

# Risikomanagement – Warum und Wofür?

Nicht nur für Aktiengesellschaften fordert **das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)** ein Überwachungssystem zur Früherkennung bestandsgefährdender Risiken einzurichten (§ 91 II AktG); Risikomanagement ist ebenso Bestandteil der Sorgfaltspflichten eines jeden GmbH-Geschäftsführers (§ 43 I GmbHG) oder GmbH & Co. KG.

Auch sie müssen wie die Vorstände einer Aktiengesellschaft im Fall einer Unternehmenskrise beweisen, dass sie sich pflichtgemäß verhalten und Maßnahmen zur Früherkennung und Abwehr der Risiken getroffen haben. Der Corporate Governance Kodex nimmt diesbezüglich auch die Aufsichtsräte in die Pflicht.

In vielen der mittelständischen Unternehmen, für die es aufgrund ihrer meist sehr niedrigen Eigenkapitalausstattung besonders wichtig ist Unternehmenskrisen zu vermeiden, wird diesem Tatbestand bisher oftmals zu wenig Bedeutung beigemessen.

Die praktische Umsetzung des Risikomanagements darf sich nicht auf die Einhaltung gesetzlicher Vorschriften in Form einer bloßen Risikobuchhaltung beschränken. Vielmehr sind mit einem Risikomanagement auch die Chancen zu erkennen, die durch ein systematisches Management der Risiken die Grundlage einer wert- und erfolgsorientierten Unternehmenssteuerung schaffen und zu Kosten- und Wettbewerbsvorteilen führen.

Der Einsatz immer neuer Informationstechnologien lässt Geschäftsprozesse effizienter werden, führt aber gleichzeitig zu einer größeren Abhängigkeit. Die zunehmende Komplexität automatisierter Prozesse stellt die Unternehmen vor eine sich ständig wandelnde Risikolage. Es ist davon auszugehen, dass sich diese Entwicklung fortsetzen wird und die operativen Risiken in der Zukunft noch stärker steigen. Deshalb müssen geeignete Instrumente zur Risikosteuerung in einem Unternehmen vorhanden sein.

- Fast ausnahmslos wird bis heute die Risikobetrachtung auf den Finanzbereich beschränkt. Häufig sind es aber gerade die Risiken, die im operativen Bereich des Unternehmens ihren Ursprung haben und vernachlässigt werden.  
In Untersuchungen ist nachgewiesen, dass die operativen Risiken durchschnittlich etwa 10% der Gesamtkosten des Unternehmens ausmachen und die daraus resultierenden Verluste mehr oder weniger „unbemerkt“ im unternehmerischen Zahlenwerk „verschwinden“.
- Durch die zunehmende globale Ausrichtung der Unternehmen ist zugleich der weltweite Wettbewerb härter und der Druck auf die Unternehmensmargen größer geworden. Der Kostenspielraum in den Unternehmen hat sich damit erheblich verringert, das Risiko jedoch vergrößert.
- Bedingt durch Basel II steigen die Anforderungen an die Kreditinstitute fundierte Risikoanalysen ihrer Kreditnehmer zu erstellen. Diese richtet sich nicht mehr nur auf die vergangenheitsorientierte Ertrags- und Finanzlage in Form einer Kreditwürdigkeitsprüfung allein, sondern eine zukunftsorientierte Beurteilung der Risiken des Unternehmens rückt in den Vordergrund (§ 18 Kreditwesengesetz KWG). Damit wird die Kreditgewährung in Abhängigkeit eines ausreichend vorhandenen Risikomanagements gebracht. Die Frage wird immer öfter lauten: „Besteht in Ihrem Unternehmen ein angemessenes Risikomanagement und Risiko-Controlling?“

## Fazit

Risikomanagement ist gleichzeitig Chancenmanagement.

# Einsatz von Risikomanagement-Systemen in der Praxis

Schätzungen zur Folge haben erst etwa 35% der im DAX-100 gelisteten Unternehmen ein angemessen funktionierendes Risikomanagement implementiert, während vor allem bei kleineren und mittelgroßen Unternehmen meist vergeblich danach gesucht wird. (Quelle)

Warum aber ist die Einführung eines Risikomanagementsystems in vielen mittelständischen Unternehmen noch immer nicht erfolgt?

- Unternehmen  
Oftmals liegt dieses Versäumnis in der Management-Struktur der Unternehmen begründet. Vermeintlich kennt die Geschäftsleitung jegliche Risiken und hat diese auch angeblich „im Griff“ – schließlich blickt „man“ auf jahrelange Erfahrungen zurück. Vor allem in den von Inhabern selbst geführten Unternehmen ist dieser Standpunkt weit verbreitet. Hinzu kommt, dass mit der Einführung eines Risikomanagements der Unternehmer nicht kalkulierbare Kosten befürchtet. Dabei wird jedoch übersehen, dass erst die Einführung eines Risikomanagementsystems dazu beiträgt Kosten zu sparen, Schadensfälle zu minimieren und darüber hinaus Chancenpotentiale für das Unternehmen zu erkennen. Der Unternehmer wird in die Lage versetzt seine Risiken zu steuern und Chancen zu nutzen.
- Steuerberater/Wirtschaftsprüfer  
Der Wirtschaftsprüfer kennt das Unternehmen seit Jahren und seitens der Unternehmen wird das umgesetzt, was von ihm empfohlen bzw. verlangt wird. Konkrete Anforderungen werden vom Wirtschaftsprüfer nur gestellt, insoweit sie im Rahmen der Jahresabschlussprüfung zwingend sind.  
Steuerberater zählen mit zu den engsten Vertrauten der mittelständischen Unternehmen. Sie kennen das Unternehmen, dessen Struktur und Entwicklung i.d.R. über mehrere Jahre. Die Steuerberater werden somit häufig Ansprechpartner für die kreditgebenden Banken ihrer Mandanten.

Die Wirtschaftsprüfer und Steuerberater – beginnen erst langsam den Bedarf ihrer Mandanten im Bereich Risikomanagement nicht nur für den Finanzbereich zu erkennen, sondern auch die Notwendigkeit der Steuerung operationaler Risiken zu berücksichtigen. Allerdings stehen viele von ihnen immer wieder vor den Fragen: „Wie setze ich ein angemessenes ganzheitliches Risikomanagement bei meinem Klienten individuell in die Praxis um?“

„Betreue ich meinen Mandanten so, dass er durch ein Risikomanagement auch den zukünftigen Anforderungen an Unternehmensführung oder Rating gewachsen ist?“

- Die Kreditinstitute.  
Die Kreditinstitute müssen sich der Herausforderung des Basel II Accords stellen. Gleichzeitig bemühen sie sich ihren Kunden die Folgen des daraus resultierenden Ratings näher zu bringen. Bei ihrer Kreditgewährung sind sie bereits überaus kritisch - jedoch für ihr Klientel haben sie momentan noch keine klare Antwort auf die Frage: „Was muss in meinem Unternehmen praktisch dafür getan werden?“
- Risikomanagement und Basel II (Rating)  
Vielfach wird nicht erkannt, dass das Risikomanagement überhaupt die Ausgangsbasis sowie wesentliche Informationsquelle für ein Rating ist. Erst die Existenz eines ganzheitlich praktizierten Risikomanagements im Unternehmen ist in der Lage die Ratinganforderungen zu erfüllen
- Seminare.  
Kein anderes Thema wird zur Zeit in Seminaren mehr angeboten als „Risikomanagement“ und „Basel II“. Die meisten Seminare sind darauf ausgerichtet, das notwendige Bewusstsein bei den Teilnehmern für diese Themenkreise zu wecken, zeigen aber die Thematik nur allgemein mit wenigen praktischen Ansätzen auf.  
So bleiben die individuellen Fragen: „Wie setze ich ein angemessenes Risikomanagement in „meinem“ Unternehmen praxisgerecht um?“ meist unbeantwortet.

## Fazit

Trotz Bemühungen bleibt in vielen Unternehmen die Einführung eines ganzheitlichen Risikomanagements vor der Frage des „WIE“ stehen.

# Fünf Schritte zur praktischen Implementierung eines Risikomanagementsystems

Die Einführung eines Risikomanagements im Unternehmen bedarf aufgrund des zunächst abstrakt wirkenden Charakters unbedingt der Unterstützung sowie der Verantwortung der Geschäftsleitung und verlangt ein strukturiertes Vorgehen, um im Ergebnis und damit auch künftig für das Unternehmen erfolgreich und von Nutzen zu sein.

Die Einführung wird im Rahmen eines eigenständig geführten Projektes vorgenommen, um auch die notwendige Signalwirkung, Bedeutung und Akzeptanz für das gesamte Unternehmen zu vermitteln.

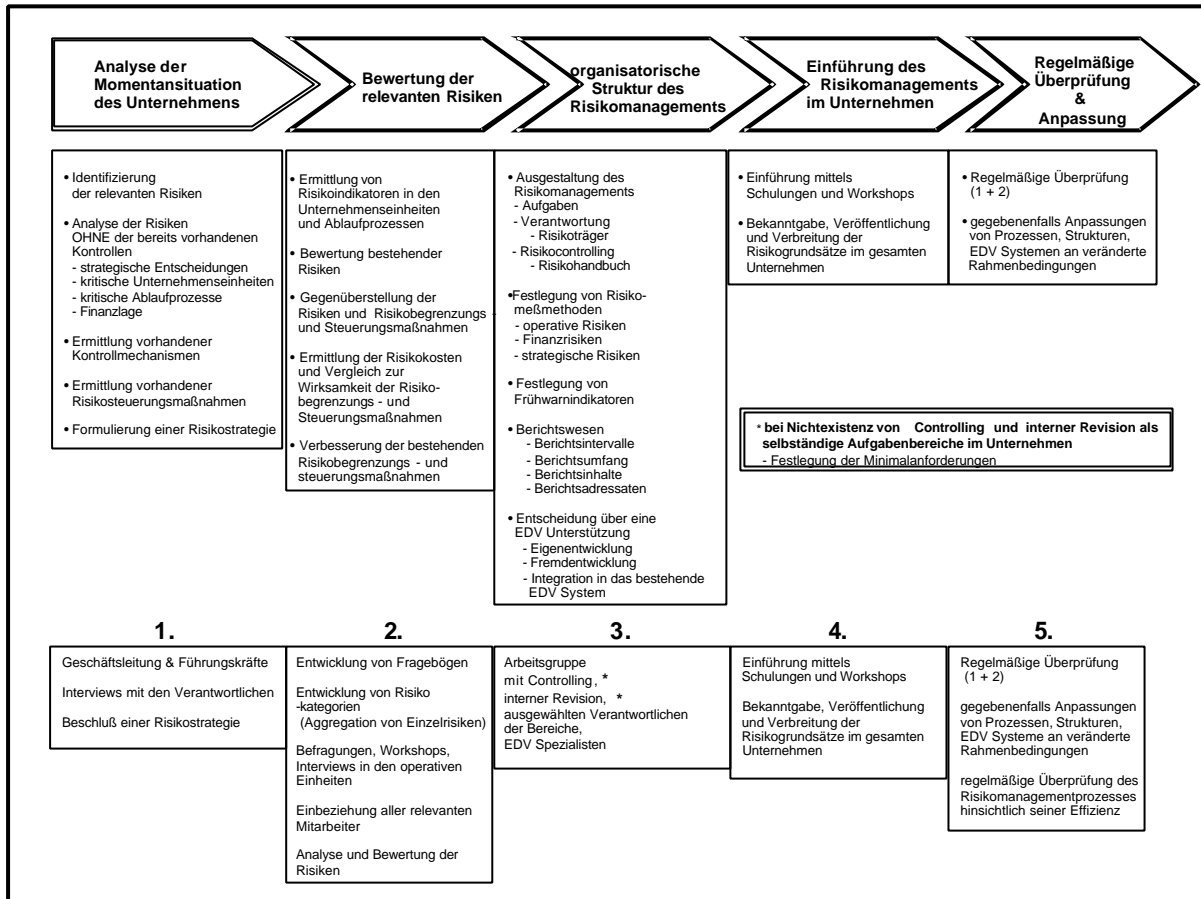
Die Projektarbeit selbst findet in Form eines Workshops statt, um alle Verantwortliche der Unternehmensbereiche einbeziehen.

## **Hinweis:**

Es soll nicht der Eindruck entstehen, ein aufwendiges Projekt initiieren zu müssen. Ziel ist es von Beginn an alle im Unternehmen Verantwortlichen und Beschäftigten effektiv einzubeziehen. Externe Berater können spezielles Know-how in das Projekt einbringen, doch umgesetzt und getragen wird das Risikomanagement durch die Mitarbeiter. Diese bringen die ihr spezifischen Unternehmenswissen und zeigen Lösungen auf die für ein Risikomanagementsystem genutzt werden können (z.B. Dokumentation in Bereich Produkt- und Qualitätsmanagement). Grundsätzlich sollen vorhandene Informationsquellen im Unternehmen genutzt werden und lediglich Anpassungen für eine unternehmensgerechte Risikosteuerung vorgenommen werden.

Die praktische Umsetzung eines Risikomanagements erfolgt in fünf Schritten.

- 1. Schritt**  
**Analyse der Momentansituation des Unternehmens**
- 2. Schritt**  
**Analyse und Bewertung der Unternehmensrisiken**
- 3. Schritt**  
**Organisatorische Struktur des Risikomanagements**
- 4. Schritt**  
**Einführung des Risikomanagements im Unternehmen**
- 5. Schritt**  
**Regelmäßige Überprüfung und Anpassung**



# 1. Schritt

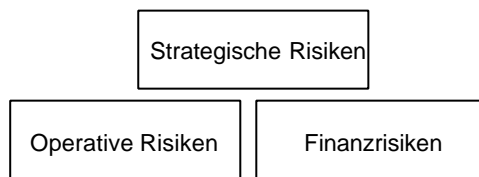
## Analyse der Momentansituation des Unternehmens

Dieser Schritt konzentriert sich auf die strategischen Unternehmensrisiken und die Darstellung der Ist-Risiko-Situation des Unternehmens. Informationslieferanten hierzu sind die Geschäftsführung und zentrale Entscheider bestimmter Unternehmensbereiche. Ziel ist es, eine dokumentierte Risikostrategie als Ausgangsbasis festzulegen. Dabei stehen die vorhandenen Kontrollmechanismen sowie die Risiko-Steuerungsmaßnahmen im Vordergrund. Die im ersten Schritt definierte Risikostrategie wird im Rahmen der weiteren Analysen stetig überarbeitet, um nach Abschluss der Implementierungsschritte eine tragfähige Strategie zu erhalten.

Ausgangspunkt ist die momentane Situation des Unternehmens und sollte anhand nachstehender Fragen zu einer Bestandsaufnahme führen:

- Wo steht mein Unternehmen derzeit?
- Wie ist meine Marktposition?
- Welche Abhängigkeiten bestehen für das Unternehmen?
- Welche internen Prozesse und Strukturen sind zu verbessern?
- Wie stellt sich die Finanzlage dar?
- Wie sieht meine Personalsituation aus?
- Welche Schwierigkeiten erwarte ich künftig?
- Wie soll das Unternehmen künftig aufgestellt sein?

Sie sollten sich zunächst auf 3 wesentliche Risikofelder konzentrieren.



Eine spätere Zerlegung in weitere Risikogruppen ergibt sich zwangsläufig bei der Weiterentwicklung des Risikomanagementprozesses.

Im Vordergrund stehen die strategischen Risiken, die die Unternehmensziele gefährden können, d.h. die Positionierung des Unternehmens selbst und zwar extern wie auch intern.

In Form eines „Top Down“ Ansatzes hilft Ihnen ein Fragenkatalog, den Prozess der Risiko Identifizierung im Unternehmen hierarchisch von „oben“ nach „unten“ zu tragen und diesen Prozess anschließend auf die einzelnen Unternehmensbereiche auszuweiten.

- Ist das Unternehmen abhängig vom technologischen Wandel?
- Ist die Unternehmenskompetenz durch Substitutsprodukte gefährdet?
- Ist das Unternehmen von rechtlichen Verordnungen abhängig?
- Unterliegt das Unternehmen politischen Einflüssen und Entscheidungen?
- Ist das Unternehmen von Großaufträgen abhängig?
- Ist das Unternehmen von einem schlechten Image umgeben?
- Bestehen Abhängigkeiten auf den Beschaffungs- / Absatzmärkten?
- Sind die internen Unternehmensbereiche hinsichtlich der Prozesse aufeinander abgestimmt?
- Ist die Produktion von häufigen Leerstandszeiten betroffen?
- Ist die Produktion von einer hohen Ausschussquote betroffen?
- Unterliegt die Produktion Qualitätsschwankungen?
- Sind die Produkte von einem schlechten Image umgeben?
- Ist das Unternehmen von langfristiger Forschung und Entwicklung abhängig?
- Treten in den Ablaufprozessen häufig Störungen auf?
- Sind die Prozessdurchlaufzeiten optimal ausgestaltet?
- Sind die Aufträge mit häufigen Terminverschiebungen verbunden?
- Ist das Unternehmen von einer überdurchschnittlichen Personalfuktuation betroffen?
- Sind hohe Personalfehlzeiten zu vermerken?
- Besteht im Unternehmen ein Teamgeist?

Besteht eine durchgängige Kommunikationskultur im Unternehmen?  
Sind Motivationslücken bei den Mitarbeitern bekannt?  
Unterliegt das Unternehmen größeren Preisschwankungen auf den Finanz-, Beschaffungs- und Absatzmärkten?  
Wird das Unternehmensergebnis durch Zusatzerträge aus Finanzgeschäften beeinflusst?  
Werden derivative Finanzinstrumente eingesetzt?  
Gibt es häufig Zahlungsverzögerungen seitens der Kontrahenten?  
Ist die unternehmerische Finanzfähigkeit gesichert?  
Besteht ein mittelfristiger Finanzplan?  
Gibt es eine Aufstellung der bestandsgefährdenden Risiken?  
Gibt es eine Aufstellung der Risiken, die Einfluss auf die Vermögenswerte haben könnten?  
Besteht im Unternehmen eine angemessene Kostenkalkulation?  
Besteht im Unternehmen ein Kontrollsystem?  
Ist die Unternehmensnachfolge geregelt?  
Werden die Führungskräfte in die Unternehmensentscheidungen einbezogen?

Diese Fragen sollten zur Analyse:

- des Marktumfeldes
- des eigenen Marktauftritts
- des Kundensegmentes
- der Produktpalette
- der Finanzlage
- der Eigentümerstruktur
- der internen Prozesse einschließlich der Informations-Technologie
- der Personalsituation
- der internen Kontrollmechanismen
- der künftigen Risiken und Chancen

und schließlich  
führen.

## 2. Schritt

# Analyse und Bewertung der Unternehmensrisiken

Die identifizierten Risikofelder werden auf die operative Ebene übertragen und dort analysiert, bewertet und dokumentiert.

Auch hierbei sind die Kontrollmechanismen und Risiko-Steuerungsmaßnahmen in den Unternehmensprozessen und der Unternehmensstruktur zu beleuchten und auf deren Risiko-Wirkungsgrad zu untersuchen.

Dieses Vorgehen erfolgt systematisch und prozessorientiert entlang der unternehmerischen Wertschöpfungskette geschehen:

Beschaffung, Produktion, Vertrieb, Finanzen, Personal, Informations-Technologie, Stabs- und Verwaltungsabteilungen.

Bei projektorientiert ausgerichteten Unternehmen empfiehlt es sich entlang der einzelnen Projektschritte:

Marketing/Akquisition, Auftragsannahme, Bestellung, Produktion/Dienstleistung, Abnahme, Verwaltung (einschl. Finanzen, IT, PE).

Es ist zu empfehlen hierzu strukturierte Fragebögen (die sicherlich hinsichtlich des Detaillierungsgrades von Unternehmen zu Unternehmen variieren) für Befragungen in den einzelnen operativen Bereichen und zu den Geschäftsprozessen zu verwenden.

Idealerweise sind die Fragebögen entsprechend der Unternehmensprozesse gegliedert, um die Auswertungen (Risikoanalyse und Risikobewertung) zu erleichtern. Damit erreichen Sie zugleich einen geordneten Überblick der identifizierten Einzelrisiken.

In den Unternehmenseinheiten werden die Befragungen mit den im Prozess involvierten Personen und unter Einbeziehung der Verantwortlichen durchgeführt. Wichtig ist eine absolut offene Mitarbeiter-Kommunikation durch alle Hierarchieebenen. Gerade sie ist geeignet bisher nicht wahrgenommene Risiken in den Prozessen aufzudecken und gegebenenfalls auch bereits Lösungsansätze zu liefern.

### Hinweis:

Es muss jedoch jedem Mitarbeiter möglich sein offen über Schwachstellen und deren Risiken zu berichten, die aus seiner individuellen gesehen werden.

Als Beispiel hier der Bereich „Beschaffung“:

- Besteht eine Lieferantenabhängigkeit?
- Unterliegen die Beschaffungsmärkte Preis- / Währungsschwankungen?
- Unterliegen die Beschaffungsmärkte saisonalen Einflüssen?
- Sind die Beschaffungsmärkte ausreichend gesichert?
- Ist ein häufiger Lieferantenwechsel erforderlich?
- Stehen die Komponenten / Leistungen im Wettbewerb mit Substituten?
- Unterliegen die Komponenten dem technischen Wandel?
- Sind die Komponenten von Trends abhängig?
- Unterliegen die Komponenten einem häufigen Modellwechsel?
- Gibt es häufig Lieferengpässe?
- Sind die Transportwege gesichert?
- Unterliegen die Komponenten / Leistungen einer hohen Reklamationsquote?
- Können Haftungsansprüche aus den Komponenten / Leistungen hergeleitet werden?
- Wird das Konkurrenzverhalten permanent beobachtet?

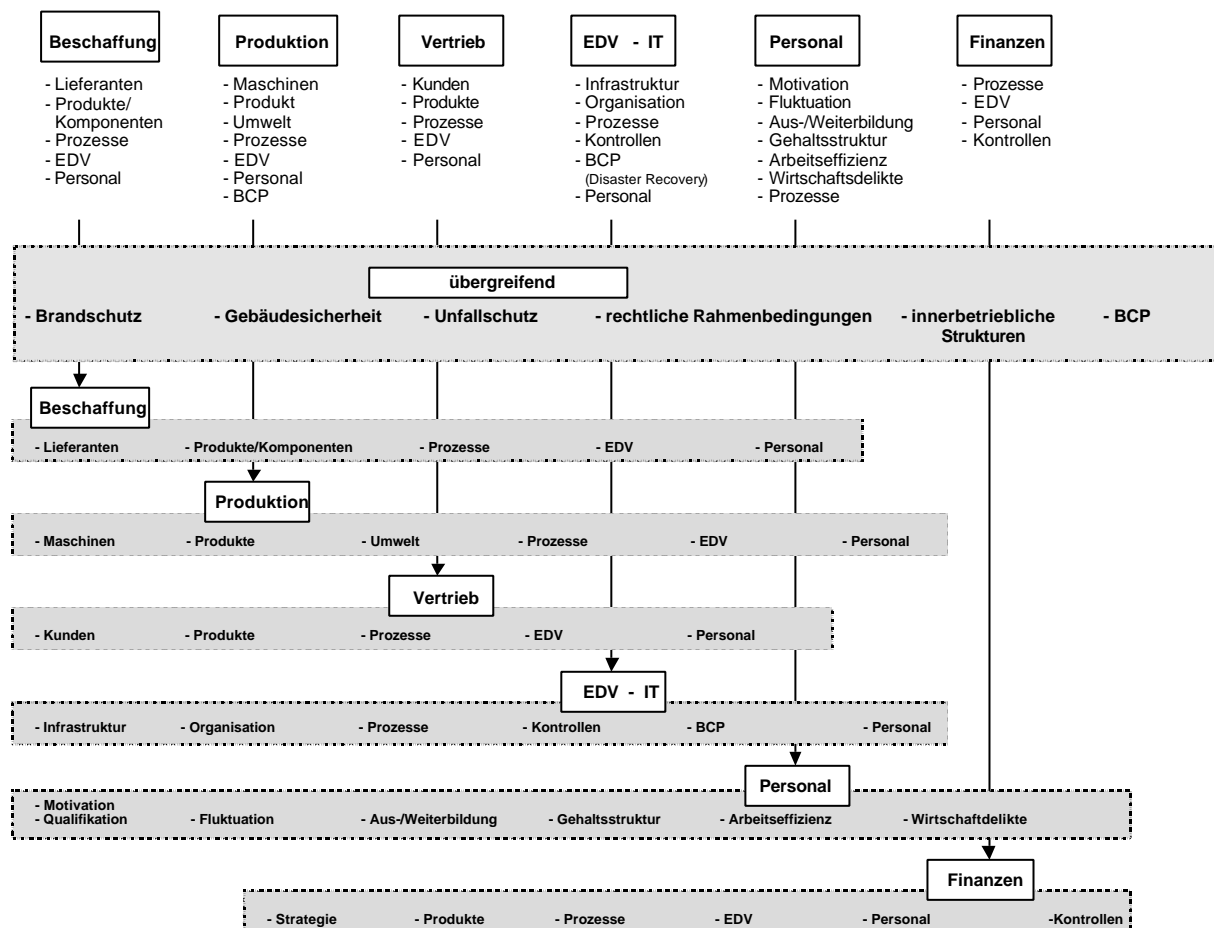
Bei der Entwicklung der Fragebögen werden Sie feststellen, dass sich neben den speziellen bereichsbezogenen Risikokategorien wiederkehrende **Risikokategorien** als Aggregat von Einzelrisiken ergeben, die für alle Bereiche Anwendung finden.

## Beschaffung

- Lieferanten	- Prozesse	- EDV	- Personal	- Produkte/Komponenten
<ul style="list-style-type: none"> <li>- Bonitätsrisiko</li> <li>- Ausfallrisiko</li> <li>- Länderrisiko</li> <li>- Währungsrisiko</li> <li>- Lieferantenabhängigkeiten</li> <li>- Länderabhängigkeiten</li> <li>- Transport</li> <li>- Lagerwesen</li> <li>- Umwelt</li> <li>- Rohstoffmärkte</li> <li>- Preisschwankungen</li> <li>- saisonale Einflüsse</li> <li>- Beschaffungszeiten</li> <li>- Lieferverzögerungsquote</li> <li>- Mindestbestellmengen</li> </ul>	<ul style="list-style-type: none"> <li>- Funktionen</li> <li>- Kontrollen</li> <li>- Kompetenzen</li> <li>- EDV Abhängigkeiten</li> <li>- Durchlaufzeiten</li> <li>- Belegwesen</li> <li>- Bestellstruktur</li> <li>- Prozeßabstimmungen</li> <li>- Abhängigkeiten zu</li> <li>- Produktion</li> <li>- Vertrieb</li> <li>- Prozeßunterbrechungen</li> <li>- Dokumentationen</li> <li>- BCP</li> </ul>	<ul style="list-style-type: none"> <li>- Systemverfügbarkeit</li> <li>- Datenverfügbarkeit</li> <li>- Systemstabilität</li> <li>- Zugriffszeit</li> <li>- Datensicherheit</li> <li>- Zugriffsrechte</li> <li>- Prozeßintegration</li> <li>- BCP (Disaster Recovery)</li> <li>- Dokumentation</li> </ul>	<ul style="list-style-type: none"> <li>- Motivation</li> <li>- Qualifikation</li> <li>- Aus-/Weiterbildung</li> <li>- Fehlzeiten</li> <li>- Fluktuation</li> <li>- Arbeitsmarkt</li> <li>- Arbeitsplatzbeschreibung</li> <li>- Kompetenzen</li> <li>- Ressourceneinsatz</li> </ul>	<ul style="list-style-type: none"> <li>- Qualität</li> <li>- Reklamationen</li> <li>- Produkt/Komponentenabhängigkeit</li> <li>- Technologieabhängigkeit</li> <li>- Umwelt</li> <li>- Preisentwicklung</li> <li>- Beschaffungskosten</li> <li>- Mindestbestellmengen</li> </ul>

## Fragebögen / Interviews

Bezogen auf Ihr Unternehmen könnten sich beispielsweise die nachstehenden Risikokategorien als **wiederkehrend in den verschiedenen Unternehmensbereichen** herauskristallisieren:



## Ausgewählte Risikobereiche

### ... Unternehmensübergreifende Risiken

Zu Beginn der Analyse sind die übergreifenden Risiken zu betrachten. Diese resultieren aus gesetzlichen und regulatorischen Auflagen, wie auch aus den allgemein im Geschäftsverkehr geschlossenen Verträgen (Rechtsrisiken).

Danach sind Risiken der Organisationsstruktur und den damit verbundenen Funktionen und Kompetenzen zu analysieren.

Das gesamte Unternehmen ist in seinem Organisationsaufbau und seinen Strukturen zu betrachten.

Der Frage nach vorhandenen Parallelfunktionen ist nachzugehen und auf Überschneidungen zu prüfen. Parallelfunktionen bieten darüber hinaus Potential zu Kosteneinsparungen und einem effizienteren Berichtswesen.

Parallelfunktionen bilden sich vor allem in dezentral strukturierten Unternehmen. Diese Funktionen sind auf Zweckmäßigkeit und Wirtschaftlichkeit zu beleuchten und anzupassen und neu zu definieren. Hierzu eignen sich Organigramme und klare, kurzgefasste Richtlinien für

- Verantwortungsbereiche und Kompetenzen,
- Berichts- und Meldewesen,
- Kontrollfunktionen.

Das Ergebnis muss zu einer klaren, eindeutigen Regelung von überschneidungsfreien Zuständigkeiten und durchgängigen Abläufen in den einzelnen Unternehmensbereichen führen. Diese sind verbindlich zu dokumentieren.

Neben den „internen“ Strukturen und Abläufen sind die externen Risikofelder in die Risikobetrachtung einzubeziehen.

Sie stehen in Zusammenhang mit örtlichen, gesetzlichen und versicherungsvertraglichen Auflagen.

- Brandschutz,
- Gebäudesicherheit,
- Unfallschutzauflagen,
- Umweltschutz,
- Produkthaftung,
- sowie arbeitsrechtliche Bestimmungen

### ... Prozessrisiken

Zur Identifizierung der Prozessrisiken eignet sich die **Risk Flow Analyse**. Sie wird mit Hilfe der erwähnten Fragebögen, mittels Befragungen der im Prozess eingebundenen Mitarbeitern sowie Verantwortlichen durchgeführt. Mit dieser Vorgehensweise lassen sich am Einfachsten die Risiken in den Geschäftsabläufen erkennen sowie fehlende Risikokontroll- und Steuerungsmaßnahmen aufzeigen.

Ausgangspunkt sind die Basisprozesse des Unternehmens. Ziel ist es die einzelnen Prozesse von ihrem Ursprung bis zu ihrem Ende durchgängig zu analysieren.

#### **Hinweis:**

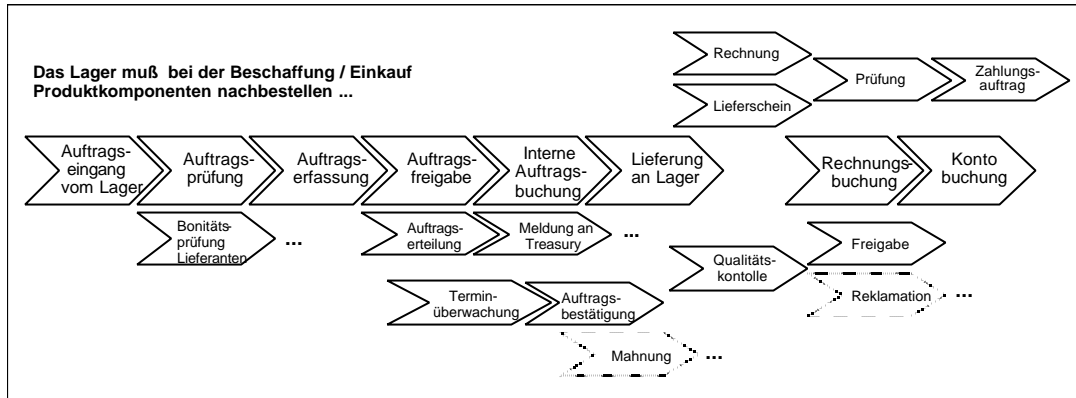
In der Prozessanalyse ist die eingesetzte Informationstechnologie als reines „Werkzeug“ zu betrachten. Jeder Prozess sollte unter Ausklammerung der EDV Anwendungen gedanklich auf den reinen manuellen Ablauf zurückgeführt und analysiert werden.

Die im Prozess integrierten „Werkzeuge“ (EDV) sind in sich auf Risiken zu untersuchen und danach im Gesamtprozess zu beurteilen. Erkannte Schwachpunkte in den eingesetzten EDV Applikationen, wie fehlende systemseitige Kontrollen, können durch zu implementierende nachgelagerte Kontrollmechanismen im Gesamtprozess das Risiko minimieren (Risk Flow).

An dieser Stelle ist deutlich hervorzuheben, dass es die Mitarbeiter und Verantwortlichen sind, die die Prozesse bestens kennen. Sie sind es auch, die den Risikomanagementprozess umzusetzen haben.

Häufig wird die Erfahrung gemacht, dass bei den im Prozess eingebundenen Mitarbeitern neben den Kenntnissen von „Schwachstellen“ bereits „Lösungen“ und Vorschläge zur Risikominimierung vorhanden jedoch nicht umgesetzt sind. Eine Ursache hierfür ist die oftmals nicht ausreichende Kommunikation von „unten“ nach „oben“. Daher ist auch die interne Kommunikation einer kritischen Betrachtung zu unterziehen.

**Basisprozesse** führen zu **Subprozessen**, diese wiederum zu noch kleineren Prozessketten bis hin zur **Tätigkeits-/Aufgabenbeschreibung**.



Nicht übersehen werden sollte, dass die Wirkung des Prozessrisikos um so höher einzuschätzen ist je früher es im Prozessverlauf entsteht. Es zeigt generell einen abnehmenden Wirkungsgrad je näher das Protzessende erreicht wird.

Beachten Sie, dass bei der Risikoanalyse insgesamt der Blick auf den **Gesamtprozess** beibehalten wird.

Bei der Risikoanalyse sind die implementierten Kontrollmechanismen – IT-seitig oder manuell - innerhalb der Prozesse zu bewerten, mit dem Ziel Fehlerquoten auszuschließen, zumindest jedoch einzuschränken.

Ebenso sind die Prozesse dahingehend zu untersuchen, ob sie den rechtlichen Rahmenbedingungen gerecht werden. Dieses gilt besonders bei unternehmensübergreifenden Abläufen, die Niederlassungen, ausgelagerte Einheiten oder Beteiligungen einbeziehen. Hier sei auf den Datenschutz, die „Zugriffsrechte“ der im Prozess involvierten Mitarbeiter sowie auf einen eingeschränkten grenzüberschreitenden Datenaustausch mancher Länder verwiesen.

Nicht zu unterschätzen ist die gegenseitige Abhängigkeit von Informationstechnologie und den Geschäftsprozessen.

Veränderungen im Prozess ziehen Veränderungen in der Informationstechnologie nach sich und umgekehrt. Das Risiko wirkt in beide Richtungen. Daher sollten die IT/EDV grundsätzlich Gesamtprozess orientiert betrachtet werden.

Für die Risikoerfassung ist es nicht sinnvoll die einzelnen kleinsten Prozessschritte zu erfassen, wohl aber sind diese zu untersuchen. Sie sind abschließend zu Risikokategorien zusammenzufassen. Sie sollten darauf achten, dass das Risiko des Gesamtprozesses (**Risk Flow** Analyse) identifiziert und bewertet wird.

### Hinweis:

Ablaufprozesse werden durch den Einsatz von moderner Informationstechnologie augenscheinlich zwar vereinfacht und „erleichtert“. Automatisiert gesteuerte Prozesse werden aber durch den Einsatz dieser Technologie gleichzeitig viel komplexer und bergen folglich zusätzliche Risiken.

## ... Risiken der Informations-Technologie

Ein nicht zu unterschätzender Bestandteil der innerbetrieblichen Prozesse ist die eingesetzte Informations-Technologie /EDV).

Die relevanten Risikofelder in diesem Bereich sind in:

- der Organisation,
- der Infrastruktur,
- und den Prozessen,

zu sehen, wobei die drei Gruppen als Gesamtheit zu betrachten sind.

Die Risiken finden ihre Ausprägung

- im Verlust und/oder Manipulation von Daten,
- in der Nichtverfügbarkeit der Systeme und Anwendungen
- in der zu späten Bereitstellung wichtiger Daten
- in einer fehlenden künftigen Weiterentwicklungsfähigkeit der Systeme.

Im **organisatorischen Bereich** liegen die Risiken vor allem in

- einer nicht klar und eindeutig geregelten Zugriffsberechtigung auf Systeme und Anwendungen mit der Gefahr des unberechtigten Zugriffs auf hoch sensible Daten oder deren Manipulation,
- einer unzureichenden Ausrichtung der Anwendungen selbst, d.h. in der Vernachlässigung wichtiger Geschäftsprozesse,
- der fehlenden Fachkompetenz der Mitarbeiter oder der Fachkompetenz an falscher Stelle, was zu Verarbeitungsfehlern oder Systemabstürzen führen kann.

Die **Infrastruktur** der EDV bezieht sich auf die Hardware und die physischen Sicherungsmaßnahmen der Systeme, die erwartungsgemäß jederzeit stabil zur Verfügung stehen sollen.

Risiken ergeben sich aus der

- Hardware, wenn diese aufgrund fehlender Neuinvestitionen nicht mehr dem neuesten Stand entspricht und damit nicht mehr weiterentwicklungsfähig ist.
- unterschiedlichen Verwendung nicht kompatibler Systeme verschiedener Hersteller verwandt werden.
- Leistungsfähigkeit der Systeme, wenn die Verarbeitung des Datenmaterials an ihre Grenze stößt und es dadurch zu Behinderungen im Tagesgeschäft kommt.
- physischen Sicherung der Server und Rechner, wenn diese nicht entsprechend gegen Feuer, Wassereintrich und Temperaturschwankungen geschützt sind und der Zugang zu ihnen jedermann möglich ist.
- Zugriffsgefahr von „außen“.

Die organisatorischen wie die infrastrukturellen Risiken werden vielfach durch Risiken in den **Prozessen** ergänzt, wenn veraltete Softwareanwendungen oder „Insellösungen“ genutzt werden.

- Notwendige Dateninformationen stehen oftmals nicht rechtzeitig zur Verfügung
- Altanwendungen können nicht mehr optimal angepasst werden,
- Schnittstellen (Interfaces) bergen die Gefahr Daten nicht korrekt zu übertragen.
- Unterschiedliche Systeme lassen sich oftmals nicht „verbinden“ oder es ist nur mit einem enormen Kostenaufwand verbunden, der sich betriebswirtschaftlich nicht rechnet.

### Hinweis:

Mit der kommunikationstechnischen Vernetzung ist ein derzeit nahezu kaum einschätzbares Risikopotential entstanden. Parallel dazu hat sich gleichzeitig die Gefahr einer Kriminalitätsdimension entwickelt. Wie schützt man die kleinen internen Netze vor dem Zugriff aus dem den gesamten Globus umspannenden großen Netz? Eine hundertprozentige Sicherheit wird es im Datennetz nicht geben. Mittels eines unternehmensübergreifenden „Firewall“-Konzeptes kann allerdings ein relativ hochgradiger Schutz erreicht werden.

Beachten Sie,

- dass alle eingesetzten Sicherheitsvorkehrungen aufeinander abgestimmt sind und miteinander „zusammenspielen“.
- dass nur integrierte Sicherheitslösungen einen ganzheitlichen Schutz vor „Angriffen“ von außen und innen bieten. Zu flankieren ist dieser technische Schutz mit einem auf das gesamte Unternehmen abgestimmten organisatorischen Sicherheitskonzept, dass alle Mitarbeiter aktiv einbezieht.
- dass die meisten Risiken und Schäden führen auf die Nachlässigkeit im Umgang mit der Informationstechnologie zurück.

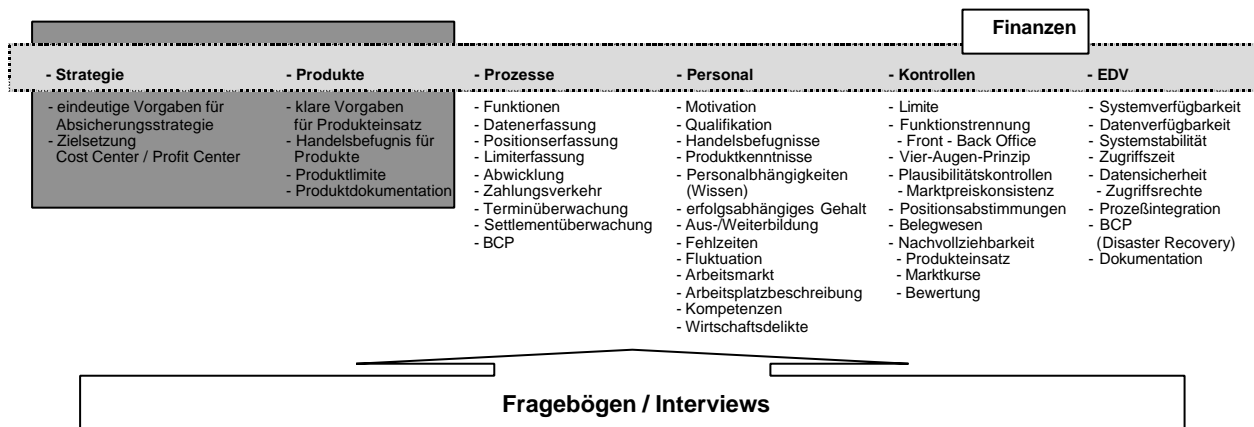
### ... Finanzrisiken

Zu den Finanzrisiken zählen an erster Stelle die Insolvenzgründe drohende Zahlungsfähigkeit, Zahlungsunfähigkeit und Überschuldung. Diese finanziellen Risiken können bei Verschleppung zu einem Straftatbestand führen bzw. schränken den Unternehmer in seiner Handlungsfähigkeit ein.

Des Weiteren sind hierunter Risiken zu betrachten die die Finanz-, Vermögens- und Ertragslage wesentlich beeinflussen. Hierunter zählen u.a. Zins-, Währungs- und Kursrisiken sowie Forderungsausfälle.

Allerdings ist auch der Finanzbereich unter operativen Risikogesichtspunkten zu betrachten. Das nachstehende Schaubild soll Ihnen einen Überblick anzuwendender Risikokategorien geben.

Entsprechend darauf aufbauend können die erforderlichen Fragebögen entwickelt werden.



## Risikoanalyse

Anhand der identifizierten Einzelrisiken sind die Risikoursachen und die Risikowirkungen in ihrem gesamten Ausmaß für das Unternehmen zu ermitteln.

Dabei ist die Risikoeintrittswahrscheinlichkeit objektiv zu ermitteln oder abzuschätzen. Hierbei sollte auf Erfahrungswerte der Vergangenheit zurückgegriffen und daraus die Wahrscheinlichkeit eines künftigen Eintritts in einer Skala erfasst und dokumentiert werden.

Beispielsweise:

höchst wahrscheinlich	6	%
sehr wahrscheinlich	5	%
wahrscheinlich	4	%
möglich	3	%
unwahrscheinlich	2	%
fast unmöglich	1	%

# Risikobewertung

Bei der Risikobewertung sollen die identifizierten Einzelrisiken zu Risikokategorien aggregieren und deren Risikopotential für die einzelnen Unternehmensbereiche und anschließend für das gesamte Unternehmen werden.

## Hinweis:

Operative Risiken sind nur schwer in Form von geldadäquaten Größen zu messen.

Daher ist es ratsam die Bewertung zunächst anhand von Erfahrungswerten vorzunehmen und darauf aufbauend an zuverlässigen Meßmethoden zu arbeiten.

Damit Sie bei der Bewertung eine relative Objektivität erreichen, sollten Sie (basierend auf den vergangenen Produktionsstillstandszeiten, Prozessunterbrechungen, Systemausfallzeiten, Ausschussquoten, Fehlerquoten, eingetretene Versicherungsfälle etc.) sowie die daraus entstandenen Schäden und Auswirkungen) mit den betreffenden Verantwortlichen Ihres Unternehmens das Ausmaß gemeinsam ermitteln und schätzen.

Diese Schätzungen können Sie zusätzlich an Finanzgrößen koppeln, wie zum Beispiel Verluste im Finanzbereich, durch Produktionsausfall, Konventionalstrafen, Verlust von Absatzmärkten / Kundengruppen und die daraus resultierenden Ausfälle.

Anschließend ist eine Zuordnung vorzunehmen.

Beispielsweise:

kritisch	6	über €
sehr hoch	5	bis €
hoch	4	bis €
mittel	3	bis €
gering	2	bis €
unbedeutend	1	bis €

Die Skalierung ist bewusst nach dem Schulnotenprinzip gewählt worden:

- Schulnoten sind aus eigenen Erfahrungen hinreichend bekannt und erleichtern eine Zuordnung
- eine „gerade“ Skalierung zwingt zu einer definitiven Entscheidung und lässt im Gegensatz zu einer „ungeraden“ Skalierung eine „Mittelpunktbildung“ nicht zu.
- Eine „gerade“ Skalierung ist darüber hinaus geeignet Risiken in zwei weitere Gruppen zu unterteilen:
  - 1-3 = gerade noch akzeptabel (bis 3). Stufe)
  - 4-6 = Handlungsbedarf ist angebracht ( ab 4. Stufe ).

## Operatives Risiko „Geld adäquat messen“

Ziel ist es, das operative Risiko in einer einzigen Zahl darzustellen.

Derzeit sind viele Ansätze in der Entwicklung, unter anderem der Ansatz eines Value-at-Risk für operationale Risiken (VaR Ops).

Mathematisch stellt dieser Ansatz kein Problem dar. Schwierigkeiten bereiten vielmehr die fehlenden zugrunde zu legenden Daten und Einflußgrößen, um ein aussagefähiges Ergebnis zu erreichen.

Ein möglicher Weg operatives Risiko „Geld adäquat“ zu erfassen und in einer Finanzgröße für das Unternehmen darzustellen ist der Basis-Kennzahlen-Ansatz. Dieser drückt das operative Risiko als Prozentsatz einer einzigen Kennzahl, wie zum Beispiel des Bruttoertragswertes oder der direkten Kosten aus, ohne auf ein umfangreiches mathematisches Formelwerk zurückgreifen zu müssen.

Verfeinert werden kann dieses durch einen bereichsbezogenen Ansatz in dem in jedem Unternehmensbereich separat der Basis-Kennzahlen-Ansatz angewandt und dabei das operative Risiko des jeweiligen Bereiches im Verhältnis zum Gesamtunternehmen erfasst wird. Die Addition aller Bereiche ergibt dann die gesamt zu kalkulierende geldadäquate Größe der operativen Risiken.

Eine andere Möglichkeit das operative Risiko in absoluten Zahlen darzustellen kann über den Risikominderungskosten-Ansatz erfolgen, der die direkten Kosten der Risikominderung erfasst. Als Grundlage sind die im Risikohandbuch dokumentierten Maßnahmen heranzuziehen.

Grundsätzlich ist zu empfehlen bei der Implementierung eines Risikomanagementsystems Risiken geldadäquat zu erfassen, um eine Risikoeintrittswahrscheinlichkeit und deren Schadenshöhe zukünftig mittels eines absoluten Risikomess-Ansatz mathematisch ermitteln zu können. Dabei ist es unumgänglich eingetretene Schadensfälle als Datengrundlage zu dokumentieren.

## Risikosteuerungsmaßnahmen

Ausgangspunkt ist die Frage, wie risikobereit sich das Unternehmen aufstellen will. Dem zur Folge sind über **Risikobegrenzungs und -steuerungsmaßnahmen** zu entscheiden und das Chancen/Risiko Verhältnis der Maßnahmen abzuwägen. Ziel ist es durch ein gesundes Verhältnis von Ertrag und Verlust (Risiko) die Risikolage des Unternehmens positiv zu gestalten.

Es gilt abzuwägen zwischen Risiken ...

- vermeiden,
- vermindern,
- verlagern (abwälzen),
- selbst tragen.

### Risiken vermeiden

Jede unternehmerische Tätigkeit ist in ihrem Ursprung risikoträchtig. Der Begriff „vermeiden“ sollte somit nicht im engeren Sinne ausgelegt werden, zumal „vermeiden“ gleichzeitig die unternehmerischen Chancen ausschließt.

Risikovermeidung ist daher unter strategischen Aspekten zu sehen, wie beispielsweise

- Vermeidung eines Großauftrages wegen der hohen Abhängigkeit
- Einstellung eines Produktes wegen zu hoher Produkthaftung.

Deutlicher als: „Wenn es dem Esel zu gut geht, begibt er sich auf das Glatteis“ kann es nicht ausgedrückt werden.

### Risiken vermindern

Die Risikoverminderung zielt darauf ab, Risiken in ihren Ursprüngen zu begegnen. Mittels Einführung von „Frühwarnindikatoren“ können bestehende und drohende Risiken rechtzeitig erkannt und begegnet werden. Risikoverminderung wird vornehmlich durch

- personelle,
- technische und
- organisatorische Maßnahmen

erreicht.

### Risiken verlagern

Im Vordergrund steht die Überlegung in wie weit das Risiko auf Andere – Dritte - zu übertragen ist.

Dieses kann erfolgen durch

- Haftungsvereinbarungen
- Haftungsausschluss in den Allgemeinen Geschäftsbedingungen
- Gewährleistungsregelungen
- Sicherheitsbestandsverträge
- Eigentumsvorbehalt
- Konventionalstrafen
- Leasing
- Factoring
- Outsourcing
- Versicherungen

### Risiken selber tragen

Ausschlaggebend für den Risikoselbstbehalt ist die „Risikotragfähigkeit“ eines Unternehmens, d.h. mittels entsprechender Deckungsmasse, Risiken selbst zu übernehmen ohne dabei das Unternehmen in eine bestandsgefährdende Situation zu begeben. Das normale unternehmerische Risikopotential muss durch die normale Gewinnspanne abgedeckt sein, andernfalls würde sich bereits eine existenzgefährdende Entwicklung abzeichnen.

Das über dem Normalmaß liegende Risikopotential ist durch Bildung von Rückstellungen und stillen Reserven abzusichern. Deren Höhe richtet sich nach dem vermutlichen in Anspruch zu nehmenden Betrag.

## Risiko-Controlling

Die Effizienz und der Wirkungsgrad der getroffenen Risikobegrenzungs/-steuerungsmaßnahmen sollte im Rahmen eines Risiko Controlling laufend überprüft werden und dabei Risikoveränderungen aufzeigen, die wiederum zu Anpassungen der Steuerungsmaßnahmen führen.

## Risikohandbuch

Die in den Unternehmensbereichen identifizierten Risiken sind in einem Risikohandbuch zu erfassen und die Ergebnisse der Analyse, Bewertung und der Risikobegrenzungs- und -steuerungsmaßnahmen zu dokumentieren.

Risikohandbuch															
Risiko Identifizierung		Risiko Analyse				Risiko Bewertung			Risiko Steuerung				Risiko Controlling		
Unternehmensbereich	Risiko kategorie	Risiko Ursache	Risiko Wirkung	Risiko Eintrittswahrscheinlichkeit	Risiko Meßmethode	Risiko potential	Risiko Betrag	Risiko Steuerungsmaßnahmen	Chancen der Maßnahmen	Risiken der Maßnahmen	Kosten der Maßnahmen	SOLL	IST	Veränderung	
Finanzen	Strategie														
	Finanzprodukte														
	Prozesse														
	Personal														
	Kontrollen														
EDV	EDV														
	:														
	Infrastruktur														
	Organisation														
	Prozesse														
Beschaffung	Kontrollen														
	BCP														
	Personal														
	Lieferanten														
	Prozesse														
Produktion	:														
	Vertrieb														
	Personal														
übergreifend	Brandschutz														

# 3. Schritt

## Organisatorische Struktur des Risikomanagements

Das weitere Vorgehen liegt in der Ausgestaltung des Risikomanagementprozesses selbst:

- Festlegung der Verantwortungen (Risikoträger) und Aufgaben für den Risikomanagementprozess
- Festlegung von aussagekräftigen Frühwarnindikatoren für das Unternehmen
- Festlegung von Risikokategorien in denen die Einzelrisiken aggregiert werden
- Festlegung von künftigen Risikomeßmethoden für
  - Operative Risiken
  - Finanzrisiken
  - Strategische Risiken
- Risikohandbuch
- Risikosteuerungsmaßnahmen
- Risiko Controlling
- Festlegung eines durchgängigen Berichtswesens,
  - Berichtsintervallen
  - Berichtsumfang
  - Berichtsinhalte
  - Berichtsadressaten.

Die zentralen Fragen sollten für Sie sein:

- Welche Frühwarnindikatoren sind für mein Unternehmen von Bedeutung und aussagefähig?
- Wie oft und in welchem Umfang benötige ich welche Informationen?
- Wo sollen die Informationen zusammen fließen?
- Wie sollen Risiken gesteuert werden?
- Wie sollen die Risiken überwacht werden?

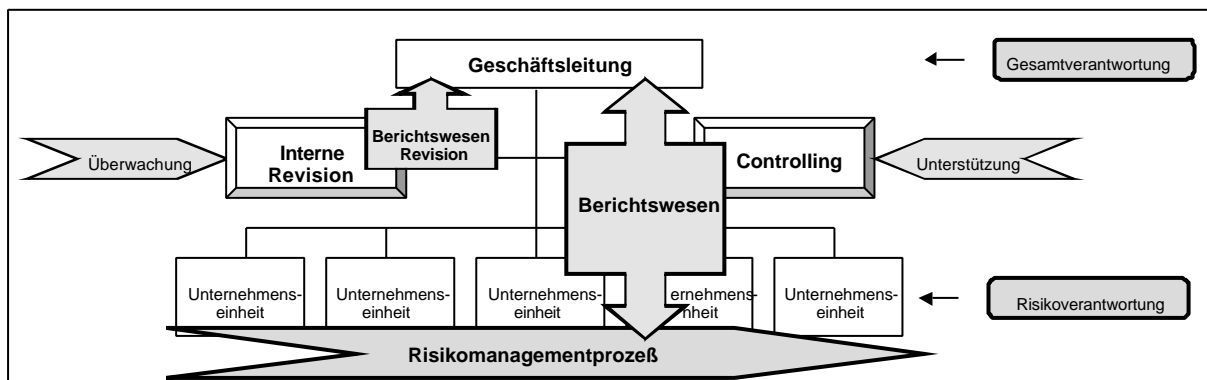
Gleichzeitig ist eine Entscheidung zu treffen wie das Risikomanagement in Ihre bestehende EDV Landschaft zu integrieren ist, um die erforderlichen Berichtsdaten zeitnah liefern zu können.

Für diese Phase ist eine kleine Arbeitsgruppe – idealer weise unter der Regie des Controllers und der internen Revision, wenn diese Funktionen im Unternehmen vorhanden sind - zu bilden, die von den EDV Fachkräften unterstützt wird und entsprechend die Verantwortlichen der einzelnen Unternehmensbereiche hinzuzieht.

### Hinweis:

Sollte die Controllerfunktion und/oder Revision in Ihrem Unternehmen nicht existent sein, könnte notfalls auch ein von der Geschäftsleitung beauftragter kompetenter Mitarbeiter zur Moderation für diese zeitlich begrenzte Aufgabe benannt werden.

Idealer weise sollten Sie auf eine externe Beratungsunterstützung zurückzugreifen, dieses auch unter dem Aspekt der Expertise und Neutralität.



## **4. Schritt**

# **Einführung des Risikomanagements im Unternehmen**

Die Einführung des Risikomanagements im gesamten Unternehmen erfolgt mittels Schulungen, Einweisungen und einer Bekanntgabe der festgelegten Risikogrundsätze.

Hierbei muss allen Mitarbeitern deutlich und klar kommuniziert werden, dass das Unternehmen im Interesse aller Beteiligten – ausnahmslos von oben nach unten – sich Risikogrundsätzen unterwirft, die verhindern sollen, dass aufgrund von Nichtbefolgung das Unternehmen in eine schwer zu meisternde Risikolage gerät.

Wichtig ist hierbei eine (eventuell noch zu schaffende und zu verkündende) Kommunikationsstruktur die offen in beide Richtungen praktiziert wird.

Diese Risikogrundsätze müssen allen Beschäftigten in schriftlicher Form bekannt gegeben werden.

# 5. Schritt

## Regelmäßige Überprüfung und Anpassung

Der Abschluss ist der Beginn eines „zu lebenden und laufend zu praktizierenden Risikomanagements über alle Unternehmens- und Hierarchieebenen hinweg“ und bedeutet aus den Risiken die Chancen zu erkennen.

Eine kontinuierliche Überprüfung des Risikomanagementprozesses und dessen eventueller Anpassung an die veränderten externen und internen Rahmenbedingungen, gegebenenfalls verbunden mit Anpassungen der Unternehmensorganisation und –struktur formt das Risikomanagement zu einem Regelkreislauf.

### **Zur Einführung eines Risikomanagements sollten:**

- Sie sich ausreichend Zeit für die Risikoidentifizierung, -analyse und –bewertung nehmen.
- Sie die erforderliche Distanz zum Tagesgeschäft in diesen Prozess bringen.
- Sie die Verantwortlichen für den späteren Prozess der Umsetzung des Risikomanagements mit einbeziehen.
- Sie eine Kontrolle für die (schrittweise) Umsetzung des Risikomanagements einführen.
- Sie durch eine klare unternehmensweite Kommunikation die Wirksamkeit der Risikosteuerungsmaßnahmen erhöhen.