IT-Risikomanagement

von
Holger Seibold

Oldenbourg Verlag München Wien

Holger Seibold
Der Autor ist als Sparkassenbetriebswirt und Dipl. Betriebswirt (FH) mit Fachrichtung Wirtschaftsinformatik langjährig bei einem großen Kreditinstitut in Deutschland tätig. Als stv. Direktor verantwortete er bereits die Themen Geschäftsprozess- und Workflowmanagement, Dokumentenmanagement, Office-Solutions sowie aufbauorganisatorische Fragestellungen und leitete erfolgreich zahlreiche Projekte. Seit 2 Jahren konzipiert und implementiert er den Auf- und Ausbau des IT-Risiko- und IT-Krisenmanagements.

Bildnachweis Umschlag:
©2005 bavaria yachtbau GmbH

Bibliografische Information Der Deutschen Bibliothek

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

Rosenheimer Straße 145, D-81671 München
Telefon: (089) 45051-0
oldenbourg.de

Lektorat: Stephanie Schumacher-Gebler
Herstellung: Anna Grosser
Umschlagkonzeption: Kraxenberger Kommunikationshaus, München
Gedruckt auf säure- und chlorfreiem Papier
Gesamtherstellung: Grafik + Druck, München

ISBN 3-486-58009-4
ISBN 978-3-486-58009-9

Inhaltsverzeichnis

Vorwort

Die Informationstechnologie hat für viele Unternehmen eine zentrale Bedeutung. Geschäftsprozesse können bei einem Ausfall der Informationstechnologie nicht mehr oder zumindest nur mit einer wesentlich geringeren Effizienz ausgeführt werden. Durch die Relevanz der Informationstechnologie, die künftig in allen Branchen noch weiter zunehmen wird, rücken deren Risiken und vor allem deren Beherrschbarkeit in das zentrale Betrachtungsfeld von Unternehmensentscheidern.

IT-Risikomanagement hat viele Facetten und greift in alle Themengebiete der Informationstechnologie ein: von der Entwicklung über die – aus technischer und fachlicher Sicht – Integration bis hin zum Infrastruktur- und Anwendungsbetrieb. Bei der Betrachtung von IT-Risikomanagement wird das Themengebiet häufig auf dedizierte Teilaspekte reduziert. Dies können die Verfügbarkeit von Anwendungen, die IT-Sicherheit im Sinne von Vertraulichkeitsrisiken, Projektrisiken oder Entwicklungsrisiken und die dadurch bedingte Softwarequalität sein. In diesem Buch wird das IT-Risikomanagement als in die einzelnen Themengebiete der Informationstechnologie und dessen Management eingebunden betrachtet. Zugleich wird es von den bereits etablierten IT-Disziplinen abgegrenzt. Zudem kann das IT-Risikomanagement in ein bestehendes Risikomanagement eines Unternehmens, welches ein explizites Management von Betriebsrisiken praktiziert, den sogenannten operationellen Risiken, integriert werden.

Das Buch stellt ein auf wissenschaftlichen Prinzipien beruhendes Praxiswerk dar. Es bietet keine Vorgehensweise in Form von Checklisten und expliziten Handlungsempfehlungen zur Einführung eines IT-Risikomanagements in ein Unternehmen an, sondern zeigt vielmehr die Inhalte und das Procedere im Rahmen eines IT-Risikomanagements auf. Dieses wurde im Bankenumfeld erarbeitet, ist desgleichen aber auch mit der Informationstechnologie anderer Unternehmen kompatibel.

Für die Unterstützung bei der Erstellung des Buches möchte ich allen Beteiligten des Oldenbourg-Wissenschaftsverlags danken. Ebenso gilt der Dank meinen Kollegen, die mir mit einer Vielzahl von Diskussionen bei der Ausarbeitung des Buches inhaltlich weitergeholfen haben. Einen besonderen Dank möchte ich an meinen Kollegen Steffen Aichholz aussprechen, der seine Erfahrung als konzernweit Verantwortlicher für operationelle Risiken mit mir geteilt hat und an Sören Hinrichsen, der seine langjährige Organisations- und IT-Erfahrung in die Qualitätssicherung des Manuskriptes eingebracht hat. Ebenso danke ich ferner meinem Freund Bernd Foschiatti, der als Verantwortlicher für IT und Controlling in einem mittelständischen Unternehmen der Investitionsgüterindustrie den Blick über den Banken-

Tellerrand sicherstellte. Herzlichen Dank an meine Freunde und Familie, insbesondere an meine Frau Doreen und Tochter Asina, die mich in schwierigen Zeiten des Schreibens stets motiviert haben.

Ich wünsche allen Lesern eine kurzweilige Lektüre und würde mich freuen, wenn Ihnen das Buch möglichst viele Anregungen für Ihre eigene Arbeit geben kann. Sollten Sie Anmerkungen zum Buch haben, so können Sie mir diese gerne per Mail unter

Holger.Seibold@IT-Risikomanagement.com

zukommen lassen.

Urbach, 2006 Holger Seibold

Einleitung

„Risiko ist die Bugwelle des Erfolgs." – Carl Amery (deutscher Schriftsteller) –

... aber auch die Höhe der Bugwelle muss angemessen sein, damit das Schiff des Erfolgs nicht untergeht. Dies könnte der nachgelagerte Satz zu der sicherlich richtigen Aussage von Carl Amery sein.

Das Thema Risikomanagement gewinnt in den letzten Jahren immer stärker an Bedeutung. Während in Produktionsbetrieben bereits seit langem mit Risiken/Wahrscheinlichkeiten, auch im Sinne einer quantitativen Analyse, gearbeitet wird, hat sich die detaillierte Risikoanalyse im Finanz- und Dienstleistungsbereich fast ausschließlich im Versicherungsgeschäft abgespielt. Durch immer höhere Komplexität von Finanzprodukten, insbesondere im derivativen Bereich, wurden Risikopotenziale aufgebaut, deren Nichtbeachtung Anfang der 1990er Jahre zu spektakulären Unternehmenskrisen führte und u.a. der Auslöser für die Asienkrise mit den in Folge aufgetretenen Bankenzusammenbrüchen war.
Dies war mit einer der Gründe, die Diskussion über unternehmerische Risiken zu intensivieren. In den angelsächsischen Ländern wurden, beispielsweise in den USA mit dem Report des Committee of Sponsoring Organizations of the Treadway Commission (COSO Report) und in Großbritannien durch das Cadbury Committee, Leitlinien für die Unternehmensüberwachung eingeführt. In Deutschland wurden solche Leitlinien durch das *Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)* umgesetzt und Vorstände verpflichtet, geeignete Maßnahmen, insbesondere ein geeignetes Überwachungssystem, zum Fortbestand der Gesellschaft zu treffen. Kapitalgesellschaften haben durch §§ 289 Abs. 1, 315 Abs. 1 HGB in ihren Lageberichten auf die Risiken der künftigen Entwicklungen einzugehen und sind durch § 91 (2) AktG verpflichtet, über Risikovorsorgemaßnahmen den Fortbestand des Unternehmens zu sichern.[1] In den USA fordert der *Sarbanes Oxley Act* ein adäquates Risikomanagementsystem. Diesem Gesetz unterliegen ebenso Firmen außerhalb der USA, sofern sie Teil eines in den USA gelisteten Konzerns sind. Für Kreditinstitute und Wertpapierabwickler gelten darüber hinaus § 25a Abs. 1 KWG bzw. § 33 Abs. 2 WpHG, die ebenfalls ein Risikomanagementsystem und den adäquaten Ausbau des internen Kontrollsystems vorschreiben. Bei der Betrachtung der Entwicklung von gesetzlichen Anforderungen erkennt man, dass bei neueren Regelungen immer stärker die Implementierung eines Risikomanagementprozesses mit Frühwarnsystemen gefordert wird. Es findet ein Wandel vom reaktiven

1 Vgl. KPMG, 1998, S. 4.

zum proaktiven Risikomanagement statt.[2] Diese Entwicklung liegt bei den heutigen wirtschaftlichen Rahmenbedingungen im ursprünglichen Interesse jedes Unternehmens. Risikomanagement wird zu einer tragenden Säule einer wertorientierten Unternehmensführung.

Über das KonTraG wurde zudem das Aufgabenspektrum von Wirtschaftsprüfern erweitert. War zuvor die Prüfung der buchhalterischen Vollständig- und Richtigkeit die Hauptaufgabe, so wurde diese um die Prüfung des einzurichtenden Risikomanagementssystems (siehe § 317 Abs. 4 HGB), der Beurteilung der künftigen Geschäftsentwicklung (siehe § 321 Abs. 4 HGB) und deren potenziellen Risiken (siehe § 317 Abs. 2 HGB) erweitert. Die im Unternehmens- bzw. Konzernlagebericht enthaltenen Informationen über Risiken fließen, über die jährlich stattfindenden Bonitätsbeurteilungen der Kreditinstitute gemäß § 18 Abs. 1 KWG, in die Kreditentscheidungsfindung ein.[3]

Durch Basel II wird weitergehend die qualifizierte Risikobetrachtung in das Kreditgewerbe eingeführt. Begonnen hat diese Risikobetrachtung bei den klassischen Bankrisiken wie Adressenausfall-, Liquiditäts- und Marktpreisrisiken. Ergänzt wird diese Risikosicht durch die Einführung der Risikokategorie „operationelle Risiken". Diese Risikokategorie soll die betrieblichen Risiken des täglichen Geschäftsablaufs darstellen. Durch die Einführung der Baseler-Konventionen werden die Kreditinstitute gezwungen, sich mit ihren betrieblichen Risiken auseinanderzusetzen und diese professionell zu managen. Diesen Anspruch werden sie eher mittel- als langfristig an die Kreditnehmer, die sich nicht unmittelbar den gesetzlichen Anforderungen wie dem KonTraG unterwerfen müssen, stellen.

Obwohl Anzahl und Risikopotenzial von operationellen Risiken wesentlich von den getätigten Geschäftsarten und dem Geschäftsvolumen abhängen, wird jede Bank verpflichtet, ein professionelles Risikomanagement für die Risikokategorie der operationellen Risiken einzurichten. Lediglich die Ausgestaltung selbst kann dann den jeweiligen institutsspezifischen Gegebenheiten angepasst werden.[4]

In die Risikokategorie der operationellen Risiken fallen u.a. die Risiken, die sich aus dem Einsatz der Informationstechnologie ergeben. Die Informationstechnologie hat in großen Teilen der Wirtschaft einen hohen und weiter anwachsenden Stellenwert[5]. Der Ausfall oder eine Fehlfunktion dieser Ressource stellt ein großes Risikopotenzial dar. Zwar werden in Unternehmen von der IT-Abteilung immer gewisse Sicherheitsvorkehrungen wie Sicherungskopien, Zutrittsberechtigungen oder gar Backup-Installationen von IT-Systemen getroffen, diese stellen aber häufig kein einheitliches Gesamtbild im Sinne eines integrierten Risikomanagements dar. Was unter IT-Risiken zu verstehen ist, wie sie identifiziert und kategorisiert werden können und wie diese Erkenntnisse in die bereits vorhandenen Themengebiete eines professionellen IT-Betriebs integriert und gemanagt werden können, erläutert dieses

2 Vgl. Romeike, 2003a, S. 65–68.

3 Vgl. Keitsch, 2000, S. 14–15.

4 Vgl. Basel Committee, 2003, S. 1.

5 IT-Risiken werden auch bei Industrieunternehmen ernst genommen und separat ausgewiesen, selbst bei konzentrierten Zusammenfassungen. Vgl. BMW, 2004, S. 57.

Buch. Auch wenn sich die Beispiele hierbei überwiegend auf Kreditinstitute beziehen, kann und soll die Quintessenz auf andere Anwendungsbeispiele der elektronischen Informationsverarbeitung übertragen werden.

Bei einem umfassenden IT-Risikomanagement werden allerdings nicht nur operationelle Risiken betrachtet, sondern auch Geschäfts- und Strategierisiken, z.B. im Rahmen von Architekturentscheidungen, bewertet. Ebenso umfasst ein ganzheitliches IT-Risikomanagement das Management von rasanten, katastrophalen Risiken durch ein Business Continuity Programm (BCP) und einem Desaster Recovery Programm (DRP), sprich einem professionellen IT-Krisenmanagement.

Abb. 1 gibt eine Übersicht über die Kernthemen des IT-Risikomanagements. Die Zusammenhänge werden in den einzelnen Kapiteln des Buches hergestellt und die sich dahinterverbergenden Details erläutert. Die Grafik soll Ihnen beim Lesen des Buches als Orientierung dienen.

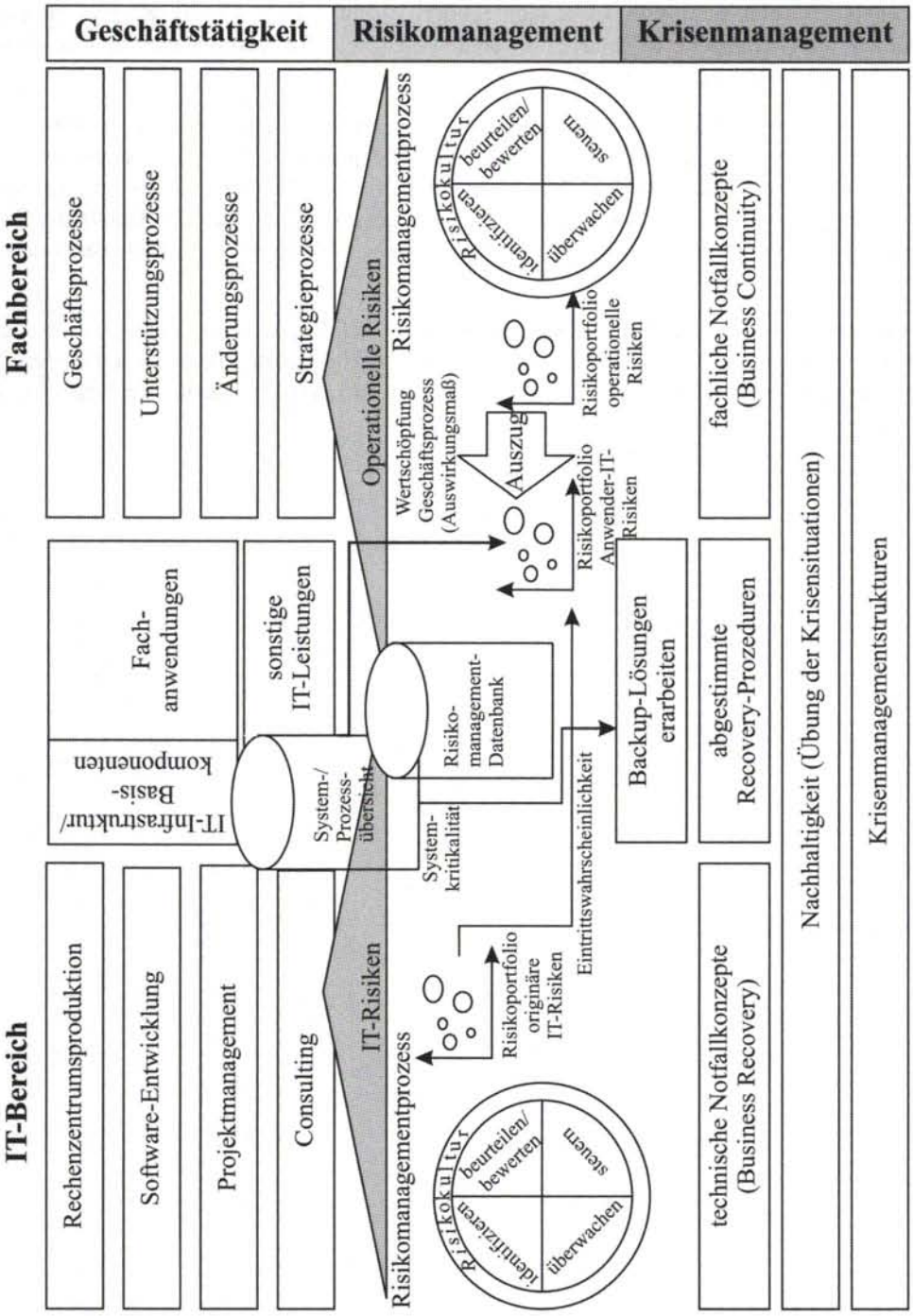

Abb. 1 Übersicht IT-Risikomanagement

1 Definition von IT-Risikomanagement

„Nichts geschieht ohne Risiko, aber ohne Risiko geschieht auch nichts."
– Walter Scheel (deutscher Bundespräsident, von 1974 bis 1979) –

In den nachfolgenden Kapiteln werden die Grundlagen für eine einheitliche Verständigung geschaffen. Gerade bei einem neuen Thema wie dem Management von betrieblichen Risiken und hier im Speziellen, die aus der Informationstechnologie entstehenden Risiken, ist es wichtig, einen einheitlichen Sprachgebrauch herbeizuführen. In der **Abb. 1.1** ist die Eingliederung des IT-Risikomanagements in die Unternehmenssicht sowie dessen grobe Aufteilung grafisch dargestellt.

Informationstechnologie (IT) wird häufig mit Synonymen wie Informations- und Kommunikationstechnologie, (elektronische) Datenverarbeitung oder gar Wissensmanagement belegt. Dies legt die Vermutung nahe, dass Daten, Informationen und Wissen das Gleiche sind, was jedoch nicht der Fall ist. Daten sind eine mit Syntax versehene Zeichenkette. Sobald diese Daten in einen inhaltlichen Kontext aufgenommen werden, handelt es sich um eine Information. Die Möglichkeit der Nutzung der Informationen, z.B. durch deren Kombination, stellt Wissen dar.[6] Das Buch zeigt das Risikomanagement für die Verarbeitung von Informationen im Rahmen einer elektronischen Datenverarbeitung auf. Zusätzlich werden weitere Leistungen, die von IT-Bereichen erbracht werden, in das IT-Risikomanagement integriert. Das IT-Risikomanagement verwendet für sich selbst ebenfalls Informationstechnologie und Techniken des Wissensmanagements. Der Begriff „IT" wird nachfolgend für die umfänglichen, technischen und organisatorischen Regelungen zur Verarbeitung und zum Transport von Informationen im Unternehmen verstanden. Sofern sich betriebswirtschaftlich oder risikopolitische Aussagen auf die IT beziehen bzw. beschränken, wird dies mit der Ergänzung „IT-" kenntlich gemacht.

---

6 Vgl. Krcmar, 2003, S. 14–15.

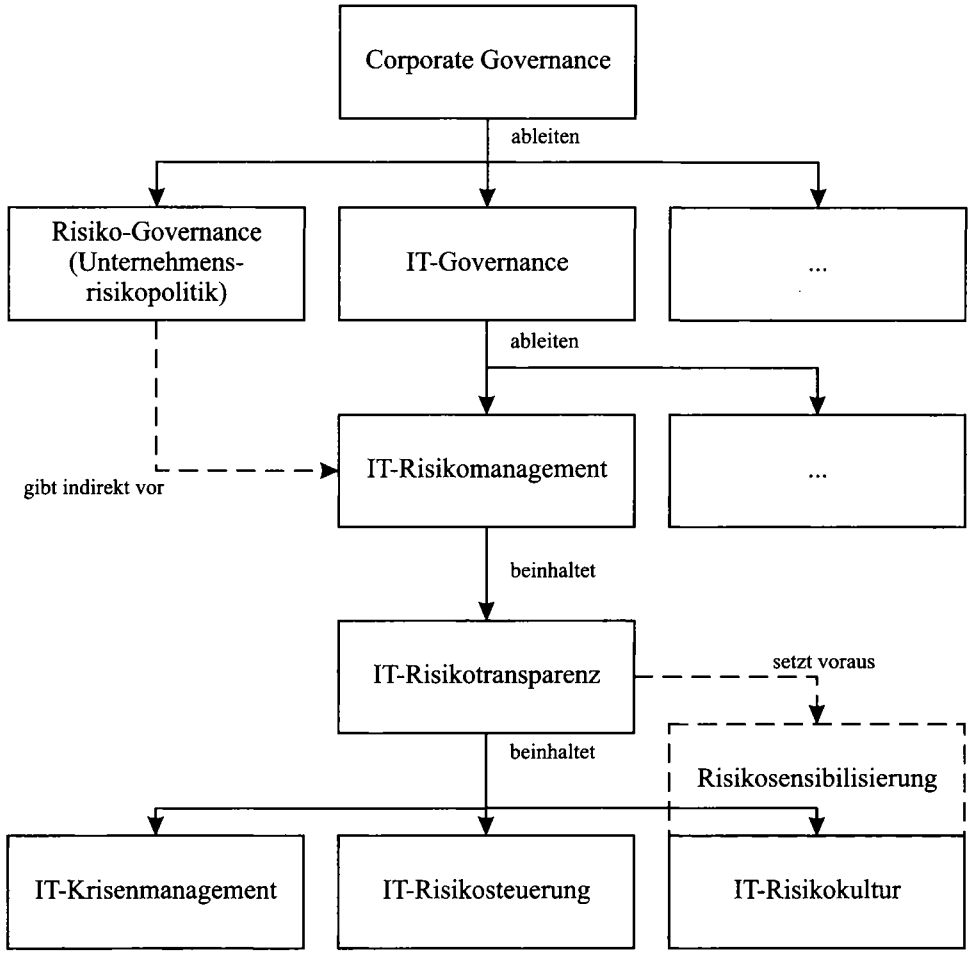

Abb. 1.1 Aufbau IT-Risikomanagement

Wichtigste Aufgabe der IT innerhalb eines Unternehmens ist es, die unternehmenseigenen Ziele optimal zu unterstützen. Die Übereinstimmung der IT-Strategie mit der Unternehmensstrategie und deren Ziele wird als IT-Governance bezeichnet. Die Kombination aus technologischem und fachlichem Wissen mit strategischer Ausrichtung bildet vielfach das Fundament für die Erarbeitung von Wettbewerbsvorteilen.[7] Aus dieser IT-Governance müssen die Handlungen der IT bezüglich des IT-Risikomanagements abgeleitet werden. Das IT-Risikomanagement muss sich über diese IT-Governance mit der Risikostrategie des Gesamtunter-

7 Vgl. Wild, 2003, S. 23.

nehmens abstimmen. Als Basis für ein effektives IT-Risikomanagement bedarf es einer IT-Risikotransparenz. Um diese Transparenz zu schaffen, wird eine Grundsensibilisierung der Mitarbeiter bezüglich des Risikomanagements benötigt. Im 2. Kapitel wird die Vorgehensweise zum Erreichen der IT-Risikotransparenz aufgezeigt. Die erforderliche Grundsensibilisierung bis hin zu einer Risikokultur wird beschrieben. Die Risikosteuerung ist anschließend Inhalt des 3. Kapitels. Es wird auf die Inhalte, Methoden und Vorgehensweisen zur effektiven Steuerung des Risikoportfolios eingegangen. Das 4. Kapitel widmet sich dem IT-Krisenmanagement.

Im Folgenden wird auf bereits bestehende Definitionen/Kategorisierungen zurückgegriffen und diese bei Bedarf an die Besonderheiten des Themengebietes angepasst. Sollten in der Literatur verschiedene Definitionen vorhanden sein, so wird die am weitesten verbreitete bzw. die im Zusammenhang mit dem Thema IT-Risikomanagement am sinnvollsten einsetzbare verwendet.

1.1 Grundlegende Definitionen

In diesem Buch wird vielfach die Sprache von Anwendungen, Systemen und Plattformen sein. Unter einer *Anwendung* wird eine abgeschlossene Softwareeinheit verstanden und stellt, wenn kein Zusatz wie „systemnah" verwendet wird, im Regelfall eine fachliche Anwendungslogik dar. Ebenso kann darunter das zur Verfügung stellen von Daten verstanden werden, wie zum Beispiel der unternehmensweite Kundenstamm. *Systeme* entstehen anwendungsübergreifend. Die beinhalteten Anwendungen kommunizieren über verschiedene Schnittstellen miteinander. Man unterscheidet zwischen Schnittstellen fachlicher Anwendungen untereinander und Schnittstellen von fachlichen Anwendungen mit Basisdiensten/Infrastrukturkomponenten, sogenannten Systemvoraussetzungen. Unter *Plattformen* wird die jeweilige Infrastruktur für das Betreiben der Anwendungen verstanden. Dieser Begriff beinhaltet die Hardware und systemnahe Software. Typische Plattformen sind der Host oder die C/S-Umgebungen, wobei Plattformen auch heterogen gestaltet sein können.

Die nachfolgenden Begrifflichkeiten werden im Zusammenhang mit dem Risikomanagement verwendet. Der unterschiedliche Gebrauch führt immer wieder zu Fehlkommunikation und Irritationen. Im Zusammenhang mit dem IT-Risikomanagement werden folgende Definitionen in diesem Buch verwendet.

1.1.1 Risiko

Risiko wird im Sprachgebrauch in unterschiedlichster Weise verwendet. In der Fachliteratur wird der Begriff Risikomanagement im Detail häufig unterschiedlich definiert. Dabei ist der

kleinste gemeinsame Nenner, dass durch ein Ereignis mit einer bestimmten Wahrscheinlichkeit Verluste eintreten.[8] Die für das Buch geltende Definition ist daran angelehnt.

Risiko ist die Möglichkeit (Wahrscheinlichkeit) einer Abweichung des tatsächlichen Ergebnisses vom erwarteten Ergebnis. Diese Abweichung kann positiv oder negativ sein. Bei negativen Abweichungen besteht die Gefahr, dass unerwünschte Ergebnisse eintreten (Verluste) oder die Gefahr, dass erwünschte Ergebnisse nicht eintreten (verpasste Chancen). Positive Risiken (Chancen) drücken sich durch ein Eintreten unerwartet positiver Ergebnisse aus. Das Risikopotenzial/-volumen ergibt sich aus dem Abweichungsdelta und dessen Eintrittswahrscheinlichkeit.

Das Risiko ist eine spezielle Form der Unsicherheit, die grundsätzlich eine nicht vorhandene Sicherheit bezüglich einer Angelegenheit ausdrückt. Das Risiko kann gegenüber der Unsicherheit aus Erfahrungsgründen eingeschätzt werden und Gegenmaßnahmen können geplant werden.[9]

Qualität ist die relative Differenz zwischen einem geplanten und dem tatsächlichen Ergebnis. Es beinhaltet gegenüber dem Risiko nicht die Wahrscheinlichkeit des Eintritts. Das Risiko beinhaltet die absolute Differenz zwischen einem geplanten und dem tatsächlichen Ergebnis und berücksichtigt dabei zusätzlich die Eintrittswahrscheinlichkeit.[10] Bei der Betrachtung von Risiko wird zwischen Risikoursachen (diese werden in den Risikoszenarien beschrieben), Risikoereignissen (welche letztlich die Schadensfälle darstellen) und Risikoauswirkung (welche das Schadensmaß wiedergeben) unterschieden. Die Komplexität des Risikomanagements von operationellen Risiken, zu denen auch die IT-Risiken gehören, entsteht dadurch, dass verschiedene Risikoursachen für ein Risikoereignis verantwortlich sein können. Zudem kann eine Risikoursache eine Vielzahl von Risikoereignissen gleichzeitig anstoßen. Die Risikoereignisse können wiederum die unterschiedlichsten Auswirkungen haben und bei gleichzeitig eingetretenen Risikoereignissen sind die Ursachen und/oder Auswirkungen untereinander nicht unbedingt voneinander abgrenzbar.

In **Abb. 1.2** wird dargestellt, wie sich aus 2 Risikoursachen unterschiedliche Auswirkungen ergeben können. Das Beispiel zeigt an einem kleinen Ausschnitt die rasch steigende Komplexität bei einer größeren Anzahl von Ursachen, Ereignissen und möglichen Auswirkungen. Das erste Risikoereignis „Fehladministration der Anwendung Risikomanagement" wird nur durch die Risikoursache „menschlicher Fehler aus Konzentrationsmangel" bewirkt und hat direkt zur Folge, dass die Anwendung ausfällt. Das zweite und dritte Risikoereignis beruht ebenfalls auf einem „menschlichen Fehler aus Konzentrationsmangel" und zusätzlich auf der Tatsache, dass die Administrationsprozesse nicht den aktuellen Anforderungen des Prozessdesigns von Administrationsprozessen entsprechen. Sie haben beide die gleichen Risikoursachen. Lediglich die Objekte, auf die diese Ursachen treffen, sind unterschiedlich und haben

8 Vgl. Wallmüller, 2002, S. 165–167.

9 Vgl. Weber/Liekweg, 2000, S. 279.

10 Vgl. auch Meier, 2004, S. 20–21.

andere Auswirkungen. Bei einem Administrationsfehler in der Anwendung „Risikoquantifizierung" fällt nur diese Anwendung aus. Findet das gleiche Ereignis im relevanten Datenbanksystem statt, so fallen die Anwendungen „Risikomanagement" und „Risikoquantifizierung" aus.

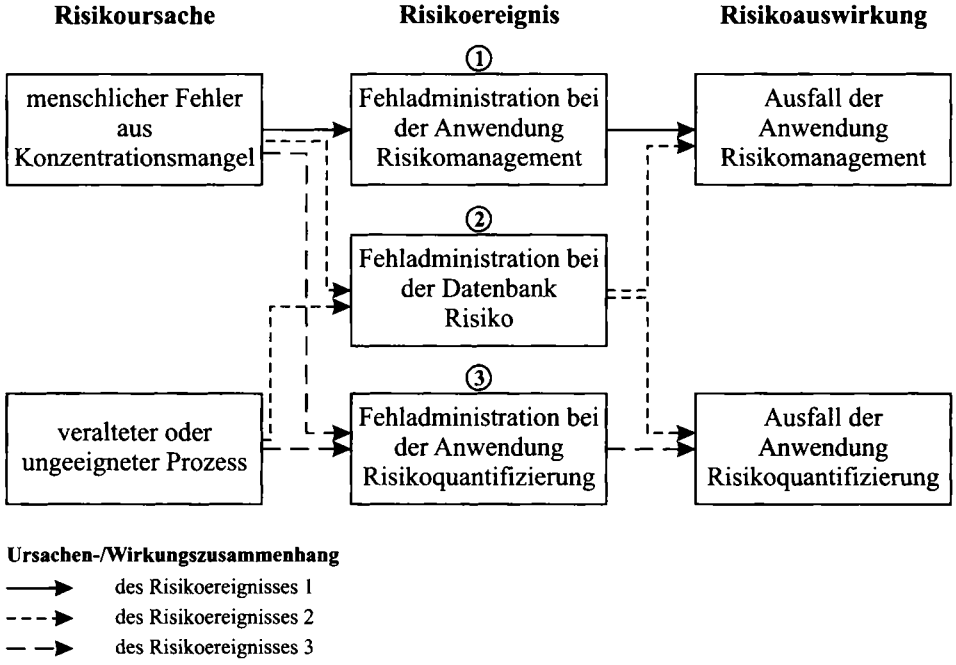

Abb. 1.2 Zusammenhang Risikoursache/-ereignis/-wirkung

1.1.2 Operationelle Risiken

Operationelle Risiken sind Risiken aus dem Geschäftsablauf heraus, sie werden auch operationale Risiken genannt. Sie stellen die ursprünglichste Form von Geschäftsrisiken dar. Unabhängig davon, welche Geschäfte betrieben werden, können Risiken wie fehlerhaftes Verhalten, Unkenntnis, Betrug, Naturkatastrophen, etc. zum Tragen kommen. Seit die Menschheit Geschäfte abwickelt, wird bewusst oder unbewusst, erfolgreich oder weniger erfolgreich mit diesen Risiken umgegangen.

Basel definiert operationelle Risiken als die Gefahr von direkten oder indirekten Verlusten, die infolge der Unangemessenheit oder des Versagens von internen Prozessen, Menschen, Systemen oder durch externe Einflüsse auftreten. Ausgeschlossen werden explizit strategische Risiken und Reputationsrisiken. Basel II gibt zugleich die individuelle Freiheit, operationelle Risiken innerhalb der einzelnen Institute unterschiedlich definieren zu können. Eine

elementare Anforderung besteht darin, dass jedes Institut für sich die gesamte Spanne möglicher, operationeller Risiken berücksichtigt und ein unternehmensweites Verständnis für die Definition vorliegt.[11]

Andere Ansätze beziehen strategische Risiken in die operationellen Risiken mit ein. Die *Group of 30* ist eine Vereinigung von hochrangigen Vertretern aus der Privatwirtschaft, dem öffentlichen Sektor und der Wissenschaft, die wirtschaftliche Situationen analysiert und Handlungsempfehlungen daraus ableitet. In ihrer Definition erscheint neben den bereits oben erwähnten Risikoursachen Prozesse, Mensch und Systeme ausdrücklich noch der Managementfehler als eigene Kategorie.[12]

Während Basel II Schadensfälle nur über realisierte Verluste definiert, wird in diesem Buch ein Schadensfall ebenso bei einer nicht geplanten, positiven Auswirkung unterstellt. Einen der großen Vorteile beim Betreiben eines Risikomanagements stellt der Lerneffekt für die Beteiligten dar. Dieser Lerneffekt kann ebenso aus Ereignissen abgeleitet werden, die sich letztlich „unerwartet" doch noch ergebnisneutral oder sogar gewinnbringend dargestellt haben. Die ausschlaggebende Eigenschaft eines eingetretenen Risikos ist, dass dessen Auswirkung nicht geplant war.

Eine Abgrenzung der operationellen Risiken gegenüber weiteren Geschäftsrisiken, beispielsweise im Kreditgewerbe die Adressausfall-, Marktpreis- und Liquiditätsrisiken, ist im Zusammenhang mit dem IT-Risikomanagement von geringer Bedeutung. Es kann davon ausgegangen werden, dass sämtliche IT-Risiken unter die Rubrik der operationellen Risiken fallen. Zwar können im IT-Betrieb Lieferanten ausfallen, das Adressausfallrisiko bezieht sich allerdings lediglich auf das Forderungsrisiko. Dies dürfte im IT-Bereich, mit Ausnahmen von Anzahlungen, von untergeordneter Bedeutung sein. Für den IT-Bereich ist der Ausfall eines Lieferanten eher mit einhergehenden Änderungen von unterstützen Technologien von Bedeutung. Ebenso können sich die Einkaufspreise für bezogene Leistungen ändern, es bestehen aber keine Marktpreisrisiken im Sinne von Handelsrisiken. Liquiditätsrisiken sind nur dann für die IT relevant, wenn diese als eigenständige Unternehmung auftritt. In diesem Fall sind jedoch grundsätzlich alle Risiken, die ein Unternehmen treffen können, zu berücksichtigen. Zusammenfassend kann gesagt werden, dass originäre IT-Risiken direkt als eine Ausprägung der operationellen Risiken einzustufen sind.

11 Vgl. Basel Committee, 2003, S. 2.

12 Vgl. Brink, 2001, S. 1–3.

1.1.3 IT-Risiko

Unter IT-Risiko versteht man die Unfähigkeit, anforderungsgerechte IT-Leistungen effektiv[13] und effizient[14] erbringen zu können. IT-Leistungen sind dabei der Betrieb und die Entwicklung von Systemlösungen, das Projektmanagement sowie – aus der Enabler-Funktion heraus – das Management dieser Leistungen und die Beratung der Fachbereiche für deren Geschäftstätigkeit. Sie sind Teil der operationellen Risiken.[15]

Bei der Betrachtung von IT-Risiken, die zum Teil nicht selbst den Schadensfall aus Unternehmenssicht darstellen, sondern vielmehr als Risikoursache für die eigentlichen Geschäftsabläufe zu verstehen sind, sind die strategischen Risiken in einen integrierten Risikomanagementansatz mit aufzunehmen. Die strategischen Entscheidungen sind bei immer kürzeren Entscheidungszyklen wesentlich für die Sicherheit, Stabilität, Skalierbarkeit und der damit einhergehenden Wirtschaftlichkeitsbetrachtung von IT-Lösungen. Es wird zwischen originären IT-Risiken und Anwender-IT-Risiken unterschieden.

1.1.4 Risikomanagement

Beim Risikomanagement wird zwischen strategischem und operativem Risikomanagement unterschieden. Das strategische Risikomanagement beinhaltet die Grundsätze zur Behandlung von Risiken, die Risikokultur sowie die Methodik.

Das operative Risikomanagement setzt sich – als Ausprägung des allgemeinen Managementprozesses – als Regelprozess aus den Komponenten

- identifizieren (und klassifizieren)[16],
- beurteilen (analysieren und bewerten),
- steuern (Maßnahmen festlegen und durchführen) und
- überwachen der Risiken

zusammen.[17] Diese vier Schritte gelten grundsätzlich für das Management des Risikoportfolios, wobei die Ausprägung der einzelnen Komponenten bei den unterschiedlichen Risikoarten differieren kann. Die regelmäßige, systematische Erhebung bzw. Überarbeitung des vorhandenen Risikoportfolios wird, in Anlehnung an die betriebswirtschaftlichen Bestandsermittlungen, als Risikoinventur bezeichnet. Den Rahmen für das Risikomanagement bietet eine individuell definierte Risikostrategie, die, abhängig von den Risikoarten und den Risikopotenzialen, die situative Anwendung von generischen Risikostrategien (siehe 1.3) festlegt.

---

13 Effektivität beantwortet die Frage „Tun wir die richtigen Dinge?". Hierzu gibt es abweichende Definitionen. Nach ISO 9000:2000 ist Effektivität z.B. „das Ausmaß, in dem geplante Tätigkeiten verwirklicht und geplante Ergebnisse erreicht werden."

14 Effizienz beantwortet die Frage „Tun wir die Dinge richtig?". Definition nach ISO 9000:2000: „Effizienz ist das Verhältnis zwischen dem erzielten Ergebnis und den eingesetzten Mitteln."

15 Vgl. Balduin/Junginger/Krcmar, 2002, S. 3.

16 Die Anmerkungen in Klammern sind die jeweiligen Ausprägungen für den Risikomanagementprozess.

17 Vgl. Pausenberger, 2000, S. 269–274 sowie Basel Committee, 2003, Principle 4, 5 und 6.

Neben dem Management des bestehenden Risikoportfolios ist es ebenso wichtig, die Entwicklung dieses Portfolios in den Entscheidungsprozess des Unternehmens mit einzubinden. Insbesondere bei Entscheidungen grundsätzlicher Art werden die Auswirkungen auf die Gesamtrisikosituation prognostiziert und in die Entscheidungsfindung mit einbezogen, z.B. Entscheidungen über neue Inhalte der Geschäftspolitik.[18] Bei der Beurteilung der Wahrscheinlichkeit kann zwischen a priori Wahrscheinlichkeiten, bei denen im Voraus die Eintrittswahrscheinlichkeit bekannt ist (z.B. bei einem Münzwurf), und a posteriori Wahrscheinlichkeiten, bei denen das Ereignis bereits eingetreten ist und dieser Eintritt hinsichtlich zukünftiger Aussagekraft untersucht wird, unterschieden werden. Beim IT-Risikomanagement sind a priori Wahrscheinlichkeiten von geringerer Bedeutung.

Sobald ein Risiko eingetreten ist, tritt zur möglichen Schadensreduzierung ein Schadensmanagementprozess in Kraft. Dieser basiert ebenfalls auf dem allgemeinen Managementprozess. Bei Risiken mit einem hohen Auswirkungsmaß und zumeist rasantem Schadensverlauf werden diese Schadensreduzierungsmaßnahmen in Form eines Krisenmanagements (siehe Kapitel 1) geplant und durchgeführt.

1.1.5 Risikoszenario

Unter einem Risikoszenario versteht man das ganzheitliche Aufzeigen von möglichen Schadensabläufen anhand von generischen Beispielen. Beim Eintritt reduziert oder verhindert es eine oder mehrere IT-/Unternehmensleistungen. Durch die Operationalisierung werden die Risikoszenarien auf die einzelnen Leistungen konkretisiert. Risikoszenarien können auf einer oder mehreren Risikoursachen beruhen. Zu den Szenarien werden die Eintrittswahrscheinlichkeit und die Auswirkungen sowie mögliche Risiko- bzw. Schadensreduzierungsmaßnahmen aufgezeigt.[19] Durch die Konkretisierung des Gefährdungspotenzials kann eine höhere Sensibilisierung der Mitarbeiter bzw. der Verantwortlichen erreicht werden. Zugleich kann das Risikopotenzial leichter geschätzt und überwacht werden.

Durch die hohe Komplexität der Risikostruktur von Unternehmen entsteht bei einer umfänglichen Betrachtung der Risikolandschaft schnell eine unüberschaubare Anzahl von Risikoszenarien. Ihre Granularität muss eine praxisbezogene Beurteilung der einzelnen Szenarien ermöglichen und muss über das Risikoportfolio hinweg in einer einheitlichen Detaillierungstiefe erfolgen. Ihre Anzahl muss überschaubar sein und dabei das gesamte Gefährdungspotenzial abbilden. Bei der Formulierung von allgemeingültigen Szenarien wird von generischen Risikoszenarien gesprochen. Die Gesamtheit aller Risikoszenarien bildet das Risikoinventar des Unternehmens. Durch Detailvarianten in Form von operationalisierten Risikoszenarien wird eine Hierarchie aufgebaut.

---

18 Vgl. auch Basel Committee, 2003, S. 3–9.

19 Vgl. Wallmüller, 2002, S.165–167.

1.1.6 Risikopotenzial

Das Risikopotenzial eines Szenarios setzt sich aus den Komponenten Eintrittswahrscheinlichkeit und Schadenshöhe (Auswirkungsmaß) zusammen. Das Produkt dieser Komponenten stellt das Risikopotenzial dar, es wird auch Risikovolumen genannt. Es bezieht sich immer auf einen definierten Zeitraum. Das Risikopotenzial eines Szenarios wird gerne in einer Risikomatrix dargestellt.

Das Gesamtrisikopotenzial setzt sich aus dem durchschnittlichen Risikopotenzial über die Laufzeit, multipliziert mit der voraussichtlichen Existenzdauer des Risikos, zusammen. Bei langfristigen Risiken ohne definiertes Risikoende ist zur Berechnung immer ein Zeitraum der Betrachtung anzugeben. Ferner kann das Risikopotenzial bei IT-Risiken zwischen einem direkten und einem indirekten Risikopotenzial unterschieden werden. Das direkte Risikopotenzial ergibt sich aus den potenziellen Schäden, die direkt in der IT anfallen (originäre IT-Risiken). Das indirekte Risikopotenzial ergibt sich aus den Risiken der tangierten Geschäftsabläufe (Anwender-IT-Risiken). Während bei fachlichen Anwendungssystemen größtenteils noch eine direkte Zuordnung auf Geschäftsprozesse möglich ist, sind Auswirkungen durch Ausfälle von IT-Infrastruktur zumeist nur unter unverhältnismäßig hohem Aufwand bzw. der Verwendung von Prämissen auf Geschäftsabläufe zuordenbar.

1.1.7 Gefahr

Gefahr wird umgangssprachlich mit im Detail verschiedenartigen Definitionen belegt. Grundsätzlich drückt der Begriff die Möglichkeit aus, dass etwas nicht Kalkuliertes (in der Regel Negatives) passiert. Im Vergleich zu Risiko ist dieser Begriff allgemeiner. Er beinhaltet nicht die Eintrittswahrscheinlichkeit. Das Auswirkungsmaß kann zusätzlich unbekannt sein.

1.1.8 Schaden

Ein eingetretenes Ereignis, das eine Abweichung vom geplanten Ziel darstellt (schlagend gewordenes Risiko), bezeichnet man als Schaden. Diese Abweichung kann im positiven oder im negativen Bereich liegen. Der Schaden drückt dabei die absolute Differenz aus. Zumeist werden nur die negativen Abweichungen bewusst wahrgenommen. Bei positiven Auswirkungen muss berücksichtigt werden, dass bei Planungen als Ziel oft ein Mindestmaß angesetzt wird und eine positive Abweichung nicht eine Außerplanmäßigkeit darstellen muss. In diesen Fällen empfiehlt es sich, bei den Planungen bereits einen Zielkorridor, unter Verwendung eines Mindestziels, zu definieren. Abweichungen können so objektiver ermittelt werden.

Die Schadenshöhe setzt sich aus dem bezifferbaren und nicht direkt bezifferbaren Schaden zusammen. Der bezifferbare Schaden kann direkt mit Aufwänden versehen werden. Er unterscheidet sich weiter durch den unmittelbaren Schaden, zum Beispiel Schadensersatzansprüche und den mittelbaren Schaden, wie zusätzliche Aufwendungen für die Schadensbehebung oder anderweitige Folgeschäden. Die nicht direkt bezifferbaren Schäden sind Reputationsschäden und Opportunitätskosten, wie zum Beispiel entgangene Geschäfte.

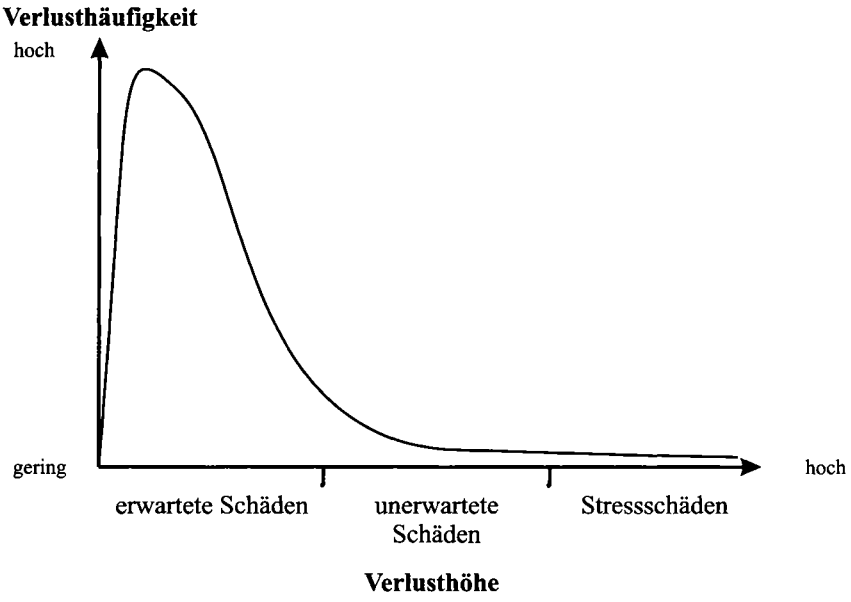

Abb. 1.3 Schadenseinteilung nach Häufigkeit

Schäden werden zudem anhand der Verlusthöhe kategorisiert. Dabei haben erwartete Schäden kleinere Schadenshöhen, kommen jedoch häufiger vor. Die unerwarteten Schäden sind seltener, haben dafür größtenteils ein höheres Schadensmaß. Sogenannte Stressschäden haben extreme Schadensmaße, kommen aber sehr selten vor. Oftmals werden diesen Kategorien in der Literatur Schadensstrategien zugeordnet. Hier wird davon ausgegangen, dass erwartete Schäden im Verkaufspreis von Produkten als Kosten berücksichtigt werden. Die unerwarteten Schäden werden über eine Eigenkapitalhinterlegung gedeckt und die Stressschäden werden versichert. Diesem pauschalierten Ansatz kann nicht einfach zugestimmt werden. Viele erwartete Schäden werden ebenfalls versichert. Beispiele hierfür sind KFZ-Versicherungen oder im IT-Bereich erweiterte Garantien für Hardwareschäden. Versicherungen stehen grundsätzlich für alle Schadensklassen zur Verfügung. Die Ausnahmen von Versicherbarkeit zeigen sich erfahrungsgemäß bei den Stressschäden. So können in bestimmten Gebieten definierte Naturkatastrophen nicht versichert werden. Ebenso können gewisse Katastrophen wie beispielsweise Krieg oder atomare Zwischenfälle nicht oder nur unzureichend versichert werden. Aus diesem Grund wird in der **Abb. 1.3** auf eine Zuordnung dieser Schadensstrategien bewusst verzichtet.

1.1.9 IT-Notfall/Krisenfall

Die komplette oder teilweise Nichtverfügbarkeit von IT-Systemen ist ein Systemausfall. Kann dieser Systemausfall nicht in einer angemessenen Zeit, mit den gewöhnlichen IT-

Prozessen in den normalen Betriebszustand zurückgeführt werden, liegt ein Notfall vor. Die Zuständigkeiten, Prozesse und Voraussetzungen zur Behebung eines solchen, sind im Notfallplan dokumentiert. Für alle kritischen IT-Systeme muss ein Notfallplan vorliegen. Hat der Notfall weitreichende Folgen auf die Geschäftsprozesse und überschreitet er eine zuvor definierte Grenze, so dass der Ausfall der Systeme z.B. existenzgefährdend für das Unternehmen werden kann, ist ein IT-Krisenfall eingetreten.

1.2 Kategorisierung von Risiken

Die Kategorisierung von betrieblichen Risiken kann anhand unterschiedlicher Kriterien erfolgen. Es entsteht eine mehrdimensionale Betrachtungsweise von Risiken. Die gängigen Unterscheidungskategorien werden nachfolgend erläutert, deren Ausprägungen beschrieben und ein Bezug zum IT-Risikomanagement hergestellt.[20] Dabei handelt es sich nicht um eine abschließende Aufstellung aller Risikokategorien. Vielmehr soll die grundsätzliche Problematik der Mehrfachkategorisierung von Risiken veranschaulicht, Methoden zu Beherrschbarkeit dieser Mehrdimensionalität (siehe 3.1.3) aufgezeigt und über die Definition der gängigsten Kriterien eine bessere Handhabung und Kommunikation der Risikoklassifizierung erreicht werden.

Durch die Kategorisierung von Risiken wird das Zusammenfassen von gleichartigen Risiken und somit die Beherrschbarkeit dieser Risiken mittels gemeinsamer oder ähnlicher Risikoindikatoren und Risikoreduzierungsmaßnahmen ermöglicht. Bei der Kategorisierung ist von besonderer Bedeutung, dass die Definition der einzelnen Kategorien möglichst exakt erfolgt. Dadurch kann eine dezentrale Risikozuordnung qualitativ hochwertig sichergestellt werden. Dies ist unternehmensintern und unternehmensübergreifend wichtig. Beispielhafte Sachverhalte hierfür sind die Bildung von Datenkonsortien für den Austausch von Schadensfällen, das Benchmarking von Risikoportfolien oder die Anwendung allgemeiner Kategorisierungskataloge zur Veröffentlichung statistischer Sachverhalte.

1.2.1 Ursachen-/Wirkungsprinzip

Durch die Betrachtung der Lebenszyklen von Risiken können Unterscheidungskriterien hergeleitet werden. Besteht ein Risiko für ein Unternehmen, so ist damit noch nicht zwingend eine Beeinträchtigung der Geschäfte einhergehend. Erst mit dem Eintritt eines bestimmten Ereignisses bzw. einer Ereigniskombination wird aus dem latent vorhandenen Risiko ein Schadensfall mit letztlich direkten oder indirekten Auswirkungen auf den wirtschaftlichen Erfolg des Unternehmens.

20 Vgl. auch Romeike, 2003c, S. 167–173.

Risikoursachen
Risiken können hinsichtlich ihrer Ursachen unterschieden werden. Diese können wiederum nach unterschiedlichen Merkmalen gruppiert werden. Wir verwenden eine aus Basel II abgeleitete Kategorisierung, die sich grundsätzlich für betriebliche Risiken eignet. Weitergehende Aspekte des IT-Risikomanagements können ebenfalls abgebildet werden.[21] Ein Vergleich mit den Kategorien des Gefährdungskataloges des IT-Grundschutzhandbuchs vom Bundesamt für Sicherheit in der Informationstechnik verdeutlicht, dass sich diese Einteilung in 5 Gefährdungskategorien für IT-Komponenten auch für IT-Risiken bewährt. Zu den Basel-Kategorien sind nur geringfügige Abweichungen zu vermerken. Die Kategorie Mensch wird dabei mit zwei Kriterien – Fehlhandlungen und vorsätzliche Handlungen – aufgeführt. Die Kategorie Prozesse/Projekte wird auf organisatorische Mängel reduziert. Externe Einflüsse werden als höhere Gewalt und Technik als technologisches Versagen bezeichnet.

Die einzelnen Kategorien können weiter untergliedert werden. Der Verband öffentlicher Banken (VÖB), Frankfurt, hat beispielsweise eine weitergehende Untergliederung für seine angeschlossenen Banken erarbeitet. Diese wird in **Tab. 1.1** mit ihren ersten zwei Kategorisierungsebenen aufgeführt. Mittels dieser Untergliederung wird eine Definition der expliziten Inhalte der einzelnen Kategorien erreicht.

Um eine höhere Trennschärfe zwischen Risikoursache und Risikotreiber (siehe 2.5.2) zu gewährleisten, wird in den nachfolgenden Kategorisierungen eine weitergehende Abgrenzung hierzu vorgenommen.

Mensch.
„Am Ende sind alle Probleme der Wirtschaft Personalprobleme."
– Alfred Herrhausen (ehemaliger Vorstandssprecher der Deutschen Bank) –

In einer weitergehenden Betrachtung kann dieser Aussage zugestimmt werden. Teile der externen Einflüsse ausgenommen, hinsichtlich derer der Mensch mangels direkter Einwirkungsmöglichkeiten nur Vorsorgemaßnahmen treffen kann, sind die anderen Risikofaktoren direkt beeinflussbar bzw. von ihm verursacht. So sind sowohl die Prozesse selbst als auch die Technik Resultate menschlichen Handelns. Fehler oder Unzulänglichkeiten daraus sind letztlich dem Menschen zuordenbar. Selbst das nicht Durchführen eines Risikomanagements und das daraus resultierende höhere Risikopotenzial ist eine Entscheidung der beteiligten Mitarbeiter.

Bei der Kategorisierung von Risiken gemäß deren Ursachen wird allerdings von einer primären Ursachenzuordnung ausgegangen. So fallen in die Kategorie Mensch nur die Risiken, die direkt zugeordnet werden können, wie menschliches Versagen oder kriminelle Handlungen.

21 Vgl. Basel Committee, 2004, S. 137.

Tab. 1.1 Risikokategorien nach VÖB[22]

Untergliederungsebene	Risikokategorien			
Primärebene	Mensch	Technologie	Prozesse und Projektmanagement	Externe Einflüsse
Sekundärebene	Gesetzeswidrige Handlungen (Interner)	Systemsicherheit	Management-, Kontroll- und Prozessschwächen	Gesetzeswidrige Handlungen (Externer)
	Verkaufspraktiken/Vertrieb	Software	Projektmanagement	Politisch
	Unautorisierte Handlungen	Hardware		Verkäufer und Lieferanten
	Humanvermögen	Haustechnik, Gebäude, Anlagen		Outsourcing
	Transaktionen			Infrastrukturlösungen
				Öffentliche Aktivitäten
				Naturkatastrophen
				Sonstige Katastrophen

Risikotreiber für Ursachen im menschlichen Bereich stellen Faktoren wie Ausbildungsstand und Motivation dar. Schlecht ausgebildete und dadurch überforderte Mitarbeiter werden häufiger Fehler begehen, ebenso Mitarbeiter mit einer geringen Motivation. Es kann ganze Risikotreiberbündel geben, die letztlich die eigentlichen Risikoursachen – in diesem Fall beispielsweise menschliches Versagen – beeinflussen.

Technologie. Eine der großen Rubriken für die Fachbereiche sind in dieser Kategorie die Risiken aus der Informationstechnologie, welche durch fehlerhafte Verarbeitung oder mangelnde Verfügbarkeit entstehen können. Darüber hinaus gibt es weitere, technische Abhängigkeiten, beispielsweise sämtliche infrastrukturelle Komponenten wie die Strom- und Wasserversorgung.

In dieser Kategorie sind für das IT-Risikomanagement im Besonderen die technischen Leistungen von Drittanbietern wie Hardware und die oben erwähnte Infrastruktur zu nennen. Zusammenfassend ist anzumerken, dass die technischen Risiken im IT-Umfeld ein geringeres Ausmaß als erwartet darstellen. Demgegenüber haben technikabhängige Fachbereiche mit unter ein enormes Risikopotenzial in Form von Anwender-IT-Risiken.

22 VÖB, 2001, S. 128.

Typische Risikotreiber in diesem Bereich sind Kosteneinsparungen bei der Wartung oder eine hohe Systemkomplexität.

Prozesse & Projektmanagement. Im Bereich Prozesse liegt ein großes Potenzial für Risikoursachen. In dieser Kategorie sind alle Arten von sogenannten Prozessschwächen enthalten. Beispiele hierfür sind unzureichend ausgeprägte Kontrollmechanismen, unvollständig definierte oder implementierte Prozesse oder mangelnde bzw. inkonsistente Rollendefinitionen.

Projekte werden gesondert in dieser Rubrik mit aufgeführt, da diese ebenfalls einen Prozess darstellen, der für viele Unternehmen von besonderer Bedeutung ist. Projekte sind zumeist einmalige oder wiederholende Vorhaben mit individuellen Anpassungen. Das Risikopotenzial ist somit tendenziell groß.

Als typische Risikotreiber im Umfeld der Prozessrisiken können Prozesskomplexität, Unternehmenskultur – insbesondere Fehlerkultur – oder Automatisierungsgrad angeführt werden.

Externe Einflüsse. Unter externen Einflüssen werden gerne zuerst Katastrophen angeführt. Angefangen bei Naturkatastrophen wie Überschwemmung oder Erdbeben, über Sabotageakte wie Feuer bis hin zu terroristischen Anschlägen. Das realistisch viel größere Risikopotenzial liegt in weniger spektakulären Umständen. Hierunter fallen Risikoursachen wie Betrug, Fehlverhalten von externen Personen oder rechtliche Gegebenheiten wie der Gesetzesgebung und deren Auslegung.

Für das IT-Risikomanagement ist diese Ursachenkategorie von großer Bedeutung. Neben den katastrophalen Risiken, die letztlich im IT-Krisenmanagement münden, sind vor allem die Entwicklung der Technologien und der Marktverhältnisse auf dem IT-Markt zu beachten. Annähernd bei jeder technologischen Neuentwicklung oder einer wesentlichen Weiterentwicklung versuchen die Hersteller über architektonische Alleinstellungsmerkmale und der daraus oft resultierenden Proprietät ihrer Systeme, Marktmacht zu erlangen bzw. diese auszubauen. Die Entscheidung für eine Technologie oder einem Technologiederivat, dass sich letztlich am Markt nicht durchsetzen kann, ist ein großer Risikofaktor. Im Umfeld der IT-Sicherheit stellt die IT-Kriminalität mit Schlagwörtern wie Hackern, Viren und Phishing ein großes Risikopotenzial dar.

Exemplarische Risikotreiber von externen Einflüssen sind die Marktmacht von Anbietern, Zeitintervalle von technologischen Innovationszyklen, Kriminalitätsentwicklungen und das politische Umfeld.

Auswirkungsart

Nachdem ein Risiko über das Schadensereignis schlagend geworden ist, ergeben sich unterschiedliche Auswirkungen. Risiken können hinsichtlich ihrer potenziellen Auswirkungen unterschieden werden.

Monetäre Risiken/Effizienzrisiken. Die monetären Risiken schlagen sich direkt in der Gewinn- und Verlustrechnung des Unternehmens nieder. Dies kann durch entgangenen Ge-

winn oder vorhandenen bzw. erhöhten Verlust stattfinden. Vielfach werden ursprünglich qualitative Risiken (verringerte Leistung) über ad-hoc Maßnahmen in monetäre Risiken umgewandelt, z.B. durch zusätzliche Qualitätsmaßnahmen.

Qualitative Risiken. Bei den Qualitativen Risiken drückt sich der Schaden in einer verringerten Leistung aus. Dies kann in einem geringeren quantitativen oder qualitativen Umfang bestehen.

Im IT-Risikomanagement sind diese Risiken, z.B. die geringere Verfügbarkeit von Systemen für die Kunden/Fachbereiche, zu identifizieren. Ebenso haben Projekte, in deren Zeitverlauf der Projektumfang angepasst wird, zumeist ein großes Potenzial für diese Risikokategorie.

Image-Risiken. Schwierig zu quantifizieren sind sogenannte Image- oder Reputationsrisiken. Die Auswirkungen dieser Risiken führen zu einer geänderten öffentlichen Meinung gegenüber dem Unternehmen. Als öffentliche Meinung wird das von der Allgemeinheit oder von einzelnen Interessengruppen empfundene Gesamtbild des Unternehmens bzw. von Unternehmensteilen verstanden.

Die Auswirkungen von Image-Risiken sind schwer auf ein einzelnes Vorkommnis zurückzuführen. Sie können meistens nur qualitativ oder indirekt quantitativ über Kundenbefragungen gemessen werden.

Hohes Potenzial für Image-Risiken beim IT-Risikomanagement bilden die Systemverfügbarkeit sowie insbesondere bei Finanzdienstleistern die IT-Sicherheit/der Datenschutz.

Schadensereignisse
Zur Vollständigkeit seien im Zusammenhang mit dem Ursachen-/Wirkungsprinzip die auslösenden Ereignisse genannt. Die Schadensereignisse sind instanzierte Risikoursachen. Beispielsweise tritt die Risikoursache menschliches Fehlverhalten in einem konkreten Fall, z.B. einer Fehlentscheidung aufgrund mangelnden Faktenwissens, als Schadensereignis auf. Die Schadensereignisse sind im Regelfall so heterogen, dass diese nur in speziellen Fällen für eine Kategorisierung verwendet werden können. Schadensereignisse werden oftmals den Klassen der Schadensursachen zugeordnet. Daneben existieren ebenso Einteilungen, die auf Schadensereignissen beruhen, diese werden jedoch gerne mit Risikoursachen vermischt.

1.2.2 Zeiträume

Risiken können nach ihren zeitlichen Dimensionen unterschieden werden. Es gibt mehrere Sichten, aus denen sich zeitliche Dimensionen ableiten lassen. Ein Risiko kann aus unterschiedlichen Perspektiven verschiedenen Zeitkategorien zugeordnet werden.

Existenzzeitraum
Ein Unterscheidungsmerkmal von Risiken liegt im zeitlichen Horizont, in dem die Risiken existent sind. Diese Betrachtungsweise ist bezüglich der Einleitung von Risikoreduzie-

rungsmaßnahmen von großer Bedeutung. Je länger mit der Existenz eines Risikoszenarios gerechnet werden muss, desto sinnvoller erweisen sich bei gleicher Eintrittswahrscheinlichkeit und erwarteter Schadenshöhe die Einleitung von entsprechenden Gegenmaßnahmen. Ebenso muss beachtet werden, ob mögliche Risikoreduzierungsmaßnahmen in der Geltungsdauer des Risikoszenarios nachhaltig greifen können.

Die Klassifizierung der Risiken nach kurz-, mittel- und langfristigen Risiken kann nach Zeiträumen oder entsprechend nachfolgender Definitionen erfolgen. Bei der Einteilung nach festen Zeiträumen ist eine Restlaufzeitbetrachtung sinnvoll. Die Einteilung der Zeiträume kann dabei frei erfolgen, üblicherweise werden betriebswirtschaftliche Regelzeiträume (z.B. bis 1 Jahr, 1–4 Jahre und länger als 4 Jahre) angesetzt. Die Einordnung gemäß der Definitionen stellt die Charakteristik der Risiken stärker heraus.

kurzfristige Risiken. Kurzfristige Risiken sind typische temporäre Risiken. Sie beziehen sich zumeist auf einmalige Situationen, die sich oftmals erst kurzfristig ergeben und schwierig vorauszusehen sind. Sie werden überwiegend durch Improvisation gemanagt. Das Risikopotenzial ist über das Bestehen des Risikos mit hoher Wahrscheinlichkeit beständig. Beispiele hierfür sind:

- Projektrisiken bei Kleinprojekten
- Risiken in Ausnahmesituationen (z.B. nach Auslösung eines Notfallplanes)

mittelfristige Risiken. Mittelfristige Risiken sind Risiken, deren Ende durchaus beschrieben bzw. erwartet werden kann. Das erwartete Ende liegt jedoch nicht in naher Zukunft. Das Risikopotenzial ist über den Risikolebenszyklus mit gewisser Wahrscheinlichkeit variabel. Beispiele hierfür sind:

- Risiken aus dem Betrieb eines konkreten Anwendungssystems heraus
- Projektrisiken bei Großprojekten

langfristige Risiken. Bei langfristigen Risiken ist ein Wegfall des Risikos nicht zu erwarten. Das Risikopotenzial ist über den Risikolebenszyklus mit hoher Wahrscheinlichkeit variabel. Beispiele hierfür sind:

- Risiko eines Terroranschlags
- Risiko des Betrugs

Entscheidungswirkung

Risiken entstehen aufgrund von unternehmerischen Entscheidungen bzw. das Risikopotenzial wird davon maßgeblich beeinflusst. Der Einflusszeitraum einer Entscheidung kann als Kategorisierungsinstrument verwendet werden.

Strategie-/Geschäftsrisiken. Strategische Entscheidungen wirken mittel- bis langfristig. Sie betreffen vielfach mehrere Risikoszenarien oder gar große Teile eines Risikoportfolios. Strategische Entscheidungen sind abstrakt und werden letztlich über verschiedene Entscheidungen im operativen Bereich umgesetzt. Basierend auf dem Grundsatz, dass die IT-Strategie der Geschäfts- oder Unternehmensstrategie folgt, entsteht die Gefahr, geschäftspolitische