

# IT-Unterstützung des Risikomanagements aus Anwendersicht

Die umfangreiche Literatur zum Thema Risikomanagement darf nicht darüber hinwegtäuschen, dass viele Unternehmen mit der IT-Unterstützung dieser wichtigen Führungsaufgabe unzufrieden sind. Verwirrt vom Angebot der Software-Hersteller halten sie an ihren selbst entwickelten Lösungen fest, die den gestiegenen Anforderungen häufig nicht mehr gerecht werden. Ausgehend von den grundsätzlichen Anforderungen und anhand eines Praxisbeispiels zur Einführung des Risikomanagements gehen wir in diesem Beitrag der Frage nach, wie sich die Anwender eine leistungsfähige IT-Unterstützung vorstellen. Hieraus ergeben sich wichtige Anregungen für die IT-Branche.

## Keywords

Risk management, IT solutions, corporate governance, user needs, risk management implementation

## Stichworte

Risikomanagement, IT-Lösungen, Corporate Governance, Anwenderforderungen, Risikomanagement-Einführung

## 1. Einleitung

Eine Reihe von Studien kommt zu dem Ergebnis, dass das Risikomanagement in deutschen Unternehmen verbessert werden muss. Gleichzeitig steigt die Zahl der Unternehmenskrisen und Insolvenzen dramatisch an. Betroffen sind nicht nur chronisch kranke Patienten, sondern zunehmend auch ehemals erfolgreiche Unternehmen, die zu spät auf Krisensignale reagiert haben. Die Unternehmensführungen und ihre Aufsichtsgremien sollten diese Situation zum Anlass nehmen, das Risikomanagement auf den Prüfstand zu stellen und gezielt weiterzuentwickeln. Einen besonderen Schwerpunkt bildet dabei oft die IT-Unterstützung, die unterschiedliche rechtliche Rahmenbedingungen berücksichtigen muss.

In der Vergangenheit haben verschiedene Länder Corporate Governance-Initiativen gestartet und versucht, einen Rahmen für das Risikomanagement zu schaffen (vgl. Abb. 1). So verpflichtet das Gesetz zu Kontrolle und Transparenz im Unternehmensbereich (KonTraG) die Vorstände deutscher Aktiengesellschaften

- Maßnahmen zur frühzeitigen Erkennung bestandsgefährdender Risiken zu treffen und
- die Einhaltung dieser Maßnahmen zu überwachen

Nicht geregelt ist allerdings, wie ein solches Früherkennungs- und Überwachungssystem ausgestaltet sein sollte.

In den USA wurde durch den Sarbanes-Oxley-Act (SOA) die Regulierung im Kapitalmarktrecht wesentlich verschärft. Zwingend vorgeschrieben ist die Einrichtung eines internen Kontrollsystems. Bereits 1992 hatte das Committee of Sponsoring Organizations of the Treadway Commission (COSO) ein Internal Control Framework veröffentlicht. Eine 2004 publizierte Weiterentwicklung (COSO II) stellt das Risikomanagement in den Mittelpunkt [1]. Dieses Rahmenkonzept für ein Enterprise Risk Management (ERM) gibt auch keine konkreten Gestaltungsempfehlungen, beeinflusst aber gleichwohl die Überlegungen vieler Unternehmen zur Verbesserung ihres Risikomanagements.

Bevor wir näher auf eine aus Anwendersicht wünschenswerte IT-Unterstützung eingehen, skizzieren wir zunächst das System, den Prozess und die Organisation des Risikomanagements, die es weiterzuentwickeln gilt.

## 2. System, Prozess und Organisation des Risikomanagements

In Anlehnung an den COSO II-Würfel gliedern wir das System des Risikomanagements in vier Subsysteme (vgl. Abb. 2):

- die strategische Frühaufklärung (Strategic)
- ein internes Kontrollsystem (Operations)
- eine Risiko-Berichterstattung (Reporting) sowie
- die Einhaltung von Vorschriften (Compliance)

In vielen Unternehmen ist die Frühaufklärung von Chancen und Risiken seit langem fester Bestandteil des strategischen Planungsprozesses. So werden z. B. bei Haniel systematisch strategische Risiken erfasst, Eintrittswahrscheinlichkeiten und Schadenshöhen abgeschätzt und die Chancen und Risiken von strategischen Initiativen bewertet. Eine Herausforderung liegt naturgemäß in der Sensibilisierung für schwache Signale, die in der Regel die Vorboten einer Krise sind.

Das interne Kontrollsystem geht von einer Beschreibung des Geschäftsmodells aus und leitet hieraus erfolgskritische Geschäftsprozesse ab. Diese Prozesse stehen bei der Dokumentation und Bewertung von Kontrollen im Mittelpunkt. In den USA tätige Unternehmen, wie Bayer, E.ON und die deutsche Telekom haben in den letzten Jahren mit erheblichem Aufwand interne Kontrollsysteme implementiert, um den SOA-Anforderungen zu entsprechen.

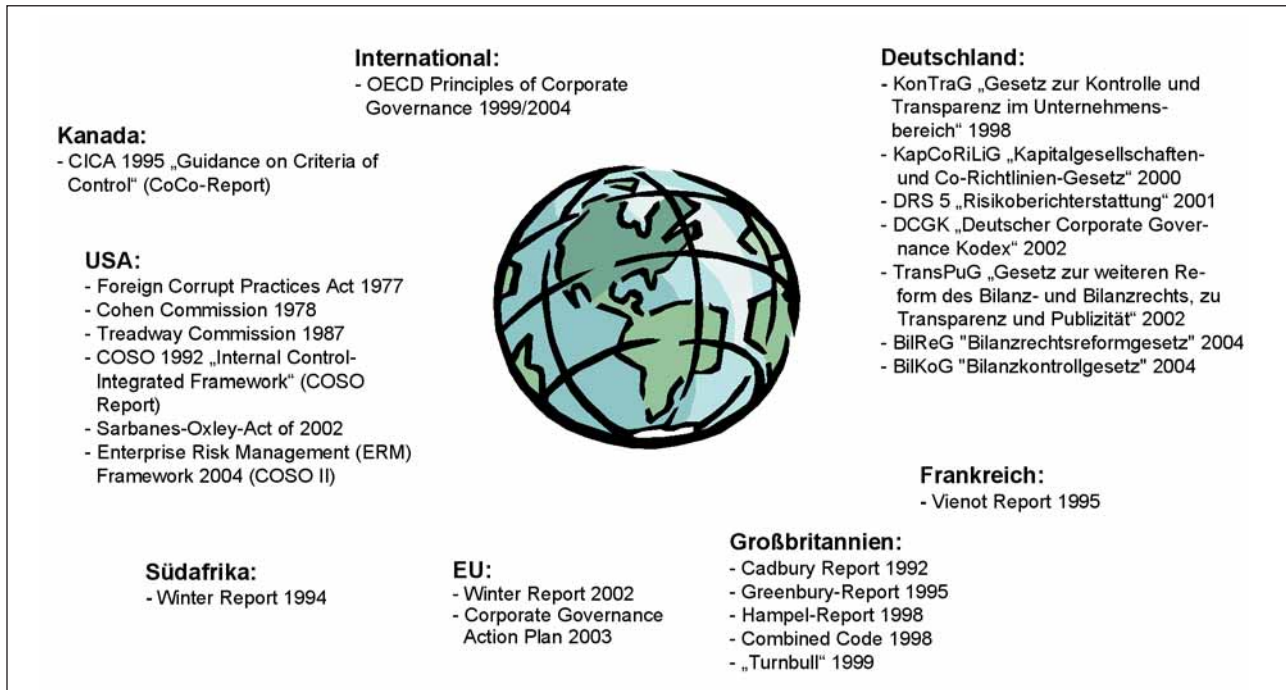


Abbildung 1: Corporate Governance-Initiativen

Die Risiko-Berichterstattung hat in den amerikanisch geprägten COSO-Ansätzen einen weitaus größeren Stellenwert als im deutschen KonTraG. Ausgehend von den Bilanzskandalen der jüngeren Geschichte (Enron, Worldcom etc.) war die Sicherung der Zuverlässigkeit der Finanzberichterstattung ein wesentliches Ziel der Sarbanes-Oxley-Gesetze. Mit dem neuen COSO II-Rahmenwerk wurde der Fokus der Berichterstattung von der Finanzberichterstattung auf alle internen und externen Berichte des Unternehmens ausgeweitet. Im Rahmen der Konvergenz der internationalen Risikomanagement-Systeme und der europäischen Erfahrungen mit Bilanzskandalen (Parmalat, Mannheimer Versicherung etc.) erwarten wir eine deutliche Aufwertung dieses Bereichs des Risikomanagements.

Die Einhaltung der Vorschriften des Risikomanagements (Compliance) wird sowohl unternehmensintern (Internal Audit) als auch extern (durch Abschlussprüfer) gewährleistet. Dabei gilt es, die rechtlichen Vorschriften (bspw. § 317 Abs. 4 HGB und § 91 Abs. 2 AktG) und berufsständische Regelungen zu adaptieren (IDW PS 340). Die multidisziplinäre Zusammensetzung von Beratungsteams gewährleistet die friktionslose Implementierung von gesetz- und empfehlungskonformen Überwachungssystemen. Vorstände von Aktiengesellschaften müssen nach § 161 AktG eine Entsprechenserklärung abgeben, mit der sie sich zur Einhaltung der Vorschriften des Deutschen Corporate Governance Kodex (DCGK) verpflichten. Das Risikomanagement bildet einen wesentlichen Kern dieses Regelwerkes. Im Falle von Unternehmenskrisen werden sich Vorstände zukünftig sowohl gegenüber ihren Aktionären als auch Gerichten verantworten müssen, wenn Krisen durch ein adäquates Risikomanagement hätten verhindert werden können.

Den Rahmen für Prozessverbesserungen bildet die Schaffung eines geeigneten internen Umfeldes. Hierzu gehört z. B. die Verankerung einer angemessenen Risikokultur im Unternehmen. Der eigentliche Risikomanagement-Prozess besteht dann aus den Schritten

- Zielbestimmung
- Ereignisidentifikation
- Risikobewertung
- Risikobewältigung sowie
- Risikosteuerung und
- Überwachung.

Neben der methodischen Unterstützung dieses Prozesses wächst die Bedeutung geeigneter IT-Systeme.

Die Herausforderung bei der Organisation des Risikomanagements liegt in der vertikalen Koordination zwischen verschiedenen Ebenen des Unternehmens sowie der horizontalen Koordination zwischen Linienfunktion und unterstützenden Einheiten, z. B. Unternehmensentwicklung, Controlling, interne Revision und Informationstechnik. Unternehmen wie die BASF haben in einem Risikomanagement-Handbuch die Aufgaben und Verantwortlichkeiten klar beschrieben. Damit wird eine wichtige Grundlage für eine interne und externe Prüfung geschaffen. Da jedoch der Wirtschaftsprüfer nicht untersucht, ob die Reaktionen auf festgestellte Risiken angemessen sind, obliegt es dem Aufsichtsrat zu prüfen, ob der Vorstand seinen Pflichten nachgekommen ist. Insofern weisen die eklatante Schwäche vieler Risikomanagement-Systeme letztlich auf Versäumnisse in der Wahrnehmung der Aufsichtsfunktion hin. Verantwortungsvolle Aufsichtsgremien erwarten daher von ihren Unternehmen einen Leistungsnachweis der Organisation des Risikomanagements. Dies gilt insbesondere für

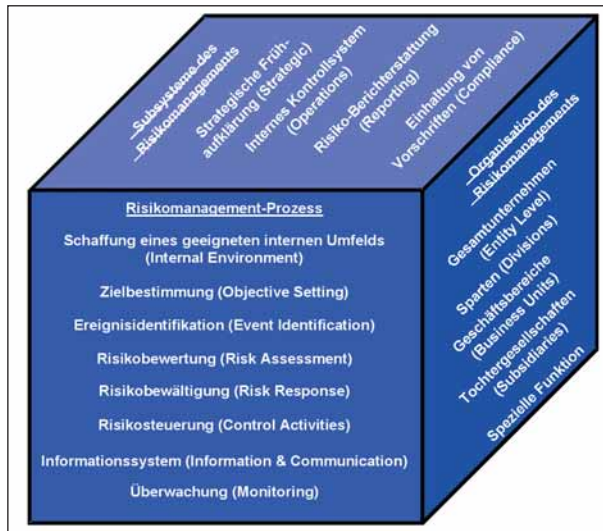


Abbildung 2: Subsysteme, Prozesse und Organisation

innovative Unternehmen, denn Chancen und Risiken sind meist zwei Seiten einer Medaille.

Eine Weiterentwicklung des Risikomanagements muss in der Regel an den drei Gestaltungsebenen System, Prozess und Organisation ansetzen, die eng zusammenhängen. In einer ersten Phase erfolgt die kritische Analyse der vorhandenen Ansätze und die Ableitung von Verbesserungsmöglichkeiten. Diese werden in einer zweiten Phase zu einem Gesamtkonzept integriert. In einer dritten Phase erfolgt dann die Umsetzung (vgl. Abb. 3).

Jenseits einer Erfüllung gesetzlicher Anforderungen muss das Risikomanagement in den Kontext einer wertorientierten Unternehmensführung eingebettet sein. So verstanden hilft das Risikomanagement nicht nur bei der Abwehr von Gefahren, sondern auch bei der Wahrnehmung von Chancen. Allerdings nutzt heute nur ein relativ geringer Teil der Unternehmen das Risikomanagement, um einen Überblick über wesentliche Chancen zu gewinnen [2].

### 3. Verwirrendes IT-Angebot

Die Zeit, bis ein Vorstand über wichtige Risiken informiert wird, streut sehr stark zwischen weniger als 30 Minuten und mehr als 7 Tagen [3]. Dieses überraschende Ergebnis einer Studie zur IT-Unterstützung des Risikomanagements ist unter anderem dadurch

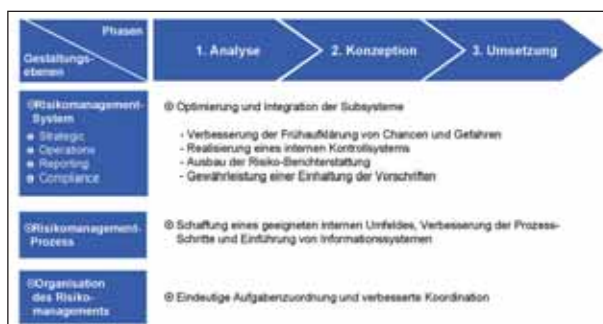


Abbildung 3: Gestaltungsebenen und Phasen

zu erklären, dass immer noch viele Unternehmen auf Excel-Tools setzen, die den Anforderungen an ein zeitgemäßes Risikomanagement nicht mehr gewachsen sind.

Die Zurückhaltung beim Einsatz von Standard-Software zur Unterstützung des Risikomanagements erklärt sich zum Teil daraus, dass viele Anwender durch das Angebot der Hersteller schlicht verwirrt sind. Business Performance Management (BPM) Software, bei der Risikoaspekte lediglich einen Teilaspekt darstellen, konkurriert mit speziellen Risikomanagementlösungen, die mit den Planungs- und Controllingprozessen verknüpft werden müssen. Außerdem benötigen die meisten Unternehmen gar nicht die komplexen Internal Control Tools, die für den Sarbanes-Oxley-Act entwickelt wurden. Viele Anwender haben das Gefühl, dass die Softwareangebote zu kompliziert sind, nicht zu ihren Bedürfnissen passen und mit einem zu großen Implementierungsaufwand verbunden wären. Sie halten daher an ihren Excel-Tools fest oder optimieren ihre Individuallösungen.

Das verwirrende Angebot der Hersteller resultiert auch aus den begrifflichen und konzeptionellen Unklarheiten beim Risikomanagement. Der betriebswirtschaftlichen Forschung und Praxis ist es – trotz unbestreitbarer Erfolge [4] – bislang noch nicht überzeugend gelungen, die gesetzlichen Vorgaben, die einen breiten Spielraum zur Ausgestaltung zulassen, in klare Best Practice-Empfehlungen für unterschiedliche Unternehmenstypen zu überführen. In dieser Situation stellt sich die Frage, welche Anforderungen die Anwender an eine IT-Unterstützung des Risikomanagements stellen.

### 4. Anforderungen der Anwender

In einer Reihe von Beratungsprojekten zum Thema Risikomanagement wurden wir immer wieder mit den Anforderungen an eine leistungsfähige IT-Unterstützung konfrontiert. Die Wünsche der Anwender lassen sich zu den folgenden Punkten zusammenfassen:

- modularer Aufbau mit klar definierten Schnittstellen
- Verknüpfung mit den strategischen und operativen Prozessen in Wertschöpfungsnetzwerken
- Unterstützung unterschiedlicher Methoden
- anpassbar an individuelle Nutzerbedürfnisse und leicht anwendbar
- in die Organisation integriert und einfach zu implementieren

#### 4.1 Modularer Aufbau mit klar definierten Schnittstellen

In den Subsystemen des Risikomanagements sind unterschiedliche Aufgaben zusammengefasst. Die strategische Frühaufklärung, das interne Kontrollsystem, die Risiko-Berichterstattung und die Prüfung der Einhaltung von Vorschriften erfordern aber auch eine differenzierte IT-Unterstützung. Die Anwender wünschen sich deshalb einen modularen Aufbau der IT-Systeme mit klar definierten Schnittstellen. So steht bei der strategischen Frühaufklärung von Chancen und Gefahren das Erfassen schwach-

cher Signale und die vertiefte Untersuchung wichtiger Umfeldbereiche im Vordergrund. Eine IT-Unterstützung sollte die relevanten Markt-, Technologie- und Wettbewerbsinformationen liefern. Zum Teil streben das auch Business Intelligence-Lösungen an, die aber eher auf harte Daten setzen. Die IT-Unterstützung der strategischen Frühaufklärung ist daher in vielen Unternehmen noch nicht befriedigend gelöst.

Einen anderen Aufgabenschwerpunkt haben interne Kontrollsysteme. Ausgehend von der Identifikation kritischer Geschäftsprozesse geht es hier vor allem darum, die finanziellen Implikationen von Prozessrisiken transparent zu machen. Dabei wirken häufig verschiedene Fehlerquellen zusammen, verstärken sich gegenseitig und führen so zu typischen Risikomustern. Die IT-Unterstützung des internen Kontrollsystems ist daher in enger Anlehnung an ein möglicherweise vorhandenes Performance Management zu konzipieren.

Diese Beispiele zeigen, dass die IT-Unterstützung des Risikomanagements mit der vorhandenen IT-Anwendungsarchitektur synchronisiert werden muss. Aufgrund der sich zum Teil überschneidenden Applikationen ist dies keine triviale Aufgabe.

## 4.2 Verknüpfung mit den strategischen und operativen Prozessen in Wertschöpfungsnetzwerken

Eine weitere Schwierigkeit besteht darin, dass der Prozess des Risikomanagements auf vielfältige Weise mit den strategischen und operativen Prozessen des Unternehmens verknüpft ist. Häufig fehlt zum Beispiel eine systematische Berücksichtigung von Risiken im Rahmen einer flexibilisierten Budgetplanung. Die Forderung nach einer verbesserten IT-Unterstützung des Risikomanagements geht dabei einher mit der Entwicklung zu einem Real-Time-Business, bei dem Entscheidungen verstärkt auf der Grundlage von tagesaktuellen Informationen getroffen werden [5]. Es stellt sich daher die Frage, ob IT-Lösungen für das Risikomanagement als additive Module konzipiert sein sollten, die lediglich an die vorhandenen Systeme "angedockt" werden. Sinnvoller, aber natürlich auch aufwändiger wäre es, von vornherein in neue Echtzeit-Infrastrukturen zu investieren, die auch die Wertschöpfungspartner mit einbeziehen. In dem Maße, wie ein immer größerer Anteil der Gesamtleistung in internationalen Netzwerken erbracht wird, müssen auch IT-Systeme die spezifischen Risiken erfassen, die aus der Zusammenarbeit von Partnern resultieren.

## 4.3 Unterstützung unterschiedlicher Methoden

Angesichts der Vielfalt unterschiedlicher Methoden des Risikomanagements und der spezifischen Anforderungen einzelner Branchen sollten IT-Lösungen dem Anwender ein Angebot machen, aus dem dieser den für seine Situation geeigneten Methodenmix auswählen kann. Komplexe mathematische Modelle, wie sie Finanzdienstleister einsetzen, werden möglicherweise in einem Industrieunternehmen nicht benötigt. Andererseits hat jede Branche spezifische Risikoarten, die zum Teil auch eigenständige Methoden erfordern.

Es kann daher nicht die eine IT-Lösung für das Risikomanagement geben, die für alle Situationen passt. Die Anwender wünschen sich einen breiten Methodenbaukasten, aus dem sie einzelne Komponenten auswählen und sinnvoll kombinieren können.

## 4.4 Anpassbar an individuelle Nutzerbedürfnisse und leicht anwendbar

Eine weitere wichtige Forderung resultiert aus den unterschiedlichen Informations- und Nutzerbedürfnissen der an Risikomanagement beteiligten Personengruppen. Diese reichen vom Aufsichtsrat über die Führungsebene bis zu den operativ Verantwortlichen und den Spezialisten im Controlling und Auditing. Wie bei anderen IT-Systemen ist auch hier eine weitestgehende Individualisierung anzustreben.

Die Schwierigkeit besteht jedoch darin, dass diese individuellen Sichtweisen auf das Gesamtsystem wie in einem Nervensystem verknüpft sein sollten. Wenn im operativen Tagesgeschäft fernab der Zentrale eine gefährliche Situation eintritt, die erhebliche finanzielle Auswirkungen haben könnte, so ist es inakzeptabel, dass der Vorstand hiervon erst nach Tagen oder Wochen erfährt. Natürlich ist es nicht einfach, die richtige Balance zwischen Informationsüberflutung und notwendiger Frühwarnung zu finden. Aber gerade das muss ein gutes Radarsystem leisten.

Dies geht einher mit der Forderung, dass ein solches System intuitiv verständlich und im Tagesgeschäft leicht anwendbar sein sollte. In einer Zeit, da jeder Manager seine Mails über ein Smartphone erhalten kann, darf sich die Risiko-Berichterstattung nicht auf monatliche Reports beschränken.

## 4.5 In die Organisation integriert und einfach zu implementieren

Eine IT-Unterstützung des Risikomanagements besteht den Praxistest, wenn sie in die Organisation integriert ist und zu einer reibungslosen Zusammenarbeit der Beteiligten beiträgt. Das frühzeitige Erkennen und erfolgreiche Bewältigen von Krisen erfordert klar definierte Notfallpläne, eine gute Kommunikation und eine wirksame Erfolgskontrolle. IT-Systeme bilden die hierfür benötigte Infrastruktur. Sie müssen leistungsfähig sein, dürfen die Anwender aber nicht überfordern.

Es mag paradox klingen, wenn ein solches System auch noch einfach zu implementieren sein soll. Dieser scheinbare Widerspruch löst sich aber zumindest teilweise auf, wenn wir von der Vorstellung eines "Human-Centered Computing" ausgehen, das die menschlichen Informations- und Kommunikationsbedürfnisse in den Mittelpunkt stellt [6]. Die Implementation von IT-Systemen für das Risikomanagement muss mit der täglichen Arbeitspraxis verwoben und als Lernprozess gestaltet sein. Wie der Manager seinen PDA im Alltag als unentbehrliches Hilfsmittel nutzt, sollte er auch mit den IT-Tools zum Management "seiner" geschäftlichen Chancen und Gefahren umgehen. Dann wird die IT-Implementation das sein, was sie sein sollte: ein willkommener Schritt zur Steigerung der persönlichen Produktivität.

## 5. Vorgehensmodell in der Praxis: Was muss die IT konkret begleiten und dokumentieren

Die Bewährungsprobe für eine IT-Lösung liegt der Einführungsphase des Risikomanagements. Das Vorgehen muss durch eine entsprechende Software von Beginn an unterstützt werden, um ein zielgerichtetes Bearbeiten hinsichtlich Informationserhebung und zukünftiger Analysemöglichkeiten zu gewährleisten. Aufgrund des zunächst abstrakt wirkenden Charakters ist die wichtigste Anforderung, ein strukturiertes aber auch pragmatisches Vorgehen zu unterstützen, bzw. vorzugeben, damit einerseits das Risikomanagement hinreichend realitätsnah ist, aber andererseits keine zu hohe Komplexität hinsichtlich Datenbeschaffung und Analytik geschaffen wird.

In diesem Abschnitt schildern wir beispielhaft den Ablauf einer Verbesserung des operativen Risikomanagements, um aufzuzeigen was die IT in der Praxis – jenseits aller grundsätzlichen Systematik – unterstützen und leisten muss[7].

Die Einführung wird üblicherweise im Rahmen eines eigenständig geführten Projektes vorgenommen, um auch die notwendige Signalwirkung und Akzeptanz für das gesamte Unternehmen zu erzielen. Die Projektarbeit selbst findet überwiegend in Form von Workshops statt, um alle Verantwortlichen der Unternehmensbereiche einzubeziehen. Das praktische Vorgehen erfolgt in fünf Phasen.

### 5.1 Analyse der Ausgangssituation des Unternehmens

Diese Phase konzentriert sich auf die strategischen Unternehmensrisiken und die Darstellung der Risiko-Situation des Unternehmens. Informationslieferanten hierzu sind die Geschäftsführung und zentrale Führungskräfte bestimmter Unternehmensbereiche. Ziel ist es, eine dokumentierte Risikostrategie als Ausgangsbasis für das Unternehmen festzulegen. Dabei stehen die vorhandenen Risikofrüherkennungs- und Überwachungssysteme im Vordergrund. Die in der ersten Phase erstellte Risikostrategie wird im Rahmen der weiteren Schritte kontinuierlich verfeinert, um mit Abschluss der Implementierung ein "lauffähiges" System zu erhalten.

Wichtige Aspekte der Ist-Aufnahme sind: die Marktposition, Abhängigkeiten zu anderen Unternehmen, interne Prozesse und Strukturen, die Finanzlage, die Personalsituation, mögliche künftige Schwierigkeiten und geplante Entwicklungen des Unternehmens.

Dabei unterscheidet man zunächst zwischen strategischen und operativen Risiken. Eine spätere Gliederung in weitere Risikokategorien ergibt sich mit der Weiterentwicklung des Risikomanagementprozesses. Die Risikomanagementsoftware unterstützt die Analyse der Ausgangssituation durch flexible Strukturierungsmöglichkeiten, vorstrukturierte Kategorien – und besonders wichtig – die Möglichkeit zur systematischen Detaillierung der zunächst top-down erarbeiteten Risikofelder.

### 5.2 Analyse und Bewertung der Unternehmensrisiken

Die identifizierten Risiken werden auf der operativen Ebene analysiert, bewertet und dokumentiert. Auch hierbei sind die Kontrollsysteme und Risiko-Steuerungsmaßnahmen in den Unternehmensprozessen und der Unternehmensstruktur zu beleuchten und auf deren Risiko-Wirkungsgrad zu untersuchen.

Dieses Vorgehen erfolgt prozessorientiert entlang der Wertschöpfungskette: Beschaffung, Produktion, Marketing, Finanzen, Personal, Informationstechnologie sowie Stabs- und Verwaltungsaufgaben. Bei projektorientiert ausgerichteten Unternehmen empfiehlt sich ein Vorgehen entlang der einzelnen Projektschritte: Marketing/Akquisition, Auftragsannahme, Bestellung, Produktion/ Dienstleistung, Abnahme und Verwaltung.

Die Risikomanagementsoftware sollte zur Unterstützung strukturierte Fragebögen anbieten, die hinsichtlich des Detaillierungsgrades von Unternehmen zu Unternehmen variieren. Diese Fragebögen sind entsprechend der Unternehmensprozesse und der Risiken zu gliedern, um entsprechende Auswertungen (Risikoanalyse und Risikobewertung) zu ermöglichen. Damit wird zugleich ein geordneter Überblick über die identifizierten Einzelrisiken erreicht.

In den Unternehmenseinheiten werden die Befragungen mit den im Prozess involvierten Personen und unter Einbeziehung der Verantwortlichen durchgeführt. Dabei ist eine offene Kommunikation sicherzustellen, da die Versuchung auf Seiten der Verantwortlichen naturgemäß groß ist, Schwächen der Systeme zu verschweigen und Risikoinformationen zurückzuhalten.

#### Wichtige Risikokategorien

**Unternehmensübergreifende Risiken:** Zu Beginn der Analyse sind die übergreifenden Risiken zu betrachten. Diese resultieren aus gesetzlichen und regulatorischen Auflagen, sowie den im Geschäftsverkehr geschlossenen Verträgen (Rechtsrisiken). Danach sind Risiken der Organisationsstruktur und die damit verbundenen Funktionen und Kompetenzen zu analysieren. Das gesamte Unternehmen ist in seinem Organisationsaufbau und seinen Beziehungen zu Wertschöpfungspartnern zu betrachten.

**Geschäftsprozessrisiken:** Die Prozessrisiken werden mittels Befragungen der im Prozess eingebundenen Mitarbeitern sowie der Verantwortlichen durchgeführt. Mit dieser Vorgehensweise lassen sich am Einfachsten die Risiken in den Geschäftsabläufen erkennen sowie fehlende Risikokontroll- und Steuerungsmaßnahmen aufzeigen. Ausgangspunkt sind die Geschäftsprozesse des Unternehmens. Ziel ist es, die einzelnen Prozesse von ihrem Ursprung bis zu ihrem Ende durchgängig zu analysieren und hierbei auch die ggf. existierenden Verknüpfungen zwischen den Prozessen zu berücksichtigen.

Häufig macht man die Erfahrung, dass bei den im Prozess eingebundenen Mitarbeitern neben der Kenntnisse von "Schwachstellen" bereits "Lösungen" und Vorschläge zur Risikominimierung vorhanden sind, die jedoch nicht umgesetzt wurden. Ursache hier-

für sind in der Regel Kommunikationsmängel. Daher ist auch die Aufnahme von Kontroll- und Risikoinformationen in die Reportingprozesse zu überprüfen und ggf. zu ergänzen. 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. Dies gilt insbesondere für die Bereiche der Rechnungslegung.

Risiken der Informations-Technologie: In modernen Unternehmen spielt die IT eine wichtige Rolle für die Durchführung und Gestaltung der Geschäftsprozesse. Die entscheidenden Risikofelder in diesem Bereich finden sich in Infrastruktur und Leistungserbringung, wobei die zwei Kategorien in der Praxis kaum zu trennen sind. Mögliche Ereignisse sind bspw.

- Systemausfall
- Datenverlust
- hohe Zugriffszeiten
- Datendiebstahl
- Ausfall Telekommunikation
- fehlende Datenintegrität

Die Ursachen dieser Ereignisse können u.a. sein:

- Computerviren
- veraltete Systeme
- fehlende Datensicherheitskonzepte
- keine, bzw. unvollständige Dokumentation.

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. Hierzu zählen u.a. Zins-, Währungs- und Kursrisiken sowie Forderungsausfälle. Allerdings ist auch der Finanzbereich unter operativen Risikogesichtspunkten zu betrachten.

Risikoanalyse: Anhand der identifizierten Einzelrisiken sind die Risikoursachen und die Risikowirkungen in ihrem gesamten Ausmaß für das Unternehmen zu betrachten. 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. Die Quantifizierung sollte in Raster und nicht zu feingranular erfolgen, da diese Scheingenauigkeit lediglich die Komplexität steigert, ohne weiteren Nutzen zu liefern.

Risikobewertung: Bei der Risikobewertung sollten die identifizierten Einzelrisiken zu Risikokategorien aggregiert und deren Risiko-

potential für die einzelnen Unternehmensbereiche und anschließend für das gesamte Unternehmen zusammengeführt werden.

Dabei ist zu berücksichtigen, dass bspw. operative Risiken nur schwer in Form von absoluten Größen (bspw. Value at Risk) zu messen sind. Daher ist es ratsam, die Bewertung zunächst anhand von Erfahrungswerten vorzunehmen und darauf aufbauend an zuverlässigen Messmethoden zu arbeiten. Damit bei der Bewertung eine relative Objektivität erreicht wird, sollte (basierend auf den vergangenen Produktionsstillstandszeiten, Prozessunterbrechungen, Systemausfallzeiten, Ausschussquoten, Fehlerquoten, eingetretenen Versicherungsfällen etc. sowie den daraus entstandenen Schäden und Auswirkungen) mit den betreffenden Verantwortlichen des Unternehmens das Ausmaß gemeinsam ermittelt und abgeschätzt werden. Diese Schätzungen können zusätzlich an Finanzgrößen gekoppelt werden, wie zum Beispiel Verluste im Finanzbereich, durch Produktionsausfall, Konventionalstrafen, Verlust von Absatzmärkten/ Kundengruppen und die daraus resultierenden Ausfälle. Anschließend ist eine Zuordnung vorzunehmen.

### 5.3 Organisatorische Struktur des Risikomanagements

Nachdem die Ausgangssituation analysiert und die Grundlage geschaffen wurden, wird im nächsten Schritt die Organisation des Risikomanagements verbessert. Wichtige Fragestellungen betreffen:

- Risikosteuerungsmaßnahmen und das Risiko-Controlling
- die Bestimmung von Verantwortlichkeiten für Prozesse und Risiken
- die Erarbeitung von Risikomessmethoden (Analytik, Datenbedarf) und Kennzahlen sowie
- die Festlegung des Risikoreportingsystems (Inhalt, Umfang, Adressaten, Frequenz, Eskalationsstufen).

Mit der Ausgestaltung des Risikomanagementsystems ist ebenfalls die Frage zu beantworten, ob und wie dieses in die bestehenden Reporting- und Controllingsysteme zu integrieren ist, bzw. wie die entsprechende IT-Unterstützung hinsichtlich Datenintegration, Schnittstellen und Konsistenz gestaltet wird. Die Erarbeitung entsprechender Konzepte sollte durch eine interdisziplinäre Projektgruppe geschehen.

### 5.4 Verbesserung des Risikomanagements im Unternehmen

Die Verbesserung des Risikomanagements im gesamten Unternehmen erfolgt mittels Schulungen, Einweisungen und einer Bekanntgabe der festgelegten Risikogrundsätze. Hierbei müssen allen Mitarbeitern nicht nur klar und deutlich die Risikogrundsätze kommuniziert werden (auch in schriftlicher Form), sondern auch die dahinterliegenden Beweggründe und Vorteile. Nur ein Mitarbeiter, der das Risikomanagement des Unternehmens versteht, wird später auch in der Praxis in diesem Sinne handeln können und wollen.

Entscheidende Voraussetzung sind entsprechende Kommunikationskanäle und -grundsätze, welche einen offenen Informationsaustausch zwischen allen Beteiligten ermöglichen. Auch hier spielt eine einfach zugängliche Transparenz, die durch eine adäquate Risikomanagementsoftware geschaffen wird, eine wichtige Rolle. Leider fehlt es in der Praxis häufig noch an Lösungen, die Risikoinformationen für "jeden Mitarbeiter" verknüpfen mit den speziellen Informationsanforderungen der im Risikomanagement tätigen Mitarbeiter. Entweder sind beide Informationsstränge weitestgehend entkoppelt und somit die Konsistenz nicht sichergestellt, oder der Schwerpunkt liegt auf den Spezialisten, was die anderen Mitarbeiter weitestgehend außen vor lässt. Beide Probleme reduzieren naturgemäß die Akzeptanz auf Mitarbeiterseite.

### 5.5 Regelmäßige Überprüfung und Anpassung

Nach der Implementierung ist eine regelmäßige Prüfung des Risikomanagements und eine Anpassung an veränderte externe und interne Rahmenbedingungen – gegebenenfalls verbunden mit Anpassungen der Unternehmensorganisation und -struktur – erforderlich. Die Risikomanagementsoftware sollte daher die Möglichkeit bieten, bei der Abbildung von entsprechenden Anforderungserfordernissen die neuen Datenstrukturen durch ein "Umhängen" der alten Strukturen zu bilden. Nur durch ein solches "Mapping" ist es möglich, Daten über viele Jahre hinweg vergleichbar und auswertbar zu machen. Weniger von Bedeutung aber hilfreich ist in diesem Zusammenhang die explizite IT-Unterstützung des kontinuierlichen Überprüfungsprozesses.

## 6. Fazit

Das Risikomanagement gewinnt in den Unternehmen aufgrund der rechtlichen und wirtschaftlichen Rahmenbedingungen zunehmend an Bedeutung. Aufgrund der Komplexität und der Informationsanforderungen ist eine optimale Unterstützung durch eine geeignete Softwarelösung unabdingbar. Allerdings gehen die meisten IT-Lösungen von der reinen Risikoanalytik und -systematik aus und lassen Rahmenbedingungen der Realität außer acht, bzw. überfordern die Anwender. Aus deren Sicht sind u.a. Anforderungen wichtig wie: Systematik von der Konzeption bis zum Betrieb, realistische Erfordernisse an die Datenerhebung, Konfigurierbarkeit für das eigene Unternehmen und die einfache, übersichtliche Bedienbarkeit für alle involvierten Mitarbeiter.

### Literaturverzeichnis

- [1] The Committee of Sponsoring Organizations of the Treadway Commission (COSO) (Hrsg.), Enterprise Risk Management Framework, 2004
- [2] O. V., Stiefmütterliches Risikomanagement, in: Frankfurter Allgemeine Zeitung, 22. August 2005, S. 20
- [3] BARC, Motor für Corporate Governance, Würzburg 2005
- [4] Dörner, D./Horvath, P./Kagermann, H. (Hrsg.), Praxis des Risiko-

managements – Grundlagen, Kategorien, branchenspezifische und strukturelle Aspekte, Stuttgart 2000

Romeike, F. (Hrsg.), Modernes Risikomanagement – Die Markt-, Kredit- und operationellen Risiken zukunftsorientiert steuern, Weinheim 2004

[5] Servatius, H. G., Strategische Führungsprozesse im Real-Time Business, in: Information Management & Consulting, 19. Jg., 2004, Nr. 2, S. 25 – 31

[6] Dertouzos, M., The Unfinished Revolution – Human-Centered Computers and What They Can Do for Us, New York 2001

[7] Hofmann, D.G., Managing Operational Risk – 20 Firmwide Best Practice Strategies, New York 2002, Keitsch, D., Risikomanagement, 2. Aufl., Stuttgart 2004

### Autoren

Prof. Dr. rer. pol. habil. Dipl.-Ing. Hans-Gerd Servatius ist Gesellschafter und Geschäftsführer der Haarmann Hemmelrath Management Consultants GmbH in Düsseldorf. Daneben lehrt er Strategie und Innovation an der Universität Stuttgart



Berliner Allee 15  
40212 Düsseldorf  
www.haarmannhemmelrath.com  
Tel.: 0211/8399-260  
Fax.: 0211/8399-333  
Email: gerd.servatius@haarmannhemmelrath.com  
www.haarmannhemmelrath.com

Lars Sørstrøm, Dipl.-Phys. Dipl.-Kfm. ist Managing Partner der BERGEN BRYGGEN GROUP Managements Consultants GmbH



Düsseldorfer Straße 21  
40545 Düsseldorf  
Tel.: 0211/171841-0  
Fax.: 0211/171841-1  
Email.: lsoerstroem@bergenbryggen.com  
www.bergenbryggen.com

## IT Supported Risk Management – A User Perspective

User who want to implement risk management solutions are confronted with an increasing complexity of software products. The "ideal" IT support would follow an evolutionary concept, which becomes more sophisticated with growing user experience.