Stefan Hunziker
Jens O. Meissner *Hrsg.*

Ganzheitliches Chancen- und Risikomanagement

Interdisziplinäre und praxisnahe Konzepte

Springer Gabler

Ganzheitliches Chancen- und Risikomanagement

Stefan Hunziker · Jens O. Meissner
(Hrsg.)

Ganzheitliches Chancen- und Risikomanagement

Interdisziplinäre und praxisnahe Konzepte

Mit einem Geleitwort von Mira Walther

Springer Gabler

Herausgeber
Stefan Hunziker
Hochschule Luzern – Wirtschaft
Zug, Schweiz

Jens O. Meissner
Hochschule Luzern – Wirtschaft
Luzern, Schweiz

ISBN 978-3-658-17723-2 ISBN 978-3-658-17724-9 (eBook)
DOI 10.1007/978-3-658-17724-9

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

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

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

Geleitwort

In meiner Funktion als Leiterin Konzernrisikomanagement bei der Schweizerischen Post AG bin ich für die Umsetzung, den Betrieb und die Optimierung des ganzheitlichen Risikomanagements zuständig. Über Risikomanagement wurde in den letzten zehn Jahren – auch in der Schweiz – viel geforscht, viel diskutiert und viel veröffentlicht. Je nach Disziplin und beruflichem Hintergrund haben Forschende, Beratende, Risikomanagerinnen und -manager, Versicherungsexperten und weitere am Risikomanagement beteiligte Interessensgruppen zahlreiche Ansätze und Instrumente entwickelt, wie Unternehmen mit Chancen und Risiken umgehen sollten. Meine Erfahrung zeigt jedoch, dass das Verständnis der unterschiedlichen Akteure zum Themenkomplex Risikomanagement immer noch sehr verschieden ausfällt und sich bis anhin kein Best-Practice-Standard durchgesetzt hat.

Die Schweizerische Post hat in den letzten Jahren ein ganzheitliches Risikomanagement-Konzept eingeführt, das in einem hohen Maße auf quantitativen Risikokennzahlen wie z. B. dem Risikoappetit und der Risikotragfähigkeit im Zusammenhang mit der Eigenkapitalallokation beruht. Unser Risikomanagement unterstützt die Konzernsteuerung, indem es die entscheidungsrelevante Risiko- und Chancensituation aufzuzeigen vermag. Wir verfügen über eine Vielzahl von Werkzeugen, um risikoinduzierte Volatilitäten aufzuzeigen, zu analysieren sowie deren Steuerung sicherzustellen. Trotz allen Kennzahlen, die ein umfassendes Risikomanagement liefern kann, dürfen weitere wichtige Eigenschaften nicht zu kurz kommen. Einerseits ist eine angemessene Risikokultur zentral, die eine aktive und offene Kommunikation auf und zwischen allen Hierarchieebenen unterstützt. Andererseits ist es schwierig, gewisse „schwache Signale“ am Horizont rechtzeitig zu erkennen und in Volatilitäten zu übersetzen, die einen Einfluss auf die Ausschöpfung der Erfolgspotenziale der Schweizerischen Post haben könnten. Schließlich besteht die grundsätzliche Herausforderung darin, Risikomanagement als effektives und effizientes, unabdingbares Führungsinstrument langfristig zu etablieren.

Forschung und Praxis sind sich einig – modernes Risikomanagement, auch als Enterprise Risk Management (ERM) bezeichnet, steckt noch in den Kinderschuhen. Wer nach einem allgemein gültigen ERM-Standard sucht, der alle Bedürfnisse abdecken kann, wird momentan nicht fündig. Es lohnt sich also das Themengebiet aus verschiedenen

Blickwinkeln zu betrachten, die für das jeweilige Unternehmen den einen oder anderen Denkansatz enthalten, um das Risikomanagement wieder einen Schritt weiterzubringen. Auch die Forschung profitiert davon, einen relativ offenen, unvoreingenommenen Ansatz zu verfolgen, der neue Lösungen zulässt.

Das vorliegende Herausgeberwerk wird diesem Ansatz gerecht und bietet dem Praktiker und Wissenschaftler gleichermaßen wertvolle Gedankenansätze. In pragmatischer Weise wird die noch junge Disziplin aus verschiedenen Perspektiven beleuchtet. Relevante Themenfelder wie die Diskussion von Bewertungsmethoden, Ansätze zur Steigerung der Robustheit von Unternehmen gegen Risiken sowie die Auseinandersetzung mit dem Nutzen der Risikoberichterstattung werden aufgegriffen und kritisch diskutiert. Konkrete Anwendungsbeispiele und Handlungsanleitungen in diesem Herausgeberwerk erleichtern dem Praktiker, sich kritisch mit dem eigenen Risikomanagement auseinanderzusetzen und dieses gegebenenfalls zu optimieren. Ich wünsche Ihnen viele „Aha-Erlebnisse“ beim Lesen und viel Erfolg bei der Weiterentwicklung Ihres strategischen Führungsinstruments „Risikomanagement“!

Mira Walther
Leiterin Konzernrisikomanagement
Die Schweizerische Post AG

Vorwort

> Enterprise Risk Management is an evolving discipline focused on a complex and still imperfectly-understood subject. In such a situation, science is advanced best by collecting data from multiple, independent sites. (Kaplan 2015, S. xiii).[1]

Das ist ein Zitat von Professor Kaplan, Senior Fellow, Marvin Bower Professor of Leadership Development, Harvard Universität. Seine Aussage ist stellvertretend für das, was wir auch im deutschsprachigen Raum zur jungen Disziplin Enterprise Risk Management (im Folgenden ERM) feststellen: ERM wird in der Forschung, Beratung und Praxis sehr verschieden interpretiert und gelebt. Unter dem Schlagwort ERM verbergen sich häufig noch traditionelle Risikomanagement-Ansätze, die einen starken Fokus auf den Finanzbereich aufweisen und keinen Bezug zur strategischen Unternehmenssteuerung erkennen lassen. Ein unternehmensweites, gleichberechtigtes Management aller Risikokategorien in einem konsistenten ERM-Framework fehlt. Zahlreiche ERM-Projekte scheitern an deren Komplexität und am Aufwand. Eine positive Risikokultur, die aus dem ERM generierte Informationen zur Unterstützung der Unternehmenssteuerung als Selbstverständnis versteht, ist leider häufig Wunschdenken.

Modernes Risikomanagement hat den Anspruch, ein strategisches Führungsinstrument zu sein, das Werte für das Unternehmen schafft. Die Forschung ist darum bemüht, mit aufwendigen Datenerhebungen und komplexen multivariaten Datenanalysen solche Werte sichtbar zu machen, aber nur teilweise mit Erfolg. Die Übertragbarkeit der Forschungsergebnisse in die Praxis ist schwierig, da sich keine konkreten Handlungsempfehlungen für das eigene Unternehmen ableiten lassen, wie ERM tatsächlich umgesetzt werden soll. Klar ist, dass sich ERM als Begriff für modernes, strategieorientiertes Risikomanagement etabliert hat. In der praktischen Umsetzung und akademischen Validierung stehen wir jedoch noch ganz am Anfang.

Das vorliegende Herausgeberwerk folgt den Gedanken von Professor Kaplan und beleuchtet die komplexe Thematik aus verschiedenen und unabhängigen Perspektiven,

[1] Kaplan RS (2015) Foreword. In: Fraser J, Simkins B, Narvaez K (Hrsg.) Implementing Enterprise Risk Management: Case Studies and Best Practices. Wiley, Hoboken, N.J.

um die Forschung und Praxis einen Schritt weiter zu bringen. Die vorliegenden Erkenntnisse und Empfehlungen zu ERM mit all seinen Facetten basieren auf Forschungsprojekten, Praxiserfahrungen der Autoren und zahlreichen formellen und informellen Diskussionen mit Risikomanagern, Vorstandsmitgliedern, Aufsichtsräten und internen Revisoren.

Vor dem Hintergrund dieses Wissens haben wir das vorliegende Herausgeberwerk wie folgt strukturiert:

Im ersten Kapitel werden die Erfolgskriterien definiert, die für ein entsprechendes, angewandtes ERM-Rahmenwerk gültig sind. Unter ERM wird dabei ein unternehmensweit abgestimmter Prozess verstanden, mit dem Unternehmen alle Schlüsselrisiken identifizieren, bewerten und aktiv steuern, um Unternehmenswerte für die Anspruchsgruppen zu generieren. Ausgehend von dieser Definition wird im Kapitel erläutert, welche zentralen Erfolgskriterien modernes Risikomanagement ausmachen und worauf in der Praxis besonders geachtet werden muss, damit die Erfolgspotenziale von ERM ausgeschöpft und Unternehmenswerte geschaffen werden können.

Noch einen Schritt weiter geht es im darauf folgenden Kapitel, wenn der Bezug von ERM zur „organisationalen Resilienz“ untersucht wird. Der Umgang mit Ungewissem erfordert von Organisationen eine Resilienzkompetenz. Diese muss organisationale, individuelle und teamorientierte Faktoren berücksichtigen und bestehende Konzepte integrieren. Zudem gilt es, die eigenen, kritischen Aktivitäten analytisch zu bewerten. Im Kapitel wird hierzu das Instrument der „Funktionalen Resonanzanalyse“ verwendet und illustriert.

Im anschließenden dritten Kapitel wird das Thema „Schutz kritischer Infrastrukturen“ systematisch aufbereitet. Das Kapitel zeigt die Relevanz kritischer Infrastrukturen für moderne Volkswirtschaften und Gesellschaften auf und weist auf die Herausforderungen hin, die mit dem Schutz solcher Infrastrukturen verbunden sind. Unter Bezugnahme auf das Konzept der Resilienz wird ein Lösungsansatz vorgestellt und mit einer Übersicht über verschiedene nationale und internationale Bestrebungen zum Schutz kritischer Infrastrukturen illustriert. Dabei wird deutlich, dass effektive Ansätze nicht nur auf der staatlichen, sondern auch auf der einzelbetrieblichen Ebene eines Infrastrukturbetreibers ihren Niederschlag finden müssen und dass eine intensive Zusammenarbeit zwischen diesen beiden Ebenen unabdingbar ist. Der Schutz kritischer Infrastrukturen ist mehr oder weniger eine Regulierung, die insbesondere großen Infrastrukturbetreibern spezifische ERM-Aktivitäten vorgibt, dort also weniger Wahlmöglichkeiten bestehen – aber umso mehr Compliance erforderlich ist.

Das nächste Kapitel wagt danach eine Standortbestimmung von ERM bei Schweizer Unternehmen und rundet das Informationsangebot zum ERM generell ab. Die Analyse basiert auf dem im Jahr 2016 veröffentlichten COSO-Rahmenkonzept-Entwurf „Enterprise Risk Management – Aligning Risk with Strategy and Performance“. Im Kapitel wird der aktuelle Stand aufgezeigt und kritisch beleuchtet. Die Analyse wurde anhand

der fünf Komponenten des neuen COSO Frameworks gegliedert. Es offenbaren sich mehrere Baustellen in der Unternehmens-ERM-Themenlandschaft. Zentral scheint unter anderem die kontinuierliche Bearbeitung der Risikokultur.

Ein weiteres Spezialthema ist das der Risikoberichterstattung. In der Schweiz müssen Unternehmen, die nach dem Rechnungslegungs-Standard IFRS ihre Jahresrechnung präsentieren, keine Informationen über die Durchführung einer Risikobeurteilung im Sinne des Schweizer Gesetzes offenlegen. Zu erwähnen ist jedoch, dass unter IFRS Offenlegungspflichten existieren, welche Elemente der Lageberichterstattung gemäß Schweizerischem Obligationenrecht enthalten. Beim Lagebericht nach neuem Rechnungslegungsrecht steht die Vermittlung des Gesamtbilds der Unternehmenslage im Zentrum. Praktisch stellen sich hier viele Fragen. Im Kapitel wird darauf eingegangen, wie die Risikoberichterstattung im Geschäftsbericht positioniert ist, wie die Inhalte des Risikoberichts ausgestaltet sind und wie detailliert die Angaben sind resp. sein sollten.

Das sechste Kapitel ist den „Risiken bei Generierung von Wachstumsoptionen“ gewidmet. Der Aufbau neuer Geschäftsfelder im dynamischen Unternehmensumfeld ist mit zahlreichen Herausforderungen und Unsicherheiten verbunden. Notwendig ist hier ein aktives Management nicht nur von Strukturen und Prozessen, sondern auch der Kernkompetenzen. Zur Herstellung von Innovationsdynamik werden verschiedene Empfehlungen formuliert: die Akzeptanz von Unsicherheit und begrenztem Wissen, die Schaffung einer offenen Unternehmenskultur, die Förderung von Experimenten in den Geschäftsbereichen, eine beschleunigte Aufnahme von externem Wissen sowie die Implementierung von Ergebnisverantwortung in den einzelnen Geschäftssparten.

Schließlich widmet sich das letzte Kapitel dem Thema des „Business Continuity Management“ (BCM). Dieser Beitrag stellt eine Einführung ins BCM für Risikomanagende zur Verfügung und erläutert dazu zentrale Konzepte, wie die Business Impact Analyse, Business Continuity Pläne, Wiederanlauf und Wiederherstellung. Da BCM heute als standard- und regulierungsgetriebene Fachdisziplin wahrgenommen werden kann, wird auch kurz auf die verschiedenen heute gebräuchlichen Standards bzw. Normen für BCM eingegangen. Die Unterschiede in der grundsätzlichen Denkweise zwischen BCM-Praxis (Business Continuity Planern) und ERM-Praxis wird deutlich. Hier wird zum sauberen Anschluss von BCM und ERM angeregt, die Gemeinsamkeiten und Synergiepotenziale zwischen den beiden Fachbereichen zu suchen und zu betonen. Dabei kann BCM als Element des ERM verstanden werden, das folgenschwere Risiken im Zusammenhang mit Betriebsunterbrechungen mittels spezifischer Instrumente identifiziert und reaktive Maßnahmen dafür entwickelt, welche letztendlich die Resilienz der Organisation stärken.

Der vorliegende Herausgeberband hält also ein reichhaltiges Programm parat und richtet sich an alle Leser, die Aufgaben in einem ganzheitlichen Risikomanagement übernehmen oder als Risikomanager tätig sind, und über die Grenzen der reinen

Risikoverwaltung hinausblicken möchten. Ebenfalls angesprochen sind alle, die zum Thema ERM forschen und lehren. Bevor wir uns nun aber vertieft mit wichtigen Aspekten von ERM auseinandersetzen, wollen wir uns ganz herzlich bedanken:

- bei allen Autoren dieses Herausgeberwerks, die sich mit viel Engagement und Herzblut ihren Beiträgen gewidmet haben;
- bei allen Risikomanagern, die uns im Verlauf der letzten zehn Jahre bereitwillig Einblick in ihre Arbeit gewährten;
- bei Herrn Marcel Fallegger der Hochschule Luzern – Wirtschaft, der uns neben seinem Fachbeitrag in allen administrativen Belangen wesentlich unterstützt hat;
- beim Departement Wirtschaft der Hochschule Luzern, das dieses Projekt finanziell unterstützt hat;
- bei allen Kolleginnen aus dem Lektorat, der Herstellung und dem Marketing für die großartige Unterstützung und die Ermöglichung dieses Herausgeberwerks;
- bei unseren Angehörigen für die Geduld und das Verständnis für die etlichen „schreibbedingten Abwesenheiten".

Wir wünschen Ihnen zahlreiche „Aha-Erlebnisse" bei der Lektüre, viel Erfolg bei der Umsetzung oder Weiterentwicklung Ihres Enterprise Risk Managements und spannende Inputs, die Sie in Ihre eigenen Praxis-, Forschungs- und Beratungstätigkeiten einfließen lassen können.

Zug — Stefan Hunziker
Luzern — Jens O. Meissner
Juni 2017

Inhaltsverzeichnis

Erfolgskriterien von Enterprise Risk Management in der praktischen Umsetzung

1

Stefan Hunziker

Zusammenfassung

Unter Enterprise Risk Management (ERM) wird ein unternehmensweit abgestimmter Prozess verstanden, mit dem Unternehmen alle Schlüsselrisiken identifizieren, bewerten und aktiv steuern, um Unternehmenswerte für alle Anspruchsgruppen zu generieren. Ausgehend von dieser Definition wird in diesem Kapitel erläutert, welche zentralen Erfolgskriterien modernes Risikomanagement ausmachen und worauf in der Praxis besonders geachtet werden muss, damit die Erfolgspotenziale von ERM ausgeschöpft und Unternehmenswerte geschaffen werden können. Insbesondere scheint es schwierig, die vom Aufsichtsorgan verabschiedete schriftliche Risikopolitik in beobachtbares Verhalten (Risikokultur) zu überführen. Unter anderem bedingt dies ein konsequentes Vorleben und Kommunizieren der Wichtigkeit von ERM durch das Management. Im Unternehmen muss es Anreize geben, damit eine unternehmensweite Risikoidentifikation bzw. die Berichterstattung an entsprechende Stellen gefördert und nicht etwa verhindert wird. Es muss zum Selbstverständnis werden, dass Risiken eingegangen werden dürfen, so lange sie sich innerhalb der festgelegten Toleranzgrenzen befinden. Es muss ein Umdenken stattfinden, dass finanzielle Risiken in den meisten Industrieunternehmen nicht die wichtigste Risikokategorie ausmachen. Weiter wird eine positive Risikokultur unterstützt, wenn historisch gewachsene „Risiko-Silos“ überwunden und eine einheitliche ERM-Sprache unternehmensweit etabliert werden kann. Wenn es ein Unternehmen schafft, ERM als selbstverständlicher Teil des Prozesses der Strategieentwicklung und -umsetzung zu festigen, kann es sein wertgenerierendes Potenzial ausschöpfen.

S. Hunziker (✉)
Institut für Finanzdienstleistungen Zug IFZ,
Hochschule Luzern - Wirtschaft, Grafenauweg 10, 6302 Zug, Schweiz
E-Mail: stefan.hunziker@hslu.ch

S. Hunziker und J.O. Meissner (Hrsg.), *Ganzheitliches Chancen- und Risikomanagement,* DOI 10.1007/978-3-658-17724-9_1

1.1 ERM unternehmensweit einführen

Enterprise Risk Management (ERM) steht grundsätzlich für den modernen Risikomanagement-Ansatz und unterscheidet sich entsprechend in wichtigen Aspekten vom „traditionellen Risikomanagement". Obwohl zahlreiche Definitionen von ERM koexistieren, wird an dieser Stelle auf eine ausführliche Diskussion derselben verzichtet. Die nachfolgende Definition von ERM reflektiert aber im Wesentlichen die zentralen, modernen Eigenschaften und eignet sich zum weiteren Verständnis der Ausführungen gut.

▶ Modernes Risikomanagement ist ein unternehmensweit abgestimmter Prozess, mit dem Unternehmen alle Schlüsselrisiken identifizieren, bewerten und aktiv steuern, um Unternehmenswerte für alle Anspruchsgruppen zu generieren.

Ein in der Praxis häufig zu beobachtendes Phänomen ist die unvollständige Einführung von ERM. Unter anderem sind drei wichtige Gründe dafür zu nennen. Erstens werden bestimmte Unternehmensbereiche aus einer Gesamtoptik als nicht relevant genug eingestuft, da sie zu klein bzw. finanziell zu unwichtig erscheinen. Bei ERM-Projekten werden daher sogenannte Pilot-Bereiche oder -Abteilungen definiert, die z. B. wesentlich zur Gesamtrechnung beitragen und somit „wirtschaftlich relevant" erscheinen. Häufig wird dann aus Zeit- und Ressourcengründen davon abgesehen, zu einem späteren Zeitpunkt die als weniger prioritär definierten Bereiche auch noch dem ERM-Prozess zu unterziehen. Dies kann allerdings zu gefährlichen Situationen führen, denn in der Regel steht das unternehmerische Risiko nicht direkt in Relation zur „wirtschaftliche Bedeutung" eines Unternehmensbereichs. Das heißt, Risiken können z. B. in eher unauffälligen, stabilen und kleineren Geschäftsfeldern ihren Ursprung haben und sich später im Rahmen einer Kettenreaktion auf das Gesamtunternehmen negativ auswirken.

Zweitens fokussieren viele Unternehmen stark auf das finanzielle Risikomanagement bzw. auf finanzielle Risiken, was ebenfalls dem Kerngedanken von ERM widerspricht. Risiken lassen sich auf stark aggregierter Ebene in strategische, operative und finanzielle Risiken klassifizieren. Die Erfahrungen in der Praxis haben gezeigt, dass sich diese Grundkategorisierung bewährt und Risiken sich ursachenorientiert einer der Kategorien zuordnen lassen. Verschiedene Publikationen in jüngerer Zeit zeigen, dass das Interesse an ERM, z. B. in Schweizer Unternehmen, zu Recht stark angestiegen ist. Eine Auswertung der Vielzahl an Fachbeiträgen und Zeitungsartikeln zum Thema zeigt jedoch, dass sich die Debatte in den letzten Jahren stark um finanzielle Risiken gedreht hat, was unter anderem mit der Finanz- und Währungskrise zu erklären ist. Besonders Finanzinstitute sind Zielscheibe stetig wachsender regulatorischer Anforderungen geworden, so z. B. im Bereich der Eigenkapitalunterlegung. Aber auch in anderen Industrien sind finanzielle Risiken wichtiger geworden bzw. wird mehr darüber berichtet. Die „Währungskrise" hat viele Schweizer Exportunternehmen in Bedrängnis gebracht, professioneller mit Währungsrisiken und Maßnahmen zur Schadeneindämmung umzugehen. Aus einer ERM-Perspektive stellt sich die Frage, ob finanzielle Risiken tatsächlich für die meisten

Unternehmen Priorität haben müssen. Segal (2011) geht noch einen Schritt weiter und spricht offen über den „Mythos finanzieller Risiken“ (S. 28). Der systematische Umgang mit Finanzrisiken ist zweifelsfrei wichtig, aber macht zumindest für die meisten Nichtfinanz-Unternehmen nur einen oft unbedeutenden Anteil vom ganzen Risikogefüge aus, was diverse Studien (u. a. Hunziker 2014; Mercer 2000; PwC 2008; Segal 2011) klar zeigen. Werden die in den Studien identifizierten Risiken in die drei oben genannten Risikokategorien Strategie, operatives Geschäft und Finanzen eingeteilt, wird ersichtlich, dass die strategischen Risiken das mit Abstand größte Schadenspotenzial aufweisen, gefolgt von den operativen Risiken. In allen Studien richten die finanziellen Risiken den kleinsten relativen Schaden an.

Ein ganzheitlicher ERM-Ansatz postuliert somit zu Recht die gleichberechtigte Identifikation, Beurteilung und Steuerung von Risiken. Gleichberechtigt meint in diesem Zusammenhang, dass Risiken unternehmensweit, d. h. in allen Bereichen und über alle Kategorien hinweg vorbehaltslos identifiziert werden. Die Dominanz strategischer Risiken lässt sich weiter anhand der Bewertung von Unternehmen am Kapitalmarkt zeigen. So weisen Smit und Trigeorgis (2004) in ihren Berechnungen nach, dass je nach Industrie ca. zwischen 45 % und 90 % des Unternehmenswerts in künftig auszunutzenden strategischen Realoptionen (= Risiko-Chancen-Abwägungen) liegt (S. 6). Strategische Optionen (Chancenpotenziale) sind somit ein wesentlicher Werttreiber, anders als finanzielle Risiken. Die wichtigsten Risikoursachen lassen sich oft direkt in der Unternehmensstrategie bzw. deren Umsetzung im Tagesgeschäft (operative Risiken) eruieren. Solche Risiken und Chancen liegen etwa im technologischen Wandel, in der Digitalisierung von Geschäftsmodellen, in sich ändernden Kundenbedürfnissen, in regulatorischen Entwicklungen, in der wachsenden Konkurrenz oder in Fehlentscheidungen der strategischen Projektpriorisierung.

Nun stellt sich die Frage, wieso das Potenzial von ERM nicht über alle Bereiche und Risikokategorien ausgeschöpft wird. Drei Gründe können dafür identifiziert werden. Erstens wird es als schwierig erachtet, strategische und operative Risiken quantitativ zu bewerten, d. h. in Zahlen auszudrücken. Da die Modelle und Methoden des finanziellen Risikomanagements sich nicht auf andere Risikobereiche direkt übertragen lassen, fehlt oft Methoden-Know-how für die Bewertung anderer Risikobereiche. Auch fehlende historische Daten, die Abbildung komplexer Ursache-Wirkungsketten und keine Anwendungsmöglichkeiten stochastischer Modelle sind oft angeführte Argumente gegen die Quantifizierung nicht-finanzieller Risiken. Andere Ansätze wie z. B. Szenarioanalysen oder die Fehlermöglichkeits- und Einflussanalyse (FMEA), die oft auf Intuition und Erfahrung von Menschen basieren, sind teilweise zu wenig bekannt und können nicht modelltechnisch quantifiziert werden. Zweitens werden viele Risiken fälschlicherweise als „Finanzrisiken“ klassifiziert. Der Grund liegt in der Verwechslung von *Ursache* und *Wirkung* eines Risikos. Z. B. tendieren Menschen in Risiko-Workshops oder bei Brainstormings zur Risikoidentifikation dazu, an die Konsequenzen von Risiken (Wirkung, ultimativer Schaden) zu denken: Was passiert, wenn ein Risiko eintritt? Was hat es für finanzielle Auswirkungen auf meinen Verantwortungsbereich? Könnte der finanzielle

Schaden gefährliche Auswirkungen auf die Liquidität oder meine Jahresziele haben? Diese Überlegungen sind zwar ebenfalls relevant, aber nicht ausreichend. Unternehmensweites Risikomanagement muss primär bei den Risikoursachen ansetzen, um eine präventive Risikosteuerung sicherzustellen: Bei welchen Risikoursachen müssen Maßnahmen oder Kontrollen implementiert werden, damit es gar nicht zu einer negativen finanziellen Konsequenz kommt, wäre die korrekte Frage. Risiken, deren Ursachen z. B. im strategischen Bereich liegen, haben in letzter Instanz immer finanzielle Auswirkungen und werden deshalb oft (fälschlicherweise) als Finanzrisiken bezeichnet. Es geht also darum, identifizierte Risiken (Events) in eine plausible Geschichte zu verpacken, d. h. in eine Ursache-Wirkungskette einzubetten. Die Ursache, die an erster Stelle der Geschichte steht, ist in der Regel der korrekte Ansatzpunkt, um Risikomaßnahmen zu überlegen. Schließlich sind die Aus- und Weiterbildungen bzw. beruflichen Erfahrungen vieler Risikomanager anzuführen. In der Regel sind die spezifischen ERM-Methoden und der Fokus auf bestimmte Risikokategorien wesentlich durch den Risikomanager geprägt. Häufig sind es Spezialisten mit einem finanziellen Hintergrund oder Erfahrungen in der Finanzbranche, mit Aus- und Weiterbildung in Mathematik, Physik, Statistik und quantitativer Risikomodellierung. Daher ist es auch nicht erstaunlich, dass das ERM vor allem auf Finanzrisiken ausgerichtet ist, da die Bewertungsmethoden bekannt und stochastische Modelle verfügbar sind. Zudem ist es auch bemerkenswert, wie viel praxisorientierte und akademische Literatur zum finanziellen Risikomanagement existiert. Literatur mit einem Fokus auf strategisches Risikomanagement sucht man vergeblich (Hunziker 2015; Segal 2011, S. 28–31).

1.2 COSO ERM und ISO 31000 mit Bedacht umsetzen

Verantwortliche für Risikomanagement-Aufgaben sind oft mit der Frage konfrontiert, welches ERM-Rahmenwerk bzw. welche ERM-Norm für einen effektiven und effizienten Betrieb von ERM geeignet ist. Im Folgenden sollen aus einer Vielzahl koexistierender Frameworks die zwei bekanntesten und weltweit am meisten diskutierten und umgesetzten Rahmenwerke COSO ERM und ISO 31000:2009 aufgegriffen werden. Neben einem kurzen Blick auf die Gemeinsamkeiten und Unterschiede von COSO und ISO scheint insbesondere die Diskussion relevant, ob die beiden wichtigsten Rahmenwerke dem modernen Verständnis von ERM gerecht werden.

Grundsätze beider Normen

Beide Normen orientieren sich letztlich an den Unternehmenszielen und sollen die Zielerreichung positiv unterstützen. ERM muss somit zwingend mit der Unternehmensstrategie abgestimmt sein bzw. auch Einfluss darauf nehmen können. Entsprechend wird die Risikobeurteilung immer im Vergleich zu den gesetzten Zielen vorgenommen. Die Empfehlungen zum Umgang mit Unsicherheit gelten grundsätzlich für alle Organisationen und Branchen; jedoch verweisen beide Normen auf die Notwendigkeit der

unternehmensindividuellen Anpassung bei der Umsetzung. Entscheidend für den Erfolg von ERM ist gemäß COSO ERM und ISO 31000 der Management-Support („tone-at-the-top“) und damit verbunden eine positive Risikokultur. Die Risikokultur kann durch wiederholte Kommunikation und Information der Wichtigkeit von ERM gestärkt und verankert werden. Beide Normen postulieren eine Umsetzung von ERM über alle Hierarchiestufen, d. h. die Sensibilisierung auf ERM muss unternehmensweit geschehen, da alle Mitarbeitenden, inkl. der Führungsebene Teil des ERM sind. Ebenfalls weitgehend Konsens besteht in der Wichtigkeit einer klaren Zuordnung von Aufgaben, Kompetenzen und Verantwortlichkeiten innerhalb des ERM-Prozesses.

COSO ERM und ISO 31000 empfehlen verschiedene Methoden zur Risikoanalyse einzusetzen. Beide Standards weisen darauf hin, dass Abhängigkeiten zwischen Risiken identifiziert und beurteilt werden müssen und der gesamte ERM-Prozess regelmäßig überwacht werden soll. Letztlich erwähnen beide die Bedeutung eines angemessenen Kosten-Nutzen-Verhältnisses. Insgesamt weisen beide Rahmenwerke große Überschneidungen auf, was den grundsätzlichen ERM-Prozess betrifft, allerdings gibt es einige Unterschiede in der Bezeichnung der einzelnen Phasen.

Obwohl beide Normen wichtige Gemeinsamkeiten aufweisen, gibt es auch bemerkenswerte Unterschiede. Bei ISO 31000 werden Events mit positiver Auswirkung explizit gleichberechtigt im gesamten ERM-Prozess berücksichtigt, wobei COSO ERM nur Risiken mit negativer Konsequenz für die Bewertung und die weiteren Prozessschritte im ERM einbezieht. Chancen (Opportunities) werden zwar auch identifiziert, jedoch nicht mehr im Rahmen des ERM gesteuert. COSO ERM nennt zur Risikosteuerung vier mögliche Strategien: Verhindern, Reduzieren, Teilen und Akzeptieren. ISO 31000 hingegen definiert eine breitere Auswahl an Maßnahmen, die ebenfalls das Ausnutzen von Chancen vorsehen (z. B. unternehmerisches Gesamtrisiko erhöhen, falls es die Chance rechtfertigt). Ein weiterer Unterschied liegt in der Bewertung von Risiken. COSO ERM schlägt vor, Risiken lediglich auf Event-Ebene (z. B. Event „Gebäudebrand“, Event „Währungsrisiko“) einmalig mit Eintrittswahrscheinlichkeit und Schadensausmaß zu beurteilen. Es bleibt damit unklar, welches Brandszenario oder Währungsszenario in die Bewertung einfließt, da der Gebäudebrand und das Währungsrisiko verschiedene Auswirkungen haben können. ISO 31000 löst diese Problematik differenzierter, in dem die Risikobeurteilung auf Auswirkungs-Ebene vorgenommen wird und somit verschiedene Szenarien bewertet werden, was zu einer realistischeren Risikobeurteilung führt.

Der Fokus von ISO 31000 liegt generell stärker auf der „Wertkreierung“ als auf der „Schadenminimierung“ wie bei COSO ERM. Allerdings wird in der revidierten Version von COSO ERM (Publikation im Verlauf von 2017/2018 vorgesehen) ein stärkerer Bezug zwischen Risiko und Wertschaffung zu erwarten sein. Insgesamt ist ISO 31000 als Anleitung zur Umsetzung des ERM-Prozesses zu verstehen, wobei COSO ERM eher ein flexibler Standard zur Selbstevaluation des bestehenden ERM-Prozesses ist (DeLoach 2012).

Letztlich setzen die beiden Normen unterschiedliche Schwerpunktthemen. So diskutiert COSO ERM die Aspekte „Menschliches Verhalten im ERM“, „Definition von Risikoappetit“ sowie „Verbindung zur Strategie und den Unternehmenszielen“ differenzierter

als ISO. ISO 31000 hingegen beschäftigt sich u. a. stärker mit dem ERM-Vokabular, den Risikobewertungsmethoden und stellt einen stärkeren Bezug zur Entwicklung einer angemessenen Risikopolitik her. Schließlich ist noch zu erwähnen, dass ISO 31000 intuitiver, tendenziell praktikabler, kürzer (ca. 10 % von COSO ERM) und weniger redundant in den Ausführungen der einzelnen Prinzipien ist als COSO.

Eignung der beiden Normen für modernes ERM

Einleitend ist zu vermerken, dass beide Normen von ISO und COSO grundsätzlich komplementär nutzbar sind, da sie sie sich in vielen Bereichen ergänzen, beide durch die längere Entwicklungsgeschichte als ausgereift gelten, einen relativ umfassenden Blickwinkel auf ERM einnehmen und in sich weitestgehend konsistent sind. Allerdings gilt, dass diese Normen den Konsens von vielen unterschiedlichen Meinungsträgern widerspiegeln müssen und somit nur für den „Durchschnitt" gelten können. Innovationen in ISO und COSO finden sich keine, da sie kaum mehrheitsfähig und somit in den Normen nicht berücksichtigt sind (vgl. auch RiskSpotlight 2015). Die beiden Normen hinken somit den neueren Erkenntnissen und Entwicklungen von ERM zeitlich nach. Zudem gibt es bis anhin keine verlässlichen Studien, ob die beiden Normen tatsächlich in der Praxis funktionieren, d. h. Werte für Unternehmen schaffen. Es ist erstaunlich, dass nach 13 Jahren COSO ERM-Existenz immer noch keine Veröffentlichungen mit Unternehmensbeispielen vorliegen, die COSO ERM als Ganzes erfolgreich umgesetzt haben.

Beide Normen postulieren eine relativ vereinfachte Risikobeurteilung, wobei ISO 31000 differenzierter und sinnvoller vorgeht. Bei COSO ERM ist keine echte (d. h. quantifizierte) Risiko-Priorisierung möglich, zumal die alleinige Risikobewertung anhand Eintrittswahrscheinlichkeit und Schadensausmaß deutlich zu wenig weit greift. Beide Normen betonen zwar die Relevanz der Verknüpfung zum strategischen Management, jedoch bleibt unklar, wie der ökonomische Nutzen von ERM gerechtfertigt wird bzw. wie der Wertbeitrag von ERM in der Praxis gemessen werden kann. Dies wäre vor dem Hintergrund, dass viele Unternehmen den Nutzen von ERM (noch) zu wenig erkennen, sehr wichtig. Insbesondere sind bei der Abstützung auf COSO ERM folgende Aspekte kritisch zu hinterfragen:

- Die Risikoidentifikation sollte auch das externe Umfeld miteinbeziehen, COSO ERM ist aber stark organisationsintern ausgerichtet. Viele Risiken werden vernachlässigt, wenn kein unternehmensexternes Screening (Wettbewerber, Trends, Gesetzesentwicklungen, internationale Marktentwicklungen etc.) durchgeführt wird.
- COSO ERM ignoriert sogenannte „Black Swan"-Ereignisse, also Risiken mit sehr kleiner Eintrittswahrscheinlichkeit und großem Schadenspotenzial.
- COSO ERM spricht von Risk Events, also Risiken, die plötzlich akut werden können. Allerdings gibt es viele Risiken, die sich langsam manifestieren, teilweise über Monate oder Jahre (z. B. Änderungen Kundenbedürfnisse). Diese sich langsam abzeichnenden Risiken können mit „Events" nicht abgebildet werden. Zudem wird in COSO das negative Risiko (was kann schiefgehen?) in den Vordergrund gestellt. Dies

kann zu einer erheblichen Überbewertung des unternehmerischen Gesamtrisikos führen, wenn Chancen aus der Risikobetrachtung ausgeklammert werden. Ein besserer Ansatz wäre es, hier in Unsicherheiten oder Volatilitäten zu denken. Sie sind neutraler und können sowohl positive wie auch negative Abweichungen (= Szenarien) vom Erwarteten (= Plan, Ziele) bedeuten.

- Eher verwirrend und unrealistisch gestalten sich die Aussagen zum Risikoappetit von COSO ERM. Der Risikoappetit ist eine konkrete Aussage darüber, welche Arten von Risiken ein Unternehmen in welchem Ausmaß und zu welcher Eintrittswahrscheinlichkeit bewusst akzeptiert, um die Geschäftsziele erreichen zu können. Bei COSO ERM wird jedoch der Fokus primär auf das Schadenspotenzial, nicht aber auf die relevante Eintrittswahrscheinlichkeit gelegt, was dem Risikobegriff grundsätzlich widerspricht. COSO ERM schlägt vor, Unternehmen können sehr einfache, qualitative Aussagen zum Risikoappetit wie z. B. „Wir akzeptieren keine ernsthaften Risiken, die unsere Strategie gefährden können" formulieren. Solche Aussagen sind für Entscheidungsträger nutzlos, sie lassen sich nicht in konkrete Handlungsempfehlungen bzw. auf die operative Ebene ummünzen. Ein sinnvoll definierter Risikoappetit macht eine überprüfbare (quantifizierte) Aussage dazu, welches Risikoexposure aus Sicht des jeweiligen Unternehmens „erwünscht" ist. Der Risikoappetit muss auf die einzelnen Geschäftsziele „runtergebrochen" werden, damit die damit verbundenen Entscheidungen tatsächlich am Risikoappetit gespiegelt werden können.
- COSO ERM schafft es leider nicht, eine in der Praxis realisierbare Verbindung zwischen Risikoappetit und Entscheidungsprozessen herzustellen. Die in dem Risikoappetit formulierten Aussagen vom Aufsichtsorgan und der Geschäftsleitung müssen sich in das operative Risikomanagement übersetzen lassen, ansonsten bleibt die Formulierung eines Risikoappetits eine wirkungslose Worthülse.
- COSO ERM wird von vielen Praktikern als zu umfangreich, zu langatmig und zu „verordnend" beschrieben. Dies hängt auch damit zusammen, wer COSO ERM entwickelt hat: Im Wesentlichen sind es große US-amerikanische Accounting- und Revisions-Verbände, die ein gemeinsames Interesse an einem stark compliance-orientierten ERM-Prozess haben, der die Wichtigkeit interner Kontrolle und der internen Revision in den Vordergrund stellt.

Insbesondere COSO ERM, aber auch ISO 31000 adressieren eher große Unternehmen. Kleine und mittelständische Unternehmen können diese Rahmenwerke nur bedingt umsetzen und müssen eine hohe „Transformationsleistung" betreiben, an derer es oft scheitert. COSO ERM ist zwar ein Rahmenwerk, aber aufgrund seines stark accounting-orientierten Hintergrunds nicht unbedingt eines für modernes ERM. ISO 31000 hingegen wird dem modernen ERM-Ansatz stärker gerecht, da es ein Konsens von vielen Risikomanagement-Praktikern darstellt. Allerdings kann es nicht als komplettes und detailliertes Framework bezeichnet werden, da es einen zu hohen Abstraktionsgrad aufweist. Vielleicht wäre es eine sinnvolle Entwicklung, wenn COSO ERM die Grundgedanken von ISO 31000 im Prozessschritt der Risikobewertung berücksichtigt oder zumindest auf

ISO 31000 verweisen könnte. Um sich als Unternehmen allerdings vom „konsensorientierten Durchschnitt“ bez. Risikomanagement abzuheben, darf man sich nicht stark auf diese beiden Normen abstützen.

1.3 Die Krux mit dem Risikoappetit

Ein korrekt formulierter Risikoappetit macht konkrete Aussagen darüber, welches Maß an Risiko die Unternehmensleitung bewusst in Kauf nimmt, um die strategischen Erfolgspotenziale ausschöpfen bzw. die strategischen (Rendite-)Ziele erreichen zu können. Der Entscheid über den Risikoappetit wird vom Aufsichtsorgan gefällt. Es ist – in Abstimmung mit den Erwartungen der Anspruchsgruppen (oft Aktionäre) – ultimativ dafür verantwortlich, eine Aussage über die Risikobereitschaft des Unternehmens zu treffen. Ohne klar definierten Risikoappetit besteht keine Zielvorgabe an das ERM, worauf es sich ausrichten bzw. wohin es steuern soll. Letztendlich geht es im ERM darum, den tatsächlichen Gesamtrisikoumfang möglichst nahe an den Risikoappetit heranzuführen bzw. diesen anschließend dort mit einer bestimmten Toleranzgrenze zu halten. Die Erfahrungen aus der Praxis zeigen, dass der Risikoappetit oft falsch, ungenügend oder gar nicht definiert wird. Folgende Gründe können dafür verantwortlich gemacht werden: Häufig wird fälschlicherweise davon ausgegangen, dass der Risikoappetit berechnet werden kann und sich direkt aus dem ERM ableiten lässt. Das ist allerdings ein Trugschluss, der sich hartnäckig hält. Der Risikoappetit hat nichts mit der Risikobewertung oder dem aktuellen Risikoumfang zu tun. Er ist eine fundierte Beurteilung des Aufsichtsorgans – in Zusammenarbeit mit dem Risikokomitee – welches Maß an Risiko aus Sicht der Anspruchsgruppen maximal akzeptierbar ist. Dies ist erfahrungsgemäß ein schwieriger Prozess und erfordert viel Diskussion und Konsensbereitschaft (KPMG 2008).

In der Praxis wird der Risikoappetit häufig mit der Risikotoleranz (Synonym: Risikokapazität) gleichgestellt, obwohl es verschiedene Konzepte sind. Der Risikoappetit leitet sich von den Zielen des Unternehmens ab; es ist eine Aussage, wie viel Risiko das Unternehmen bez. Märkten, Dienstleistungen, Produkten etc. gewillt ist einzugehen, um die Unternehmensziele bzw. die gewünschte Rendite zu erreichen. Die Risikotoleranz hingegen ist das maximale Risikomaß, das ein Unternehmen tragen kann, damit es nicht illiquide oder insolvent wird, die gesetzlichen Auflagen nicht mehr erfüllen oder den Verpflichtungen gegenüber den Kunden und Lieferanten nicht mehr nachkommen kann.

Leider fällt es dem Aufsichtsorgan oft auch schwer, sich auf einen Konsens hinsichtlich des Risikoappetits zu einigen. Eine präzise, quantifizierte Aussage zum Risikoappetit schafft eine Transparenz, die teilweise gar nicht erwünscht bzw. unangenehm sein kann. Stellt sich etwa heraus, dass der aktuelle (berechenbare!) Risikoumfang den Risikoappetit überschreitet, kann das zu unschönen Situationen führen, die das Aufsichtsorgan zu Rechtfertigungen zwingt. Eine nachträgliche Anpassung des Risikoappetits an den tatsächlichen Risikoumfang kann die Glaubwürdigkeit des ganzen ERM-Programms erheblich reduzieren. Damit es nicht dazu kommen kann, ist es sinnvoller, den tatsächlichen Risikoumfang bereits vor der Diskussion um den Risikoappetit zu kennen.

Die Nutzenaspekte eines präzis definierten Risikoappetits sind mehrdimensional. Einerseits ist es ein Hilfsmittel, um Entscheide vor dem Hintergrund einer Risiko-Chancenabwägung begründet zu treffen. Die Auswirkungen eines Entscheids „Hinzufügen von Risiko" zum Gesamtrisiko werden transparenter: Lässt es der Risikoappetit zu, neue Erfolgspotenziale angehen zu können? Geht ein Unternehmen sogar zu wenig Risiko ein und verpasst so strategische Optionen? Der Risikoappetit stellt ebenfalls eine Leitlinie für die strategische Planung und den Budgetierungsprozess dar und fördert die Konsistenz in beiden Prozessen. Weiter kann eine effektive unternehmensweite Kommunikation des Risikoappetits zur Stärkung der Risikokultur beitragen. Es wird ein Bewusstsein geschaffen, dass das Eingehen von Risiken und Chancen konsequent an der maximal möglichen Risikokapazität reflektiert wird und Risiko per se nicht zu vermeiden ist. Schließlich wird die Risikoberichterstattung an das Aufsichtsorgan aussagekräftiger – der Vergleich zwischen dem Risikoappetit und dem Gesamtrisikoumfang ist wahrscheinlich eine der wichtigsten Informationen für die Unternehmensleitung in der ERM-Berichterstattung überhaupt (KPMG 2008, S. 10).

Auch die Kommunikation des Risikoappetits nach außen an die Anspruchsgruppen kann Nutzen stiften: Die Transparenz trägt zu einem besseren Erwartungsmanagement bei. Die Bemühungen um eine gute Corporate Governance werden transparent, was Signalwirkung haben kann. Ein angemessenes ERM mit einem klaren Bekenntnis zum Risiko schafft Vertrauen (Willis 2015, S. 5). Der Risikoappetit kann mehrdimensional operationalisiert werden, d. h. es können maximal akzeptierbare Veränderungen bez. Unternehmenswert, Reputation, Umsatzwachstum, Cashflow-Stabilität, Gewinn pro Aktie, Ratinglevel u. a. definiert werden. Es ist empfehlenswert, dass der Risikomanager vor dem Risikoappetit-Meeting bereits eine Dokumentation zum Gesamtunternehmensrisiko, zur Risikobewertung aller Top-Risiken mit verschiedenen Szenarien sowie einige Vorschläge zur Risikoreduktion bereithält. Vorschläge für risikosenkende Maßnahmen sind wichtig, falls ein Risikoappetit beschlossen wird, der kleiner als der Risikoumfang ausfällt. So hat das Aufsichtsorgan bereits Lösungsansätze zur Hand, wie der Risikoumfang reduziert werden könnte (Segal 2011, S. 231–232). Nachfolgend wird am Beispiel eines Unternehmens erläutert, wie ein Risikoappetit entwickelt bzw. formuliert werden kann.

Beispiel

Der ERM-Ausschuss eines Produktionsunternehmens mit zwei Geschäftsbereichen, bestehend aus fünf Mitgliedern (CEO, Geschäftsbereichsleitende A und B, Risikomanager, Finanzvorstand), hat den Auftrag, dem Aufsichtsorgan einen Vorschlag für den Risikoappetit zu unterbreiten. Es wurde in vorhergehenden Meetings bereits vorbesprochen, mit welchen Risikoparametern der Risikoappetit operationalisiert werden soll. Der Risikomanager spielt eine entscheidende Rolle in der Moderation dieser heiklen Diskussion. Er ist sich bewusst, dass die anwesenden Personen aus dem ERM-Ausschuss verschiedene Rollen und Interessen vertreten, was die Konsensfindung schwierig machen kann. Nach einer längeren Diskussion ist folgender Risikoappetit definiert worden, der noch vom Aufsichtsorgan abgesegnet werden muss.

Operationalisierte Dimensionen des Risikoappetits	Weiches Limit (Jahreswahrscheinlichkeit) (%)	Hartes Limit (Jahreswahrscheinlichkeit) (%)	IST-Jahreswahrscheinlichkeit (%)
Durchschnittlicher Umsatzverlust >10 % des vergangenen Drei-Jahres-Durchschnitts	15	20	10
Unternehmenswertverlust von >20 %	5	10	3
Ratingherabstufung um 1 Level	10	15	11
Reputationsverlust um >20 Indexpunkte		5	9
Gewinn je Aktie <30 Cent	10	15	12

Insgesamt hat sich der ERM-Ausschuss auf fünf operationalisierte Dimensionen geeinigt, wobei jede einzelne eine „kritische Schmerzgrenze“ des Unternehmens ausweist (vgl. Tabelle). In einem nächsten Schritt beurteilt der ERM-Ausschuss nun die bereits bekannten Eintrittswahrscheinlichkeiten der jeweiligen Szenarien im nächsten Jahr. Weiter hat der Ausschuss entschieden, weiche und harte Limiten zu definieren. Weiche Limiten können kurzzeitig überschritten werden, falls damit eine lohnenswerte Chance ausgenutzt werden kann. Harte Limiten dürfen zu keinem Zeitpunkt überschritten werden. Falls doch, muss der Risikoumfang durch Risikostrategien reduziert werden. In der Tabelle wird ersichtlich, dass bei zwei Risikodimensionen die weiche Grenze überschritten wird (Rating, Gewinn je Aktie), beim Reputationsverlust sogar das harte Limit.

Der Risikoappetit muss regelmäßig an neue Gegebenheiten angepasst werden. Das erfordert ein mindestens jährliches Überprüfen sowie ad-hoc Prüfungen bei sich abzeichnenden Veränderungen des Risikoumfangs (z. B. durch Zukäufe, Produktlancierungen, Eintritt neuer Wettbewerber oder regulatorische Veränderungen).

1.4 Zum korrekten Risikoverständnis im ERM-Ansatz

In der Praxis wurde und wird oft befürchtet, dass ERM als umfassender Ansatz unweigerlich die aktive Steuerung von hunderten oder von tausenden Risiken bedeutet. Insbesondere in den USA war eine große Skepsis vorhanden, dass ERM eine erweiterte Sarbanes-Oxley-Übung ist. Auch das Rahmenwerk COSO ERM hat diese Vermutung bekräftigt, da es eine Ergänzung von COSO IC darstellt, das ja primär für interne Kontrollsysteme (IKS) entwickelt wurde. ERM hat jedoch nicht zum Ziel, alle im Unternehmen identifizierten Risiken umfassend zu bewerten, zu steuern und zu überwachen. ERM