

### SYSTEM CHECK WAS EIN RISIKOMANAGEMENTSYSTEM KÖNNEN MUSS ...



**Die Auswirkungen von Subprime- und Kapitalmarktkrise und hohe Volatilitäten bei Rohstoffpreisen und Wechselkursen zeigen es derzeit schonungslos auf: Zahlreiche Risikomanagementsysteme funktionieren nicht ausreichend. Auch im Jahr 10 nach KonTraG dienen viele Systeme in erster Linie der formalen Pflichterfüllung - über den Status eines Papiertigers kommen sie selten hinaus. Mehrwert stiftet Risikomanagement erfahrungsgemäß immer nur dann, wenn das System auch einen betriebswirtschaftlichen Wertbeitrag leistet! Die Praxis zeigt, dass mit einem Risikomanagementsystem, das aktiv in die Unternehmenssteuerung integriert ist, nicht nur Krisen vermieden und Schäden reduziert, sondern auch ökonomische Potenziale gehoben und Risikokosten optimiert werden können.**

Die Nutzenargumente, die für die Einführung und den aktiven Betrieb eines Risikomanagementsystems sprechen, sind schnell benannt: Risikomanagement schafft Transparenz über die betriebliche Risikolage und reduziert die Wahrscheinlichkeit einer Unternehmenskrise, die von Fehlentscheidungen aufgrund nicht rechtzeitig erkannter bzw. falsch bewerteter Gefahrenpotenziale herrühren. Letzteres zumindest dann, wenn das Risikomanagementsystem in der Praxis auch tatsächlich funktionstüchtig ist. Inwieweit dies sichergestellt ist, lässt sich mit Hilfe sogenannten System-Audits hinterfragen.

Im ersten Schritt gilt es zu hinterfragen, inwieweit das Unternehmen die relevanten formalen Anforderungen an ein Risikomanagementsystem tatsächlich erfüllt (wie z. B. nach KonTraG, DRS 5, IDW PS 340, EURO SOX, etc.). Die Erfüllung regulatorischer oder formaljuristischer Vorgaben ist zwingend. Sie sagt jedoch nichts über die tatsächliche Funktionalität und Effizienz eines Risikomanagementsystems in der Praxis sowie den zu generierenden betriebswirtschaftlichen Nutzen aus. Entsprechend gilt es zusätzlich zu prüfen, ob die vom Risikomanagementsystem zur Verfügung gestellten Informationen auch einen ökonomischen Mehrwert generieren und die Unternehmensführung in der Entscheidungsfindung unterstützen. Eine quantifizierte Aussage über den Gesamtrisikoumfang des Unternehmens oder über die Einschätzung zu möglichen risikobedingten Planabweichungen seien exemplarisch genannt.

Ob das Risikomanagement diesbezüglich zuverlässig funktioniert, lässt sich relativ einfach durch die Analyse von vorausgegangenen Planabweichungen feststellen. Risiko stellt per Definition die Möglichkeit einer Planabweichung dar. Deswegen sollte ein Risikomanagementsystem auf grundsätzlich mögliche, bedeutende Planabweichungen der zukünftigen Geschäftsentwicklung bereits im Vorfeld hinweisen. So gesehen dürfte es in einem Unternehmen mit funktionierendem Risikomanagement keine nachhaltigen Planabweichungen geben, die nicht bereits im Vorfeld als Risiko definiert wurden.

Die Funk RMCE GmbH hat in den vergangenen zehn Jahren eine Vielzahl von Unternehmen sowohl bei der Ersteinführung ihres Risikomanagements begleitet als auch bei der Optimierung bestehender Systeme beraten und unterstützt. Hierbei hat sich immer wieder gezeigt, dass es oft die gleichen Fehler und Missstände sind, die Risikomanagementsysteme in ihrer Leistungsfähigkeit hemmen. Nachstehend werden häufig anzutreffende Problemfelder von Risikomanagementsystemen im Kontext der Chronologie eines Risikomanagementprojektes aufgeführt und praxisbewährte Maßnahmen zur Optimierung dargestellt:

#### Phase 1: Risiko-Identifikation

Im Rahmen der Risiko-Identifikation werden alle relevanten Unternehmensrisiken systematisch erfasst. Folgende Fehler werden in der Praxis immer wieder beobachtet:

Keine Vorgabe von Risikokategorien: Es hat sich in der Praxis bewährt, im Rahmen der Risiko-identifikation Kategorien vorzugeben, denen die jeweiligen relevanten Einzelrisiken zugeordnet werden. Das können z. B. strategische Risiken, Marktrisiken, Finanzmarktrisiken, Risiken aus dem politischen und rechtlichen Umfeld, Risiken aus Corporate Governance oder Leistungsrisiken aus



der Wertschöpfung sowie deren Unterstützungsprozessen sein. Die vorgegebene Risikokategorisierung erleichtert die Identifikation von relevanten Einzelrisiken erheblich und hilft Doppelnennungen sowie Überschneidungen weitestgehend zu vermeiden.

**Risiko Identifikation - Bottom Up statt Top Down:** In vielen Unternehmen werden nach einem „Jäger und Sammler-Ansatz“ möglichst alle Mitarbeiter schriftlich oder mündlich befragt, um die ihnen einfallenden Risiken zu erheben und zusammenzutragen. Diese Methodik ist äußerst arbeits- und zeitaufwendig und zudem nicht besonders leistungsfähig. Mitarbeiter neigen dazu, gerade aktuelle Informationen weiterzugeben. Grundsätzlich bedeutsame Risiken, die jedoch derzeit nicht auf der Tagesordnung stehen, werden dagegen oftmals vergessen. Hier spielen auch psychologisch bedingte Fehleinschätzungen eine Rolle.

**Fehlender Bezug zur Unternehmensstrategie und den Erfolgsfaktoren:** Ein erheblicher Schwachpunkt der Risikoidentifikation ist das Fehlen eines klaren strategischen Bezuges. Grundsätzlich sollte systematisch abgeleitet werden, welche Risiken die Erreichung der maßgeblichen strategischen Ziele gefährden. Dazu gehören alle Arten von Bedrohungen zentraler Erfolgsfaktoren wie beispielsweise die Kernkompetenzen. Risikoidentifikations-Prozesse ohne Bezug zur Unternehmensstrategie laufen Gefahr, von den wirklich wesentlichen bestandsgefährdenden Risiken abzulenken.

**Kein Bezug zur Unternehmensplanung:** Jede unsichere Annahme, die in Controlling, Unternehmensplanung oder Budgetierung berücksichtigt wird - z. B. bezüglich des zukünftigen Dollarkurses - weist ein Risiko auf, das auch im Rahmen der Risikoidentifikation zu berücksichtigen ist. Da Risiken als mögliche Planabweichungen definiert sind, zeigt zudem jede tatsächlich eingetretene Planabweichung, dass ein Risiko wirksam geworden ist. Alle eingetretenen Planabweichungen sollten sich auf bekannte (identifizierte) Risiken zurück führen lassen.

## Phase 2: Risiko-Bewertung

Die in der Identifikationsphase erfassten Risiken werden im nächsten Schritt hinsichtlich Eintrittswahrscheinlichkeit und Auswirkung bewertet. Nachstehende Fehler sind im Kontext der Risiko-Bewertung immer wieder festzustellen:

**Fehler bei der Abgrenzung von Risiken:** Überschneidungen zwischen separat identifizierten Risiken werden nicht erkannt und Risiken doppelt gezählt.

**Verwechslung von Risiken und sicheren Schäden:** Sicher erwartete und in der Unternehmensplanung bereits erfasste Entwicklungen werden zusätzlich als Risiken eingestuft, wie etwa der sichere Verlust eines Großkunden. Solche Ereignisse sind zwar unangenehm, stehen aber fest und stellen definitionsbedingt kein Risiko dar.

**Fehlende Begründung der Risikobewertung:** Obwohl objektive Daten wie z. B. Zeitreihen verfügbar sind, werden subjektive Werte - also Schätzungen - verwendet. Diese subjektiven Daten sind insbesondere dann von geringer Qualität, wenn keine detaillierte und nachvollziehbare Herleitung oder Begründung zur Plausibilitätsprüfung angegeben wird. Schätzungen von Schadenshöhen, die nicht detailliert begründet oder hergeleitet werden, sind für Dritte nicht prüfbar und verstoßen gegen den Transparenzanspruch des Risikomanagements. Grundsätzlich ist auch die Berücksichtigung subjektiver Schätzungen von Risiken zulässig und nötig, weil ein scheinbarer Verzicht auf die Quantifizierung eines „qualitativen Risikos“ eine (falsche) Quantifizierung mit Null bedeutet.

**Null-Quantifizierung:** Sind objektive Wahrscheinlichkeiten nicht verfügbar, sollten bedeutende Risiken durchaus auch subjektiv bewertet werden, z. B. durch Expertenschätzungen. Jede subjektive Schätzung ist erfahrungsgemäß sinnvoller als eine Nichtquantifizierung, im Rahmen derer das Risiko ausgeblendet wird (Eintrittswahrscheinlichkeit null). Bei einem qualitativ vorhandenen Risiko ist dies die schlechteste aller Alternativen, da das Risiko folgend gänzlich aus der Betrachtung verschwindet.

Vernachlässigung der Wirkungsdauer von Risiken: Risiken, die nur einen einmaligen Schaden verursachen können und solche mit langanhaltenden Wirkungen, werden nicht unterschieden.



Nicht adäquate quantitative Beschreibung des Risikos: Für jedes Risiko ist zur quantitativen Beschreibung eine geeignete Wahrscheinlichkeitsverteilung zu wählen. In der Praxis werden häufig einheitlich Binomialverteilungen verwendet, also eine Beschreibung durch „Schadenshöhe“ und Eintrittswahrscheinlichkeit. Statt dessen können aber andere Verteilungen häufig besser geeignet sein, so etwa die Normalverteilung für hoch aggregierte Risiken, wie z. B. Umsatzenschwankungen oder Rohstoffpreisveränderungen. In der Praxis ebenfalls bedeutsam ist die sogenannte Dreiecksverteilung, bei der ein Risiko beschrieben wird durch Mindestwert, wahrscheinlichstem Wert und Maximalwert, sogenannten Szenarioschätzungen.

Fehlende Festlegung eines geeigneten Risikomaßes: Um die einzelnen Risiken miteinander vergleichen und priorisieren zu können, ist ein einheitliches Risikomaß erforderlich. In der Praxis werden häufig so genannte Downside-Risikomaße angewandt, die insbesondere die Konsequenzen möglicher negativer Planabweichungen (z. B. für das Rating) verdeutlichen. Zu diesen gehört der Value-at-Risk (VAR). Er beschreibt den maximal in einer Planungsperiode zu erwartenden Verlust, der mit einer vorgegebenen, von den Gläubigern akzeptierten, Wahrscheinlichkeit nicht überschritten wird. Ein anderes Downside-Risikomaß ist der auf dem ähnlichen Konzept basierende risikoadjustierte Eigenkapitalbedarf in einem zu definierenden Planungszeitraum. Die angesprochenen Downside-Maße werden in der Praxis gerne mit einem realistischen Höchstschaden verwechselt, was im Zweifelsfall ein fataler Fehler sein kann. So ist bei einem VAR5% zu beachten, dass zwar 95% aller Schäden den hierzu ausgewiesenen Wert nicht überschreiten, die verbleibenden 5% aber darüber liegen, ggf. sogar deutlich.

Vernachlässigung von Abhängigkeiten zwischen den Risiken (Korrelationen): In der Phase der Risikoaggregation werden die komplexen Wechselwirkungen zwischen den Risiken nicht berücksichtigt. Eine isolierte Betrachtung einzelner Risiken ist grundsätzlich wenig aussagefähig, weil deren Relevanz sich oft erst im Gesamtkontext bewerten lässt.

### Phase 3: Risiko-Aggregation

Zielsetzung der Risikoaggregation ist die Bestimmung der Gesamtrisikoposition der Unternehmung sowie der relativen Bedeutung der Einzelrisiken (Sensitivitätsanalyse). Dabei sind Wechselwirkungen durch Risikosimulationsverfahren zu berücksichtigen. Hierzu werden Wirkungen der Einzelrisiken im Kontext der im Unternehmen genutzten Planungsmodelle integriert und mögliche risikobedingte Zukunftsszenarien des Unternehmens berechnet und analysiert. Diese Vorgehensweise ermöglicht die Verbindung von Risikomanagement und „traditioneller“ Unternehmensplanung. Folgende Fehler werden in der Praxis beobachtet:

Addition von Risiken statt Aggregation: Hierbei werden die Schadenshöhen verschiedener Risiken einfach addiert. Eine Addition von Schadenshöhen einzelner Risiken ist jedoch nur für den völlig unrealistischen Fall angemessen, dass alle denkbaren Risiken des Unternehmens gleichzeitig eintreten. Auch die Addition von Schadenswerten auf ordinalen Skalen („Schadensklassen“, „Tragweite“) führt bei der Risikoaggregation zu falschen Ergebnissen und ist mathematisch unsinnig.

Aggregation von Einzelrisiken ohne Bezugnahme zur Unternehmensplanung: Risiken führen letztendlich zu Abweichungen der tatsächlichen und geplanten Unternehmensergebnisse. Für einen ökonomisch sinnvollen Umgang mit Risiken ist es erforderlich, dass die einzelnen Risiken in den Kontext der Unternehmensplanung gestellt werden. Risikomanagement zielt im Ergebnis darauf ab, die durch die jeweiligen Risiken hervorgerufenen Schwankungen der tatsächlichen Werte mittels festgesetzter Planwerte messbar und „managebar“ zu machen.

Fehlende Berechnung des Gesamtrisikoumfangs: Der aggregierte Gesamtrisikoumfang zeigt auf, wie hoch der risikoadjustierte Eigenkapitalbedarf für ein Unternehmen ist, um die gegebene Risikosituation z. B. im Rahmen eines definierten Betrachtungszeitraumes tragen – sprich überleben

- zu können. Wird eine solche Risikoaggregation und damit eine Berechnung des Eigenkapitals nicht vorgenommen, ist die fundierte Beurteilung einer angemessenen Eigenkapitalausstattung nicht möglich: Der Grad der Bestandsgefährdung eines Unternehmens ist somit nicht bestimmbar. Eine zentrale Aufgabe des Risikomanagements wird damit nicht gelöst und die Chance vergeben, auf Basis des ermittelten Eigenkapitalbedarfs, fundierte Kapitalkosten zu berechnen.

Überinterpretation der Aggregationsergebnisse: Die Ergebnisse einer Risiko-Aggregation basieren auf Annahmen und Schätzungen und können somit maximal eine näherungsweise richtige Aussage liefern. Nicht zuletzt auch deshalb, da im Rahmen einer Aggregation nur ausgesuchte Risiken berücksichtigt werden. Entsprechend ist bei der Interpretation und Nutzung der Ergebnisse Vorsicht geboten.

Übertheoretisierung: Risiko-Aggregationsmodelle sind hochkomplex und in der Praxis oftmals nicht leicht zu vermitteln. Entsprechend dienen sie Projektkritikern gerne als erste Angriffsfläche um das Gesamtprojekt zu torpedieren. Um auf die Erkenntnisse der Risiko-Aggregation nicht verzichten zu müssen, hat es sich in der Praxis bewährt, das Thema im kleinen Kreis zu behandeln und nicht in den Mittelpunkt des Gesamtprojektes zu stellen.

### Phase 4: Risiko-Bewältigung

Nachdem Risiken identifiziert und bewertet und im Rahmen einer Risiko Aggregation Erkenntnisse über die Risikotragkraft des Unternehmens ermittelt wurden, gilt es folgend geeignete Maßnahmen zu treffen, um die Risikoposition des Unternehmens zu optimieren. Um Chancen nicht zu verhindern geht es hierbei explizit nicht darum Risiken zu verhindern. Nachstehende Fehler werden immer wieder gemacht:



Ausschließliche Betrachtung von Versicherungslösungen: Der Risikobewältigung können völlig unterschiedliche Strategien dienen: Risikoreduzierung, Risikotransfer - z. B. durch Versicherungen oder geeignete Verträge mit Lieferanten - oder Selbsttragung des Risikos und Schaffung eines adäquaten Risikodeckungspotenzials durch Eigenkapital- und Liquiditätsreserven. Selbst unter den Risikotransfer-Möglichkeiten stellt das Versichern nur einen Weg dar. Ebenfalls zu berücksichtigen ist die Alternative, Risiken über Kapitalmärkte zu transferieren. Welche Risikobewältigungsstrategie die beste ist, kann nicht a priori entschieden werden. Hierzu sind detaillierte Analysen, wie die Berechnung des Wertbeitrags erforderlich, die leider zu oft unterbleiben.

Getrennte Betrachtung von Risiko- und Versicherungsmanagement: Das Versicherungsmanagement ist ein Instrument der Risikobewältigung, das integraler Bestandteil eines Risikomanagementsystems sein sollte und dessen Vorgaben folgt. In der Praxis besteht das Versicherungsmanagement aber oftmals als historisch gewachsenes, autonomes Subsystem, das vom Risikomanagement losgelöst agiert. Entsprechend wird der ökonomische Wertbeitrag von Versicherungslösungen selten hinterfragt. Konsequenz: Es wird häufig zu viel oder falsch versichert. Die Risikokosten sind zu hoch. Risikotransfer auf eine Versicherung ist insbesondere dann sinnvoll, wenn die zu bezahlende Versicherungsprämie unter Kapitalkosten liegt, die zur Risikoeigentragung zu kalkulieren sind. Demnach ist Versicherungsschutz zumeist nur im Bereich mittlerer Risiken und für Großschäden sinnvoll, Klein- und Frequenzschäden sollten tendenziell selbst getragen werden.

Fehlende Beachtung unternehmerischer Entscheidungsrisiken: Die psychologische Forschung belegt, dass die für den betrieblichen Erfolg maßgeblichen Entscheidungen der Unternehmer und Führungskräfte nicht nur von deren Fachkompetenz und von der Qualität der verfügbaren Informationen abhängt. Nicht selten führen psychologisch bedingte „Denkfallen“ zu bestimmten typischen Fehlentscheidungen und hohen unternehmerischen Risiken.

Fehlende Abgrenzung von Kern- und Randrisiken: Kernrisiken sind jene Risiken, die im unmittelbaren Zusammenhang mit dem Aufbau und der Nutzung von Erfolgspotenzialen stehen. Diese können kaum sinnvoll auf Dritte übertragen werden. Durch den Transfer aller anderen Randrisiken kann ein Unternehmen mehr Risiken beim Aufbau von Erfolgspotenzialen eingehen, ohne das

Risikodeckungspotenzial des vorhandenen Eigenkapitals zu überziehen. Eine unterlassene Trennung von Kern- und Randrisiken verhindert die systematische Prüfung darüber, welche Risiken das Unternehmen selbst tragen kann, soll oder will.

Fehlende (quantitative) Frühaufklärungssysteme: Frühwarnsysteme sind eine spezielle Art von Informationssystemen. Sie zielen darauf ab, zukünftige Entwicklungen und Ereignisse mit Bedeutung für das Unternehmen vorab zu erkennen. Damit schaffen sie die Möglichkeit, diese Entwicklungen durch geeignete vorbeugende Maßnahmen zu antizipieren. Frühwarnsysteme können operativ-quantitativer Natur, z. B. ökonomische Umsatzprognosesysteme, oder strategischer Natur sein, wie etwa die Balanced Scorecard. Fehlende Frühwarnsysteme haben negative Auswirkungen auf die Zukunftsorientierung des Risikomanagements und letztlich auf die Steuerbarkeit des Unternehmens.

### Phase 5: Risiko-Überwachung

Wirksames Risikomanagement erfordert dessen vollständige Verankerung in den Geschäftsprozessen des Unternehmens sowie die Einbeziehung aller Mitarbeiter bei der Umsetzung. Die sich ständig ändernden Umweltbedingungen wirken auch auf die Risikosituation des Unternehmens ein. Das Risikomanagementsystem hat daher durch organisatorische Regelungen sicherzustellen, dass Risiken frühzeitig identifiziert und regelmäßig bewertet werden. Außerdem sind für ein KonTraG-konformes Risikomanagementsystem die Berichtswege zu Vorstand und Aufsichtsrat respektive Geschäftsführung festzulegen. Die folgenden Fehler sind bei der organisatorischen Gestaltung des Risikomanagementsystems immer wieder zu beobachten:

Fehlende Schwerpunktsetzung und vermeidlicher bürokratischer Aufwand: Auch bei der organisatorischen Gestaltung des Risikomanagementsystems gilt der Grundsatz, dass nur dort größere organisatorische Maßnahmen sinnvoll sind, wo auch bedeutende Risiken behandelt werden sollen. Gestützt auf die Daten der Risikoanalyse muss festgelegt werden, welche Risiken eine so große Bedeutung für das Unternehmen haben, dass Arbeitsanweisungen für eine regelmäßige Risikoüberwachung erforderlich sind. Ein effizientes und funktionsfähiges Risikomanagementsystem beinhaltet im Kontext der fortlaufenden Risikoberichterstattung selten mehr als 15 Einzelrisiken.

Fehlende Verbindung mit bestehenden Organisations- und Berichtssystemen: Risikomanagement wird teilweise als eigenständiges organisatorisches und planerisches System verstanden. So begriffen wird das Risikomanagement auf wenig Akzeptanz im Unternehmen stoßen und nur unnötigen bürokratischen Aufwand auslösen. Richtig ist es, das Risikomanagement mit den vorhandenen Systemen zu vernetzen. Das bedeutet, dass beispielsweise die Informationen aus dem Controlling (etwa unsichere Planannahmen) oder aus dem Qualitätsmanagement (z. B. aus FMEA) genutzt werden.

Mangelhafte Dokumentation im Risikomanagement: Ein nachvollziehbares Risikomanagementsystem benötigt eine ordentliche, für Dritte (z. B. Wirtschaftsprüfer) verständliche Dokumentation. Zudem müssen alle Erkenntnisse des Risikomanagements sinnvoll und möglichst einheitlich aufbereitet, dokumentiert und an die Entscheidungsträger weitergeleitet werden, etwa wenn es Veränderungen bei bestimmten Risiken gibt.

Unklare Aufgabenzuordnung und Fehlen eines Verantwortlichen: Für alle maßgeblichen Risiken, die regelmäßig zu überwachen sind, sollte ein Verantwortlicher eindeutig benannt werden, ein sogenannter „RiskOwner“. Nur so ist gewährleistet, dass das Risiko im gewünschten Umfang betrachtet wird. Zudem muss geklärt sein, welche Stelle die Gesamtverantwortung für das Risikomanagementsystem trägt. Diese muss über ausreichende Kompetenzen sowie Reputation im Unternehmen verfügen, damit seine Aussagen den nötigen Stellenwert erhalten.

Fehlende organisatorische Trennung zwischen Risikomanagement und interner Revision: Spätestens nach der Phase des Aufbaus sollten Risikomanagementsystem und interne Revision



getrennt werden. Nur so wird sichergestellt, dass das Risikomanagement durch eine neutrale Stelle bezüglich seiner Arbeitsweise und seiner Effizienz geprüft werden kann.

Unbefriedigende Einbindung der Mitarbeiter ins Risikomanagement: Nicht selten existiert ein Risikomanagementsystem nur auf dem Papier. Die Mitarbeiter – oft einschließlich der Führungskräfte – engagieren sich nicht für das Risikomanagement und sehen dessen Bedeutung als unwesentlich an. Besonders kritisch ist, wenn Mitarbeiter entweder aus Angst keine betriebsnotwendigen Risiken eingehen wollen, oder umgekehrt keine ausreichende Sorgfalt bei risikobehafteten Aktivitäten zeigen (Defizite in der Risikokultur).

Fehlende Risikopolitik und Limitsysteme: Die Risikopolitik stellt den Teil der Unternehmensstrategie dar, der explizit Aussagen zur Risikobereitschaft und zum Umgang mit Risiken trifft. Sie setzt damit auch die Rahmenbedingungen für den Aufbau des Risikomanagementsystems. Die Risikopolitik hat insbesondere Aussagen zu Entscheidungskriterien zu treffen, die ein Abwägen erlauben von: Rendite und Risiko, der Obergrenze für den Gesamtumfang der Risiken, der Aufteilung der Risiken in Kern- und Randrisiken sowie Limits für einzelne Risiken. Ohne eine fixierte Risikopolitik fehlt der Orientierungsrahmen zum Umgang mit Risiken.

#### KONTAKT

Funk RMCE GmbH  
Hendrik Löffler  
Geschäftsführer  
Valentinskamp 20 • 20354 Hamburg  
fon +49 (0)40 35914-642  
fax +49 (0)40 35914-433  
h.loeffler@rmce.de • www.rmce.de