Hans-Peter Königs

IT-Risiko-Management mit System

- Von den Grundlagen bis zur Realisierung
- Ein praxisorientierter Leitfaden

Mit Online-Service zum Buch

vieweg

Edition <kes>

Geleitwort

Das IT-Risiko-Management hat sich als Element der „Corporate Governance“ zu einem wesentlichen Bestandteil der nachhaltigen Unternehmensführung entwickelt, Es gewinnt angesichts wachsender Bedrohungen und Schäden weiter an rechtlicher, regulatorischer und geschäftlicher Bedeutung. Dementsprechend hoch ist die Aufmerksamkeit für dieses Thema seitens der Gesetzgeber, der Regulatoren, der wirtschaftlichen Entscheidungsträger und der Nutzer von IT-Dienstleistungen, aber auch der breiten Öffentlichkeit.

Während sich inzwischen viele Publikationen mit den Grundlagen des Risko-Managements und der entsprechenden Theoriebildung beschäftigen, existieren bislang nur sehr wenige unmittelbar nachvollziehbare und umsetzbare Leitfäden für die Praxis. Insbesondere die nicht-technischen Aspekte wie die nötige Bewusstseinsbildung für Risiken seitens der IT-Anwender, die komplexe Wechselwirkung von IT-Risiken mit ihrer geschäftlichen, technischen und organisatorischen Umgebung und die Integration des IT-Risiko-Managements in die geschäftlichen Entscheidungsprozesse benötigen Umsetzungs- und Anwendungshinweise aus der täglichen Praxis.

Es ist das besondere Verdienst des vorliegenden Werkes und seines Autors, basierend auf langjähriger Erfahrung im IT-Risiko-Management und in der Vermittlung der entsprechenden Inhalte an der Hochschule für Wirtschaft in Luzern, diese Lücke zu schliessen und damit einen praktischen und unmittelbar nutzbringenden Beitrag zur systematischen Erkennung, Behandlung und Bewältigung von IT-Risiken zu leisten.

Computer Associates als führender Anbieter von Lösungen für das IT-Sicherheits-Management ist stolz darauf, die Publikation dieses Werkes empfehlen zu dürfen.

Dr. Hannes P. Lubich
IT Security Strategist
Computer Associates AG

Computer Associates International, Inc. (NYSE: CA)
www.ca.com/ch

Hans-Peter Königs

IT-Risiko-Management mit System

Edition <kes>

Herausgegeben von Peter Hohl

Mit der allgegenwärtigen Computertechnik ist auch die Bedeutung der Sicherheit von Informationen und IT-Systemen immens gestiegen. Angesichts der komplexen Materie und des schnellen Fortschritts der Informationstechnik benötigen IT-Profis dazu fundiertes und gut aufbereitetes Wissen.

Die Buchreihe Edition <kes> liefert das notwendige Know-how, fördert das Risikobewusstsein und hilft bei der Entwicklung und Umsetzung von Lösungen zur Sicherheit von IT-Systemen und ihrer Umgebung.

Herausgeber der Reihe ist Peter Hohl. Er ist darüber hinaus Herausgeber der <kes> – Die Zeitschrift für Informations-Sicherheit (s. a. www.kes.info), die seit 1985 im SecuMedia Verlag erscheint. Die <kes> behandelt alle sicherheitsrelevanten Themen von Audits über Sicherheits-Policies bis hin zu Verschlüsselung und Zugangskontrolle. Außerdem liefert sie Informationen über neue Sicherheits-Hard- und -Software sowie die einschlägige Gesetzgebung zu Multimedia und Datenschutz.

Die ersten Titel der Reihe:

Praxis des IT-Rechts
Von Horst Speichert

IT-Sicherheit – Make or Buy
Von Marco Kleiner, Lucas Müller und Mario Köhler

Mehr IT-Sicherheit durch Pen-Tests
Von Enno Rey, Michael Thumann und Dominick Baier

IT-Risiko-Management mit System
Von Hans-Peter Königs

www.vieweg-it.de

Hans-Peter Königs

IT-Risiko-Management mit System

Von den Grundlagen bis zur Realisierung – Ein praxisorientierter Leitfaden

vieweg

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.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne von Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürfen.

Höchste inhaltliche und technische Qualität unserer Produkte ist unser Ziel. Bei der Produktion und Auslieferung unserer Bücher wollen wir die Umwelt schonen: Dieses Buch ist auf säurefreiem und chlorfrei gebleichtem Papier gedruckt. Die Einschweißfolie besteht aus Polyäthylen und damit aus organischen Grundstoffen, die weder bei der Herstellung noch bei der Verbrennung Schadstoffe freisetzen.

Das Buch wurde in seiner vorliegenden Ausstattung freundlich unterstützt durch die Telekurs Group, Zürich.

Onlineservice: http://www.koenigs-media.ch/viewegbuch/

1. Auflage Juni 2005

Alle Rechte vorbehalten
© Springer Fachmedien Wiesbaden 2005
Ursprünglich erschienen bei Friedr. Vieweg & Sohn Verlag/GWV Fachverlage GmbH, Wiesbaden 2005
Softcover reprint of the hardcover 1st edition 2005

Lektorat: Dr. Reinald Klockenbusch / Andrea Broßler

Der Vieweg Verlag ist ein Unternehmen von Springer Science+Business Media.
www.vieweg-it.de

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Konzeption und Layout des Umschlags: Ulrike Weigel, www.CorporateDesignGroup.de
Umschlagbild: Nina Faber de.sign, Wiesbaden

ISBN 978-3-322-99321-2 ISBN 978-3-322-99320-5 (eBook)
DOI 10.1007/978-3-322-99320-5

Vorwort

Die Unternehmen sehen sich neuerdings zunehmend einem ganzen Bündel verschiedenartiger operationeller Risiken sowie Markt- und Finanzrisiken gegenüber. Eine wichtige Kategorie der operationellen Risiken sind die IT-Risiken, dies vor allem deshalb, weil die meisten Unternehmen immer stärker von der Informationstechnologie abhängig sind (z.B. Spitäler, Banken, Presse). Die Anforderungen an die „Corporate Covernance" des Unternehmens legen den obersten Aufsichts- und Führungsgremien funktionstüchtige Prozesse für ein gesamtheitliches und integratives Risiko-Management nahe. Das IT-Risiko-Management ist ein Baustein im Gesamtrisiko-Prozess eines Unternehmens. Die Verantwortlichen der Informations-Technologie (IT) eines Unternehmens müssen die Sicherheit der Informationen und der IT-Systeme vermehrt an den Risiken orientieren, da eingetretene Schadensereignisse nicht nur stark zu Buche schlagen, sondern sogar den Bestand eines Unternehmens gefährden.

Da die Sicherheitsmassnahmen einen beträchtlichen Teil des IT-Budgets ausmachen, müssen die IT-Verantwortlichen vermehrt den Nutzen solcher Sicherheits-Aufwendungen rechtfertigen. Für unnötigen Überschutz ist in der Regel kein Budget vorhanden. Zur Rechtfertigung der Kosten für die Sicherheitsmassnahmen müssen diese den vorhanden Risiken systematisch gegenübergestellt werden können.

Folgerichtig werden in diesem Buch der gesamte Risiko-Management-Prozess in einem Unternehmen aufgezeigt und in diesem Rahmen die Methoden und Werkzeuge des IT-Risiko-Managements behandelt. Eine vom Gesamtrisiko-Prozess eines Unternehmens isolierte Behandlung des IT-Risiko-Managements könnte der Sache nicht gerecht werden und wäre in der Umsetzung längerfristig zum Scheitern verurteilt.

Das Buch vermittelt, dass IT-Risiko-Management nicht alleinige Aufgabe und Verantwortlichkeit einer IT-Abteilung sein kann, sondern dass es im Rahmen der Unternehmens-Strategie- und Risiko-Management-Prozesses durch die Führung des Unternehmens geprägt und getragen werden muss.

Um die integrative Darstellung mit einem möglichst hohen praktischen Nutzen zu verknüpfen, habe ich das Buch in die folgenden vier Teile unterteilt

- Grundlagen erarbeiten
- Anforderungen berücksichtigen
- IT-Risiken erkennen und bewältigen
- Unternehmensprozesse meistern

und jedem Kapitel eine Zusammenfassung mit einigen Kontrollfragen zugefügt.

Dank

Liegt das Manuskript eines Buches nach vielen Wochenenden, Abenden und eingesetzten Ferientagen endlich vor, dann sind die „wohlmeinende" fachliche Beurteilung sowie die erforderlichen Korrektur-Hinweise überaus wertvoll.

Emmerich Fuchs, mit dem ich zusammen eine Lehrveranstaltung an der Hochschule für Wirtschaft in Luzern durchführe, hat zu meinem Entschluss, das Buch zu schreiben, massgeblich beigetragen. Aus seiner Schulungs- und Berater-Tätigkeit hat er mich stets auf die Notwendigkeit eines solchen Buches hingewiesen. Ich danke ihm dafür und für seine wertvollen Korrekturen und Hinweise bei der Durchsicht des Manuskriptes.

Ulrich Moser, mit dem ich in der Telekurs Group zusammenarbeite, danke ich für seine spontane Bereitschaft, das Manuskript gegenzulesen und für seine dabei gemachten wertvollen Korrekturen und Hinweise. Die Gespräche und Diskussionen mit Uli sind für mich schon deshalb wertvoll, da er nebenamtlich an der Fachhochschule Konstanz einer Dozententätigkeit im Themenbereich IT-Sicherheit nachgeht, wie ich dies an der Fachhochschule in Luzern praktiziere.

Meiner Frau, Diemuth Königs, Autorin historischer Bücher und Fachartikel, danke ich für so Vieles, dass ich es hier nicht aufzuzählen vermag. Zeitgleich mit meinem Buch muss Sie ebenfalls ein eigenes Buch fertigstellen. Trotz des Zeitdrucks war es ihr möglich, mir in schriftstellerischen Angelegenheiten und auch sonst stets zu helfen. Ihr gilt mein ganz besonderer Dank.

Zürich, im April 2005 Hans-Peter Königs

Inhaltsverzeichnis

1 Einführung ... 1

1.1 Warum beschäftigen wir uns mit Risiken? ... 1

1.2 Risiken bei unternehmerischen Tätigkeiten ... 2

1.3 Inhalt und Aufbau dieses Buchs ... 3

Teil A ... 5

2 Elemente für die Durchführung eines Risiko-Managements ... 7

2.1 Fokus und Kontext Risiko-Management ... 8

2.2 Definition des Begriffs „Risiko" ... 9

2.3 Anwendung der Risiko-Formel ... 12

2.4 Subjektivität bei der Risiko-Einschätzung ... 13

2.5 Hilfsmittel zur Risiko-Einschätzung ... 13

2.5.1 Risiko-Matrix ... 13

2.5.2 Schadenseinstufung ... 15

2.5.3 Risiko-Karte und Risiko-Portfolio ... 17

2.5.4 Risiko-Katalog ... 18

2.5.5 Risiko-Aggregierung ... 19

2.6 Risiko-Kategorien, Risiko-Arten und Top-Down-Vorgehen ... 20

2.6.1 Bedrohungslisten ... 21

2.6.2 Beispiele von Risiko-Arten ... 22

2.7 Zusammenfassung ... 24

2.8 Kontrollfragen und Aufgaben ... 25

3 Risiko-Management als Prozess ... 27

3.1 Festlegung Risiko-Management-Kontext ... 29

3.2 Durchführung der Risiko-Analyse ... 30

3.2.1 Analyse-Arten ... 30

3.2.2 Durchführung der Risiko-Analyse in einem RM-Prozess ... 32

3.2.3 Value at Risk-Methode ... 34

3.2.4 Analyse-Methoden ... 36

3.2.5 Such-Methoden ... 38
3.2.6 Szenarien-Analyse ... 39
3.3 Durchführung von Teil-Analysen ... 39
3.3.1 Schwächen-Analyse ... 39
3.3.2 Impact-Analyse ... 40
3.4 Risiko-Bewertung ... 41
3.5 Risiko-Bewältigung ... 42
3.6 Risiko-Kontrolle und -Reporting ... 44
3.7 Risiko-Kommunikation ... 45
3.8 Anwendungen eines Risiko-Management-Prozesses ... 45
3.9 Zusammenfassung ... 46
3.10 Kontrollfragen und Aufgaben ... 47

Teil B ... 49

4 Risiko-Management, ein Pflichtfach der Unternehmensführung ... 51

4.1 Corporate Governance ... 52
4.2 Anforderungen von Gesetzgebern und Regulatoren ... 54
4.2.1 Gesetz KonTraG in Deutschland ... 54
4.2.2 Obligationenrecht in der Schweiz ... 55
4.2.3 Swiss Code of best Practice for Corporate Governance ... 56
4.2.4 Basel Capital Accord (Basel II) ... 57
4.2.5 Sarbanes-Oxley Act (SOX) der USA ... 60
4.3 Risiko-Management: Anliegen der Kunden und Öffentlichkeit ... 62
4.4 Hauptakteure im unternehmensweiten Risiko-Management ... 63
4.5 Zusammenfassung ... 66
4.6 Kontrollfragen und Aufgaben ... 67

5 Risiko-Management integriert in das Management-System ... 69

5.1 Integrativer Risiko-Management-Prozess ... 70
5.2 Normatives Management ... 72
5.2.1 Unternehmenspolitik ... 72
5.2.2 Unternehmensverfassung ... 72
5.2.3 Unternehmenskultur ... 73
5.2.4 Mission und Strategische Ziele ... 73

5.2.5 Vision als Input des Strategischen Managements 74
5.3 Strategisches Management 74
5.3.1 Strategische Ziele 76
5.3.2 Strategien 80
5.4 Strategie-Umsetzung 80
5.4.1 Strategieumsetzung mittels Balanced Scorecards (BSC) 80
5.4.2 Unternehmensübergreifende BSC 85
5.4.3 Balanced Scorecard und CobiT für die IT-Strategie 85
5.4.4 IT-Indikatoren in der Balanced Score Card 87
5.4.5 Operatives Management (Gewinn-Management) 91
5.4.6 Policies und Pläne 91
5.4.7 Risikopolitische Grundsätze 93
5.5 Zusammenfassung 94
5.6 Kontrollfragen und Aufgaben 95
Teil C 97
6 Informations- und IT-Risiken 99
6.1 Veranschaulichung der Risikozusammenhänge am Modell 99
6.2 Informationen – die risikoträchtigen Güter 101
6.3 Systemziele für den Schutz von Informationen 103
6.4 Informations-Sicherheit versus IT-Sicherheit 105
6.5 IT-Risikomanagement, IT-Sicherheit und Grundschutz 106
6.6 Zusammenfassung 107
6.7 Kontrollfragen und Aufgaben 108
7 Informations-Sicherheit und Corporate-Governance 109
7.1 Management von IT-Risiken und Informations-Sicherheit 109
7.1.1 IT-Governance und Informations-Sicherheit-Governance 110
7.1.2 Leitfaden für Informations-Sicherheit-Governance 111
7.2 Organisatorische Funktionen für Informations-Risiken 115
7.2.1 Chief Information Officer (CIO) 116
7.2.2 Chief (Information) Security Officer 116
7.2.3 Checks and Balances durch Organisations-Struktur 118
7.3 Zusammenfassung 120

7.4 Kontrollfragen und Aufgaben ... 121

8 IT-Risiko-Management in der Führungs-Pyramide ... 123

8.1 Ebenen der IT-Risiko-Management-Führungspyramide ... 124

8.1.1 Risiko- und Sicherheitspolitik auf der Unternehmens-Ebene ... 124

8.1.2 Informations-Sicherheitspolitik ... 125

8.1.3 IT-Sicherheitsweisungen und Ausführungsbestimmungen ... 127

8.1.4 IT-Sicherheitsarchitektur und -Standards ... 129

8.1.5 IT-Sicherheitskonzepte ... 132

8.2 Zusammenfassung ... 133

8.3 Kontrollfragen und Aufgaben ... 134

9 IT-Risiko-Management mit Standard-Regelwerken ... 135

9.1 Bedeutung der Standard-Regelwerke ... 135

9.2 Wichtige Regelwerke der Informations-Sicherheit ... 137

9.2.1 IT-Risiko-Bewältigung mit ISO/IEC 17799 ... 141

9.2.2 IT-Risiko-Bewältigung mit CobiT ... 144

9.3 Zusammenfassung ... 149

9.4 Kontrollfragen und Aufgaben ... 150

10 Methoden und Werkzeuge zum IT-Risikomanagement ... 151

10.1 IT-Risikomanagement mit Sicherheitskonzepten ... 151

10.1.1 Ausgangslage ... 155

10.1.2 Systembeschreibung und Schutzobjekte ... 156

10.1.3 Risiko-Analyse ... 158

10.1.4 Schwachstellen-Analyse anstelle einer Risiko-Analyse ... 161

10.1.5 Anforderungen an die Sicherheitsmassnahmen ... 162

10.1.6 Beschreibung der Sicherheitsmassnahmen ... 164

10.1.7 Umsetzung der Sicherheitsmassnahmen ... 164

10.1.8 Iterative und kooperative Ausarbeitung der Kapitel ... 166

10.2 Die CRAMM-Methode ... 167

10.3 Fehlermöglichkeits- und Einflussanalyse ... 173

10.4 Fehlerbaumanalyse ... 176

10.5 Ereignisbaum-Analyse ... 180

10.6 Zusammenfassung ... 182

10.7 Kontrollfragen und Aufgaben ... 184
Teil D ... 189
11 Risiko-Management-Prozesse im Unternehmen ... 191
11.1 Verzahnung der RM-Prozesse im Unternehmen ... 191
11.1.1 Risiko-Konsolidierung ... 193
11.1.2 Subsidiäre RM-Prozesse ... 194
11.1.3 IT-RM im Gesamt-RM ... 195
11.2 Risiko-Management im Strategie-Prozess ... 197
11.2.1 Risiko-Management und IT-Strategie im Strategie-Prozess ... 198
11.2.2 Periodisches Risiko-Reporting ... 201
11.3 Zusammenfassung ... 201
11.4 Kontrollfragen und Aufgaben ... 202
12 Geschäftskontinuitäts-Planung und IT-Notfallplanung ... 205
12.1 Einzelpläne zur Unterstützung der Geschäft-Kontinuität ... 206
12.1.1 Geschäftskontiuitäts-Plan (Business Continuity Plan) ... 206
12.1.2 Geschäftswiedererlangungs-Plan (Business Recovery Plan) ... 207
12.1.3 Betriebskontinuitäts-Plan (Continuity of Operations Plan) ... 207
12.1.4 Notfall-Plan (Disaster Recovery Plan) ... 207
12.1.5 IT-Notfall-Plan (IT Contingency Plan) ... 208
12.1.6 Vulnerability- und Incident Response Plan ... 208
12.2 Geschäftskontinuitäts-Planung ... 209
12.2.1 Start Geschäftskontinuitäts-Plan ... 210
12.2.2 Bedrohungs- und Verletzlichkeits-Analyse ... 211
12.2.3 Geschäfts-Impact-Analyse ... 211
12.2.4 Problemerfassung und Lagebeurteilung ... 212
12.2.5 Kriterien für Plan-Aktivierungen ... 213
12.2.6 Ressourcen und externe Abhängigkeiten ... 215
12.2.7 Zusammenstellung Kontinuitäts-Plan ... 215
12.2.8 Kommunikationskonzept ... 217
12.2.9 Tests, Übungen und Plan-Unterhalt ... 218
12.3 IT-Notfall-Plan, Vulnerability- und Incident-Management ... 220
12.3.1 Organisation eines Vulnerability- und Incident-Managements ... 222

12.3.2 Behandlung von plötzlichen Ereignissen als RM-Prozess 225
12.4 Zusammenfassung 226
12.5 Kontrollfragen und Aufgaben 228
13 Risiko-Management im Lifecycle von Informationen und Systemen 229
13.1 Schutz von Informationen im Lifecycle 229
13.1.1 Einstufung der Informations-Risiken 229
13.1.2 Massnahmen für die einzelnen Schutzphasen 230
13.2 Risiko-Management im Lifecycle von IT-Systemen 231
13.3 Synchronisation RM mit System Lifecycle 233
13.4 Zusammenfassung 235
13.5 Kontrollfragen und Aufgaben 236
14 Sourcing-Prozesse 239
14.1 IT-Risiko-Management im Outsourcing-Vertrag 240
14.1.1 Sicherheitskonzept im Outsourcing-Lifecycle 242
14.1.2 Sicherheitskonzept im Insourcing-Lifecycle 245
14.2 Zusammenfassung 247
14.3 Kontrollfragen 248
Anhang 249
A.1 Beispiele von Risiko-Arten 251
A.2 Muster Ausführungsbestimmung für Informationsschutz 255
A.3 Formulare zur Einschätzung von IT-Risiken 259
Literatur 263
Abkürzungsverzeichnis 267
Stichwortverzeichnis 269

1 Einführung

„Erstens kommt es anders und zweitens als man denkt". Dieses allseits bekannte Prinzip wird im vorliegenden Buch nicht widerlegt. Doch warum beschäftigen wir uns denn überhaupt mit Risiken? Diese Frage und wie wir uns mit den Risiken allgemein und mit den IT-Risiken im Besonderen auseinandersetzen können, sollte spätestens nach dem Lesen dieses Buches beantwortet werden können.

1.1 Warum beschäftigen wir uns mit Risiken?

Unsere tagtäglichen Erfahrungen zeigen an einfachen Beispielen, dass wir mit geeigneten Vorkehrungen und Massnahmen das Auftreten von negativen Ereignissen oder auch die Konsequenzen solcher Ereignisse vermindern können. Wem es je passiert ist, dass kurz vor der Fertigstellung einer umfangreichen Schreibarbeit am PC die Informationen unwiederbringlich gelöscht waren, wird die Nützlichkeit einer regelmässigen Informationensicherung auf ein anderes Speicher-Medium kaum in Frage stellen.

Häufigkeiten reduzieren oder negative Konsequenzen mildern

Negative Ereignisse (z.B. Unfälle) können mit noch so weiser Voraussicht und entsprechenden Massnahmen nie gänzlich vermieden werden. Doch können mit entsprechenden Vorkehrungen die Häufigkeiten der Ereignisse reduziert oder ihre negativen Konsequenzen gemildert werden.

Die am 26.12.2004 in den Küstenregionen des indischen Ozeans stattgefundene schwere Tsunami-Katastrophe hat eindrücklich gezeigt, dass ein Frühwarnsystem und entsprechende bauliche Massnahmen die Katastrophe zwar nicht hätten verhindern, aber das Ausmass der Katastrophe wesentlich reduzieren können.

Andere Beispiele sind die Fussgänger-Unterführungen, mit denen Unfälle mit Fussgängern im Strassenverkehr reduziert werden können; die Sicherheitsgurte im Auto, die gemäss der Statistiken zu deutlich weniger schweren Unfällen beitragen.

Auch denken wir sofort an mögliche Unterlassungen, wenn wir, wie am am 8. Februar 2005 lesen: „Zwei Tage lang standen beim

Migros-Genossenschaftsbund alle PCs still. Viele Mitarbeiter gingen wegen der fatalen Computerpanne nach Hause."

Ähnliches, aber in umgekehrter Richtung, gilt für die positiven Ereignisse, die wir selbstverständlich herbeiwünschen und für die wir uns einen möglichst positiven Effekt erhoffen. Solche ungewissen positiven Ereignisse bezeichnen wir als Chancen.

Für solche Ereignisse ergreifen wir Massnahmen, um den positiven Effekt mit grösstmöglicher Wahrscheinlichkeit oder mit möglichst günstigen Ergebnissen herbeizuführen. So sollen beispielsweise die Fernsehwerbung für ein Kosmetikprodukt dafür sorgen, dass das Produkt möglichst häufig gekauft wird. Oder ein Softwareprodukt wird so angeboten, dass es zum Einen möglichst häufig gekauft wird und zum Anderen einen möglichst hohen Preis erzielt.

Risiken und Chancen

Sowohl für die Risiken als auch die Chancen gibt es Massnahmen, die das gewünschte Resultat besser oder schlechter herbeiführen können. Ein zentraler Aspekt des Umgangs mit Risiken und Chancen ist, unter den massgeblichen Bedingungen die optimal geeigneten Massnahmen herauszufinden und zu realisieren.

„Risiko-Management" mit systemischen Modellen

Die eben skizzierte Beschäftigung mit Risiken ist grob vereinfacht das, was wir unter „Risiko-Management" verstehen. Um mit allen und zum Teil hoch abstrakten Aspekten zu den gewünschten optimalen Ergebnissen zu kommen, braucht es ein grosses Mass an Systematik. Gerade wenn es um hohe Risiken und hohe Massnahmenkosten geht, die den Unternehmen durch die Informations-Technologie entstehen, ist es wichtig, diese ganzheitlich, systematisch und transparent zu behandeln.

Die dafür in diesem Buch verwendeten Modelle sind als „systemische" Modelle zu verstehen: Dabei kann eine Risiko-Ursache verschiedene Auswirkungen und eine Auswirkung verschiedene Ursachen haben. Dementsprechend müssen die Problemlösungsprozesse des Risiko-Managements mit Rückkopplungen, Wiederholungen und Iterationen die Wirklichkeit möglichst gut modellieren können ([Ulri91], 114). Somit findet auch der Titel dieses Buches „IT-Risiko-Management mit System" seine Erklärung.

1.2 Risiken bei unternehmerischen Tätigkeiten

Risiken und Chancen sind in jedem Unternehmen - wenn auch nicht immer offensichtlich - vorhanden. Es gilt der Grundsatz,

dass mit der Ausnützung von Chancen auch immer Risiken eingegangen werden müssen. Dabei ist es eine normale menschliche Eigenschaft, die Risiken aus dem Bewusstsein zu verdrängen. Dennoch ist der sorgfältige Umgang mit Risiken gleichermassen wie das Wahrnehmen von Chancen eine der wichtigsten unternehmerischen Verantwortlichkeiten und muss in der Unternehmens-Politik, in der Unternehmens-Strategie sowie in allen unternehmerischen Operationen gepflegt werden. Ist es doch das Wohl des Unternehmens und gar sein Überleben, das vom richtigen Umgang mit den Risiken abhängig ist.

Leidtragende

Die Leidtragenden der Risiken sind auch nicht alleine die Eigentümer des Unternehmens, sondern alle an einem Unternehmen beteiligten Kreise, die sog. Anspruchsgruppen (Stakeholders), wie Beschäftigte, Kapitalgeber, Verbände, , Gesellschaft, Partner, Lieferanten, Behörden, Kommunen und der Staat.

1.3 Inhalt und Aufbau dieses Buchs

Die unterschiedlichen Risiken in einem Unternehmen sind in ihrer Art und Entstehung stark voneinander abhängig und tragen letztendlich zum Erfolg oder Misserfolg eines Unternehmens in entscheidendem Masse bei. Deshalb muss die Steuerung der Risiken bereits auf der Ebene der Unternehmensleitung erfolgen. Das Buch behandelt zwar im Speziellen die IT-Risiken, dennoch müssen die Bedrohungen, Massnahmen und Prozesse zum Management der IT-Risiken in einem ganzheitlichen Zusammenhang zur Unternehmenssicht und dessen Zielen, Anforderungen und Management-Prozessen gesehen werden. Demzufolge wird vor der detallierten Behandlung der IT-Risiken im Teil C des Buches der dazu notwendige Vorspann in den Teilen A und B behandelt.

Teil A: Grundlagen erarbeiten

Somit werden in **Teil A** des Buches die für ein ganzheitliches Risiko-Management in einem Unternehmen allgemeinen Grundlagen und Instrumente aufgezeigt.

Teil B: Anforderungen berücksichtigen

Im Teil B werden die an das Unternehmen gestellten heute aktuellen Anforderungen an ein Risiko-Management und die Voraussetzungen und Prozesse für die in die Management-Prozesse des Unternehmens integrierten Risiko-Aspekte beleuchtet. Die dazu zusammengestellten Konzepte, Methoden und Instrumente haben zum Ziel, ein möglichst effektives Risikomanagement mit vertretbarem Aufwand aufzubauen und zu betreiben.

Teil C: IT-Risiken erkennen und bewältigen

Im Teil C werden die IT-Risiken detailliert behandelt und entsprechende Methoden und Verfahren speziell zum Management der IT-Risiken beschrieben.

Teil D: Unternehmensprozesse meistern

Im Teil D wird sodann gezeigt, wie sich die verschiedenen Risiken, darunter die operationellen Risiken der Informations-Technologie, in einen gesamten Risiko-Management-Prozess des Unternehmens einfügen lassen und wie unternehmenswichtige Risiko-Management-Prozesse wie Geschäftskontinuitäts-Planung im Risiko-Management-Prozess verankert werden können.

Teil A

Grundlagen erarbeiten

2 Elemente für die Durchführung eines Risiko-Managements

Akzeptable Retsrisiken

Die Beschäftigung mit den Risiken dient ihrer Erkennung und Bewertung sowie der Erarbeitung von Massnahmen und deren Umsetzung. Durch die Massnahmen sollen die Risiken auf akzeptable „Restrisiken" reduziert werden.

Risiko-Management

Auf der Basis von Art, Quantität und Qualität der Risiken sowie einiger weiterer Kriterien sollen möglichst optimale Massnahmen-Lösungen gefunden werden. Diese Beschäftigung mit Risiken wird als „Risiko-Management" bezeichnet (Abbildung 2.1).

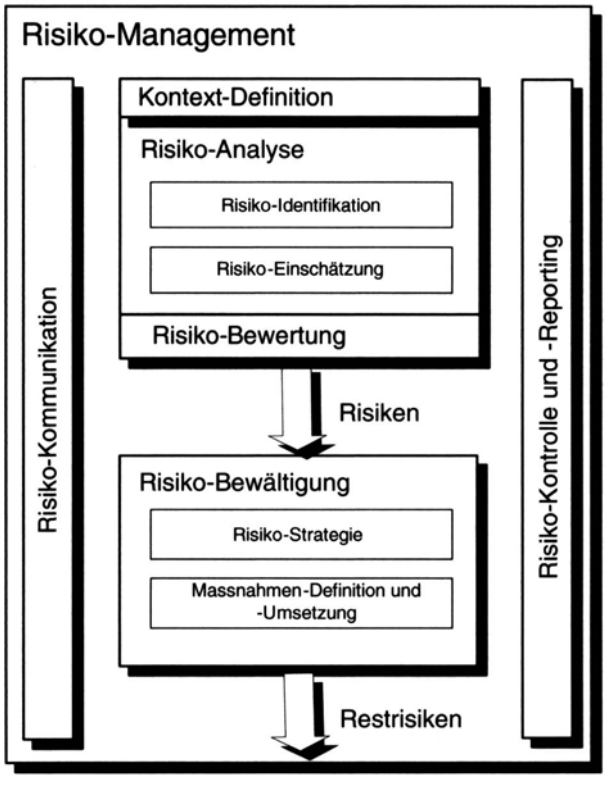

Abbildung 2.1: Aktivitäten für das Risiko-Management

Risiko-Management wird in den verschiedensten Disziplinen wie Wirtschaft, Informationstechnologie, Soziologie, Natur und Technik benötigt. Die Anwendung des Risiko-Managements hat einen hohen interdisziplinären Stellenwert, können doch die „IT-Risiken" grosse andere Risiken im wirtschaftlichen Sektor, im Gesundheitswesen, im Kommunikations-, Energie-, Verkehrs- und Transportwesen nach sich ziehen. Alle diese Disziplinen haben bezüglich der Risiken starke Vernetzungen untereinander.

Terminologie

Die Terminologie bezüglich „Risiko-Management" ist demzufolge vielfältig und teilweise uneinheitlich. Auf diesem Hintergrund sind die jüngsten Standardisierungen einer Terminologie in der [Isor02] und eines „Frameworks" für Risiko-Mmanagement des Standardisierungs-Gremiums Australia/New Zealand" [Asnz04] als sehr nützlich anzusehen.

2.1 Fokus und Kontext Risiko-Management

Fokussierung auf Betroffene

Die aus dem Risiko-Management resultierenden Massnahmen bezwecken, die Gefahrensituationen oder die Folgen von Schadensereignissen für die „Betroffenen" zu beseitigen oder zu vermindern.

Je nachdem wie die Aufgabenstellung für das durchzuführende Risiko-Management lautet, können die Betroffenen, Einzelpersonen, Gruppen von Personen oder auch, wie in diesem Buch, Unternehmen sein. Die Risiken, die wir im Rahmen dieses Buchs betrachten, fallen bei einzelnen Produkten oder Dienstleistungen, bei einzelnen Organisationseinheiten oder auf der Ebene des Gesamtunternehmens an.

Neben der Fokussierung auf die Betroffenen ist die Bezeichnung und Abgrenzung der Gegenstände für die möglichen Schadensereignisse nötig. Auch das Umfeld der betrachteten Gegenstände bedarf der Definition und Abgrenzung. Diese Definitionen und Abgrenzungen sind aus den Blickwinkeln der Gefahrensituationen, der am Analyse- und Bewältigungsprozess beteiligten Stellen und der massgeblichen funktionalen Zusammenhängen notwendig.

Massgeblicher Kontext

Bereits beim Beginn einer Risiko-Management-Aufgabe ist die Fokussierung und Bestimmung des massgeblichen Kontextes unabdingbare Voraussetzung.

2.2 Definition des Begriffs „Risiko“

Der Begriff „Risiko“ wird je nach Anwendungsgebiet unterschiedlich definiert*. Für betriebswirtschaftliche Fragestellungen, wie sie in diesem Buch vorkommen, werden Verluste oder Schäden als die negativen Folgen von „**Zielabweichungen**“ eines vorgängig definierten Ziels verstanden. Damit ergibt sich folgende Risiko-Definition [Brüh01]:

Betriebswirtschaftliche Risiko-Definition

> Ein Risiko ist eine nach Häufigkeit (Eintrittserwartung) und Auswirkung bewertete Bedrohung eines zielorientierten Systems. Das Risiko betrachtet dabei stets die negative, unerwünschte und ungeplante Abweichung von Systemzielen und deren Folgen.

Risiko / Chance

Dem Risiko steht meist eine Chance gegenüber, welche ein positives Ergebnis in Aussicht stellt. (Risiken und dazugehörige Chancen lassen sich jedoch oft nicht im selben Koordinaten-System behandeln, was das Abwägen der Chancen mit den Risiken entsprechend schwierig gestaltet.)

Folgen der Ziel-Abweichungen

Wird diese Risiko-Definition auf Projektrisiken angewendet, dann sind hauptsächlich die Folgen der Ziel-Abweichungen bezüglich „Dauer“, „Budget“ und „Qualität“ zu betrachten.

Wenden wir die oben angegebene Definition auf IT-Risiken an, dann ergeben sich die Risiken als Konsequenzen der Abweichungen von den System-Zielen, „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“ der Informationen und/oder der IT-Systeme.

Unerwünschte Zielabweichungen

Solche „unerwünschten Ziel-Abweichungen“ können eintreten, wenn entsprechende Bedrohungen vorhanden sind. So kann die Bedrohung „Krankheit Mitarbeiter“ eine negative Abweichung vom Ziel: „Fertigstellungs-Termin“ eines Projekts bewirken.

Bedrohungen

Eine Bedrohung wirkt sich umso häufiger und stärker aus, als geeignete Massnahmen fehlen. Eine geeignete Massnahme im gerade gegebenen Beispiel wäre, den krank gewordenen Mitarbeiter kurzfristig durch eine andere gleichermassen geeignete

---

* Der ISO/IEC Guide 73:2002 definiert rudimentär: „Risiko ist die Kombination der Wahrscheinlichkeit eines Ereignisses und seiner Konsequenzen“.

Person ersetzen zu können. Ist eine solche Massnahme nicht vorhanden, sprechen wir von einer Schwäche, Verletzlichkeit oder Schwachstelle des Systems.

Schwäche / Schwachstelle / Verletzlichkeit

Aus den Bedrohungen und den Schwächen des Systems ergibt sich die Wahrscheinlichkeit, mit der eine Abweichung vom gesetzten Ziel mit bestimmten negativen Folgen eintritt.

Wahrscheinlichkeit von möglichen Folgen

Die Folgen (Konsequenzen) einer Abweichung vom Ziel bezeichnen wir als Schaden (auch Tragweite, Verlust oder Impact).

Schäden sind Folgen einer Ziel-Abweichung

Die Abweichung von einem geplanten Projekttermin kann finanzielle Einbussen zur Folge haben und/oder das Ansehen der Firma auf dem Markt beeinträchtigen (Reputations-Schaden). Die Folgen einer Ziel-Abweichung können ein konstantes oder ein mit der Zeit veränderliches Ausmass haben. (Die Folgen mit zeitlich anwachsendem Ausmass, z.B. Brandschäden, bedürfen einer besonderen Risikobewältigung.)

Keine Möglichkeiten von Zielabweichungen = „sicher"

Bestehen hingegen keine Möglichkeiten von Ziel-Abweichungen, so erhalten wir definitionsgemäss auch keinen Schaden, wir sind also „sicher".

Bei bestimmten System-Zielen (z.B. Fertigstellungstermin in einem Projekt) kann eine Zielwabweichung durchaus auch positive Folgen aufweisen. In diesem Falle haben wir es mit einer Chance zu tun. Bei den Massnahmenentscheidungen zur Bewältigung eines Risikos sind die möglichen Chancen ebenfalls in geeigneter Weise zu berücksichtigen.*

Wir verwenden deshalb für diese Art von Zielen den Begriff „System-Ziel". Ein solches System-Ziel ist wiederum nicht zu verwechseln mit einem „Risiko-Ziel", bei dem es um eine Zielvorgabe geht, eine bestimmte Risikogrösse nicht zu überschreiten.

Beispiele:

- Es besteht das Ziel, den Einführungstermin des Produktionssystems „FabriStock" am 1. November 2005 in Betrieb nehmen zu können. Das Ziel heisst somit „Einhaltung des Einführungstermins". Hingegen könnte ein mögliches Risiko-Ziel heissen: Die Kostenfolge durch ei-

* Die Analyse von Chancen und die Massnahmen zur deren Realisierung werden im Rahmen dieses Buches über IT-Risiko-Management nicht speziell behandelt.

ne Terminabweichung, gewichtet mit der Wahrscheinlichkeit ihres Auftretens (=Risiko), darf nicht mehr als 20' 000 € betragen. Bei einem Risiko von 10' 000 € ist das Risiko-Ziel noch bestens eingehalten. Wir sind sozusagen noch im „grünen Bereich“. Das Beispiel zeigt, dass erst mit der Einführung eines „Risiko-Ziels“ die Nichteinhaltung eines System-Ziels relativiert werden kann. Wir sehen später, dass wir diese Relativierung mit der Aufgabe „Risiko-Bewertung“ (risk evaluation) durchführen.

Beim Autofahren haben wir das System-Ziel, uns bei einem Unfallereignis körperlich nicht zu verletzen. Mit einigen Sicherheitsmassnahmen (z.B. Sicherheitsgurte, Knautschzone) kann erreicht werden, dass der Verletzungsgrad und die daraus resultierenden Kosten mit einer bestimmten Wahrscheinlichkeit ein vorgegebenes Mass nicht überschreitet. Ein solches Risiko-Ziel kann demnach eine entscheidende Grösse für die Festlegung der Prämien für die Unfall- und Haftpflicht-Versicherung sein.

Die oben angeführte verbale Definition des Risikos liefert jedoch noch keine „messbaren“ Ergebnisse. Messbare Ergebnisse sind aber für die Massnahmen-Entscheide oder die Vergleichbarkeit mit anderen Risiken wichtig.

Risiko-Formel

Eine solche „Messbarkeit“ des Risikos in der Messeinheit des Schadens, z.B. Schweizer Franken, kann mit der folgenden Risiko-Formel erreicht werden:

$$\mathbf{R = p_E * S_E}$$

R: Risiko; p_E: Wahrscheinlichkeit, dass ein Schadensereignis mit dem Schaden S_E eintritt; S_E: Ausmass des Schadensereignisses (auch Tragweite oder Verlust).

Anm.: Im praktischen Umgang mit dieser Formel wird meist anstelle der Eintrittswahrscheinlichkeit p_E die Häufigkeit H_E des Schadendenseintritts eingesetzt.

2.3 Anwendung der Risiko-Formel

Diese Formel liefert bei relativ häufig auftretenden Ereignissen plausible Risikowerte. Tritt beispielsweise ein bestimmtes Ereignis zweimal so häufig ein, dann verdoppelt sich auch das Risiko.

Doch kommen sehr hohe Schäden im selben Unternehmen sicherlich nur mit sehr geringer Wahrscheinlichkeit vor. Für solche sehr hohen Schäden ist es nicht sinnvoll, das Risiko mit dieser Formel zu bestimmen, da die arithmetische Multiplikation eines sehr grossen Schadens mit einer sehr geringen Wahrscheinlichkeit ein für das Unternehmen geringes und damit „tragbares Risiko" vortäuschen würde. Ereignet sich beispielsweise innert 10 Jahren in einem von tausend Computerräumen in der Schweiz ein Brand und zieht dieser Brand einen Schaden von 10 Millionen Franken nach sich, dann würde das rechnerische Risiko pro Jahr gerade nur 1000 Franken betragen. Dieses errechnete sehr kleine Risiko könnte ein Unternehmen mit einem Jahresumsatz von 10 Millionen Franken dazu verleiten, keine Vorkehrungen gegen das Brandrisiko zu treffen. Ein verantwortungsbewusstes Management wird hingegen - ungeachtet dieser Risiko-Berechnung - den Brandrisiken im Rechenzentrum mit umfassenden Massnahmen begegnen, da bei einem tatsächlichen Brandereignis ohne Massnahmen das Unternehmen wahrscheinlich nicht überleben würde.

Sehr grosse Schadensereignisse

Dieses Beispiel zeigt, dass für sehr seltene, aber sehr grosse Schadensereignisse aus der Sicht des Unternehmens einzig der mögliche Schaden und nicht das rechnerische Risiko als Entscheidungsgrundlage herbeigezogen werden sollte. Bei der „Risiko-Bewertung" kann solchen Umständen Rechnung getragen werden.

Anwendungs-Schwierigkeiten der oben angegebenen Risikoformel können sich auch ergeben, wenn beispielsweise die geschätzte Eintrittswahrscheinlichkeit eines Schadensereignisses pro Jahr und die Schadenshöhe in einer Währungseinheit (z.B. Euro) eingesetzt werden. Die solchermassen auf einer arithmetischen Multiplikation beruhende Risiko-Berechnung täuscht einerseits ein zu genaues Ergebnis vor und trägt andererseits der aus dem obigen Beispiel ersichtlichen „Risiko-Wahrnehmung" in einem Unternehmen zu wenig Rechnung.

2.4 Subjektivität bei der Risiko-Einschätzung

Die Einschätzung der beiden Risiko-Dimensionen Wahrscheinlichkeit und Konsequenzen (Tragweite) eines Schadensereignisses erfolgt einerseits aus den Erfahrungen der Vergangenheit (Fachbegriff: ex post) und/oder aus der Prognose für zukünftige Ereignisse (Fachbegriff: ex ante). Die Einschätzung für die Zukunft sowie die Einstellung zur Tragbarkeit der Risiken hängen stark von der Subjektivität der am Risiko-Management-Prozess beteiligten Personen ab.

Rieiko-Bereitschaft / Risiko-Aversion

So neigen die einen Personen zur Risiko-Bereitschaft (risk propensity)*. Andere wiederum zur Risiko-Aversion (risk aversion)†. Auch sind einer einzelnen Person kaum alle relevanten Fakten für die Beurteilung eines Risikos bekannt. Es empfiehlt sich deshalb, in den Risiko-Management-Prozess die Möglichkeit einer breiten Abstützung unter vielen Gesichtswinkeln einzubauen, wie z.B. durch ein interdisziplinär zusammengestelltes Risiko-Analyse-Team.

2.5 Hilfsmittel zur Risiko-Einschätzung

2.5.1 Risiko-Matrix

Das Dilemma mit der Risiko-Formel können wir lösen, indem wir beispielsweise das „Produkt" einiger Häufigkeitswerte und einiger Schadenswerte (als Funktion) in einer Risikomatrix festlegen.

Risiko-Wahrnehmung

Bei der Festlegung der Produktwerte kann die Risiko-Wahrnehmung des Managements, insbesondere für grosse und seltene Schadensereignisse, berücksichtigt (vorprogrammiert) werden.

---

* Ein Entscheidungsverhalten, bei dem die jeweils riskantere Handlungsalternative im Hinblick auf Gewinnchancen bevorzugt wird, auch wenn die Erfolgsaussichten ungewiss sind oder Misslingen droht.

† Ein Entscheidungsverhalten, bei dem die jeweils weniger riskante Handlungsalternative bevorzugt wird.

Risiko-Matrix für „Wahrnehmung" und „Einschätzung" der Risiken im Unternehmen

Die solchermassen enstandende „Risiko-Matrix" werden wir sodann für die Einschätzung der Risiken im Unternehmen einsetzen. Natürlich ist es in einem grösseren Unternehmen auch möglich, mit unterschiedlichen „Risiko-Matrizen" für unterschiedliche Bereiche (z.B. für Tochtergesellschaften) zu arbeiten.

Das Beispiel einer Risiko-Matrix, ist in der nachfolgenden Abbildung 2.2 gezeigt.

Monetarisierte Risiko-Grössen					
sehr klein	klein	mittel	gross	sehr gross	katastrophal
bis 50 T. €	50 T. €	500 T. €	5 Mio. €	15 Mio. €	über 15 Mio. €

Schadenshöhe pro Fall / Häufigkeit der Fälle	E klein	D mittel	C gross	B sehr gross	A katastrophal
sehr oft (10 mal pro Jahr)	mittel	gross	sehr gross	irreal	irreal
oft (1 mal im Jahr)	klein	mittel	gross	sehr gross	irreal
selten (1 mal in 10 Jahren)	sehr klein	klein	mittel	gross	katastrophal
sehr selten (1 mal in 30 Jahren)	sehr klein	klein	klein	mittel	katastrophal
unwahrscheinlich (1 mal in mehr als 30 Jahren)	sehr klein	sehr klein	klein	mittel	katastrophal (*)

*) Für seltene Fälle mit katastrophalen Schäden wird das Risiko mit der Höhe des Schadens gleichgesetzt.

Abbildung 2.2: Ordinalskala für Risiko-Grössen und Risiko-Matrix

2.5.2 Schadenseinstufung

Kardinale und ordinale Skalen

Die direkten finanziellen Verluste werden oft mit „kardinalen" (rechenbaren) Grössen (z.B. Euro) eingeschätzt. Hingegen werden die sonstigen Schadensauswirkungen, die sich in der langen Frist ebenfalls indirekt als finanzielle Schäden auswirken, meist in „ordinalen" Grössen (z.B. klein, mittel, gross) angegeben. Um der Schadens- und Risiko-Wahrnehmung des Unternehmens gerecht zu werden, empfiehlt es sich, auch die direkten finanziellen Verluste mit Grössen einer für das Unternehmen einheitlichen Ordinalskala einzustufen.

Schadens-Metrik

Die Abbildung 2.3 zeigt, wie die Schadenseinstufungen vorgenommen werden können. Eine solche Einstufungstabelle kann für ein Unternehmen einmalig erstellt werden. Sie richtet sich nach der Grösse und der Branche des Unternehmens sowie nach den Besonderheiten seiner Risiko-Objekte und kann damit als **Schadens-Metrik** (Impact-Metrik) für das gesamte Unternehmen eingesetzt werden.

Für eine solche einheitliche Schadens-Metrik wird die Geschäftsleitung die monetäre Höhe eines für das Unternehmen „sehr hohen Schadens" festlegen (z.B. Höhe eines durchnittlichen jährlichen Betriebsgewinns über die letzten 5 Jahre). Die festgelegten monetären Werte für „direkte finanzielle Schäden" können dann als Äquivalente für die „indirekten Schäden"* herangezogen werden.

In einem grösseren Unternehmen sind u. U. für einzelne Risiko-Gebiete auch spezifische Schadens-Einstufungstabellen sinnvoll. Für ein integriertes Unternehmens-Risiko-Mangement müssen diese Einstufungstabellen jedoch untereinander abgestimmt werden.

Reduktion Wahrscheinlichkeit oder Schaden

Im Weiteren ist es für viele Massnahmen-Entscheide sinnvoll, das Risiko in beiden Dimensionen (Wahrscheinlichkeit und Schaden) darzustellen, da die einen Massnahmen eher der Reduktion der Eintrittswahrscheinlichkeit (Beispiel: Vieraugenprinzip) und die anderen eher der Schadensreduktion dienen (Beispiel: Katastrophenorganisation).

---

* Indirekte Schäden (z.B. Reputations-Schäden) wirken sich nur unmittelbar auf das finanzielle Ergebnis aus.

Impacts / Stufe	Direkter finanzieller Verlust [€] (Barwert der Ersatzkosten + Opportunitäts-Kosten)	Sonstige firmentypische Schadensauswirkungen		
		Schädigung der geschäftlichen und wirtschaftlichen Interessen Beeinträchtigung der Geschäfts- und Management-Vorgänge Verlust an Reputation und Goodwill	Nichteinhaltung gesetzlicher und regulativer Verpflichtungen (*)	Beeinträchtigung der Gesundheit, Sicherheit und des Schutzes anderer Personen
A **katastrophal**	über 15 Mio. € (z.B. Verlust einer wichtigen Lizenz, so dass Geschäftstätigkeit aufgegeben werden muss)	z.B. Grossabnehmer künden Verträge aufgrund bekannt gewordener negativer Produkteigenschaften (z.B. krebserregendes Nahrungsmittel)	-	Systematische Schädigung von Leib und Leben anderer Personen
B **sehr gross**	5-15 Mio. € (z.B. aufgrund lang anhaltender Produktions-Ausfälle)	z.B. Einige Abnehmer stellen auf Alternativprodukte um, infolge preisgegebener Produktionsgeheimnisse oder irreparabler Imageschäden	Strafe infolge Verstoss gegen Kartellrecht	Schädigung von Leib und Leben anderer Personen im Einzelfall
C **gross**	0.5-5 Mio. € (z.B. aufgrund Zerstörung von Produktionsmaschinen und entsprechende Produktionsausfälle)	z.B. Abnehmer drücken Preis aufgrund von durchgesickerten Geschäftsgeheimnissen	Sanktionen wegen grober Sorgfaltspflichtverletzung	Klage und Schadensersatz wegen Verletzung des Geschäftsgeheimisses der Abnehmer
D **mittel**	50-500 T. € (z.B. aufgrund Schadensersatzforderungen bei falschen Lieferungen)	z.B. Erhöhte Werbeaktionen nötig, infolge Imageschäden	Verfahren wegen Mängel in der ordnungsgemässen Geschäftsführung	Klagen wegen indiskreter Behandlung von Personaldaten in grösserem Umfang
E **klein**	bis 50 T. € (z.B. aufgrund kleinerer Störungen und daraus entstandenen Ausschussteilen)	-	-	Schadensersatz wegen vereinzelter Verletzung des Datenschutzes

* z.T. persönliche Haftung verantwortlicher leitender Personen

Abbildung 2.3: Beispiel Schadens-Metrik in einem Unternehmen