

- Teledienstgesetz
- Teledienstedatenschutzgesetz (TDDSG)
- Grundgesetz Artikel 10 und G10- Gesetz
- Urheberrechtsgesetz (UrhG)
- Strafgesetzbuch
- Sicherheitsüberprüfungsgesetz (SÜG)

3.1.2.4 Wesentliche Anforderungen durch SOX und EuroSOX

Der Sarbanes Oxley Act ist 2002 durch eine Initiative der amerikanischen Politiker Paul S. Sarbanes und Micheal G. Oxley in den USA in Kraft getreten. Dadurch ergeben sich Forderungen nach einem Risikomanagement in allen AG oder deren Tochterunternehmen, die an den US-Börsen notiert sind. Der Hintergrund dieses Gesetzes liegt in den aufsehenerregenden Finanzskandalen der Unternehmen Worldcom und Enron sowie der Wirtschaftsprüfungsgesellschaft Anderson.[97] Im Falle von Worldcom kam es zu Bilanzmanipulationen in einer Höhe von 11 Mrd. US$ und dem Zusammenbruch des Unternehmens. Kapitalgesellschaften werden nun mehr durch das Gesetz aufgefordert, ein internes Kontrollsystem zu führen, welches jährlich auf seine Funktion zu überprüfen ist. Die gewonnenen Ergebnisse sind in einem Report zu dokumentieren und dienen der Unternehmensberichterstattung. Darin soll die Richtigkeit des Finanzergebnisses und der UN-Prozesse nachgewiesen werden. Für die Absicherung der IT werden keine expliziten Aussagen getroffen. Ohne eine systematische Sicherstellung der IT lässt sich jedoch keine Konformität zu diesem Gesetz herstellen. Darüber hinaus werden die meisten Report-Ergebnisse aus IT-Systemen gewonnen und mit den Bilanzdaten abgeglichen. Der verantwortungs-volle Umgang mit unternehmensinternen Informationen und deren Schutz ist im Sinne dieses Gesetzes unerlässlich.[98] Eine weitere sinnvolle Vorschrift aus diesem Gesetz verpflichtet zum Schutz der „Whistleblower"-Mitarbeiter, die Informationen über illegale Manipulationen des Managements an staatliche Kontrollbehörden weiterleiten.[99]

[96] Vgl. Kersten/Reuter/Schröder: IT, S.6.
[97] Vgl. Siepermann: Risikokostenrechnung, S.1.
[98] Vgl. Königs: IT, S.90- 92.
[99] Vgl. Volkwein: Die Umsetzung, S.39.

In Europa gab es ähnliche Vorfälle von Finanzmanipulationen in UN. Das veranlasste die EU dazu, die EuroSOX Richtlinie (8.EU-Richtlinie) ins Leben zu rufen, die seit dem Juni 2006 in Kraft ist. Durch die unterschiedliche Auffassung in Bezug auf die Corporate Governance in den UN der einzelnen Mitgliedsländer wurde EuroSOX nicht so streng wie das SOX gefasst. Es wird den Staaten selbst überlassen, Regeln zur Ausgestaltung der Corporate Governance für die UN aufzustellen. Damit ist im EuroSOX ein Ziel definiert, nicht die Art und Weise wie es zu erreichen ist. Im Ergebnis geht es aber auch hier, um die Einrichtung eines internen Kontrollsystems, das wiederum auf seine Effizienz zu überprüfen ist. Klare Aussagen zu der Informationstechnologie werden auch hier nicht getroffen.[100] Es lässt sich aber feststellen, dass wie bei SOX die UN angehalten sind gesetzeskonforme IT-Systeme zu führen. Daher fordert der deutsche Gesetzgeber seit Juli 2008 Kapitalgesellschaften auf, ein entsprechendes IT-Sicherheitskonzept vorzuhalten. Aus EuroSOX lassen sich wesentliche Anforderungen an die IT ableiten: Gewährleistung der Zugriffs- und Zutrittssicherheit, Kontrolle der Kommunikationssicherheit, Softwareschutz, Erhaltung der Betriebsfähigkeit sowie Ausarbeitung von Notfallplänen. Sowohl durch SOX als auch EuroSOX haftet die Unternehmensleitung vollumfänglich für auftretende Mängel.[101]

3.2 Wesentliche Regelwerke und Standards

3.2.1 Regelwerke des BSI

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat auf der Basis des IT-Grundschutzhandbuches durch stetige Ergänzungen ein umfangreiches Regelwerk zur IT-Sicherheit geschaffen. Neben dem Katalog für Grundschutzmaßnahmen gibt es darüber hinaus Standards für ein ISMS und zur Risikoanalyse. Die Publikationen werden in gewissen Abständen modifiziert und aktuellen Bedürfnissen angepasst. Die Zielsetzung des Regelwerkes ist es, mit infrastrukturellen, personellen, technischen und organisatorischen Basissicherheitsmaßnahmen ein Grundschutzniveau für die IT zu erzielen, das dem aktuellen Stand der Technik entspricht.[102]

[100] Vgl. Tiemeyer: Handbuch, S.671.
[101] Vgl. Königs: IT, S.95.
[102] Vgl. Junginger: Wertorientierte, S.145.

Die Einhaltung der Schutzziele, wie Verfügbarkeit, Vertraulichkeit und Integrität ist ein zentrales Element der BSI-Regelwerke. Weiterhin gilt es, die Authentisierung, Autorisierung, den Datenschutz und die Datensicherheit zu gewährleisten. Dazu sollen die IT-Systeme überprüft werden und eine Ermittlung des Bedrohungspotenzials durchgeführt werden.[103] In Anlehnung an die ISO 27001 ist es möglich, im Bereich Grundschutz der IT, die Zertifizierung des UN durch das BSI zu erlangen. Dadurch werden in UN implementierte IT-Sicherheitsmanagementmaßnahmen auch international vergleichbar.[104] Die einzelnen Veröffentlichungen sind wie folgt aufgebaut:

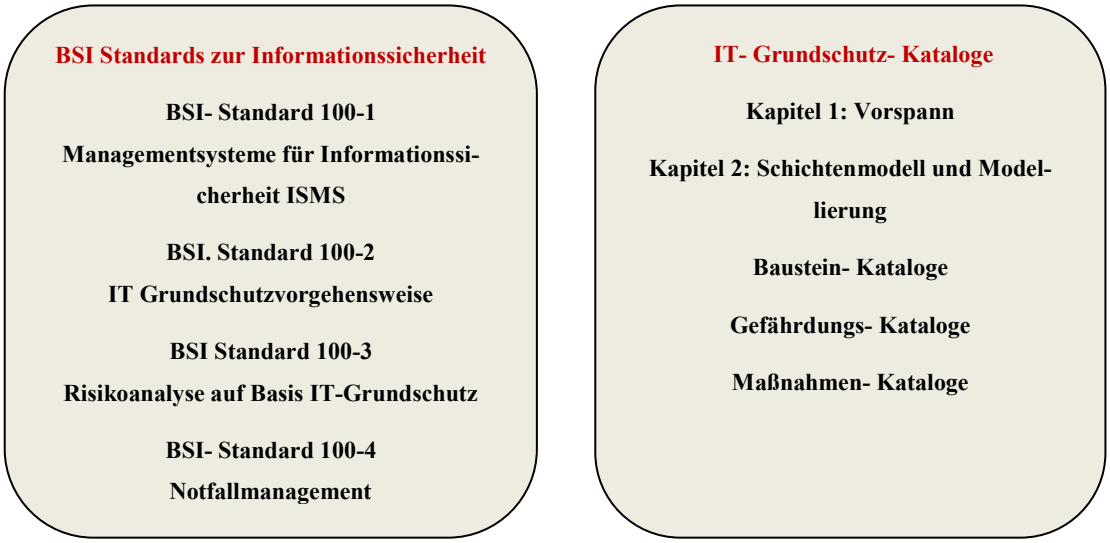

Abbildung 10: BSI Veröffentlichungen
Eigene Darstellung

Aus den Standards für ein ISMS und zur Risikoanalyse ergibt sich die Forderung nach einer IT-Sicherheitspolitik. Diese wird im Rahmen der Risikostrategie von den Unternehmenszielen abgeleitet und durch ein IT-Risikomanagement umgesetzt. So wird durch das BSI die strategische Bedeutung eines Risikomanagement verdeutlicht. Eine hohe Aufmerksamkeit schenkt das BSI den stetig zunehmenden Bedrohungen im Bereich des E-Business und steuert dem zweimal jährlich mit neuen Anpassungen des Grundschutzes entgegen.[105] Der gestiegene Handlungsbedarf in diesem Bereich wird durch die Lageberichte des BSI zur IT-Sicherheit deutlich. Mit großer Sorge werden die drastisch angestiegenen Angriffe durch Trojaner betrachtet. Solche Code-Spionagen richten oft große Finanz- oder Reputationsschäden an.[106]

[103] Vgl. BSI: GS-Leitfaden, S.14.
[104] Vgl. Kersten/Reuter/Schröder: IT, S.16-18.
[105] Vgl. Junginger: Wertorientierte, S.146.
[106] Vgl. Eckert: IT, S.25.

Die Maßnahmenkataloge im IT-Grundschutzkatalog des BSI enthalten eine Vielzahl von Vorkehrungen zum Aufbau und zur Ausgestaltung eines IT- Sicherheitsmanagements. Inhaltlich werden strukturelle, organisatorische, personelle und technische Maßnahmen detailliert erläutert und entsprechende Notfallvorsorgen besprochen.[107] Um die Bedeutung des IT-Risikomanagements aufzuzeigen, werden im Folgenden exemplarisch einige Vorgaben erörtert. In der Maßnahme M 2.335 wird eine detaillierte Beschreibung der Sicherheitsstrategie und -ziele im IT-Umfeld empfohlen, die konsequent durch die UN-Leitung zu unterstützen und zu verantworten sind. Weiter wird dazu geraten, die Strategien und Ziele regelmäßig auf ihre Wirksamkeit zu überprüfen und sie bei Bedarf zu modifizieren. Damit wird offensichtlich die Implementierung eines IKS und IT-Risikomanagement in die UN-Organisationstruktur empfohlen. Die Maßnahme 2.336 zeigt weiter, die UN-Leitung ist regelmäßig über mögliche Risiken und deren Konsequenzen bezüglich der Informationssicherheit zu informieren. Dieses setzt ein effizientes und auf Fehler überwachtes IT-Risikomanagement voraus. Eine Integration der Informationssicherheit in alle Geschäftsprozesse und die Verknüpfung des etablierten Risikomanagements mit einem spezifischen IT-Risikomanagement geht als Empfehlung aus der Maßnahme M 2.337 hervor. Weiterhin wird die Auffassung vertreten, Arbeitsanweisungen, die Risiken betreffen, sollten stets in allen UN-Bereichen konform sein. Dies unterstreicht die Einbindung des Risikomanagementprozesses in den gesamten UN-Prozess.[108]

Die Gefährdungs-Kataloge bieten den Unternehmen ein weiteres praktisches Werkzeug für das Risikomanagement, mit einer umfangreichen Aufstellung von Gefährdungen, die wiederum übersichtlich in verschiedene Gruppen eingeteilt sind. Mit einer analytischen Überprüfung der Aufstellung und einem Abgleich der Risikorelevanz im UN lassen sich so leichter wirtschaftliche Risiken identifizieren.[109] Viele weitergehende Risikoanalysen sind mit einem hohen finanziellen und zeitlichen Aufwand verbunden. Daher empfiehlt das BSI solche Analysen nur in Systemen durchzuführen, deren Sicherheitsanforderungen über ein niedriges bis mittleres Maß hinausgehen oder in UN bzw. Behörden, die IT-Systeme betreiben, die mit den Maßnahmen aus dem BSI IT-Grundschutzhandbuch nicht ausreichend abgesichert werden können.[110]

---

[107] Vgl. Seibold: IT, S.193.
[108] Vgl. BSI: IT, S.2040- 2046.
[109] Vgl. Knoll: Praxisorientiertes, S.130.
[110] Vgl. Eckert: IT, S.214.

Neben dem Management, der IT-Infrastruktur und dem Personal gehört nach dem Verständnis des BSI zu einem ISMS ein ganzheitlicher IT-Sicherheitsprozess (vgl. Abb.11, S.29). Dieser befasst sich mit der IT-Sicherheitslinie, dem IT-Sicherheitskonzept und der IT-Sicherheitsorganisation. In dem BSI-Standard 100-1 werden die allgemeinen Anforderungen an ein Managementsystem für Informationssicherheit (ISMS) definiert. Dieser Standard kann mit der ISO/IEC 27001 verknüpft werden und ermöglicht die Zertifizierung auf der Basis „IT-Grundschutz" durch das BSI.[111] Mit der Zertifizierung der UN nach ISO sind deren IT-Sicherheitsmaßnahmen auch international vergleichbar.[112] Der vom BSI definierte IT-Sicherheitsprozess beginnt mit der IT-Sicherheitsleitlinie. In ihr werden die IT-Sicherheitsziele und deren strategische Umsetzung fixiert. Das IT-Sicherheitskonzept und die IT-Sicherheitsorganisation dienen dem Management zum Aufbau einer IT-Sicherheitsstrategie. Das IT-Sicherheitskonzept basiert auf den Grundschutzkatalogen. Darin enthaltene Maßnahmen beziehen die Vorgaben aus der ISO/IEC 27001/2 mit ein und legen notwendige Vorkehrungen für den sicheren Betrieb von IT-Systemen fest.[113] Der IT-Sicherheitsprozess startet mit einer IT-Strukturanalyse. Hier werden wichtige Schutzobjekte wie Informationen, Anwendungen und Systeme der IT, Netze, bauliche Strukturen und die Mitarbeiter ermittelt, deren Abhängigkeiten identifiziert und dokumentiert. Anschließend findet die Schutzbedarfsfeststellung auf der Grundlage von Verfügbarkeit, Vertraulichkeit sowie Integrität statt. Im Ergebnis sollen hochschutzbedürftige Zielobjekte identifiziert werden, die anhand zusätzlicher Gefährdungskriterien zu analysieren sind. Zeigt die Analyse, dass die betroffenen Zielobjekte, mit den jetzt in den UN praktizierten Sicherheitsmaßnahmen nicht zu schützen sind, so ist das IT-Sicherheitskonzept zu konsolidieren.[114]

Abschließend lässt sich feststellen, die „IT-Grundschutz-Kataloge" bieten UN mit moderaten Schutzbedürfnissen im IT-Bereich ausreichende Möglichkeiten zum IT-Grundschutz. Auf individuelle und kostenintensive Risikoanalysen kann somit verzichtet werden. Für UN mit hohem IT-Sicherheitsansprüchen kann der Grundschutz mit den „BSI-Standards zur Informationssicherheit" zielführend aufgewertet werden (z.B. BSI Standard 100-3 Risikoanalyse auf Grundschutzbasis).[115]

[111] Vgl. BSI: Publikationen, S.13.
[112] Vgl. Kersten/Reuter/Schröder: IT, S.16.
[113] Vgl. Königs: IT, S.222.
[114] Vgl. Eckert: IT, S.214.
[115] Vgl. Seibold: IT, S.193.

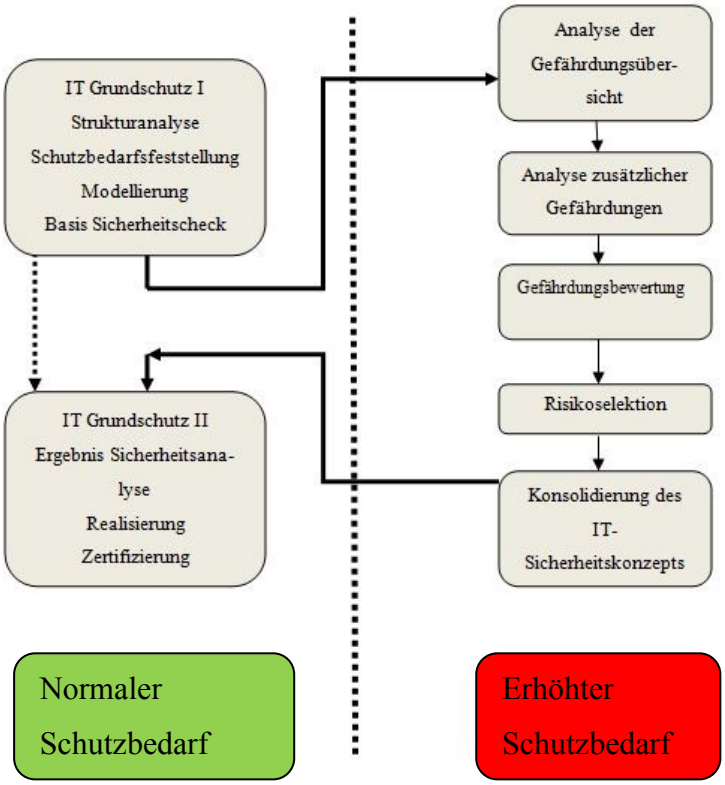

Abbildung 11: BSI IT -Sicherheitsprozess

Eigene Darstellung

3.2.2 ISO Norm 27001

Die ISO Normen sind international gültige Standards für nahezu alle Bereiche unseres Umfeldes und werden von der International Organisation of Standardization mit Sitz in Genf aufgestellt. Sie ist ein Teil der World Standards Cooperation. Große Popularität erlangten die ISO Normen, als erste UN begannen z.B. ihr Qualitätsmanagement nach der 9000er Reihe zertifizieren zu lassen.[116] Der ISO Standard 27001 ist das zentrale Element der 2700x Normen. Er bietet die Möglichkeit, standardisiert ein professionelles ISMS in den UN aufzubauen und auf Dauer zu bewirtschaften. Zudem bildet er die Schnittstelle zu dem BSI Standard 100-1, und macht dadurch das Unternehmen zertifizierbar und international an erkennbar im Bereich „IT-Grundschutz“, was den meisten UN wiederum Wettbewerbsvorteile verschafft.[117] Die Normenreihe der ISO 2700X enthält insgesamt 19 weitere Standards.[118]

[116] Vgl. Lenges: Framework, S.73.
[117] Vgl. Kamiske: Managementsysteme, S.284.
[118] Vgl. Kersten/Reuter/Schröder: IT, S.13.

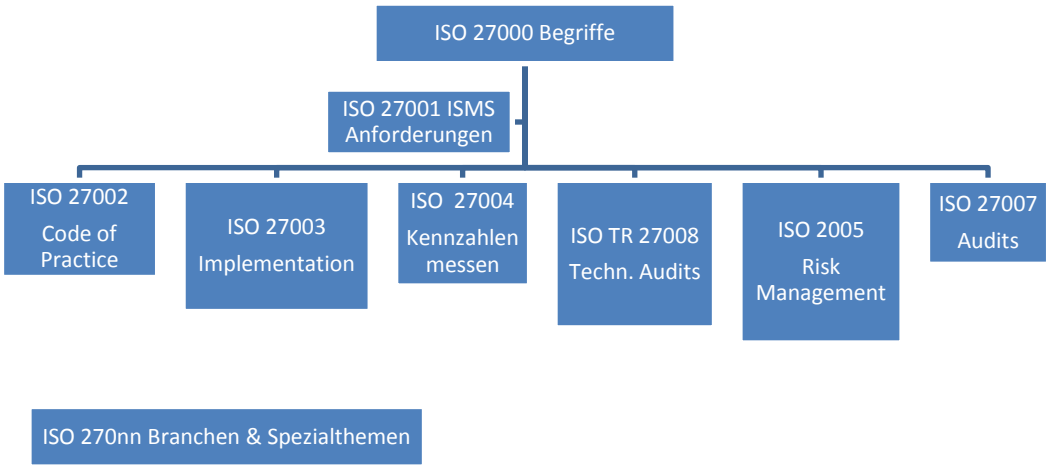

Abbildung 12: ISO 27000 Normenreihe
Eigene Darstellung

ISO 27001 gilt, im Hinblick auf die Managementsystem-Standards ISO 9001:2000 und ISO 14001: 2004, als eine Norm, die ein prozessgesteuertes Managementsystem beschreibt, welches dem Aufbau und der Erhaltung der IT-Sicherheit dient (ISMS). Die Gestaltung des Prozesses zieht Parallelen zu dem aus Qualitätsmanagementprozessen bekannten Vier- Phasen Zyklus. Dieses als „Plan-Do-Check-Act“ bekannte Modell ging aus dem von Shewhart und Deming entwickelten Lernzyklus „ Plan-Do-Study-Act“ hervor.[119] So werden in der Planungsphase (Plan) Risiken mit den Unternehmenszielen und den regulatorischen Vorgaben des UN in Abstimmung gebracht. Dazu werden die ISO/IEC 13335 (Technikreport) und die ISO/IEC TR 13335 (Code of Practice) mit hinzugezogen.[120] In der Phase der Umsetzung (Do) werden die Rahmenbedingungen zur Implementierung und Aufrechterhaltung eines ISMS geschaffen. Dabei kann der BSI 100-1 Standard als Regelwerk mit einbezogen werden.[121] Die Überwachung der Effizienz und Effektivität des ISMS, die Risikobeobachtung sowie Bewertung der Wertigkeit der Maßnahmen werden in der dritten Phase (Check) vollzogen. Anschließend in der vierten Phase gilt es, notwendige Verbesserungen oder Veränderungen am ISMS vorzunehmen. Im IT-Sektor treten immer wieder neue Risiken auf, daher bildet der Prozess einen stetigen Kreislauf.[122]

[119] Vgl. Königs: IT, S.198.
[120] Vgl. Ebert: Risikomanagement, S.99.
[121] Vgl. BSI: Publikationen, S.9.
[122] Vgl. Kersten/Reuter/Schröder: IT, S.48.

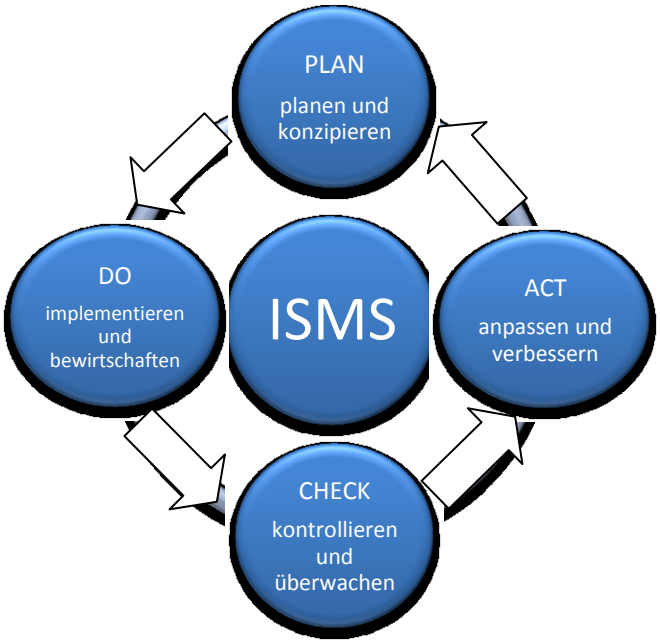

Abbildung 13: PDCA Kreislauf des ISMS nach ISO/IEC 27001
Eigene Darstellung

Die ISO 27001 baut auf ein risikoorientiertes Sicherheitsmanagement und zeigt zielführend wichtige Abläufe, die dem Aufbau und der dauerhaften Erhaltung der Informationssicherheit dienen. Damit setzt diese Norm, implizit ein effizientes IT-Risikomanagement innerhalb des ISMS voraus. Das Kapitel 4 dieser Norm unterstreicht die zuvor getroffene Aussage, in dem es folgende generelle Bedingungen nennt: ein Unternehmen soll unter Beachtung seiner gesamten Geschäftstätigkeiten und Risiken ein ISMS installieren, realisieren, führen, überwachen, kontrollieren, anpassen und optimieren.[123] Ein verantwortungsbewusstes Management wird sich demnach für den Aufbau eines ISMS entscheiden. Die weitere Planung und auf welchen Grundlagen die Einführung eines ISMS basiert, wird in der ISO 27003 festgelegt.[124] Wichtige Normenforderungen der ISO 9001 sind analog in der ISO 27001 enthalten, dazu zählen Dokumentationen, Beweissicherungen, interne Audits sowie Optimierung der Prozesse. Das unterstreicht die Bedeutung der ISO 27001 und spricht für ein wirkungsvolles IT-Risikomanagement in den Unternehmen.[125]

[123] Vgl. Königs: IT, S.200.
[124] Vgl. Blumberg/Pohlmann: Der IT, S.140.
[125] Vgl. Kersten/Reuter/Schröder: IT, S.10.

3.2.3 CobiT

Die „Best Practice"-Empfehlung „CobiT" ist ein managementorientierter Prozess zur Kontrolle der gesamten IT. Es handelt sich um ein international anerkanntes Framework, in dessen Mittelpunkt die IT-Governance steht.[126] Es wurde ursprünglich von der ISACF (Information Systems Audit and Control Foundation) als eine Methode der Auditierung und als Lernprozess für das Managementsystem entwickelt. Die Entwicklung begann im Jahr 1994, 2012 erschien das letzte Upgrade, die aktuelle Version 5, die nun die bisher eigenständigen Frameworks „RiskIT" und „VaiIT" enthält. Darüber hinaus wird in dieser Version neuerdings zwischen einer Governance- und Management Ebene differenziert. Für die Governace-Ebene gilt, durch explizite Vorgaben, permanentes Monitoring und stetige Bewertungen der IT, das Erreichen der UN-Ziele sicherzustellen. Die daraus abgeleiteten Governance-Vorgaben ergeben in der Management-Ebene die Strukturierung und Kontrolle der IT.[127] Das Rahmenwerk „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 die Aktivitätsebene. Diese Aktivitäten werden benötigt, um ein vorgegebenes Ziel zu erreichen. Die nächst höhere Ebene ist die der Prozesse. In ihr werden Aktivitäten zu „natürlichen Gruppen" zusammengefasst, die spezifische Kontrollen ermöglichen. Auf der obersten Ebene werden Prozesse konsolidiert und zu vier Domänen zusammengefasst. Diese Domänen entsprechen häufig den Organisationsanforderungen von IT-Bereichen in Unternehmen.[128]

Das „CobiT" impliziert ein Steuersystem, welches den Focus auf IT-Ressourcen und Geschäftsanforderungen richtet. 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.[129]

Im CobiT-Framework werden insgesamt 37 Prozesse behandelt, 5 auf der Governance Ebene und 32 im Managementbereich. Dabei wird das Augenmerk,

[126] Vgl. Gadatsch: IT, S.11.
[127] Vgl. Knoll: Praxisorientiertes, S.75.
[128] Vgl. Junginger: Werteorientierte, S.149.
[129] Vgl. Seibold: IT, S.185.

die IT- Governance betreffend, auf fünf wesentliche Kernbereiche gerichtet.[130] Die Bereiche umfassen folgende elementare Aufgaben:

- Strategische Orientierung des IT-Umfeldes
- Kosten/ Nutzen Analysen für die IT-Systeme
- Risikomanagement
- Beurteilung des IT-Leistungsvermögens
- IT-Ressourcenmanagement

CobiT 5 lenkt eine große Aufmerksamkeit auf ein wesentliches Governace-Ziel, das der Wertschöpfung. Damit sollen insbesondere Forderungen der Stakeholder erfüllt werden, durch eine Nutzen-, Bedarfs- und Risikooptimierung des IT-Umfeldes den UN-Fortbestand zu sichern.[131] Die zuvor erwähnten Prozesse dienen der Umsetzung der Unternehmens- und IT-Strategie. Dazu wird eine Einteilung in vier Domänen vorgenommen. Die Domänen lauten wie folgt:

- Planung und Organisation (Plan and Organize): Hier geht es in erster Linie um die Planung einer IT-Strategie, d.h. inwiefern kann die IT dazu dienen, die Geschäftsziele umzusetzen. Desweiteren ist die Informationsarchitektur zu bestimmen und eine IT-Infrastruktur festzulegen.
- Beschaffung und Implementierung (Acquire and Implement): Diese Domäne widmet sich dem Eruieren geeigneter IT-Lösungen, deren Beschaffung bzw. dem Entwickeln eigener IT-Lösungen. Darüber hinaus werden in dieser Phase Wartungs- und Anpassungsarbeiten an bereits implementierten IT-Feldern vorgenommen.[132]
- Liefern und Unterstützen (Deliver and Suport): Dabei handelt es sich um das Bereitstellen von Dienstleistungen durch renommierte externe Servicepartner, Sicherstellung der Leistung von IT-Systemen und dem IT-Personal.[133]
- Überwachen und Beurteilen (Monitor and Evaluate): Die letze Domäne befasst sich mit Kontrollprozessen, wie der Überwachung und Beurtei-

[130] Vgl. Knoll: Praxisorientiertes, S.75.
[131] Vgl. Königs: IT, S.212.
[132] Vgl. Junker/Marx/Odebrecht: IT, S.44.
[133] Vgl. Seibold: IT, S.186.

lung der IT-Leistung und interner Kontrollsysteme, sowie der Sicherstellung der IT-Compliance und der Gewährleistung der IT- Governance.[134]

In dem Prozess PO9, aus der Domäne „Planung und Organisation“, werden präzise der Aufbau und die Betreibung eines IT- Risikomanagement dargelegt. Damit wird die Implementierung eines ISMS und IKS indirekt vorausgesetzt. Im Weiteren werden einzelne Aufgaben explizit Personen bzw. UN-Bereichen zugeordnet.[135] Die folgende grafische Darstellung zeigt die Struktur des CobiT-Frameworks, wie sie zuvor beschrieben wurde.[136]

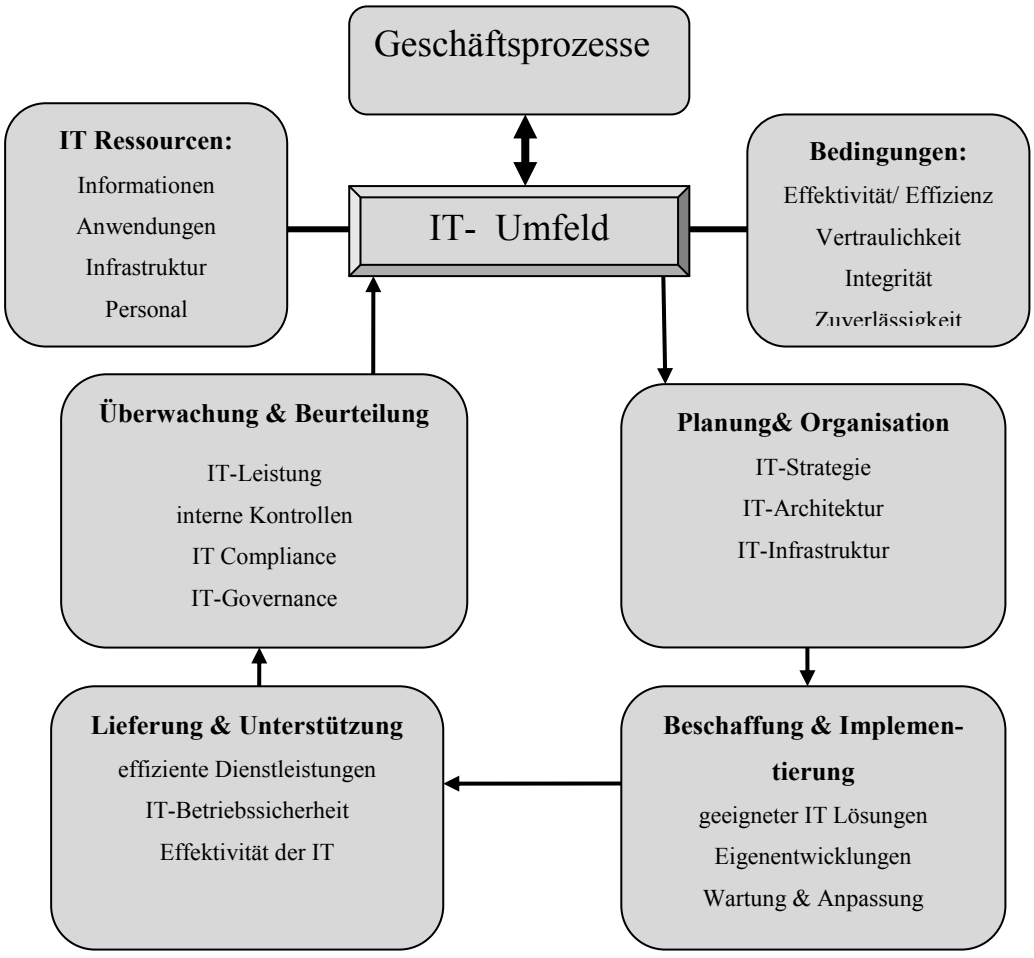

Abbildung 14: CobiT-Framework
Eigene Darstellung (in Anlehnung an Seibold: IT, S.186.)

[134] Vgl. Junker/Marx/Odebrecht: IT, S.44.
[135] Vgl. Knoll: Praxisorientiertes, S.76f.
[136] Vgl. Seibold: IT, S.186.

Anhand des CobiT-Würfel (Cube) lassen sich Ressourcen, anvisierte UN- Ziele und zielführende Prozesse des IT-Umfeldes grafisch darstellen.

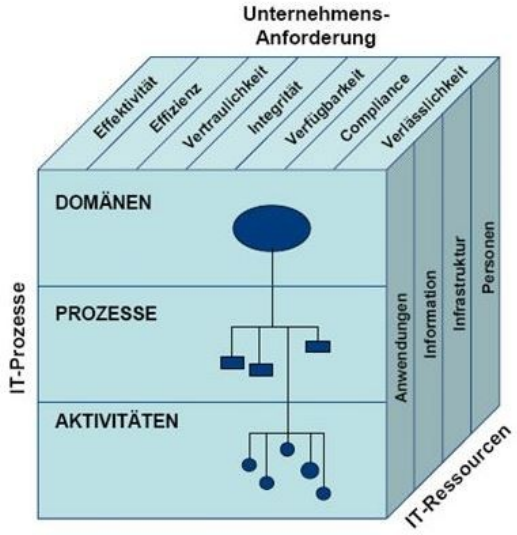

Abbildung 15: CobiT-Würfel (Cube)
Eigene Darstellung (in Anlehnung an Königs: IT, S.215.)

Das CobiT bietet auf der Grundlage eines Best Practice Ansatzes eine effiziente und effektive Grundlage, ein IT-Risikomanagement aufzubauen und zu pflegen.[137] Wenngleich es sich nicht um ein reines IT-Risikomanagement-Framework handelt, so wird, durch viele Ansätze und Inhalte die Implementierung eines IT- Risikomanagement ermöglicht. Das CobiT-Rahmenwerk orientiert sich an UN-Anforderungen, steuert mit Kontrollzielen die IT-Prozesse und analysiert die IT-Ressourcen. Daher übernehmen viele UN die Vorgaben des Frameworks und nutzen es als Basis für ihre spezifischen Unternehmensanforderungen.[138] Die Integration der bisher eigenständigen Frameworks „Val IT“ und „Risk IT“ baut das CobiT zu einem ganzheitlichen Framework aus. So wird mit „Val IT“ der Lebenszyklus eines Investitionsprogramms über alle Phasen überwacht, um wesentliche Argumentationen für den Investitionsentscheid zu liefern. Das „Risk IT“ widmet seine ganze Aufmerksamkeit den Risiken. Die Integration in das UN- Risikomanagement, eine Analyse der Risiken und die Risikosteuerung sind einige bedeutende Funktionen von „Risk IT“.[139] Trotz seiner Best Practice Empfehlung verfügt CobiT über gewisse Nachteile. Das Framework gilt als sehr komplex und umfangreich. Das erschwert den Einsatz in kleineren UN, z.B. auf Grund von geringeren personellen IT-Risikomanagementressourcen.[140]

[137] Vgl. Gadatsch: IT, S.11.
[138] Vgl. Knoll: Praxisorientiertes, S.79.
[139] Vgl. Königs: IT, S.289f.
[140] Vgl. Junginger: Werteorientierte, S.150.

4 Wesentliche Methoden des IT-Risikomanagements

4.1 Methoden der Risikoidentifizierung

4.1.1 Wesentliche Merkmale und Aufgaben

Die Risikoidentifikation erfolgt in Abhängigkeit von der Risikokategorie, im Falle der IT sind das vor allem operationale Risiken.[141] Dazu sind sämtliche IT- Ressourcen, deren Anwendungen und Besitzer zu erfassen und alle Angriffspfade anhand von Bedrohungs- und Verwundbarkeitsanalysen herzuleiten.[142] Anhand der Basis die den Analysemethoden zugrunde gelegt wird, kann eine Unterscheidung nach analytischen, prognostischen und kreativen Methoden vorgenommen werden. Die zur Anwendung kommenden Methoden werden in der Risikomanagement-Organisation fixiert.[143] Die Zahl der Analysemethoden ist umfangreich. Im Folgenden soll auf einige in der IT-Risikoidentifikation häufig benutze Verfahren näher eingegangen werden.

Eine Schadensausmaßanalyse ist oft kompliziert oder gar unmöglich, da sich die Schutzobjekte nicht konkret bewerten lassen. In diesen Fällen ist es empfehlenswert, mit einer Schwachstellenanalyse z.B. mangelhaft umgesetzte Grundschutzmaßnahmen zu identifizieren. Eine Schwachstelle bedeutet, wenn momentan angewandte Methoden keinen oder nur unzureichenden Schutz eines zu sichernden Objektes bieten. Die Risiko-Analysen dagegen wirken nur zielführend, wenn aus ihnen entsprechende Sicherheitsvorkehrungen abgeleitet werden können. In Fällen, bei denen dies nicht möglich ist, bietet die Schwachstellenanalyse zur Schutzmaßnahmenbildung, eine mögliche Alternative. Dazu sollten die Schwachstellen und die Relevanzen existenter Bedrohungen genau analysiert werden. Im Ergebnis der beiden Analysen kann eine Gesamteinschätzung der untersuchten Schwachstellen getroffen werden. Sollte sich in der Praxis im weiteren Zeitablauf zeigen, dass die zuvor vorhanden Bedrohungen nicht mehr bestehen, ist die Schwachstelle als unbedeutend einzustufen.[144]

[141] Vgl. Wolke: Risikomanagement S.4.
[142] Vgl. Knoll: Praxisorientiertes, S.126.
[143] Vgl. Junginger: Werteorientierte, S.213- 215.
[144] Vgl. Königs: IT, S.241f.

Dies gilt vor allem im Hinblick auf den Kosten-Nutzen-Aspekt, da die aufgezeigten Analysen und die daraus resultierenden Maßnahmen sich leicht kostenintensiv auswirken können.[145]

4.1.2 Fehlermöglichkeits- und Einflussanalyse (FMEA)

Die FMEA geht auf eine Entwicklung des US-Verteidigungsministeriums in den 1940er Jahren zurück, sie sollte Schwachstellen in technischen Systemen aufzeigen. Später wurde sie auch in modifizierter Form in der Luft- und Raumfahrt eingeführt. FMEA legt ein intaktes und störungsfreies System zugrunde und wird bereits in der Entwicklungsphase eines Produktes bzw. Prozesses genutzt, um frühzeitig das Ausmaß möglicher Komplikationen anhand von Fehleranalysen abschätzen zu können.[146] Die zur Analyse genutzte „Bottom up Methode“ soll aufzeigen, inwieweit fehlerhafte Einzelsysteme zu Störungen ganzer Systemkomplexe auf den nachfolgenden Ebenen führen können.

So wird zu Beginn der Analyse der gesamte IT-Komplex in einzelne Segmente differenziert und auf eventuelle Störquellen untersucht. Das Prinzip entspricht einer Schwachstellenanalyse, wodurch Maßnahmen eruiert werden können, die Störungen in einzelnen IT-Komponenten beseitigen und somit Fehler im gesamten IT-System abschwächen. Die Absicherung des Qualitätsmanagements ist heute das wesentliche Einsatzgebiet der FMEA, insbesondere in der Automobilindustrie und Medizingeräteherstellung. Der Verband der deutschen Automobilindustrie hat dazu standardisierte Vorlagen entwickelt, so werden für jeden Bereich potenzielle Fehler und deren Folgen, die damit verbundenen Fehlerursachen sowie geeignete Maßnahmen registriert. Im Bereich der IT wird FMEA in modifizierter Form genutzt, um die Sicherstellung großer bzw. komplexer Systeme zu ermöglichen oder für Anbieter von IT-Serviceleistungen, bei denen ein hohes Niveau der Verfügbarkeit und Sicherheit von IT-Komponenten zum Unternehmenserfolg führt.[147] Die FMEA untersucht in den einzelnen Fehlerzweigen die zu ermittelnden Fehlerquellen hinsichtlich der Auftrittswahrscheinlichkeit, der Bedeutung sowie der Entdeckungswahrscheinlichkeit. Diesen drei Faktoren werden stufenweise Werte von 1-10 zugeordnet, wobei 1 sehr gering und 10 sehr hoch darstellt. Das aus diesen drei Faktoren ermittelte

[145] Vgl. Ebert: Risikomanagement, S.70.
[146] Vgl. Prokein: IT, S.25.
[147] Vgl. Thies: Management, S.41f.

Produkt stellt die Risikoprioritätenzahl dar. Das wesentliche Merkmal der FMEA ist die konsequente Standardisierung und einheitliche Analyse anhand von Formblättern, die zu einer chronologischen und verständlichen Aufzeichnung erkannter Risiken führen.[148]

4.1.3 Fehlerbaumanalyse

Diese Methode begeht den Weg einer Analyse nach dem „Top-Down Prinzip". Dazu wird ein vorgegebenes Ereignis, welches unerwünscht ist, untersucht. Die möglichen Ereignisse werden logisch zu einer Baumstruktur verknüpft. Der Baum zeigt auf, welche sekundären Ereignisse innerhalb welcher Verknüpfung ein jeweils primäres Fehlerereignis herbeiführen.[149] Aus der Modellierung entsteht eine grafische Darstellung von Störereignissen, die durch systematisches Fortführen der Analyse zur Top - Störung führen. Diese Systematik wird solange fortgeführt, bis keine weiteren Unterscheidungen hinsichtlich neuer Störereignisse zur Top Störung mehr realisierbar sind.[150] Eine wesentliche Vorrausetzung für die Aussagekraft dieser Analyse ist die richtige Auswahl des initialen Störereignisses. Ist die Auswahl zu simpel gehalten, kann sich der Fehlerbaum unübersichtlich ausweiten, dagegen lässt eine zu konkrete Auswahl wichtige Fehlerquellen möglicherweise nicht in Erscheinung treten. Darüber hinaus erscheint die Untersuchung komplexer Systeme nur mit geeigneter Software realisierbar.[151] Die Symbole des Fehlerbaums werden dem Standard IEC 1025 entnommen. Durch die grafische Darstellung lassen sich mögliche Verknüpfungen mit Redundanzsystemen gut identifizieren, die somit Eintrittswahrscheinlichkeiten für das Top-Ereignis verringern. Außerdem können übersichtlich Modifizierungen vorgenommen werden, die eventuell eine bessere Finanzierung der Abwehrmaßnahmen zulassen. Zur Durchführung einer IT-Fehlerbaumanalyse wird die Fachkenntnis einer professionellen IT-Abteilung empfohlen. Die Anwendungsmöglichkeiten der Analyse erstrecken sich über Qualitätssicherungen, Systemanalysen bis zu Konfliktlösungen bei neuen bisher unbekannten Störereignissen.[152] Die Fehlerbaumanalyse soll eine qualitative und quantitative Betrachtung eines Systems ermöglichen.

---

[148] Vgl. Thies: Management, S.42f.
[149] Vgl. Siepermann: Risikokostenrechnung, S.38.
[150] Vgl. Bärwolf/Hüsken/Victor: IT, S.221.
[151] Vgl. Junginger: Wertorientierte, S.216.
[152] Vgl. Königs: IT, S.262f.

Der mögliche Mangel an Wahrscheinlichkeitsdaten erschwert vereinzelt eine umfassende quantitative Analyse.[153]

4.1.4 Checklisten

Checklisten sind als Methode der Risikoanalyse sehr weit verbreitet. Hierbei werden Erfahrungen aus der Vergangenheit genutzt, um vergleichbare zukünftige Risiken erkennen zu können. Die Form basiert auf Listen, die auf der Grundlage zurück liegender bekannter Ereignisse erstellt wurden. Dabei können sowohl interne aus dem UN bekannte Ereignisse, als auch extern identifizierte Risiken zum Aufstellen von Checklisten genutzt werden.[154] Sie dienen durch den Vergleich gesetzter Sollzustände, bei der Überprüfung von Systemen und Prozessen, zur Identifizierung von Schwachstellen. Durch eine Aufstellung von Fragen in Tabellenform, die meist einfach mit ja oder nein zu beantworten sind, kann so eine schnelle und effiziente Überprüfung vorgenommen werden. Die extern zur Verfügung gestellten Checklisten beruhen meist auf Best-Practice Ansätzen bzw. Standards. Das BSI hält zum Beispiel im Rahmen des IT-Grundschutzes dazu geeignete Checklisten bereit.[155] Die folgende Abbildung zeigt eine Checkliste aus einem Fragenkatalog des BSI. [156]

IT-Sicherheitsprodukte:

	PC	Ja	Nein
M 4.3	Setzen Sie ein Viren-Suchprogramm auf Ihrem PC ein? Wenn Ja, in welchem Turnus oder bei welchen Gelegenheiten?	☐	☐
M 4.4	Sind die Diskettenlaufwerke Ihres Rechners verschlossen? Alle Nur das Boot-Laufwerk	 ☐ ☐	 ☐ ☐
M 4.30	Nutzen Sie die in Anwendungssoftware angebotenen Sicherheitsfunktionen (z. B. die Verschlüsselung in Access oder Winword)? Wenn Ja, welche:	☐	☐
M 4.44	Überprüfen Sie eingehende Dateien auf Makro-Viren? Wenn Ja, in welchem Turnus oder bei welchen Gelegenheiten?	☐	☐

Abbildung 16: BSI: IT- Grundschutz Checkliste

Quelle: BSI: Grundschutz, S.9.

[153] Vgl. Bärwolf/Hüsken/Victor: S.221.
[154] Vgl. Ebert: Risikomanagement, S.20.
[155] Vgl. Junginger: Wertorientierte, S.220.
[156] Vgl. BSI: Grundschutzhilfsmittel, S.9.

4.1.5 Expertenbefragung

Diese prognostizierende Methode weist einen qualitativ geprägten Charakter auf und wird in der Praxis häufig angewendet. Sie eignet sich für Schwachstellen- und Risikoanalysen. So liefern Experten des eigenen UN oder unabhängige Experten mit einem moderaten Aufwand fachlich kompetente Einschätzungen zu Risiken. Eine große Bedeutung haben Betrachtungen von Verlustereignissen, Schwachstellen und Risiken, durch die oft objektiveren externen Berater. Sie profitieren von besseren Erfahrungen und Vergleichsmöglichkeiten. Wesentlich entscheidend für den Erfolg dieser Methode ist der offene Umgang mit Risiken. Zur Erörterung werden Fragebögen genutzt, persönliche Gespräche geführt oder Workshops betrieben.[157] Bei der Befragung ist es sinnvoll, die Risiken nicht isoliert aus dem Blickwinkel des IM zu betrachten, sondern aus Sicht aller Geschäftsprozesse in die das IM involviert ist. Damit wird ein rein technikfixiertes Risikomanagement verhindert.[158]

4.1.6 Delphi- Methode

Im Rahmen dieses Verfahrens wird eine mehrstufige, systematische und anonyme Befragung von Experten zu Risiken durchgeführt. Jede abgeschlossene Fragerunde wird anschließend statistisch ausgewertet. Im Technologiebereich hat diese Befragungstechnik in den letzten Jahren an Zustimmung gewonnen.[159] Das Ziel der Befragungen ist anhand von vorgefertigten Fragebögen, Erkenntnisse über Eintrittswahrscheinlichkeiten, Zeitspannen und Konsequenzen von IT-Risiken zu erlangen. Demnach werden Ursache-Wirkungsprinzipien im IT-Risikomanagement besser verstanden, um zukünftige Bedrohungen zu erkennen. Bei großen UN kann z.B. durch Chat-Technik die Expertenrunde einfach auf mehrere Bereiche oder Standorte ausgeweitet werden. Die erforderliche Rückkopplung erfolgt somit zeitnah aus der letzten Fragerunde an die Teilnehmer. Die anonyme Befragung kann auch Nachteile mit sich bringen, da gerade bei der Bewertung von IT-Risiken eine Meinungsvielfalt oft zielführend ist. Des Weiteren ist dieses Verfahren oft kosten- und zeitaufwendig.[160]

---

[157] Vgl. Seibold: IT, S.88.
[158] Vgl. Junginger: IT, S.225.
[159] Vgl. Knödler: Puplic, S.173.
[160] Vgl. Knoll: Praxisorientiertes, S.157f.

4.1.7 Brainstorming und Brainwriting

Brainstorming ist eine sehr populäre Kreativtechnik, deren Erfindung durch Alex F. Osborn auf das Jahr 1939 zurückgeht. Vor allem im IM sind solche Techniken beliebt, da sich Risiken in diesem Bereich oft besser kreativ lösen lassen.[161] Die Ideenfindung erstreckt sich über drei Ebenen. Auf der logischen Ebene wird rational das Problem erörtert und die möglichen Lösungsansätze aufgestellt. Im nächsten Schritt wird die Problemstellung intuitiv weitergeführt, um im dritten Abschnitt letztlich verwendbare Lösungen zu selektieren und rational zu begründen. Der Erfolg eines Brainstormings ist von der strikten Einhaltung bestimmter Regeln abhängig. So ist Kritik während dessen absolut unerwünscht, jeder Beteiligte darf unvoreingenommen seine Ideen äußern, alle dargelegten möglichen Lösungen sind durch jeden Teilnehmer zu verinnerlichen, mit dem Ziel in kürzester Zeit einen großen Ideenpool zu bilden. Eine große Spontanität soll den Prozess der Ideenfindung auf einem hohen Niveau halten. Soll die Gleichgewichtigkeit und der gegenseitiger Respekt erhöht werden, bietet sich das Brainwriting in schriftlicher und anonymer Form an.[162]

Als Handlungsempfehlung für die IT-Risikoidentifizierung lässt sich feststellen: In diesem Prozess sollten mehrere Verfahren genutzt werden, wobei ausreichend Zeit und ein betriebswirtschaftlich vertretbares Budget benötigt wird. Dabei sind alle Indikationen (rechtliche, technische, fachliche) mit einzubeziehen und das Vorgehen methodisch zu gestalten und offen zu vertreten. Auf externe Informationen sowie Beratung durch externe Experten sollte bei Unsicherheiten nicht verzichtet werden.[163]

Zusammenfassend werden die vorgestellten Methoden der Risikoidentifizierung in der folgenden Abbildung nach ihrer Funktionsweise dargestellt.

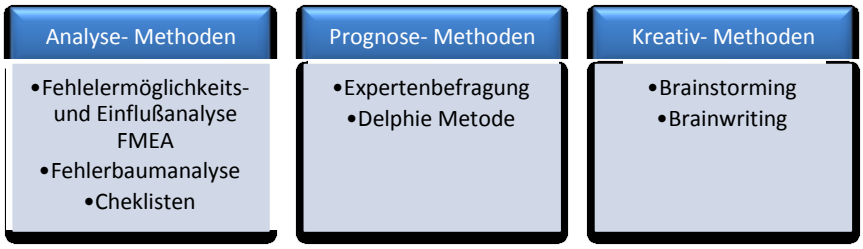

Abbildung 17: Übersicht der vorgestellten Risikoidentifizierungsmethoden
Eigene Darstellung

[161] Vgl. Seibold: IT, S72.
[162] Vgl. Junginger: Werteorientierte, S.232f.
[163] Vgl. Knoll: S.129.

4.2 Methoden der Risikobewertung

4.2.1 Merkmale der Risikobewertung

Dieser Teil des Risikomanagementprozesses schließt sich der zuvor beschriebenen Risikoidentifizierung an und ist ein grundlegender Bestandteil für das IT- Risikomanagement. Die Identifikation und Bewertung von IT-Risiken wird in der ISO 27001 zur Risiko-Einschätzung zusammengefasst.[164] Eine reelle und effektive Bewertung der Risiken bildet das Fundament, um in der nächsten Prozessstufe IT-Risiken wirtschaftlich zu steuern. In der Hinsicht sind gesamtunternehmerische Ziele wie Gewinnmaximierung und Kostensenkung bei gleichzeitig verbesserten IT- Schutzmaßnahmen vereinbar.[165] Eine primär vorgenommene Einteilung in quantitative und qualitative Risikobewertungen wird im Allgemeinen als sinnvoll erachtet.[166]

Der Begriff des Schadens spielt eine entscheidende Rolle. Er beschreibt das eingetretene Ereignis, welches von einem geplanten Ziel abweicht (schlagend gewordenes Risiko). Die Schadenshöhe resultiert aus einem messbaren und nicht direkt messbaren Schaden. Die unmittelbaren Schadensersatzleistungen werden den messbaren Schäden zugerechnet, ungewisse Reputationsschäden oder Opportunitätskosten werden jedoch als nicht direkt messbarer Schaden bezeichnet.[167] Ein weiteres Kriterium ist die Verlusthöhe, die im Verhältnis zur Eintrittshäufigkeit betrachtet wird. Dabei haben häufig zu erwartende Schäden eine geringe Verlusthöhe, dem gegenüber haben selten auftretende unerwartete Schäden und Extremereignisse (Stressschäden) eine sehr hohe Verlusthöhe. Die Grafik auf der folgenden Seite stellt diesen Sachverhalt dar.

Die Bewertung der Schadenshöhe, der Verlusthöhe und der Verlusthäufigkeit sind für den nächsten Prozessabschnitt, der Risikosteuerung, elementar.[168] Das Risiko stellt das Produkt aus der Eintrittswahrscheinlichkeit und der Schadenshöhe dar. Der zu erwartende Schaden wird aus den Faktoren der Schadenshäufigkeit und der durchschnittlich zu erwartenden Schadenshöhe gebildet. Die Eintrittswahrscheinlichkeit definiert mit welcher Wahrscheinlichkeit ein Ereignis in einer bestimmten Periode auftritt.[169]

---

[164] Vgl. Kersten/Reuter/Schröder: IT, S.32.
[165] Vgl. Seibold: IT, S.87.
[166] Vgl. Wolke: Risikomanagement, S.4; Eckert: IT, S.210.
[167] Vgl. Knoll: Praxisorientiertes, S.138.
[168] Vgl. Königs: IT, S.34- 36.
[169] Vgl. Ebert: Risikomanagement, S.34.

Hier ergibt sich vielfach das Problem beim Aufbau einer IT-Infrastruktur und des ISMS. IT-Konzepte mit reduzierter Eintrittswahrscheinlichkeit sind kostenintensiv. Das Dilemma entsteht in einer unzulänglichen Risikobewertung, wenn die Eintrittswahrscheinlichkeit überschätzt und für den IT-Bereich ein irrationales Budget aufgewendet wurde. [170]

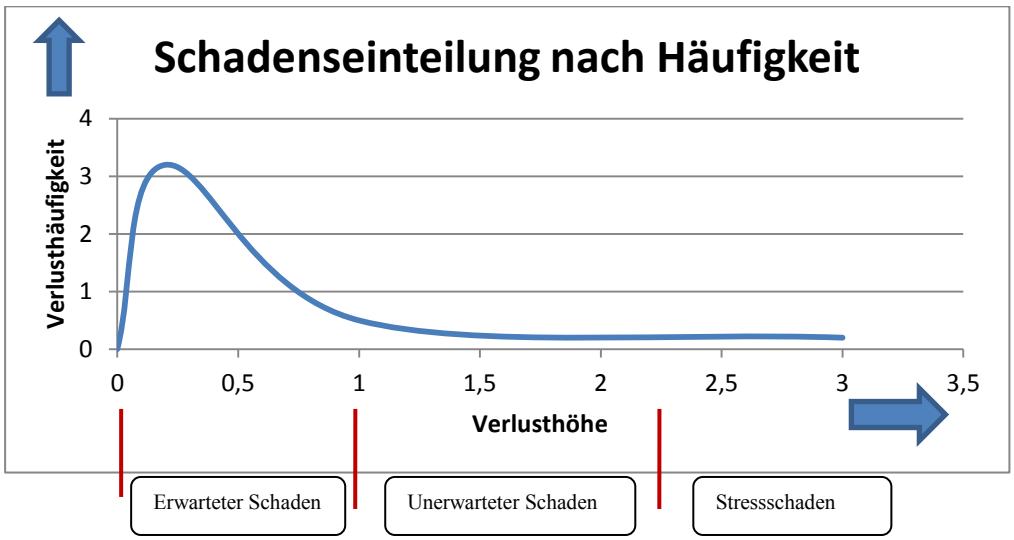

Abbildung 18: Schadenseinteilung nach Häufigkeit
Eigene Darstellung (in Anlehnung an Seibold: IT, S.14.)

4.2.2 Quantitative Bewertungen

4.2.2.1 Bedeutende Merkmale der Quantitativen Bewertungen

Die Quantitativen-Methoden sollen evidente Werte bereitstellen und dienen in erster Linie der Analysierung wesentlicher IT-Risiken. So lassen sich konkrete Zahlen beispielsweise im Rahmen einer Revision oder Wirtschaftsprüfung darlegen. Diese Verfahren sind aber in vielen Fällen kosten- und zeitintensiv. Das ist insbesondere problematisch, wenn sich aus einer quantitativen Analysierung kein Erkenntnisgewinn über die wesentlichen IT-Risiken ergibt.[171] Daher sollte diese Form der Risikobewertung immer an Positionen zur Prozess- und Systemverbesserung eingesetzt werden, woraus ein optimaler Nutzen resultiert.[172]

[170] Vgl. Königs: IT, S.274.
[171] Vgl. Knoll: Praxisorientiertes, S.133.
[172] Vgl. Ebert: Risikomanagement, S.37.

4.2.2.2 Value at Risk

Der Value at Risk wird auch als Probale Maximum Loss[173], Money at Risk, Capital at Risk, Cashflow at Risk oder Operational at Risk bezeichnet. Die Entwicklung des VaR, durch die Investmentbank Morgan Stanley, geht auf das Jahr 1994 zurück, nachdem in den Jahren zuvor Finanzmarktrisiken eklatant angestiegen waren. In Folge wurde der VaR weiterentwickelt, wobei der Focus auf den ausfallorientierten Risiken lag. Der Value at Risk ist ein verlustorientiertes Risikomaß, der eine negative Abweichung des Zielwertes ausdrückt. Mit dem VaR lassen sich verschiedene Risikokategorien verknüpfen und analysieren.[174] Übertragen auf den IT-Bereich ist der VaR der maximale Schaden, der unter normalen Bedingungen innerhalb eines bestimmten Zeitraums und einer bestimmten Wahrscheinlichkeit (Konfidenzniveau z.B. 90%) nicht überschritten wird. In der Beurteilung der operationalen Risiken (IT-Risiken) hat sich die simulierte VaR-Methode nach dem Monte-Carlo-Prinzip bewährt. Dazu werden verschiedene Situationen mit Werten definiert und mit Wahrscheinlichkeitsaussagen verknüpft. Aus dem Ergebnis werden nachfolgend willkürlich Daten herausgezogen und Berechnungen unterworfen. Dieses Zufallsexperiment wird sehr oft wiederholt. Als Endergebnis liegt eine empirische Wahrscheinlichkeitsverteilung vor, die zur VaR Berechnung genutzt wird.[175] Mit dieser Verfahrensweise lassen sich weiterhin aggregierte Risikosituationen darstellen. Auf Grund des großen Erstaufwandes bei den Planungen der Simulationssituationen wird der VaR in den meisten UN zur Bestimmung des gesamten operationalen Risikovolumens genutzt, um im Weiteren daraus das Risikovolumen der IT-Benutzerrisiken herzuleiten.[176]

Die folgende vereinfachte Darstellung zeigt eine hypothetische Kreuztabelle für eine Monte-Carlo-Simulation eines IT-Dienstleisters, in Bezug auf die einzelnen Dienstleistungen an seinen Kunden und den auftretenden Störungen im zentralen Rechenzentrum.

[173] Vgl. Siepermann: Risikokostenrechnung, S.28.
[174] Vgl. Wolke: Risikomanagement, S.27.
[175] Vgl. Knoll: Praxisorientiertes, S.169.
[176] Vgl. Seibold: IT, S.101

Auswirkungen im Bezug auf die Verfügbarkeit der erforderlichen IT- Service-leistungen						
IT Risiko P in %/AV in %	Kunde 1		Kunde 2		Kunde 3	
	DL A	DL B	DL C	DL B	DL A	DL D
Ausfälle der Energiever-sorgung	1,5/0	1,5/0	3/0	0,5/0	0,02/0	2/0
Ausfälle des Primär-Backupsystems	0,05/95	1,2/0	3,5/0	0,02/0	0,1/95	0,5/85
Leistungsprobleme der Datenverschlüsselung	0,01/70	0,1/85	0,05/65	1,5/95	5/99	0,001/15
DL: IT-Dienstleistung ; P: Eintrittswahrscheinlichkeit in%; AV: Verfügbarkeit in %						

Abbildung 19: Kreuztabelle: IT Risiken für eine Monte Carlo Simulation
Eigene Darstellung (in Anlehnung an Knoll: Praxisorientiertes, S.169.)

4.2.2.3 Sensitivitätsanalyse

Mit dieser Methode - auch umschrieben als „Was wenn"-Analyse[177]- überprüft das IT-Risikomanagement, inwieweit sich Veränderungen bezüglich der IT-Risikoursachen, der Verwundbarkeit oder möglichen Schutzmaßnahmen auf die Eintrittswahrscheinlichkeit und die Schadenshöhe auswirken. Dieses Verfahren kann immer dann im Rahmen der IT-Risikobewertung eingesetzt werden, wenn die Folgen von Maßnahmen bekannt sind. Lassen sich veränderte Faktoren bewerten und Abhängigkeiten verständlich darlegen, so kann ein exaktes Ergebnis herbeigeführt werden. Gibt es keine mathematischen Erkenntnisse oder sind diese zu umfangreich, kann mit Hilfe von Iterationen oder Schätzungen die Analyse durchgeführt werden.[178] Dieses Verfahren ist damit gut zur Analyse der Risikofaktoren (Einflussgrößen) geeignet. [179]

[177] Vgl. Fiege: Risikomanagement, S.172f.
[178] Vgl. Knoll: Praxisorientiertes, S.175.
[179] Vgl. Wolke: Risikomanagement, S.26.

Mit der Sensitivitätsanalyse lassen sich zwei Aufgaben lösen: Zum einen können Veränderungen bezüglich der Höhe von Risikowirkungen ermittelt werden. Im Focus sollten dabei Einflüsse stehen, die schon bei geringen Variationen das Ergebnis erheblich beeinflussen. Zum anderen zeigt die Analyse auf, in welchen Intervallen die Einflüsse variieren, ohne signifikant das Ergebnis zu beeinflussen. Häufig wird die Sensibilitätsanalyse, als ergänzendes Instrument im Rahmen einer BSC, durch das IM eingesetzt. Die Sensitivitätsanalyse ermöglicht, die Veränderungen der Risikoursachen und in welchem Ausmaß sie die Risikofolgen beeinflussen, besser zu verstehen.[180]

4.2.2.4 Stresstest

Die Stresstest-Methode ist eine spezielle Sensitivitäts- bzw. Szenarioanalyse. Sie bewertet mit Hilfe des VaR die Auswirkungen von speziell(en), bedrohenden Ursachen auf die IT-Ressourcen. Damit werden nur solche Ereignisse untersucht, die mit einer geringen Eintrittswahrscheinlichkeit verbunden sind und plötzliche Veränderungen hervorrufen und zu außerordentlichen Konsequenzen führen. Dieses Worst-Case-Szenario soll nach dem „entweder- oder- Prinzip“, Entscheidungen für die notwendigen Maßnahmen erleichtern. Diese Form der Risikoanalyse wird somit vorrangig selten bis einmalig, im Rahmen von generellen Katastrophen- und Notfallplanungen durchgeführt und antizyklisch auf Grund maßgeblich veränderter UN-Umfeldbedingungen, erneut initialisiert und wenn nötig angepasst.[181]

4.2.3 Qualitative Bewertungen

4.2.3.1 Bedeutende Merkmale der Qualitativen Bewertung

Qualitative Methoden werden oft für einen ersten Überblick und zur Abschätzung nicht monetärerer Schäden genutzt sowie bei der Bewertung von Reputationsschäden benötigt. Die qualitative Analyse verfolgt das Ziel, primär nicht messbare Risiken quantifizieren zu können.[182] Mitunter kann auf eine ressourcenhungrige quantitative Bewertung verzichtet werden, insofern das IT-Risikomanagement seinen Verpflichtungen nachkommt und die gesetzten Ziele erreicht. Bisweilen und im Hinblick auf

[180] Vgl. Junginger: Werteorientierte, S.265.
[181] Vgl. Knoll: Praxisorientiertes, S.178.
[182] Vgl. Wolke: Risikomanagement, S.63.

die zu platzierenden Schutzmaßnahmen zeigt sich, dass nachträgliche quantitative Bewertungen gegenüber den qualitativen Einschätzungen keine wesentlichen Nutzensteigerungen ergeben. Darüber hinaus mangelt es oft an aussagekräftigen Daten, die aber für eine quantitative Risikobewertung unerlässlich sind. So kann eine zunächst qualitativ durchgeführte Risikobewertung, zu einer nachfolgenden quantitativen Einschätzung herangezogen werden.[183] Im Rahmen Qualitativer-Methoden werden zuvor verbal formulierte Risiken (gering, mittel, hoch oder katastrophal), um quantitative Merkmale ergänzt, indem die Verbalaussagen numerisch skaliert werden.[184]

4.2.3.2 Scoring- Methode

Diese Methode ist sowohl zur qualitativen als auch quantitativen Bewertung von IT-Risiken geeignet, darüber hinaus leicht zu Handhaben und stellt einen moderaten Aufwand dar.[185] Es werden im Wesentlichen zwei Verfahren genutzt, zum einen die Nutzwertanalyse und zum anderen die Ereignisbaumanalyse.

Die Nutzwertanalyse stellt eine optimale Grundlage dar, die zu erbringenden Leistungen festzulegen und die dazu notwendigen Mehrkosten zu ermitteln. Die Festlegung der Risikoklassen erfolgt durch logische ODER-Verknüpfungen. So kann beispielsweise der Risikoklasse „Niedrig“, Mehrkosten von 1 Mio. Euro, 2 Monate Lieferverzug oder ein Performancerückgang von 10% zugeordnet werden.[186]

Die Ereignisbaumanalyse (ETA: Event Tree Analysis) untersucht eine primäre Störung und die sich hieraus ergebenden systematischen Veränderungen. Eine Störung kann z.B. eine ausgefallene Systemkomponente oder ein Systemfehler sein. Dieses Verfahren beschreitet den Weg einer „Bottom-Up“-Analyse und wird den Kausal-Methoden zugerechnet. Ausgehend von dem zu untersuchenden Ereignis, wird eine Baumstruktur von links nach rechts grafisch entwickelt. Die Kausalität wird durch entsprechende UND/ ODER-Verknüpfungen hergestellt und die Ereignisse an den Gabelpunkten mit Eintritts-Wahrscheinlichkeiten bewertet.[187]

[183] Vgl. Knoll: Praxisorientiertes, S.133.
[184] Vgl. Königs: IT, S.50.
[185] Vgl. Fiege: Risikomanagement, S.182f.
[186] Vgl. Wolke: Risikomanagement, S.66.
[187] Vgl. Seibold: IT, S.96f.

Der Baum endet, mit dem höchsten Schadensausmaß bzw. mit dem Eintritt eines maximalen Schadensereignisses oder einer neu zu analysierenden Störung. Für große komplexe IT-Systeme eignet sich diese Analyse trotz PC- Unterstützung nur bedingt, da das numerisch ermittelte Ergebnis anhand der geschätzten Wahrscheinlichkeiten zu erheblichen Abweichungen führen kann. Eine ganzheitliche Risiko- oder Schwachstellenanalyse von IT-Komplexen ist daher mit dieser Methode unrealistisch.[188] Die subjektive Betrachtungsweise im Rahmen der Analyse stellt einen weiteren wesentlichen Nachteil dar.[189]

In Anbetracht der Quantifizierung von betriebswirtschaftlichen Risiken sind die Scoring-Methoden jedoch ein unverzichtbares Instrument, insbesondere im Rahmen eines VaR orientierten Risikomanagements.[190]

4.2.3.3 Kennzahlen

Die Kennzahlen aus betriebswirtschaftlichen Analysen können ebenso zur Beurteilung von Risiken genutzt werden. Sie beruhen meist auf Kosten- und Nutzenbewertungen. So können im Rahmen der Risikoanalysen die Auswirkungen von Störungen auf die entsprechenden Kennzahlen untersucht werden, um daraus finanzielle Auswirkungen abzuleiten. Dafür kommt insbesondere die für den IT-Bereich ohnehin relevante TCO-Kennzahl in Betracht, aber auch Kennzahlen der BSC spielen hierbei eine große Rolle. In vielen Fällen existiert zudem für das IM eine BSC, basierend auf dem CobiT-Framework, das sich wiederum detailliert mit dem IT-Risikomanagement befasst. Mit Hilfe von Kennzahlen lassen sich Sachverhalte quantitativ ausdrücken, um komplexe Strukturen überschaubar zu gestalten. Aus den klassischen IT-Kennzahlen können nicht unmittelbar Risiken hergeleitet werden, aber entsprechende Szenario-Analysen projiziert auf die Kennzahlen können die Auswirkungen von Störungen ermitteln. Die typischen IT-Kennzahlen besitzen meist einen technischen Charakter und weisen somit Werte zur Verfügbarkeit, Schnelligkeit und Leistungsfähigkeit von IT-Systemen aus. Auch daraus lassen sich Erkenntnisse zur Analyse nutzen.[191]

---

[188] Vgl. Königs: IT, S.264f.
[189] Vgl. Knoll: Praxisorientiertes, S.174.
[190] Vgl. Wolke: Risikomanagement, S.66.
[191] Vgl. Seibold: IT, S.94f.

Funktional differenzieren sich qualitative IT-Risikokennzahlen, die Sachverhalte verbal beschreiben (z.B. hoch, stark oder moderat), gegenüber quantitativen IT-Risikokennzahlen, die mathematische Beziehungen und Messvorschriften beschreiben. Über die zuvor dargelegten klassischen IT-Kennzahlen hinaus, gibt es auch moderne spezifische IT-Risikokennzahlen, die IT-Schlüsselkennzahlen, wie z.B. Key Risc Indicator, IT-Risikotreiber oder die Risikoprioritätszahl. Neben der qualitativen Analyse eignen sich alle zu einer weiteren quantifizierten Bewertung.[192] Eine wichtige Rolle kommt der Risikoprioritätszahl (RPZ) zu. Sie stellt das Produkt aus drei Faktoren dar:

- **S**ubjektive Bedeutung eines IT-Risikos- **S**
- Geschätzte **A**uftritts- bzw. Eintrittswahrscheinlichkeit eines IT-Risikos- **A**
- Geschätzte **E**rkennungs- bzw. Entdeckungswahrscheinlichkeit- **E**
-  RPZ = **S** x **A** x **E** [193]

Dabei kann jeder Faktor mit einem Wert von 1 – 10 bestimmt werden, daraus ergibt sich die niedrigste RPZ = 1 und die größte RPZ = 1000. Je größer der Wert, desto höher liegt das IT-Risiko und umso schwerwiegender sind die damit verbundenen Ursachen. Die einzelnen Werte werden übersichtlich in einer Tabelle in Verbindung zu verbal formulierten Klassifikationen geordnet. Die RPZ weist eine enge Verbindung zur FMEA auf.[194]

4.2.4 Risikoportfolio

Das Risikoportfolio ist eine zweidimensionale graphische Darstellung der Risk-Map (Risikolandkarte). Die verbal formulierten und numerisch unterlegten Eintrittswahrscheinlichkeiten sowie Schadensausmaßklassen können so Risikoszenarien zugeordnet werden. Das ist insbesondere für das strategische IT-Risikomanagement von Interesse. Durch Risikoakzeptanzlinien, die in dieses Portfolio übernommen werden können, lassen sich mögliche strategische Ausrichtungen besser erkennen und planen. Des Weiteren ermöglichen Risikoakzeptanzlinien schnell Risiken zu erkennen, die keiner Maßnahmen bedürfen und akzeptiert werden können. Diese Möglichkeiten sind wiederum für die Risikosteuerung, im nächsten Prozessabschnitt, elementar.[195]

---

[192] Vgl. Prokein: IT, S.36f.
[193] Vgl. Lenges: Framework, S.32f.
[194] Vgl. Knoll: Praxisorientiertes, S.165.
[195] Vgl. Junginger: Werteorientierte, S.250f.

Die folgende Darstellung zeigt ein mögliches Risikoportfolio.

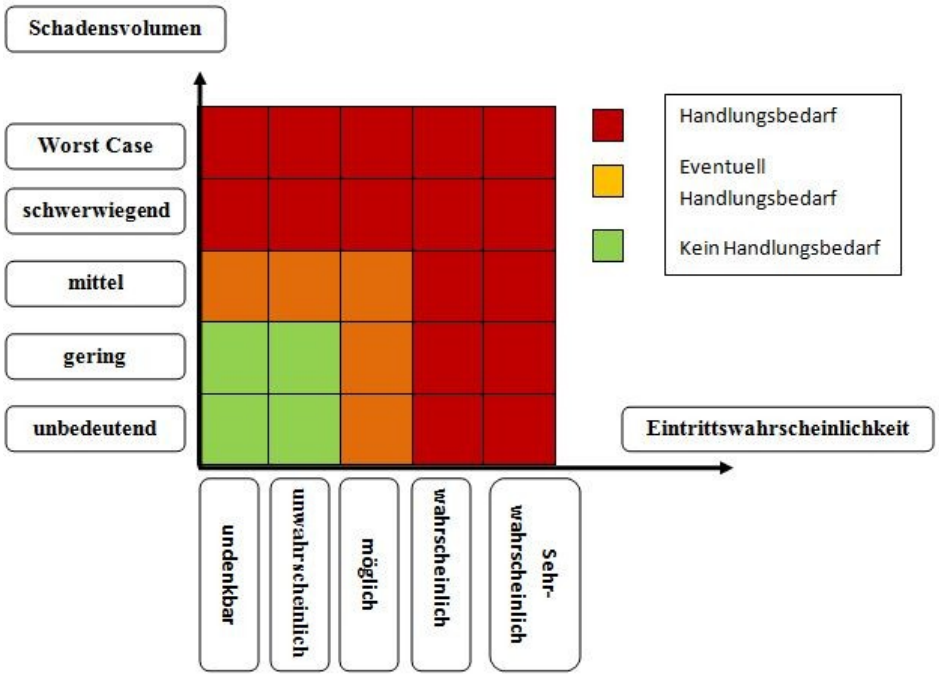

Abbildung 20: Risikoportfolio

Eigene Darstellung (in Anlehnung an Königs: IT, S.25.)

Die UN- Leitung wird ihrerseits, über die Akzeptanzlinie hinaus, weiter Akzente im Umgang mit Risiken setzen, insbesondere aus betriebswirtschaftlicher Sicht, anhand von Kosten-Nutzen-Analysen, um im Prozess der Risikosteuerung eine ökonomische Bewirtschaftung der Risiken zu ermöglichen.[196]

Der Vorteil der Darstellung von Risiken in einem Portfolio ergibt sich auch aus operativer Sicht, durch die grafische und glaubhafte Darstellung von Risikosituationen. Darüber hinaus bietet die Möglichkeit einer quantitativen sowie qualitativen Darstellung, eine einfache Art verschiedene Risiken zu vergleichen, ohne dabei komplizierte nummerische Darstellungen analysieren zu müssen. Damit hat sich die Portfoliotechnik in der Praxis, als ein wesentliches Element des IT-Risikomanagements etabliert.[197] Die mangelnde temporäre Betrachtung der Risikotreiber, also die Risikoentwicklung, sowie die einseitige Schadensbetrachtung ohne Chancen-Berücksichtigung sind die wesentlichen Nachteile des Risikoportfolios.[198]

[196] Vgl. Königs: IT, S.24f.
[197] Vgl. Finke/Romeike: Erfolgsfaktor, S.193.
[198] Vgl. Junginger: Wertorientierte, S.251f.

4.2.5 Risiko -Katalog

Für eine nachhaltige Risikobewirtschaftung ist eine Registrierung von Risiken mit Hilfe eines Risiko-Kataloges (IT-Risikoregister, -inventar oder -lexikon) durchzuführen. Der Risiko-Katalog ist nicht trennscharf dem Bereich der Risikobewertung zuzuordnen, sondern wird in den meisten Fällen bereits bei der Risikoidentifikation genutzt und eignet sich darüber hinaus zur Vollständigkeitsprüfung von Portfolien. Im Rahmen der Best-Practice Empfehlungen (z.B. CobiT) sind diese Kataloge bereits enthalten.[199] Dabei ist ein modularer Aufbau zu beachten, der flexible Anpassungen, an häufig ändernde Bedrohungen ermöglicht. Somit kann der Rahmen der Kataloge unternehmensabhängig stark variieren und sich in seiner Aufgabe erheblich unterscheiden (Nachweis für Zertifizierungen, Berichterstattungen oder Risikokontrolle in verschiedenen Bereichen). Aus dieser Differenzierung ergibt sich, dass mehrere Risiko-Kataloge in einem UN existieren können, die ausgerichtet an den gesamtunternehmerischen Zielen, durch die UN-Leitung zu einem Gesamtrisiko-Katalog zusammengefasst werden.[200]

So werden beispielsweise auch in den Basel II/III Regeln explizit operationelle IT-Risiken benannt. (vgl. Kapitel 3.1.2.2 S.20). In der ISO 27005 (Annex C) sollen entsprechende kategorisierte Bedrohungslisten die Grundlage zum Aufbau unternehmensspezifischer Risiko-Kataloge bilden und zugleich eine normierte Schwachstellenanalyse ermöglichen.[201] Das BSI stellt im Rahmen des „IT-Grundschutz“ entsprechende Gefährdungs- und Maßnahmen-Kataloge bereit, die ebenfalls für die Ausgestaltung detaillierter Risiko-Kataloge in den UN genutzt werden können.[202]

Ein IT-Risikokatalog kann mit geeigneter Software geführt werden und wird damit als IT-Risikodatenbank bezeichnet. In einem Risikokatalog wird häufig ein entsprechender Maßnahmenkatalog nach dem Schema bestehende bzw. vorgeschlagene Maßnahmen integriert. Diese Zusammenführung beschreibt einen IT-Risikoplan. Eine Risikoliste ist ein anhand von Dringlichkeiten geführter Risikokatalog. Daraus lassen sich für die UN-Leitung die elementarsten Risiken zu einer „Hitliste“ zusammenfassen.[203]

---

[199] Vgl. Seibold: IT, S.71.
[200] Vgl. Königs: IT, S.25f.
[201] Vgl. Kersten/Reuter/Schröder: IT, 129f.
[202] Vgl. BSI: Grundschutz, o.S.
[203] Vgl. Knoll: Praxisorientiertse, S.187.

4.3 Methoden der Risikosteuerung

4.3.1 Wesentliche Merkmale und Aufgaben

Die zuvor vorgestellten Methoden der Risikoidentifikation und Risikobewertung bilden die Basis für den Kern des IT-Risikomanagements, die IT-Risikosteuerung. Das Ziel einer nachhaltigen Risikobehandlung kann nur erreicht werden, wenn die Risiken effizient und effektiv steuerbar sind. Für den Umgang mit Risiken sind klare Maßnahmen und geeignete Instrumente zu bestimmen. Daran sind wesentliche Ziele des IT-Risikomanagement geknüpft: Eine durch alle Mitarbeiter getragene Risikopolitik und -kultur, eine offene und ungehinderte Kommunikation von Risikosituationen, Risiken tolerierbar zu gestalten und dabei Chancen zu erhalten, das Risikomanagement ökonomisch zu betreiben, Krisensituationen zu beherrschen, Schäden und deren Folgen zu reduzieren und Risikotendenzen vorhersagen zu können.[204] Auf dieser Grundlage ist eine Risikostrategie im Bezug auf die Steuerung der Risiken zu entwickeln. Im Mittelpunkt stehen dabei Eintrittswahrscheinlichkeit sowie Schadenshöhe, zu deren Reduzierung sind meist sich monetär auswirkende Maßnahmen notwendig. Daher gilt für die Strategiefindung, der Aufwand für diese Maßnahmen sollte niedriger sein, als die Summe der Risiken der das UN ausgesetzt ist.[205]

Die Risikosteuerung baut im Wesentlichen auf vier Strategien:

- Risikovermeidung
- Risikoverminderung
- Risikoübertragung
- Risikoakzeptanz

Die ISO 27001 (Anhang A) weist hierzu geeignete Techniken aus. Darüber hinaus ist es den UN freigestellt, diese mit weiteren Möglichkeiten beispielsweise aus anderen Standards oder Frameworks zu ergänzen oder zu kombinieren.[206]

[204] Vgl. Seibold: IT, S.135.
[205] Vgl. Ebert: Risikomanagement, S.70.
[206] Vgl. Kersten/Reuter/Schröder: IT, S.103-108.

4.3.2 Risikovermeidung

Das ist die effektivste Form der Risikosteuerung, mit der die Eintrittswahrscheinlichkeit bzw. die Schadenshöhe absolut optimiert wird. Ein auf null gesetztes Risiko birgt keine Gefahr oder Störung, allerdings klammert diese Strategie auch kategorisch Geschäftserfolge aus.[207] Somit kommt diese Methode für eine Steuerung von expliziten Risiken in Betracht, die entweder einen Existenz bedrohenden Charakter aufweisen oder extreme monetäre Schäden verursachen.[208] Andererseits kann eine konsequente temporäre Risikovermeidung, die mit einem unmittelbaren monetären Aufwand verbunden ist, einen möglichen gravierenderen Reputationsschaden verhindern. (z.B. Abschaltung eines E- Shops in Folge eines Hacker-Angriffs).[209] Die Verlagerung bzw. Verteilung identifizierter Schwachstellen (z.B. in UN-externe Backup-Systeme) oder zusätzliche Maßnahmen (Brandschutzverbesserungen im Servergebäude) ermöglichen eine Risikovermeidung.[210]

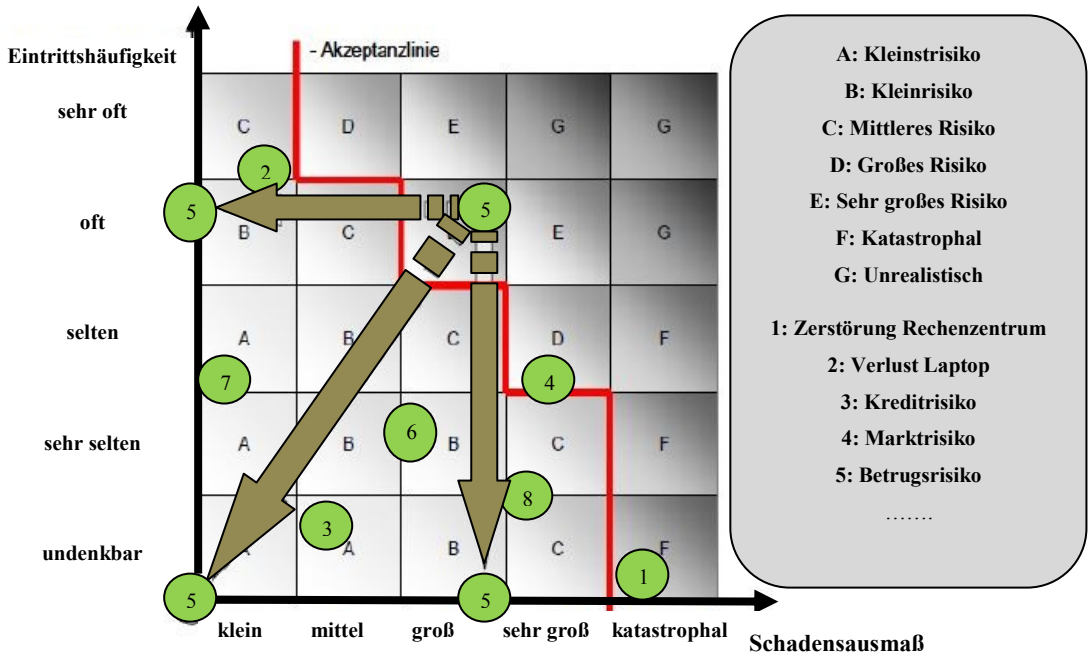

Abbildung 21: Risikovermeidung

Eigene Darstellung (in Anlehnung an Königs: IT, S.25.)

[207] Vgl. Lenges: Framework, S.132.
[208] Vgl. Siepermann: Risikokostenrechnung, S.44.
[209] Vgl. Seibold: IT, S.30.
[210] Vgl. Kersten/Reuter/Schröder: IT, S.58.

4.3.3 Risikoverminderung

Ein identifiziertes Risiko kann mit gezielten Maßnahmen verändert werden, d.h. die Eintrittswahrscheinlichkeit oder das Schadensmaß kann deutlich verringert werden. So könnte beispielsweise eine Arztpraxis, anstatt wie bisher mit einer klassischen DSL Verbindung, eine sichere VPN Line nutzen, um Patientendaten zu versenden. So wird die Eintrittswahrscheinlichkeit eines Reputationsschadens auf Grund mangelnder Vertraulichkeit reduziert. Eine Reduzierung kann jedoch nicht vollständig das Risiko und seine Folgen eliminieren.[211] Je nach Vorgehensweise werden aktive (ursachenbezogene) oder passive (folgebezogene) Reduzierungsmaßnahmen unterschieden. Aktive Maßnahmen beeinflussen direkt Eintrittswahrscheinlichkeit und/oder das Schadensausmaß, passive Verminderungen wirken in der Folge einer bereits eingetretenen Störung und gehen strategisch in einen Risikotransfer über.[212] Eine Risikodiversifikation wird zum Teil der Risikoverminderung unterstellt, was aber nicht zwangsläufig eine Reduzierung des Risikovolumens bedeuten muss, sondern eine Umwandelung des Schadenvolumens in eine Eintrittswahrscheinlichkeit bedeuten kann.[213] Ein IT-Dienstleister baut zum Beispiel zur Sicherheit einen zweiten Serverstandort auf. Die Möglichkeit eines Ausfalls verdoppelt sich so. Fällt jedoch nur ein Standort aus, ist nur ein Teil der Kunden betroffen und somit verringert sich die Schadenshöhe.

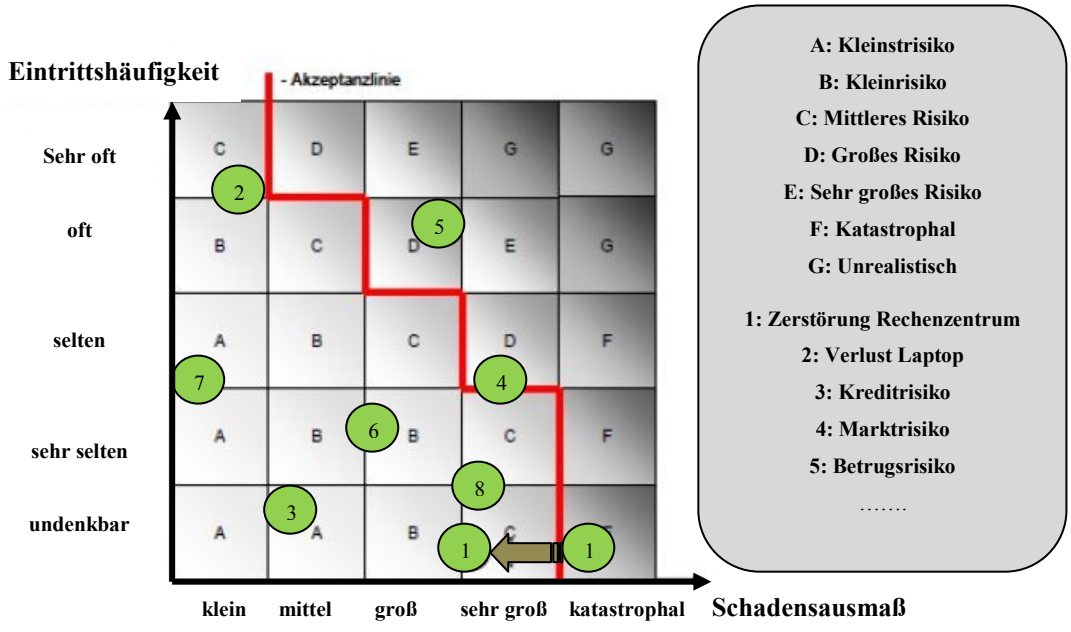

Abbildung 22: Risikoverminderung

Eigene Darstellung (in Anlehnung an Königs: IT, S.25.)

[211] Vgl. Siepermann: Risikokostenrechnung, S.46.
[212] Vgl. Ebert: Risikomanagement, S.60.
[213] Vgl. Wolke: Risikomanagement, S.83.

4.3.4 Risikoübertragung

Hierbei handelt es sich um den Risikoübergang in Gänze, meist aber in Teilen auf andere Vertragspartner. Die gängigste Form einer Übertragung ist der Abschluss von Versicherungen. So werden zwar nicht die Eintrittswahrscheinlichkeit und das mögliche Schadensmaß verringert, dennoch erleidet das UN keinen bzw. einen geringeren Verlust im Falle des Ereignisses. Darüber hinaus lassen sich Risiken auch an Geschäftspartner weitergeben. Das können bestimmte Änderungen in Lieferantenverträgen oder modifizierte Garantieverträge der Kunden sein.[214] Finanzierungsmodelle wie z.B. Factoring oder Leasing können indirekt auch eine Risikoübertragung herbeiführen.[215] Eine weitere zunehmend beliebte Variante ist das Outsourcing, dabei sollte bedacht werden, dass ein vollständiger Risikoübergang selten der Fall ist.[216] So kann das auftragsausführende UN möglicherweise für einen monetären Schaden haftbar gemacht werden (z.B. geschätzte Umsatzeinbußen bei Ausfall des Internetshops), die verbleibenden Image- bzw. Reputationsschäden dagegen fallen meist auf den Auftraggeber zurück.

4.3.5 Risikoakzeptanz

Diese Strategie wird initialisiert, wenn die zuvor definierten Maßnahmen wie Risikominderung, Risikovermeidung oder -übertragung nicht möglich waren oder ökonomisch als nicht vertretbar erachtet wurden. Weiterhin besteht die Möglichkeit, dass Risiken im Rahmen der Identifikation nicht erkannt oder falsch eingeschätzt wurden. Um den Schadenseintritt solcher Risiken abzudecken sind entsprechende monetäre Mittel zu bilanzieren. Das Risiko kann prinzipiell auch bewusst akzeptiert werden. Dabei sollte jedoch der folglich entstehende Nutzen höher sein als das Potenzial des eingegangenen Risikos. Die Vorrausetzung dazu ist, dass die Einschätzung des Risikos in vollem Umfang erfolgt ist, dokumentiert wurde (z.B. im Risikokatalog) und im Konsens mit der UN-Strategie steht.[217] Grundsätzlich muss sich jedes Unternehmen mit der Tatsache auseinandersetzen, dass trotz professioneller Risikosteuerung ein Restrisiko zu akzeptieren ist.[218]

---

[214] Vgl. Kersten/Reuter/Schröder: IT, S.59.
[215] Vgl. Wolke: Risikomanagement, S.85.
[216] Vgl. Junginger: Werteorientierte, S.172.
[217] Vgl. Seibold: IT, S.33.
[218] Vgl. Ebert: Risikomanagement, S.63.

4.4 Aufgaben der Risikokontrolle/ des Risikocontrolling

Der Begriff Risikokontrolle wird sukzessive durch den des Risikocontrollings ersetzt und damit einer Überwachungs-, Informations- und Anpassungsfunktion gerecht.[219] In diesem letzen Segment des IT-Risikomanagementprozesses werden Informationen über den gesamten Prozessablauf gesammelt, Veränderungen im Prozess dokumentiert, die aktuelle Risikolage in Abhängigkeit der zu erzielenden Risikopolitik beschrieben und der Erfolg der Maßnahmen anhand von Soll-Ist Vergleichen bewertet.[220] Die Informationstechnologie vollzieht in stets kürzeren Zeitabschnitten immer größere Entwicklungssprünge in Verbindung mit wechselnden Anforderungen. Daher ist das Risikocontrolling auch ein stetiger Ausgangspunkt des Kreislaufs eines Risikomanagementprozesses. Die Risikokontrolle erfüllt vorrangig zwei wesentliche Aufgaben: Die Erfolgskontrolle ermittelt, kommuniziert und dokumentiert inwieweit die durchgeführten Maßnahmen im Bezug der Risikosteuerungen den prognostizierten Erwartungen entsprechen. Die Änderungskontrolle identifiziert Modifikationen der Risikolage des Unternehmens, führt eine genaue Berichterstattung und ermöglicht so eine Risikofrüherkennung. Aus diesen zwei wesentlichen Aufgaben des Risikocontrolling lassen sich weitere Funktionen ableiten: Die Zyklen der Überwachungen, Kontrollen und Kennzahlenabfragen werden festgelegt und eine Bewertung und Klassifizierung der Effizienz der Maßnahmen vorgenommen. Im Weiteren wird das Management hinsichtlich der möglichen Maßnahmenanpassungen beraten, insbesondere mit Blick auf absehbare Trends und prognostizierte Erwartungen. Die Hilfestellung bei der Auswahl von geeignetem IT-Fachpersonal, die Gestaltung von Fortbildungen, die Weiterentwicklung des IT-Risikomanagement-Prozesses und die kompetente Auswertung von Wirtschaftlichkeitsdaten sind weitere wesentliche Funktionen des IT-Risikocontrollings. Abschließend verantwortet es die IT-Risikoberichterstattung und wirkt bei der Entwicklung der Risikostrategie maßgeblich mit.[221]Aus betriebswirtschaftlicher Sicht ist die Risikokontrolle der Prozessabschnitt, in der sich die Wertigkeit der Risikosteuerung messen lässt, anhand des Vergleichs der tatsächlich erreichten Sollrisikosituation mit der prognostizierten Sollrisikosituation. Damit lassen sich sowohl die Effizienz als auch Optimierungsfelder für das IT-Risikomanagement aufzeigen.[222]

[219] Vgl. Wolke: Risikomanagement, S.239.
[220] Vgl. Knoll: Praxisorientiertes, S.152.
[221] Vgl. Fiege: Risikomanagement, S.8.
[222] Vgl. Junginger: Werteorientierte S.298f.

5 Wirtschaftliche Betrachtungen des IT-Risikomanagement

5.1 Grundlagen der Betrachtung

Galt die IT in ihrer Anfangszeit ausschließlich als Instrument zur Datenverarbeitung, so hat sie heute in vielen Unternehmen einen hohen Stellenwert und begründet mitunter das eigentliche Geschäftsfeld des UN. Somit differieren auch die Aufwendungen für das IT-Risikomanagement.[223] Die Planung und Realisierung des gesamten IT-Umfeldes basiert auf den Vorgaben des IT-Controllings und des UN-Managements. Dabei werden die IT-Kosten in direkte und indirekte Kosten kategorisiert. Den direkten Kosten können einfach monetäre Kennzahlen zugeordnet werden (z.B. IT-Anschaffungskosten). Die indirekten Kosten (z.B. Unternehmensrisiken) lassen sich dagegen mitunter schwer, oft gar nicht, mit quantifizierbaren Kennzahlen untermauern. Weitaus gravierender ist die komplizierte oder teils unmögliche Quantifizierung der Nutzenfaktoren im Bereich der IT.[224] Daraus resultiert das Dilemma des IT-Risikomanagements, Kosten für Maßnahmen der Risikosteuerung lassen sich unmittelbar monetär bewerten, der Nutzengewinn von Sicherheit, Verfügbarkeit, Vertraulichkeit und Integrität dagegen ist häufig nicht quantifizierbar. Das erschwert die Argumentation für ein professionelles IT-Risikomanagement gegenüber der UN-Leitung. Ungeachtet dessen muss auch ein modernes IT-Risikomanagement auf einer ökonomisch vertretbaren Basis beruhen.[225]

5.2 Wesentliche Kennzahlen

5.2.1 Return on Security Investment (ROSI)

Diese Kennzahl liefert wesentliche Informationen, um erforderliche Investitionen in die IT-Sicherheit bzw. das IT-Risikomanagement weithin ökonomisch begründen zu können.[226]

Dabei handelt es sich um die nummerische Berechnung der Rentabilität von Sicherheitsinvestitionen und um ein wichtiges Steuerelement des IT-Risikocontrollings zur permanenten Verbesserung des IT-Risikomanagementprozesses. Die Basis der Berechnung des ROSI resultiert aus der Differenz, der durch Angriffe und Sicher-

[223] Vgl. Knoll: Praxisorientiertes, S.1.
[224] Vgl. Tiemeyer: IT, S.57.
[225] Vgl. Junginger: Werteorientierte, S.284.
[226] Vgl. Lenges: Framework, S.33.

heitsverletzungen entstehenden Aufwendungen (ohne Risikosteuerung) und den zu erwartenden Schäden (nach Risikosteuerung).[227] Dies stellt aber lediglich die Netto-Verlustreduktion dar. Der tatsächliche ROSI ist eine Verhältniszahl, d.h. das Ergebnis der Netto-Verlustreduktion wird dazu im Verhältnis zu dem Maßnahmenaufwand pro Jahr betrachtet. Für fundierte Ergebnisse sind sowohl genaue Kenntnisse über die Schadenshöhe mit entsprechenden Risikosteuerungsmaßnahmen als auch ohne gezielte Steuermaßnahmen notwendig. Bei der Berechnung wird der Erwartungswert zu Grunde gelegt. Das ist bei häufigen Schäden sinnvoll. In den Fällen von unerwarteten Schadensereignissen ist der Erwartungswert selten zu quantifizieren, daher kommen hier z.B. quantifizierte Werte in Form von Scores zur Anwendung. Die ROSI Berechnung stellt eine gute Hilfe bei der Wirtschaftlichkeitsberechnung der Risikomaßnahmen dar und bildet sekundär eine Aussage über die Wertschöpfung und Wirtschaftlichkeit des IT-Risikomanagements. Da eine ROSI Analyse recht umfangreich sein kann, bietet z.B. die Information Security& Business Continuity Academy kostenlos gutbedienbare Online- ROSI- Rechner an.[228]

5.2.2 Weitere bedeutende Kennzahlen

5.2.2.1 Total Cost of Ownership (TCO)

Die TCO-Kennzahl wurde in den 1980er Jahren von dem amerikanischen Unternehmen Gartner entwickelt, um die Kosten im Bereich der IT zu quantifizieren. Damit werden die monetären Aufwendungen zum Erwerb, zur Einrichtung, zur Wartung(Support) und zum Recycling des IT-Equipments ermittelt. Die TCO-Kennzahl aggregiert und kommuniziert umfassend die Gesamtkosten einer IT-Investition über die volle Lebensdauer, so auch im Bereich der IT-Sicherheit und des IT-Risikomanagements.[229] Die verursachten Kosten der IT-Systeme lassen sich in direkte und indirekte Kosten differenzieren. Direkte Kosten resultieren aus Beschaffung, Installation und Support oder baulichen Maßnahmen. Die indirekten Kosten entwickeln sich, z.B. aus Systemstörungen, Sicherheitsmängeln und den daraus resultierenden Risiken.[230] Mit Hilfe einer TCO-Analyse werden die direkten und

[227] Vgl. Junginger: Werteorientierte, S.286.
[228] Vgl. Knoll: Praxisorientiertes, S.278.
[229] Vgl. Junker/Marx Gómez/Odebrecht: IT, S.59.
[230] Vgl. Tiemeyer: IT, S.24f.

indirekten IT-Kosten übersichtlich gegliedert, für die IT-Bereiche differenziert und vollständig erfasst. Daraus ergibt sich eine bessere Kostentransparenz für alle Bereiche der IT, so auch für das IT-Risikomanagement. Nur eine genaue Vorstellung über die Kosten in den einzelnen Bereichen, ermöglichen wirtschaftliche und nutzenwertorientierte Steuerungsmaßnahmen. Die wesentlichen Nachteile der TCO sind: eine mangelnde Betrachtung von Nutzen bzw. Erlösen, die statische Methodik sowie Personalkosten in IT-gestützten Prozessen bleiben unbewertet. Abhilfe schaffen hier weiter entwickelte TCO-Methoden, die ein TBO-Konzept mit einbeziehen[231].

5.2.2.2 Balance Score Card (BSC)

Die BSC wurde von R.S. Kaplan und D.P. Norton als neue Methode für das Controlling-Konzept entwickelt.[232] Eine BSC wird inhaltlich gezielt abgestimmt und im IT-Bereich spezifisch für das IT- Risikomanagement ausgestaltet. Die BSC umfasst eine Finanzielle Perspektive, eine Kundenperspektive, eine Interne-Prozessperspektive sowie eine Lern- und Entwicklungsperspektive. Jede dieser Perspektiven enthält aussagefähige Daten über Ziele, Kennzahlen, Vorgaben und Maßnahmen.[233] Für die Ausgestaltung einer BSC des IT-Risikomanagements empfiehlt sich als Basis ein Best Practice Ansatz. Das CobIT-Framework ist dafür bestens geeignet. So lassen sich die aus dem Regelwerk adaptierte, strategische Unternehmensziele in messbare zielorientierte Maßnahmen übertragen. CobiT verwendet zur Messung geeignete Instrumente, wie den Key Goal Indikator (KGI), Key Performance Indikator (KPI) sowie Critical Sucess Factor (CSF). Aus diesen Indikatoren lassen sich wertvolle ökonomische Erkenntnisse im Bezug auf die Effektivität und Effizienz der IT-Prozesse ableiten. Der CSF ermöglicht eine Steigerung der Prozessperformance, zu Gunsten der Zielsetzungen. Der KGI und KPI können auch als Risikoindikatoren fungieren, um beispielsweise eine mangelhafte Kostenoptimierung der IT Sicherheitsleistungen oder Defizite bei der Nutzung der IT- Ressourcen aufzuzeigen.[234]

---

[231] Vgl. Gadatsch: IT, S.53.
[232] Vgl. Nguyen: Handbuch, S.233.
[233] Vgl. Tiemeyer: IT, S.143- 146.
[234] Vgl. Königs: IT, S.124- 127.

5.3 Kosten- Nutzenausrichtung an den Unternehmenszielen

Das IT-Risikomanagement sollte einen ökonomischen Maßnahmenpool entwickeln, bei dem die Grenzkosten gleich dem Grenznutzen sind und im Schnittpunkt dieser Funktionen das optimale Sicherheitsniveau liegt.[235] Die folgende Abbildung stellt diese Situation grafisch dar.

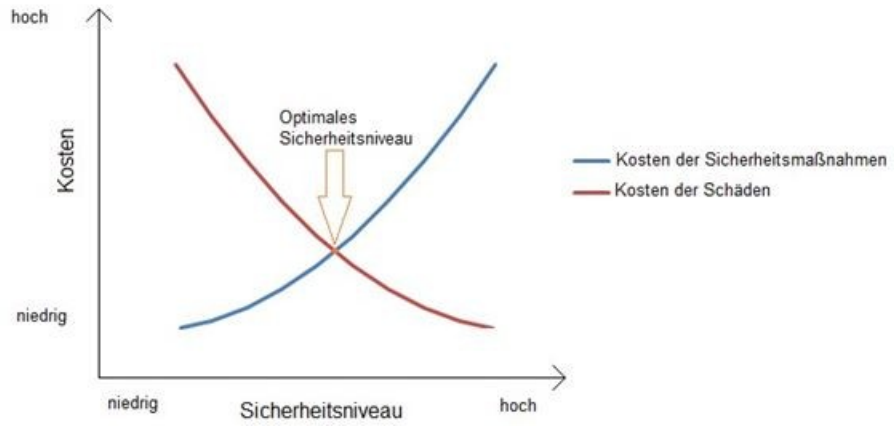

Abbildung 23: Optimales wirtschaftliches Sicherheitsniveau
Eigene Darstellung (in Anlehnung an Junginger: Werteorientierte, S.285)

Der Nutzen eines werteorientierten umfassenden Risikomanagement kann nicht an den Einsparungen der Risiko- und Maßnahmenkosten allein festgestellt werden. Vielmehr geht es um die Frage, inwieweit Sicherheitsprozesse und -aufgaben die UN-Strategie festigen können. Im Mittelpunkt steht die Identifizierung eines optimalen Sicherheitsniveaus. Das CobiT mit seinen „Val IT“ und „Val Risk“ Regeln sowie die ISO/IEC 27001 setzen für das strategische Sicherheitsmanagement, die Orientierung an der UN-Strategie voraus. Das „IT-Governance Institut“ meint, der entstehende Nutzen durch die IT ist direkt auf die Grundsätze des UN und dem Umgang mit Risiken und Chancen zurückzuführen.[236]

5.4 Outsourcing

Die Methode des Outsourcings wird im Bereich des Informationsmanagements häufig kontrovers diskutiert. Strategisch handelt es sich um mittel- bzw. langfristige zu übertragende Aufgaben an externe Dienstleister.[237] Das Outsourcing kann für einzelne Unternehmensfunktionen oder ganze UN- Bereiche erfolgen, wie z.B. im

[235] Vgl. Junginger: Werteorientierte, S.284.
[236] Vgl. Königs: IT, S.289.
[237] Vgl. Tiemeyer: IT, S.75.

IT-Umfeld, Logistik- oder Marketingbereich. Gegenüber dem Vorteil von möglichen Kosteneinsparungen und Aufgabenübertragungen an spezialisierte, professionelle Dienstleister sollten in jedem Fall eventuell entstehende Nachteile sorgfältig geprüft werden, wie z.B. Aufgabe von Geschäftsbereichen, Abhängigkeit vom Dienstleister und Mängel in der Haftung des Dienstleisters.[238] Darüber hinaus werden teilweise die Kosten nur bedingt gesenkt, stattdessen lassen sich für das Outsourcing notwendige Aufwendungen besser planen und damit die Kosten besser kontrollieren.[239] Das kann für die Aufgaben des IT-Risikomanagements zum Vorteil gereichen. Da Quantifizierungen im Bereich des Risikomanagements sich oft schwierig gestalten und bisweilen unmöglich sind. So ergeben sich aus der festen Budgetierung des Outsourcings klar definierte Kosten für die Risikomaßnahmen und das Risikomanagement. Besonders im Prozessabschnitt der Risikosteuerung gilt das Outsourcing als ein geeignetes Instrument zur Risikoübertragung. Dem stimmt Basel II/III in seinen Sound Practices zu und räumt die Möglichkeit des Outsourcings zur Risikosteuerung ein. Somit liegt das primäre Ziel des Outsourcings in der Risikoübertragung im Rahmen der Risikosteuerung. Das Outsourcing kann sekundär, durch die Vergabe von Aufgaben an hochspezialisierte Dienstleister, bis dahin erheblich gebundene Ressourcen (z.B. Risikoanalyse-Aufwand) des IT-Risikomanagement freisetzen, die so anderweitig genutzt werden können. Dadurch ist eine indirekte Kostensenkung möglich. Die Auslagerung von IT-Risikomanagement Funktionen, dürfen die mit der Unternehmensstrategie abgestimmte IT-Strategie nicht beeinträchtigen. Darüber hinaus sollten für das UN benötigte Fachkompetenzen verfügbar bleiben.[240] Für ein Outsourcing können eine Verminderung des Umfangs an IT-Prozessen, Nutzung neuster Innovationen der spezialisierten IT-Dienstleister, eine Ressourcenfreisetzung im IT-Bereich oder eine mögliche Kostenreduktion sprechen. Die neuen Kosten für das Outsourcing sind genau zu betrachten und wichtige rechtliche, regulative sowie formelle Vorgaben sind einzuhalten. Die Gartner Group gibt anhand ihres Sourcing-Lifecycle Modells die Empfehlung einer genauen Analyse aller Risiken bis zum Vertragsabschluss. Bleibt festzuhalten das Outsourcing ist ein gebräuchliches Instrument in einem modernen Risikomanagementprozess.[241]

[238] Vgl. Junginger: Werteorientierte, S.165f.
[239] Vgl. Tiemeyer: IT, S.79.
[240] Vgl. Seibold: IT, S.201- 206.
[241] Vgl. Königs: IT, S.377.

6 Fazit

Die vorliegende Arbeit hat zum besseren Verständnis zunächst wesentliche Grundbegriffe des Risikomanagements dargestellt und definiert. Damit wurde eine wichtige Basis geschaffen, um im weiteren Verlauf der Ausführungen gezielt das IT-Risikomanagementsystem zu analysieren. Dazu wurden dem Leser detailliert und ganzheitlich wichtige Informationen über den IT-Risikomanagementprozess bereitgestellt. Eine breite und tiefe Darstellung von wesentlichen rechtlichen Normen sowie elementaren Standards und Regelwerken hat die große Bedeutung eines umfassenden wertorientierten IT-Risikomanagementsystems nachvollziehbar belegt. Des Weiteren wurde anhand der vorgestellten Regelwerke und Standards gezeigt, wie mit deren Hilfe ein modernes IT-Risikomanagement implementiert und bewirtschaftet werden kann. Darüber hinaus wurde großes Augenmerk auf die wirtschaftlichen Aspekte im Bereich des IT-Risikomanagements gelegt. Das gilt sowohl im Hinblick auf das IT-Risikomanagement an sich, als auch für die Bewirtschaftung der Risiken, soll heißen die Steuerung der Risiken. Dazu wurden für den Leser bedeutende Methoden der Risikosteuerung vorgestellt und bewertet.

Die Informationstechnologien haben eine große Bedeutung im privaten, gesellschaftlichen, wirtschaftlichen und politischen Umfeld. Innovationen in diesem Bereich werden stetig bedeutender und vollziehen sich in einem wachsenden Tempo. Dadurch entstehen für die Unternehmen enorme wirtschaftliche Chancen. Aus der weltweiten Vernetzung von IT-Systemen und deren großer wirtschaftliche Bedeutung entwickeln sich aber auch hohe Abhängigkeiten und ein steigendes Risikopotenzial. So warnt aktuell das BSI vor einem millionenfachen Identitätsdiebstahl im E-Mailbereich und einem nicht abschätzbaren finanziellen Schaden.[242] Damit erhalten die in dieser Arbeit geschilderten Sachverhalte eine würdigende Rechtfertigung und der Bedarf an einem spezifischen IT-Risikomanagement wird deutlich.

Die Arbeit hat jedoch auch gezeigt, keine Form eines Risikomanagements ist in der Lage alle Risiken zu beseitigen. Ein gewisses Restrisiko muss jede Unternehmung tolerieren. Dazu wurde deutlich gemacht, dass eine langfristige Gewinnerzielung ohne eine bestimmte Risikotoleranz nicht möglich ist. Des Weiteren wurde darauf hingewiesen, dass es auch aus betriebswirtschaftlicher Sicht bestimmte Grenzen im Rahmen der Risikosteuerung gibt. Eine teilweise komplizierte, bisweilen unmögliche

[242] Vgl. BSI: Presse, S.1f.

Quantifizierung von Risiken stellt ein weiteres Problem des IT-Risikomanagement dar. Trotz dieser Defizite wurde im Laufe dieser Arbeit deutlich, wollen die Unternehmen zukünftig ihre Chancen nutzen und sich gesetzeskonform aufstellen, sind Risikomanagements im Allgemeinen und IT-Risikomanagements im Besonderen notwendig. Dazu ist es erforderlich, das Risikomanagement selbst auf seine Funktionsweise mit geeigneten Instrumenten zu kontrollieren. Zukünftig werden eher solche Unternehmen bessere Marktchancen erhalten, die eine Verfügbarkeit, Vertraulichkeit und Integrität von Informationen sicherstellen, Datensicherheit gewährleisten und mit Hilfe eines modernen IT-Risikomanagements dazu notwendige Maßnahmen treffen.

Literaturverzeichnis

Bärwolf, Hartmut/Hüsken, Volker/Viktor, Frank: IT-Systeme in der Medizin, Vieweg Verlag, Wiesbaden 2006.

Blumberg, Hartmut/Pohlmann, Norbert: Der IT- Sicherheitsleitfaden, 2.Auflage, Redline GmbH, Heidelberg 2006.

Buchard, Anton/Burger, Anton: Risiko Controlling, Oldenbourg Verlag, München 2002.

Diederichs, Marc: Risikomanagement und Risikocontrolling, 3.Auflage, Vahlen Verlag, München 2013.

Disterer, Georg/Wittek, Michael: IT-Risikomanagement in Versicherungen, 11.Heft, dpunkt.verlag, Heidelberg 2012.

Dransfeld, Ingmar: Operationelle Risiken und Basel II: Messverfahren als Wettbewerbsvorteil?, Diplomica Verlag, Hamburg 2014.

Ebert, Christof: Risikomanagement Kompakt. Risiken und Unsicherheiten bei IT- und Softwareprojekten, Spectrum Akademischer Verlag, Heidelberg 2006.

Eckert, Claudia: IT-Sicherheit, 8.Auflage, Oldenbourg Verlag, München 2013.

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

Finke, Robert B./Romeike, Frank: Erfolgsfaktor Risikomanagement, Betriebswirtschaftlicher Verlag Dr. Th. Gabler, Wiesbaden 2003.

Gadatsch, Andreas/Mayer, Elmar: Masterkurs IT-Controlling: Grundlagen und Praxis für IT-Controller und CIO,s, 4.Auflage, Springer Vieweg Verlag, Wiesbaden 2010.

Gadatsch, Andreas: IT-Controlling: Praxiswissen für IT-Controller und Chief-Information Officer, Springer Vieweg Verlag, Wiesbaden 2012.

Hartmann, Horst: Modernes Einkaufsmanagement. Global Sourcing- Methodenkompetenz- Risikomanagement, Deutscher Betriebswirte Verlag, Gernsbach 2007.

Hohrath, Philipp Alexander: Analyse der strategisch und strukturell induzierten Verwundbarkeit von Wertschöpfungsnetzwerken, Josef Eul Verlag, Köln 2013.

Horváth, Péter: Controlling, 12.Auflage, Vahlen Verlag, München 2012.

Junginger, Markus: Werteorientierte Steuerung von Risiken im Informationsmanagement, Deutscher Universitäts Verlag, Wiesbaden 2005.

Junker, Horst/Marx Gómez, Jorge/Odebrecht, Stefan: IT-Controlling: Strategien, Werkzeuge, Praxis, Erich Schmidt Verlag, Berlin 2009.

Kamiske, Gerd F.: Managementsysteme: Begutachtung, Auditierung und Zertifizierung, Symposium Puplishing GmbH, Düsseldorf 2008.

Kersten, Heinrich/Reuter, Jürgen/Schröder Klaus-Werner: IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz, 4.Auflage, SpringerVieweg, Wiesbaden 2013.

Kirsch, Markus: Datenschutz im Unternehmen: Leitfaden für Datenschutzrechtliche Fragestellung im Rahmen unternehmerischer IT-Compliance, Books on Demand GmbH, Norderstedt 2011.

Klinger, Michael A./Klinger, Oskar: Das interne Kontrollsystem im Unternehmen, 2. Auflage, Vahlen Verlag, München.

Knödler, Torsten: Puplic Relation und Wirtschaftsjournalismus: Erfolgs- und Risikofaktor für ein Win- Win, Verlag für Sozialwissenschaften, Wiesbaden 2005.

Knoll, Matthias: Praxisorientiertes IT- Risikomanagement, dPunkt.verlag, Heidelberg 2014.

Königs, Hans-Peter: IT- Risikomanagement mit System, 4.Auflage, Springer Vieweg Verlag, Wiesbaden 2013.

Lenges, Michael: Framework zum IT-Risikomanagement, Books on Demand, Norderstedt 2008.

Lister Michael/Schierenbeck, Henner: Value Controlling- Grundlagen wertorientierter Unternehmensführung, 2.Auflage, Oldenbourg Wissenschaftsverlag, München 2002.

Nguyen, Tristan: Handbuch der wert- und risikoorientierten Steuerung von Versicherungsunternehmen, Verlag Versicherungswirtschaft GmbH, Karlsruhe 2008.

Prokein, Oliver: IT-Risikomanagement, Gabler Verlag, Wiesbaden 2008.

Runzheimer, Bodo/Wolf, Klaus: Risikomanagement und KonTraG, 4.Auflage, Betriebswirtschaftlicher Verlag Gabler GmbH, Wiesbaden 2003.

Schneck, Ottmar: Risikomanagement: Grundlagen, Instrumente, Fallbeispiele, Wiley-VCH Verlag, Weinheim 2010.

Seibold, Holger: IT-Risikomanagement, Oldenbourg Verlag, München 2006.

Siepermann, Markus: Risikokostenrechnung, erfolgreiche Informationsversorgung und Risikoprävention, Erich Schmidt Verlag, Berlin 2008.

Stiefl, Jürgen: Risikomanagement und Existenzsicherung, Oldenbourg Wissenschaftsverlag, München 2010.

Strohmeier, Georg: Ganzheitliches Risikomanagement in Industriebetrieben, Deutscher Universitäts Verlag, Wiesbaden 2007.

Thies, Karlheinz H.W.: Management operationaler IT- und Prozessrisiken, Springer Verlag, Heidelberg 2008.

Tiemeyer, Ernst: Handbuch IT-Management. Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis, 5.Auflage, Carl Hanser Verlag, München 2013.

Tiemeyer, Ernst: IT-Controlling Kompakt, Spektrum Akademischer Verlag, Heidelberg 2005.

Volkwein, Ellen: Die Umsetzung des Sarbanes Oxley Act 2002 in Deutschland, Salzwasserverlag, Hamburg 2007.

Wanner, Roland: Risikomanagement für Projekte, 2.Auflage, Amazon Distrubtion GmbH, Leipzig 2013.

Wiederkehr, Bruno/Züger, Rita-Maria: Risikomanagementsystem im Unternehmen, Compendio Bildungsmedien AG, Zürich 2010.

Wolke, Thomas: Risikomanagement, 2.Auflage, Oldenbourg Wissenschaftsverlag, München 2008.

Internetquellen

BSI: Grundschutz-Gefährdungskatalog. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Gefaehrdungskatalog-G0-ElementareGefaehrdungen.pdf?__blob=publicationFile, eingesehen am 18.04.2014, 46 Seiten

BSI: Grundschutz- GS Leitfaden. http://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile ,eingesehen am: 06.04.2014, 91 Seiten.

BSI: Grundschutz-Hilfsmittel. http://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Check/04pc_f_pdf.pdf?__blob=publicationFile, eingesehen am: 12.04.201, 11 Seiten.

BSI: IT-Grundschutz-Kataloge. http://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/IT-Grundschutz-Kataloge_2013_EL13_DE.pdf?__blob=publicationFile, eingesehen am: 06.04.2014, 4482 Seiten

BSI: Pressemitteilung-Mailtest.

https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Mailtest_21012014.html, eingesehen am: 28.04.2014, 2 Seiten

BSI: Publikationen. IT-Grundschutzstandards: Standard 100-1.

http://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1001_pdf.pdf?__blob=publicationFile, eingesehen am: 07.04.2014, 37 Seiten

FH-Kiel: Studie IT-Wirtschaftlichkeit. http://fh-kiel.de/fileadmin/data/wirtschaft/Dozenten/Vanini__Ute/Studie_IT-Wirtschaftlichkeit.pdf, eingesehen am: 27.04.2014, 7 Seiten

Koebler, Gerhard: Deutsches Etymologisches Wörterbuch. http://www.koeblergerhard.de/der/DERA.pdf, eingesehen am: 15.03.2014, 483 Seiten

Statistisches Bundesamt: Anteil der Unternehmen mit Computernutzung in Deutschland 2005 – 2013. http://de.statista.com/statistik/daten/studie/151762/umfrage/anteil-der-unternehmen-mit-nutzung-von-computern-in-deutschland/, eingesehen am 17.04.2014, 1 Seite

TÜV- Süd: Studie RCM Mittelstand. http://www.tuev-sued.de/uploads/images/1319789287655663060667/studie-rcm-mittelstand.pdf, eingesehen am: 27.04.2014, 16 Seiten

Eidesstattliche Versicherung

Guido Helbich

Zielhecke 13

37339 Worbis

Matrikel-Nr.: BW11.W.049

Worbis, den 13.05.2014

Hiermit versichere ich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe angefertigt habe. Ich versichere auch, dass ich bei allen Gedanken, Befunden und anderen Inhalten, die nicht von mir stammen, direkt vor Ort auf die entsprechenden Quellen verwiesen habe. Alle wörtlichen Zitate sind als solche kenntlich gemacht. (gemäß §16 der Prüfungsordnung)

Abgabe: 13.Mai 2014

Unterschrift

Guido Helbich