Risk-Management-Informationssysteme
– Potentiale einer umfassenden IT-Unterstützung des Risk Managements –

Dr. Roland F. Erben / Frank Romeike

Inhaltsübersicht

Zusammenfassung

Um bei zunehmenden Risiken wirtschaftlich erfolgreich zu sein, wird eine adäquate Informationsversorgung der Entscheider immer wichtiger. Im folgenden Beitrag wird – ausgehend von einer Analyse der Ursachen für die verschärfte Risikosituation – die Rolle von Informationssystemen im Rahmen des Risk Managements untersucht. Besonderer Augenmerk liegt dabei auf der Frage, inwieweit bzw. in welchen Phasen ein RMIS den Risk Management Prozess effizient unterstützen kann.

1 Einleitung

Der zunehmend globalisierte Wettbewerb auf deregulierten Märkten, die wachsende Komplexität der Unternehmensumwelt sowie rasante Entwicklungen im Bereich der Informations- und Kommunikationstechnologie (IuK) eröffnen neue Chancen, bergen aber gleichzeitig auch neue Risiken für die Unternehmen. Die wachsende Komplexität und Dynamik der Unternehmensprozesse und dezentrale Unternehmensstrukturen sowie kürzere Reaktionszeiten haben in den letzten Jahren zu einer fundamental veränderten Risikolage der Unternehmen geführt. [0, Romeike,

S. 412] Gleichzeitig sind Unternehmen auch einem verstärkten Kostendruck ausgesetzt. Mit Hilfe von „unternehmerischer Intuition“ und reaktiven Steuerungssystemen dürfte es immer schwieriger werden, diese Komplexität der Prozesse und Risiken zu erfassen und zu analysieren. Ein funktionierendes und effizientes Risikomanagement, eine gelebte Risiko- und Kontrollkultur sowie ein effizientes IT-gestütztes Risk-Management-Informationssystem entwickelt sich zunehmend zu einem wesentlichen Erfolgsfaktor für Unternehmen. Nur diejenigen Unternehmen, die ihre Risiken effizient steuern und kontrollieren sowie ihre Chancen erkennen und nutzen werden langfristig erfolgreich sein und ihren Unternehmenswert steigern. Eine zentrale Rolle bei der Erreichung dieses Ziels spielt dabei die moderne Informationstechnologie, mit deren Hilfe sich der Prozess des Risk Managements auf vielfältige Weise optimieren lässt.

Im 21. Jahrhundert sind Unternehmen aufgrund völlig veränderter Rahmenbedingungen mit neuen Herausforderungen konfrontiert. Unternehmerisches Handeln ist sicherlich seit jeher untrennbar mit der Übernahme von Risiken verbunden – Chance und Risiko sind die beiden Seiten ein und derselben Medaille. Die teilweisen spektakulären Fälle der jüngeren Vergangenheit (in diesem Zusammenhang seien nur kurz die Namen Holzmann, Enron, Metallgesellschaft oder Barings erwähnt) machen schmerzhaft deutlich, dass das Management dieser Chancen und Risiken in vielen Unternehmen offensichtlich nicht den Stellenwert einnimmt, der eigentlich erforderlich wäre.

Zu viele Unternehmen konzentrieren ihre Risikomanagement immer noch auf technische Gefahrenpotentiale oder so genannte „financial risks“, wie z. B. die Absicherung von Fremdwährungspositionen, das Debitorenmanagement oder die Auswahl einer geeignet erscheinenden Versicherungslösung. Zudem basiert eine solche „Risikobuchhaltung“ in vielen Fällen weniger auf der systematischen Gewinnung und Verarbeitung relevanter Informationen, als vielmehr auf subjektiven Einschätzungen oder der vielzitierten „unternehmerischen Intuition“ [1, Braun, S. 57] Es erscheint offensichtlich, dass eine derartige Vorgehensweise, die unter den relativ konstanten Umweltbedingungen der vergangenen Jahrzehnte vielleicht noch hin-

genommen werden konnte, in Anbetracht der dramatisch verschärften Risikosituation in der heutigen Zeit keinesfalls mehr akzeptabel ist.

In diesem Zusammenhang kommt der modernen Informations- und Kommunikationstechnologie eine Schlüsselrolle zu: Ein holistisches Risikomanagement, mit dessen Hilfe sich die externen und internen Chancen und Risiken eines Unternehmens adäquat abbilden und analysieren lassen, setzt die Verarbeitung einer Unmenge von Informationen aus unterschiedlichsten Quellen voraus. Diese Herausforderung kann nur bewältigt werden, wenn Informationssysteme zur Verfügung stehen, die dem Manager die entscheidungsrelevanten Informationen auch tatsächlich liefern können [2, Erben/Nagel/Piller, S. 32].

2 Komplexität als Ursache von Risiken

Die steigende Komplexität des Unternehmensumfelds und der Unternehmen selbst hat weitreichende Folgen für die Risikosituation – stellt sie doch einen fundamentalen Aspekt bei der Erklärung der Risikoentstehung dar. Auf theoretisch-abstrakter Ebene kann dies anschaulich mit Hilfe der Systemtheorie gezeigt werden, die einen adäquaten Erklärungsansatz für das Komplexitätsphänomen bietet:

Ein *System* wird allgemein aus einer „... Anzahl von in Wechselwirkung stehenden Elementen“ [3, BERTALANFFY, S. 32] gebildet. Unternehmen können als zielgerichtete, offene und hochgradig komplexe sozio-ökonomische Systeme charakterisiert werden. Sie zeichnen sich durch eine Vielzahl von heterogenen Elemente aus, die durch zahlreiche unterschiedliche Beziehungen sowohl untereinander als auch mit anderen Umweltelementen verknüpft sind. Außerdem ist das System „Unternehmen“ ständigen, starken – teilweise sogar abrupten Veränderungen unterworfen.

Die steigende Anzahl und Varietät des Systems „Unternehmen“ hat zur Folge, dass bei einer Regelung immer mehr Einflussfaktoren berücksichtigt werden müssen und das System in einem definierten Zeitraum eine immer größere Zahl unterschiedlicher Zustände annehmen kann [4, HAZEBROUCK, S. 9 und S. 25]. Dieses Charakteristikum hat nun wiederum weitreichende Konsequenzen für die Risikobeurteilung: Schließlich erhöht sich durch die steigende Anzahl der möglichen Sys-

temzustände naturgemäß auch die Anzahl der – wie auch immer definierten – ungünstigen Systemzustände. Wird die weitverbreitete Definition des Begriffs *Risiko* als die „Möglichkeit einer negativen Zielabweichung“ [siehe hierzu u. a. 5, NEUBÜRGER, S. 37-39] zugrunde gelegt, resultiert ein steigendes Risiko c. p. allein schon aus der steigenden Systemkomplexität [6, SCHUY, S. 65].

2.1 Risikomanagement als schlecht strukturiertes Entscheidungsproblem

Problematisch bei der Analyse und dem adäquaten Umgang mit Risiken ist jedoch nicht nur diese steigende Anzahl möglicher negativer Systemzustände, die bei unternehmerischen Entscheidungen zu berücksichtigen sind. Vielmehr ergeben sich auch durch die spezifische Struktur der Problemstellungen im Bereich des Risikomanagements kaum mehr zu bewältigende Anforderungen an den Entscheider – Fragestellungen des Risikomanagements waren schließlich schon immer so genannte *schlecht strukturierte* Probleme. Diese sind dadurch gekennzeichnet, dass die relevanten Ursache-Wirkungs-Beziehungen nicht genau bekannt sind (*Wirkungsdefekt*), bestimmte Zustände nicht vollständig quantifizierbar sind (*Bewertungsdefekt*), Zielgrößen unbekannt oder mehrdimensional ausgeprägt sind (*Zielsetzungsdefekt*) und keine bzw. keine hinreichend exakten und/oder effizienten Lösungsverfahren existieren (*Lösungsdefekt*) [7, Adam, S. 315 f.] im folgenden gezeigt wird, sind all diese Defekte im wesentlichen auf eine mangelnde Informationsversorgung zurück zuführen, die sich durch den Einsatz von Informationssystemen (IS) maßgeblich verbessern lässt.

2.1.1 Wirkungsdefekt

Bei technisch bedingten Schäden (z. B. durch Material- oder Maschinendefekte, Bedienungsfehler usw.) oder dem Eintritt von Elementarrisiken (z. B. Brand, Wassereinbruch, Sturmschäden usw.) sind sowohl der direkte Risikoauslöser und die unmittelbare Wirkung als auch der zugrundeliegende Wirkungsmechanismus relativ schnell erkennbar, eindeutig von anderen Phänomenen abzugrenzen und damit auch vergleichsweise einfach und exakt zu quantifizieren [6, SCHUY, S. 68-98]. In

vielen anderen Fällen ist eine solch eindeutige Identifikation und Zuordnung von Ursache und Wirkung jedoch nicht mehr ohne weiteres möglich. Ein entscheidender Grund hierfür ist in der bereits diskutierten komplexen Struktur der betrachteten Systeme und der damit eng verbundenen mangelnden Prognostizierbarkeit ihres Verhaltens zu sehen. Innerhalb eines dynamischen Systems sind Elemente und Beziehungen ständigen Veränderungen unterworfen. Es kann daher praktisch ausgeschlossen werden, dass ein bestimmter Auslöser zweimal auf die exakt gleichen Ausgangsbedingungen trifft. Demzufolge wird er auch nicht zweimal die exakt gleichen Wirkungen hervorrufen [8, KOPEL, S. 4 f.]

Eine wesentliche Ursache für diese Intransparenz risikoauslösender Kausalzusammenhänge ist insbesondere darin zu sehen, dass ein einzelner Einflussfaktor häufig nicht nur ein bestimmtes, sondern mehrere unterschiedliche Risiken verursacht [6, SCHUY, S. 84 f]. Als Beispiel hierfür ist unter anderem eine Terminverzögerung zu nennen, die in der Folge u. U. Kostenüberschreitungen, Pönalzahlungen, Imageverluste usw. verursacht. Andererseits kann ein bestimmtes Risiko in vielen Fällen nicht auf einen singulären Auslöser zurückgeführt werden, sondern entsteht erst durch das simultane Zusammenwirken mehrerer unterschiedlicher Faktoren [8, KOPEL, S. 79]. Zusätzlich kompliziert wird die Identifikation von Kausalzusammenhängen noch durch den Umstand, dass diese oftmals nicht nur in eine Richtung wirken, sondern auch in Form von Rückkopplungen auftreten können. So beeinflusst beispielsweise ein Unternehmen mit seiner Preispolitik auch die Preispolitik seiner direkten Konkurrenten, während es gleichzeitig von diesen beeinflusst *wird*. Es ist also häufig zu beobachten, „... dass das, was als Wirkung bezeichnet wird, auf die Ursache zurückwirkt und damit selbst zur Ursache wird.“ [6, SCHUY, S. 68] Solche rekursiven Beziehungen – die klassische Frage nach „der Henne und dem Ei“ – tragen zu einer weiteren Verringerung der Transparenz von Ursache-Wirkungs-Zusammenhängen bei.

Zusätzlich erschwert wird die Bewertung von Risiken schließlich noch dadurch, dass Unternehmen als offene Systeme vielfältige Beziehungen zu ihrer Systemumwelt aufweisen. Die meisten Umweltelemente entziehen sich dabei einem direkten Einblick oder gar einer Kontrollmöglichkeit durch das einzelne Unternehmen.

Aufgrund dieser Tatsache können von diesen Elementen immer wieder Wirkungen ausgelöst werden, die ex ante nicht unbedingt erkennbar sind [8, KOPEL, S. 76].

Einen weiteren Grund für die meist mangelhafte Transparenz des Verhaltens von komplexen Systemen stellen auch die zeitlichen Verzögerungen dar, welche zwischen Ursache einerseits und Wirkung andererseits auftreten. Aufgrund dieser Time-lags ist die zeitliche Verteilung der hervorgerufenen Effekte oft nicht eindeutig prognostizierbar [4, HAZEBROUCK, S. 31]. Als wohl bekanntestes Beispiel sind hierbei die dynamischen Carry-Over-Effekte im Zusammenhang mit den Marketingaktivitäten eines Unternehmens zu nennen. Im allgemeinen beeinflussen Werbemaßnahmen das Käuferverhalten noch nicht bzw. nicht nur in der aktuellen Periode, sondern erst bzw. auch in den Folgeperioden [9, Kotler/Bliemel, S. 1005]. Eine exakte Vorhersage der genauen Verteilung dieser Wirkungen auf die einzelnen Zeiträume ist hierbei allerdings nicht möglich – der zugrundeliegende Kausalzusammenhang kann allenfalls vage beschrieben und ungefähr abgeschätzt werden [8, KOPEL, S. 71 u. 79]. Selbst wenn die Höhe des Gesamteffekts exakt bekannt wäre (wovon in der Praxis allerdings ebenfalls nicht auszugehen ist), entsteht also durch die unzureichende Prognose der zeitlichen Verteilung die Gefahr, dass in einer oder mehreren Perioden negative Zielabweichungen auftreten.

Aufgrund der steigenden Dynamik ist es zudem erforderlich, dass sich Unternehmen in immer kürzeren Abständen auf neue Situationen einstellen müssen. Die Zeitspanne, die den Entscheidungsträgern quasi als Lernprozess zur Verfügung steht, um die jeweiligen Kausalzusammenhänge überhaupt erfassen zu können, hat sich gerade in jüngster Zeit dramatisch verkürzt [4, HAZEBROUCK, S. 31].

2.1.2 Bewertungsdefekt

Ähnlich schwierig wie die Erfassung der einzelnen Kausalzusammenhänge, die dem Prozess der Risikoentstehung und -wirkung zugrunde liegen, gestaltet sich auch die Risikobewertung. Eine vollständige Erfassung und Bewertung aller denkbaren Risiken scheiden schon deshalb aus, weil die Anzahl der möglichen Zustände bei komplexen Systemen gegen unendlich tendiert. Beispielhaft sei an dieser

Stelle ein einfach strukturiertes System mit lediglich zehn Elementen angeführt, die jeweils nur fünf unterschiedliche Zustände annehmen können. Bereits in dieser Situation ergeben sich über 5^{10} (also über 9,7 Millionen) mögliche Systemzustände. Auch wenn in der Praxis aus Plausibilitätsüberlegungen viele Situationen von vornherein ausgeschlossen werden können, wird dennoch eine kaum überschaubare Anzahl zur Analyse verbleiben. Darüber hinaus steht den Unternehmen auch ein äußerst breites Spektrum an Handlungsmöglichkeiten zur Risikobewältigung offen, die in unterschiedlichen Abstufungen eingesetzt werden können und fast beliebig miteinander kombinierbar sind. Insgesamt umfassen also sowohl die Input- als auch die Outputseite einer Risikoanalyse eine fast unüberschaubare Anzahl an unterschiedlichen Alternativen, so dass die vollständige Erfassung und Bewertung aller Möglichkeiten von einem einzelnen Entscheider nicht zu bewältigen sind [10, Simon, S. 82 f.].

Auch im Hinblick auf die adäquate Bewertung von Risiken ist ein schwerwiegendes Hindernis in der steigenden systeminternen und -externen Dynamik zu sehen. Je früher Entscheidungen über Art und Umfang eventueller Risikobewältigungsmaßnahmen getroffen werden, desto effektiver und effizienter können diese Instrumente wirken. Da bei zunehmender innerer und äußerer Dynamik auch unerwünschte Systemzustände immer schneller eintreten, verkürzt sich die Reaktionszeit, die den betreffenden Unternehmen zur Verfügung steht, um wirksame Maßnahmen zur Risikobewältigung ergreifen zu können. Hieraus ergibt sich die Erfordernis, im Rahmen des Risikomanagements mitunter schon auf (im Sinne ANSOFF'S) *schwache Signale* [11, Ansoff] aus der Unternehmensumwelt reagieren zu müssen. Dies bedeutet jedoch, dass die entsprechenden Entscheidungen bereits zu einem Zeitpunkt getroffen werden müssen, zu dem die konkrete Ausprägung und Entwicklung der relevanten Einflussfaktoren noch nicht präzise prognostizierbar sind [12, Erben, S. 45]. Einen weiteren wesentlichen Grund für die oft mangelnde Quantifizierbarkeit von Risiken stellt auch die Existenz der bereits diskutierten Wirkungsdefekte dar. Eine Bewertung der Auswirkungen einer Entwicklung fällt natürlich um so schwerer, je intransparenter sich der zugrundeliegende Ursache-Wirkungs-Zusammenhang darstellt. Da Risiken häufig aus dem simultanen Zusammenwirken mehrerer Auslö-

ser entstehen, ist der exakte Wirkungsbeitrag eines einzelnen Einflussfaktors zur Entstehung des Risikos kaum mehr isolier- und quantifizierbar [13, FARNY, Sp. 1752 f.].

Folgendes Beispiel mag diese Zusammenhänge verdeutlichen: Sinken die Devisenkurse anderer Währungen gegenüber dem Euro, so schlagen sich die veränderten Wechselkursrelationen nach der Konvertierung unmittelbar in einer Erlösschmälerung bei den getätigten Exportgeschäften nieder. Das Ausmaß dieses Effekts ist unmittelbar erkennbar und kann problemlos quantifiziert werden. Mittel- bis langfristig werden sich allerdings auch indirekte Konsequenzen ergeben, die darauf zurückzuführen sind, dass durch die währungsbedingten Preisänderungen eine Verschlechterung der relativen Wettbewerbsposition eintritt [14, Meyer, S. 19]. So trägt das Absinken der Devisenkurse zu einer Schwächung der Wettbewerbsfähigkeit der Unternehmen auf dem betreffenden Auslandsmarkt und gleichzeitig zu einer Stärkung der Wettbewerbsfähigkeit ausländischer Konkurrenten auf dem Heimatmarkt bei. Daher ist in der Folge auch ein Rückgang der Auftragseingänge und Umsätze wahrscheinlich. Dieser Effekt wird jedoch vom Zusammenwirken einer ganzen Reihe von Faktoren ausgelöst, verstärkt oder abgemildert (z. B. der Preispolitik der Konkurrenten, staatlichen Maßnahmen der Exportförderung, verstärkten Marketingaktivitäten usw.). Der genaue Beitrag des Faktors Devisenkursänderung zur Gesamtwirkung „Umsatzrückgang“ lässt sich nicht mehr isolieren oder genau quantifizieren, zumal auch hier wiederum diverse Time-lags innerhalb der Wirkungskette auftreten.

Da Bewertungsdefekte bei komplexen Zusammenhängen auf analytisch-theoretischem Wege kaum behebbar sind, käme als Lösungsalternative u. U. eine empirische Ermittlung der benötigten Werte in Betracht. So könnten mit Hilfe von mathematisch-statistischen Methoden (z. B. der Regressionsanalyse oder des Diskriminanzverfahrens) geeignete Werte aus Vergangenheitsdaten abgeleitet und in die Zukunft extrapoliert werden. Zu diesem Zweck wäre allerdings zunächst die Analyse einer hinreichend großen Grundgesamtheit erforderlich. Dies würde wiederum voraussetzen, dass sich das zugrundeliegende Systemverhalten bereits sehr häufig, in weitgehend identischer Form und unter praktisch konstanten Bedin-

gungen wiederholt hat [15, Bosch, S. 60 f.]. Bei Problemstellungen im Rahmen des Risikomanagements ist die Voraussetzung repetitiver Prozesse schon allein wegen der hohen Dynamik in vielen Fällen nicht erfüllt. Risiken, die mehr oder weniger regelmäßig wiederkehren, finden sich allenfalls in bestimmten, relativ eng abgegrenzten Teilbereichen. Als Beispiele können in diesem Zusammenhang unter anderem Schadensereignisse wie der Ausfall von Forderungen, die Produktion von Ausschuß, Maschinenstörungen, Qualitätsmängel bei bezogenen Teilen genannt werden. Bei diesen Risiken handelt es sich allerdings meist um so genannte Bagatellrisiken, die zwar relativ häufig auftreten, jedoch im Einzelfall nur verhältnismäßig geringe Schäden verursachen (so genannte „high frequency – low severity Risks“). Aufgrund der sehr breiten empirischen Datenbasis ist in diesen Fällen mit vergleichsweise einfachen statistischen Modellen eine relativ präzise Prognose des Schadenverlaufs und -umfangs möglich.

Zahlreiche Entscheidungen im Rahmen des betrieblichen Risikomanagements weisen demgegenüber einen ausgeprägten Einzelfallcharakter auf. Dies trifft natürlich insbesondere auf die Risikoanalyse von langfristig-strategischen Projekten zu, wie beispielsweise die Entwicklung eines neuen Produkts, den Eintritt in einen neuen Markt oder Investitionen in ein neues Produktionswerk. Zum einen unterscheiden sich derartige Projekte in aller Regel relativ stark voneinander, zum anderen werden sie im allgemeinen nur einmalig bzw. in sehr großen zeitlichen Abständen durchgeführt. Insgesamt ist daher nicht davon auszugehen, dass zwei inhaltlich weitgehend identische Projekte unter weitgehend identischen Umweltbedingungen stattfinden. Aufgrund dieser Tatsache können die Erfahrungen der Vergangenheit also in der Regel nicht unverändert auf aktuelle Entscheidungen übertragen werden. Dies bedeutet, dass die Ungewißheit der Aussagen nicht durch die Gegenüberstellung empirisch gewonnener Ergebnisse reduziert werden kann [15, Bosch, S. 60 f.]. Problematisch ist hierbei insbesondere die Tatsache, dass in den letztgenannten Fällen ein Risikoeintritt verhältnismäßig hohe Schäden verursacht (sogenannte high severity – low frequency Risiken). Eventuelle Fehleinschätzungen können daher gravierende, mitunter sogar existenzgefährdende Konsequenzen zur

Folge haben. Insofern ist gerade bei denjenigen Entscheidungen, bei denen in Anbetracht ihrer Bedeutung eine empirische Validierung der Entscheidungsmodelle am wichtigsten wäre, eine solche Überprüfung äußerst schwierig.

2.1.3 Zielsetzungsdefekt

Die zentrale Zielsetzung des Risikomanagements besteht in der Erreichung eines unter Wirtschaftlichkeitsgesichtspunkten optimalen Risiko- bzw. Sicherheitsniveaus [1, Braun, S. 45]. Hierbei zeigt sich jedoch schnell ein sehr grundsätzlicher Zielsetzungsdefekt. Das Gut „Sicherheit“ ist ein relativ abstraktes, hochaggregiertes und schwer fassbares Konstrukt. Nur in vergleichsweise seltenen und eng abgegrenzten Teilbereichen auf operativer Ebene kann dieses Ziel objektiv definiert und operationalisiert werden. Dies ist etwa der Fall, wenn für bestimmte Produkte oder betriebliche Prozesse gesetzliche Sicherheitsbestimmungen eingehalten werden müssen [16, Kratzheller, S. 25 f.]. In aller Regel besitzen dagegen die persönliche Einstellung und Risikobereitschaft des einzelnen Entscheiders eine ganz wesentliche Bedeutung bei der Wahrnehmung und Einschätzung bestehender Risiken und der darauf aufbauenden Formulierung von Sicherheitszielen. So kann ein Sicherheitsniveau, das einem Entscheider bereits als übertrieben hoch erscheint, von einem anderen als noch lange nicht ausreichend beurteilt werden [13, Farny, Sp. 1753]. In einer Vielzahl von Studien konnte nachgewiesen werden, dass das wahrgenommene Risiko – also die individuelle Beurteilung seines Ausmaßes durch Individuen oder gesellschaftliche Gruppen – häufig ganz erhebliche Diskrepanzen zu der tatsächlichen, statistisch ermittelbaren Risikohöhe aufweist [17, Wildawsky].

2.1.4 Lösungsdefekt

Für Problemstellungen, die ausgeprägte Wirkungs-, Bewertungs- und Zielsetzungsdefekte aufweisen, also beispielsweise durch Ungenauigkeit und Unvollständigkeit gekennzeichnet sind, können selbstverständlich auch keine exakten und effizienten Lösungsmethoden existieren. Die betriebswirtschaftliche Forschung konzentrierte sich lange Zeit vor allem auf gut strukturierte Probleme, bei denen ein-

deutig definierte Zielsysteme vorgegeben werden und die unterschiedlichen Handlungsalternativen eindeutig quantifizierbar sind [18, Keil, S. 10]. Da im Rahmen des Risikomanagements allerdings viele Sachverhalte und Zusammenhänge abzubilden sind, die nur verbal-qualitativ umschrieben werden können oder anderweitig mit Unsicherheiten bzw. Ungenauigkeiten behaftet sind, kann schon das zu lösende Problem nicht vollständig erfasst und genau beschrieben werden [18, Keil, S. 10 f.]. Dementsprechend schwierig gestaltet sich natürlich auch die Entwicklung und Anwendung eines geeigneten Lösungsverfahrens. In vielen Fällen ergeben sich Lösungsdefekte daher quasi zwangsläufig als Folgeerscheinung der bisher diskutierten Strukturmängel [7, Adam, S. 315].

2.2 Bedeutung von Informationssystemen für das Risikomanagement

Wie in den vorangegangenen Abschnitte gezeigt wurde, können die Kausalzusammenhänge zwischen Risikofaktoren einerseits und den von ihnen ausgelösten Wirkungen andererseits von einem einzelnen Entscheider kaum mehr erfasst und quantifiziert werden. Daher besteht die latente Gefahr, dass eine bestimmte Entscheidung einen unerwünschten – zumindest jedoch suboptimalen – Systemzustand zur Folge hat.

Umeine vorgegebene Aufgabenstellung erfüllen bzw. eine bestimmte Entscheidung treffen zu können und dabei die systemimmante Gefahr von Fehlentscheidungen zu vermeiden bzw. weitmöglichst zu minimieren und, sind also Informationen in bestimmter (d. h. „ausreichender“) Quantität und Qualität erforderlich. Dieser *objektive Informationsbedarf* ist dabei in jüngster Vergangenheit erheblich gestiegen. Im Gegensatz dazu umfasst der *subjektive Informationsbedarf* des Entscheiders nur all jene Informationen, die er aus seiner spezifischen (subjektiven) Sicht als relevant für die vorliegende Problemstellung erachtet. Es kann davon ausgegangen werden, dass sich diese Komponente tendenziell zurück gebildet hat, da der einzelne Entscheider Infolge der steigenden Komplexität und Dynamik und der zahlreichen Strukturdefekte überfordert ist und sich bestimmter Problembereiche gar nicht mehr bewusst wird. Aufgrund der Tatsache, dass für die Beschaffung von Informationen

Kosten entstehen und zur Verarbeitung nur begrenzte Kapazitäten zur Verfügung stehen, wird von diesem subjektiven Informationsbedarf auch nur ein Teil als tatsächliche *Informationsnachfrage* artikuliert. Diese kann wiederum nur partiell vom vorhandenen *Informationsangebot* gedeckt werden. Der (in aller Regel unvollkommene) *Informationsstand* eines Entscheidungsträgers ergibt sich somit als Schnittmenge aus objektivem Informationsbedarf, Informationsnachfrage und Informationsangebot (vgl. Abb. 1) [19, Picot/Reichwald, S. 275 f.].

Durch den Einsatz eines Informationssystems ergeben sich nun mehrere positive Effekte auf den Informationsstand des Entscheiders und damit auf die Qualität seiner Entscheidung. Zum einen vergrößert sich der subjektive Informationsbedarf, da die Komplexität der Entscheidungssituation transparenter wird und der Entscheider das Ausmaß des Problems besser erfassen kann – durch die Transparenzverbesserung wird dem Entscheider also bewusst, dass er eigentlich wesentlich mehr Informationen bräuchte, als er bisher (d. h. vor dem Einsatz des IS) vermutet hatte. Infolgedessen wird auch seine Informationsnachfrage steigen, zumal da durch moderne Informations- und Kommunikationstechnologien die Kosten für die Informationsbeschaffung und -verarbeitung sinken, während gleichzeitig die Kapazitäten steigen. Aufgrund der effizienteren und schnelleren Informationsbereitstellung steigt schließlich auch das Angebot an Informationen. Diese Aussage gilt nicht nur in quantitativer, sondern vielmehr auch in qualitativer Hinsicht. Schließlich werden durch die vergleichsweise hohe Verarbeitungsgeschwindigkeit und -kapazität moderner IS auch die Negativeffekte der vielfältigen Strukturdefekte maßgeblich abgeschwächt. So erlauben umfangreiche Simulationsläufe beispielsweise das „Durchspielen“ mehrerer komplexer Alternativszenarien – Wirkungs- und Bewertungsdefekte lassen sich auf diese Weise also verringen oder zumindest analysieren. Auch der Aufbau und die Auswertung bereits relativ einfacher Schadensfalldatenbanken kann entscheidend dazu beitragen, die Ursachen und Auswirkungen von Schadensfällen und Risken besser zu verstehen und damit zu bewältigen. Insgesamt kann also festgehalten werden, dass sich aus einer systemtheoretischen Sichtweise bereits bei einer relativ abstrakten Betrachtung der Informationsstand eines Entscheiders wesentlich verbessern lässt – Durch den Einsatz vergrößert

sich die Schnittmenge aus objektivem Informationsbedarf, Informationsnachfrage und Informationsangebot, so dass der Informationsstand des Entscheiders insgesamt zunimmt [11, Erben, S. 45].

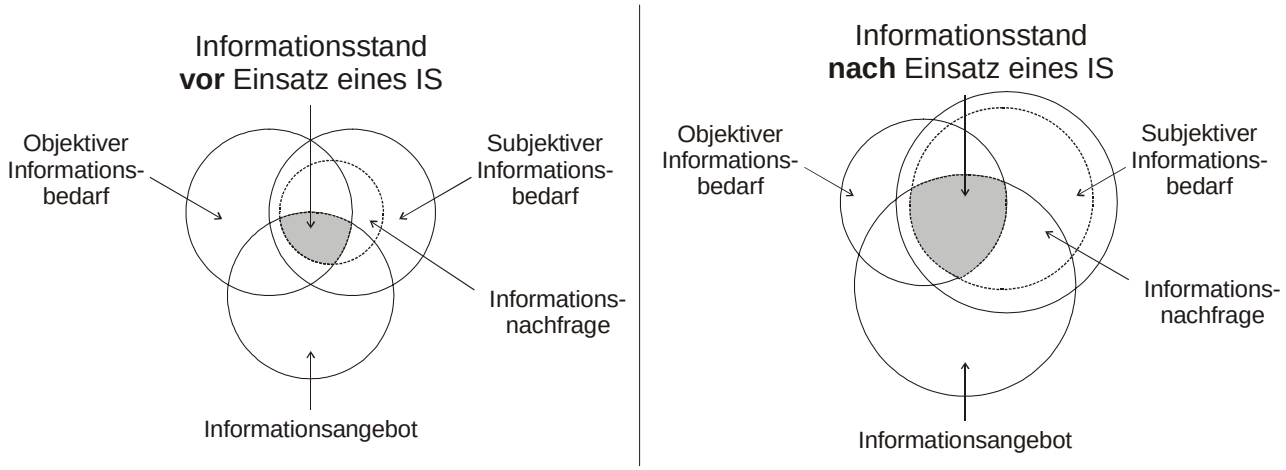

Abb. 1: Informationsstand eines Entscheiders [19, Picot/Reichwald, S. 276].

3 Klassifikation von Informationssystemen

Nachdem in den vorangegangenen Abschnitten zahlreiche positive Effekte identifiziert werden konnten, die aus einem Einsatz adäquater Informationssysteme im Bereich des Risikomanagements resultieren, sollen diese im folgenden weiter konkretisiert werden.

3.1 Begriff des Informationssystems

Die Aufgabe eines Informationssystem ist ganz allgemein die rechtzeitige Versorgung der Handlungs- und Entscheidungsträger mit allen notwendigen und relevanten Informationen in wirtschaftlich sinnvoller Weise. Mit Hilfe von Informationssystemen sollen die richtigen Informationen zum richtigen Zeitpunkt am richtigen Ort in adäquater Form bereitgestellt werden. Informationssysteme bilden als ein zentrales Medium für die Entscheidungsfindung und –durchsetzung das Fundament für den gesamten Managementprozess. Dazu müssen Daten erfasst, gespeichert, zu Informationen verarbeitet und zur Verfügung gestellt werden. Durch den Einsatz von

Informationstechnologie (IT) werden bei rechnergestützten Informationssystemen diese Aufgaben teilweise automatisiert [20, Schneck, S. 316].

Durch die Vielzahl der Bestandteile betrieblicher Informationssysteme ist deren Klassifikation zweckmäßig. Sie lassen sich in Administrations- und Dispositionssysteme (ADS) sowie Entscheidungsunterstützungssysteme (EUS) unterteilen [21, Stahlknecht, S. 330]. Diese gängige Klassifikation folgt der hierarchischen Gliederung eines Unternehmens (siehe Abb. 2).

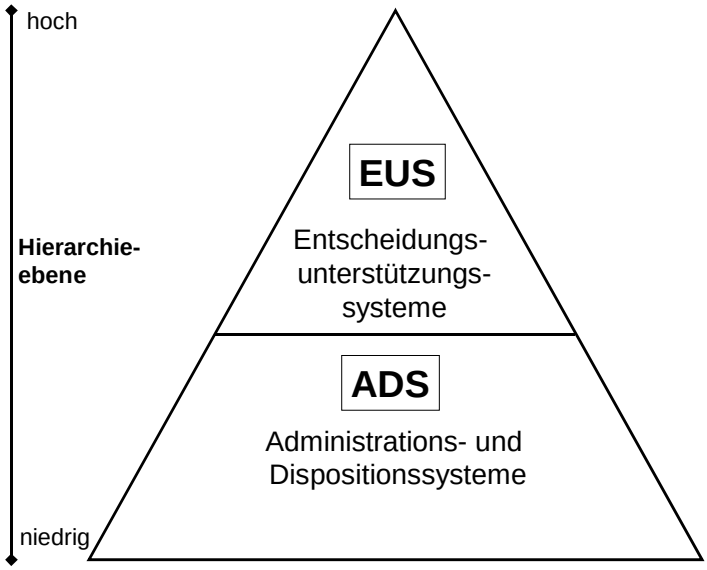

Abb. 2: Klassifikation von Informationssystemen

ADS werden überwiegend in den operativen Bereichen eines Unternehmens eingesetzt und dienen der Abwicklung der laufenden Geschäftsvorfälle (Finanzbuchhaltung, Warendisposition, PPS etc.) [22, Henneböle, S. 18]. Die Benutzergruppen von ADS sind in aller Regel hierarchisch niedriger angesiedelt als die der EUS.

EUS, wie z. B. Executive Information Systems und Controlling Support Systems, werden in der Regel von Entscheidungsvorbereitern und Entscheidungsträgern der oberen Hierarchieebenen benutzt. Sie unterstützen den gesamten Entscheidungsprozess sowie den Informationsaustausch und die Kommunikation zwischen der

Unternehmensleitung und den Entscheidungsvorbereitern (z. B. Controllern und Risk Managern) durch Verwendung von Daten, Methoden und Modellen [22, Henneböle, S. 19]. Die für die folgenden Abschnitte relevanten Bestandteile eines EUS sind [23, Pfohl, S. 180 f.]:

- **Datenbanken:** Sammlung organisierter Daten für bestimmte Zwecke (z. B. Datenbank für die Schadensanalyse),
- **Methodenbanken:** Sammlung programmierter Methoden, die im RM-Prozeß eingesetzt werden können (z. B. Algorithmen und statistische Verfahren),
- **Modellbanken:** Analyse- und Entscheidungsmodelle (z. B. Modell zur Simulation eines Schadenszenarios).

3.2 Risk Management-Informationssysteme

Nachdem in den vorangegangenen Abschnitten eine allgemeine Systematisierung von (Management) Informationssystemen vorgenommen wurde, werden im folgenden die spezifischen Anforderungen und Aufgaben eines IS im Kontext des Risk Managements detaillierter dargestellt.

3.2.1 Sinn und Zweck eines RMIS

Ein RMIS ist ein IT-gestütztes, daten-, methoden- und modellorientiertes EUS für das RM, das inhaltlich richtige und relevante Informationen zeitgerecht und formal adäquat zur Verfügung stellt und somit methodische Unterstützung bei der Entscheidungsvorbereitung bietet. Es erfasst und verarbeitet in der Regel sowohl interne Daten aus den betrieblichen ADS als auch externe Daten (z. B. Informationen aus öffentlich zugänglichen Datenbanken, dem Internet oder von Versicherern).

Idealtypisch orientiert sich sich ein integriertes Risikomanagement an der Funktionsweise des Nervensystems des menschlichen Organismus. Dieses besteht zum einen aus Sensoren, die über den gesamten Körper verteilt sind und alle internen und externen Ereignisse sowie Gegebenheiten erfassen. Diese erfassten Daten werden über die Leiterbahnen des Nervensystems an ein zentrales Organ, unser

Gehirn, weitergeleitet, das über die entsprechende Reaktionen entscheidet und diese im Anschluss steuert. Unser Gehirn integriert dabei auch ein Frühwarnsystem (weitgehend synonym spricht man auch von Frühaufklärungssystemen oder Prognosesystemen), um zukünftige Entwicklungen und Ereignisse zu antizipieren und Gefahren durch geeignete präventive Maßnahmen evtl. zu vermeiden oder zu vermindern [24, Romeike].

Ein derartiges Frühwarnsystem sollte auch fester Bestandteil eines unternehmensweiten RMIS sein, da sie die Steuerbarkeit des Unternehmens verbessern. Wie bereits dargestellt, muss bei einer steigenden Komplexität und Dynamik besonderes Augenmerk auf die Berücksichtigung von „schwachen Signalen“ liegen [11, Ansoff].

Durch den Einsatz eines Ein RMIS können dabei mehrere Schwachstellen vermieden werden, die bei der Umsetzung des modernen Risk Managements in der Praxis auftreten. Zu derartigen Schwachstellen zählen u. a.:

- ein fehlendes oder unvollständiges Risikoinventar (auch Risikolandschaft, Risikomatrix)
- der fehlender Überblick über die Risikolage eines Unternehmens,
- die redundante und inkonsistente Erfassung und Speicherung von Daten,
- fehlende bzw. gestörte Informations- und Kommunikationswege sowie -abläufe,
- eine nicht ausreichend informierte bzw. sensibilisierte Unternehmensleitung,
- eine verzögerte Entscheidungsfindung.

Das Risk Management beschäftigt sich primär mit dem „Management" von Informationen. Ein „Risk Manager“ sieht sich bei seiner alltäglichen Arbeit mit einer Fülle von unterschiedlichen Informationen konfrontiert, die ihm meist unkoordiniert und unvollständig zur Verfügung gestellt werden. In der Regel existieren die für das RM erforderlichen Daten bereits in unterschiedlichen Unternehmensbereichen. Es mangelt lediglich an deren koordinierten Erfassung, Speicherung, Verarbeitung und Bereitstellung.

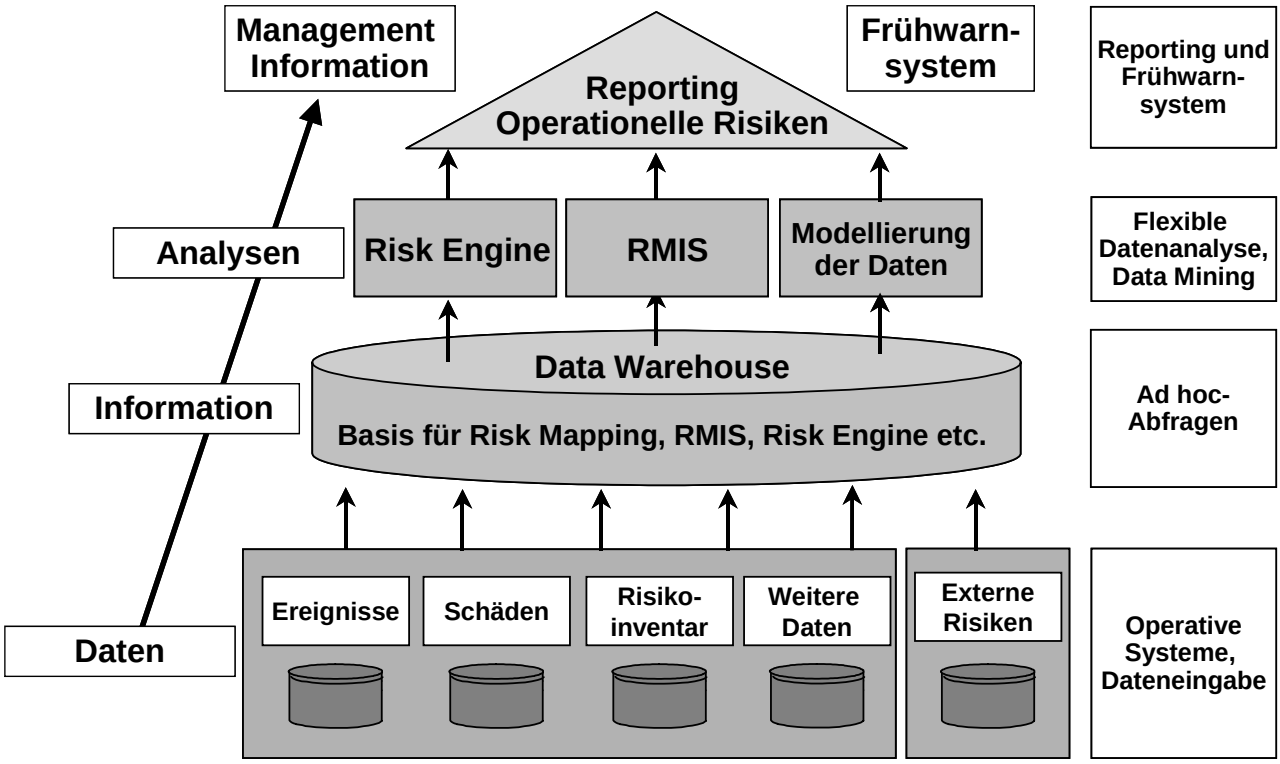

Abb. 3: Von Daten zu relevanten Managementinformationen

Eine wesentliche Anforderung an ein RMIS besteht deshalb u. a. darin, einen reibungslosen Informations- und Kommunikationsfluss zwischen den am RM beteiligten Organisationseinheiten und betrieblichen Funktionsträgern zu gewährleisten.

Diese Sicherstellung des Informations- und Kommunikationsflusses reicht jedoch nicht aus. Die zur Verfügung gestellten Daten müssen zusätzlich auch noch verarbeitet werden [25, Hornung/Reichmann/Baumöl, S. 38]. Deshalb soll das RMIS den Risk Manager zusätzlich bei der Aufbereitung und Bereitstellung der gesammelten Daten unterstützen. Der Unterstützungsgrad hängt dabei von der Strukturierbarkeit und Formalisierbarkeit der jeweiligen Aufgabe ab. Ein großer Teil der Aufgaben im RM kann von einem RMIS übernommen werden. Das moderne RM umfasst jedoch auch Tätigkeiten, welche die „menschlichen" Fähigkeiten des Risk Managers (Intuition, Erfahrung, Erkennen von Mustern, Suche von Analogien etc.) erfordern, wie z. B. die Bewertung nicht quantifizierbarer Risiken (Industriespionage, Computerkriminalität etc.). Schließlich hat das RM für einen erfolgreichen Einsatz neben technischen auch bestimmte betriebswirtschaftliche Anforderungen zu erfüllen.

3.2.2 Anforderungen an ein RMIS

Entsprechend den unterschiedlichen individuellen Bedürfnissen der einzelnen Unternehmen variieren die Anforderungen an ein RMIS. Deshalb ist die Ermittlung der betriebswirtschaftlichen Anforderungen ein zentrales Problem bei der Auswahl bzw. Entwicklung und Implementierung eines RMIS. Trotz dieser hohen Spezifität lassen sich einige grundlegende Anforderungen definieren:

Um die Planung, Steuerung, Durchführung und Kontrolle der Risikopolitik rechnerorientiert unterstützen zu können, reicht die Speicherung vergangener und aktueller Daten (Schadensdaten, Daten über Risikolage und Wirksamkeit der risikopolitischen Maßnahmen, etc.) nicht aus. Vielmehr muss das RMIS den gesamten Risk Management Prozess, also die Risikoanalyse, die Beurteilung von risikopolitischen Handlungsalternativen, die Abschätzung der Auswirkungen der geplanten Maßnahmen und den Soll-Ist-Vergleich zur Erfolgskontrolle umgesetzter Maßnahmen unterstützen. Dabei sind nicht nur risikobezogene, sondern auch betriebswirtschaftliche Daten zu verarbeiten, etwa die mit den risikopolitischen Maßnahmen verbundenen Investitionen [26, Haasis, S. 11].

Ein RMIS muss daher in die bestehende IT-Landschaft eines Unternehmens integriert werden und über passende Schnittstellen zu anderen Bestandteilen des betrieblichen Informationssystems, z. B. zum betrieblichen Rechnungswesen, verfügen. Die Notwendigkeit eines integrierten Systems ergibt sich zusätzlich daraus, dass der Risk Manager an allen Entscheidungen teilhaben sollte, welche die Risikolage des Unternehmens tangieren [27, Hertel, S. 78]. Eine weitere wichtige Anforderung besteht in der Implementierung geeigneter Kommunikationsschnittstellen (z. B. Electronic-Mail), um den Informations- und Kommunikationsfluss zwischen den am RM beteiligten Funktionen sicherstellen zu können [22, Henneböle, S. 4]. Von zentraler Bedeutung ist auch ein flexible Aufbau, damit das RMIS den kontinuierlichen Unternehmensveränderungen (z. B. Akquisition eines Unternehmens) angepasst werden kann. Um die Anforderungen der unterschiedlichen Benutzergruppen (u. a. der Risk Manager und die Unternehmensleitung) optimal berücksichtigen zu können, muss ein RMIS auch verschiedene Sichten auf die Daten anbieten, wo-

bei die Gestaltung der Benutzeroberfläche (z. B. grafische Unterstützung) den unterschiedlichen fachlichen Voraussetzungen und Erfahrungsniveuas der Benutzer gerecht werden sollte [26, Haasis, S. 13].

Um die Auswirkungen von Risikoeintritten (z. B. bei einer Betriebsunterbrechung) oder die Wirksamkeit geplanter risikopolitischer Maßnahmen (z. B. Sprinklerung) nachvollziehen zu können, ist es schließlich wünschenswert, dass das RMIS aufgrund der Komplexität der Aufgabe die Modellierung und Simulation von Szenarien gestatten.

Abschließend lassen sich die wichtigsten Anforderungen an ein RMIS also folgendermaßen zusammen fassen:

Betriebswirtschaftliche Anforderungen an ein RMIS	
☑	Verfügbarkeit eines integrierten Datenbestandes / geeignete Schnittstellen,
☑	Integration eines Frühwarnsystems, um künftige Entwicklungen zu antizipieren
☑	Umfangreiche Methodendatenbanken
☑	Flexibler Aufbau mit Erweiterungsmöglichkeiten,
☑	Unterstützung verschiedener Sichten auf den Datenbestand,
☑	benutzerfreundliche Gestaltung und Funktionalität,
☑	Verfügbarkeit von aktuellen Daten zu jedem beliebigen Zeitpunkt,
☑	Individuelle Gestaltung von Berichten,
☑	Bereitstellung und Verdichtung von Daten auf beliebigen Verdichtungsebenen,
☑	schnelle und flexible Simulationen,
☑	ausgereifte Präsentationstechniken etc.
☑	Komfort, Wirtschaftlichkeit, Schnelligkeit, Aktualität der Daten, Konsistenz etc.

Abb. 4: Anforderungen an ein RMIS aus betriebswirtschaftlicher Sicht

3.2.3 Aufbau eines RMIS

Aufgrund der Flexibilitätsanforderungen bietet sich ein modularer Aufbau des RMIS an. Ein RMIS umfasst u. a. die nachfolgend aufgeführten Module:

- Simulationen
- Reporting
- Asset-Verwaltung
- Verwaltung von Policen sowie des Versicherungsprogramms- und / oder Risikofinanzierungsprogramms
- Identifikationsmethoden für Risiken (Kollektionsmethoden, Kreativitätsmethoden, Analytische Methoden)
- Bewertungsmethoden für Risiken (Top Down, Bottom Up)
- Schadensadministration
- Schadensstatistiken
- Risikokostenanalyse (Total Cost of Risk)
- Analyse risikopolitischer Handlungsalternativen (Risk Mitigation Strategy)

Typische Datenbanken eines RMIS enthalten:

- Daten über Vermögenswerte, Umsätze, Gewinne etc.
- Daten über Abhängigkeiten zu Beschaffungs- und Absatzmärkten: Schlüssellieferanten, Schlüsselkunden, Wiederbeschaffungszeiten von Maschinen etc.
- Daten über aufgetretene Schäden: Schadenumfang, Schadenursache, Rückwirkungsschäden (Kausalwirkungen eines Sachschadens) etc.,
- Daten über sämtliche Risiken: potentielles Störungsereignis, gefährdete Objekte, Schadeneintrittswahrscheinlichkeit, potentielles Schadenausmaß, Risikokosten etc.,

Darüber hinaus enthält ein effizentes RMIS in der Regel Methodenbanken und Modellbanken, die auf die jeweiligen Aufgaben (z. B. Modell zur Simulation eines Schadenszenarios) abgestimmt sind [28, Beroggi, S. 80].

4 Die IT-gestützte Umsetzung des operativen Risk Managements

Immer mehr Unternehmen gehen dazu über, ihr Risk Management als ganzheitlichen Prozess zu implementieren, bei dem die einzelnen Phasen sukzessive und kontinuierlich durchlaufen werden kann. Infolge dieser prozessuralen Sichtweise ist es von entscheidender Bedeutung, dass ein RMIS in sämtlichen Phasen dieses Prozesses eine adäquate Unterstützung bieten kann.

4.1 Übersicht

Risikomanagement war immer schon implizit Bestandteil der Unternehmenssteuerung. Häufig war das RM jedoch rein reaktiv ausgestaltet – es wurde erst dann reagiert, wenn das Unternehmen bereits „in stürmischer See“ oder gar „in akuter Seenot“ war. In der Industrie und im Handel lag der primäre Fokus auf der Erfüllung von gesetzlichen Vorschriften (etwa Vorschriften bzgl. Brand- oder Arbeitsschutz) oder Auflagen der Versicherer (etwa des Verbandes der Schadensversicherer (VdS), der umfangreiche Brandschutzrichtlinien heraus gibt oder den Bestimmungen für hochgeschützte Anlagen und Systeme, „Highly Protected Risks“ / HPR). Aufgrund der veränderten Rahmenbedingungen für Unternehmen ist ein proaktives, systematisches und holistisches Risikomanagement jedoch Voraussetzung, um die Klippen in stürmischer See rechtzeitig zu erkennen und zu umschiffen. Die von dem RMIS bereit gestellten Module dienen der Unterstützung des gesamten RM-Prozesses.

Die von der Unternehmensleitung im Rahmen des strategischen RM vorgegebenen Risikoziele (etwa Reduzierung der Produkthaftpflichtansprüche, Schutz vor Betriebsunterbrechungen) können als Sollzustand der gewünschten Unternehmensrisikolage in das RMIS eingehen. Damit stehen dem Risk Manager die Risikoziele jederzeit abrufbereit zur Verfügung.

4.2 Risikoanalyse

Das **operative Risk Management** beinhaltet den Prozess der systematischen und laufenden Risikoanalyse der Geschäftsabläufe. Ziel der Risikoidentifikation ist die

frühzeitige Erkennung von „... den Fortbestand der Gesellschaft gefährdende Entwicklungen“, d. h. die möglichst vollständige Erfassung aller Risikoquellen, Schadensursachen und StörpotenzialenFür einen effizienten Risikomanagementprozess kommt es insbesondere darauf an, dass Risikomanagement als kontinuierlicher Prozess – im Sinne eines Regelkreises – in die Unternehmensprozesse integriert wird (siehe Abb. 4):

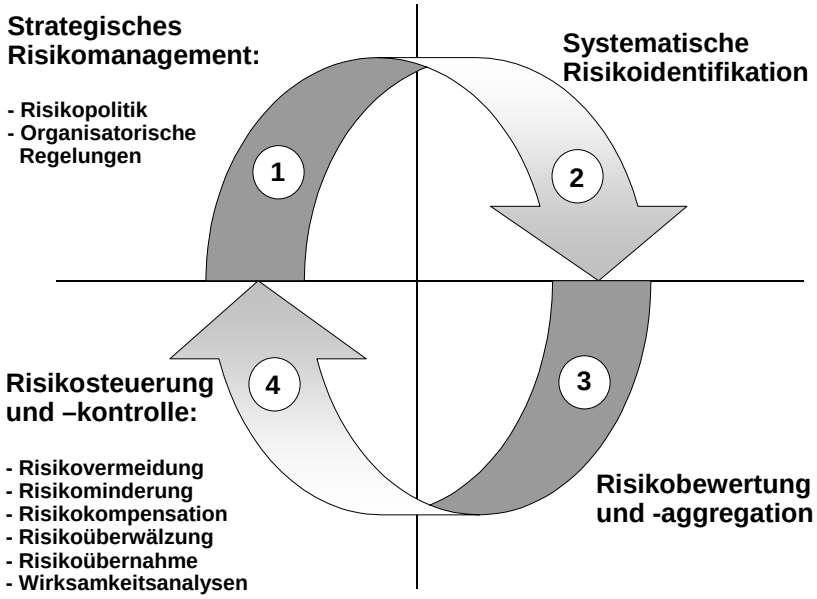

Abb. 4: Prozessstruktur des Risikomanagements

Die Risikoanalyse dient zum einem der Sammlung von Daten (Risikoidentifikation) und zum anderen der Verarbeitung der Daten zu aussagekräftigen Informationen (Risikobewertung). Das RMIS unterstützt den Risk Manager bei der Risikoanalyse u. a. durch statistische Verfahren, probabilistische Berechnungen sowie unterschiedliche Methoden und Modelle [28, Beroggi, S. 85].

Die Informationsbeschaffung ist die schwierigste Phase im gesamten Risk Management Prozess und eine Schlüsselfunktion des Risk Managements, da dieser Prozessschritt die Informationsbasis für die nachgelagerten Phasen liefert. Erforderlich ist eine systematische, prozessorientierte Vorgehensweise. – schließlich können alle weiteren risikopolitischen Maßnahmen trivialerweise nur bei denjenigen Risiken angewandt werden, die auch rechtzeitig erkannt wurden Die Identifikation

kann je nach Unternehmen aus verschiedenen Perspektiven erfolgen; beispielsweise auf der Ebene der Risikoarten (leistungswirtschaftliche, finanzwirtschaftliche, externe Risiken etc.), der Ebene der Prozesse (Projekte, Kern- und Unterstützungsprozesse etc.) sowie der Geschäftsfelder (Dienstleistungen, IT Services, Produktion etc.). In der Praxis wird man erkennen, dass Risikokategorien nicht losgelöst voneinander erfasst werden können, sondern vielmehr durch positive und negative Rückkoppelungen miteinander verbunden sind [11, Erben, S. 12 f.].

Bei der Erfassung der Risiken helfen Checklisten, Workshops, Besichtigungen, Interviews, Organisationspläne, Bilanzen Schadenstatistiken, Fehlerbaumanalysen, die Fehlermöglichkeits- und -einflußanalyse (FMEA), das Brainstorming und -writing, Szenarioanalysen sowie die Delphimethode. Ergebnis der Risikoanalyse sollte ein Risikoinventar sein. Die identifizierten Risiken müssen im anschließenden Prozessschritt detailliert analysiert und bewertet werden. Ziel sollte dabei ein sinnvolles und möglichst für alle Risikokategorien anwendbares Risikomaß sein (etwa der „Value-at-Risk“).

Der Risk Manager bzw. das RMIS greifen dabei u. a. auf folgende Informationsquellen zu:

- das Rechnungswesen (Daten über Vermögenswerte, Umsätze, Gewinne etc.),
- interne Schadensstatistiken (Daten über innerbetriebliche Schäden etc.),
- den Einkauf (Daten über Lieferanten, Wiederbeschaffungszeiten von Maschinen etc.),
- die Lagerverwaltung (Daten über Roh-, Hilfs- und Betriebsstoffe),
- die Rechtsabteilung (Daten über Haftungsklauseln, neue Gesetzesgrundlagen, AGB etc.),
- die Liegenschaftsabteilung (Daten über Eigentum von Gebäuden, gemietete Flächen etc.),
- die Brandschutzfunktion (technische Daten über Wirksamkeit von Schadenverhütungsmaßnahmen etc.),
- die Verbesserungsvorschläge der Mitarbeiter,

- die Versicherungsunternehmen (externe Schadendaten etc.),
- die externen Servicepartner (Daten über Empfehlungen zur Schadenverhütung etc.).

Von der Bewertungsmethodik bietet sich entweder ein „Top-Down"- oder ein „Bottom up"-Ansatz an. Das Spektrum der verschiedenen Bewertungsansätze für operationelle Risiken ist in Abb. 5 dargestellt:

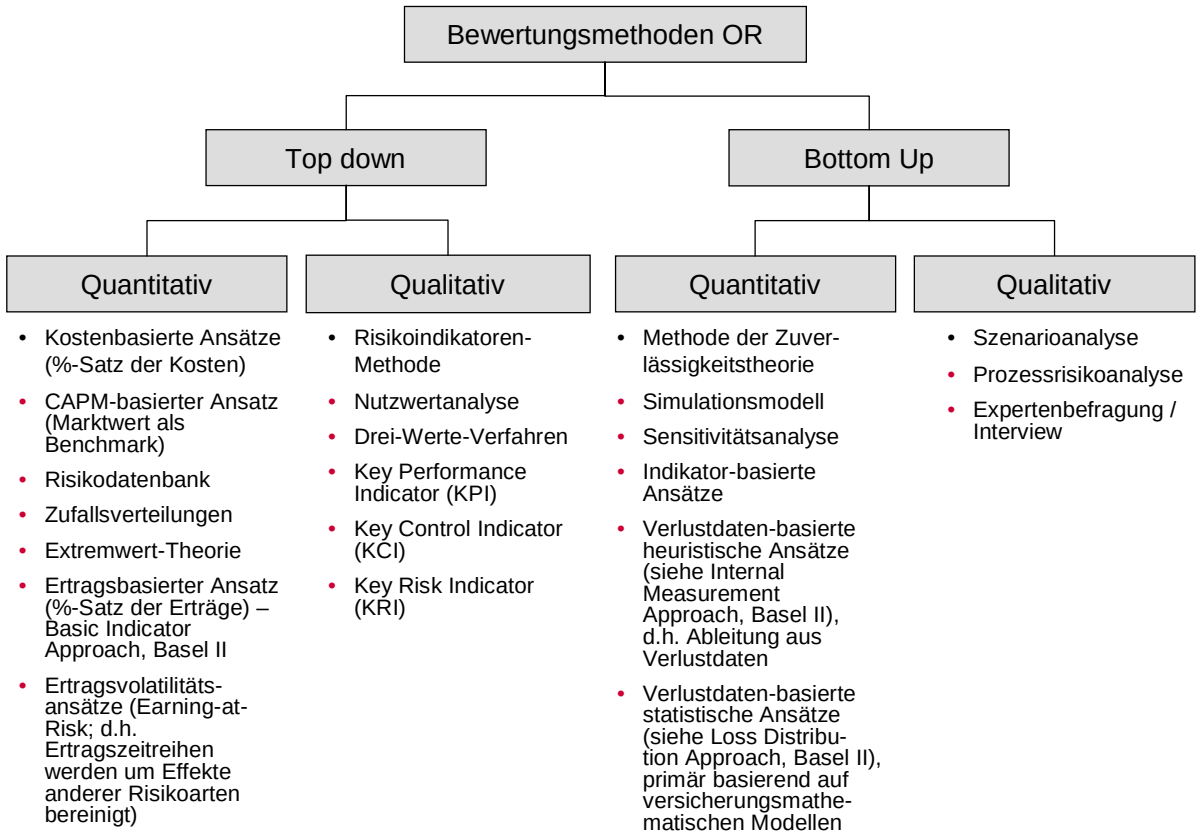

Abb. 5: Bewertungsmethoden für operationelle Risiken

Der „Top down"-Ansatz bietet den Vorteil einer relativ schnellen Erfassung der Hauptrisiken aus strategischer Sicht. Diese „Makroperspektive" kann jedoch auch dazu führen, dass bestimmte Risiken nicht erfasst werden oder Korrelationen zwischen Einzelrisiken nicht korrekt bewertet werden. Demgegenüber bietet ein „Bottom-up"-Ansatz den Vorteil, dass sämtliche Geschäftsbereiche und Prozesse erfasst und analysiert werden können. Allerdings ist der „Bottom-up"-Ansatz auch um ein Vielfaches aufwendiger. In der Praxis bietet sich eine Kombination beider Methoden an.

Sind die Risiken erkannt, so erfolgt in der nächsten Phase der Risikobewertung eine Quantifizierung der Risiken hinsichtlich Erwartungswert. Der Erwartungswert bestimmt sich aus der Multiplikation der Eintrittswahrscheinlichkeit mit dem Schadensausmaß (Risikopotenzial, Tragweite). Die **Risikobewertung** zielt darauf ab, die Risiken hinsichtlich ihres Gefährdungspotenzials in eine Rangordnung zu bringen sowie ein unternehmensindividuelles Risikoportfolio (auch Risikolandschaft, Risikomatrix oder Risk Map bezeichnet; vgl. Abb. 6) abzubilden.

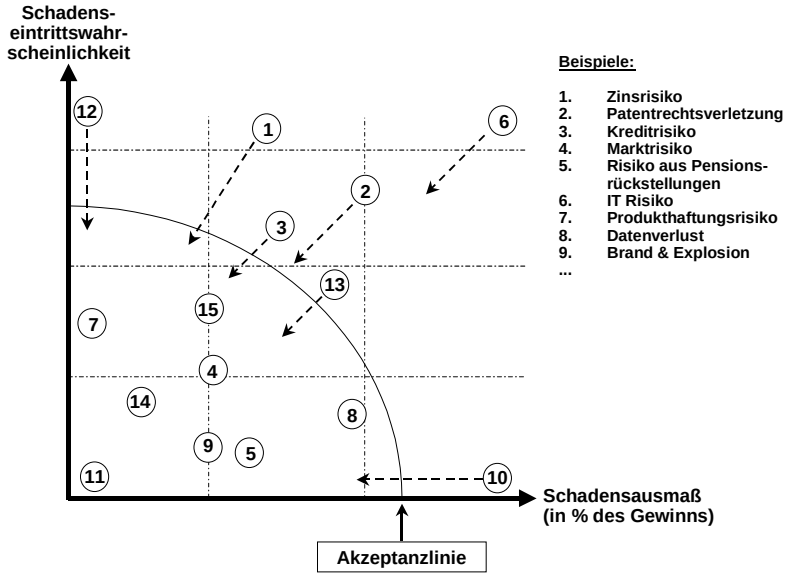

Abb. 6: Risikomatrix

Bei der Bewertung bedient man sich diverser Analysemethoden, wie beispielweise Equity-Risk-Contour-Methode, Fehlerbaumanalysen, Störfallablaufanalysen, Value-at-Risk, ABC-Analyse, Scoringmodelle, Szenariotechnik, Sensitivitätsanalysen, Monte-Carlo-Simulationen etc. Mit Hilfe von Stresssimulationen können „low frequency – high severity“ Risiken analysiert werden. Insbesondere bei Finanzrisiken wurden in den vergangenen Jahren diverse mathematisch-statistische Modelle entwickelt.

Die Aufgabe der Risikobewertung besteht darin, aus den gesammelten Daten aussagekräftige Informationen über die Risikolage des Unternehmens zu generieren. Durch eine quantitative Bewertung mittels der Parameter Schadenausmaß und Schadeneintrittswahrscheinlichkeit können Risiken zahlenmäßig charakterisiert werden. Die quantitative Risikobewertung hat verschiedene Vorteile. Erstens ermöglicht sie eine Erfassung, Beschreibung, Darstellung und Gegenüberstellung der einzelnen Risiken. Ein Vergleich der Risiken erlaubt zweitens eine differenzierte Einschätzung der Ist-Risikolage eines Unternehmens. Diese Erkenntnis ist drittens von praktischem Interesse, weil sich mit der quantitativen Bewertung zukünftige, wünschenswerte Risikosituationen zahlenmäßig beschreiben lassen (z. B. mit quantifizierten Risikozielen) [29, Brühwiler, S. 49 f.].

Das RMIS unterstützt den Risk Manager hierbei durch statistische Verfahren und Berechnungen. Um beispielsweise das Schadenausmaß eines Feuerrisikos in einem „Worst-case"-Szenario quantifizieren zu können, stehen dem Risk Manager verschiedene Berechnungsmethoden innerhalb des RMIS zur Verfügung. Für die Quantifizierung des maximal möglichen Höchstschadens, den z. B. ein Feuer verursachen kann, wird der Maximum Possible Loss (MPL) dieses Ereignisses berechnet. Der MPL ist der Schaden, „der sich ereignen kann, wenn die ungünstigsten Umstände in mehr oder weniger ungewöhnlicher Weise zusammentreffen, wenn das Feuer nicht oder nur unzureichend bekämpft werden kann und nur durch ein unüberwindbares Hindernis aufgehalten wird oder mangels Nahrung zum Erlöschen kommt“ [30, Wyss, S. 2 f.].

Für die Gegenüberstellung von Risiken muss neben dem MPL die Schadeneintrittswahrscheinlichkeit (relative Häufigkeit eines Schadeneintritts) ermittelt werden. Mit Hilfe der Schadeneintrittswahrscheinlichkeit wird die Bewertung des Schadenausmaßes um eine probabilistische Komponente erweitert, so dass der erwartete Höchstschaden (den so genannten „Estimated Maximum Loss“ / EML) quantifiziert werden kann. Der EML ist der Schaden, „der sich unter den normalen Betriebs-, Benutzungs- und Schadenabwehrbedingungen des in Frage kommenden Gebäudes ereignen kann, wobei außergewöhnliche Umstände (Unfall oder unvorhergesehenes Ereignis), die das Risiko wesentlich verändern könnten, nicht in Betracht

gezogen werden" [30, Wyss, S. 2 f.]. Der Unterschied zum maximal möglichen Höchstschadens (MPL) liegt darin, dass im Falle des EML das Funktionieren der risikopolitischen Maßnahmen berücksichtigt wird. Für die Quantifizierung der Schadeneintrittswahrscheinlichkeit sind unterschiedliche Alternativen denkbar. Neben der Dichtefunktion werden zur Beschreibung einer Wahrscheinlichkeitsverteilung insbesondere verschiedene statistische Maßzahlen, wie der Erwartungswert, die Streuung und der Variationskoeffizient verwendet. Die mathematischen Grundlagen hierfür liefert die Risikotheorie [31, Heilmann].

Die so ermittelten Ergebnisse der Risikoidentifikation und -bewertung werden in einem rechnerunterstützten Risikoinventar bzw. in einer Risikomatrix (auch „Risk Landscaping“ oder „Riskmap“ genannt) festgehalten. Die rasante Entwicklung in Wirtschaft und Technik sowie die Komplexität der Risiken lässt zunehmend die Notwendigkeit einer IT-gestützten Risikoidentifikation (z. B. durch computergestützte Checklisten und Schadenanalysen) erkennen. Ein RMIS kann z. B. durch eine rechnergestützte Schadenanalyse häufig auftretende Schäden und deren Schadenursachen aus den Datenbanken identifizieren oder zumindest eingrenzen.

Ist aufgrund der Datenlage eine objektive Quantifizierung nicht möglich (beispielsweise bei Imageverlust), so wird das Risiko subjektiv bewertet (existenzbedrohend, schwerwiegend, mittel, gering, unbedeutend). Eine Bewertung mit Hilfe von mathematisch-statistischen Modellen ist insbesondere bei operationellen Risiken problematisch, da häufig keine sinnvolle Datenbasis vorliegt. Gerade in diesem Zusammenhang eröffnet ein effizientes RMIS wiederum zahlreiche Ansatzpunkte, um die genannten Nachteile zu vermeiden. Darüber hinaus kann das RMIS das „Durchspielen" von „Worst-case"-Szenarien unterstützen. Das ist insofern nützlich, als dass bei der Analyse der Risikolage grundsätzlich ereignisorientiert vorgegangen und der „Worst-case"-Fall unterstellt werden sollte [32, Ibing, S. 13]. Im Bereich des Brandschutzes sind u. a. folgende Schadenszenarien denkbar:

- Sachschadenszenario
- Personenschadenszenario
- Betriebsunterbrechungsszenario.

Die bei den Schadenszenarien auftretenden Interdependenzen der Schadenpotentiale (z. B. Vermögensschaden durch nicht erfüllbare Lieferverpflichtungen aufgrund einer durch einen Sachschaden verursachten Betriebsunterbrechung) erfordern eine systematische Analyse bzw. Simulation aller möglichen Ablaufvarianten eines Schadeneintritts. Wie bereits am Beginn des Beitrags gezeigt wurde, kann ein Mensch kann diese komplexen Verknüpfungen häufig nicht mehr gedanklich nachvollziehen. Mit Hilfe eines RMIS ist der Entscheider jedoch in der Lage, diese Szenarien u. a. durch Rückgriff auf geeignete Analyseverfahren und Simulationsmodelle durchzuführen [21, Stahlknecht, S. 330].

Bei einem Betriebsunterbrechungsszenario werden beispielsweise die sich im ganzen Unternehmen fortpflanzenden Auswirkungen des Ausfall eines beliebigen Betriebsteils, einer Anlage oder einer Maschine auf den betrieblichen Ablauf und auf die Ertragslage des Unternehmens simuliert. Dabei müssen die Abhängigkeiten des Unternehmens zu den Beschaffungs- und Absatzmärkten beachtet werden. Derartige Analysen sind aufgrund ihrer hohen Komplexität und der zahlreichen Interdependenzen wiederum nur mit Hilfe eines RMIS möglich. Das RMIS ermittelt anhand der verfügbaren Daten (Lagerbestand, Auftragsbestand, Wiederbeschaffungszeiten von technischen Einrichtungen etc.), dann beispielsweise, wann ein Unternehmen unter Berücksichtigung von Ausweich- und Zukaufmöglichkeiten die Produktion sicher wiederaufnehmen kann [32, Ibing, S. 32 f].

Um ein Gesamt-Risikoportfolio des Unternehmens oder einzelner Unternehmensbereiche zu ermitteln, müssen die positiven und negativen Rückkoppelungen sowie eine eventuelle Kumulierung berücksichtigt werden. Eine Methode zur Aggregation der Einzelrisiken ist beispielsweise die Monte-Carlo-Simulation. In diversen Risikosimulationen werden bestimmte Risikoparameter abgebildet. Basierend auf einer Risikomodellierung können dann mit Hilfe eines Zufallszahlengenerators beispielsweise mehrere Geschäftsjahre „durchgespielt“ und die Auswirkungen auf die Bilanz berechnet werden. Insbesondere bei der Analyse und Bewertung von relativ großen Gesamt-Risikoportfolios zeigen sich die Effizienzvorteile eines rechnergestützten RMIS.

Schließlich kann auch das Risikoinventar als abschließender Bestandteil der Risikoanalyse innerhalb des RMIS IT-gestützt abgebildet werden. Es speichert alle Risikoinformationen, die für die Entscheidungsvorbereitung und -findung erforderlich sind. Das Risikoinventar enthält: u. a.

- die Erfassung aller Risiken, gegliedert nach den betrieblichen Funktionsbereichen,
- die quantitative und qualitative Bewertung der Risiken, gegliedert nach Risikoklassen,
- die Erfassung der Risikokosten,
- die Beurteilung der Wirksamkeit der bestehenden risikopolitischen Maßnahmen,
- die Ansatzpunkte zur Verbesserung der Risikobewältigung,
- die Priorität, mit welcher die Maßnahmen zur Risikobewältigung realisiert werden sollen.

Das Risikoinventar zeigt somit auf, für welche Risiken Maßnahmen zur Risikobewältigung erforderlich sind und mit welcher Priorität diese Maßnahmen realisiert werden müssen.

4.3 Prozess der Risikosteuerung und -kontrolle

Eine Schlüsselstelle im gesamten Risk Management Prozess nimmt die **Risikosteuerung und -kontrolle** ein. Diese Phase zielt darauf ab, die Risikolage des Unternehmens positiv zu verändern bzw. ein ausgewogenes Verhältnis zwischen Ertrag (Chance) und Verlustgefahr (Risiko) zu erreichen. Die Risikosteuerung und -kontrolle umfasst alle Mechanismen und Maßnahmen zur Beeinflussung der Risikosituation, entweder durch eine Verringerung der Eintrittwahrscheinlichkeit und / oder dem Schadensausmaß. Dabei sollte die Risikosteuerung und -kontrolle mit den in der Risikostrategie definierten Zielen übereinstimmen.

Im Hinblick auf die Gestaltung von Risiken bestehen prinzipiell drei Strategiealternativen (vgl. Abb. 7). Die sogenannte *ätiologische* (oder *präventive*) Risikopolitik zielt darauf ab, Risiken durch eine Beseitigung oder Reduzierung der entsprechen-

den *Ursachen* zu vermeiden oder zu vermindern. Dies setzt trivialerweise voraus, daß überhaupt die Möglichkeit zur Beeinflussung der Risikoursache besteht, was jedoch bei sogenannten *exogenen* Risiken (wie z. B. Naturkatastrophen) nicht der Fall ist. Im Gegensatz dazu wird bei der sogenannten *palliativen* (oder *korrektiven*) Risikopolitik der Eintritt eines Risikos bewußt akzeptiert. Durch geeignete Maßnahmen versucht der Risikoträger allerdings, die *Auswirkungen* des Risikoeintritts zu vermeiden oder zu vermindern [33, Schierenbeck, S. 3]. Dies kann beispielsweise in Form der häufig praktizierten Überwälzung von Risiken auf andere Risikoträger geschehen [34, Imboden, S. 113]. Eine weitere Alternative besteht schließlich darin, keinerlei risikopolitischen Maßnahmen zu ergreifen, sondern das Risiko selbst zu übernehmen.

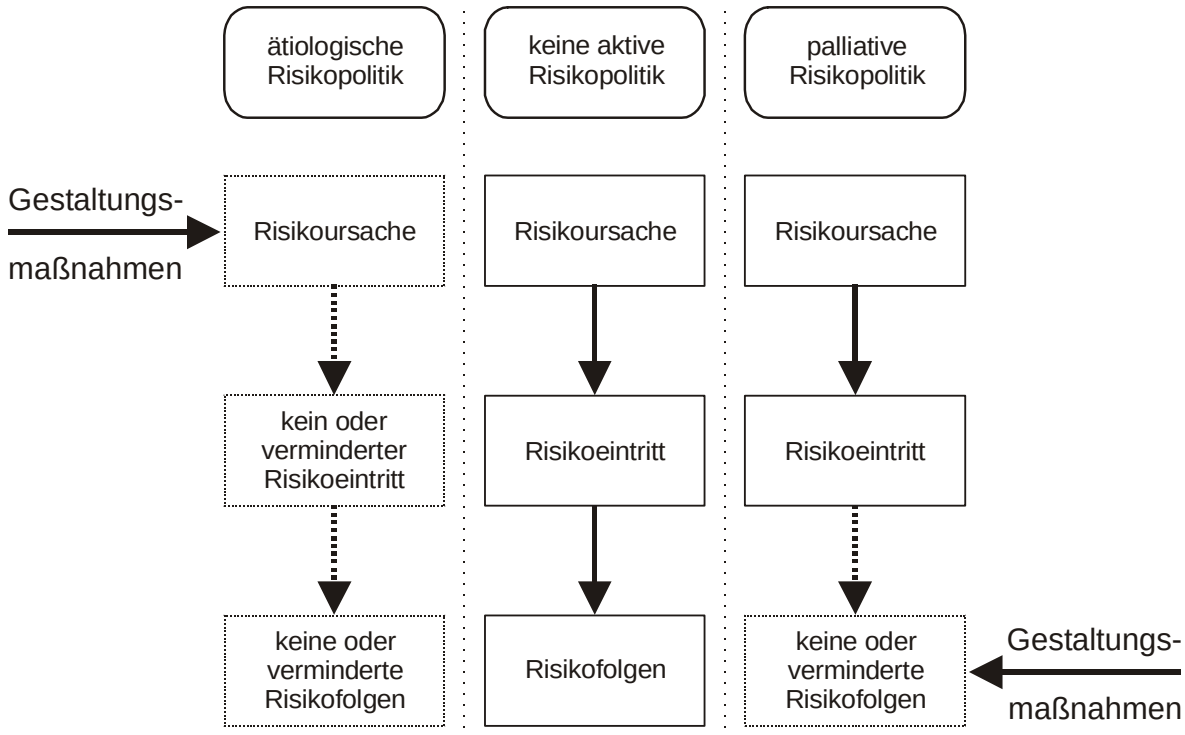

Abb. 7: Arten der Risikopolitik [35, GUTMANNSTHAL-KRIZANTIS, S. 357].

Bei komplexeren Modellen der Risikosteuerung und -kontrolle bietet sich ebenfalls der Einsatz von Computersimulationen an. Die simulierten Daten werden mit den gleichen Methoden und Modellen des RMIS bewertet und verdichtet, wie die realen Daten, welche die Ist-Risikolage des Unternehmens charakterisieren. Die für die Risikoanalyse bereits eingesetzten Modelle (z. B. das Simulationsmodell für das

Sachschadenszenario) werden durch Veränderung von Parametern oder durch strukturelle Modelländerungen in den gewünschten Zustand gebracht und ausgewertet. Das RMIS schätzt dabei u. a. durch „What-if"-Analysen (Wirkungsrechnungen) die Auswirkungen der quantifizierbaren Maßnahmen ab [36, Mertens/Griese, S. 4-6]. Im Bereich des Brandschutzes sind beispielsweise folgende Analysen zweckmäßig:

- Die Schadenverhütungsanalyse untersucht die Auswirkungen von geplanten Maßnahmen zur Risikokontrolle. Beispielsweise kann die Effektivität einer Sprinkler-Anlage im Brandfall analysiert werden. Das bereits bestehende Modell für die Simulation eines Sachschadenszenarios wird dazu so verändert, dass in dem Modell die Installation einer Sprinkler-Anlage berücksichtigt wird.
- Die Risikofinanzierungsanalyse überprüft, inwieweit die einzelnen Risiken eines Unternehmens durch die bestehenden Risikofinanzierungsmaßnahmen abgedeckt sind. Anhand der Ergebnisse kann analysiert werden, ob beispielsweise die Selbstbehalte, die Versicherungssummen und die daraus resultierenden Versicherungsprämien in ihrer Höhe risikoadäquat vereinbart sind. Darüber hinaus können die Auswirkungen eines Sachschaden- bzw. Betriebsunterbrechungsszenarios auf die unterschiedlichen Risikofinanzierungsmaßnahmen analysiert werden. Es kann beispielsweise überprüft werden, ob das Unternehmen auch im „Worst-case"-Fall in der Lage ist, die notwendigen finanziellen Mittel aufzubringen. Das Ziel der Risikofinanzierungsanalyse besteht in einer Optimierung der einzelnen Risikofinanzierungsmaßnahmen.

4.4 Entscheidung über risikopolitische Handlungsalternativen mit Hilfe einer Cockpitlösung

Die Unternehmensleitung kann nur dann risikoadäquate Entscheidungen treffen, wenn sie ausreichend über die Risikolage des Unternehmens informiert ist [27, Hertel, S. 83]. Hierfür benötigt sie komprimierte und übersichtlich aufbereitete Informationen, welche die Problemerkennung und Alternativenauswahl unterstützen [27, Haasis, S. 8]. Ein RMIS hat die Aufgabe, diesen internen Informationsbedarf zu

decken. Es muss die bisher gewonnen Informationen zweckmäßig bündeln und die Risikolage losgelöst von den Einzelrisiken darstellen [27, Haasis, S. 8]. Beispielsweise könnte die Risikolage eines Unternehmens in Form einer Risikomatrix dargestellt werden (siehe Abb. 6). Das RMIS kann diese Aufgaben der Informationsverdichtung and -aggregierung vollständig übernehmen.

Die Unternehmensleitung sollte jederzeit die Möglichkeit haben, die aktuelle Risikosituation des Unternehmens (ad hoc) abrufen zu können. Dabei kann eine mehrdimensionale Datenhaltung und Darstellung einen wahlfreien und interaktiven Zugriff auf die selektierten Daten bieten. Eine weitere Anforderung an ein RMIS besteht darin, eine vereinfachte Sicht auf die Daten zu ermöglichen – etwa basierend auf einer Management Cockpit Lösung - und unterschiedliche Verdichtungsstufen der Daten bereit zu stellen [25, Hornung/Reichmann/Baumöl, S. 40]. Das RMIS kann demnach eine schnellere und einfachere Entscheidungsfindung ermöglichen. Durch die Aggregation und Vereinfachung wird zwar zwangsläufig ein Informationsverlust in Kauf genommen – jedoch besteht das Primärziel einer Cockpitlösung darin, dem Management nur die wirklich zentralen Informationen zur Verfügung zu stellen, um einen „Information-Overload“ zu verhindern. Auf diese Weise kann auf jeden Fall erreicht werden, dass auch die Unternehmensführung für „Risikothemen“ sensibilisiert wird und sich intensiver mit diesen Fragestellungen beschäftigt. Gleichzeitig bietet eine derartige Lösung auch die Chance, dass das (in der Regel eher generalistisch orientierte) Topmanagement einerseits und die Spezialisten in den Risk Management und Controllingabteilungen andererseits sprachlich und gedanklich auf einer gemeinsame Ebene kommunizieren können.

Schließlich müssen die umgesetzten Maßnahmen hinsichtlich ihrer Wirksamkeit und ihres Nutzens auch kontrolliert werden. Die Effektivität der Maßnahmen kann beispielsweise durch Abweichungsanalysen untersucht werden. Dabei werden die Ist-Daten der Risikolage dem Sollzustand, den die Unternehmensleitung im Rahmen des strategischen RM vorgegeben hat, gegenübergestellt. Die Umsetzung der risikopolitischen Maßnahmen führt in der Regel zu einer Veränderung der Risikolage, so dass eine neue Erfassung der Daten erforderlich ist, um die Datenbanken des RMIS auf einem aktuellen Stand zu halten.

5 Schlussbetrachtung und Ausblick

„Computer schaffen die Möglichkeit einer völlig neuartigen Beziehung zwischen Theorien und Modellen“, so Joseph Weizenbaum 1976 in seinem Buch „Die Macht der Computer und die Ohnmacht der Vernunft“ [37, Weizenbaum]. Die bisherige Betrachtung hat gezeigt, dass mit dem Einsatz von RMIS eine Reihe von Vorteilen verbunden sind. Das RMIS kann einen großen Teil der Aufgaben erledigen, die der Risk Manager in der Vergangenheit manuell durchgeführt hat, wie etwa das Erstellen eines Risikoinventars oder einer Risikomatrix. Darüber hinaus enthält das RMIS Funktionen, die dem Risk Manager bisher in der Form nicht zur Verfügung standen, wie etwa die Funktion zur Simulation von Schadenszenarien.

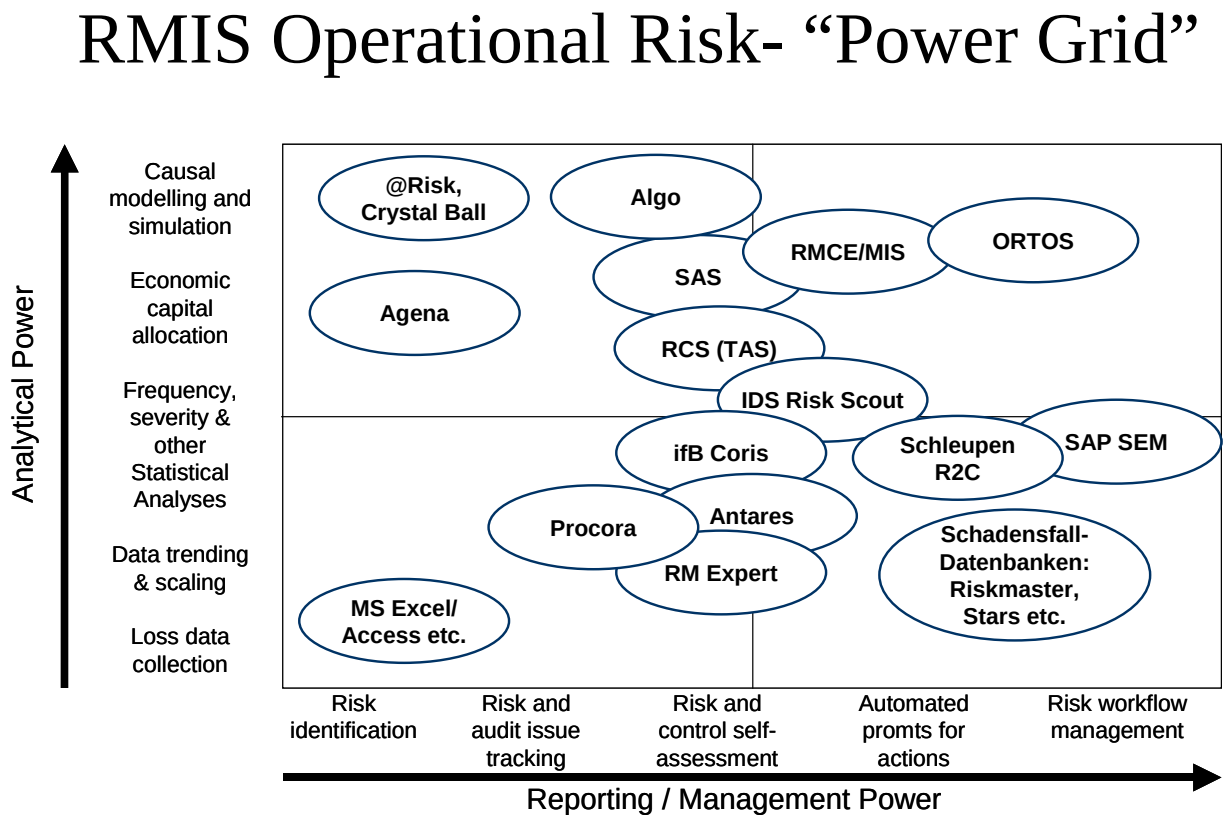

Abb. 8: Produktmatrix im Bereich der RMIS

Die heute am Markt angebotenen RMIS unterscheiden sich sehr stark bezüglich ihrer analytischen Fähigkeiten und Berichtsmöglichkeiten. Die Bandbreite im Bereich der analytischen Möglichkeiten reicht von einfachen Excel Datenblättern bis zu komplexen Simulationstools. Wie in der folgenden Klassifikation deutlich wird, sind zahlreiche Tools mit umfangreichen Methoden-Bibliotheken ausgestattet (What-if

Analysen, Simulationen, Prognoseverfahren, Abbildung von Ursache-Wirkungs-Zusammenhängen, Data-Mining-Werkzeuge, etc.). Einige Produkte haben Management Cockpits integriert, die speziell an den Bedürfnissen der Entscheidungsträger ausgerichtet sind.

Trotz ihrer vielfältigen Vorteile müssen auch gewisse Einschränkungen bei der Benutzung eines RMIS beachtet werden. Die Unterstützung durch ein RMIS darf keinesfalls dazu führen, dass sich die Entscheidungsträger in Sicherheit wiegen, wenn sämtliche Risiken im Computersystem als tragbar eingestuft werden. Das bedeutet, dass die Unternehmensleitung die Erwägungen über zukünftige Risikoentwicklungen nicht auf die Variablen beschränken darf, die sich im RMIS abbilden lassen. Weiter ist kritisch zu beurteilen, dass Simulationen und Modelle häufig auf vergangenheitsorientierten Daten basieren [38, Bernstein, S. 116]. Damit ist die als kritisch zu bewertende Annahme verbunden, dass die Ursache-Wirkungs-Zusammenhänge von Risiken für jeden Schadenfall gleich sind.

Das RMIS kann zwar in kurzer Zeit viele Szenarien durchrechnen und die Ergebnisse in verschiedenen Farben visualisieren, dass dies jedoch für jedes Entscheidungsproblem im RM tatsächlich zu optimalen Entscheidungen führt, kann nicht allgemein postuliert werden [28, Beroggi, S. 57 f.]. Nicht zuletzt hängt die Qualität der Ergebnisse auch immer von der Qualität der verwendeten Inputs sowie der Abbildungsgenauigkeit der hinterlegten Modelle ab. Gerade bei hochkomplexen Problemen, wie sie für das Risk Management charakteristisch sind, stoßen diese Modelle jedoch oft an ihre Grenzen, da bei jeder Modellierung Vereinfachungen unerlässlich sind. ZADEH drückt diese Diskrepanz zwischen (Schein-)Präzision und semantischem Gehalt bei Aussagen über komplexe Systeme beispielsweise folgendermaßen aus: „As the complexity of a system increases, our ability to make precise and yet significant statements about its behavior diminishes until a threshold is reached beyond which precision and significance (or relevance) become almost mutually exclusive characteristics. ... Precise quantitative analyses of the behavior of ... systems are not likely to have much relevance to real-world problems.“ [39, Zadeh, S. 30]. Unter diesem Aspekt werden (und müssen!) Entscheidungen auch beim Ein-

satz des besten RMIS auch weiterhin noch oft auf Intuition und persönlichen Erfahrungen basieren.

Daher wird ein RMIS auch nie in der Lage sein, den Risk Manager oder einen externen Berater vollständig zu substituieren und strebt dies auch nicht an. Vielmehr wird mit dem Einsatz eines RMIS versucht, die „menschlichen" Vorzüge des Risk Managers oder Entscheidungsträgers mit der Leistungsfähigkeit eines Computers (fehlerfreies Arbeiten, schnelle Verarbeitung von Daten etc.) in einem effizienten und effektiven Mensch-Maschine-System zu verbinden. Die Arbeitsteilung ist besonders bei solchen Aufgaben sinnvoll, bei denen die Komplexität der Daten die kognitiven Fähigkeiten des Menschen überfordern. In diesen Fällen ist die formale Strukturierung - beispielsweise durch ein computergestütztes Modell - von Vorteil.

Mit Hilfe von „unternehmerischer Intuition“ und reaktiven Steuerungssystemen dürfte es immer schwieriger werden, die Komplexität der Prozesse und Risiken eines Unternehmens zu erfassen, zu analysieren und vor allem zu aggregieren. Ein funktionierendes und effizientes Risikomanagement, eine gelebte Risiko- und Kontrollkultur sowie ein effizientes IT gestütztes Risk Management Informationssystem entwickelt sich immer mehr zu einem wesentlichen Erfolgsfaktor für das Unternehmen. Nur die Unternehmen die ihre Risiken effizient steuern und kontrollieren sowie ihre Chancen erkennen und nutzen werden langfristig erfolgreich sein und ihren Unternehmenswert steigern.

Literatur

0 Romeike, Frank: Integration von E-Business und Internet in das Risk Management des Unternehmens, in: Kommunikation & Recht (Betriebs-Berater), Ausgabe 8, August 2001, S. 412-417.

1 Braun, H.: Risikomanagement, Darmstadt 1984.

2 Erben, R. F.; Nagel, K., Piller, F.: Informationsrevolution und industrielle Produktion, in: Erben, R.; Nagel, K.; Piller, F. [Hrsg]: Produktionswirtschaft 2000, Wiesbaden 1999, S. 3-32.

3 Bertalanffy, L. v.: Zu einer allgemeinen Systemlehre, in: Bleicher, K. [Hrsg.]: Organisation als System, Wiesbaden 1972, S. 31-45.

4 Hazebrouck, J.-P.: Konzeption eines Management Support Systems zur Frühaufklärung, Wiesbaden 1998.

5 Neubürger, K. W.: Risikobeurteilung bei strategischen Unternehmensentscheidungen, Stuttgart 1980.

6 Schuy, A.: Risiko-Management, Frankfurt a. M. et al. 1989.

7 Adam, D.: Heuristische Planung, in: Schulte, C. [Hrsg.]: Lexikon des Controlling, München 1996, S. 314-317.

8 Kopel, M.: Komplexe Unternehmensdynamik, Wiesbaden 1994.

9 Kotler, P.; Bliemel, F.: Marketing-Management, 10. Aufl., Stuttgart 2001.

10 Simon, H. D.: Administrative Behavior, 4. Aufl., New York 1997.

11 Ansoff, H. I.: Managing Surprise and Discontinuity, in: Zeitschrift für betriebswirtschaftliche Forschung (1976), H. 2, S. 129-152.

12 Erben, R. F.: Fuzzy-Logic-basiertes Risikomanagement, Aachen 2000.

13 Farny, D.: Risk Management und Planung, in: Szyperski, N. [Hrsg.]: Enzyklopädie der Betriebswirtschaftslehre, Bd. 9: Handwörterbuch der Planung, Stuttgart 1989, Sp. 1749-1758.

14 Meyer, M.: Die Beurteilung von Länderrisiken der internationalen Unternehmung, Berlin 1987.

15 Bosch, H.: Entscheidung und Unschärfe, Bergisch Gladbach; Köln 1993.

16 Kratzheller, J. B.: Risiko und Risk Management aus organisationswissenschaftlicher Perspektive, Wiesbaden 1997.

17 Wildawsky, A.: Vergleichende Untersuchung zur Risikowahrnehmung, in: Bayerische Rückversicherung AG [Hrsg.]: Risiko ist ein Konstrukt, München 1993, S. 191-211.

18 Keil, R.: Strategieentwicklung bei qualitativen Zielen, Berlin 1996.

19 Picot, A.; Reichwald, R.: Informationswirtschaft, in: Heinen, E. [Hrsg.]: Industriebetriebslehre, 9. Aufl., Wiesbaden 1991, S. 241-393.

20 Schneck, O.: Lexikon der Betriebswirtschaft, 2. Aufl., München 1994.

21 Stahlknecht, P.: Einführung in die Wirtschaftsinformatik, 6. Aufl., Berlin et al. 1993.

22 Henneböle, J.: Executive Information Systems für Unternehmensführung und Controlling, Wiesbaden 1995.

23 Pfohl, H.-C.: Planung und Kontrolle, Stuttgart et al. 1981.

24 Romeike, F.: Risikomanagement als Basis einer wertorientierten Unternehmenssteuerung, in: AssCompact - Fachmagazin für Risiko- und Kapitalmanagement (2001), H. 11.

25 Hornung, K.; Reichmann, T.; Baumöl, U.: Informationsverarbeitungsstrategien für einen multinationalen Konzern - Risikomanagement mit Hilfe innovativer Informationssysteme. In: Controlling (1997), H. 1, S. 38-45.

26 Haasis, H.-D. et al.: Anforderungen an Betriebliche Umweltinformationssysteme (BUIS) und Ansätze zur Realisierung. In: Haasis, H.-D. et al. (Hrsg.), Umweltinformationssysteme, München 1995, S. 7-25.

27 Hertel, A.: Risk Management in der Praxis, hrsg. von Gerling Consulting Gruppe, Köln 1991.

28 Beroggi, Giampiero E.G. [Technologien, 1995]: Neue Technologien zur Unterstützung des Risikomanagements - Eine Systems Engineering Betrachtungsweise zum Entwurf von Risikoinformationssystemen, Zürich 1995.

29 Brühwiler, B.: Risk Management - eine Aufgabe der Unternehmensführung, Bern, Stuttgart 1980.

30 Wyss, A.: MPL / EML Assessment, interne Arbeit der Schweizerischen Rückversicherungs-Gesellschaft, Zürich 1981.

31 Heilmann, W.-R.: Grundbegriffe der Risikotheorie, Karlsruhe 1987.

32 Ibing, H.-P.: Sicherheitsmanagent - Ein Instrument der Ergebnissteuerung, Landsberg/Lech 1996.

33 Schierenbeck, H.: Ertragsorientiertes Bankmanagement, Bd. 2: Risikocontrolling und Bilanzstruktur-Management, 5. Aufl., Wiesbaden 1997.

34 Imboden, C.: Risikohandhabung: Ein entscheidbezogenes Verfahren, Bern; Stuttgart 1983.

35 Gutmannsthal-Krizantis, H.: Risikomanagement von Anlageprojekten, Wiesbaden 1994.

36 Mertens, P.; Griese, J.: Integrierte Informationsverarbeitung 2: Planungs- und Kontrollsysteme in der Industrie, 7. Aufl., Wiesbaden 1993.

37 Weizenbaum, J.: Die Macht der Computer und die Ohnmacht der Vernunft, Frankfurt 1977.

38 Bernstein, P. L.: Risiken gehorchen keinen Zahlen. In: Harvard Business Manager (1996), H. 3, S. 113-116.

39 Zadeh, L. A.: Outline of a new approach to the analysis of complex systems and decision processes, in: IEEE Transactions on Systems, Man and Cybernetics, New York 1973, S. 28-44.

Über die Autoren

Frank Romeike, Jahrgang 1968, Studium der Betriebswirtschaft in Köln und Norwich (UK), anschließend Studium der Politikwissenschaften, Psychologie und Philosophie. Als Unternehmensberater im Bereich Risk Management, Asset Liability Management und Alternative Risk Financing tätig. Zuvor war er Risk Manager bei der IBM Deutschland in Stuttgart, wo er u.a. an der Implementierung eines weltweiten Risk Management Prozesses beteiligt war. Er war verantwortlich für den Risikomanagement-Prozess der IBM Central Region und leitete mehrere internationale Projekte, u.a. die Einführung eines Risk Management Informationssystems bei der IBM.
Er hat sich intensiv mit dem Einsatz und der Steuerung integrativer Produkte aus dem Bereich „Alternative Risk Transfer“ zur Absicherung von Betriebs-, Marktrisiken etc. beschäftigt. Er ist Mitglied in verschiedenen Fachverbänden und Autor zahlreicher Publikationen rund um die Themen Risk Management, Krisenmanagement und Risikofinanzierung. Frank Romeike hat einen Lehrauftrag an der FHTW Berlin (Schwerpunkt: Innovatives Controlling; Risikomanagement).
Mit RiskNET (www.RiskNet.de) hat er das führende, deutschsprachige Internet-Portal zum Thema Risk Management aufgebaut. Er ist Chefredakteur und Herausgeber des Online-Magazins RiskNEWS (www.risknews.de). Beim Bank-Verlag (Köln) ist er stellvertretender Chefredakteur der Zeitschrift RATINGaktuell.

Dr. Roland Franz Erben, Jahrgang 1970, Studium der Betriebswirtschaft an der Bayerischen Julius-Maximilians-Universität Würzburg, Promotion zum Thema „Fuzzy-Logicbsiertes Risikomanagement“ am Lehrstuhl für Industriebetriebslehre (Prof. Dr. H. Koller). Nach einer Tätigkeit im Konzerncontrolling eines Telekommunikationsunternehmens arbeitete Dr. Erben als Consultant für die Bereiche Risk Management (insbes. Operationelle Risiken) sowie Controlling bei einer großen deutschen Unternehmensberatung. Im Rahmen eines Forschungsprojekts war er im Sommer 2002 außerdem an der Technischen Universität München tätig. Seine

Spezialgebiete innerhalb des Risk Manangements sind operative und strategische Risiken, insbesondere „Brand Risk Management“ (Risikoschutz für Marken).
Dr. Erben ist stellvertretender Chefredakteur des Online-Magazins RiskNEWS (www.risknews.de), Gründungsmitglied der European Academy of Management (EURAM), Mitglied in verschiedenen Fachverbänden und Autor zahlreicher Publikationen rund um die Themen Risiko- und Krisenmanagement sowie strategisches und operatives Controlling.

Der Beitrag wird in dem Buch

Risiken des Unternehmens - Denk- und Handwerkzeuge, Innovationen, nachhaltige Erfolge; Herausgeber: P.M.Pastors / PIKS, 2002

erscheinen.