Hans-Peter Königs

IT-Risiko-Management mit System

Von den Grundlagen bis zur Realisierung –
Ein praxisorientierter Leitfaden

3. Auflage

PRAXIS

VIEWEG+
TEUBNER

<kes>

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 Secu-Media 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.

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

Der IT Security Manager
Von Heinrich Kersten und Gerhard Klett

ITIL Security Management realisieren
Von Jochen Brunnstein

IT-Sicherheit kompakt und verständlich
Von Bernhard C. Witt

Praxis des IT-Rechts
Von Horst Speichert

IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz
Von Heinrich Kersten, Jürgen Reuter und Klaus-Werner Schröder

Datenschutz kompakt und verständlich
Von Bernhard C. Witt

Profikurs Sicherheit von Web-Servern
Von Volker Hockmann und Heinz-Dieter Knöll

www.viewegteubner.de

Hans-Peter Königs

IT-Risiko-Management mit System

Von den Grundlagen bis zur Realisierung –
Ein praxisorientierter Leitfaden

3., überarbeitete und erweiterte Auflage

Mit 88 Abbildungen

PRAXIS

VIEWEG+
TEUBNER

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der
Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über
<http://dnb.d-nb.de> abrufbar.

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.

1. Auflage 2005
2. Auflage 2006
3., überarbeitete und erweiterte Auflage 2009

Lektorat: Sybille Thelen | Christel Roß

Vieweg+Teubner ist Teil der Fachverlagsgruppe Springer Science+Business Media.
www.viewegteubner.de

Umschlaggestaltung: KünkelLopka Medienentwicklung, Heidelberg
Druck und buchbinderische Verarbeitung: MercedesDruck, Berlin
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.
Printed in Germany

ISBN 978-3-8348-0359-7

Vorwort zur 1. und 2. Auflage

Bei den Risiken von Unternehmen nehmen die „operationellen Risiken“ eine immer bedeutendere Rolle ein. Nicht von ungefähr verlangen neuere Regulative und Gesetze, wie beispielsweise Basel II, ein funktionstüchtiges Management und Reporting der operationellen Risiken. Die „IT-Risiken“ sind eine wichtige Kategorie der operationellen Risiken, vor allem deshalb, weil die meisten Unternehmen immer stärker von der Informationstechnologie abhängig sind (z.B. Spitäler, Banken, Bahn, Presse).

Die Anforderungen an die „Corporate Governance“ des Unternehmens legen den obersten Aufsichts- und Führungsgremien funktionstüchtige Prozesse für ein integriertes Risiko-Management aller Risiken nahe (z.B. Markt-, Kredit- und operationelle Risiken). Dabei ist das IT-Risiko-Management ein Baustein im Gesamt-Risiko-Management-Prozess eines Unternehmens. 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. Deshalb wird in diesem Buch der gesamte Risiko-Management-Prozess eines Unternehmens aufgezeigt, in den sich das IT-Risiko-Management mit entsprechenden Methoden und Werkzeugen einfügt.

Die Verantwortlichen der Informations-Technologie (IT) eines Unternehmens müssen die einzuschlagenden Sicherheitsmassnahmen vermehrt an den mit der Informationstechnologie einhergehenden Risiken orientieren, da allfällige Schäden nicht nur stark zu Buche schlagen, sondern sogar den Bestand eines Unternehmens gefährden können. Andererseits nehmen die Kosten für die Sicherheit einen beträchtlichen Teil des IT-Budgets ein. Zur Rechtfertigung dieser Kosten müssen die Risiken in überzeugender Weise gezeigt und den Kosten gegenüber gestellt werden können. Für unnötigen Überschutz ist in der Regel kein Budget vorhanden.

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

Diese Beweggründe haben sich seit der 1. Auflage dieses Buches vor eineinhalb Jahren nicht verändert. Wohl haben sich hinsichtlich der Standardisierung einige Ergänzungen und Korrekturen aufgedrängt. So wurden beispielsweise die Standards ISO/IEC 17799 und ISO/IEC 27001 sowie das BSI-Grundschutzhandbuch in neuen Fassungen mit stärkerem Bezug zum „Risiko-Management" herausgegeben. Auch konnte ich von Lesern und Rezensenten wertvolle Anregungen gewinnen, die ich in die 2. Auflage eingebracht habe.

Dank

Der Telekurs Group für die Unterstützung des Buches. Ulrich Moser für die nützlichen Diskussionen und das Gegenlesen. Emmerich Fuchs, mit dem ich eine Lehrveranstaltung an der Hochschule für Wirtschaft in Luzern durchführte, für das Gegenlesen und für die spontanen Hinweise aus seiner Berater- und Schulungstätigkeit.

Meiner Frau, Diemuth Königs, Autorin historischer Bücher und Fachartikel, danke ich für so Vieles, dass ich es hier nicht aufzuzählen vermag. Trotz ihres Zeitdrucks mit eigenen Büchern und Artikeln war sie stets bereit, mir in schriftstellerischen und auch sonstigen Angelegenheiten zu helfen. Ihr gilt mein ganz besonderer Dank.

Zürich, im September 2006 Hans-Peter Königs

Vorwort zur 3. Auflage

Das IT-Risiko-Management hat sich seit der Veröffentlichung der ersten und zweiten Auflage rasant weiter entwickelt. Diese Entwicklung ist einerseits durch die konkret gewordenen Anforderungen an die Unternehmen aufgrund der gesetzlichen und regulativen Vorgaben und andererseits durch die Verfügbarkeit von Standards, Rahmen- und Regelwerken bedingt. Als Beispiele solcher Rahmen- und Regelwerke sind die ISO/IEC-Standards der 2700x-Reihe, die britischen „Business Continuity Management“ - Standards BS 25999-x, die deutschen BSI-Standards 100-x oder die österreichischen Standards der Reihe ONR 4900x zu nennen, die sich bestimmten Aspekten des Risiko-Managements widmen.

Die Thematisierung des IT-Risiko-Managements und ganz allgemein des Risiko-Managements im Rahmen der Corporate Governance hat gerade in jüngster Zeit zur Steigerung des Bewusstseins um die Risiken aus Unternehmenssicht beigetragen.

Wenn auch in der derzeitigen Finanz- und Wirtschaftskrise die operationellen IT-Risiken nicht im Blickpunkt stehen, wird doch gerade jetzt sichtbar, wie die Wirtschafts- und Finanzsysteme global vernetzt und von den Informationen und Informationstechnologien abhängig sind.

Das Ziel, den derzeitigen Stand des Informations- und IT-Risiko-Managements in der für den Anwender in der Praxis notwendigen Übersicht und Ausführlichkeit zu behandeln, hat sich als grosse Herausforderung erwiesen. Um den Fokus eines „Leitfadens“ beizubehalten, wurden die aufwändigen quantitativen Analyse-Methoden, welche hohe Anforderungen an das statistische Datenmaterial und an ihre praktische Umsetzung stellen, mit den entsprechenden Hinweisen lediglich übersichtsmässig behandelt.

Das in der Praxis immer wichtiger werdende und aus der Perspektive des Riskomanagement kontrovers diskutierte Thema der Kosten-/Nutzen-Analysen wird in einem eigenen Kapitel behandelt. Vertieft behandelt werden die Themen der „Compliance“ und der für die IT und die Informations-Sicherheit wichtigen Geschäftskontinuität und des Notfallmanagements.

Auch wurde das Buch den gewachsenen Anforderungen der Ausbildungsgänge zum „Master of Advanced Studies in Information Security“ an der Hochschule Luzern angepasst, wo ich neben meiner Beratertätigkeit als Dozierender für Risiko-Management tätig bin.

Der Aufbau des Buches in der Reihenfolge

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

wurde auch in dieser dritten Auflage beibehalten, da es bei den heute vielfältigen Anforderungen und Standards vor allem um die richtige Positionierung des Risiko-Managements im Unternehmen geht.

Am Ende eines jeden Kapitels finden sich eine Zusammenfassung sowie einige Kontrollfragen und Aufgaben. Die Musterlösungen für die Kontrollfragen und Aufgaben können über den Online-Service im Internet abgerufen werden. Die URL dafür ist:

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

Fragen, fachliche Hinweise oder gar einen über den Online-Service möglichen Dialog sind mir herzlich willkommen.

Dank

Für die vielen Diskussionen sowie die Durchsicht und wertvollen Ratschläge zu den Erweiterungen in der dritten Auflage danke ich meinem langjährigen Berufskollegen Domenico Salvati. Mein Dank gilt auch dem Lektorat des Vieweg+Teubner-Verlags für seine Unterstützung und wertvollen Hinweise.

Nicht zuletzt geht mein besonderer Dank an meine Frau Diemuth Königs, Autorin historischer Bücher, die mir in allen Belangen mit Rat und Tat zur Seite steht.

Olsberg im Mai 2009 Hans-Peter Königs

Inhaltsverzeichnis

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 im Allgemeinen 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 15. Januar 2009 lesen: „Die elektronischen Fahrpläne und das Buchungssystem der Deutschen Bahn waren in ganz Deutschland stundenlang ausgefallen. Der Computerausfall hatte

am Mittwoch bundesweit zu Verspätungen im Bahnverkehr geführt."

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 soll 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.

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.

„Risiko-Management" mit systemischen Modellen

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. Um die meist „komplexe" Wirklichkeit möglichst gut zu modellieren, enthalten daher die Problemlösungs-Prozesse des Risiko-Managements entsprechende Rückkopplungen und Iterationen ([Ulri91], S. 114). Mit diesem systemischen Ansatz 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 dem Ergreifen 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 Handlungen 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, Partner, Lieferanten, Behörden, Kommunen und der Staat. So haben die in den letzten Jahren aufgetretenen Schadensereignisse bewirkt, dass das Risiko-Management in den meisten Industriestaaten zu einer vom Gesetzgeber verordneten „Muss-Disziplin" der Unternehmensführung geworden ist.

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 und Überwachung der Risiken bereits auf der obersten Ebene der Unternehmensführung erfolgen. Das Buch behandelt zwar speziell 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 detaillierten 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 Risiko-Management mit vertretbarem Aufwand aufzubauen und zu betreiben.

Teil C: IT-Risiken erkennen und bewältigen

Im Teil C werden die Risiken der Informationen und der Informationstechnologie detailliert behandelt und entsprechende Methoden und Verfahren speziell zum Management der Informations-Sicherheit- und IT-Risiken beschrieben. Der gebräuchliche aber unscharfe Begriff der „IT-Risiken" schliesst dabei die Informations-Sicherheits-Risiken wie die Risiken im Zusammenhang mit der Leistungserbringung der Informatik ein.

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 die 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 vor allem 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. Die in Abbildung 2.1 gezeigten Aktivitäten werden, wie in den weiteren Ausführungen dieses Buches gezeigt wird, in prozessorientierter Weise durchgeführt.

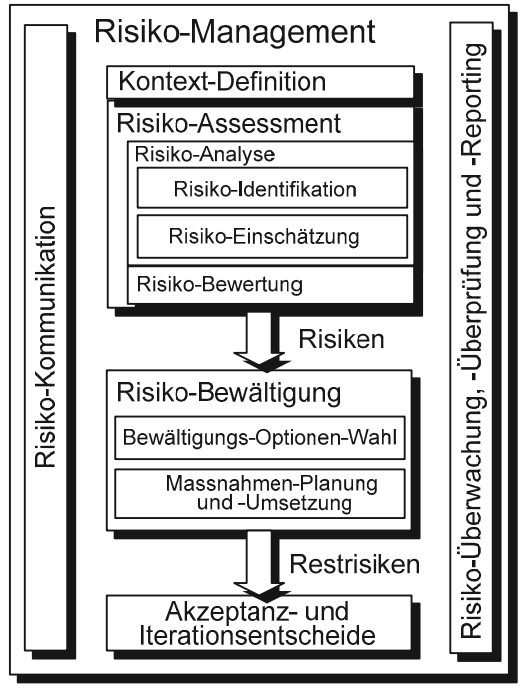

Abbildung 2.1: Aktivitäten für das Risiko-Management

Das „Risiko-Management“ wird in den verschiedensten Disziplinen wie Wirtschaft, Informationstechnologie, Soziologie und Technik benötigt.

Interdisziplinäre Vernetzung der Risiken

Die Anwendung des Risiko-Managements hat einen hohen interdisziplinären Stellenwert, können doch beispielsweise die „IT-Risiken“ grosse andere Risiken in der Volkswirtschaft, im Gesundheitswesen, im Kommunikations-, Energie-, Verkehrs- und Transportwesen nach sich ziehen. Alle diese Disziplinen haben bezüglich der Risiken starke Vernetzungen untereinander.

Terminologie und Standards

Die im Zusammenhang mit „Risiko-Management“ in den einzelnen Disziplinen verwendete Terminologie ist vielfältig und teilweise auch uneinheitlich. Auf diesem Hintergrund sind die Standardisierungen einer Terminologie in der ISO [Isog02] sowie eines „Frameworks“ für Risiko-Management durch das Standardisierungs-Gremium Australia/New Zealand“ [Asnz04] oder durch das US-amerikanische „Committee of Sponsoring Organisation of the Treadway Commission“ [Cose04] als sehr nützlich anzusehen. Doch weisen diese Standards wie auch die neueren Standards ISO/FDIS 31000 [Isor09] und ISO/IEC 27005:2008 Unterschiede auf, die wahrscheinlich, aufgrund der Anforderungen für einen bestimmten Kontext, nie vollständig harmonisiert werden können. Die erwähnten Standards über Risiko-Management haben somit meist auch lediglich Empfehlungscharakter, was in den Standard-Klauseln mit dem englischen Hilfsverb „should“ zum Ausdruck gebracht wird.

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 System-Zielen 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.) Bei den in diesem Buch angeprochenen IT-Risiken, die in die Kategorie der „operationel-

---

* Der Begriff „Gegenstand“ wird in diesem Buch synonym zu „Objekt“ sowohl für greifbare als auch für abstrakte Güter, Objekte und Strukturen verwendet und schliesst den in der englischsprachigen Standardisierung oft verwendeten Begriff „Asset“ ein.

† Der ISO/IEC Guide 73:2002 [Isog02] definiert rudimentär: „Risiko ist die Kombination der Wahrscheinlichkeit eines Ereignisses und seiner Konsequenz“.

len Risiken“ gehören, besteht keine direkte Verknüpfung mit einer für die Chancen massgeblichen Ertragsquelle.

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 Informations- und IT-Gegenstände an, dann resultieren die Sicherheits-Risiken aus Abweichungen von den System-Zielen, „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“.

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

Schwäche / Schwachstelle / Verletzlichkeit

Wahrscheinlichkeit von möglichen Folgen

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

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

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 entweder ein zeitunabhängiges oder ein mit der Zeit veränderliches Ausmass aufweisen. (So bedürfen die Ereignisse mit zeitlich anwachsendem Ausmass, z.B. Brandschäden, auch einer entsprechenden Risikobewältigung.)

---

* Die bewertete Auswirkung eines Ereignisses wird auch als „Impact“ bezeichnet. Die gesamthaften Konsequenzen können aus mehreren Impacts resultieren. Die negativen Konsequenzen eines Ereignisses bezeichnen wir in diesem Buch als Schaden oder Verlust.

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 Zielabweichung 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.*

„System-Ziel“/ „Sicherheits-Ziel“

Wir verwenden deshalb für diese Art von Zielen den Begriff „System-Ziel“. In der Informations-Sicherheit wird statt System-Ziel oft auch der Begriff „Sicherheits-Ziel“ verwendet. Ein System-Ziel ist wiederum nicht zu verwechseln mit einem „Risiko-Ziel“, bei dem es um eine Vorgabe geht, eine bestimmte Risikogrösse nicht zu überschreiten. Risiko-Ziele werden oft auch in der Form von akzeptierbaren „Risiko-Toleranzen“ ausgedrückt.

Beispiele:

- Es besteht das Ziel, das Produktionssystems „FabriStock“ am 1. November 2009 in Betrieb nehmen zu können. Das Ziel heisst somit „Einhaltung des Einführungstermins“. Hingegen könnte ein mögliches Risiko-Ziel heissen: Die Kostenfolge durch eine Terminabweichung, multipliziert mit der Wahrscheinlichkeit ihres Auftretens, darf nicht mehr als 20’000 € betragen (=Risiko). Bei einem Risiko von 10’000 € ist das Risiko-Ziel noch bestens eingehalten, wir befinden uns 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, Airbags, Knautschzone) kann erreicht werden, dass der Ver-

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

letzungsgrad 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:

$$R = p_E \times S_E$$

R: Risiko;

p_E: Wahrscheinlichkeit, dass ein Schadensereignis mit dem Schaden S_E eintritt;

S_E: Ausmass des Schadensereignisses (auch Tragweite oder Verlust).

Im praktischen Umgang mit dieser Formel wird die „theoretische Wahrscheinlichkeit" p_E oft subjektiv bestimmt oder anstelle der Wahrscheinlichkeit p_E die empirisch bestimmte „relative Häufigkeit" H_E des Schadendenseintritts eingesetzt.

Wenn mehrere Schadensereignisse statistisch verteilt eintreten, ist mit der Formel alleine noch nicht festgelegt, welche Kombination von Schaden und Häufigkeit dem Ergebnis zugrundeliegen soll.

Erwarteter Schaden pro Jahr

Eine für viele betriebswirtschaftliche Entscheidungen zweckmässige Variante für die Berechnung eines Risikos ist es daher, den jährlich zu „erwartenden" Schaden aus der Multiplikation der in einem Jahr zu „erwartenden" Eintrittshäufigkeit mit der „erwarteten" Schadenshöhe zu berechnen:

$R_A = H_A \times S_A$

R_A: jährlich „erwarteter" Schaden;
H_A: erwartete Häufigkeit der Schadensereignisse in einem Jahr;
S_A: erwartete Schadenshöhe aus den jährlich eintretenden Schadensereignissen.

Diese im Zusammenhang mit „operationellen Risiken" gebräuchliche Risiko-Darstellung beruht auf der „Aggregation" mehrerer Schadensereignisse und wird auch als „erwarteter Verlust" bezeichnet.

Beispiel:

Anzahl Schadens-ereignisse	Häufigkeit der Anzahl pro Jahr	Schadenshöhe [Mio. €]	Häufigkeit der Schadenshöhen pro Jahr
0	0.2	1	0.4
1	0.6	2	0.5
2	0.3	4	0.2

$H_A = 0 \times 0.2 + 1 \times 0.6 + 2 \times 0.3 = 1.2$
$S_A = 1 \times 0.4 + 2 \times 0.5 + 4 \times 0.2 = 2.2$ [Mio. €]
$R_A = H_A \times S_A = 2.64$ Mio. € (erwarteter Verlust)

Weitere sinnvolle Varianten, um das Risiko auszudrücken werden im Abschnitt 3.2.2 behandelt.

2.3 Anwendung Risiko-Formeln

Die oben angeführten Risiko-Formeln liefern bei relativ häufig auftretenden Ereignissen plausible Risikowerte. Doch kommen sehr hohe Schäden im selben Unternehmen sicherlich nur mit sehr geringer Häufigkeit vor. Für solche sehr hohen Schäden ist es nicht sinnvoll, das Risiko mit einer Multiplikations-Formel zu bestimmen, da die arithmetische Multiplikation eines sehr grossen Schadens mit einer sehr geringen Wahrscheinlichkeit (Häufigkeit) ein für das Unternehmen geringes und damit „tragbares Risiko" vortäuschen würde.

Beispiel

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 mit obiger Formel errechnete 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.

Seltene, aber sehr grosse Schadensereignisse

Dieses Beispiel zeigt, dass für sehr seltene, aber sehr grosse Schadensereignisse Berechnungen mit den oben angeführten „einfachen Risikoformeln" keine adäquaten Entscheidungsgrundlagen liefern. Hier helfen Analyse-Methoden, wie sie in den Abschnitten 3.2.3 und 3.2.4 dargelegt werden.

In einem alternativen pragmatischen Ansatz wird für die seltenen aber sehr grossen Schadensereignisse vorrangig der mögliche Schaden und nicht ein über die Wahrscheinlichkeit rechnerisch ermitteltes Risiko als Entscheidungsgrundlage herbeigezogen. Bei der „Risiko-Bewertung" kann diesem Umstand mit einer entsprechend ausgelegten Risiko-Bewertungs-Matrix (s. Abbildung 2.2) Rechnung getragen werden.

Vorsicht mit den einfachen Risikoformeln ist auch geboten, wenn Schätzwerte für Häufigkeit und Schadenshöhe in die Formel eingesetzt werden. Die mit solchen Werten vorgenommene Multiplikation erweckt zwar den Eindruck eines genauen rechnerischen Ergebnisses; ein genaues Ergebnis ist aber bei geringen Eintrittswahrscheinlichkeiten (-Häufigkeiten) überhaupt nicht möglich.

2.4 Subjektivität bei Einschätzung und Bewertung der Risiken

Die Einschätzung der beiden Risiko-Dimensionen „Wahrscheinlichkeit" und „Schaden" (Konsequenzen, Tragweite) eines Schadensereignisses erfolgt einerseits aus den Erfahrungen der Vergangenheit (ex post) und/oder aus der Prognose für zukünftige Ereignisse (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.

Risiko-Freudigkeit / Risiko-Aversion

So neigen die einen Personen zur Risiko-Freude*, andere wiederum zur Risiko-Aversion†.

Auch sind einer einzelnen Person kaum alle relevanten Fakten für die Beurteilung eines Risikos bekannt. Aufgrund der Subjektivität bei der Wahrnehmung (Perzeption), aber auch bei der Risikobehandlung empfiehlt es sich, die Analysen und Entscheidungen beim Risiko-Management möglichst unter vielen Gesichtswinkeln breit abzustützen. Es empfiehlt sich beispielsweise, die Analyse mit einem interdisziplinär zusammengestellten Risiko-Analyse-Team durchzuführen und die Handlungs- und Akzeptanzentscheide über grosse Risiken im Team (z.B. Geschäftsleitung, Sicherheitskommission) zu fällen.

2.5 Hilfsmittel zur Einschätzung und Bewertung der Risiken

2.5.1 Risiko-Bewertungs-Matrix

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

Risiko-Wahrnehmung

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

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

Die solchermassen enstandende „Risiko-Bewertungs-Matrix", oder kurz Risiko-Matrix genannt, werden wir sodann als Hilfsmittel für die „Bewertung" 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. Dabei sollte aber auf die Kompatibilität der Skalen geachtet werden. Das Beispiel einer solchen Risiko-Matrix ist in der nachfolgenden Abbildung 2.2 gezeigt.

---

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

† Risiko-Aversion bewirkt ein Entscheidungsverhalten, bei dem die jeweils weniger riskante Handlungsalternative bevorzugt wird.