

# Prüfung des Risikomanagements durch die Interne Revision

Von Thomas Mohnike - Revisionsleiter bei der Stadtwerke Hannover AG und Rolf-Dieter Epkenhans -  
Personalrevisor bei der Stadtwerke Hannover AG

## Einleitung

Der Gesetzgeber hat auf die Schwächen im System der Unternehmenskontrolle reagiert und sah sich gezwungen, die vorhandenen Überwachungs- und Kontrollstrukturen per Gesetz einer Neuordnung zu unterziehen. Daher wurde das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (*KonTraG*) formuliert, das am 01. Mai 1998 in Kraft getreten ist. Hiermit wurde auch die Einrichtung eines *Risikofrüherkennungssystems* als Organisationspflicht des Vorstandes fixiert (§ 91 Absatz 2 Aktiengesetz).

Das *KonTraG* sieht vor, dass "der Vorstand geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten hat, damit der Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden."

Danach sind die Unternehmen nunmehr ausdrücklich verpflichtet, für ein aktives Risikomanagement und eine angemessene Interne Revision zu sorgen.

## Veränderte Rolle der Internen Revision im Unternehmen

Bis zum Jahr 2000 war die Überprüfung des *Risikomanagementsystems* durch die Interne Revision oder andere unabhängige Überwachungsinstanzen in der Regel noch nicht erfolgt, häufig noch nicht einmal geplant.

Zwischenzeitlich mussten sich aber durch zunehmende Geschwindigkeit, Kostendruck und neue Risiken nicht nur die Unternehmen verändern, sondern insbesondere auch die Interne Revision. Künftig wird sie sich nicht mehr als "Unternehmenspolizei" vergangenheitsorientiert und isoliert von Unternehmenszielen darstellen können, sondern zur Überwachung der Geschäftsrisiken beitragen, Prozesse optimieren und kundenorientiert denken und arbeiten.

Die Interne Revision prüft im Auftrag der Unternehmensleitung ganz allgemein die Ordnungsmäßigkeit, Rechtmäßigkeit, Zweckmäßigkeit und Wirtschaftlichkeit der übrigen Organisationseinheiten sowie die Abwicklung der Prozesse im Unternehmen.



## Gesetzliche Grundlagen des Risikomanagements

Nach § 91 AktG ist der Vorstand zur Einrichtung eines Risikomanagement- und -überwachungssystems verpflichtet. Nach § 317 HGB ist bei einer Aktiengesellschaft, die Aktien mit amtlicher Notierung herausgegeben hat, außerdem im Rahmen der Abschlussprüfung zu beurteilen, ob der Vorstand die ihm nach § 91 Abs. 2 des AktG obliegenden Maßnahmen in einer geeigneten Form getroffen hat und das danach einzurichtende Überwachungssystem seine Aufgaben erfüllen kann.

### Gesetzliche Grundlagen des Risikomanagements

Anforderungen gemäß IDW PS 340\*



\* IDW PS 340: Prüfungsstandard (PS) des Instituts der Wirtschaftsprüfer (IDW) für die Prüfung des Risikomanagementsystems im Rahmen der Jahresabschlussprüfung.

Der Deutsche Rechnungslegungsstandard Nr. 5 regelt die Grundsätze der Risikoberichterstattung für alle Mutterunternehmen, die gemäß § 315 Abs. 1 2 Hs. HGB über die Risiken der künftigen Entwicklung im Konzernlagebericht zu berichten haben und empfiehlt eine entsprechende Anwendung im Lagebericht gemäß § 289 Abs. 1 2 Hs. HGB. Der Standard ist auch anzuwenden auf die Rechnungslegung des § 292a HGB. Ziel der Risikoberichterstattung nach diesem Standard ist es, den Adressaten des Konzernlageberichts entscheidungsrelevante und verlässliche Informationen zur Verfügung zu stellen, die es ihnen ermöglichen, sich ein zutreffendes Bild über die Risiken der künftigen Entwicklung des Konzerns zu machen.

Berichtspflichtig sind alle Risiken, die die Entscheidungen der Adressaten des Konzernlageberichts beeinflussen könnten. Schwerpunkt der Berichterstattung sollten somit die mit den spezifischen Gegebenheiten des Konzerns und seiner Geschäftstätigkeit verbundenen Risiken bilden.

Auch für nicht unter die Gesetzgebung fallende Unternehmen ergibt sich dennoch die Notwendigkeit, sich intensiv mit dem Thema auseinander zu setzen und ein funktionierendes Risikomanagementsystem auszugestalten - zum einen durch die Ausstrahlungswirkung der gesetzlichen Entwicklungen auf den Pflichtenrahmen der Geschäftsführer und ggf. Aufsichtsräte anderer Gesellschaftsformen (Sorgfaltspflicht, Möglichkeit der Exkulpation), vor allem aber aus originär betriebswirtschaftlichen Gründen (z.B. als integrierter Bestandteil der Unternehmensführung und als Kriterium für das Rating).

## Risiken aus Unternehmenssicht

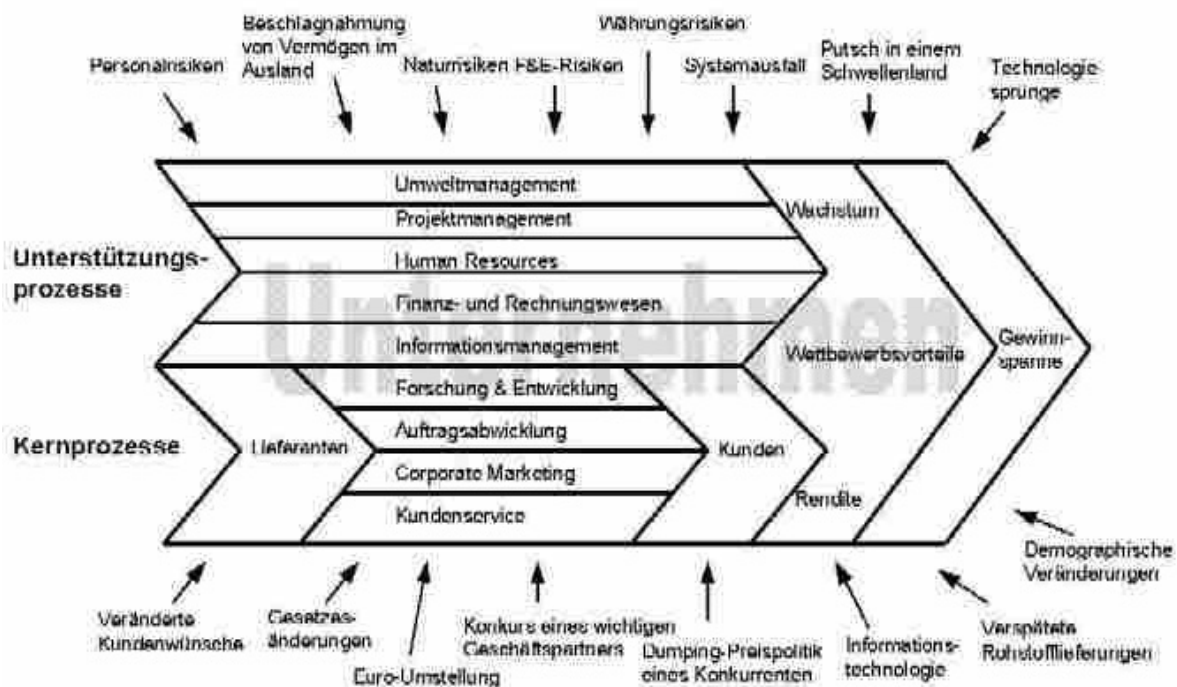
Jede unternehmerische Entscheidung ist mit Risiken verbunden, da die Auswirkungen dieser Entscheidungen i.d.R. nicht vorhergesagt werden können. Risiken werden jedoch in Kauf genommen, um Chancen wahrzunehmen und Erfolge zu erzielen - es gilt der Grundsatz: Keine Chance ohne Risiko. Für eine erfolgs- und wertorientierte Unternehmensführung ist somit eine zielorientierte, bewusste und systematische Auseinandersetzung mit Risiken und Chancen erforderlich. Daher ist es notwendig, dass in jedem Unternehmen organisatorische Regelungen zur Erkennung wesentlicher Risiken existieren.

Für einen sinnvollen und effektiven Umgang mit Risiken ist es unumgänglich, zunächst die Risikolage des Unternehmens einzuschätzen und zeitnah abbilden zu können. Unternehmen - unabhängig von ihrer Branche und Größe - sind im Rahmen ihrer Geschäftstätigkeit einer unbegrenzten Zahl von Risiken ausgesetzt.

Bei der Beurteilung der (Gesamt-) Risikolage eines Unternehmens ist zu beachten, dass das aggregierte Unternehmensrisiko aufgrund möglicher kompensatorischer bzw. kumulativer Effekte der Einzelrisiken untereinander nicht unbedingt der Summe der Einzelrisiken entspricht.

Im Zusammenhang mit Risikomanagement denkt man zunächst an den Finanzbereich des Unternehmens und die Risiken in Verbindung mit dem Einsatz von derivativen Finanzinstrumenten. Vorhandene Risikomanagementsysteme beschränken sich meist nur auf diesen Bereich. Die folgende Abbildung zeigt jedoch, wie viel umfangreicher und vielfältiger die Risikolandschaft ist, die es bei der Einrichtung eines Risikomanagementsystems zu berücksichtigen gilt.

### Risikolandschaft



Die angeführten Risiken können sich sehr kurzfristig auswirken (z.B. Systemausfälle, die -kurzzeitig- zu Handlungsunfähigkeit führen), sie können aber auch das Ergebnis langsamer und schleichender Prozesse sein (z.B. die versäumte Anpassung der eigenen Produkte und Dienstleistungen an sich ändernde Kundenwünsche).

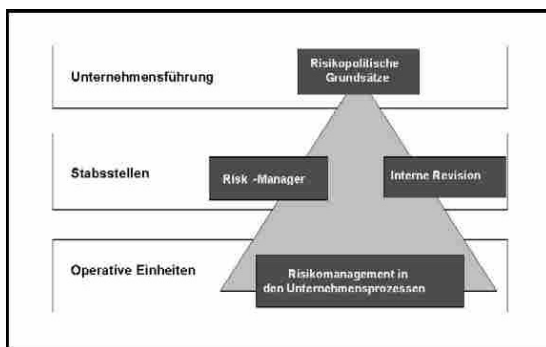
Gerade die Risiken aus strategischen Entscheidungen sind diejenigen, die hinsichtlich einer möglichen Bestandsgefährdung eine besondere Beachtung verdienen.

## Organisation des Risikomanagementsystems

Das Risikomanagementsystem bzw. das Risikofrüherkennungssystem setzt sich aus folgenden Elementen zusammen:

- ❑ *Internes Überwachungssystem* mit organisatorischen Sicherungsmaßnahmen, internen Kontrollen und *Interner Revision*.
- ❑ *Controlling* (als Grundlage für eine zielgerichtete Steuerung des Unternehmens) mit den Subsystemen Planungssystem, Informationssystem, Kontrollsystem und Steuerungssystem einschließlich Dokumentationssystem und Reportingsystem.
- ❑ *Risikomanagementsystem* im engeren Sinne mit Risikostrategie, Risikomanagementprozess und Risiko-Controlling.

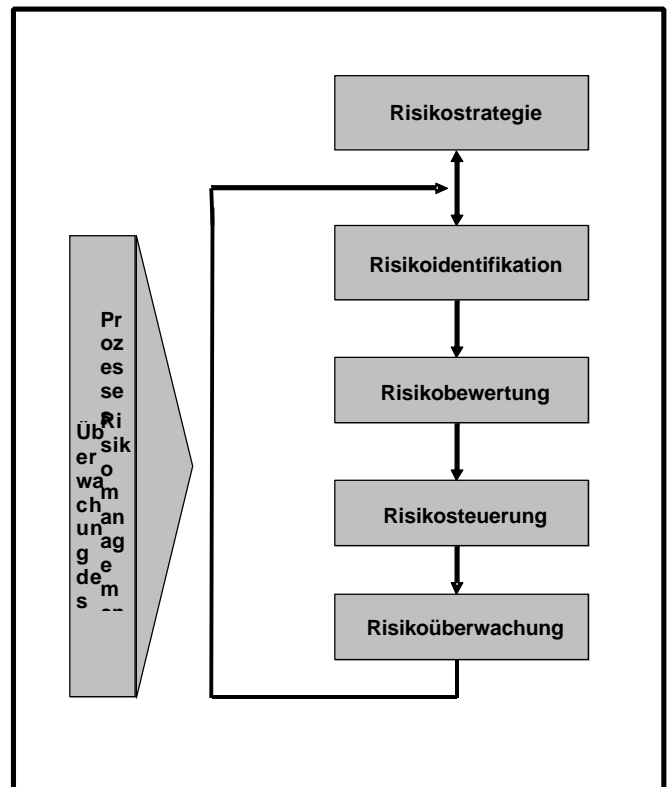
## Risikomanagement - Organisation



## Prozess des Risikomanagements

Der Risikomanagementprozess ist das Kernstück des Risikomanagements und stellt dessen Integration in die Abläufe des Unternehmens dar. Der Prozess ist nicht als einmalig zu verstehen. Es handelt sich vielmehr um einen kontinuierlichen Kreislauf, der alle Aktivitäten zum systematischen Umgang mit Risiken umfasst.

Der Prozess beginnt mit der möglichst vollständigen Erfassung aller relevanten Risiken (Risikoidentifikation). Nach der Ermittlung des erforderlichen Handlungs- und Steuerungsbedarfs (Risikobeurteilung) folgt die aktive Beeinflussung aller wesentlichen Risiken (Risikosteuerung). Im nächsten Schritt wird die Durchführung der Maßnahmen zur Risikosteuerung kontrolliert (Risikoüberwachung). Unternehmensgrundsätze zum Risikomanagement sind als risikopolitische Grundsätze zu dokumentieren. Werden während des Risikomanagementprozesses Veränderungen des Unternehmensumfeldes bzw. Veränderungen der das Unternehmen betreffenden Risiken festgestellt, ist evtl. eine Anpassung der Risikostrategie notwendig. Die Überwachung des gesamten Risikomanagementprozesses erfolgt prozessunabhängig, ggf. durch die interne Revision.



## **Interne Revision im Risikomanagement**

Da die Gesetzesbegründung *Risikomanagement* und *Interne Revision* nebeneinander stellt, aber nicht die Beziehung zueinander formuliert, kann weder aus dem Gesetz noch aus der Gesetzesbegründung unmittelbar abgeleitet werden, dass die *Interne Revision* das *Risikomanagement* grundsätzlich prüfen muss. Es bleibt dem Vorstand im Rahmen seiner allgemeinen Verantwortung entsprechend § 76 AktG überlassen, in welcher Weise er absichert, dass das *Risikomanagement* seine Aufgabe erfüllt.

Es ist davon auszugehen, dass zumindest in Großunternehmen die notwendige Überwachung des Risikomanagementsystems ohne eine leistungsfähige Revision nicht sichergestellt werden kann und der Internen Revision aufgrund ihrer allgemeinen Aufgabenstellung sowie ihrer neutralen Position auch die unternehmensinterne Überwachung der Funktionsfähigkeit der Risikomanagementsysteme zu übertragen ist.

Sollte aufgrund der Größe u/o der Struktur eines Unternehmens keine interne Revisionsfunktion vorhanden sein, hat die Geschäftsleitung in geeigneter Weise die Prüfung des Risikomanagements sicherzustellen.

Die *Interne Revision* kann wie bisher schon bei der Einführung neuer Systeme bereits bei der Konzeption und Einführung des Risikomanagementsystems beratend tätig sein. Die laufende Verantwortung für das Risikomanagement kann aber wegen des bestehenden Interessenkonfliktes nicht der Internen Revision übertragen werden.

Die Interne Revision bewertet das Risikomanagement, unterstützt das Unternehmen bei der Identifizierung und Bewertung wesentlicher Risikopotentiale und leistet Beiträge zur Verbesserung der Risiko- und Kontrollsysteme. Überwachung, Qualität und Effizienz des Risikomanagements gehören in diesem Zusammenhang untrennbar zusammen. Dabei ist jedoch zu beachten, dass ihre Möglichkeiten von Art und Umfang ihres Auftrags durch die Geschäftsleitung bzw. den Aufsichtsrat begrenzt sind. Bestimmte Überwachungsaufgaben im strategischen Bereich können letztlich nur durch den Aufsichtsrat wahrgenommen werden, während im operativen Bereich insbesondere die Unternehmensleitung gefordert ist.

Ausgangspunkt der Prüfung des Risikomanagementsystems ist die *Risikomanagementstrategie*. Hierbei ist insbesondere sicherzustellen, dass das Risikomanagement von der Unternehmensleitung als Teil der *Corporate Governance* gesehen wird und ein entsprechender Beschluss der Unternehmensleitung hinsichtlich der Einrichtung und des laufenden Erhaltes des Risikomanagementsystems existiert. Die Revision hat festzustellen, ob

- ⇒ ein fundiertes, von der Unternehmensleitung getragenes und dokumentiertes Risikomanagementsystem existiert.
- ⇒ der Risikomanagementprozess umfassend und kontinuierlich durchgeführt wird und die Ergebnisse in geeigneter Weise dokumentiert und kommuniziert werden.
- ⇒ die festgelegten Maßnahmen tatsächlich umgesetzt wurden.

Darüber hinaus ist die Risikoidentifikation, die Risikobewertung und die Zweckmäßigkeit der Maßnahmen inhaltlich zu beurteilen. Intensität und Häufigkeit der Prüfungen sind u.a. in Abhängigkeit von der Komplexität der Wertschöpfung, Unternehmensgröße und Dynamik der Unternehmensentwicklung festzulegen.

## **Prüfung der Konzeption und Organisation des Risikomanagements**

Die Interne Revision hat zu prüfen, ob eine klare Konzeptbeschreibung und eindeutige Regelungen hinsichtlich Zuständigkeiten und Dokumentation für alle Unternehmensbereiche vorliegen.

Im Einzelnen sind folgende Punkte zu untersuchen:

- Existiert ein Risikomanager (u/o eine andere Stelle oder Funktion im Unternehmen), der (die) für die Koordination und Unterstützung hinsichtlich des Risikomanagements verantwortlich ist ?
- Gibt es eine Organisations-Richtlinie, ein Handbuch oder Arbeitsanweisungen, in denen die organisatorischen Regelungen und Maßnahmen des Risikomanagementsystems einschließlich der Implementierung und der Durchführung geregelt sind ?
- Ist im Unternehmen geregelt, dass die Verantwortung für ein funktionierendes Risikomanagementsystem bei den Geschäfts- / Organisationseinheiten liegt ?
- Wurden adäquate Schwellenwerte hinsichtlich der Risikoanordnung zu verantwortlichen Bereichen definiert ?
- Wird die Risikolage des Unternehmens im Rahmen einer vorgegebenen Systematik regelmäßig mindestens jährlich auf Aktualität geprüft ?
- Ist sichergestellt, dass bei plötzlichen unvorhergesehenen Veränderungen in der Risikolandschaft des Unternehmens eine Aktualisierung der Risiken hinsichtlich Organisation, Verantwortlichkeit und Dokumentation in angemessenen Zeitabständen erfolgt ?
- Werden Risiken mit gleicher Ursache kumuliert ?

### Risikoidentifikation

Die Risikoidentifikation stellt den ersten Schritt eines Risikomanagementprozesses dar. Dieser Phase obliegt die vom KonTraG geforderte systematische Identifikation aller auf das Unternehmen einwirkenden Risiken - insbesondere der bestandsgefährdenden Risiken. Dabei sind neben den Kerngeschäftsprozessen (z.B. Forschung und Entwicklung, Einkauf, Produktion, Marketing und Vertrieb, Kundendienst) auch die Unterstützungsprozesse (z.B. Finanzen, Personal, Informationstechnologie, Logistik) einzubeziehen.

#### Risikoidentifikation Bsp.: Risikoinventar

Risiko	Risikofeld	
Neue Wettbewerber	Markenlären	Marktposition und Wettbewerbsstärke
Abhängigkeit von XYZ AG	Wertschöpfungskette	Akquisition
Haftpflichtschaden bei Kunde Z	Rechtliche Risiken	Produkt Haftung
Kalkulationsfehler	Wertschöpfungskette	Angebote, Kalkulation und Preissetzung
Abstandsverschmäkung	Markenlären	Abstimmungen und Abstanzfolge
Anstieg des Tariflohn	Spezielle Risiken	Personalwirtschaft und Personalmanagement
Anzahl der ABC-Anlage	Spezielle Risiken	Business-Continuity-Plan
Wachstumsbedingter EE-Mangel	Strategische Risiken	Finanz- und Kostenstruktur
Übersicht der Muster AG	Finanzmarkt Risiken	Debtengängen, Unternehmensläufe
Reifende Kompetenzen	Strategische Risiken	Kernkompetenzen und kritische Erfolgsfaktoren
Motivationsprobleme im Vertrieb	Risiken aus Corporate Governance	Betriebsklima und Motivation
Sitzfall im Werk C	Spezielle Risiken	Arbeitsicherheit

Die Identifikation von Risiken wird im Idealfall von den Prozessverantwortlichen im Unternehmen durchgeführt. Diese sind in die operativen Geschäftsprozesse eingebunden und sollten in der Lage sein, entsprechende Frühwarnindikatoren zu definieren und danach auch korrekt zu deuten.

Als Ergebnis der Risikoidentifikation werden die identifizierten Risiken bzw. Risikobereiche in einem *Risikokatalog* dokumentiert, der als Grundlage für die anschließende Risikoanalyse dient. Bei der Dokumentation sollten die Unternehmensstrukturen und -prozesse berücksichtigt und die Risiken soweit wie möglich zu einem Risikoprofil zusammengefasst werden.

Bei der Prüfung der Risikoidentifikation ist im Wesentlichen auf die verwendete Methodik, die Vollständigkeit, die zeitnahe Erfassung und die regelmäßige Aktualisierung zu achten.

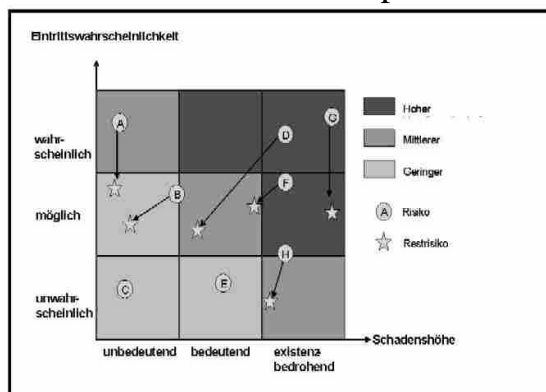
## Risikoanalyse

Zur Ableitung von angemessenen Steuerungsmaßnahmen müssen die identifizierten Risiken weiter untersucht und bewertet werden. Ziel der Risikoanalyse ist die *qualitative Beurteilung* bzw. *quantitative Messung* der Risiken, um das Risikoportfolio des Unternehmens abzubilden. Dabei sollten die Wirkungszusammenhänge einzelner Risiken berücksichtigt werden.

Für die Risikoanalyse empfiehlt es sich, zunächst eine grobe Beurteilung des originären Risikos, d.h. der Risikosituation vor Kontrollen und Risikomanagement, durchzuführen.

Die Ergebnisse dieser ersten Analyse können ergänzend in den *Risikokatalog* aufgenommen werden. Dieser sollte als Ergebnis der Risikoidentifikation bereits die *erkannten Risiken* einschließlich einer kurzen Beschreibung enthalten. Ergänzt wird er nun um weitergehende Erläuterungen zur Risiko-ursache, die Häufigkeit des Auftretens (Eintrittswahrscheinlichkeit) sowie eine Bewertung der Schadenhöhe. Schließlich werden *Risikoverantwortliche* festgelegt sowie notwendige *Maßnahmen* u/o *Empfehlungen* festgehalten.

## Risikoportfolio



Als Grundlage für die Risikosteuerung sind die Ergebnisse der Risikoanalyse kontinuierlich zu erfassen und durch eine angemessene *Berichterstattung* den Entscheidungsträgern zeitnah zur Verfügung zu stellen. Dabei sollte im Zweifel der Grundsatz *Aktualität vor Genauigkeit* gelten. Soweit wie möglich sollten die Risiken quantifiziert werden. Dies kann beispielsweise in Form von Risikomaßzahlen, z.B. dem "Value-at-Risk", d.h. dem mit mathematisch-statistischen Verfahren bewerteten Verlustpotential aus einem Geschäft oder einer Aktivität, erfolgen.

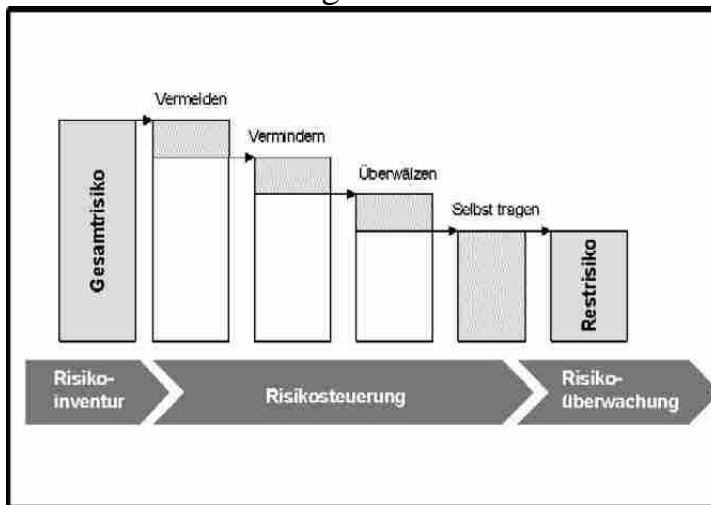
Während sich die finanziellen Risiken eines Unternehmens weitgehend exakt quantifizieren lassen, gilt dies kaum für die Gesamtheit der Risiken, denen das Unternehmen ausgesetzt ist. Insbesondere die Quantifizierung von Risiken, die sich aus den strategischen Entscheidungen der Unternehmensleitung ergeben, ist nur begrenzt möglich. In der Regel ist sie im hohen Maße von der subjektiven Einschätzung der Entscheidungsträger abhängig.

Die Interne Revision hat im Zusammenhang mit der Risikoanalyse und -bewertung insbesondere zu prüfen, welche Methoden zur Quantifizierung und Klassifizierung der Risiken angewandt werden, wie die Bestandsgefährdung bestimmt wird und ob Abhängigkeiten und kumulative Effekte festgestellt werden.

## Risikosteuerung

Gegenstand der Risikosteuerung ist die *aktive Beeinflussung* der im Rahmen von Risikoidentifikation und Risikoanalyse ermittelten *Risikopositionen*. Sie muss in Einklang mit den Unternehmenszielen und den daraus abgeleiteten Zielen des Risikomanagements stehen. Steuerungsmaßnahmen zielen dabei auf eine *gezielte Verringerung der Eintrittswahrscheinlichkeit* (z.B. durch Kontrollen oder andere Präventivmaßnahmen) oder aber eine Begrenzung der Auswirkungen von Risiken (z.B. durch Versicherungen). Sie müssen dazu führen, dass für das Unternehmen nicht akzeptable Risiken vermieden und nicht vermeidbare Risiken auf ein akzeptables Maß reduziert werden können. Hierzu sind die Einzelrisiken gemäß der für ihre Risikokategorie festgelegten Risikostrategien zu steuern. Dies setzt allerdings voraus, dass die Entscheidungsträger kontinuierlich über ihre Risikosituation bzw. ihr Risikoportfolio unterrichtet sind.

### Steuerungsmaßnahmen



Wesentliche Fragestellungen bei der Prüfung der Risikosteuerung sind:

- Welche Frühwarnindikatoren mit welchen quantitativen und qualitativen Limits / Schwellenwerte gibt es ?
- Welche Maßnahmen existieren und sind Maßnahmenverantwortliche benannt ?
- Werden die Maßnahmen umgesetzt, kommuniziert und sind sie wirksam ?

## Risikoüberwachung

In der letzten Phase des Prozesses soll sichergestellt werden, dass durch die Risikoüberwachung die Risikolage des Unternehmens jederzeit der angestrebten Risikosituation entspricht. Alle Risikopotentiale und die Wirksamkeit der Maßnahmendurchführung werden kontinuierlich überwacht. Es soll so festgestellt werden, ob die Maßnahmen zur Risikobewältigung optimal eingesetzt wurden. Aufgrund der Veränderung einzelner Risikopositionen ist zu überprüfen, ob die jeweilige risikobewältigende Maßnahme angepasst werden muss.

Die Aufgabe des Risikocontrollings im Rahmen der Überwachung besteht in der optimalen Koordination der Prozessphasen, insbesondere der Identifikation und Beurteilung. Die Koordination erfolgt, indem die Schritte und Elemente des Risikomanagements in zeitlicher und sachlicher Hinsicht aufeinander abgestimmt werden. Dadurch soll sichergestellt werden, dass ein permanenter Überwachungsprozess entsteht, d.h. erkannte Risiken ständig überwacht und neu auftretende Risiken sofort aufgenommen werden. Außerdem überwacht das Risikocontrolling die Einhaltung der Grenzwerte und Limite und analysiert Risikokennzahlen auf der Basis eines Soll-/Ist-Vergleichs. Es

versorgt dann das Management mit Informationen über die gewonnenen Ergebnisse. Organisatorisch ist das Risikocontrolling beim Controlling als zentrale und koordinierende Funktion für Planung, Steuerung und Kontrolle anzusiedeln. Solch eine prozessunabhängige Controllingabteilung existiert i.d.R. im Unternehmen bereits.

Die Überwachung des Risikomanagementsystems bezieht sich dagegen auf die Beurteilung der Effektivität der gesamten Organisation sowie auf die Angemessenheit der Berichterstattung. Diese Überwachung soll die Funktionsfähigkeit des Systems aufrechterhalten. Sie kann durch prozessunabhängige Organe (Interne Revision, Abschlussprüfer) wahrgenommen werden.

### **Risikoorientierte Prüfungsplanung**

Der Gesamtprüfungsplan enthält alle Betriebs- und Geschäftsabläufe, welche Prüfungsfelder im Sinne der Revision darstellen können. Dieser Plan wird auch als Prüfungslandkarte bezeichnet. Jedoch können aufgrund der steigenden Komplexität der Prozesse nicht mehr alle Felder geprüft werden - es muss eine Auswahl getroffen werden. Von daher führt die Interne Revision eine Risikoanalyse aller Prüfungsfelder durch, um das Prüfungsprogramm für die nächste Periode zu erstellen. Dazu werden die potentiellen Bereiche anhand von Risikokriterien beurteilt. Solche Kriterien können beispielsweise lauten:

- Zeitabstand zur letzten Prüfung
- Ergebnis der letzten Prüfung
- Organisationsänderungen
- Personalveränderungen
- Relevanz für die Bilanz und Gewinn- und Verlustrechnung
- ...

Weitere Faktoren können die Ergebnisse aus dem Risikomanagement sein:

- Identifizierte Risiken
- Entwicklung in der Zukunft
- Eintrittswahrscheinlichkeit und Schadenshöhe.

Die von allen Revisionsmitarbeitern gemeinsam erarbeiteten Prüfungskriterien werden mit einer Gewichtung und mit einer Punktbewertung versehen.

Aus dem risikoorientierten Gesamtprüfprogramm wird das Jahresprüfprogramm abgeleitet und mit den zur Verfügung stehenden Kapazitäten unter Berücksichtigung der Qualifikationen abgeglichen. Natürlich sind jährlich fixierte Prüfungen (z.B. Finanz- und Energiehandel) in den Jahresprüfplan aufzunehmen. Dieser Jahresprüfplan wird durch den Vorstand genehmigt. Daraus abgeleitet werden die individuellen Prüfungspläne der jeweiligen Revisoren. Die Berichterstattung der Internen Revision erfolgt durch Einzel-, Quartals- und Jahresberichte an den Vorstand.

### **Schlussbetrachtung**

Neue Aufgaben und neue Herausforderungen gehen mit dem Management der Risiken einher. Immer dynamischer werdende Märkte machen einen systematischen Umgang mit den Risiken des Unternehmens notwendig. Das aktive Identifizieren, Gestalten und Steuern der Risiken ist ein wichtiges Mittel zur Sicherstellung der Existenz und des zukünftigen Erfolges. Das Risikomanagementsystem schafft die Voraussetzungen, Risiken frühzeitig zu erkennen, zu bewerten und zu steuern und kann zudem bei richtiger Ausgestaltung als nachhaltiges Chancenmanagement verstanden werden. Im Kontext der Unternehmensüberwachung fällt der Internen Revision eine wichtige Rolle zu. Die Zielsetzungen des Risikomanagements und der Internen Revision stimmen weitgehend überein. Beide unterstützen die Unternehmensleitung und -bereiche bei der Erreichung der Ziele sowie die dezentralen Führungsebenen bei der eigenverantwortlichen Selbststeuerung. Weiterhin sollen durch Risikomanagement und Interne Revision Vermögensverluste vermieden sowie die Vorschriften des KonTraG erfüllt werden.

Insgesamt ist festzuhalten, dass der Erfolg von Risikomanagementprojekten - nämlich die Steigerung des Unternehmenswertes durch die Verbesserung der Risikoposition des Unternehmens - durch eine Reihe häufig beobachteter Fehlerquellen bedroht ist.

Für sämtliche Phasen eines Risikomanagementprojektes bestehen schwerwiegende methodische Gefahren. Diese können dazu führen, dass Risikomanagementprojekte in der Praxis trotz massiven Einsatzes an Zeit- und Mitarbeiterressourcen keinen befriedigenden Erfolg zeigen und oft die in sie gesetzten hohen Erwartungen nicht erfüllen. Gründe hierfür können z. B. sein, dass der Bezug zur Unternehmensstrategie und zu den Erfolgsfaktoren fehlt, dass Fachexperten bei der Risikoanalyse und einheitliche Risikobewertungseinheiten fehlen, dass das Risikomanagementsystem mangelhaft dokumentiert ist und dass keine Trennung von Risikomanagement und Interner Revision besteht.

Mit besonderem Dank an Herrn Christoph Wildensee. - [www.wildensee.de/veroeff.htm](http://www.wildensee.de/veroeff.htm)