Alexander Mahnke
Torsten Rohlfs *Hrsg.*

Betriebliches Risikomanagement und Industrieversicherung

Erfolgreiche Unternehmenssteuerung durch ein effektives Risiko- und Versicherungsmanagement

Springer Gabler

Betriebliches Risikomanagement und Industrieversicherung

Alexander Mahnke • Torsten Rohlfs
Hrsg.

Betriebliches Risikomanagement und Industrieversicherung

Erfolgreiche Unternehmenssteuerung durch ein effektives Risiko- und Versicherungsmanagement

Springer Gabler

Hrsg.
Alexander Mahnke
Siemens AG
München, Deutschland

Torsten Rohlfs
TH Köln, Institut für Versicherungswesen
Köln, Deutschland

ISBN 978-3-658-30420-1 ISBN 978-3-658-30421-8 (eBook)
https://doi.org/10.1007/978-3-658-30421-8

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

Springer Gabler

Springer Gabler ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Vorwort

Die vorliegende Ausarbeitung ist im Rahmen eines gemeinsamen Forschungsprojektes des Gesamtverbands der versicherungsnehmenden Wirtschaft e. V. (GVNW) und des Instituts für Versicherungswesen (IVW) an der Technischen Hochschule Köln entstanden. Die Studierenden des (auch international ausgerichteten) Studiengangs „Master of Risk & Insurance" des IVW haben dazu zusammen mit ausgewählten Vertretern des Industrieversicherungsmarktes an spezifischen Fragestellungen aus den Bereichen Risikomanagement und Industrieversicherung gearbeitet.

Ziel des Projektes war es, ein vertieftes und praxisorientiertes Verständnis für das industrielle Risikomanagement zu entwickeln und strukturiert für interessierte Studenten und Praktiker aufzubereiten. In den verschiedenen Beiträgen werden hierzu der Risikomanagementprozess ausführlich dargestellt, auf verschiedene Aspekte des unternehmerischen Risikomanagements eingegangen, der Industrieversicherungsmarkt vorgestellt und ausgewählte Unternehmensrisiken mit möglichen Versicherungslösungen diskutiert. Die Ausarbeitungen geben dabei ausschließlich Meinung und Standpunkt der Autoren wieder.

Dieses Projekt hätte nicht entstehen können ohne die tatkräftige Unterstützung vieler Seiten. Unser herzlicher Dank gilt zunächst allen Studierenden und Praxisvertretern, die uns mit ihren Beiträgen einen Einblick in die Praxis des Risikomanagements und der Industrieversicherung geben. Darüber hinaus bedanken wir uns bei den beiden Geschäftsführen des GVNW, Herrn Jörg F. Henne und Herrn Reiner Siebert, die uns bei der Suche nach Autoren und bei der Koordination im gesamten Projektablauf tatkräftig unterstützt haben. Schließlich bedanken wir uns auch bei dem sehr engagierten studentischen Projektleitungsteam, Frau Katharina Faßbender und Herrn Philipp Nießen, welche das Projekt auf Seiten des IVW koordiniert haben.

Wir wünschen allen Lesern eine interessante Lektüre mit vielen Anregungen für den praktischen Alltag.

Bonn, Deutschland — Dr. Alexander Mahnke
Köln, Deutschland — Prof. Dr. Torsten Rohlfs

Inhaltsverzeichnis

Teil I

Einführung

Risikomanagement im Unternehmen

1

Torsten Rohlfs und Alexander Mahnke

Zusammenfassung

Aus der heutigen Perspektive kann Risikomanagement als Gesamtheit aller Maßnahmen nur durch eine unternehmensweite, ganzheitliche und antizipative Betrachtung sämtlicher Risiken in einem bereichsübergreifenden Prozess sinnvoll und effektiv betrieben werden. Die Risiken werden nicht mehr isoliert betrachtet, sondern werden im Unternehmenskontext global analysiert. Der mit dieser Zielsetzung ausgerichtete Risikomanagementprozess wird auch als Enterprise Risk Management bezeichnet.

1.1 Enterprise Risk Management

Unternehmen agieren unter **Unsicherheit**. Die zentrale Herausforderung für das Management besteht darin, zu entscheiden, wie groß die Unsicherheit im Rahmen der unternehmerischen Tätigkeit werden darf bzw. wie viel Risiko das Unternehmen bereit ist einzugehen.

Somit kann auch der unternehmerische Erfolg nicht ohne das eingegangene Risiko betrachtet werden. Über eine **wert- und risikoorientierte Steuerung** sollen gerade Geschäftsstrategie und eingegangene Risiken als Mehrwert-Betrachtung verbunden werden. Aus Sicht der Unternehmenssteuerung sind die Geschäfts- und Risikostrategie gemeinsam abzubilden und zu beurteilen. Die aus den Unternehmenszielen abgeleiteten Geschäfts-

T. Rohlfs (✉)
TH Köln, Institut für Versicherungswesen, Köln, Deutschland
E-Mail: torsten.rohlfs@th-koeln.de

A. Mahnke
Siemens AG, München, Deutschland
E-Mail: mahnke.alexander@siemens.com

A. Mahnke, T. Rohlfs (Hrsg.), *Betriebliches Risikomanagement und Industrieversicherung*, https://doi.org/10.1007/978-3-658-30421-8_1

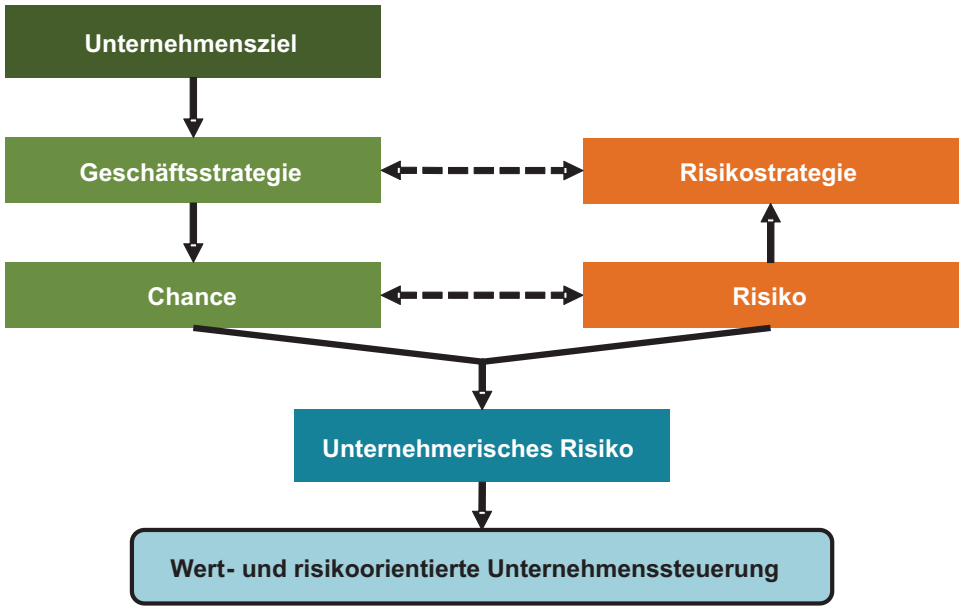

Abb. 1.1 Unternehmenssteuerung. (Quelle: eigene Darstellung in Anlehnung an Rohlfs et al. 2019, S. 18)

strategien werden nicht isoliert festgelegt, sondern immer im Kontext mit dem eingegangenen Risiko beurteilt (vgl. Abb. 1.1; vgl. hierzu Rohlfs et al. 2019, S. 17 ff.).

Ausgangspunkt sind die von der Geschäftsführung formulierten zentralen **Unternehmensziele** als definiertes Ambitionsniveau im Hinblick auf

- Gewinn,
- Wachstum,
- Sicherheit und
- Steigerung des Unternehmenswertes.

Die so vorgegebenen Unternehmensziele werden über eine Gesamtplanung mit aufeinander aufbauenden Teilplänen als konkrete Geschäftsstrategie umgesetzt.

Da die **Geschäftsstrategie** unter Unsicherheit bestimmt wird, sind die ausgearbeiteten Maßnahmen und entsprechenden Chancen mit Geschäftsrisiken verbunden. Diese strategiebezogenen Risiken wiederum bedrohen die ursprünglich der Geschäftsstrategie zugrunde gelegten Unternehmensziele. Durch das direkte Zusammenspiel von Unternehmenszielen, Geschäftsstrategien und Geschäftsrisiko sind daher **Risikostrategie** und Geschäftsstrategie eng miteinander verzahnt. Beide sind Bestandteil der strategischen Unternehmenspolitik.

Die Wechselwirkung von Geschäfts- und Risikostrategie beschreibt das **unternehmerische Risiko** (spekulatives Risiko). In Unternehmen sollte daher ein starkes Bewusstsein (Risikokultur) dafür herrschen, dass Risiken im Rahmen der eigenen Geschäftstätigkeit bestehen, welche das Erreichen von Unternehmenszielen und Geschäftsstrategien erschweren können. Dies ist auch im Interesse der im Unternehmen handelnden Leitungs- und Aufsichts-

organe (Vorstände, Geschäftsführer, Aufsichtsräte etc.), da sie ggf. für die Folgen ihrer Tätigkeiten gegenüber dem Unternehmen (und im Ausnahmefall Dritten gegenüber) haften können.

Dies ist so auch in der **Gesetzgebung** verankert. Der Vorstand einer Aktiengesellschaft hat gemäß § 76 Abs. 1 AktG unter eigener Verantwortung die Gesellschaft zu leiten. Im Hinblick auf das Risikomanagement gibt es im deutschen Aktiengesetz (AktG) zwei wichtige Regelungen:

Nach § 91 Abs. 2 AktG (eingeführt im Jahre 1998 durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich, KonTraG) hat der Vorstand ein Risikofrüherkennungssystem für solche Risiken einzurichten, die den Fortbestand der Gesellschaft gefährden. Auch wenn es vordergründig um das Analysieren bestandsgefährdender (also extremer) Risiken geht, verankert dies ein Risikomanagementsystem in der Geschäftsorganisation. Denn folgerichtig muss dann auch der Umgang mit diesen Risiken geklärt werden. Ebenso müssen identifiziert „wesentliche" (aber nicht bestandsgefährdende) Risiken weiter analysiert und behandelt werden, auch wenn sie dem Wortlaut nach nicht unter das Risikofrüherkennungssystem fallen.

§ 93 Abs. 1 S. 1 AktG regelt, dass die Vorstandsmitglieder bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden haben (§ 43 Abs. 1 GmbHG enthält eine nahezu wortgleiche Regelung). Tun sie dies nicht, so haften sie nach § 93 Abs. 2 S. 1 AktG für den daraus entstehenden Schaden (hierzu ausführlich Lange, D&O-Versicherung und Managerhaftung, § 2). Dies zwingt den Vorstand unter anderem dazu, im Rahmen der Unternehmenssteuerung ein funktionierendes Risikomanagement zu implementieren. Dabei ist allerdings zu berücksichtigen, dass eine die Haftung auslösende Pflichtverletzung dann nicht vorliegt, „wenn das Vorstandsmitglied bei einer unternehmerischen Entscheidung vernünftigerweise annehmen durfte, auf der Grundlage angemessener Information zum Wohle der Gesellschaft zu handeln" (§ 93 Abs. 1 S. 2 AktG). Diese, nach US-amerikanischem Vorbild konzipierte sogenannte „Business Judgement Rule" gilt entsprechend für Geschäftsleiter anderer Unternehmen, wie zum Beispiel der GmbH (vgl. hierzu Lange, D&O-Versicherung und Managerhaftung, § 2, Rn. 48 m. w. N.).

Betrachtet man das Zusammenspiel von Geschäftsstrategien und Geschäftsrisiken, benötigt man im Unternehmen Prozesse, die die Geschäftsrisiken entsprechend steuern können (Prozesssicht) (vgl. Abb. 1.2).

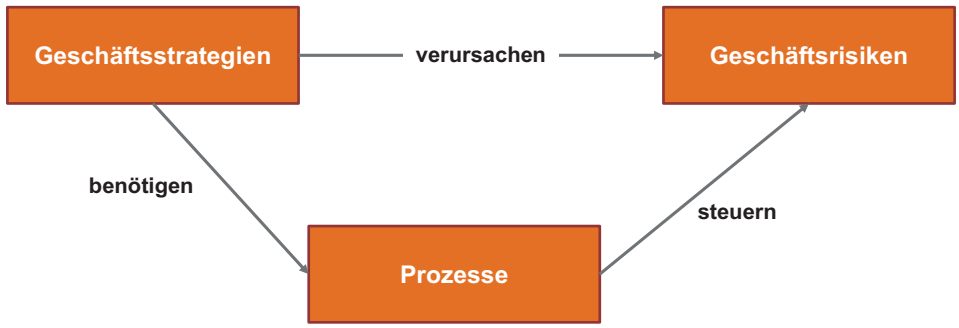

Abb. 1.2 Strategie und Risiko. (Quelle: eigene Darstellung in Anlehnung an Rohlfs 2018, S. 47)

Grundsätzlich können die **notwendigen Prozesse** unterteilt werden in

- Geschäftsprozesse für die Wertschöpfung,
- Informations- und Entscheidungsprozesse für die Unternehmenssteuerung,
- Kontrollprozesse als Risikomanagementprozesse.

Um im Unternehmen eine wert- und risikoorientierte Steuerung umsetzen zu können, braucht man also eine Geschäftsorganisation, die **Kontrollinstanzen bzw. Koordinationsfunktionen** vorsieht. Sämtliche Kontrollaspekte können dabei als Absicherung von Risiken verstanden werden. Entsprechend können finanzielle, technische und organisatorische Risiken abgesichert werden. Mit dem **Risikomanagement** als strukturiertem Umgang mit Chancen und Risiken im Unternehmen (DRS 20.11) versucht man eben diese Risiken zu steuern.

Als **finanzielles Risikomanagement** kann die Absicherung der Bilanz und die Steuerung der Risikotragfähigkeit verstanden werden. Hierzu gehören Instrumente wie Einkauf von Versicherungsschutz, Hedging, alternativer Risikotransfer, Steuerung der Durationslücke, allgemeine Risikostreuung, Liquiditätsmanagement.

Mithilfe des **technischen Risikomanagements** sollen die betriebliche Infrastruktur und die Arbeitsprozesse abgesichert werden. Im Fokus stehen Materialnutzung, Anlagensicherheit, Produktsicherheit & Produkthaftung, Arbeitnehmerschutz & Umweltschutz, Aufrechterhaltung der Geschäftstätigkeit einschließlich dem Business Continuity Management.

Das **organisatorische Risikomanagement** dient der Absicherung der gesamten Geschäftsorganisation im Normalbetrieb und in Krisensituationen. Hierunter fallen sämtliche Maßnahmen im Rahmen der Organisationsstruktur, die sich auf die Ausgestaltung bzw. Sicherung von Aufbau- und Ablauforganisation beziehen. Ebenso verlangt die Steuerung und Kontrolle der Geschäftsorganisation ein funktionierendes Informationssystem.

All diese Schwerpunkte im Risikomanagement bilden das **Risikomanagementsystem** als „Gesamtheit der Regelungen, die einen strukturierten Umgang mit Chancen und Risiken im Unternehmen sicherstellt“ (IDW PS 981, Tz. 17).

Ein solches Risikomanagementsystem muss durch eine unternehmensweite, ganzheitliche und antizipative Betrachtung sämtlicher Risiken in einem bereichsübergreifenden Prozess systematisch und effektiv steuern (vgl. Diederichs 2012, S. 12 f.). Somit werden Risiken nicht mehr isoliert betrachtet, sondern im Unternehmenskontext global analysiert. Der mit dieser Zielsetzung ausgerichtete Ansatz wird auch als **Enterprise Risk Management** bezeichnet (vgl. Rohlfs 2018, S. 1). Das Enterprise Risk Management unterstellt für das Risikomanagement, dass es

- ein Prozess ist, der sich ununterbrochen und über die gesamte Organisation erstreckt;
- durch Menschen auf jeder Ebene einer Organisation ausgeführt wird;
- bereits bei der Strategiefestlegung angewendet wird;
- unternehmensübergreifend angewendet wird (auf jeder Ebene und in jeder Einheit) und das organisationsweite Risikoportfolio betrachtet;

- so gestaltet ist, dass mögliche das Unternehmen beeinflussende Ereignisse erkannt und Risiken auf Grundlage der Risikoneigung gesteuert werden können;
- geeignet ist, den Führungskräften sowie den Überwachungs- und Leitungsorganen einer Organisation hinreichend Sicherheit zu gewährleisten;
- ausgerichtet ist auf das Erreichen von (zusammenhängenden) Zielen (vgl. COSO 2004, S. 2).

Der gewählte Risikomanagementansatz ist natürlich auch im Rahmen der Mehrwert-Betrachtung zu analysieren. So gibt es sicherlich auch Steuerungsmaßnahmen für eingegangene Risiken, die unter Effizienz- und Effektivitätsgesichtspunkten nicht sinnvoll sind. Somit hat auf den **Unternehmenswert** neben der Geschäftsstrategie auch immer der Umgang mit Risiken im Rahmen des Risikomanagementsystems einen wesentlichen Einfluss. Dieser Einfluss kann über ein **Total Cost of Risk-Modell** (TCOR) als gemeinsame Betrachtung von Risikofinanzierung und Risikokontrolle schematisch dargestellt werden (vgl. Abb. 1.3).

Der Total Cost of Risk erfasst alle relevanten Kosten aus dem Management der Risiken und stellt sie den möglichen Verlusten aus der Realisierung der Risiken gegenüber. Somit sind alle ergriffenen Kontroll- und Absicherungsmaßnahmen aus ökonomischer Sicht zu beurteilen, inwieweit diese sich in einer Gesamtbetrachtung positiv auf den Unternehmenswert auswirken.

Zur systematischen Beurteilung wird der Total Cost of Risk in **verschiedene Bestandteile** untergliedert:

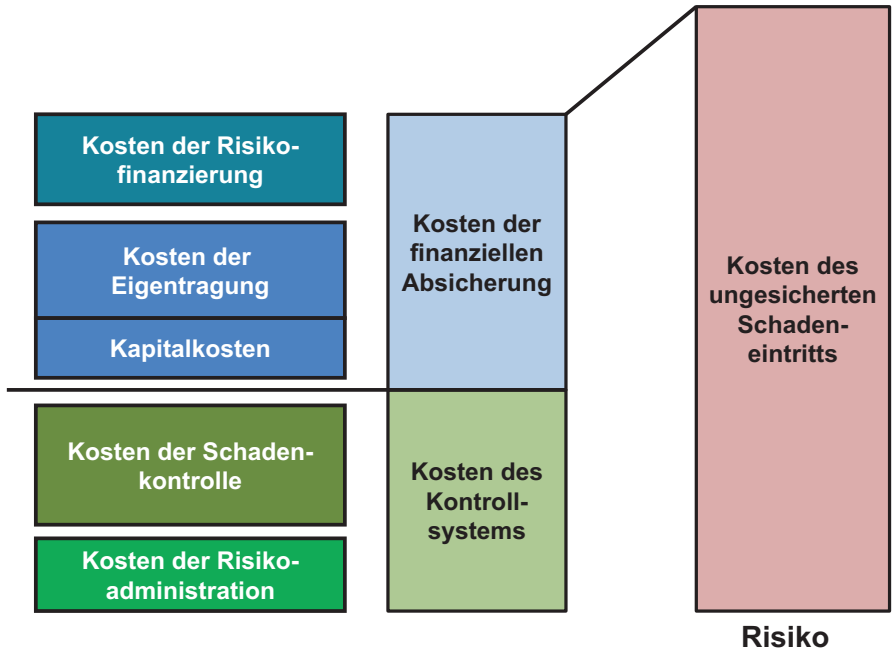

Abb. 1.3 TCOR-Ansatz. (Quelle: eigene Darstellung)

- **Kosten der Risikofinanzierung:** Können Risiken extern abgesichert werden (absicherbare Risiken), sind hier Versicherungsprämien oder Kosten für Kapitalmarktinstrumente zu erfassen.
- **Kosten der Eigentragung:** Hierunter fallen Schadenkosten durch bewusst oder unbewusst nicht versicherte Schäden, nichtversicherbare Schäden und vereinbarte Selbstbeteiligungen. Auch die Kosten für den Einsatz einer firmeneigenen Versicherung (Captive) können hierunter fallen. Die Schadenkosten können in der Bewertung dabei auch mit einer Risikomarge für die mögliche Volatilität der Schadenhöhe versehen werden.
- **Kapitalkosten:** Ansatz von kalkulatorischen Kosten für gebundenes Eigenkapital, das zur Risikofinanzierung benötigt wird.
- **Kosten der Schadenkontrolle:** sämtliche externen und internen Kosten der Kontrollprozesse (Kontrolle des Risikos). Hierzu zählen zum Beispiel Maßnahmen für den Brandschutz, das Qualitätsmanagement oder auch Kontrollen im Rahmen der Geschäftsorganisation.
- **Kosten der Risikoadministration:** Kosten für die interne und externe Administration rund um das Risikomanagement oder auch das Versicherungsmanagement. Hierzu gehören zum Beispiel die Kosten für eine eigene Risikomanagement- und Versicherungsabteilung (ggf. einen firmenverbundenen Versicherungsvermittler) oder auch für den Einsatz eines externen Versicherungsmaklers oder sonstiger eingekaufter Expertise.

Je nach Betrachtungsgegenstand ist der Total Cost of Risk (TCOR) eher ein akademisches Gedankenspiel (zum Beispiel zur Bewertung der Internen Revision als Maßnahme im organisatorischen Risikomanagement). Er kann aber auch konkret in unternehmerische Entscheidungen einfließen, zum Beispiel bei der Auswahl von Versicherungslösungen über den Ansatz der sogenannten „Total Cost of Insurable Risk“ (TCOIR). Mit dem TCOIR werden nur die Kosten gemessen, die dem Unternehmen im Zusammenhang mit dem Einkauf von Versicherungen, dem Einsatz interner und externer Versicherungsberatung (eigene Versicherungsexperten, externe Versicherungsmakler und sonstige) und dem Eigenbehalt bestimmter versicherungsfähiger Risiken (zum Beispiel über Selbstbehalte oder den Einsatz einer Captive-Versicherung) entstehen.

1.2 Risikomanagementprozess

Das Risikomanagementsystem als Unternehmensfunktion im Sinne eines **Enterprise Risk Management** kann einerseits als Absicherungssystem und andererseits als Informationssystem verstanden werden. Das System ist zur Unternehmenssteuerung als fortlaufender Prozess zu gestalten.

Zum klassischen Aufbau eines **Risikomanagementprozesses** gehören die Prozessschritte der Risikoanalyse, der Risikosteuerung sowie der Risikokontrolle und Berichterstattung. Die Risikoanalyse beinhaltet die Identifizierung und Bewertung der Risiken sowie ggf. deren Aggregation.

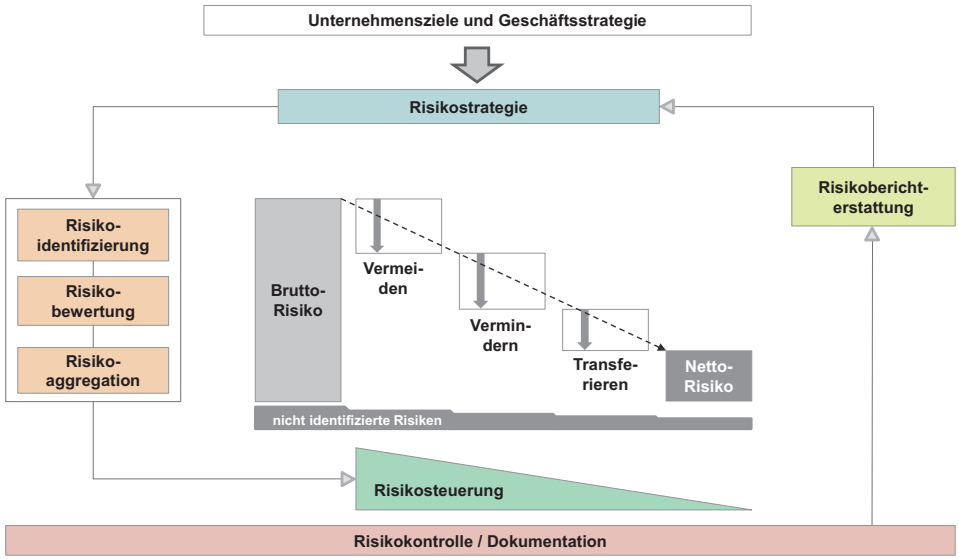

Abb. 1.4 Risikomanagementprozess. (Quelle: eigene Darstellung)

Die Vorgabe der Unternehmensziele und die Aspekte der Risikostrategie und Risikotoleranz (Unternehmensplanung) sind dem eigentlichen Risikomanagementprozess vorgelagert (vgl. Abb. 1.4).

1.2.1 Risikostrategie

Die Risikostrategie schildert insbesondere die Auswirkungen der Geschäftsstrategie auf die **Risikosituation** des Unternehmens und beschreibt den Umgang mit den vorhandenen Risiken und die Fähigkeit des Unternehmens, neu entstehende Risiken zu tragen. Durch die festgelegten Ziele und Entscheidungen, die in der Geschäftsstrategie beschrieben werden, ergeben sich Risiken aus den verschiedenen unternehmensinternen und externen Umweltfaktoren. Ähnlich zu der Beurteilung von miteinander verbundenen Zielen sind unter Risikogesichtspunkten dabei auch Risikozusammenhänge festzustellen (vgl. Rohlfs 2018, S. 49 f.).

In der Risikostrategie werden neben der grundsätzlichen Risikoausrichtung Leitlinien festgelegt, die den Risikomanagementprozess gestalten.

Der **Inhalt der Risikostrategie** muss sich beschäftigen mit

- Art des Risikos,
- Herkunft des Risikos,
- Zeithorizont der Risikobetrachtung,
- Risikotoleranz und
- Risikotragfähigkeit.

Die konkret angestrebte Höhe von Risiko und Risikotragfähigkeit wird über die **Risikobereitschaft** definiert (Risikoappetit und Risikotoleranz).

Beim **Risikoappetit** stellt man sich die Frage, was das Unternehmen sich insgesamt an Risiken erlauben will. Er beschreibt somit die „Haltung" der Entscheidungsträger gegenüber den wesentlichen Risikokategorien und Risikoarten (vgl. BaFin, Rn. 2.77). Der Risikoappetit gibt an, wie viel des ökonomischen Eigenkapitals zur Abdeckung aller wesentlichen Risiken verwendet werden soll. Er steht für die individuelle Risikobereitschaft der Entscheidungsträger und orientiert sich an den strategischen Zielen des Unternehmens. Der Risikoappetit spiegelt sich in der Risikostrategie wider (vgl. Ellenbürger et al. 2009, S. 166).

Im Hinblick auf die **Risikotoleranz** stellt man sich dagegen die Frage, was das Unternehmen sich erlauben kann bzw. darf. Es kann sich um Beschränkungen handeln, die sich das Unternehmen bei der Übernahme von Risiken selbst auferlegt – der Risikoappetit („erlauben kann") – oder solche, die die Risikoübernahmekapazität durch externe Vorgaben tatsächlich beschränken („erlauben darf"). Hier kann es sich zum Beispiel um Beschränkungen handeln, um ein marktakzeptables Mindest-Rating zu erhalten oder um ggf. aufsichtsrechtliche Anforderungen zu erfüllen (vgl. BaFin, Rn. 2.77).

1.2.2 Risikoidentifizierung

Risiken ergeben sich aus der Geschäftsstrategie und allen daraus abgeleiteten operativen Tätigkeiten. Um den Umgang mit den Risiken vorgeben zu können, müssen diese zunächst **identifiziert** werden. Dies beinhaltet die möglichst vollständige Erfassung aller Risikobereiche, Risikoursachen und Risikoobjekte.

Risikoidentifizierung beschreibt die Suche und Bestimmung aller Einzelrisiken sowie das Bilden von Risikogruppen bzw. -kategorien. Sie liefert damit Informationen, welche unerlässlich sind, um relevante Risiken systematisieren, analysieren und bewerten zu können. Indem **gleichartige Risiken** zusammengefasst werden, erhalten Unternehmen einen besseren Überblick hinsichtlich der Risiken und auch den damit verbundenen Chancen. Eine **Risikokategorisierung** vereinfacht den gesamten Prozess der Risikoanalyse, insbesondere der Bewertung eines Risikokapitalbedarfs sowie der Erfassung von Diversifikationseffekten. Auch bietet sie den Unternehmen die Möglichkeit, verschiedene Risikoarten mit entsprechend zugeschnittenen Maßnahmen und Instrumentarien zu steuern (vgl. Sartor und Bourauel 2013, S. 10 ff.).

Die Methoden zur Risikoidentifizierung sind vielfältig und können in zwei Bereiche unterteilt werden: Managementmethoden und unterstützende Methoden zur Informationssammlung und -generierung. Unter **Managementmethoden** werden Analyseansätze verstanden, die im Unternehmen zur Bildung der Geschäftsstrategie verwendet werden und daher auch zur Aufdeckung von Risiken verwendet werden. Hierzu zählen beispielsweise Wertschöpfungsketten, SWOT-Analysen, Benchmarks, die Balanced Scorecard etc. Um Informationen zu sammeln oder zu generieren, die bei Anwendung der Managementme-

thoden weiter verarbeitet oder strukturiert werden können, eignen sich dann verschiedene **Kollektions- und Suchmethoden** wie Checklisten, Dokumentenanalysen, Fehlerbaumanalysen, Brainstorming oder Szenario-Techniken.

Das Übersehen von Risiken oder deren zu späte Identifizierung kann zu unternehmerischen Gefahren (bis hin zur Existenzgefährdung) führen. Eine **spätere Fehlerkorrektur** erweist sich häufig als schwierig. Oftmals ist sie mit einem hohen Kostenaufwand verbunden. In der Unternehmenspraxis besteht unter Umständen aber auch die Gefahr, dass ein späteres Eingreifen nicht mehr möglich ist. Da Unternehmen in der heutigen Zeit einem ständigen Wandel und neuen Rahmenbedingungen ausgesetzt sind, ist eine **kontinuierliche und systematische** Risikoidentifizierung und -beobachtung unabdingbar (vgl. Diederichs 2012, S. 50 f.).

Das Ergebnis der Risikoidentifizierung ist eine **strukturierte Darstellung** von allen bestehenden und potenziellen Risiken inklusive ihrer Auswirkungen in einem **Risikokatalog** (Risikoinventar). Ziel der Risikoidentifizierung ist eine möglichst konsistente und überschneidungsfreie Bestandsaufnahme aller Risiken. Durch den Risikoidentifizierungsprozess wird das **Gesamtrisikoprofil** eines Unternehmens bestimmt.

1.2.3 Risikobewertung

Die Risikobewertung verfolgt das Ziel, das von den identifizierten Risiken ausgehende **Gefahrenpotenzial** transparent zu machen und deren Wirkung offen zu legen (vgl. Altenähr et al. 2009, S. 63). Dies geschieht durch die Analyse, welche Bedrohungen von den Risiken ausgehen (unwesentliche, wesentliche oder bestandsgefährdende Risiken). Basis dieser Analyse ist somit die Festlegung von Wesentlichkeitsgrenzen, wobei es Risiken gibt, die quantitativ und andere, die lediglich qualitativ beurteilt werden können.

Die Risikobewertung dient dabei einerseits als Grundlage für die Festlegung der Maßnahmen im Rahmen der Risikosteuerung. Andererseits dient sie zur Bestimmung des einzelnen Risikokapitalbedarfs als Basis für die daran anschließende Aggregation zur Ermittlung eines Gesamtrisikokapitalbedarfs.

Im **ersten Schritt** der Bewertung können Risiken durch folgende Methoden eingeschätzt werden („Allgemeine Bewertungs-/Beurteilungsmethoden“):

- Relevanzeinschätzungen,
- Scoring-Modelle,
- ABC/XYZ-Analysen oder
- Ratings (Qualitätsstufen).

Durch diese Methoden können die unterschiedlichen Aspekte eines Risikos verdichtet und die Komplexität der realen Gegebenheiten reduziert werden. Dabei besteht auch die Möglichkeit, Risiken in eine Reihenfolge („Ranking“) zu bringen und entsprechend zu analysieren. Des Weiteren können wesentliche von unwesentlichen Risiken getrennt wer-

den, um einen unwirtschaftlichen Mehraufwand im weiteren Bewertungsverfahren zu verhindern.

Infolgedessen werden im **zweiten Schritt** meist nur Risiken intensiver untersucht und präziser bewertet, die nach erster Einschätzung relevant für das Unternehmen sind. Dies geschieht durch eine Quantifizierung, die mithilfe statistischer Methoden und unter Zugrundelegung eindeutig definierter Größen (Schadenausmaß, Eintrittswahrscheinlichkeit, Streuung) die Risiken misst und die Auswirkungen im Zusammenspiel mit anderen Risiken beurteilt.

Dies kann zum Beispiel durch folgende Methoden erreicht werden („Methoden zur Bewertung des Risikoausmaßes"):

- Ratings (Ausfallwahrscheinlichkeiten),
- Quantitative Risikomatrix,
- Wahrscheinlichkeitsverteilungen,
- Stresstests und Szenariorechnungen.

Wegen der Problematik der möglichen Fehleranfälligkeit komplexer Bewertungsmethoden sind an die Bewertung bestimmte **Qualitätsanforderungen** zu stellen. Grundsätzlich sind anerkannte Risikobewertungsmethoden zu verwenden. Um eine Willkürlichkeit zu vermeiden, ist ein unternehmensweites einheitliches Sicherheitsniveau zu unterstellen. Die zu schätzenden Parameter sollten so gewählt und bestimmt werden, dass eine Vergleichbarkeit und Transparenz gegeben ist. Dort, wo es die Bewertung zulässt, sollten im Idealfall vorhandene aktuelle Marktdaten zum Einsatz kommen.

1.2.4 Risikoaggregation

Ziel der Aggregation im Rahmen der Analyse ist es, den gesamten **Risikokapitalbedarf** eines Unternehmens zu ermitteln, welcher sich auf die Entwicklung von Eigenkapital und Gewinn auswirken kann. Hierfür bedarf es einer allgemein gültigen Definition des Gesamtrisikos auf Basis aller Einzelrisiken. Dabei ist die Aggregation nicht zu verwechseln mit der Summe der Einzelrisiken. Die aggregierten Einzelrisiken sind (sofern keine vollständig positive Korrelation vorliegt) grundsätzlich kleiner als die Summe aller Einzelrisiken. Grund hierfür ist die **Diversifikation**, bei der Risikoausgleichseffekte zwischen den Einzelrisiken berücksichtigt werden.

Die Frage, die sich an die Bestimmung des gesamten Risikokapitalbedarfs anschließt, ist die, inwiefern das Gesamtrisiko auch getragen werden kann: Weist das Unternehmen ausreichend hohes ökonomisches Eigenkapital aus? Diese Frage nach der Überdeckung wird durch das Maß der **Risikotragfähigkeit** veranschaulicht. Sie beschreibt die Fähigkeit, Verluste aus Risiken zu absorbieren, ohne dass daraus eine direkte Gefahr für die Existenz des Unternehmens entsteht:

$$\text{Risikotragfähigkeit} = \frac{\text{ökonomisches Eigenkapital}}{\text{Gesamtrisikokapitalbedarf}} \geq 100\,\%$$

Je nach Rechnungs- und Bilanzierungsgrundlagen kann die Risikotragfähigkeit zu ökonomischen, ratingbezogenen oder aufsichtsrechtlichen Zwecken ermittelt werden.

1.2.5 Risikosteuerung

Im Rahmen der Risikosteuerung ist sicherzustellen, dass der **Risikoumfang** nicht größer als die angestrebte **Risikotragfähigkeit** ist. Zudem sollte die derzeitige Risikosituation mit den damit verbundenen Chancen in Relation gesetzt werden. Risiken sollten nur eingegangen werden, sofern ihnen ein angemessenes Ertragspotenzial gegenüber steht. Entspricht das **Chancen-Risiko-Verhältnis** nicht den Zielvorstellungen des Unternehmens, wird mittels der Risikosteuerung versucht, die Herstellung der geplanten Soll-Risikosituation zu erreichen (vgl. Vanini 2012, S. 224). Dabei wird das ursprüngliche Bruttorisiko auf ein angemessenes Maß reduziert. Die Risikosteuerung umfasst

- Risikovermeidung,
- Risikoverminderung,
- Risikotransfer.

Das nach den Steuerungsmaßnahmen **verbleibende Restrisiko** (Netto-Risiko) wird dann vom Unternehmen selbst getragen. Auf der einen Seite will man gewisse Ertragspotenziale nutzen und somit Risiken bewusst eingehen, auf der anderen Seite ist die **Selbsttragung** aufgrund von mangelnden adäquaten Steuerungsmaßnahmen zwangsläufig notwendig.

Bei der **Risikovermeidung** wird auf das Eingehen von bestimmten Risiken (prospektiv) gänzlich verzichtet. Dies kann aus Gründen des Risikomanagements sinnvoll sein, wenn die Risiken durch ein unverhältnismäßig hohes Risikopotenzial gekennzeichnet sind. Mit der Risikovermeidung geht aber auch einher, dass auf entsprechende mögliche Chancen (Geschäftsstrategien) verzichtet wird.

Im Rahmen der **Risikoverminderung** wird durch die Beeinflussung der Risikostruktur der gesamte Risikogehalt reduziert, aber nicht vollständig eliminiert. Hier steht den Unternehmen eine Vielzahl von Möglichkeiten zur Verfügung, mithilfe geeigneter Maßnahmen auf die Eintrittswahrscheinlichkeit und/oder das Schadenausmaß eines Risikos einzuwirken. Die Risikoverminderung führt dazu, dass auch weiterhin Ertragspotenziale genutzt werden können, da das eingegangene Risiko und die damit verbundene Chance nicht vollständig ausgeschlossen wird.

Bei der Steuerung können **ursachen- und wirkungsbezogene Maßnahmen** unterschieden werden. Ursachenbezogene Strategien zielen darauf ab, die Eintrittswahrschein-

lichkeit des Risikos zu vermeiden oder zu vermindern. Wirkungsbezogene Maßnahmen hingegen sollen die Auswirkungen bei Realisation des Risikos verringern (vgl. Altenähr et al. 2009, S. 117).

Außerdem können Risiken zur Reduzierung der eigenen Risikoexponierung an einen Dritten **transferiert** werden. Das ursprüngliche Risiko bleibt bestehen, es wird jedoch nicht mehr allein getragen. Eine klassische Form des Risikotransfers ist die Versicherung. Vorstellbar ist aber auch der Transfer von Risiken auf den Kapitalmarkt, auf den Kunden oder auf Lieferanten. Aber auch Ausgliederungen oder die Gründung von Gesellschaften können je nach Gestaltung als Transfer gesehen werden.

Die Abbildung zum Risikomanagementprozess veranschaulicht schematisch, wie das ursprüngliche **Brutto-Risiko** grundsätzlich durch geeignete Steuerungsmaßnahmen auf das beim Unternehmen verbleibende **Netto-Risiko** reduziert werden kann. Neben den identifizierten Risiken besteht trotz umfassender Risikoanalysen die Gefahr, dass Risikopotenziale nicht erkannt werden. Diese nicht identifizierten Risiken können natürlich nicht bewusst gesteuert werden. Sie werden jedoch unbewusst auch durch die Etablierung allgemeiner Steuerungsmaßnahmen vermindert.

1.2.6 Risikokontrolle und Berichterstattung

Die Risikokontrolle (auch Risikocontrolling) beschreibt ein zusammenfassendes und zugleich steuerndes Element innerhalb des gesamten Risikomanagementprozesses. Sie ist zur Beurteilung von Effizienz und Wirksamkeit des Risikomanagements sowie zur Feststellung möglicher Verbesserungspotenziale erforderlich. Kontrolle verlangt auch immer eine Dokumentation bzw. eine Berichterstattung. Nur eine angemessene Berichterstattung ermöglicht es den verschiedenen Parteien, die in den Risikomanagementprozess eingebunden sind, ihrer Überwachungs- oder Entscheidungsfunktion auf Basis der erhaltenen Informationen nachzukommen.

Die **Risikokontrolle** durch das Risikomanagement beinhaltet im Wesentlichen folgende Aspekte:

- Überprüfung der Angemessenheit der eingerichteten Maßnahmen zum Aufbau und Ablauf des Risikomanagementprozesses (einschließlich der Weiterentwicklung);
- Sicherstellung der vollständigen Erfassung aller wesentlichen Risiken und deren angemessene Beurteilung/Bewertung;
- Kontinuierliche Anwendung der risikorelevanten Maßnahmen bzw. deren Anpassung;
- Einhaltung der integrierten Kontrollen;
- Kommunikation.

Die Prozesse und die Ergebnisse der Risikoanalyse und Risikosteuerung sind laufend zu kontrollieren, damit sichergestellt ist, dass eingegangene Risiken in einem tolerierbaren Ausmaß bleiben. Aus dieser Anforderung heraus ist ein unternehmensweites **Kontroll-**

system zu implementieren, in dem alle operativen Bereiche und das Risikomanagement eingebunden sind. Die Risikokontrolle verlangt dabei natürlich auch eine systematische Dokumentation, um später eine Überprüfung vornehmen zu können.

In der **Risikoberichterstattung** soll über das Risikoprofil des Unternehmens berichtet werden. Sie dient somit der permanenten Überwachung und stellt sicher, dass identifizierte und bewertete Risiken den (internen und externen) Entscheidungsträgern mitgeteilt werden. Bei der Kommunikation kann eine interne und eine externe Berichterstattung unterschieden werden.

Die Unternehmen müssen über eine angemessene und aussagefähige **interne Risikoberichterstattung** verfügen. Es ist Aufgabe des Risikomanagements, die Risikoberichterstattung in Abstimmung mit den verschiedenen Unternehmensbereichen aufzustellen und diese der Geschäftsführung, dem Aufsichtsrat, den entsprechenden Managementebenen, anderen Unternehmensfunktionen und den Mitarbeitern zur Verfügung zu stellen. Dadurch soll sichergestellt werden, dass die Informationsadressaten alle wichtigen Informationen zur Risikosituation erhalten. Die Kommunikation kann **regelmäßig** (zum Beispiel wöchentlich, monatlich, jährlich) oder **ad hoc** erfolgen. Letzteres führt zum Beispiel zu einer sofortigen Meldung bei der Überschreitung eines Schwellenwertes bei einer Risikokennzahl oder dem Eintreten eines außergewöhnlichen Ereignisses.

Für die **externe Berichterstattung** bildet das Handelsgesetzbuch die gesetzliche Grundlage. Gemäß § 264 Abs. 1 HGB ist bei Kapitalgesellschaften der Jahresabschluss, bestehend aus der Bilanz, der Gewinn- und Verlustrechnung und dem Anhang, um einen **Lagebericht** zu erweitern. Aus Sicht der Risikoberichterstattung ist insbesondere der Lagebericht gemäß der **§§ 289 bis 289f HGB** von Bedeutung. Konkretisiert wird die Risikoberichterstattung für den Lagebericht durch den **DRS 20**, der jedoch für Konzernlageberichte gilt. Die Anwendung des DRS 20 auf den Einzelabschluss ist somit nicht zwingend, sie wird aber empfohlen (vgl. DRS 20, Tz. 2). Aus diesem Grund kann er als Rahmenwerk für eine angemessene öffentliche Berichterstattung angesehen werden.

Die externe Berichterstattung kann in Abhängigkeit von speziellen Zielsetzungen (wie Verkaufsprospekte) oder Branchen (wie die aufsichtsrechtliche Berichterstattung bei Versicherungsunternehmen oder Banken) zusätzlich variieren.

Literatur

Altenähr, V., Nguyen, T., & Romeike, F. (2009). *Risikomanagement kompakt*. Karlsruhe: Versicherungswirtschaft.

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). (2016). Erläuterungen zu Leitlinien zum Governance-System der EIOPA, Übersetzung durch die BaFin, 20.05.2016. https://www.bafin.de/SharedDocs/Downloads/DE/Aufsichtsrecht/dl_erl_texte_leitlinien_zu_governance_system_de_va.html?nn=7850436. Zugegriffen am 04.03.2020.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2004). COSO II, Unternehmensweites Risikomanagement – Übergreifendes Rahmenwerk, Zusammenfassung, September 2004.

Deutscher Rechnungslegungs Standard Nr. 20 (DRS 20). (2012). Konzernlagebericht, Deutsche Rechnungslegungs Standards Committee/DRSC (Hrsg.), 2012.
Diederichs, M. (2012). *Risikomanagement und Risikocontrolling* (3. Aufl.). München: Franz Vahlen GmbH.
Ellenbürger, F., Ott, P., Frey, C., & Boetius, F. (2009). *Mindestanforderungen an das Risikomanagement (MaRisk) für Versicherungen – Eine einführende Kommentierung*. Schäffer-Poeschel.
Institut der Wirtschaftsprüfer. (2017). IDW Prüfungsstandards, Grundsätze ordnungsmäßiger Prüfung von Risikomanagementsystemen (IDW PS 981), Düsseldorf.
Lange, O. (2014). *D&O-Versicherung und Managerhaftung*. München: C.H. Beck.
Rohlfs, T. (2018). *Risikomanagement im Versicherungsunternehmen* (2. Aufl.). Karlsruhe: Versicherungswirtschaft.
Rohlfs, T., Savic, B., & Will, D. (2019). *Rechnungslegung und Controlling der Versicherungsunternehmen*. Karlsruhe: Versicherungswirtschaft.
Sartor, F. J., & Bourauel, C. (2013). *Risikomanagement kompakt – In 7 Schritten zum aggregierten Nettorisiko des Unternehmens*. Oldenbourg Wissenschaftsverlag.
Vanini, U. (2012). *Risikomanagement: Grundlagen, Instrumente, Risikopraxis*. Stuttgart: Schäffer-Poeschel.

Prof. Dr. Torsten Rohlfs lehrt am Institut für Versicherungswesen der Technischen Hochschule Köln. Seine Fachgebiete sind insbesondere das Rechnungswesen und Risikomanagement von Versicherungsunternehmen. Er ist Wirtschaftsprüfer und war vor seiner Tätigkeit an der TH Köln Senior Manager bei der KPMG AG Wirtschaftsprüfungsgesellschaft im Bereich Prüfung und Beratung von Versicherungsunternehmen. Prof. Dr. Torsten Rohlfs ist Mitglied im Ratingkomitee der ASSEKURATA Assekuranz Rating-Agentur GmbH und im wissenschaftlichen Beirat des Gesamtverbands der versicherungsnehmenden Wirtschaft e.V. (GVNW). Darüber hinaus ist er Mitglied der Prüfungskommission für Wirtschaftsprüfer.

Dr. Alexander Mahnke begann seine berufliche Laufbahn im Jahr 1999 bei Siemens, wo er zuletzt bei SFS für die Koordination der weltweiten Konzern-Haftpflichtversicherungsprogramme zuständig war. Von 2004 bis 2010 war er bei AON Jauch & Hübener unter anderem als Leiter des Geschäftsfelds Financial Services Group tätig. 2010 übernahm er bei Marsh die Leitung der beiden Geschäftsgebiete Financial & Professional Services (FINPRO) und Credit & Political Risks und wurde Anfang 2011 in die erweiterte Geschäftsleitung der Marsh GmbH berufen.

Im April 2011 übernahm er die Leitung Versicherungen bei Siemens in München und ist in dieser Funktion für alle versicherungsfähigen Risiken des Konzerns weltweit zuständig.

Dr. Alexander Mahnke ist Vorsitzender des Vorstandes des Gesamtverbandes der versicherungsnehmenden Wirtschaft e. V. (GVNW).

Er hat Rechtswissenschaften in Bayreuth, München und Montpellier studiert und an der Universität Bochum promoviert.

Teil II

Risikomanagementprozess

Risikoidentifizierung und -klassifizierung

2

Wolfgang Knauf und Jessica Bender

Zusammenfassung

In diesem Kapitel wird der erste Schritt des Risikomanagementprozesses erläutert. Bei der Risikoidentifizierung geht es darum, unter Beachtung der Vollständigkeit, Wirtschaftlichkeit, Zukunftsbezogenheit, Aktualität und Konsistenz, diejenigen Entwicklungen oder Ereignisse zu bestimmen, die zu einer für ein Unternehmen negativen Prognose- oder Zielabweichung führen können. Dabei kann ein Unternehmen aus verschiedenen Perspektiven an die Identifizierung herangehen und aus einer Vielzahl an Risikoidentifizierungsmethoden wählen. Wurden alle relevanten Risiken identifiziert, findet dann die Risikoklassifizierung statt. Hierbei werden die zuvor identifizierten Risiken den unternehmensindividuell gebildeten Klassen zugeordnet. Innerhalb der Risikoklassen hat ein Unternehmen die Möglichkeit noch weitere Systematisierungen der Risiken vorzunehmen. Sind Risikoidentifizierung und -klassifizierung abgeschlossen, werden die Ergebnisse strukturiert dargestellt.

2.1 Aufgabe der Risikoidentifizierung

Um zu verdeutlichen, worum es bei der Risikoidentifizierung geht, werden zunächst einmal die beiden Begriffe „Risiko“ und „Identifizierung“ definiert.

W. Knauf (✉)
Henkel AG & Co. KGaA, Düsseldorf, Deutschland
E-Mail: wolfgang.knauf@henkel.com

J. Bender
TH Köln, Institut für Versicherungswesen, Köln, Deutschland
E-Mail: bender.jessica@t-online.de

A. Mahnke, T. Rohlfs (Hrsg.), *Betriebliches Risikomanagement und Industrieversicherung*, https://doi.org/10.1007/978-3-658-30421-8_2

Je nach Kontext, wird der Begriff „Risiko“ anders verwendet. Allgemein kann jedoch unter einem Risiko eine Abweichung von einem erwarteten Ergebnis verstanden werden. In diesem Buch wird die Risikodefinition des DRS 20 zugrunde gelegt, welche Ergebnisabweichung in positive oder negative Abweichungen differenziert. „Mögliche künftige Entwicklungen oder Ereignisse, die zu einer für das Unternehmen negativen Prognose- oder Zielabweichung führen können“ (DRS 20, Tz. 11), werden im Folgenden als Risiko bezeichnet. Während „mögliche künftige Entwicklungen oder Ereignisse, die zu einer für das Unternehmen positiven Prognose- oder Zielabweichung führen können“ (DRS 20, Tz. 11) als Chancen für das Unternehmen verstanden werden.

Der Begriff „Identifizierung“ wird im Alltag oft im Zusammenhang mit der Identifizierung von Menschen, zum Beispiel anhand eines Personalausweises benutzt. Doch genauso wie Menschen anhand von gewissen Merkmalen identifiziert werden können, können auch Risiken identifiziert werden. Dazu wird die Definition von einem Risiko zur Hilfe genommen, um nach allen Entwicklungen oder Ereignissen zu suchen, die ein Risiko für das Unternehmen darstellen könnten.

In einem Unternehmen gibt es zahlreiche Risiken, welche die Ziele und damit die ganze Unternehmung an sich gefährden können. Die Risiken ergeben sich nicht nur aus der verfolgten Geschäftsstrategie, sondern auch aus dem operativen Geschäft. Damit die Risiken jedoch zu keinen existenzbedrohenden Gefahren für das Unternehmen werden, bedarf es einen strukturierten Umgang mit diesen Risiken. Den Rahmen dafür bildet der Risikomanagementprozess. Beginnend mit der Risikoidentifikation werden die Risiken im Laufe des Prozesses noch bewertet, aggregiert und durch Risikosteuerungsmaßnahmen gemindert oder sogar ganz vermieden. Die Risikoidentifizierung ist deshalb so wichtig, weil ein Unternehmen zunächst einmal wissen muss, welchen Risiken es überhaupt ausgesetzt ist, um überhaupt geeignete Maßnahmen einleiten zu können (vgl. Siemens und Dahms 2014, S. 1).

Ziel der Risikoidentifizierung ist es, alle aktuellen, zukünftigen und potenziellen Einzelrisiken für das Unternehmen aufzudecken und zu erfassen. Denn werden Risiken nicht identifiziert, werden sie im Risikomanagementprozess auch nicht weiter betrachtet (vgl. DIN 2010, S. 10).

2.1.1 Anforderungen an die Risikoidentifizierung

Da die Risikoidentifizierung als Grundlage für alle anderen Schritte im Risikomanagementprozess dient, sollte sie möglichst strukturiert in einem Unternehmen durchgeführt werden. Um dies zu gewährleisten, müssen bestimmte Anforderungen an die Identifizierung gestellt werden. Die geläufigsten Anforderungen sind folgende fünf (vgl. Rohlfs 2018, S. 98):

1. Vollständigkeit,
2. Wirtschaftlichkeit,

3. Zukunftsbezogenheit,
4. Aktualität,
5. Konsistenz.

Bezüglich der **Vollständigkeit** muss darauf geachtet werden, dass die Risikoidentifikation möglichst detailliert und lückenlos erfolgt. Dabei sollen alle aktuellen, zukünftigen sowie potenziellen Risiken aufgedeckt werden. Wird diese Anforderung nicht eingehalten, dann besteht die Gefahr, dass einzelne Risiken nicht erkannt werden. Diese können dann logischerweise nicht im weiteren Verlauf des Prozesses berücksichtigt werden, sodass das Unternehmen keine Möglichkeit hat geeignete Gegenmaßnahmen einzuleiten und im schlimmsten Fall durch diese nicht erkannten Risiken in der Zukunft Verluste erleidet (vgl. Diederichs 2018, S. 93).

Bei der Anforderung an die **Wirtschaftlichkeit** geht es darum, eine Kosten-Nutzen-Betrachtung durchzuführen. Hierbei sollen die Kosten, die ein Risikoidentifizierungsprozess verursacht, in Relation zum Nutzen, also der Menge und der Qualität der erzielbaren Erkenntnisse, gesetzt werden. Dabei kommt es vor allem darauf an, nur die wesentlichen Risiken zu erfassen (vgl. Rohlfs 2018, S. 98). Nimmt die Risikoidentifizierung beispielsweise eine erhebliche Zeit in Anspruch und bindet damit wertvolle Mitarbeiterressourcen, gleichzeitig wurden aber bereits alle wesentlichen Risiken aufgedeckt, dann ist es unwirtschaftlich für das Unternehmen den Identifizierungsprozess weiter laufen zu lassen und nur noch Risiken zu erfassen, welche lediglich einen geringen Einfluss auf das Unternehmen haben. Genauso ist es bei der Methodenwahl. Es sollten nach Möglichkeit nur die wirtschaftlich sinnvollsten Methoden für das Unternehmen gewählt werden (vgl. Siemens und Dahms 2014, S. 10).

Auch sollte eine Risikoidentifizierung immer **zukunftsbezogen** erfolgen. Das heißt, dass das Unternehmen vorausschauend denken muss und Veränderungen im Umfeld des Unternehmens mitberücksichtigen sollte. Diese Veränderungen sollten vom Unternehmen sowohl prospektiv als auch antizipativ betrachtet werden. Bei der prospektiven Betrachtung wird versucht aus den Vergangenheitsdaten zu analysieren, welche Risiken in Zukunft entstehen könnten, wobei zum Beispiel erkennbare Trends weiterverfolgt werden können. Bei der antizipativen Betrachtung geht es um die von Vergangenheitsdaten losgelöste Suche nach Risiken, die in Zukunft das Unternehmen gefährden könnten (vgl. Rohlfs 2018, S. 98).

Hinsichtlich der **Aktualität** ist gefordert, dass die Risikoidentifizierung kontinuierlich und frühzeitig durchgeführt wird. Durch das sich immer verändernde Umfeld des Unternehmens ist es wichtig, jederzeit die aktuelle Situation abzubilden und regelmäßig neu die Risiken zu identifizieren. Vor allem sollte diese Identifizierung aber früh genug geschehen, um noch rechtzeitig mit präventiven Maßnahmen agieren zu können. Wurde ein Risiko zu spät identifiziert, kann das Unternehmen oft nur noch reagieren, was bedeutet, dass das Risiko bereits eine tatsächliche Gefahr für das Unternehmen darstellt (vgl. Diederichs 2018, S. 93).

Des Weiteren sollte die Anforderung einer **konsistenten** Risikoidentifizierung beachtet werden. Hierbei geht es darum, dass Risiken möglichst eindeutig und überschneidungsfrei identifiziert werden. Diese Anforderung dient als Vorarbeit für die auf die Risikoidentifizierung folgende Risikoklassifizierung. Wurden die Risiken eindeutig und überschneidungsfrei erfasst, ist eine spätere Klassifizierung einfacher vorzunehmen. Diese sind für den weiteren Verlauf des Risikomanagementprozesses wichtig, da beispielsweise gleichartige Risiken bei der Risikobewertung auch gleichen Bewertungsgrundsätzen unterliegen (vgl. Rohlfs 2018, S. 99).

Wie in den näheren Beschreibungen zu den Anforderungen zu sehen ist, kann ein Unternehmen nicht alle Anforderungen gleichzeitig optimieren. So stehen beispielsweise die Vollständigkeit und die Wirtschaftlichkeit einer Risikoidentifizierung in Konkurrenz zueinander. Ein Unternehmen kann also nur für sich individuell priorisieren, welche Anforderungen an erster Stelle stehen und muss dann bei der Optimierung der Anforderungen Kompromisse eingehen (sogenannter Trade-off; vgl. Diederichs 2018, S. 94).

2.2 Durchführung der Risikoidentifizierung

Unter Beachtung der allgemeinen Anforderungen an die Risikoidentifizierung gibt es verschiedene Ansätze, wie an die Identifizierung von Risiken herangegangen werden kann und auch diverse Methoden, die dabei verwendet werden können.

2.2.1 Ansätze zur Herangehensweise an die Risikoidentifizierung

Wie ein Unternehmen bei der Risikoidentifizierung vorgeht, hängt vor allem von seinen Interessenschwerpunkten ab und aus welcher Perspektive es auf die Risiken blickt. Je nach Perspektive wird die Risikoidentifizierung beispielsweise ausgehend von den Risikoursachen oder auf der Ebene des Unternehmensmanagement durchgeführt. Generell können vier allgemein gültige Ansätze unterschieden werden, wie in Abb. 2.1 dargestellt.

Bei dem **progressiven Ansatz** werden die Risiken des gesamten Unternehmens ausgehend von den Risikoquellen des Unternehmens identifiziert. Zunächst fragt sich das Unternehmen, in welchen Bereichen des Unternehmens Risiken auftreten können, um risiko-

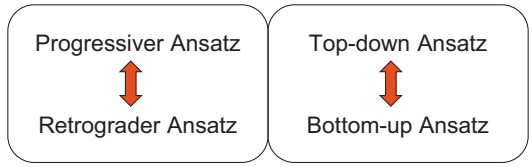

Abb. 2.1 Vier Ansätze zur Herangehensweise an die Risikoidentifizierung. (Quelle: eigene Darstellung in Anlehnung an Rohlfs 2018, S. 99)

behaftete Unternehmensbereiche aufzudecken. Dann werden die Ursachen für diese Risiken bestimmt, indem die Entstehung eines Risikos solange zurückverfolgt wird, bis die Risikoquelle gefunden ist. Im Anschluss wird dann erst geschaut, wie sich die Risikoquellen auf die Unternehmensziele auswirken können. Die Risikoquellen werden hiermit also als der Ursprung des Risikowirkungsprozesses gesehen, der die Unternehmensziele oder -strategie gefährden kann. Dieser Ansatz führt zu einer nahezu vollständigen Erfassung von Risiken, da das gesamte Unternehmen auf alle Risikoquellen hin untersucht wird (vgl. Diederichs 2018, S. 95).

Beim **retrograden Ansatz** hingegen bilden die vorhandenen Unternehmensziele und -strategien die Ausgangsbasis. Hierbei werden direkt die Risiken identifiziert, die unmittelbare Auswirkungen auf diese Ziele und Strategien haben. Dafür müssen zunächst alle definierten Ziele aus den verschiedenen Unternehmensebenen und auch die Ziele des Gesamtunternehmens als Grundlage herangezogen werden. Wurden in einer Unternehmensebene noch keine Ziele formuliert, müssen diese erst einmal hergeleitet werden. Dann wird untersucht, welche Risiken das Unternehmen daran hindern können, diese definierten Ziele zu erreichen. In welchen Unternehmensbereichen diese Risiken verursacht werden, wird erst anschließend betrachtet. Der Vorteil dieses Ansatzes liegt darin, dass Risiken zielgerichteter gesucht und identifiziert werden. Dies ist in der Regel weniger aufwändig als der progressive Ansatz und geht daher oft schneller (vgl. Diederichs 2018, S. 96).

Bei dem **Top-down-Ansatz** beginnt die oberste Ebene des Unternehmensmanagements mit der Risikoidentifizierung, bevor die nachfolgenden Hierarchieebenen den Prozess der Risikoidentifizierung fortsetzen. Dieser Ansatz hat den Vorteil, dass die relevanten Risiken zügig identifiziert werden und der Aufwand relativ gering ist. Allerdings kann es hierbei auch vorkommen, dass die relevanten Risiken, die in den unteren Unternehmensebenen später noch identifiziert werden, nicht mehr zusammengetragen werden und mögliche Abhängigkeiten zwischen verschiedenen Risiken nicht erkannt werden, was ein Nachteil dieses Ansatzes ist (vgl. Sartor und Bourauel 2013, S. 41).

Im Gegensatz dazu wird beim **Bottom-up-Ansatz** auf der niedrigsten Hierarchieebene in den operativen Einheiten des Unternehmens mit der Risikoidentifizierung begonnen. Die Mitarbeiter dort identifizieren die Risiken unmittelbar, mit welchen sie bei ihrer täglichen Arbeit konfrontiert werden können. Danach geht der Risikoidentifizierungsprozess weiter auf die oberen Hierarchieebenen. Der Vorteil dabei ist, dass wenn die Risikoidentifizierung auf der obersten Managementebene endet, dort alle relevanten Risiken an einer zentralen Stelle zusammengetragen wurden. Die Kehrseite dieser vollständigen Erfassung ist jedoch der hohe Aufwand, der dafür betrieben werden muss (vgl. Sartor und Bourauel 2013, S. 41).

Durch die Ausdifferenzierung dieser vier Ansätze soll jedoch nicht der Eindruck entstehen, dass ein Unternehmen sich für einen einzigen davon entscheiden muss. Oft ist es sogar sinnvoll mehrere Ansätze miteinander zu kombinieren. So kann nach einer zunächst einmal retrograden Identifizierung von Risiken der progressive Ansatz genutzt werden, um im Sinne einer vollständigen Erfassung weitere Risiken zu ermitteln. Oder es erfolgt erst eine grobe Identifizierung der relevanten Risiken nach dem Top-down -Ansatz, bevor

diese Identifizierung durch den Bottom-up Ansatz noch weiter konkretisiert wird (vgl. Rohlfs 2018, S. 100 f.).

Um zu zeigen, dass diese Ansätze auch in der Unternehmenspraxis angewendet werden, soll die Henkel AG & Co. KGaA als Praxisbeispiel dienen. In diesem Unternehmen findet einmal jährlich eine Risikoinventur statt, bei der die Unternehmensrisiken identifiziert werden. Die Risikoinventur beginnt sowohl in den lokalen Forschungs- und Entwicklungsstandorten als auch in den lokalen Produktions- und Vertriebsstandorten der verschiedenen Länder, in denen Henkel tätig ist. Bei Betrachtung der Unternehmenshierarchie fällt auf, dass dies die niedrigste Hierarchieebene des Unternehmens ist. Nachdem die Identifizierung auf Länderebene stattgefunden hat, geht der Risikoidentifizierungsprozess weiter bei den Experten der einzelnen Unternehmensbereiche und Zentralfunktionen. Zuletzt werden alle identifizierten Risiken im Bereich Corporate Accounting zusammengetragen. Ein solches Vorgehen bei der Risikoidentifizierung ist ein gutes Beispiel für einen Bottom-up-Ansatz. Neben der jährlichen Risikoinventur ist nicht auszuschließen, dass eine weitere Risikoidentifizierung nach anderen Ansätzen im Unternehmen durchgeführt wird (auch ad hoc) (Henkel AG & Co. KGaA 2018, S. 107 f.).

2.2.2 Methoden zur Risikoidentifizierung

Es gibt diverse Methoden zur Risikoidentifizierung und für ein Unternehmen ist es wichtig, möglichst viele von ihnen zu kennen. Denn wenn ein Unternehmen weiß, welche Methoden es gibt, kann es die vorteilhaften Methoden für den eigenen Risikoidentifizierungsprozess auswählen. Werden Methoden gewählt, die für die jeweilige Zielsetzung unpassend sind, kann dies zur Folge haben, dass die Unternehmensrisiken unzureichend identifiziert werden, was wiederum negative Folgen für die weiteren Schritte im Risikomanagementprozess hat.

Generell können die Methoden in zwei Gruppen unterteilt werden. In Managementmethoden sowie Methoden zur Informationssammlung und -generierung. Bei den Managementmethoden handelt es sich um Ansätze, die zur Bildung der Geschäfts- und Risikostrategie dienen, mit denen aber auch Risiken aufgedeckt werden können. Bei der zweiten Gruppe werden Informationen zunächst nur generiert und gesammelt, können aber dann auch für die Managementmethoden genutzt werden, wo sie weiterverarbeitet werden (vgl. Rohlfs 2018, S. 103). In diesem Kapitel soll nur eine grobe Übersicht über risikoidentifizierende Methoden gegeben werden, sodass nicht alle existierenden Methoden genannt werden können.

2.2.2.1 Managementmethoden

Die Managementmethoden werden zunächst in Ansätze unterschieden, die sich auf die unternehmensinternen Risiken fokussieren, und andere, die sich auf Risiken fokussieren, die außerhalb das Unternehmen entstehen können. Bei den Methoden mit dem internen Fokus kann entweder der retrograde Ansatz gewählt werden, indem die Unternehmens-