Veröffentlicht in

Wertorientiertes Risikomanagement für Industrie und Handel
(Hrsg. Werner Gleißner/Günter Meier)
2001

„Organisatorische Gestaltung von RisikoManagement-Systemen“

S. 199-232

Mit freundlicher Genehmigung des
Gabler Verlag, Wiesbaden
(www.gabler.de)

Organisatorische Gestaltung von Risiko-Managementsystemen

Bernd P. Mott

1. Vorbedingungen

Die Organisation eines Risiko-Managementsystem wird in der Regel eine Teilaufgabe innerhalb eines umfassenderen Projektes sein, das sich mit dem Aufbau eines Risiko-Managements für ein Unternehmen beschäftigt. Sinnvollerweise sollte daher der Organisation des Risiko-Managementsystems die Phase der Risikoidentifikation und -bewertung (auch als Risikoanalyse bezeichnet) vorangegangen sein. Da es für den Erfolg und den Nutzen eines Risiko-Managements zudem unerlässlich erscheint, die Ergebnisse in die Planung des Unternehmens zu integrieren, sollte zudem eine Risikoaggregation stattgefunden haben. Damit kann nicht nur die Gesamtrisikoposition des Unternehmens, z. B. gemessen am Value-at-Risk, aufgezeigt werden, sondern der quantifizierbare Teil der Risikowelt wird in das Planungsmodell des Unternehmens eingebunden. Darüber hinaus bietet die Risikoaggregation die Möglichkeit, die Bedeutung von Risiken anhand ihres Beitrags zur Streuung des Unternehmensergebnisses zu beurteilen.

Auf jeden Fall sollte im Vorfeld der Organisation des Risiko-Managements jedoch ein Risikoinventar vorliegen sowie eine Einschätzung der Geschäftsleitung, welche Risiken aus dem Risikoinventar weiter zu behandeln sind (Priorisierung des Handlungsbedarfs).

Unter einem Risikoinventar wird dabei ein systematisches Verzeichnis der Risiken des Unternehmens verstanden. Dieses sollte bereits um Überschneidungen, Doppelnennungen etc. bereinigt sein. Wichtige Ordnungskriterien der Risiken im Inventar sind die Relevanz eines Risikos (unbedeutende Risiken sollten im Inventar nicht aufgenommen werden) sowie seine „Herkunft" und seine Folgen (potenzielle Auswirkungen des Risikos). Unter Herkunft wird dabei das Risikofeld verstanden, in welchem das Risiko identifiziert wurde (die Bezeichnung der Risikofelder kann sehr unternehmensspezifisch sein).[1]

Die Priorisierung des Handlungsbedarfs kann z. B. durch folgende Matrix (siehe Abbildung 1) unterstützt und anschließend dargestellt werden:

2. Die Gestaltung des Risiko-Managementsystems

Die Gestaltung des Risiko-Managementsystems kann nicht im „freien" Raum erfolgen, sondern sie muss diversen Ansprüchen genügen. Insbesondere natürlich den „typischen" an Managementsysteme zu stellenden Anforderungen, unabhängig davon, ob der Gegen-

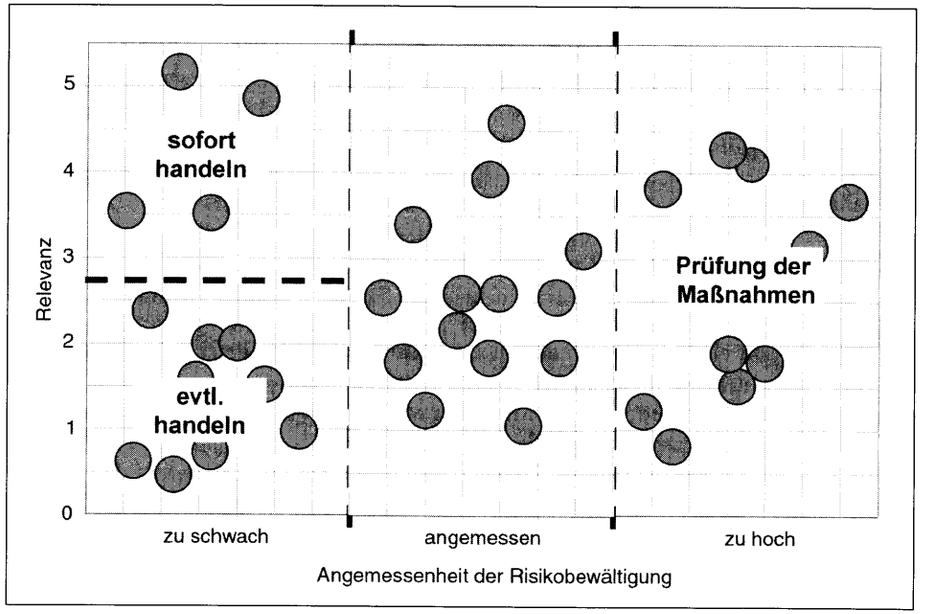

Abbildung 1: Handlungsbedarfs-Matrix (die Punkte stellen die identifizierten, relevanten Risiken dar)

standsbereich Risiko, Qualität oder Führungsinformationen ist. Zu diesen gehören vor allem Festlegungen zur Zielsetzung, Verantwortungsregelungen und Vereinbarungen über Vorgehensweise und Informationsfluss.

Einflussgröße KonTraG

Vor allem in Deutschland stellt das KonTraG eine wesentliche Vorgabe für die Organisation des Risiko-Managementsystems dar. Allerdings hat sich der Gesetzgeber hinsichtlich der konkreten Ausgestaltung eher vage geäußert. Dem Gesetzestext zufolge ist „... *insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden*" (§ 91 Abs. 2 AktG) und nach § 317 Abs. 4 HGB ist bei einer Aktiengesellschaft mit amtlich notierten Aktien „... *im Rahmen der Prüfung*[2] *zu beurteilen, [...] ob das danach einzurichtende Überwachungssystem seine Aufgabe erfüllen kann*".

Dem Gesetzestext kann also die Mindestzielsetzung für Risiko-Managementsysteme entnommen werden, nämlich dass diese Systeme als Frühwarnsysteme geeignet sein müssen, um damit für ein Unternehmen bestandsgefährdende Risiken zu erkennen.

Erheblich konkretisiert wurden die Anforderung an ein KonTraG-konformes Risiko-Managementsystem durch das Institut der Wirtschaftprüfer (IDW), das einen Prüfungsstandard für die Wirtschaftprüfer ausarbeitete (IDW PS 340 vom 25.6.1999).

Zu den **Anforderungen dieses Prüfungsstandards** zählen:

- **Festlegung der Risikofelder:**
  - Erstreckung auf das gesamte Unternehmen (sämtliche Prozesse und Funktionsbereiche);
  - Erfassung von Risiken von besonderem Ausmaß und insbesondere bestandsgefährdende Risiken.
- **Risikoerkennung und Risikoanalyse:**
  - Erkennung von bestimmten und unbestimmten Risiken;
  - Schaffung eines Risikobewusstseins;
  - quantitative Beurteilung von Tragweite und Eintrittswahrscheinlichkeit;
  - Beachtung der gemeinsamen Wirkung von Einzelrisiken (Aggregation).
- **Risikokommunikation:**
  - Schulung von Kommunikationsbereitschaft;
  - nachweisbare Berichterstattung über nicht bewältigte Risiken;
  - Festlegung von Schwellenwerten für die Berichtspflicht;
  - Festlegung von angemessenen Überwachungsrhythmen (auch Ad-hoc-Berichterstattung).
- **Zuordnung von Verantwortlichkeiten und Aufgaben:**
  - abgestufte Verantwortlichkeiten für die Erfassung und Bewältigung in den Bereichen, in denen die Risiken auftreten;
  - Rückkopplung;
  - Weiterleitung an übergeordnete Stellen bei Nichtbewältigung.
- **Einrichtung eines Überwachungssystems:**
  - Überwachung der Einhaltung der eingerichteten Maßnahmen und integrierten Kontrollen;
  - Prüfung durch die Interne Revision auf vollständige Erfassung aller Risikofelder, Angemessenheit der Maßnahmen, kontinuierliche Anwendung der Maßnahmen, Einhaltung der integrierten Kontrollen.
- **Dokumentation der getroffenen Maßnahmen:**
  - Nachweisfunktion der Dokumentation;
  - Risikohandbuch mit folgenden Inhalten: Aussagen zur Bedeutung der Früherkennung, Definition von Risikofeldern, Grundsätze der Risikoerkennung, -analyse und -kommunikation, Regelungen zur Berichterstattung.

Einflussgrößen Risikoanalyse und Risikoaggregation

Neben den „externen" Vorgaben zur Gestaltung von (Risiko-)Managementsystemen erstellt das Unternehmen – zuweilen nur implizit – auch einen internen Anforderungskatalog an das Risiko-Managementsystem. Aus „technischer" Sicht beinhaltet dieser Anforderungskatalog vor allem Elemente, die sich aus der Zielsetzung des Risiko-Managements ergeben. So führen z. B. die Einbindung in das Planungssystem, die Risikoaggregation oder

auch nur der Wunsch nach zielgerichteten Auswertungen zur Risikosituation zu Anforderungen an die Analyse und Systematisierung der Risiken. Diese können sich dann auch auf die organisatorischen Handhabung des Managementsystems auswirken.

So setzt z. B. die Quantifizierung qualitativer Risiken, wie beispielsweise die Mitarbeitermotivation, Möglichkeiten für eine umfassende Mitarbeiterbefragung voraus. Die Qualität der Ergebnisse und die Akzeptanz der Befragung verlangen dann aber eine entsprechende Schulung bzw. Information aller Mitarbeiter sowie eine adäquate Rückkopplung über die Ergebnisse.

Einflussgröße „Bestehende Organisation"

Ebenso wesentlich wie rechtliche oder „technische" Anforderungen an die Organisation des Risiko-Managements, aber oftmals nur implizit festgelegt, ist die Berücksichtigung der formellen und vor allem auch der informellen Organisation des Unternehmens. Allein schon an der Fragestellung, inwieweit das Risiko-Managementsystems „unauffällig" in die bestehende Organisation integriert werden soll (oder auch nicht!) scheiden sich die Meinungen. Auch der bestehende Führungsstil, vor allem die Offenheit im Umgang mit Problemen, können einen erheblichen Einfluss auf die sinnvolle Gestalt des Risiko-Managementsystems haben. Gerade jene „soften" organisatorischen Faktoren spielen für die spätere Akzeptanz des Risiko-Managementsystems bei den Mitarbeitern und speziell den Führungskräften des Unternehmens eine wesentliche Rolle.

Das Risiko-Management sollte in jedem Fall angepasst werden an die bestehenden organisatorischen Regelungen – selbstverständlich ohne die Aufgabe des Systems aus den Augen zu verlieren. Häufig vorgebrachte Bedenken zur Manipulation des Risiko-Managements bzw. der in den System verarbeiteten Informationen dürfen nicht zu einer Abschottung und Überdimensionierung führen. Dabei sollte vor allem nicht übersehen werden, dass die Aufgabe des Risiko-Managements nicht sein kann, unternehmensinterne Konflikte zu lösen. Wohl aber kann es einen nützlichen Beitrag zu einer verbesserten Kommunikation leisten.

Handhabung der Systemgestaltung im Projekt

Wie können nun die vielfältigen Anforderungen an das Risiko-Managementsystems im Laufe eines Projektes zur Gestaltung eines solchen berücksichtigt werden? Sicherlich gibt es nicht den Königsweg für alle Fälle. Dennoch zeigt die umfangreiche Beratungserfahrung (mit allen Arten von Managementsystemen), dass nur ein integratives Vorgehen über die verschiedenen Hierarchiestufen des Unternehmens und die verschiedenen Phasen eines Projektes erfolgversprechend ist. Möglichst frühzeitig sollten Rahmenbedingungen festgelegt werden, die laufend an der Praxis getestet werden und somit automatisch zu einer Anpassung an die Erfordernisse und eine zunehmende Detaillierung erlauben. Bereits von Anfang an sollte deshalb ein klares Konzept existieren, dass sich im Projektverlauf konkretisieren kann. Ansonsten ist die Gefahr zu groß, dass nur ein System entsteht, dass die ad hoc geäußerten Vorstellungen Einzelner widerspiegelt, aber nicht den komplexen Anforderungen gerecht wird und vor allem nicht als geschlossen und systematisch bezeichnet werden kann. Ein solches Konzept wird im Folgenden vorgestellt.

3. Die Ablauforganisation

Grundsätzlich kann man – wie oben bereits dargestellt – folgende wesentliche Teilaufgaben des Risiko-Managements unterscheiden:[3]

- Identifikation der Risiken und deren Systematisierung nach relevanten Risikoarten;
- Analyse und Bewertung der Risiken;
- Bestimmung und Beurteilung der aggregierten Wechselwirkungen auf das Unternehmen;
- Bewältigung und Überwachung der Risiken.

Die zur Identifikation, Aggregation und Steuerung von Risiken eingesetzten Instrumente unterscheiden sich je nach zugrunde liegender Risikoart in ihrer Art und Komplexität stark. Außerdem müssen bei deren Auswahl und Einsatz die Situation in dem Unternehmen sowie in den einzelnen Teilbereichen beachtet werden. Insbesondere darf der Risiko-Managementprozess kein Fremdkörper im Unternehmen sein, sondern sollte zur Vermeidung von Reibungsverlusten in die bestehenden Abläufe so gut wie möglich integriert werden.

Risikoidentifikation und -systematisierung

Aufgabe der Risikoidentifikation ist das Ausmachen bestehender Gefährdungspotenziale, d. h. die Beschreibung der auf ein Unternehmen einwirkenden Störgrößen. Hierzu ist es erforderlich, effektiv und zeitnah alle relevanten Risiken systematisch zu erfassen. Das Ergebnis der Risikoidentifikation ist also eine systematisierte Sammlung aktueller, zukünftiger, potenzieller und theoretisch denkbarer Risiken (Risikoinventar).[4]

Dabei ist zu beachten, dass die Identifikation von Risiken (wie auch die anderen Teilaufgaben des Risiko-Managements) keine einmalige Aufgabe ist, sondern kontinuierlich erfolgen muss. So können sich Risiken z. B. durch wechselnde Umfeldbedingungen oder durch unternehmensinterne Neuregelungen ändern. Risikopositionen können entfallen oder sich in ihren Auswirkungen vermindern bzw. verstärken. Es ist daher erforderlich, ein Konzept zur Risikoidentifikation aufzubauen, das eine dauerhafte Beobachtung der Risikofelder eines Unternehmens ermöglicht.

In einem ersten Schritt sollten aus Praktikabilitätsgründen die unter Risikogesichtspunkten wesentlichen Funktionsbereiche und Geschäftsprozesse identifiziert und abgegrenzt werden. Das Gesamtunternehmen wird dazu in relevante Untersuchungsbereiche zerlegt, wobei darauf zu achten ist, dass nicht bereits durch die Festlegung der Bereiche wesentliche Risikopositionen unberücksichtigt bleiben.

Zur Vorbereitung der Risikoidentifikation sollten daher mögliche Risikofelder festgelegt werden. Risikofelder dienen der Vorstrukturierung denkbarer Einzelrisiken nach bestimmten Risikoarten. Sie sollen insbesondere eine vollständige Erfassung aller für die Identifikation relevanter Risiken sicherstellen. Durch das RiskManagement CompetenceCenter Europe (RMCE), Nürnberg, wird eine Einteilung der Risikofelder vorgeschlagen, die sich – vergleichbar den Inhalten eines Businessplans – an den für Unternehmen grundsätzlich festzulegenden Fragestellungen orientiert:

- strategische Risiken;
- Marktrisiken;
- Finanzmarktrisiken;
- politisch/rechtliche und gesellschaftliche Risiken;
- Risiken aus Corporate Governance;
- Leistungsrisiken:
  - Wertschöpfungskette,
  - spezielle Risiken und Unterstützungsprozesse.

Die Erfassung von Einzelrisiken innerhalb der einzelnen Untersuchungsbereiche kann mit unterschiedlichen Methoden unterstützt werden. Denkbar sind z. B. eine regelmäßige Durchführung von Risiko-Workshops mit den verantwortlichen Mitarbeitern, Checklisten bzw. Fragebögen zur systematischen Risikoerfassung, Benchmarking, Dokumenten- und Organisationsanalysen, Werksbesichtigungen oder eine analytische Auswertung von Schadensstatistiken.[5] Um das gesamte, im Unternehmen vorhandene Risikowissen zu nutzen, könnte z. B. auch für alle Mitarbeiter die Möglichkeit zur Meldung von Risiken per E-Mail bzw. Hauspost vorgesehen werden.

Wie auch vom IDW vorgeschlagen sollte die Identifikation der Risiken durch die so genannten „Risk-Owner" durchgeführt werden. Unter einem Risk-Owner wird dabei diejenige Stelle bzw. Person verstanden, die die Verantwortung für die Handhabung eines Risikos übernimmt. Alle Risk-Owner organisieren für ihren Verantwortungsbereich individuell, wie sie die Identifikation von Risiken gestalten möchten. Diese Vorgehensweise wird mit dem zentralen Risikocontrolling abgestimmt (siehe unten). Für die dezentral nicht erfassten Risikofelder, die also keinem Risk-Owner sinnvoll zugewiesen werden können, legt der zentrale Risikocontroller eine geeignete Vorgehensweise fest.

Vom Grundgedanken her wird so die gesamte Risikolandschaft des Unternehmens in Verantwortungsbereiche zerlegt, die an geeignete Stellen delegiert werden. Dort wo diese Übertragung nicht möglich ist, stellt das zentrale Risikocontrolling die Vollständigkeit der Risikoüberwachung sicher. Weiterhin hat das zentrale Risikocontrolling sicherzustellen, dass Risikoidentifikation und weiterführende Risikoanalysen besonders auf die Risikofelder fokussiert werden, die einen sehr hohen Risikoumfang erwarten lassen.

Nach der Meldung der identifizierten Risiken an das zentrale Risikocontrolling muss die bisher zumindest teilweise unsystematische Sammlung von Einzelrisiken durch Systematisierung in ein Risikoinventar überführt werden. Dazu sind Doppel- und Mehrfachnennungen zu eliminieren, sinnvolle Zusammenfassungen vorzunehmen, Konsistenz- und Plausibilitätsprüfungen durchzuführen sowie Kodierungen und Klassifizierungen vorzunehmen.[6] Allerdings setzt diese Systematisierung der Risiken voraus, dass nicht nur eine reine Identifikation – also Benennung – der Risiken stattgefunden hat, sondern dass zu jedem Risiko genügend Informationen vorliegen, um ein Risiko anhand seiner Ursachen- oder Wirkungsbeschreibung „zu erkennen" (siehe dazu unten Risikoanalyse und -bewertung).

Auf jeden Fall sollte in einer sehr frühen Phase des Projektes überprüft werden, ob alle gewünschten Informationen zur Systematisierung von Risiken erhoben werden. Vor allem bei der späteren Nutzung der Risikoinformationen erweist sich frühzeitige Auseinandersetzung mit dieser Fragestellung als wertvoll. Mögliche (Auswertungs- und) Systematisierungsansätze seien im Folgenden beispielhaft genannt.

Auswertungs- und Systematisierungsmöglichkeiten für Risiken:

- **Wer** ist **betroffen?** (Abteilung, Standort, Branche etc.)
- Auf welche **Planungsgrößen** wirkt das Risiko? (Umsatz, Personalkosten etc.)
- Welche **Wirkungsdauer** hat das Risiko? (kurzfristig, mehrjährig o. Ä.)
- Hat das Risiko einen **zeitlichen Trend?** (wird bedeutsamer etc.)
- Aus welchem **Risikofeld** stammt das Risiko? (strategisches Risiko etc.)
- **Soll** bzw. **kann** das Risiko **bewältigt werden?** (z. B. Eintrittswahrscheinlichkeit verminderbar)
- Wie ist die **Qualität der Risikobewertung?** (gering, sehr präzise etc.)

Risikoanalyse und -bewertung

Ziel dieser Phase ist die Ermittlung des durch ein Risiko ausgelösten Gefährdungspotenzials, welches z. B. auf die Bezugsgrößen Umsatz oder Ertrag einer Gesellschaft wirkt. Dazu müssen die Ursachen-Wirkungs-Zusammenhänge einer Risikoposition analysiert werden. Unter Berücksichtigung der bereits getroffenen Maßnahmen zur Risikobewältigung ist zu beurteilen, ob wesentliche oder sogar bestandsgefährdende Risiken bestehen. Dabei ist sowohl die Intensitäts- (Eintrittswahrscheinlichkeit) als auch die Qualitätsdimension (Höhe des drohenden Schadens) zu bewerten.

Risikoidentifikation und Risikobewertung gehen dabei oft fließend ineinander über. Durch die Nutzung der vom RMCE RiskCon GmbH, entwickelten Arbeitsunterlagen gelingt in der Regel schon bei der Identifikation der Risiken eine erste Bewertung.[7] Anhand dieser kann über das zentrale Risikocontrolling entschieden werden, ob eine detailliertere Untersuchung des Risikos und seiner Auswirkungen erforderlich ist.

Die Risikobewertungen sollten hinsichtlich unterschiedlicher Schadensszenarien differenziert werden. Dies erleichtert nicht nur den Beteiligten die Beschreibung eines Risikos, sondern erlaubt darüber hinaus auch die Abschätzung der Verteilungsfunktion, gemäß der sich das Risiko verhält. Außerdem sollte eine Wahrscheinlichkeitsbetrachtung durchgeführt

werden, um fundierte Aussagen über die erwarteten Auswirkungen auf die Unternehmens- bzw. Sicherheitsziele zu ermöglichen. Selbstverständlich sollte – wo sinnvoll – auch für die Risikobewertung eine unterjährige Anpassung bzw. Neubewertung möglich sein.

Bei der Quantifizierung der Schadenshöhe sollte beispielsweise zwischen einem realistischen Höchstschaden, mittleren Schäden und Kleinschäden differenziert werden. Jedem dieser Schadensszenarien können dann Eintrittswahrscheinlichkeiten im Sinne von Häufigkeiten des Auftretens zugeordnet (z. B. Höchstschaden tritt einmal in hundert Jahren, ein mittlerer Schaden einmal in zwanzig Jahren und ein Kleinschaden einmal im Jahr auf). Wenn möglich sollten auch Abhängigkeiten zwischen den Schadensszenarien, Wirkungsdauer und mögliche Eintrittszeitpunkte angegeben werden.[8]

Erfahrungsgemäß ist eine exakte Quantifizierung von Risiken oft schwierig und mit erheblichen Unsicherheiten behaftet. Es sollte jedoch versucht werden, zumindest näherungsweise das Gefährdungspotenzial abzuschätzen. Dabei kann es hilfreich sein, einzelne Schadensfälle konkret zu benennen (z. B. Verlust eines bestimmten Großabnehmers) und die Auswirkungen auf wesentliche Bezugsgrößen (z. B. Umsatz, Kosten, Ertrag etc.) überschlägig zu berechnen. Soweit möglich sollte auf vorhandene statistische Informationen zurückgegriffen werden. Erst in letzter Annäherung kann auch eine rein qualitative Abschätzung der Auswirkungen eines Risikos genutzt werden.

Die Risikomeldungen der einzelnen damit beauftragten Unternehmensbereiche werden durch den zentralen Risikocontroller gesammelt, ergänzt und zu einem Risikobericht verdichtet (siehe unten).

Risikoaggregation

Ziel der Risikoaggregation ist es, die Gesamtrisikoposition eines Unternehmens zu ermitteln. Dabei müssen insbesondere Wechselwirkungen zwischen einzelnen Risiken berücksichtigt werden. Solche Wechselwirkungen äußern sich z. B. in einer gegenseitigen Kompensation oder Verstärkung von Risiken.[9]

Risikobewältigung und -überwachung

Im Anschluss an die Risikobewertung und -aggregation ist zu entscheiden, welche Risiken unmittelbaren Handlungsbedarf auslösen. Ein „automatischer" zwingender Handlungsbedarf ergibt sich in der Regel nur bei Überschreiten eines vorgegebenen Limits (siehe unten). Häufig wird durch Entscheidungen von Vorstand oder Bereichsverantwortlichen ein von festen Limite unabhängiger Handlungsbedarf geäußert. Wird ein Handlungsbedarf festgestellt, so müssen entsprechende Maßnahmen generiert werden. In Abhängigkeit von der Risikopolitik des Unternehmens und vom jeweiligen Risiko sind dabei folgende grundsätzliche Zielrichtungen der Maßnahmen denkbar:[10]

- **Risikovermeidung:** Risikovermeidung bedeutet, dass das Unternehmen auf die risikobehaftete Aktivität gänzlich verzichtet. Risiko entsteht somit nicht.

- **Risikominderung:** Die Risikominderung soll die Wahrscheinlichkeit des Risikoeintritts verringern. Durch entsprechende Maßnahmen wird also die Häufigkeit vermindert.
- **Risikobegrenzung:** Maßnahmen, die auf die Risikobegrenzung abzielen, begrenzen das Ausmaß eines möglichen Schadens.
- **Risikoüberwälzung:** Bei der Risikoüberwälzung wird das Risiko auf ein anderes Unternehmen, oft auf Versicherungsunternehmen oder Subunternehmer, übertragen.
- **Risikokompensation:** Risikokompensation bedeutet, dass das Unternehmen das Risiko bzw. den nicht sinnvoll verminderbaren „Rest" selbst trägt. Zur Absicherungen dienen in der Regel dann entsprechende Deckungspotenziale in Form von Liquiditätsreserven und Eigenkapital.

Die Generierung von Maßnahmen wird in der Regel zumindest in Form von ersten Anregungen fließend aus der Identifikation und Bewertung der Risiken hervorgehen. Die eigentliche Ausarbeitung einer Maßnahme kann einen solchen Umfang annehmen, dass die Initiierung eines Projektes erforderlich wird. In einer ersten Stufe bietet es sich jedoch meist an, zunächst sogenannte Bewältigungs-Workshops durchzuführen. In diesen Workshops kann mit den Risk-Ownern die organisatorische Zuordnung der Risikohandhabung diskutiert werden und vorhandene Maßnahmenentwürfe einer inhaltlichen Prüfung unterzogen werden. Auch für die Workshops bietet sich die Unterstützung mit den durch die RMCE RiskCon GmbH, Leinfelden-Echterdingen/Nürnberg, entwickelten Arbeitsunterlagen an.[11]

Neben der sofortigen Bewältigung von Risiken muss auch eine permanente Überwachung der relevanten Risiken sichergestellt sein. Dazu sollte für jedes identifizierte Risiko ein entsprechender Ordner bzw. eine Datei mit standardisierten Formblättern angelegt werden.[12] Auf den Formblättern sollten die Ergebnisse der Risikoidentifikation, Überlegungen zur Risikobewältigung sowie zur dauerhaften Überwachung der Risiken vermerkt werden. Darüber hinaus können sogenannte „Schubladenpläne" entwickelt werden, nach denen im Fall einer negativen Entwicklung des Risikos ohne Zeitverlust entsprechende Maßnahmen eingeleitet werden können.

Voraussetzungen für eine gut funktionierende Risikoüberwachung sind ein leistungsfähiges Risikoberichtswesen sowie eine effiziente Organisation des Risiko-Managements. Darauf soll im nächsten Abschnitt näher eingegangen werden.

Die Integration der Aufgaben des Risiko-Managements in bestehende Systeme

Bei der Integration des Risiko-Managements in die bestehende Ablauforganisation sind zwei zentrale Herausforderungen zu bedenken, die sich fast durch die gesamte Aufgabe der Gestaltung eines Risiko-Managements wie ein roter Faden ziehen. Einerseits ist Risiko-Management nichts Neues. Der Grundgedanke – sich über Unsicherheiten der Zukunft und

mögliche Zielverfehlungen bewusst zu werden – begleitet uns durch Alltag und Berufsleben. Demnach scheint eine Einbindung der Aufgaben des Risiko-Managements in die betrieblichen Abläufe einfach. Andererseits führt gerade dieser scheinbar so alltägliche Umgang mit Risiko-Management dazu, das Risiko nur als vage Andeutung möglicher Entwicklungen im operativen Tagesgeschäft untergeht. Gerade Forderungen nach der systematischen Vorgehensweise oder der expliziten und quantitativen Darstellung von Risiken werden nur selten befriedigend erfüllt. Darüber hinaus fordert uns Risiko-Management auch auf, das strategische und operative Handeln im Unternehmen einmal aus der Vogelperspektive zu betrachten und gerade dadurch den Blick auf das Wesentliche zu schärfen. Damit bedeutet Risiko-Management immer auch eine gewisse Abkopplung von den routinemäßigen Abläufen im Unternehmen. Eine Integration von Risiko-Management in bestehende betriebliche Abläufe gelingt daher typischer Weise umso besser, je mehr diese Abläufe zumindest regelmäßig auch ein kritisches Überdenken der jeweiligen Prozesse vorsehen.

Wie kann dies konkret für die einzelnen Schritte des Risiko-Managements aussehen?

In der Phase der Risikoidentifikation geht es vor allem darum, mögliche Risiken überhaupt zu erkennen. Bei der Einführung eines Risiko-Managementsystem wird man dazu wie oben beschrieben vorgehen können. Im späteren Risiko-Managementprozess wird dieses Verfahren als zu aufwendig erscheinen. Um die Belastung für die Ressourcen des Unternehmen möglicht gleichmäßig zu verteilen, bietet es sich an, die einzelnen Beobachtungsbereiche jeweils Fachspezialisten zuzuweisen, die auch zukünftig in der Lage sind, neue Risiken zu erkennen, die sich aus internen oder externen Veränderungen ergeben. Für Bereiche, bei denen dies nicht gelingt, könnte die Verantwortung für die wiederkehrende Identifikation von Risiken über das zentrale Risikocontrolling koordiniert bzw. durchgeführt werden. Die eigentliche Identifikation wird jeweils mit für diesen Bereich geeigneten Methoden – Checklisten, Workshop, Expertenbefragung, externe Gutachten etc. – durchzuführen sein. Die Anwendung dieser Methoden kann in der Regel sehr gut in jährlich stattfindende Veranstaltungen integriert werden, die der grundsätzlichen Meinungsbildung über den betrachteten Bereich dienen. Beispielsweise sind dies jährliche Planungsgruppen im Produktionsbereich, Jahresmeetings im Vertrieb, Auswertungs- und Besprechungsrunden im Rahmen des Qualitätsmanagement oder der Investitionsplanung, strategische Planungstage der Geschäftsleitung etc., wie sie in fast allen Bereichen eines Unternehmens zu finden sind.

Die Phase der Analyse und Bewertung von Risiken, die sich an deren Identifikation anschließt, wird meist iterativ stattfinden. Eine erste Bewertung eine Risikos gelingt oft schon bei seiner Identifikation. Oft aber fehlen dann noch wesentliche Informationen aus anderen Unternehmensbereichen, die in die Analyse und Bewertung mit einbezogen werden müssen. Oder auch für die Bewertung notwendige Daten sind nicht sofort bzw. in geeigneter Form verfügbar. Die dazu notwendigen Schritte gehören jedoch sehr wohl zum betrieblichen Alltag. Eine Rücksprache mit der Leitung eines bestimmten Unternehmensbereichs oder die Anforderung von benötigten Informationen aus dem Controlling sind typische Aufgaben, die allerdings durch klare Aufgaben- und Verantwortungsregelungen begleitet werden sollten (vgl. dazu auch Aufbauorganisation des Risiko-Managementsystems). Wichtig erscheint vor allem bei subjektiv bewerteten Risiken am Schluss nicht durch Konsensbildung die erforderliche Transparenz zu vernachlässigen. Risiko bedeutet nunmal Unsicherheit und nicht Eindeutigkeit.

Die Aufgabe der Vorbereitung und Durchführung der Risikoaggregation wird sich sicherlich am Besten in den Planungsprozess des Unternehmens in einer dafür zuständigen zentralen Abteilung – z. B. das Controlling – einbinden lassen. Dort können in der Regel am einfachsten Verflechtungen zwischen unterschiedlichen Unternehmensbereichen oder Überschneidungen zwischen einzelnen Risiken erkannt werden. Daneben fordert die Unternehmensplanung ohnehin, dass alle Einschätzungen über die zukünftige Entwicklung in ein Zahlenwerk gegossen werden. Auch werden in den zentralen Planungseinheiten des Unternehmens am ehesten die notwendigen fachlichen Kompetenzen für die Risikoaggregation vorhanden sein.

Die Risikobewältigung und die Risikoüberwachung werden in den meisten Fällen sinnvoll in die Aufgaben der einzelnen Unternehmenseinheiten integriert werden können. Dem zentralen Risikocontrolling obliegt dann weiterhin die Koordination und Zusammenführung der Informationen. Grundsätzliche Aufgaben – wie sie typischerweise bei der Risikobewältigung anzugehen sind – werden häufig in die bereits oben erwähnten Planungsgespräche und Sitzungen integriert werden können. Meist wird man jedoch nicht die nächste Jahrestagung abwarten, sondern wird im Rahmen z. B. quartalsweise stattfindender Sitzungen arbeiten können. Ähnliches gilt für die laufende Überwachung einzelner Risiken. Je nachdem für das jeweilige Risiko angemessenen Turnus wird die Durchführung und die Berichterstattung über die Messung der Risikoposition in die bestehenden betrieblichen Abläufe und das diese begleitende Berichtwesen integriert werden. So kann beispielsweise die Vertriebsabteilung in ihren Quartalsbesprechungen die Einschätzung über die Preisentwicklung in den kommenden Monaten aktualisieren und in das normale Berichtswesen einfließen lassen. Sicherlich wird eine besondere Hervorhebung in den Berichten oder eine Zusammenfassung der Risikoinformationen in einem kurzen „Summary" die Transparenz erhöhen und die weitere Bearbeitung der Informationen erleichtern.

Die Unterstützung der Ablauforganisation mittels Risikomappen

Die Ablauforganisation des Risiko-Managements umfasst gemäß obigere Darstellung folgende **Aufgabenbereich:**

- Identifikation von Risiken;
- Analyse und Bewertung von Risiken;
- Ausarbeitung von Handlungsalternativen (u. a. von präventiven Maßnahmen);
- Überwachung von Risiken;
- reaktive Maßnahmen (Bewältigung- oder Notfallpläne);
- Berichtswesen/Informationsweitergabe.

Zur Unterstützung dieser Aufgaben wurde durch RMCE in Zusammenarbeit mit Kundenunternehmen ein Formblattsystem entwickelt. Dieses Formblattsystem basiert auf der Idee, dass möglichst für alle relevanten Risiken, die in den laufenden Prozess des Risiko-Managements integriert sind, die benötigten Informationen im Überblick verfügbar sein sollten. Entstanden sind dabei die sogenannten Risikomappen. Diese werden im folgenden Beitrag ausführlich erläutert. Typischerweise werden die Risikomappen im Unternehmen zunächst in der Papierform eingeführt und aufgrund der unternehmensspezifischen Erfahrungen modifiziert. Wenn der Informationsbedarf des Unternehmens und seine Anforderungen an die Handhabung geeignet abgebildet sind, werden die Mappen dann in eine EDV-gestützte Version (basierend auf einer Datenbank) überführt.

4. Die Aufbauorganisation und das Berichtswesen

Grundsätzlich gehört das Risiko-Management als eine wesentliche Aufgabe zu den Sorgfaltspflichten der Geschäftsführung bzw. dem Vorstand eines jeden Unternehmens. Da die Geschäftsleitung diese Aufgabe jedoch meist nicht in vollem Umfang selbst wahrnehmen kann, hat diese durch Zielvorgaben und Aufgabendelegation sicherzustellen, dass ein adäquates Risiko-Management im Unternehmen einführt und gelebt wird.

Als alleinige Aufgabe der Geschäftsführung ist die Erfüllung der Überwachungsfunktion anzusehen. Die Forderung nach einem Risiko-Managementsystem (seitens des Gesetzgebers) kann demnach nicht bedeuten, dass der Vorstand künftig sämtliche Risiken selbst steuert. Auch in den Konkretisierungen des Instituts der Wirtschaftprüfer (IDW)[13] zur Gestaltung eines Risiko-Managementsystems, wird explizit die Delegation von Aufgaben und der dezentralen Aufbau betont. Die Steuerung der Risiken wird demnach überwiegend von entsprechenden Entscheidungsgremien im Unternehmen übernommen und der Geschäftsleitung obliegt die Überwachung (im Sinne einer sogenannten Management-Attention). Damit verbleibt die Verantwortung für das Risiko-Management explizit bei der Geschäftsleitung.[14]

Im Folgenden geht es insbesondere um die Frage, wie die in den vorigen Kapiteln beschriebenen Teilaufgaben des Risiko-Managements auf die vorhandenen bzw. neu zu schaffenden Organisationseinheiten übertragen werden können.

Als eine allgemeine Voraussetzung für die Funktionsfähigkeit eines Risiko-Managementsystems kann die Schaffung einer zentrale Stelle (im Folgenden als zentrales Risikocontrolling bezeichnet) genannt werden. Darunter kann in den einzelnen Unternehmensbereichen bzw. Unterstützungsfunktionen ein dezentrales Risiko-Management (besetzt durch die Risk-Owner) eingerichtet werden. Die Hauptaufgabe des zentralen Risikocontrolling besteht dann darin, das Risiko-Management zu einem konsistenten und effizienten System auszubauen und die Funktionsfähigkeit des Systems zu gewährleisten – z. B. durch Koordination und Unterstützung aller Aufgaben und beteiligten Personen.

In komplexeren Unternehmen wird es sich bei dem zentralen Risikocontrolling daher auch um ein RiskBoard handeln, in dem mehrere fachkompetente Mitarbeiter des Unternehmens als (virtuelles) Team die Aufgabe des Risikocontrolling übernehmen. Gerade für die fachliche und inhaltliche Unterstützung werden dann derart viele unterschiedliche Kompetenzen benötigt, dass sie sich kaum auf einer Stelle vereinen lassen. Aber auch bei einem RiskBoard (z. B. bestehend auf fünf Mitgliedern) wird nicht jeder stets vertreten sein müssen. Es ist durchaus vorstellbar, einige Mitglieder je nach Tagesordnungspunkt passend zusammenzurufen und durch andere Mitarbeiter des Unternehmens gezielt zu verstärken.[15]

Neben der Strukturierung und inneren Gestaltung des zentralen Risikocontrolling ist die Struktur der darunter liegenden Organisation ein wesentliches Gestaltungselement eines Risiko-Managementsystems.

Meist kann mit einem einstufigen System eine für die zu bewältigenden Aufgaben ausreichend Struktur geschaffen werden. Einstufig meint dabei, dass das Risiko-Managementsystem nur über eine zentrale Koordinationsstelle – eben das zentrale Risikocontrolling – verfügt. Direkt darunter angeordnet sind dann die Verantwortlichen für einzelne Bereiche bzw. Teilaufgaben des Systems.

Bei großen oder sehr stark verflochtenen Unternehmen mit einer entsprechend komplexen Risikolandschaft scheint es in jedem Fall empfehlenswert, ein mehrstufiges System zu gestalten. In einem solchen wird die Koordinationsaufgabe des zentralen Risikocontrollings durch vergleichbare dezentrale Stellen unterstützt, die für einen Teilbereich des Unternehmens die Koordination für das dort angesiedelte Subsystems des Risiko-Managements übernehmen. Besonders häufig anzutreffen sind solche mehrstufigen Systeme in Holdingstrukturen oder vergleichbaren Organisationen, in denen eigenständig agierende und ausreichend bedeutsame Unterorganisationen existieren.

Vorstellbar ist natürlich auch eine teilweise Zweistufigkeit eines Risiko-Managementsystems, indem in einem Bereich ein Subsystem aufgebaut wird, während alle anderen Bereiche von einer Zentralstelle aus gesteuert und koordiniert werden. Beispielsweise dürfte man solche Systeme in (kleineren) Banken finden, in denen aufgrund der Regelungen der Mindestanforderungen an das Betreiben von Handelsgeschäften der Kreditinstitute (MAH) ein eigenständiges Subsystem aufgebaut wird.[16]

Ein solches, teilweise zweistufiges, System würde folgender Aufbaustruktur entsprechen (siehe Abbildung 2).

Die Stelleninhaber von Risiko-Managementaufgaben erhalten aus dieser Aufgabe heraus keine Weisungsbefugnis gegenüber anderen Mitarbeitern. Sie haben jedoch ein ausgeprägtes Recht auf Information. Theoretisch sinnvoll wäre natürlich eine grundlegende Trennung von Risikoverursachung und Risikoüberwachung. In der Praxis wird jedoch mindestens auf der Ebene der Risk-Owner eine Personalunion mit Linienfunktionen nahezu unumgänglich sein, wodurch einerseits eine faktische Entscheidungsbefugnis der am Risiko-Managementprozess Beteiligten gegeben ist und die Trennung von Ausführung und Überwachung nur in Teilen gelingt. Insbesondere durch die Doppelfunktion von Risk-Ownern als „Risikoverursacher" steigt die Bedeutung der Unabhängigkeit des zentralen Risikocontrollings. Die Aufgabe des zentralen Risikocontrollings besteht allgemein in

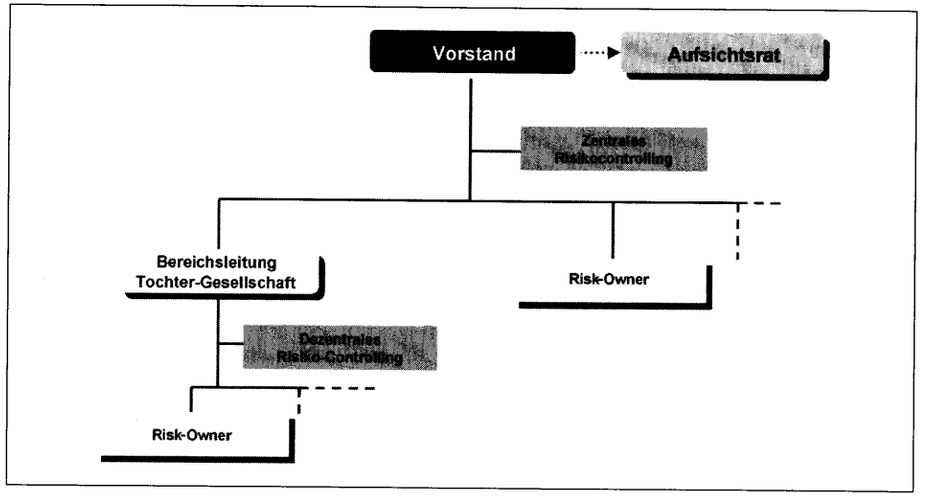

Abbildung 2: Aufbaustruktur eines zweistufigen Risiko-Managementsystems

der Steuerung und Begleitung des Risiko-Managementprozesses (siehe unten). Die Risk-Owner tragen die Verantwortung für die Um-/Durchsetzung des Risiko-Managementprozesses in den Unternehmensbereichen bzw. in den Unterstützungsprozessen (siehe unten).

Der Risiko-Managementprozess muss zwingend von einer vom zentralen Risikocontrolling unabhängigen Instanz überwacht werden.[17] Diese Funktion wird in der Regel von der Internen Revision wahrgenommen. Deren Aufgabe ist die Überprüfung der vorhandenen sowie der geplanten Konzepte und Systeme auf ihre Effektivität und Effizienz. Die Interne Revision beurteilt also die Wirksamkeit bestehender Risiko-Managementsysteme, identifiziert vorhandene Lücken und leistet Hilfestellung bei der Verbesserung des Risiko-Managements. Außerdem wirkt sie mit bei der Entwicklung von Grundsätzen und Standards und überwacht die Einhaltung integrierter Prüfmechanismen. Als anzustreben gilt, die Überwachungsinstanz „Interne Revision" organisatorisch von dem Bereich Risiko-Management zu trennen.

Wie bereits oben angesprochen, sind einige Aufgaben des Vorstands im Risiko-Managementprozess nicht delegierbar. Die Entwicklung eines funktionsfähigen Risiko-Managements setzt voraus, dass neben der Erfüllung der Überwachungsfunktion vom Vorstand eine Unternehmensstrategie sowie strategische Unternehmensziele vorgegeben werden. Dies ist eine originäre Aufgabe des Top-Managements. Aus der Unternehmensstrategie wird die Unternehmensplanung entwickelt. Diese basiert auf Annahmen über die künftige Entwicklung des Unternehmens und seiner Umwelt. Die damit verbundenen Unsicherheiten bzw. strategischen Risiken sind somit selbst Gegenstand des Risiko-Managements. Risiko-Management im Bereich der Unternehmensplanung kann aufgrund seiner Bedeutung nur teilweise an nachgeordnete Hierarchieebenen delegiert werden. Es sollte überwiegend in

der Verantwortung des Top-Managements selbst liegen. Dies setzt selbstverständlich ein funktionsfähiges Managementinformationssystem voraus.

Eine weitere nicht-delegierbare Aufgabe des Vorstands ist die regelmäßige Information des Aufsichtsrats hinsichtlich wesentlicher Risiken. Dies könnte mit Hilfe kurzer Risikoberichte erfolgen (siehe unten).

Die oben angesprochene Überwachungsfunktion des Vorstands ist ebenfalls grundsätzlich nicht delegierbar. Sie wird allerdings typischerweise unterstützt durch die Aktivitäten der Internen Revision und der Wirtschaftsprüfer. Der Vorstand wird außerdem regelmäßig direkt durch das zentrale Risikocontrolling über die Risikosituation sowie über die Erreichung der Ziele des Risiko-Managements informiert. Bei Bedarf sollte er zusätzliche Überwachungsmaßnahmen – z. B. durch unabhängige Dritte – einleiten.

Der Aufsichtsrat als Kontrollgremium der Eigentümer und der Belegschaft überwacht u. a. die Entscheidungen des Vorstands. Für die bedeutsamen Risiken aus strategischen Planungen/Entscheidungen des Vorstands ist eine gesonderte Kontrolle durch den Aufsichtsrat sinnvoll. Der Aufsichtsrat sollte zur Verstetigung des Informationsflusses zwischen Vorstand und Aufsichtsrat eine Informationsordnung erlassen, in der die Berichtspflichten des Vorstands über das Risiko-Management und seine Überwachung geregelt sind. Damit wird der Intention des KonTraG, den Aufsichtsrat stärker in die Überwachung der Unternehmen einzubeziehen, Rechnung getragen.

Somit erhält man die in Abbildung 3 dargestellte grobe Zuordnung von Verantwortlichkeiten für das Risiko-Management.[18]

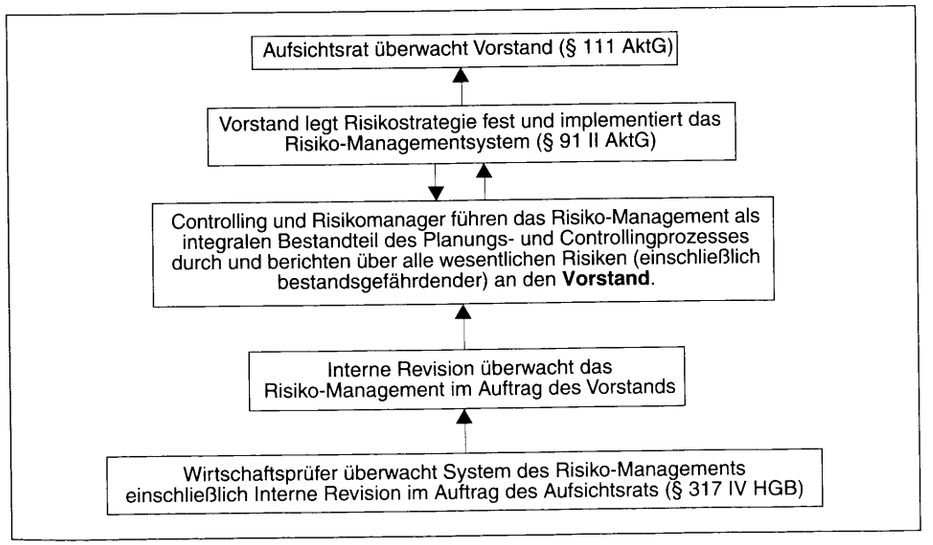

Abbildung 3: Zuordnung von Verantwortlichkeiten

Im Folgenden sollen die Aufgaben des zentralen Risikocontrollings und des dezentralen Risiko-Managements näher beschrieben werden.

Zentrales Risikocontrolling

Das zentrale Risikocontrolling trägt die Gesamtverantwortung für den Risiko-Managementprozess. Daher sollte es bereits bei der Entwicklung der Risikostrategie und bei der Festlegung der strategischen Ziele des Risiko-Managements durch den Vorstand einbezogen werden. Das zentrale Risikocontrolling sollte dabei die für die Strategie-Formulierung notwendigen Risikoinformationen bereitstellen. Die Entwicklung der grundsätzlichen Richtlinien zum Risiko-Management sollte ebenfalls in enger Zusammenarbeit mit dem Vorstand erfolgen. Ein wesentlicher Bestandteil dieser Richtlinien sollte die Festlegung sogenannter Sicherheitsziele sein, deren Verletzung oder Gefährdung Handlungsbedarf auslöst und zu einer Rückmeldung an das Top-Management führen muss.

In Abstimmung mit dem Vorstand müssen von dem zentralen Risikocontrolling die Unternehmensbereiche sowie die Unterstützungsfunktionen festgelegt werden, für die ein dezentrales Risiko-Management einzurichten ist. Dabei können auch mehrere Bereiche/Funktionen zusammengefasst werden. In besonders komplexen Gebieten ist auch eine mehrstufige dezentrale Organisation denkbar (siehe oben).

Das zentrale Risikocontrolling ist verantwortlich für die Implementierung der geplanten Organisation des dezentralen Risiko-Managements. Es muss außerdem die festgelegte Risikostrategie sowie die strategischen Ziele des Risiko-Managements kommunizieren. Dabei sollte die Kommunikation nicht auf die Risk-Owner beschränkt bleiben. Auch die übrigen Mitarbeiter müssen für unternehmerische Risiken sensibilisiert werden. Dies ist insbesondere für die Identifikation neuer Risiken von elementarer Bedeutung, da jeder einzelne Mitarbeiter die Probleme seines Tätigkeitsumfeldes in der Regel am besten kennt und somit wertvolle Frühwarninformationen liefern kann. Maßnahmen zur Risikosensibilisierung der Mitarbeiter (z. B. Schulungen, Informationsbroschüren) sowie zur Erfassung von Mitarbeiterinformationen (z. B. Festlegen von Ansprechpartnern) sind daher für ein funktionierendes Risiko-Management äußerst wichtig.

Die Festlegung der operativen Ziele des Risiko-Managements für die einzelnen dezentralen Bereiche ist eine weitere Aufgabe des zentralen Risikocontrollings. Um unnötige Reibungsverluste zu vermeiden, sollte dies allerdings in enger Abstimmung mit den dezentralen Risiko-Managern erfolgen. Dabei sollten unter Beachtung der Sicherheitsziele auch konkrete Schwellenwerte („limits") definiert werden, ab denen einzelne Risikopositionen gemeldet bzw. bearbeitet werden müssen (siehe unten).

Weiterhin muss das zentrale Risikocontrolling das dezentrale Risiko-Management, soweit möglich, methodisch unterstützen und dabei auf eine Vereinheitlichung der Methoden achten. So sollten z. B. die Risikosystematisierung und -bewertung unternehmensweit möglichst einheitlich erfolgen. Wünschenswert ist daher ein intensiver Know-how-Transfer zwischen zentralem Risikocontrolling und dezentralem Risiko-Management.

Eine wesentliche Bedeutung für die Funktionsfähigkeit des Risiko-Managementsystems hat die Berichterstattung über die (nicht bewältigten) Risiken sowie über die (Nicht-)Erreichung der festgelegten Ziele des Risiko-Managements einschließlich der Sicherheitsziele. Es ist grundsätzlich notwendig, dass ein relevantes, Risiko – gegebenenfalls in aggregierter Form – bis zum Vorstand berichtet wird. Gleiches gilt bei Nichterreichen der Ziele des Risiko-Managements. Das zentrale Risikocontrolling muss ein dazu geeignetes Berichtswesen entwickeln und implementieren (siehe unten). Aus Wirtschaftlichkeitsgründen könnte dabei eventuell an das bestehende Berichtswesen angeknüpft werden. Es muss jedoch eine ausreichende Flexibilität sichergestellt werden. So sollten z. B. einerseits regelmäßig Risikoberichte erstellt werden, die sowohl die Gesamtrisikoposition als auch einzelne wesentliche Risiken bzw. deren Veränderungen beschreiben. Andererseits muss sichergestellt sein, dass bei Eilbedürftigkeit förmliche Berichtsstrukturen überwunden und institutionalisierte Kommunikationswege sowie Periodizitäten der Berichterstattung verkürzt werden (Ad-hoc-Berichterstattung).

Die an das zentrale Risikocontrolling gemeldeten Risiken müssen dort nochmals eingehend analysiert, bewertet und gegebenenfalls aggregiert werden. Die gemeldeten Risiken sind insbesondere hinsichtlich einer wechselseitigen Verstärkung oder Kompensation zu beurteilen. In enger Abstimmung mit den betroffenen Bereichen sind detaillierte Maßnahmen zur Risikobewältigung zu entwickeln und einzuleiten. Ist ein funktionsfähiges Planungssystem vorhanden, so sollte dieses schon allein aus Wirtschaftlichkeitsgründen einbezogen werden. Im Extremfall übernimmt das zentrale Risikocontrolling dann nur eine reine Koordinations- und Beratungsfunktion. Es analysiert und aggregiert die gemeldeten Risiken, stößt eine Maßnahmenplanung im Planungssystem an und greift bei Bedarf unterstützend in den Planungsprozess ein. Darüber hinaus muss der Vorstand insbesondere bei bestandsgefährdenden Risiken, die eine gewisse Dynamik haben, laufend über die Entwicklung der Risikoposition unterrichtet werden.

Von besonderer Bedeutung für die Koordinationsaufgabe des zentralen Risikocontrollings sind Risiken, die sich aus mehreren Teilrisiken entlang einer Prozesskette zusammensetzen. Solche Risiken müssen auf zentraler Ebene aggregiert und die entsprechenden Bewältigungsmaßnahmen koordiniert werden, da den einzelnen Bereichen unter Umständen die Gesamtsicht fehlt. Isolierte Risikobewältigungsstrategien innerhalb der einzelnen dezentralen Risiko-Managementbereichen (Stand-alone-Lösungen) können eine optimale Risikobewältigung nicht sicherstellen und wirken unter Umständen sogar kontraproduktiv.

Schließlich sollte das zentrale Risikocontrolling bei der Entwicklung von Krisenstrategien mitwirken. Eine zentrale Rolle kommt dabei – wie oben bereits ausgeführt – der zeitnahen und flexiblen Kommunikation zu. Eventuell sind für besonders wahrscheinliche und bestandsgefährdende Krisenszenarien Krisenpläne zu entwickeln („Schubladenplanung").

Dezentrales Risiko-Management

Grundsätzlich tragen die einzelnen Unternehmensbereiche und Unterstützungsfunktionen die Verantwortung dafür, dass die dort auftretenden Risiken erfasst und – bei entsprechender Relevanz – an die festgelegten Berichtsempfänger weitergeleitet werden (Risk-Owner bei

dezentralem Aufbau des Risiko-Managements). Dabei müssen die organisatorischen Vorgaben des zentralen Risikocontrollings umgesetzt werden.

Für die Organisation des dezentralen Risiko-Managements können allgemein folgende **Ansätze** unterschieden werden:

- Die im Rahmen des Risiko-Managementsystems angesprochenen Stellen haben Stabscharakter mit umfassenden Informationsrechten aber ohne Weisungsbefugnis gegenüber Linienfunktionen. Nach dem Prinzip der strikten Funktionstrennung kann Risiko-Management organisatorisch/personell getrennt von den operativen Einheiten in den einzelnen Bereichen ausgeübt werden. Das dezentrale Risiko-Management ist dann zwar in dem jeweiligen Unternehmensbereich angesiedelt, es wird jedoch von Mitarbeitern ausgeübt, die nicht an den risikobehafteten operativen Geschäftsprozessen beteiligt sind.
- Aufgrund der Fachkompetenz durch den täglichen Umgang mit den maßgebenden Risikofaktoren kann Risiko-Management von den operativen Einheiten selbst ausgeübt werden.

Die Wahl der sachgerechten Organisationsform hängt von den Verhältnissen des Einzelfalls ab. So ist in Bereichen mit sehr hohen Risiken eine strikte Funktionstrennung sinnvoll. In allen anderen Fällen wird das dezentrale Risiko-Management schon aus Praktikabilitätsgründen von den direkt an den Geschäftsprozessen beteiligten Mitarbeitern selbst ausgeübt werden. Dies verhindert ein unnötiges Aufblähen der Organisation.

Unabhängig von der jeweils gewählten Organisationsform sollen im Folgenden mögliche Aufgaben der Risk-Owner im Rahmen eines dezentralen Risiko-Managements allgemein skizziert werden:

Wie oben bereits erwähnt hängt die Qualität eines Risiko-Managementsystems stark von dem Risikobewusstsein der einzelnen Mitarbeiter ab, da diese die Risikoauswirkungen in ihrem Tätigkeitsfeld am besten einschätzen können. Das dezentrale Risiko-Management sollte daher möglichst viele Mitarbeiter des Bereichs in den Risiko-Managementprozess einbinden. Dies gilt insbesondere für die Risikoidentifikation. Zudem kann im Falle einer Durchführung der Aufgaben des Risk-Owners in Personalunion mit den Aufgaben der Linienfunktion eine Überlastung der Verantwortlichen nur durch eine angemessene Delegation der Aufgaben vermieden werden.

Zur Systematisierung der Risikoidentifikation könnte das dezentrale Risiko-Management zunächst in Anlehnung an die Risikofelderstruktur des Unternehmens detailliertere Untersuchungsbereiche festlegen. Für jeden Untersuchungsbereich wird wiederum ein verantwortlicher Ansprechpartner benannt, der für die Identifikation der Risiken in seinem Bereich verantwortlich ist. Die auf unterster Ebene identifizierten Risiken könnten z. B. per Standard-E-mail an den jeweiligen Ansprechpartner übermittelt werden.

Weiterhin ist das dezentrale Risiko-Management zuständig für die Analyse und Beurteilung der identifizierten Risiken. Die Beurteilung erfolgt je nach Risikoart quantitativ und/oder qualitativ in Bezug auf die Bereichs- und Unternehmensziele. Auch hierbei sollte wieder

das gesamte Wissen des Bereichs genutzt werden. Eventuell muss dabei auch auf externe Quellen zurückgegriffen werden. Dies gilt insbesondere wenn für ein Risiko nur schwerlich quantitative Messgrößen bestimmt werden können. In solchen Fällen sollte eine qualitative Einschätzung in ihrer Qualität durch die Reflexion mit anderen fachkompetenten Personen erhöht werden.

Sofern für ein Risiko eine gezielte Risikobewältigung erforderlich wird oder vereinbart wurde, sind dazu konkrete Maßnahmen zu entwickeln. Die Beurteilung der Relevanz eines Risikos erfolgt über vorher definierte Limits. Wie oben schon dargestellt sollten zur Verhinderung eines unnötigen Aufblähens der Organisation bestehende Planungs- und Managementsysteme eingebunden werden. Unter Umständen übernimmt der dezentrale Risiko-Manager die Maßnahmenplanung dann nicht selbst, sondern ist nur verantwortlich dafür, dass die Planung angestoßen wird und die relevanten Risikoinformationen zur Verfügung stehen. Der Risk-Owner übernimmt dann eine dem zentralen Risikocontrolling vergleichbare Funktion und begleitet den Planungsprozess beratend.

Eine wesentliche Aufgabe des dezentralen Risiko-Managements ist die Kommunikation relevanter Risikoinformationen entsprechend dem vorgegebenen Berichtswesen. Regelmäßig sollte an das zentrale Risikocontrolling über die Risiken sowie über die (Nicht-)Erreichung der Ziele des Risiko-Managements berichtet werden. Zur Vermeidung einer Überlastung der Berichtsempfänger ist die Vorgabe von Limits oder die Festlegung aggregierter, knapper Berichtsstandards sinnvoll. Außerdem sollte in bestimmten zeitlichen Abständen eine Gesamtrisikoposition ermittelt und kommuniziert werden (siehe oben). Dies ist vor allem unter dem Aspekt der Risikokumulation und -kompensation auf der Ebene des zentralen Risiko-Managements wichtig. Weiterhin müssen besonders dringlich erscheinende Risikopositionen sofort und direkt kommuniziert werden (Krisenmanagement; Ad-hoc-Berichterstattung).

Berichtswesen

Der im Rahmen eines funktionsfähigen Risiko-Managementsystems erforderliche Informationsfluss innerhalb der Organisation wurde oben beschrieben. Im Folgenden soll auf die einzelnen Berichte näher eingegangen werden. Dabei werden insbesondere Berichtsinhalte und -formen in Abhängigkeit der jeweiligen Adressaten dargestellt.

Innerhalb der beschriebenen Aufbauorganisation können im Wesentlichen drei Berichtsadressaten unterschieden werden:

- **Zentrales Risikocontrolling:** Das dezentrale Risiko-Management berichtet dem zentralen Risikocontrolling in regelmäßigen Abständen über die Risiken, eventuell in aggregierter Form über die Gesamtrisikoposition des Teilbereichs sowie über eingeleitete bzw. geplante präventive oder reaktive Risikobewältigungsmaßnahmen.
- **Vorstand:** Das zentrale Risikocontrolling berichtet dem Vorstand in regelmäßigen Abständen u. a. über bestandsgefährdende Risiken sowie über die Gesamtrisikoposition.
- **Aufsichtsrat:** Der Vorstand erstattet dem Aufsichtsrat in der Regel hochaggregierte Kurzberichte über die Risikosituation im Unternehmen.

Darüber hinaus ist natürlich eine Rückkopplung an die einzelnen dezentralen Risk-Owner oder Bereichsleiter über die Risiken in ihrem Bereich erforderlich. Dabei ist es wichtig zu unterscheiden, ob die Berichterstattung aus den dezentralen Bereichen über die Linienfunktionen erfolgt oder unter Umgehung von Linienkompetenzen. Letzteres dürfte eine „ungetrübtere" Sicht auf die Risikosituation des Unternehmens ermöglichen, kann aber durchaus zu erheblichen Spannungen zwischen Risk-Owner und Bereichverantwortlichem führen.

Bei einer direkten Berichterstattung könnte der Bereichsleitung der vom Risk-Owner für das zentrale Risikocontrolling erstellte Bericht zur Verfügung gestellt werden. In diesem Fall sollte der dezentrale Risiko-Manager ohnehin in ständigem Kontakt mit dem zuständigen Bereichsleiter stehen (vgl. dazu die aufgeführten Ansätze zur Organisation des dezentralen Risiko-Managements).

Die Berichtswege sollten wegen der skizzierten Problemstellungen – wenn dies nicht als kontraproduktiv eingeschätzt wird – an die bestehenden Gepflogenheiten im Unternehmen angepasst und in das bestehende Berichtswesen eingegliedert werden. Die Erstellung zusätzlicher Standardberichte kann u. a. aus Wirtschaftlichkeitsgründen in der Regel unterbleiben. So könnte z. B. die Risikoberichterstattung an den Vorstand zusammen mit den üblichen Monats-/Quartalsberichten erfolgen. Es muss allerdings sichergestellt werden, dass insbesondere bei drohenden Unternehmenskrisen zeitnah aktuelle Risikoinformationen bereitgestellt werden. Das Berichtswesen muss daher ausreichend flexibel sein und bei Eilbedürftigkeit unabhängig von institutionalisierten Kommunikationswegen und Periodizitäten eine direkte und schnelle Berichterstattung vorsehen.

Ein weiterer potenzieller Empfänger von Informationen aus dem Risiko-Management ist die Interne Revision zur Wahrnehmung ihrer Überwachungsfunktion auch über das Risiko-Managementsystem. Die Interne Revision kann zur Informationsbeschaffung einerseits auf die vorgesehenen Standardberichte zurückgreifen. Andererseits kann sie gezielt weitere Informationen anfordern bzw. selbst erheben. Aufgrund der hohen Spezifität ihrer Aufgabe ist aus heutiger Sicht die Erstellung weiterer Standardberichte für die Interne Revision nicht erforderlich. Zukünftig kann die Interne Revision selbstverständlich weitere Standardberichte einfordern, sofern diese für ihre Arbeit hilfreich sind.

Die Gesamtverantwortung für das Berichtswesen im Bereich Risiko-Management liegt bei dem zentralen Risikocontrolling. Es muss bei der Implementierung des Berichtswesens sicherstellen, dass der von Vorstand und Aufsichtsrat vorgegebene Informationsbedarf durch die (Standard)-Berichte gedeckt wird. Dabei ist insbesondere auf die Aktualität der Informationen zu achten.

Im Folgenden wird beispielhaft eine typische im Rahmen von Risiko-Management-Systemen (*RMS*) festgelegte Zuordnung der Aufgaben auf Vorstand, Risikocontrolling (*RC*) und Risk-Ownern (*RO*) dargestellt.

Aufgaben des Vorstandes:

- Der Vorstand ist gemäß § 91 Abs. 2 AktG verantwortlich für die Einrichtung eines Risiko-Managementsystems (*RMS*).
- Er legt die Unternehmensstrategie fest und entwickelt darauf aufbauend die Risikostrategie/-politik.
- Der Vorstand entscheidet über die strategische Risikoposition auf Basis der Unternehmensplanung und des Management Informationssystems (*MIS*)
- Er definiert die Ziele des Risikomanagementsystems (*RMS*) und die Aufgabenverteilung/-delegation.
- Er stimmt erforderliche Maßnahmen (Änderungen, Erweiterungen, Anpassungen) mit Risikocontrolling ab und informiert über risikorelevante Erkenntnisse (z. B. aus den Aufsichtsratsitzungen).
- Der Vorstand informiert regelmäßig den Aufsichtsrat (*AR*) durch komprimierte Risikoberichte.
- Er kommuniziert Risikostrategie und *RMS* im Unternehmen.

Aufgaben des Risikocontrollings:

- Das Risikocontrolling (*RC*) ist die zentrale Anlauf- und Kommunikationsstelle für alle Beteiligten des *RM*-Prozesses.
- Das *RC* steuert und begleitet den Risiko-Managementprozess.
- Es arbeitet an der Entwicklung/gegebenenfalls an den erforderlichen Anpassungen der Risikostrategie/-politik mit.
- Das *RC* kommuniziert Risikostrategie und *RMS* im Unternehmen (gemeinsam mit Vorstand).
- Es veranlasst Identifikation neuer Risiken: Risikoerfassung und -bewertung unter Beteiligung der Abteilungsleitungen (*AL*) und Beauftragten. Methode: Fragebogen, Workshops o. ä., einschließlich Ursachen-Wirkungs-Zusammenhänge, Szenario-Entwicklung, Einstufen in Relevanzkategorien.
- Das *RC* systematisiert die Einzelrisiken, definiert Doppel- und Mehrfachnennungen, fasst Risiken zusammen (bündelt), prüft Plausibilität und Konsistenz und stellt die Kommunikation mit dem Risk-Owner (*RO*) sicher.
- Das *RC* legt Indikatoren/Messgrößen/Limite mit *RO* fest.
- Es unterstützt *RO* methodisch und achtet auf Einheitlichkeit der Methoden (Coaching-Funktion).
- Das *RC* definiert Aufgaben/Verantwortlichkeiten/Berichtswesen für neu identifizierte Risiken.
- Es überwacht den Status der Risikobewältigungsmaßnahmen und koordiniert übergreifende Maßnahmen.
- Das *RC* wirkt bei der Entwicklung von Notfallplänen mit (unterstützt *RO*).

- Es stimmt Risikoinformationen mit anderen relevanten Projekten ab.
- Das *RC* stimmt sich mit dem Rechnungswesen regelmäßig über erforderliche Rückstellungen ab.
- Es ist für die Gestaltung und erforderliche Anpassungen der Arbeitsunterlagen zum *RMS* verantwortlich.
- Das *RC* aggregiert Risiken jährlich mittels Monte-Carlo-Simulation.
- Es informiert den Vorstand regelmäßig über die Risikosituation und die Erreichung der Risikoziele.

Aufgaben der Risk-Owner:

- Der Risk-Owner (*RO*) setzt Risiko-Management in Unternehmensbereichen um.
- Er nimmt wiederkehrende Risikoidentifikation und -bewertung vor.
- Er schlägt geeignete Risikobewältigungsmaßnahmen vor (Dokumentation in Risikomappen oder Datenbank).
- Der *RO* entwickelt gegebenenfalls Notfallpläne.
- Er aktualisiert/pflegt die Risikomappen für weiterbearbeitungsrelevante Risiken.
- Der *RO* setzt nach Beschluss Risikobewältigungsmaßnahmen um bzw. veranlasst Umsetzung durch andere Fachbereiche.
- Er kommuniziert relevante Risikoinformationen entsprechend dem vorgegebenen Berichtswesen.

Aufgaben der internen Revision:

- Die interne Revision (*IR*) überprüft das implementierte *RMS* auf Effektivität und Effizienz.
- Sie entwickelt Grundsätze und Standards für die Überwachung (Prüfung) des *RMS*.
- Die *IR* unterstützt und berät das Risikocontrolling bei der Entwicklung von Grundsätzen und Standards zum *RMS*.
- Sie informiert das Risikocontrolling über Prüfungsergebnisse und stimmt erforderliche Änderungen ab.

Berichterstattung an das zentrale Risikocontrolling

Das dezentrale Risiko-Management hat dem zentralen Risikocontrolling regelmäßig über die ausgewählten Risiken zu berichten. Soweit als möglich sollte eine quantitative Beurteilung der einzelnen Risiken erfolgt sein. Wesentlich sind dabei Angaben zur erwarteten Schadenshöhe, zur Eintrittswahrscheinlichkeit sowie zu bereits eingetretenen Schäden. Optimalerweise kann die Verteilungsfunktion des Risikos angegeben werden. Mindestens sollte das Risiko qualitativ in seiner Relevanz beurteilt werden.

Außerdem sollten wesentliche Änderungen in dem Umfeld bzw. in der Beurteilung einzelner Risiken dargestellt werden. Ergänzend können Informationen gegeben werden, wie

die Bewertung aus Sicht des Risk-Owners – mit einem entsprechenden Aufwand – noch verbessert werden könnte. Häufig kann z. B. durch externe Gutachten eine deutliche Verbesserung der Risikoquantifizierung erreicht werden.

Darüber hinaus muss über die bisher ergriffenen Maßnahmen zur Risikobewältigung, über bisher erreichte Erfolge und über zukünftig geplante Maßnahmen berichtet werden. Dabei sollte der erwartete Grad der Risikobewältigung – möglichst unter Angabe von Zeithorizonten – sowie die verbleibenden Restrisiken aufgezeigt werden. Besonders wertvoll für die weitere Analyse und Bearbeitung durch das zentrale Risikocontrolling sind Angaben zur Korrelation mit anderen Risiken, zur Systematik des Risikos sowie zur Relevanz des Risikos für andere Unternehmensbereiche.

Zur Vermeidung einer Überlastung der Berichtsempfänger sollte bei der Berichterstattung zwingend eine Abstufung nach der Relevanz der Risiken erfolgen. Diese Abstufung könnte z. B. anhand Tabelle 1 vorgenommen werden, wobei die Dynamik des Risikos zusätzlich zu berücksichtigen ist:

Tabelle 1: Berichterstattung an das Risikocontrolling

Relevanz	Berichtshäufigkeit
1	*j*
2	*q*
3	*q*
4	*m*
5	*w*
Legende: *j* = jährlich, *q* = quartalsweise, *m* = monatlich, *w* = wöchentlich	

Auch über weniger relevant erscheinende Risiken sollte zumindest einmal jährlich berichtet werden. Dies ist einerseits erforderlich zur Ermittlung einer unternehmensweiten Gesamtrisikoposition. Andererseits ist die Kenntnis auch weniger relevanter Risiken auf der Ebene des zentralen Risikocontrollings zur Risikoaggregation und -kompensation wichtig. Mehrere auf Bereichsebene als weniger relevant eingeschätzte Risiken können sich aus Gesamtunternehmenssicht unter Umständen zu einer bestandsgefährdenden Risikoposition kumulieren. Dabei ist nämlich zu beachten, dass Risiken sich gegenseitig verstärken können. Demgegenüber können sich wesentliche Risiken unterschiedlicher Bereiche ausgleichen. Aus dezentraler Sicht sinnvolle Risikobewältigungsmaßnahmen werden dann – zumindest teilweise – überflüssig. Ein Beispiel hierfür wären Währungsrisiken aus langfristigen Liefer- und Abnahmeverträgen.

Über das beschriebene formale Berichtssystem hinaus muss die Möglichkeit bzw. die Pflicht bestehen, bei Eilbedürftigkeit direkt und sofort an das zentrale Risikocontrolling (oder einen anderen „passenden" Adressaten) zu berichten. Eine solche „Sofortberichter-

stattung" kann z. B. bei neu auftretenden, bestandsgefährdenden Risiken, bei einer drastischen Änderung der Risikoeinschätzung grundsätzlich bekannter Risiken oder bei bedeutenden, tatsächlich eingetretenen Schäden notwendig sein.

Ein wesentlicher Erfolgsfaktor bei der Risikobewältigung ist die dann oft Schnelligkeit, mit der die entsprechende Maßnahme umgesetzt wird. So können z. B. Imageschäden im Zusammenhang mit Umweltverstößen/Störfällen/Unfällen häufig durch eine rechtzeitige, gezielte und koordinierte Information der Öffentlichkeit gemindert werden. Wird die Öffentlichkeit hingegen zunächst durch externe Quellen informiert, so ist der Schaden in der Regel größer, da externe Quellen meist keine Rücksicht auf „Imagewirkungen" eines Berichts nehmen. Das Unternehmen kann dann allenfalls mit einer Gegendarstellung reagieren. Eine flexible und unbürokratische Risikokommunikation zwischen dezentralem Risiko-Management und zentralem Risikocontrolling hilft also insbesondere bei drohenden Unternehmenskrisen die meist knappe Reaktionszeit optimal zu nutzen.

Berichterstattung an den Vorstand

Die Berichterstattung an den Vorstand erfolgt grundsätzlich entsprechend den Informationsbedürfnissen des Vorstands. Diese sind von dem Vorstand selbst zu definieren und von dem zentralen Risikocontrolling bei der Implementierung des Risiko-Berichtswesens umzusetzen. Dabei sind insbesondere die Sicherheitsziele des Vorstands zu beachten.

Das KonTraG fordert zumindest eine regelmäßige Information des Vorstands über alle nicht bewältigten, bestandsgefährdenden Risiken. Wahrscheinlich wird der Vorstand jedoch darüber hinausgehend weitere Risikoinformationen wünschen, eventuell abgestuft nach der Relevanz der einzelnen Risiken. Zur Vermeidung einer Überlastung des Vorstands könnte dabei ähnlich wie bei der Berichterstattung von dem dezentralen Risiko-Management an das zentrale Risikocontrolling Tabelle 2 verwendet werden, wobei die Dynamik des Risikos zusätzlich zu berücksichtigen ist:

Tabelle 2: Berichterstattung an den Vorstand

Relevanz	Berichtshäufigkeit
1	–
2	*j*
3	*q*
4	*m*
5	*m*

Legende: *j* = jährlich, *q* = quartalsweise, *m* = monatlich, *w* = wöchentlich

Selbstverständlich wird die Risikoberichterstattung an den Vorstand in aggregierter Form erfolgen. Hinsichtlich der Informationen zu einem einzelnen Risiko wird sich der Bericht des zentralen Risikocontrollers/-managers an den Vorstand jedoch kaum von den Berichten der jeweiligen Risk-Owner unterscheiden. So ist auch hier eine Klassifizierung der Risiken vorzunehmen und die Risiken sind – insbesondere hinsichtlich Ursachen und Wirkungen – näher zu beschreiben und quantitativ oder qualitativ zu beurteilen. Änderungen im Umfeld bzw. in der Beurteilung einzelner Risiken müssen ebenso erläutert werden wie die bereits eingetretenen Schäden.

Das zentrale Risikocontrolling muss außerdem sowohl die schon ergriffenen als auch die geplanten Risikobewältigungsmaßnahmen beschreiben. Dabei sind Angaben zum zeitlichen Verlauf der Risikobewältigung, zu den bereits erzielten Erfolgen sowie zu den verbleibenden „Rest"-Risiken zu machen.

Die von dem zentralen Risikocontrolling auf Basis der Berichte der Risk-Owner und unter Nutzung des Aggregationsmodells ermittelte Gesamtrisikoposition ist in die Berichterstattung an den Vorstand ebenfalls einzubeziehen. Für die Unternehmenssteuerung besonders wichtig sind dabei Informationen zu den möglichen Auswirkungen der Risiken auf den ökonomischen Wert des Eigenkapitals.

Wie bereits mehrfach ausgeführt muss bei Eilbedürftigkeit eine flexible, direkte und zeitnahe Berichterstattung erfolgen. Eilmeldungen an den Vorstand können z. B. bei drohenden Unternehmenskrisen oder bei plötzlichen, drastischen Umfeldveränderungen erforderlich sein. Operationalisierbare Schwellenwerte für solche Eilmeldungen sind schwer festzulegen, da meist eine Einzelfallbetrachtung erforderlich ist. Im Zweifel sollte aufgrund der unter Umständen hohen Bedeutung für den Fortbestand des Unternehmens lieber zu oft als zu selten außerhalb der formalen Berichte gemeldet werden.

Berichterstattung an den Aufsichtsrat

Ähnlich wie der Vorstand muss auch der Aufsichtsrat seine Informationsbedürfnisse selbst definieren. Dies könnte z. B. im Rahmen einer Informationsordnung erfolgen. Der Vorstand muss dem Aufsichtsrat entsprechend dieser Informationsordnung berichten bzw. die Bereitstellung der gewünschten Informationen sicherstellen.

Grundsätzlich hat der Aufsichtsrat ähnliche Informationsbedürfnisse wie der Vorstand. Allerdings wird er für seine Überwachungstätigkeit (im Gegensatz zur Leitungs- und Steuerungsfunktion des Vorstands) eine noch höhere Aggregationsebene sowie höhere Meldegrenzen vorgeben. Außerdem wird er eine geringere Berichtshäufigkeit verlangen. Diese könnte – abgestuft nach der Relevanz eines Risikos – z. B. wie in Tabelle 3 dargestellt – bestimmt werden, wobei die Dynamik des Risikos zusätzlich zu berücksichtigen ist:

Der Aufsichtsrat wird insbesondere Informationen zu Ursachen und Wirkungen der gemeldeten Risiken erwarten. Außerdem müssen Risikobewältigungsmaßnahmen, bereits eingetretene Erfolge und Schäden sowie der prognostizierte Schadensverlauf (unter Berücksichtigung der Maßnahmen) je Risiko dargestellt werden. Dabei sollte sich die

Tabelle 3: Berichterstattung an den Aufsichtsrat

Relevanz	Berichtshäufigkeit
1	–
2	–
3	*j*
4	*q*
5	*q*
Legende: *j* = jährlich, *q* = quartalsweise, *m* = monatlich, *w* = wöchentlich	

Berichterstattung auf wesentliche Aspekte beschränken (Kurzberichterstattung). Zusätzlich sollte dem Aufsichtsrat ebenfalls über die Gesamtrisikoposition berichtet werden. Dies kann wiederum durch Darstellung der Ergebnisse des Risikoaggregationsmodells erfolgen.

Zudem ist auch der Aufsichtsrat bei drohenden Unternehmenskrisen zeitnah und direkt zu informieren. Gerade in Krisenzeiten gewinnt die Überwachungsfunktion des Aufsichtsrats an Bedeutung. Die Berichtsfrequenz kann auf Anordnung des Aufsichtsrats dann deutlich erhöht werden. Informationen sollten bei solchen Krisen möglichst ungefiltert den Aufsichtsrat erreichen. Dies muss organisatorisch – bereits vor Eintritt der Krise – sichergestellt werden.

Überwachungsfunktion und Revision

Zu einem funktionsfähigen Managementsystem gehört immer auch die regelmäßige „Selbstprüfung". Dabei ist zu untersuchen, ob das System nicht nur auf dem Papier existiert, sondern auch in der Praxis angewendet wird. Daneben können sich durch veränderte Umfeldbedingungen Änderungsanforderungen für das System ergeben. Beispielsweise könnten Veränderungen in der Risikolandschaft des Unternehmens es erforderlich machen, neue Risiken in das Risiko-Managementsystem aufzunehmen oder Veränderungen der grundsätzlichen Organisationsstruktur machen eine Neuzuordnung der Risk-Owner erforderlich. Die Einarbeitung solcher Änderungen stellt einen weiteren Prüfungsschwerpunkt dar.

Die Aufgabe der Überprüfung des Risiko-Managements im Hinblick auf Funktionsfähigkeit und auf die Anwendung des Systems wird typischerweise durch die interne Revision übernommen. Sofern eine interne Revision im Unternehmen etabliert ist, stellt dies in der Regel keine besondere Herausforderung dar. Die interne Revision wird ihre Prüfpläne anpassen und die Überprüfung des Risiko-Managementsystem in ihre ohnehin stattfinden Untersuchungen integrieren. Voraussetzung dafür ist natürlich, dass die interne Revision

die Zielsetzungen kennt, die mit dem Risiko-Management verbunden sind. Entsprechende Schulungen der Mitarbeiter der internen Revision zum Verständnis für Risiko-Managementsysteme sind daher erforderlich.

Nicht selten findet eine intensive Auseinandersetzung der Revision mit dem Thema Risiko-Management bereits in der Phase des Systemaufbaus statt. Häufig wird die Revision nicht nur beratend und informativ in die Gestaltung und den Aufbau des System involviert, sondern übernimmt sogar verantwortlich das Projektmanagement.

Sicherlich ist es kritisch zu bewerten, dass die Revision später dann für die Überprüfung eines Systems zuständig ist, das sie maßgeblich selbst mit gestaltet hat. Eine gewisse Befangenheit kann wohl unterstellt werden. Andererseits ist die interne Revision dann in besonderem Maße mit der Zielsetzung des Risiko-Managementsystems vertraut und kann hinterher umso präziser überprüfen, ob das unter ihrer Mithilfe geschaffene System tatsächlich das leistet, was es soll.

Dieser Aspekt – zusammen mit dem umfangreichen Wissen, das die interne Revision mit in das Projekt einbringen kann – überwiegen m.E. den Nachteil der Befangenheit bei der Überprüfung des Systems. Dies gilt allerdings vor allem unter der Rahmenbedingung, dass das Unternehmen sein Risiko-Managementsystem dann nicht ausschließlich von der internen Revision sondern auch durch externe Stelle prüfen lässt. Im Falle einer Aktiengesellschaft, die Aktien mit amtlicher Notierung herausgibt, ist die externe Prüfung des Systems durch den Wirtschaftsprüfer sogar vorgeschrieben (§317 HGB). Sofern eine interne Revision nicht im Unternehmen etabliert ist, könnte die Überprüfung des Risiko-Managementsystem dann auch grundsätzlich durch Externe vorgenommen werden, beispielsweise durch die Erweiterung des Prüfungsauftrags des Wirtschaftprüfers.

Natürlich sind – unter Berücksichtigung gesetzlicher und inhaltlicher Anforderungen an eine solche Systemprüfung – auch andere Möglichkeiten der Systemprüfung vorstellbar, beispielsweise durch Beratungsgesellschaften oder andere unabhängige interne Stellen oder „Überkreuzprüfungen" innerhalb der Gesellschaft bzw. zwischen verschiedenen Tochtergesellschaften eines Konzerns.

5. Die Dokumentation im Überblick: das Risikohandbuch

Das Risiko-Managementhandbuch

Es gibt keine eindeutigen und verbindlichen Regelungen für Aufbau und Inhalt eines Risiko-Managementhandbuchs. Es sollte jedoch alle wesentlichen Elemente eines Risiko-Managementsystems beschreiben oder beinhalten.

Die einzelnen Kapitel des Handbuchs haben dabei die im Folgenden kurz skizzierte Bedeutung bzw. sind wie folgt zu handhaben. Im Falle von Aktualisierungen oder Fortschreibungen wird die Aufbewahrung der vorangegangenen Dokumentationen mit dem Hinweis „Nicht mehr gültig" empfohlen, da dadurch automatisch eine „Historie" der Ent-

wicklung des Risiko-Managementsystems entsteht. Eine vergleichbare Regelung sollte sich auch im Bereich der EDV-gestützen Dokumentation und Handhabung eines Risiko-Managements finden.

Kapitel „Projektmanagement“

Das Handbuchkapitel „Projektmanagement“ verfolgt zwei Intentionen. Zum einen dokumentiert es den Ablauf des Projektes zur Einführung eines Risiko-Managementsystems und hat für spätere Revisionen des Systems richtungsweisenden und informativen Charakter. Zum anderen empfiehlt es sich, an einer Stelle der Gesamtdokumentation ein „Lexikon“ zum Thema Risiko-Management einzufügen. In diesem finden sich dann fachlichen Erläuterungen. Ein solches Lexikon dient dann der laufenden Sammlung von Informationen z. B. über Neuerungen zum Thema Risiko-Management und erleichtert damit auch die Einarbeitung von neuen Mitarbeitern in das Thema.

Der erste Teil dieses Kapitels hat dementsprechend reinen Dokumentationscharakter; der zweite Teil wird an das unternehmensindividuelle Informationsbedürfnis und an externe Veränderungen angepasst werden.

Kapitel „Risikoanalyse“

Dieses Kapitel beschreibt die Anwendung der Methoden zur Risikoanalyse eines Unternehmens und dokumentiert die Ergebnisse dieser Risikoanalyse. Es beschreibt somit die Risikosituation des Unternehmens nach der Risikoidentifikation und nach der Risikobewertung zu einem bestimmten Zeitpunkt. Da alle relevanten Risiken anschließend in das Risiko-Managementsystem des Unternehmens eingestellt werden und dort laufend dokumentiert werden (siehe Kapitel Monitoring & Coaching) bleibt das Kapitel Risikoanalyse in der Regel unverändert (gegebenenfalls kann zum Beispiel nach dem Ablauf von mehreren Jahren oder grundlegender Veränderung im Unternehmen die Wiederholung einer entsprechend umfassenden Analyse und Dokumentation sinnvoll erscheinen).

Kapitel „Risikoaggregation“

Das Kapitel Risikoaggregation dokumentiert die Ermittlung der zusammengefassten Wirkung aller als relevant erachteten Risiken. In der Regel geschieht dies mittels eines dafür entwickelten Unternehmensmodells und durch den Einsatz der Monte-Carlo-Simulation. Dabei wird u. a. der Value-at-Risk bestimmt und der Einfluss einzelner Risiken auf die Gesamtrisikoposition analysiert. Diese Informationen sind von zentraler Bedeutung für die Steuerung des Risiko-Managementsystems, für die Simulation von Unternehmensszenarien sowie beispielsweise für das Kreditmanagement und müssen daher regelmäßig neu berechnet werden. Jede Aktualisierung wird der bestehenden Dokumentation angefügt.

Kapitel „Risikobewältigung“

Das Kapitel Risikobewältigung beschreibt die ersten Maßnahmen, die als direkter Ausfluss der vorangehenden Riskomanagementaktiviäten umgesetzt werden. Diese Maßnahmen werden also in der Regel ad hoc beschlossen und dienen der präventiven Veränderung der Risikosituation des Unternehmens. Maßnahmen zur Risikobewältigung werden auch nach Abschluss des Projekts initiiert werden und können in diesem Handbuchkapitel dokumentiert werden. Aus Gründen der Übersichtlichkeit bietet es sich jedoch an, in diesem Kapitel nur eine Übersicht über die Maßnahmen zu geben, die Risiken betreffen, die in das kontinuierliche Risiko-Management des Unternehmens eingestellt werden. Für solche Risiken existiert in der Regel eine Risikomappe (vgl. unten Kapitel „Monitoring und Coaching), in der alle relevanten Informationen um dieses Risiko dargestellt werden. Möglicherweise besteht das Kapitel Risikobewältigung im Kern dann nur aus Querverweisen in das Kapitel Monitoring und Coaching.

Kapitel „Systemgestaltung“

Das Risiko-Management eines Unternehmens endet nicht nach der einmaligen Erhebung und Bewertung der Risiken. Risiko-Management ist ein permanenter Prozess. Die Gestaltung dieses Prozesses sowie die zugehörige Gestaltung der Aufbauorganisation und des Berichtswesens wird im Kapitel Systemgestaltung beschrieben. Die Systemgestaltung unterliegt ebenso wie das Risiko-Management einer Dynamik, die Anpassungen an Veränderungen erforderlich macht. Diese zukünftigen Veränderungen und Anpassungen sind ebenfalls in diesem Kapitel zu dokumentieren.

Kapitel „Implementierung“

Das Kapitel Implementierung dokumentiert die Einführung des Risiko-Managementsystems. Dieses Kapitel dient damit in der Regel nur der Dokumentation der erstmaligen Einführung (sofern dies nicht im Kapitel Projektmanagement ausführlich geschah) sowie der in dieser Zeit gültigen Übergangsregelungen. Spätere Veränderungen werden in den entsprechenden Kapiteln beschrieben (z. B. in den Kapiteln Risikobewältigung oder Systemgestaltung).

Kapitel „Risikokultur“

Das Kapitel Risikokultur beinhaltet als zentrale Bestandteile der Risikokultur einerseits die Erklärung des Vorstandes bzw. der Geschäftsleitung zur Risikopolitik des Unternehmens und andererseits die Dokumentation aller Maßnahmen, die der Umsetzung der Risikopolitik und der Förderung eines bewussten Umgangs der Mitarbeiter mit Risiken im Unternehmen dienen. Beide Abschnitte unterliegen aufgrund der Dynamik des Risiko-Manage-

ments einem Anpassungs- und Änderungsbedarf. Diese Veränderungen werden in diesem Kapitel dokumentiert.

Kapitel „Monitoring & Coaching“

Das Kapitel Monitoring & Coaching dokumentiert eines der „Herzstücke“ des Risiko-Managements, nämlich die laufenden Aktivitäten zur Überwachung und Handhabung der als relevant erachteten Risiken. Dieses Kapitel unterliegt einer ständigen Veränderung und Anpassung. Insbesondere werden hier die regelmäßige Berichterstattung der Risk-Owner an den zentralen Risikocontroller und dessen Berichterstattung an den Vorstand des Unternehmens dokumentiert. Zur besseren Gliederung besteht dieses Kapitel vor allem aus den einzelnen Risikomappen, in denen alle zu einem Risiko relevanten Informationen zusammengefasst werden. Diese Risikomappen dienen dabei nicht nur einfach der Dokumentation sondern sind die Arbeitsunterlage für die Risk-Owner (vgl. Kapitel 13 „Hilfsmittel im Risiko-Management: Risikomappen und Analyseblätter“).

6. Die Kultur des Risiko-Managements

Ausgangspunkt der Entwicklung von Risikopolitik und -strategie sind die Unternehmensziele. Diese werden unter Beachtung externer und interner Faktoren (z. B. ökonomische, technologische und soziale Faktoren) festgelegt. Bei Unternehmenszielen kann es sich u. a. um finanzielle Zielgrößen (z. B. Shareholder-Value) oder um leistungswirtschaftliche Ziele (z. B. Marktziele und Qualitätsziele) handeln. Die einzelnen Unternehmensziele sind in ein unternehmensweites Zielsystem zu überführen. Unmittelbar damit verbunden sind die Ziele des Risiko-Managements: die Abwehr der Gefahren für die Unternehmensziele sowie, daraus abgeleitet, die Sicherung des Unternehmensbestands und des künftigen Erfolgs. Die Vermeidung sämtlicher Risiken bzw. die Schaffung eines risikolosen Zustands ist hingegen **nicht** Ziel des Risiko-Managements.

Aus diesen Risiko-Managementzielen sind die Risikostrategie und -politik sowie die konkreten Vorgaben für die Identifizierung, Bewertung und Bewältigung der Risiken herzuleiten. Diese Vorgaben umfassen auch die Toleranzgrenzen (Limite), bei deren Überschreiten ein Risiko für das Unternehmen nicht mehr akzeptabel ist und Abwehrmaßnahmen erforderlich sind. An diesen Sicherheitszielen sind die identifizierten und bewerteten Risiken zu messen.

Die strategischen Vorgaben für die Steuerung von Risiken hängen von dem Ausmaß und der Anzahl (Gefährdungspotenzial hinsichtlich der Eintrittswahrscheinlichkeit und der Schadenshöhe) einzelner Risikopositionen ab. Unternehmen werden regelmäßig mit einer Vielzahl verschiedener Risiken konfrontiert, die gesondert oder gemeinsam zu bewältigen sind. Das Ausmaß der Risiken reicht dabei von geringfügigen bis hin zu existenzbedrohenden Risiken. Die Unternehmensleitung muss daher eine Antwort auf die Frage finden, welche Auswirkungen ein Schadensfall für das Unternehmen im Einzelnen oder mit anderen Risken verbunden hat bzw. haben könnte.[19]

Die Risikostrategie ist in die gesamte Unternehmensstrategie einzubinden und schriftlich zu fixieren. Sie muss außerdem an die Mitarbeiter in den Unternehmensbereichen ausreichend kommuniziert werden. Dazu gehört auch die Schaffung und Förderung einer Risikokultur im Unternehmen.

Voraussetzung dafür ist, dass durch die Geschäftsleitung des Unternehmens zunächst allgemeine Aussagen zur Risikokultur des Unternehmens formuliert werden, an denen sich die Mitarbeiter orientieren können und die die Einstellung der Geschäftsleitung zum Thema „Risiko“ transparent machen. Zur Konkretisierung bietet es sich an, sowohl die strategische Zielsetzung des Unternehmen im Kontext des Risiko-Managements zu beleuchten und ein Limitsystems zu verabschieden, das den Mitarbeiter als Leitlinie in ihrer täglichen Arbeit dient.

Dieses Limitsystem wird zunächst festlegen, welches Gesamtrisiko für das Unternehmen überhaupt akzeptabel ist (z. B. als Verhältnis von Value-at-Risk zu (ökonomischem Eigenkapital). Daneben sollte festgezurrt werden, welche Risiken das Unternehmen zu seinen Kernrisiken zählt und was Randrisiken sind. Unter Kernrisiken werden dabei diejenigen Risiken verstanden, die aus den Kerngeschäfts des Unternehmen resultieren und somit Ausdruck seiner eigentlichen unternehmerischen Tätigkeit sind. Diese Risiken muss das Unternehmen selbst tragen. Es würde sich sonst seiner unternehmerischen Chancen berauben. Randrisiken sind im Prinzip alle Nicht-Kernrisiken. Diese Risiken sind „nicht im Interesse“ des Unternehmens. Sie sollten „bewältigt“ werden, d. h. es sollte nach Handlungsalternativen im Umgang mit den Risiken gesucht werden die die Belastung des Risikodeckungspotenzial des Unternehmens reduzieren, damit dieses für „die richtigen“ Risiken zur Verfügung steht. Die Kompetenzen und Ressourcen des Unternehmens sind also möglichst so einzusetzen, das sich für das Unternehmen aus der Risikohandhabung auch Chancen für den Unternehmenserfolg ergeben.

Für alle relevanten Risiken sollten daher Limite oder auch sogenannte Sicherheitsziele geben an, ab wann eine Risikoposition nicht mehr akzeptabel ist und Maßnahmen zur Bewältigung des Risikos ergriffen werden müssen. Die Limite sind u. a. in Abhängigkeit von der Risikobereitschaft des Managements, den Unternehmenszielen sowie den Umweltbedingungen festzulegen. Ist das Unternehmen eher risikofreudig, so werden die Limite tendenziell höher liegen als bei einem vergleichbaren risikoaversen Unternehmen. Sicherheitsziele sind also für jedes Unternehmen individuell zu formulieren und können nicht pauschal vorgegeben werden.

Allerdings muss das Risiko-Managementsystem von Aktiengesellschaften und deren Tochterunternehmen aufgrund des KonTraG (vgl. § 91 Abs. II AktG) gewährleisten, dass bestandsgefährdende Risiken frühzeitig erkannt werden. Bei der Gefährdung des Fortbestands des Unternehmens ist daher ein Limit zu setzen, dessen Überschreitung in jedem Fall entsprechende Maßnahmen auslösen muss. Ab wann eine Risikoposition als bestandsgefährdend einzustufen ist, ist wiederum von der speziellen Situation des Unternehmens abhängig. Risiken werden jedoch häufig dann als bestandsgefährdend eingestuft, wenn ihr Eintreten mehr als die Hälfte des Eigenkapitals aufzehrt. Besitzt eine solche Risikoposition zudem eine hohe Eintrittswahrscheinlichkeit, dann muss von einer eklatanten Be-

standsgefährdung ausgegangen werden. In der Regel wird die Unternehmensleitung jedoch nicht erst bei einer solchen Bestandsgefährdung Bewältigungsmaßnahmen einleiten wollen. Daher sollten die Limite in der Praxis deutlich niedriger festgelegt werden. Bei dieser Beurteilung sollte auf ökonomische Größen und nicht auf buchhalterische Daten Bezug genommen werden (sinnvoller Weise sollte der Bezug zum Unternehmenswert hergestellt werden). Darüber hinaus ist zu beachten, dass der Verzehr von Eigenkapital nicht das ausschließliche Kriterium für die Beurteilung der Relevanz eines Risiko sein wird. Im Kontext der Unternehmensplanung – in dem Risiko-Management zu sehen ist – wird häufig eine Orientierung an den planerischen Zielgrößen – z. B. Gewinn oder Cash-Flow – stattfinden.

Sicherheitsziele sind nicht nur auf der obersten Unternehmensebene zu formulieren. Sie müssen vielmehr für jeden risikobehafteten Unternehmens- bzw. Fachbereich definiert werden. Die Limite sollten dabei umso detaillierter bzw. operationaler festgelegt werden, je stärker die Risikobewältigung an Mitarbeiter nachgelagerter Hierarchieebenen delegiert wird. Bei der Festlegung der einzelnen Limite ist auf eine unternehmensweite Konsistenz des Limitsystems zu achten. Es empfiehlt sich ein Top-down-Vorgehen, also ein Ableiten der Bereichs-Limite aus den übergeordneten unternehmensweiten Limiten.

Das Limitsystem ist zudem von zentraler Bedeutung bei der Implementierung eines Risiko-Berichtwesens. Aus methodischen Gründen ist darauf hinzuweisen, dass die Entwicklung eines sinnvollen Limitsystems kaum ohne eine „echte" Risikoaggregation möglich sein dürfte. Zwar kann bei isolierter Betrachtung für ein einzelnes Risiko ein Limit festgelegt werden, aus der Sicht des Gesamtsystems ist dies jedoch unbefriedigend. Genauso wenig wie Risiken additiv aggregiert werden können (es sei denn, sie sind zu 100 Prozent korreliert) lässt sich ein Limitsystem über diese Methode sinnvoll gestalten.

Zur Schaffung einer Risikokultur gehören jedoch nicht nur die Festlegung der Regeln dieser Kultur sondern auch „das Leben" dieser Regeln. Implementierung des Systems und Schaffung einer entsprechenden Kultur sind daher eng miteinander verzahnt (vgl. hierzu das Kapitel „Einführung eines Risiko-Managementsystems" in diesem Handbuch).

7. Ausblick: die (risiko-)strategiekonforme Gestaltung des Unternehmens

Von der Gestaltung des Risiko-Managements klar zu unterscheiden ist die strategie- bzw. risikokonforme Gestaltung des Unternehmens als Ganzes. Auch im Rahmen des Risiko-Managements sollten natürlich die Schwerpunkte so gesetzt werden, dass die Handhabung eines Risikos in Relation zu den Relevanz steht. Dies sollte sich z. B. bei der Intensität der Überwachung, Dokumentation und Berichterstattung niederschlagen.

Ein Risiko-Managementsystem aufzubauen kann als erster Schritt einer risikokonformen Unternehmensgestaltung gesehen werden. Zumindest, wenn es in die Planung des Unternehmens integriert wird und somit das Risiko-Management den gleichen Stellenwert erhält wie die Erlösplanung. Diesbezüglich wäre dann „Konformität" gegeben.

Wesentlich diffiziler wird es, wenn nun aber das gesamte Unternehmen adäquat zu seiner Strategie (einschließlich der Risikostrategie) ausgerichtet werden soll. Dazu wäre es erforderlich den Beitrag zur Strategieerfüllung einzelner Organisationseinheiten zu messen und ein möglichst ausgeglichenes Verhältnis zwischen Nutzen der Einheit und durch die Einheit verursachten Kosten sowie dem Beitrag (Verursachung oder Bewältigung) zur Risikosituation zu schaffen.

Wenn gleich diese Fragestellung derzeit noch nicht befriedigend beantwortet werden kann, so gibt es doch einige Anhaltspunkte für eine zielführende Vorgehensweise.

Ein Mehrwert für ein Unternehmen entsteht dann, wenn eine Handlungsoption dem Unternehmen einen positiven Kapitalwert bringt. Dieser Kapitalwert ist als diskontierte Summe der aus der Handlungsoption resultierenden Free-Cash-Flows zu berechnen. Die Diskontierung muss zu einem risikoadäquaten Zins erfolgen. „Riskantere" Handlungsoptionen sind mit einem höheren Zins zu belasten.

Dementsprechend sollte auch der einer Organisationseinheit zuzuordnende Nutzen nicht nur größer als die verursachten Kosten sein, auch sollte das Kosten-Nutzen-Verhältnis entsprechend zu dem durch die Organisationseinheit verursachten Risiko stehen. Je größer also das verursachte Risiko, desto weiter sollte der Nutzen die Kosten überragen.

Anmerkungen

1 Siehe dazu auch die Erläuterungen zur Risikoidentifikation und Risikoanalyse in diesem Handbuch.

2 Anmerkung des Autors: Gemeint ist die Prüfung des Jahresabschlusses durch den Wirtschaftprüfer.

3 Vgl. Füser/Gleißner/Meier, Der Betrieb 1999, S. 753.

4 Vgl. Weitekamp, Versicherungswirtschaft 1997, S. 1759.

5 Vgl. Jacob, Wpg 1998, S. 1045.

6 Vgl. Füser/Gleißner/Meier, Der Betrieb 1999, S. 754.

7 Vergleiche dazu den Abschnitt „Hilfsmittel im Risiko-Management: Risikomappen und Analyseblätter" dieses Handbuches.

8 Eine ausführlichere Darstellung der Vorgehensweise finden Sie im Abschnitt „Die Analyse von Leistungsrisiken – eine Methodenbeschreibung" dieses Handbuches.

9 Vgl. dazu ausführlich Gleißner, Versicherungswirtschaft 13/1999, S. 926ff.

10 Vgl. Füser/Gleißner/Meier, Der Betrieb 1999, S. 757.

11 Vergleiche dazu den Abschnitt „Hilfsmittel im Risiko-Management: Risikomappen und Analyseblätter" dieses Buches.

12 Dies ist außerdem im Hinblick auf die aus dem KonTraG abgeleiteten Dokumentationspflichten hilfreich, vgl. dazu IDW EPS 340 Nr. 3.6.

13 Vergleiche dazu vor allem den Prüfungsstandard IDW PS 340 sowie den Prüfungsstandard IDW PS 720 für Unternehmen, die dem Haushaltsgrundsätzegesetz unterliegen.

14 Vgl. Vogler, M./Gundert, M. (1998), Einführung von Risiko-Managementsystemen, Der Betrieb, Heft 48,51. Jg., 1998, S. 2378.

15 Vgl. Kendall, Robin, Riskmanagement, 1998.

16 Vgl. dazu die Verlautbarung des Bundesaufsichtsamtes für das Kreditwesen vom 23.10.1995.

17 Vgl. IDW EPS 340 Tz. 3.5.

18 In Anlehnung an Vogler, M./Gundert, M. (1998), Einführung von Risiko-Managementsystemen, Der Betrieb, Heft 48,51. Jg., 1998, S. 2378.

19 Vgl. Füser/Gleißner/Meier, Der Betrieb 1999, S. 753.