Risiko Management 2004

Mit Risiken umgehen 1

Umfrage 3

Formale Richtlinien 6

Ausgestaltung des internen Umfeldes (Internal Environment) 8

Klare Unternehmenszielsetzungen (Objective Setting) 10

Erfassung zielgefährdender Ereignisse (Event Identification) 12

Risiko- und Chancenbeurteilung (Risk Assessment) 14

Risikooptimierung (Risk Response) 16

Überwachung (Control Activities) 18

Reporting (Information and Communication) 20

Monitoring des Risikomanagement-Systems (Monitoring) 22

Funktionsträger 24

Schlussbemerkungen 25

Mit Risiken umgehen

Das Risiko haftet dem Gewinn an den Fersen wie ein Schatten. Weder Unternehmen noch die öffentliche Hand oder nicht-gewinnorientierte Organisationen agieren im risikofreien Raum. Die Risiken zu erkennen und damit umzugehen ist Aufgabe des unternehmerischen Risikomanagements («Enterprise Risk Management», ERM). Als Baustein der Corporate Governance hat es in jüngster Zeit deutlich an Stellenwert gewonnen.

Verwaltungsrat und Management kommt in verschiedenen aufsichtsrechtlichen Vorstössen (Swiss Code of Best Practice for Corporate Governance, Sarbanes Oxley-Act) die Aufgabe zu, für die Einrichtung und den Unterhalt von ausreichenden internen Kontrollen über die Finanzberichterstattung zu sorgen. Das betreffende Risikomanagement-System ist regelmässig auf die Funktionstüchtigkeit und Angemessenheit zu prüfen.

Ein Risikomanagement-System ist nicht Selbstzweck. Vielmehr dient es der Führung des Unternehmens. Die Ziele eines ausgewogenen Risikomanagements sind...

- die Verknüpfung von Wachstum, Risiko und Gewinn
- die Identifikation von unternehmerischen Chancen
- die Verknüpfung von Risikobereitschaft und Unternehmensstrategie
- die Verbesserung der Kommunikation und des Umgangs mit Risiken und Chancen
- die Verhinderung unternehmerischer Überraschungen und die Minimierung von Verlusten
- die Identifikation und das Management von unternehmensübergreifenden Risiken und Chancen
- die integrierte Betrachtung interdependenter Risikofaktoren
- die Rationalisierung des Kapitaleinsatzes.

So einleuchtend und notwendig diese Zielsetzungen sind, so uneinheitlich und unklar ist die Terminologie, die Ausgestaltung und die Einführung eines angemessenen Risikomanagement-Systems. Die am weitesten beachtete Initiative zur Schliessung dieser Lücke geht vom «Committee of Sponsoring Organizations of the Treadway Commission» (COSO) aus. Das «Enterprise Risk Management Framework» – kurz COSO-ERM-Framework[1] – definiert die Komponenten eines angemessenen Risikomanagement-Systems. Damit steht erstmals eine standardisierte und vergleichbare Vorgehensweise zur Verfügung.

Im Rahmen des Audit Committee Institute (ACI) von KPMG Schweiz[2] setzen sich Verwaltungsrats- und Geschäftsleitungs-Mitglieder sowie Experten aus Wissenschaft und Praxis regelmässig mit dem Thema Risikomanagement auseinander. Das ACI ist eine Plattform für den Erfahrungsaustausch und die Wissensvermittlung. Dies trägt dazu bei, die Diffusion dieses wichtigen Themas in der Schweiz in den Unternehmen zu beschleunigen.

[1] Zur Zeit als Entwurf verfügbar; Stellungnahme abgeschlossen, definitive Version wird nächstens erwartet
[2] Weitere Informationen zum ACI finden Sie unter www.auditcommittee.ch

KPMG hat die gegenwärtige dynamische Entwicklung zum Anlass genommen, Unternehmen in der Schweiz nach dem Status ihres Risikomanagement-Systems zu befragen. Aus der Umfrage im Kreis der Verwaltungsräte leiten sich Handlungsfelder für Unternehmen, aber auch Revisoren und Aufsichtsbehörden ab. Die bisher in der Schweiz einzigartige Umfrage ohne wissenschaftlichen Anspruch hilft, bestehende Lücken in den Risikomanagement-Systemen zu identifizieren. Eine kürzlich verfasste Studie von KPMG zum Thema «Früherkennung und Überwindung von Unternehmensrisiken» zeigte, dass erst 44% der Unternehmen über ein institutionalisiertes Risikomanagement System verfügen. In dieser Studie gaben 30 Prozent der Unternehmen an, über ein umfassendes Risikomanagement-System verfügen.

KPMG Schweiz

Unterschriften

Dieter Widmer

Günter Haag

Umfrage

Was ist Risikomanagement?

Risikomanagement bezweckt, durch den bewussten Umgang mit Chancen und Risiken die Zielsetzungen einer Organisation zu erreichen bzw. zu übertreffen. Beurteilt werden Ereignisse, Handlungen und Entwicklungen, die eine Unternehmung daran hindern können, die Zielsetzungen zu erreichen bzw. ermöglichen, diese zu übertreffen, und die Strategien erfolgreich umzusetzen.

Das COSO-ERM-Framework unterstützt Unternehmen und nicht-gewinnorientierte Organisationen bei der Einführung und Umsetzung eines angemessenen Risikomanagements. Das Framework definiert erstmals und bisher einmalig die umfassenden Prinzipien und zentralen Schritte. Es dient als gemeinsame Basis und Sprache für Verwaltungsrat, Management, Aufsichtsbehörden und Wissenschaft.

Die im Rahmen des COSO-ERM-Framework festgelegten Komponenten sind in ihrer Gesamtheit eine unabdingbare Voraussetzung für ein lückenloses Risikomanagement. Diese sind auf die Führung des Unternehmens abgestimmt und sind Bestandteil des Managementprozesses.

Das COSO-ERM-Framework bildet auch die Struktur der Umfrage, die KPMG Schweiz Ende 2003 im Rahmen des Audit Committee Institute durchführte. Insgesamt wurden 146 Fragebogen an Verwaltungsratsmitglieder mittlerer und grösserer Schweizer Unternehmen verschickt. Der Rücklauf von 50 Fragebogen ergibt eine beachtliche Quote von 34%. Die nachfolgende Übersicht zeigt eine Gliederung in Unternehmen mit mehr resp. weniger als 2000 Mitarbeitenden sowie nach Branchen in Finanz- und Nicht-Finanzsektor.

Die erfassten Unternehmen im Überblick
Von den befragten Unternehmen beschäftigen 34% mehr als 2000 Mitarbeiter. Davon verfügen knapp die Hälfte über ein Risikomanagement-System. Bei den Unternehmen mit weniger als 2000 Mitarbeitern verfügt nur jede fünfte Organisation über ein institutionalisiertes Risikomanagement.

Rund die Hälfte der befragten Finanzdienstleistungsunternehmen (22% der erhaltenen Antworten) hat angegeben, über ein Risikomanagement-System zu verfügen; der Anteil bei den anderen Branchen liegt bei 20%. Insgesamt zeigt sich daraus, dass über alle Branchen hinweg bereits 30% ein Risikomanagement-System implementiert haben.

Von den Unternehmen sind 28% ausschliesslich in der Schweiz tätig. Weitere 12% verfügen über Tochtergesellschaften in bis zu 3 Ländern, 30% in 4 bis 10 Staaten, 14% in 11 bis 30 Nationen und 10% in mehr als 30 Ländern (6% ohne Angabe).

Die Ergebnisse sind in der Folge in Unternehmen einerseits mit einem umfassenden Risikomanagement-System und anderseits solche ohne bzw. nur mit Risikomanagement-System in Teilbereichen des Unternehmens dargestellt. Dies ermöglicht den besseren Vergleich der betreffenden Erkenntnisse, da diese im Gruppenvergleich sehr unterschiedlich ausfallen. Der Gruppe der Unternehmen ohne Risikomanagement-System wurden jene Gesellschaften zugeteilt, die nach eigenen Angaben kein oder nur in Teilbereichen ein systematisches Risikomanagement-System unterhalten.

Um die Wirkung des Risikomanagement-Systems entfalten zu können, müssen die Komponenten des COSO-ERM-Frameworks vorhanden, dokumentiert und kommuniziert sein. Als kommuniziert gilt das Risikomanagement-System, wenn alle Mitarbeitenden stufengerecht über den Inhalt und die Systematik des Risikomanagement-Systems informiert sind. Die Ergebnisse werden einem identifizierten Kreis von Adressaten in geeigneter Form (z.B. in Risk Maps) zur Kenntnis gebracht.

In der Studie wurden die Verwaltungsratsmitglieder deshalb befragt, ob die Komponenten des COSO-ERM-Frameworks erstens vorhanden, zweitens dokumentiert und drittens kommuniziert sind.

Überblick über die Ergebnisse
Aus der Umfrage ergibt sich folgende Zusammenfassung der Ergebnisse:

- Risikomanagement-Systeme sind über Branchengrenzen und Unternehmensgrössen hinweg vorhanden.
- 30% der antwortenden Unternehmen verfügen über ein umfassendes und integriertes System.
- 70% der Unternehmen geben an, über kein umfassendes System zu verfügen. Die meisten dieser Unternehmen betreiben hingegen ein systematisches und dokumentiertes Risikomanagement in einzelnen Teilbereichen.
- Der Finanzsektor weist tendenziell eine höhere Durchdringung von Risikomanagement-Systemen auf als die übrigen Branchen. 45% der Banken und Versicherungen haben ein entsprechendes System implementiert. In den übrigen Branchen sind es erst 26%.
- Grössere Unternehmen mit mehr als 2000 Mitarbeitenden verfügen eher über ein Risikomanagement-System (47%) als mittlere mit weniger als 2000 Angestellten (21%). Unternehmen mit komplexeren Strukturen und solche mit Vertretungen im Ausland verfügen eher über ein Risikomanagement-System.
- Viele Komponenten des Risikomanagement-Systems sind zwar vorhanden, werden aber nur teilweise dokumentiert und noch weniger häufig kommuniziert.
- 60% der Unternehmen mit Risikomanagement-System bewerten nicht sämtliche Risiken und Chancen.
- Die Funktion des Chief Risk Officers ist in 60% der Unternehmen mit einem Risikomanagement-System etabliert. Bei Unternehmen mit einem Risikomanagement System geben ebenfalls 80% der Verwaltungsratsmitglieder an, dass die Interne Revision das Risikomanagement unterstützt.
- Interne Projekte (z.B. Einführung neuer Software, Restrukturierung) werden im Rahmen des Risikomanagements vergleichsweise selten geprüft.
- Risiken- und Chancenmodelle mit einer Übersicht über alle möglichen Ereignisse mit negativen wie auch positiven Auswirkungen auf die Unternehmensziele sind auch bei Unternehmen mit Risikomanagement-System nicht immer vorhanden.
- Im Bereich der Reportingstrukturen besteht auch bei Unternehmen mit Risikomanagement-System ein Verbesserungspotential.

Formale Richtlinien

«Das Risikomanagement-System ist ein zentraler Baustein der unternehmensweiten Assurance und ein wichtiges Instrument in der Unternehmensführung.»
Dave Schnell

«In welchen Bereichen in Ihrer Unternehmung sind formale Richtlinien vorhanden?»
Die Antworten der Unternehmen zeigen grosse Unterschiede zwischen den verschiedenen Risikobereichen. Finanzielle Risiken und solche im Bereich des Treasury werden am besten abgedeckt. Insgesamt geben 74% der Verwaltungsräte an, dass hier formale Richtlinien existieren. Hier werden demnach die grössten unternehmerischen Risiken geortet bzw. tritt der finanzielle Schaden am offensichtlichsten zu Tage. Auf der anderen Seite des Spektrums steht die Prüfung von internen Projekten mit lediglich 24% der Nennungen.
Daraus lässt sich schliessen, dass die Risiken solcher Projekte als untergeordnet eingeschätzt oder die Mehrkosten für eine Projektprüfung gescheut werden. Angesichts der Tragweite, die interne Projekte jedoch haben können – zu nennen sind beispielsweise Restrukturierungen und IT-Projekte – dürften diese Risiken und auch die damit verbundenen Chancen eher unterschätzt werden.

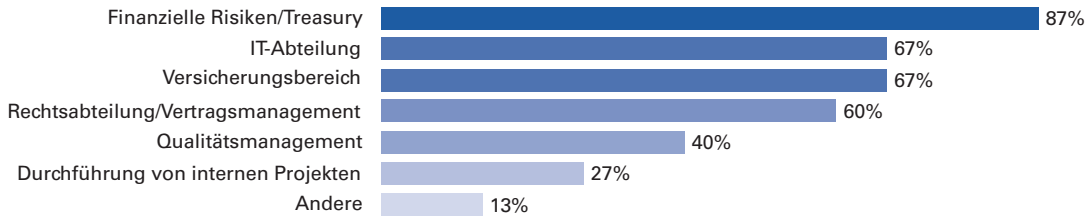
Unternehmen ohne Risikomanagement-System
Unternehmen ohne Risikomanagement-System zeichnen sich gerade dadurch aus, dass formale Richtlinien nicht vorhanden sind. Immerhin werden auch hier finanzielle Risiken und solche im Bereich des Treasury besonders häufig analysiert. 69% der Verwaltungsräte geben an, dass dieser Bereich in ihrem Unternehmen systematisch geprüft werde. Hier manifestiert sich ein Nachholbedarf bei der Ausdehnung auf sämtliche Unternehmensbereiche.

Unternehmen mit Risikomanagement-System

Erwartungsgemäss sind die verschiedenen Risikobereiche in den Unternehmen mit einem umfassenden Risikomanagement-System häufiger in formalen Richtlinien dokumentiert. Auch hier schwingen die finanziellen Risiken und solche im Bereich des Treasury obenaus. Auffallend ist der Unterschied zu den Unternehmen ohne Risikomanagement-System hinsichtlich der Versicherungen. 67% der Unternehmen mit einem Risikomanagement System geben an, diesen Bereich abzudecken währenddem nur 34% der Unternehmen ohne ein solches System über formale Richtlinien verfügen. Die finanzielle Tragweite – gemäss unserer Erfahrung schätzen wir, dass nur rund 10% bis 15% der unternehmerischen Risiken im Durchschnitt überhaupt versicherbar sind – wird demnach von den beiden Unternehmensgruppen sehr unterschiedlich eingeschätzt.

Die Risiken in den IT-Bereichen werden nach Massgabe der Nennungen ebenfalls als überdurchschnittlich hoch eingestuft, was sich entsprechend im höheren Formalisierungsgrad niederschlägt.

Bereiche mit formalen Richtlinien



Ausgestaltung des internen Umfeldes (Internal Environment)

«Nur durch eine konsequente Integration aller Aktivitäten, die in ein unternehmerisches Risikomanagement-System münden, kann sich im Unternehmen eine eigentliche Risikokultur entwickeln. Die (Weiter-) Entwicklung des Risikomanagements bedingt ein Change-Management. Dieser Kulturwandel muss durch den Verwaltungsrat und die Geschäftsleitung initiiert werden.»
Flemming Ruud, Universität Zürich

«Wie ist das interne Umfeld des Risikomanagement-Systems ausgestaltet?»
Das interne Umfeld des Unternehmen bildet die Grundlage für sämtliche Komponenten des Risikomanagement-Systems. Es hat einen massgeblichen Einfluss darauf, wie unternehmerische Strategien, Zielsetzungen und Geschäftsaktivitäten etabliert sowie Risiken identifiziert und behandelt werden. Der Aufbau und das Funktionieren der Kontrollaktivitäten, des Informations- und Kommunikations- sowie Überwachungssystems sind vom internen Umfeld beeinflusst. Ethische Werte, Kompetenz, Entwicklung der Mitarbeitenden, Managementstil, Risikobereitschaft, Risikokultur und Verantwortung sind die wesentlichen Komponenten des Umfeldes. Dem Verwaltungsrat und insbesondere den unabhängigen Verwaltungsrats-Mitgliedern kommt bei der Ausgestaltung eine entscheidende Rolle zu.

Unternehmen ohne Risikomanagement-System
Unternehmen ohne Risikomanagement-System haben zumeist keine Risikomanagement-Philosophie oder -Strategie definiert. Gleichzeitig findet in einigen der erfassten Unternehmen keine Mitarbeit eines unabhängigen Verwaltungsrat-Mitgliedes bei der Unternehmensüberwachung sowie der Festlegung der Unternehmensethik und -kultur statt. Rund 50% der erfassten Unternehmen erfüllen diese beiden Kriterien nicht oder lediglich teilweise.

Unternehmen mit Risikomanagement-System

Die erforderlichen Bedingungen des internen Umfeldes werden auch von den Unternehmen mit Risikomanagement-System nur teilweise erfüllt, jedoch mit einer deutlich höheren Quote. So verfügen 33% über keine Risikomanagement-Philosophie und -Strategie, welche die Basis und Leitplanken für das gesamte Risikomanagement darstellen würde.

20% der Unternehmensvertreter geben an, dass die Organisationsstruktur mit Zuteilung von Kompetenzen und Verantwortlichkeiten nicht oder nur teilweise festgelegt sei. In diesen Unternehmen herrscht somit Unklarheit darüber, wer die Verantwortung für die systematische Risikobeurteilung, die entsprechenden Massnahmen zur Risikosteuerung sowie für die stufen- und zeitgerechte Risikoberichterstattung trägt. Die geringste Durchdringung haben Richtlinien zur Unternehmensethik und -kultur. Angesichts der öffentlichen Diskussion manifestiert sich hier ein Nachholbedarf.

Ausgestaltung Internes Umfeld

Klare Unternehmenszielsetzungen

(Objective Setting)

«Die äusserst erfolgreiche Entwicklung und das Erreichen von zentralen Zielen wie die langfristige Zukunftssicherung aller Stakeholder, die langfristige Sicherung der Finanzen sowie die Verhinderung einer möglichen unfreundlichen Übernahme waren nur dank eines guten, proaktiven Risikomanagements möglich.»
Etienne Jornod, Galenica Gruppe

«Wie werden die Zielsetzungen Ihres Unternehmens bestimmt?»
Im Rahmen der Risikomanagement-Philosophie und -Strategie setzt das Management Ziele und Strategie fest. Diese sind die unabdingbare Grundlage für die Identifikation von potentiellen Risiken und Chancen auf dem Weg zu den Unternehmenszielen. Das unternehmerische Risikomanagement stellt sicher, dass dem Management Prozesse zur Verfügung stehen, um Strategie, Risikobereitschaft und Risikomanagement-Instrumente aufeinander abzustimmen.

Die Unternehmenszielsetzungen sind aus dem Blickwinkel des Risikomanagements hinsichtlich...

- ihrer Übereinstimmung mit der übergeordneten Strategie,
- der Effektivität und Effizienz aus operativer Warte,
- des internen und externen Reportings und
- ihrer Übereinstimmung mit den geltenden Gesetzen und Regulierungen (Compliance)

zu überprüfen.

Unternehmen ohne Risikomanagement-System
Zwar verfügen alle Unternehmen dieser Gruppe über eine greifbare Unternehmensstrategie, davon abgeleitete quantifizier- und messbare Zielsetzungen sind hingegen nur bei 57% der Firmen umfassend festgelegt und nur 34% kommunizieren diese. In der Hälfte der Gesellschaften sind die unternehmerischen Ziele nur in den Köpfen des Managements vollständig verankert, nicht jedoch auf Papier festgehalten. Hinsichtlich des Risikomanagements liessen sich deutliche Verbesserungen erzielen, wenn den Mitarbeitenden die Unternehmensstrategie bekannt wäre und sie somit den Risiken und Chancen besser begegnen könnten.

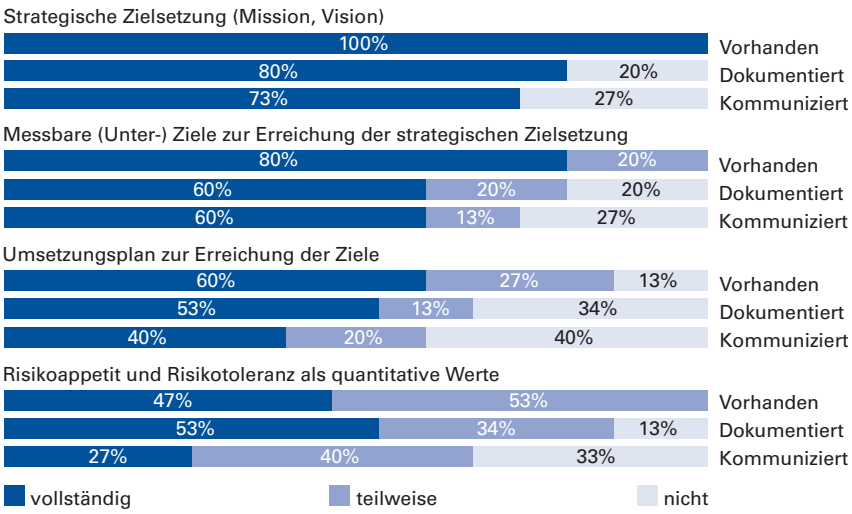
Lediglich 40% der erfassten Unternehmen setzen sich mit der eigenen Risikofähigkeit auseinander. Dies lässt die Vermutung zu, dass teilweise auch Risiken eingegangen werden, die das Mass des Verkraftbaren ungewollt übersteigen. Diese Erkenntnis kontrastiert deutlich zu den Unternehmen mit Risikomanagement-System.

Unternehmen mit Risikomanagement-System

Während alle Unternehmen mit einem Risikomanagement-System ihre strategischen Zielsetzungen formuliert haben, fehlt es in dieser Gruppe ebenfalls an den weiteren Detaillierungsschritten. Messbare Ziele und Umsetzungspläne werden deutlich weniger häufig definiert, festgehalten und kommuniziert. Letztere sind den betroffenen Stellen und Abteilungen gar nur in 40% der erfassten Gesellschaften vollumfänglich bekannt.

Risikobereitschaft und Risikofähigkeit werden in allen Unternehmen vollumfänglich oder teilweise ermittelt, jedoch nur in 27% der erfassten Gesellschaften auch detailliert kommuniziert. Dies zeigt, dass die Umsetzung eines umfassenden Risikomanagements noch nicht vollumfänglich abgeschlossen wurde.

Bestimmung Zielsetzungen



Erfassung zielgefährdender Ereignisse (Event Identification)

«Die Vergangenheit ist nicht identisch mit der Zukunft. Wer bei der Beurteilung seiner Risiken und Chancen nicht versucht, die möglichen künftigen Veränderungen zu formulieren, bildet nur einen Teil des Gesamtbildes ab.»
Andreas Koopmann, Nestlé, SIG Holding AG

«Sind die möglichen zielgefährdenden Ereignisse bekannt?»
Um die Risiken und Chancen beurteilen zu können, sind diese zuerst zu identifizieren. Das Ziel ist eine abschliessende Auflistung aller zielgefährdenden Ereignisse, wobei sowohl interne wie auch externe Faktoren berücksichtigt werden müssen. Die Suche nach Risiken richtet sich nicht nur auf die Vergangenheit, sondern ebenso auf mögliche zukünftige Ereignisse aus. Im Weiteren sind Risiken und Chancen nicht statisch. So können Ereignisse, deren Potential bei einer früheren Prüfung als nicht existenzgefährdend eingestuft wurde, im schlimmsten Fall zu einem Konkurs führen. Gleichzeitig bestehen zwischen den Ereignissen u.U. Interdependenzen, die zu einer Kumulation führen. Diese gilt es in einer Gesamtschau zu erfassen.

Für die Identifikation derartiger Ereignisse stehen verschiedene Instrumente und Informationsquellen zur Verfügung. Vergangenheitsbezogene Informationen beruhen zum Beispiel auf Debitorenausfällen, Garantieleistungen oder Wechselkursentwicklungen. Die zukunftsgerichtete Suche nach möglichen Risikopotentialen zieht beispielsweise demographische Entwicklungen, neue Märkte, Konkurrentenstrategien oder technologische Entwicklungen in Betracht.

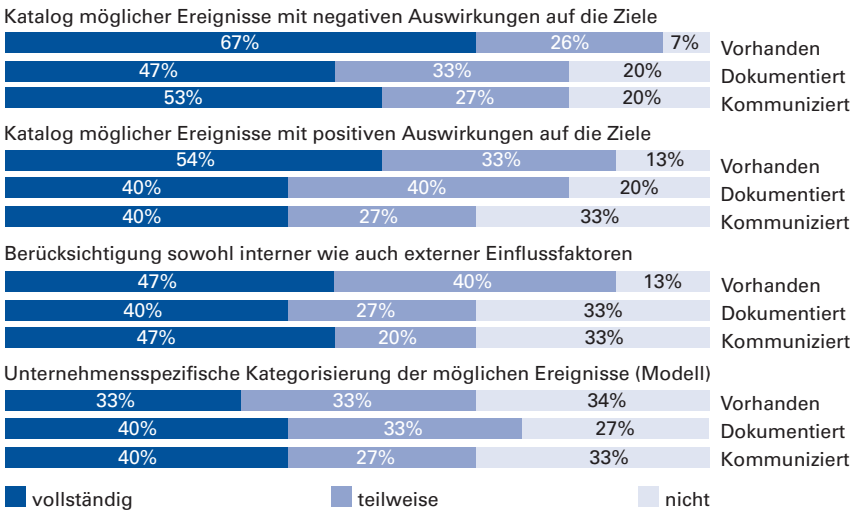
Unternehmen ohne Risikomanagement-System
Vereinzelt haben Unternehmen mögliche Ereignisse mit negativen und positiven Auswirkungen auf die Unternehmensziele erhoben. Eine Kategorisierung in Form eines eigentlichen Risiko- und Chancenmodells existiert jedoch kaum. Dieses Modell würde die Unternehmen dabei unterstützen, mögliche aussergewöhnliche und nicht alltägliche Ereignisse frühzeitig zu erkennen.

Unternehmen mit Risikomanagement-System
Mit wenigen Ausnahmen führen alle Unternehmen eine Bestandesaufnahme der möglichen zielgefährdenden Ereignisse durch. Positiv zu werten ist die Erkenntnis, dass nur unmerklich weniger Unternehmen nicht nur potentielle negative Ereignisse (Risiken), sondern auch positive Auswirkungen (Chancen) erfassen.

87% der Verwaltungsräte geben an, dass in ihren Unternehmen sowohl interne wie auch externe Ereignisse berücksichtigt oder teilweise berücksichtigt würden. Erfahrungsgemäss werden externe Faktoren häufiger vernachlässigt als interne. Dies erklärt sich mit der schwierigen Erfassbarkeit und der fehlenden Beeinflussbarkeit. Die Auseinandersetzung mit diesen Grössen und Einflüssen würde jedoch die Erarbeitung von Konzepten und Reaktionen auf solche Veränderungen unterstützen.

Das grösste Defizit besteht gemäss der Umfrage bei der Kategorisierung der Ereignisse. Lediglich 33% der Unternehmen verfügen über ein umfassendes Risiko- und Chancenmodell. Unstrukturierte Listen können in Missverständnissen und einer ablehnenden Haltung der Mitarbeiter münden. Ausserdem ist die Gefahr gross, dass nicht alle wesentlichen Gebiete erfasst werden. Darum sollte nicht auf ein unternehmensspezifisches Modell für die Auflistung der Risiken und Chancen verzichtet werden.

Erfassung Risiken



Risiko- und Chancenbeurteilung

(Risk Assessment)

«Neben den kurzfristigen Profiten muss vor allem die mittel- und langfristige Ertragsfähigkeit gefördert werden. Es gilt, eine eigenständige Risikokultur zu entwickeln.»
Fritz Rufer

«Wie erfolgt die Beurteilung/Bewertung der möglichen zielgefährdenden Ereignisse?»
Nach der Identifikation möglicher Ereignisse folgt die Beurteilung derselben im Rahmen eines Risk Assessment. Dieses erlaubt es einer Organisation festzulegen, mit welcher Eintretenswahrscheinlichkeit (in Prozent) und welchem Auswirkungspotential (in Franken) ein bestimmtes Ereignis das Erreichen der Unternehmensziele beeinflusst. Auf dieser Grundlage kann die tatsächliche Risiko- und Chancensituation eines Unternehmens ermittelt werden.

Die Risikobeurteilung erfolgt stufen- und organisationsgerecht. Die Beurteilung von Einzelrisiken ist beispielsweise für die oberste Führungsebene soweit zu aggregieren, dass die Zahl der Risiken überschaubar bleibt. Das Überblicken von 80 verschiedene Risiken erfordert bereits eine erhöhte Aufmerksamkeit, während sich ein Katalog von über 300 Risiken kaum noch mit der notwendigen Qualität durch eine Person beurteilen lässt. So ist es für den CEO nicht möglich und nicht stufengerecht, sämtliche mögliche Detailereignisse zu beurteilen, die zu Produktionsausfällen führen können. Demgegenüber sollte sich der Produktionsleiter über alle betreffenden Einzelrisiken ein Bild machen können.

Bei der Beurteilung wird zwischen Bruttorisiko und aktuellem Restrisiko unterschieden. Das Bruttorisiko stellt das Risikopotential dar, das ohne Berücksichtigung der bereits wirksamen Massnahmen in der Natur des Geschäfts liegt. Das aktuelle Restrisiko zieht dagegen die bereits wirksamen Massnahmen in Betracht (Prozesse, interne Kontrollen, Versicherungen usw.).

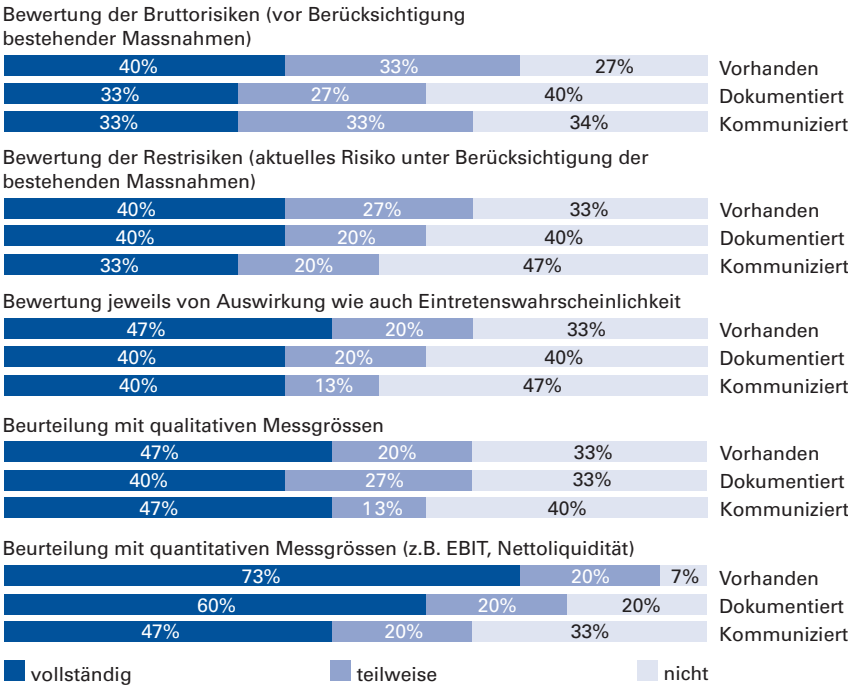
Unternehmen ohne Risikomanagement-System
Unternehmen ohne Risikomanagement-System verfügen typischerweise über keinen umfassenden Risiko- und Chancenkatalog und können demzufolge keine umfassende Beurteilung der Risiken und Chancen vornehmen. Hier zeigt sich ein wesentlicher Nachholbedarf für diese Gesellschaften, auch wenn rund die Hälfte der antwortenden Verwaltungsrats-Mitglieder angibt, eine solche (unvollständige) Bewertung vorzunehmen.

Unternehmen mit Risikomanagement-System

Auf die Fragen nach der Beurteilung der möglichen zielgefährdenden Ereignisse antworten jeweils rund 70% der Vertreter, ihr Unternehmen würde eine solche sowohl nach Bruttomassstäben, nach Restrisiko, nach Eintretenswahrscheinlichkeit und Auswirkungspotential sowie nach qualitativen Messgrössen durchführen. Damit ist umgekehrt der Anteil der Unternehmen, die keine Bewertungen vornehmen, mit rund 30% nach wie vor gross. Eine Priorisierung und Abschätzung des Auswirkungspotentials ist ohne Bewertung nicht möglich.

Quantitative Messgrössen sind weit verbreitet. 93% geben an, teilweise oder vollständig auf Zahlen wie EBIT, Nettoliquidität usw. abzustellen. Darin kommt deren einfachere Visualisierung, Vergleichbarkeit und Verständlichkeit zum Ausdruck, während qualitative Kriterien schwerer greifbar sind.

Bewertung Risiken



Risikooptimierung (Risk Response)

«Risikomanagement spielt bei Akquisitionen eine wichtige Rolle. Keine Übernahme sollte ohne klare Vorstellung der Risiken für das Gesamtunternehmen erfolgen. Zum Risikomanagement gehört auch der Mut, nein zu sagen. Auch wenn damit wichtige Kunden verloren gehen.»
Paul Otth

«Wie erfolgt die Entscheidung zur Riskooptimierung (Aktionsplan mit Massnahmen)?»
Im Rahmen der Risikooptimierung steht die Verbesserung der vorgängig festgestellten Risikoposition im Zentrum. Ziel ist es, mit Hilfe der gewonnen Informationen Massnahmen zur besseren Erreichung der Unternehmensziele einzuleiten.

Risiken können durch geeignete Massnahmen vermieden, verringert oder übertragen werden. Die Vermeidung des betreffenden Risikos bedingt den Verzicht auf die betreffende Tätigkeit, während die Verringerung auf die Senkung der Eintretenswahrscheinlichkeit und das Auswirkungspotential abzielt. Mit Massnahmen zum Risikotransfer oder Risiko-Sharing werden Risiken zum Beispiel an eine Versicherungsgesellschaft übertragen oder durch Geschäftspartner, Kunden oder Lieferanten mitgetragen. Schliesslich können Risiken aber auch im Rahmen der eigenen Risikofähigkeit angenommen werden. Für jedes signifikante Risiko können mit diesen Massnahmen alternative Strategien erarbeitet werden.

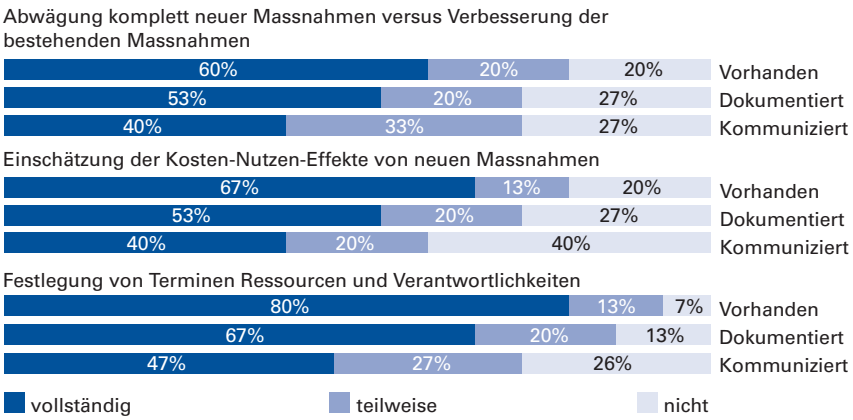
Unternehmen ohne Risikomanagement-System
Erwartungsgemäss setzt sich nur ein kleiner Anteil der Unternehmen ohne Risikomanagement-System mit der Risikooptimierung und einem Aktionsplan auseinander. Ohne eine systematische Erfassung und Beurteilung möglicher Ereignisse erschöpfen sich die eingeleiteten Massnahmen in einer reaktiven Vorgehensweise beim Auftreten oder Bekanntwerden von Risiken oder Kontrolllücken.

Unternehmen mit Risikomanagement-System

Risikooptimierung kann auch beinhalten, bereits eingeleitete Massnahmen zu hinterfragen und gegebenenfalls durch neue zu ersetzen. 60% der Unternehmensvertreter geben an, dass ihr Unternehmen in allen Fällen vor der Implementierung neuer Massnahmen die Verbesserung bereits eingeleiteter Massnahmen abwägt. Dabei spielt das Kosten-Nutzen-Verhältnis neben der eigentlichen Risikooptimierung eine mitentscheidende Rolle. Nicht zuletzt aus Kostenüberlegungen geben 80% der Unternehmen an, eine Kosten-Nutzen-Erwägung in jedem Fall oder teilweise durchzuführen. Ausnahmen von diesem Grundsatz sind vor allem dort angezeigt, wo die Risikofähigkeit des Unternehmens auch in aufsichtsrechtlicher Hinsicht überschritten wird und eine Reduktion unter allen Umständen angezeigt ist.

Noch konsequenter gehen die Unternehmen bei der Festsetzung von Terminen, Ressourcen und Verantwortlichkeiten vor. Lediglich 7% der Unternehmen geben an, Massnahmen nicht in dieser Weise zu konkretisieren.

Entscheidung Risikooptimierung



Überwachung (Control Activities)

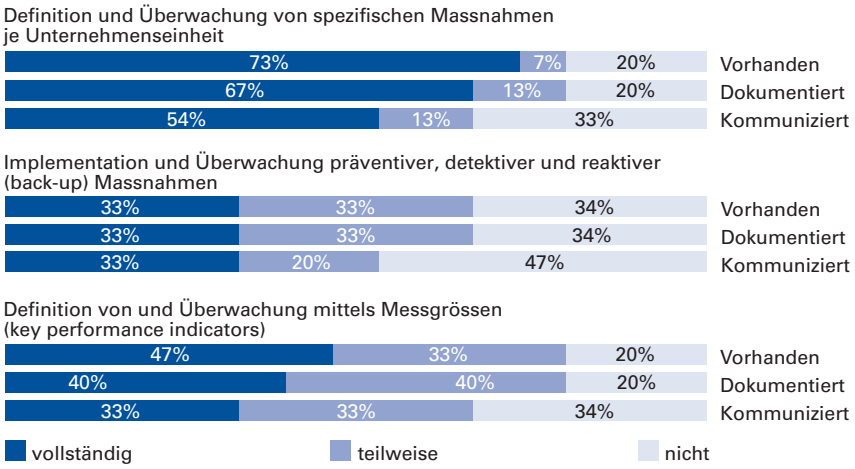
«Wie erfolgt die Risikosteuerung und Überwachung der Massnahmenumsetzung?»
Aufgabe der Überwachung ist es dafür zu sorgen, dass Massnahmen zur Risikooptimierung in der vorgesehenen Weise umgesetzt werden und zum angestrebten Ergebnis führen. Kontrollaktivitäten sind integraler Bestandteil des Unternehmensprozesses.

Unternehmen ohne Risikomanagement-System
Die Absenz einer systematischen Überwachung der Massnahmenumsetzung deckt sich mit dem bisherigen Bild über Unternehmen ohne Risikomanagement-System. Ausnahme bilden jene Gesellschaften, die sich systematisch und umfassend den für sie relevanten Teilgebieten widmen.

Unternehmen mit Risikomanagement-System

80% der Verwaltungsräte geben an, in ihrem Unternehmen Massnahmen je Unternehmenseinheit teilweise oder vollumfänglich zu überwachen. Key Performance Indicators dienen in vier von fünf Fällen als Messgrössen; lediglich 20% der Unternehmen nutzen diese Parameter nicht.

Überwachung Massnahmeumsetzungen



Reporting (Information and Communication)

«Ein effektiver und effizienter Risikomanagement-Prozess ermöglicht einem Unternehmen die Früherkennung, Minimierung und Bewältigung von Gefahren und Risiken sowie die Identifikation und Realisation unternehmerischer Chancen. Risikomanagement ist nicht eine «lästige Pflichtübung», sondern vielmehr ein wirkungsvolles Mittel zur Verbesserung der Wettbewerbsfähigkeit. Modernes Risikomanagement ist ein unerlässliches Führungs- und Kontrollinstrument, das es aktiv einzusetzen gilt.»
Dieter Widmer, KPMG Schweiz

«Welche Gliederung des Risikomanagement-Systems bezüglich Information und Kommunikation ist vorhanden?»
Informationen aus internen und externen Quellen haben eine zentrale Bedeutung im Risikomanagement. Sie müssen adäquat und fristgerecht zur Verfügung stehen, damit die mit dem Risikomanagement und den daraus abgeleiteten Massnahmen betrauten Personen ihre Verantwortung wahrnehmen können. Informationen fliessen nicht nur Bottom-up oder Top-down, sondern ebenso quer über Abteilungs-, Funktions- oder Divisionsgrenzen hinweg. Gleichsam findet ein Austausch mit externen Stellen wie beispielsweise Lieferanten, Aktionären, Kunden und Kreditgebern statt.

Informationen sind auf allen Stufen des Unternehmens erforderlich, um Risiken zu erkennen, einzuschätzen und schliesslich gezielte Massnahmen zu ergreifen. Die Herausforderung besteht jedoch darin, grosse Datenmengen – unter Zuhilfenahme von Informationssystemen – zu adäquaten Informationen zu verdichten.

Unternehmen ohne Risikomanagement-System
Ein Reporting fehlt bei dieser Unternehmensgruppe fast vollständig, was angesichts der Lücken im Aufbau des Risikomanagement-Systems nicht überrascht. Der Unternehmensführung und dem Verwaltungsrat stehen demzufolge keine angemessenen Informationen über wesentliche Veränderungen der Risiken zur Verfügung. In über 50% der Gesellschaften sind weder der sachliche Detaillierungsgrad des Reportings, noch der zeitliche Rahmen oder die Informations- bzw. Kommunikationswege und Tools definiert.

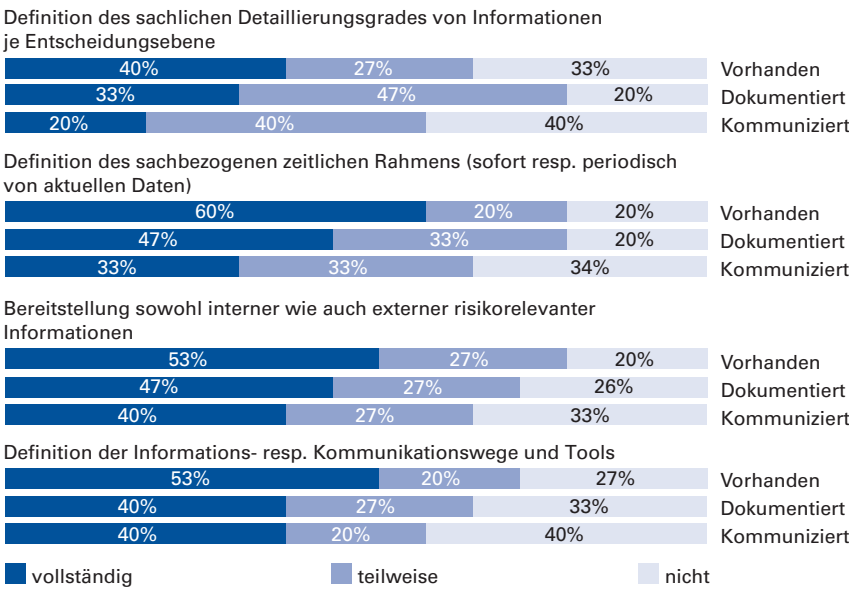
Unternehmen mit Risikomanagement-System

Eine klare Reportingstruktur ist eine der Voraussetzungen für das einwandfreie Funktionieren des Risikomanagement-Systems. Die Umfrageergebnisse zeigen, dass jeweils rund die Hälfte der Unternehmen den sachlichen Detaillierungsgrad je Entscheidungsebene (stufengerecht), richtige Informationen, den zeitlichen Rahmen (zeitgerecht) sowie die Kommunikationswege noch nicht vollständig definiert hat.

Um mit einer klareren Reportingstruktur aktuellere Informationen zu Risiken und Chancen zu erlangen, ist in einem ersten Schritt der sachliche Detaillierungsgrad je Entscheidungsebene zu definieren. Diese Aufgabe haben 33% der Unternehmen noch nicht angegangen und weitere 27% noch nicht abgeschlossen. In diesen Unternehmen ist somit nicht sichergestellt, dass die richtigen Informationen zu den richtigen Entscheidungsträgern gelangen (stufengerechtes Reporting).

Demgegenüber haben deutlich mehr Unternehmen (60%) den sachbezogenen zeitlichen Rahmen definiert, also die Reportingzeitpunkte klar festgelegt. Damit wissen verschiedene Unternehmen zwar wann rapportiert werden muss, kennen aber den Detaillierungsgrad je Unternehmenseinheit nicht. Ebenso sind die Informations- und Kommunikationswege sowie die erforderlichen Instrumente bei 47% der Unternehmen nicht oder nur teilweise festgelegt. Einige Unternehmen verfügen somit über keine einheitliche, standardisierte Vorgehensweise für das Reporting.

Gliederung Reporting



Monitoring des Risikomanagement-Systems (Monitoring)

«Von einem umfassenden und transparenten Risikomanagement-System erwarte ich, dass ich proaktiv über Veränderungen der Risikolage informiert werde nach dem Motto: No surprises, please!»
Robert Schlup, The Crypto Group

«Wie wird das Vorhandensein und das Funktionieren des Risikomanagement-Systems sichergestellt?»
Das Risikomanagement-System eines Unternehmens gilt es regelmässig auf die Funktionstüchtigkeit und Performance auf allen Unternehmensstufen hin zu überwachen. Dieses Monitoring kann auf zwei Arten erfolgen: Als fortlaufende Tätigkeiten oder durch periodische Prüfungen.

Die fortlaufende Überwachung findet im Rahmen der normalen, wiederkehrenden Tätigkeiten der Unternehmenseinheit statt. Sie erfolgt in Echtzeit und kann damit situativ und rascher auf veränderte Bedingungen reagieren. Sie ist damit wirkungsvoller als die periodische Prüfung. Gleichsam verzichten Unternehmen mit fortlaufender Prüfung nicht auf punktuelle Prüfungen, wobei deren Häufigkeit der Einschätzung des Managements obliegt.

Der Umfang einer Dokumentation eines Risikomanagement-Systems hängt unter anderem von der Grösse des Unternehmens, der Komplexität und der Zahl der Risikofaktoren ab. Eine angemessene Dokumentation erleichtert und verbessert das Monitoring. Werden im Monitoring Mängel im Risikomanagement-System festgestellt, sind jene Entscheidungsträger darüber zu informieren, die Kraft ihrer Funktion die notwendigen Schritte zur Behebung einleiten können.

Unternehmen ohne Risikomanagement-System
Nicht anwendbar.

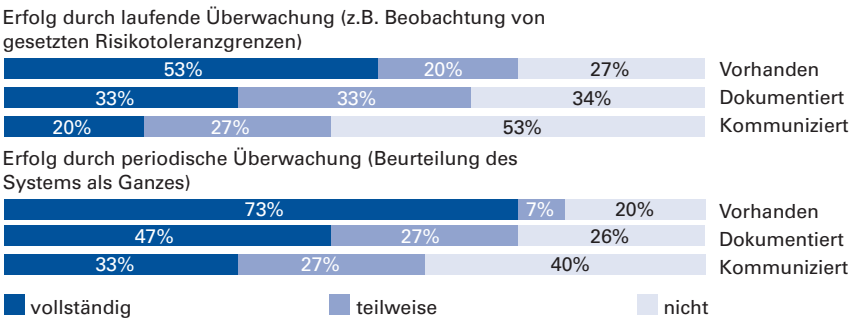
Unternehmen mit Risikomanagement-System

Zahlreichen Firmen in der Gruppe der Unternehmen mit Risikomanagement-System haben sowohl ein laufendes Monitoring als auch eine periodische Prüfung implementiert. 53% der Verwaltungsräte geben an, dass ihr Unternehmen das gesamte Risikomanagement-System z.B. mittels Risikotoleranzgrenzen laufend beobachtet. Damit ist sichergestellt, dass die Richtlinien jederzeit eingehalten werden.

Gleichzeitig geben 73% der Unternehmensvertreter an, das Risikomanagement-System in seiner Gesamtheit regelmässigen Prüfungen zu unterziehen. Diese erfolgt beispielsweise durch die Interne Revision, die das System auf seine Funktionsfähigkeit und auf Qualitätsmängel untersucht.

27% der Unternehmen geben an, kein laufendes Monitoring implementiert zu haben; 20% nehmen keine regelmässige Prüfung vor. Der Schluss liegt nahe, dass verschiedene Unternehmen weder die eine noch die andere Methode anwenden und damit keine Rückschlüsse auf die Funktionstüchtigkeit ihres Risikomanagement-Systems ziehen können.

Monitoring Risikomanagement-System



Funktionsträger

«Viele Unternehmen verfügen über nicht aufeinander abgestimmte Risikosysteme. Mit einem ganzheitlichen und integrierten Risikomanagement-System könnten die grössten Risiken identifiziert und dokumentiert werden, und es stünden laufend aktuelle Informationen über wesentliche Veränderungen zur Verfügung.»
Günter Haag, KPMG Schweiz

«Welche Stellen/Abteilungen unterstützen das Risikomanagement in Ihrem Unternehmen?»

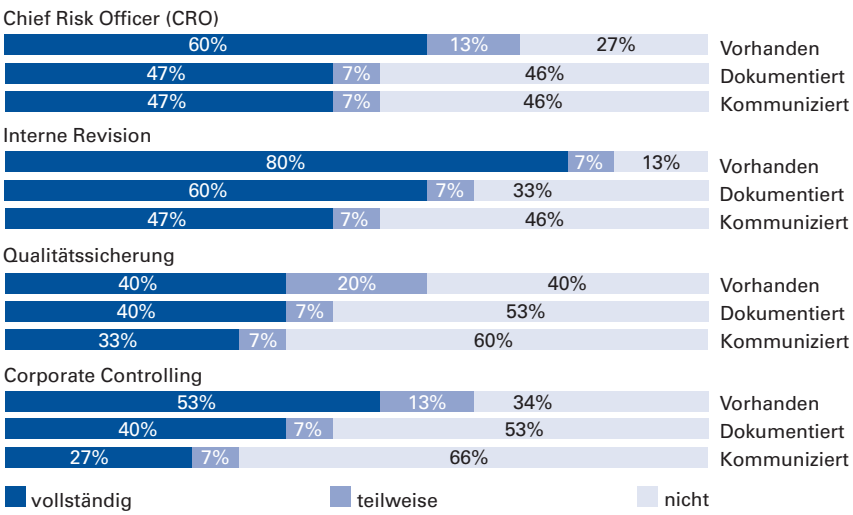
Unternehmen ohne Risikomanagement-System
Trotz Absenz eines Risikomanagement-Systems haben einzelne Unternehmen die Funktion des Chief Risk Officer besetzt. Der Funktionsträger widmet sich jedoch in erster Linie und vorwiegend den finanziellen Risiken und/oder Versicherungsrisiken.

Teilweise werden Interne Revision, Qualitätssicherung und Corporate Controlling in diesen Unternehmen in Aspekte des Risikomanagement-Systems eingebunden.

Unternehmen mit Risikomanagement-System
60% der in der Umfrage erfassten Unternehmen haben die Funktion des Chief Risk Officer etabliert. Die Frage nach dem Einsetzen der Internen Revision für das Risikomanagement bejahen sogar 80%. Demzufolge betrauen zahlreiche Unternehmen beide Funktionen gemeinsam mit der Aufgabe des Risikomangements. Corporate Controlling (53%) und Qualitätssicherung (40%) werden demgegenüber weniger häufig zugezogen.

Das Bild der heterogenen Aufgabenverteilung im Risikomanagement deckt sich mit der Theorie und den aufsichtsrechtlichen Vorgaben, welche die Frage nach der funktionalen Zuordnung offen lassen.

Unterstützende Bereiche



Schlussbemerkungen

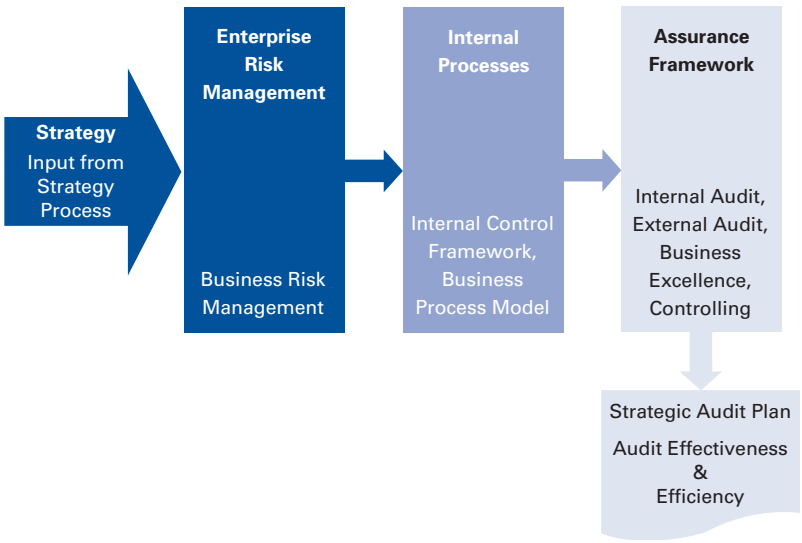
«Investoren haben die Wichtigkeit des Risikomanagements längst erkannt. Die Attraktivität der Aktie dürfte wohl auch von dessen Güte abhängen.»
Peter Küpfer, Valora, Swisscom, Unaxis, Holcim, Julius Bär Holding, LB (Swiss) Privatbank, UFJ Bank (Schweiz)

Das Management von Risiken und die Ausschöpfung von Chancen ist für Unternehmen und nicht gewinnorientierte Organisationen mehr denn je eine Überlebensnotwendigkeit. Regulatorische Bestimmungen, gesetzliche und branchenspezifische Standards, aber auch Aktionäre und Mitarbeiter erhöhen den Druck auf die Unternehmen zur Einführung eines Risikomanagements als Gesamtsystem. Es fehlen jedoch bisher Standards und mehrjährige Erfahrungswerte. Mit der Entstehung internationaler Richtlinien, wie z.B. des COSO-ERM-Frameworks, können Unternehmungen erstmals standardisierte und vergleichbare Vorgehensweisen heranziehen.

KPMG verfügt über eine langjährige Erfahrung im Bereich des Risikomanagements und der Assurance. In der Praxis setzt sich dabei eine Kombination – ein Zusammenspiel der Assurance-Anbieter – immer mehr durch. Dadurch können die vorhandenen Ressourcen effizient eingesetzt und aufeinander abgestimmt werden. Wichtigste Bereiche als Assurance Anbieter sind:

- Verwaltungsrat bzw. Audit Committee
- Interne Revision
- Risiko- und Chancenmanagement-System
- Corporate Controlling
- Externe Revision

Die Dienstleistungen der verschiedenen Assurance-Anbieter werden idealerweise in einer Gesamtschau – «Assurance-Konzept» – abgebildet und in einem strategischen Audit-Plan auf das betreffende Unternehmen abgestimmt. Dadurch werden nicht nur die Kosten der Überwachungsfunktionen optimiert. Diese Vorgehensweise bietet auch die Gewähr, dass sämtliche Chancen und Risiken durch das Risikomanagement-System umfassend abgedeckt werden, d.h. ohne Lücken und ohne Doppelspurigkeiten. In das umfassende Assurance-Konzept fliessen die Anforderungen und Zielsetzungen aller Anspruchsgruppen ein, also der Gesetzgeber, der Aktionäre bzw. Verwaltungsräte, der Internen Revision, der Versicherer usw.



Die Praxis von KPMG zeigt im Weiteren, dass verschiedene Faktoren für den Erfolg des Risikomanagement-Systems eine notwendige Voraussetzung sind und diesen erhöhen.

- Unterstützung/Sponsoring vom Top Management
- gemeinsame Risikokultur, in der über Risiken und Chancen offen sowie zeit- und stufengerecht kommuniziert wird
- einheitliches Risikoverständnis und eine gemeinsame Risikosprache
- einheitliche Methoden und Messgrössen bei der Bewertung der Risiken und Chancen
- definierter Zeithorizont bei der Bewertung
- einheitlicher Aufbau und Abgrenzung von Risiko- und Chancenkategorien sowie Risiko- und Chancenbeschreibungen
- transparente Auswertungen und Berichte

Die Implementierung eines Risikomanagement-Systems stellt hohe Anforderungen an ein Unternehmen, zumal das Management und der Verwaltungsrat in der Regel nicht über eine einschlägige und vertiefte Erfahrung in diesem Bereich verfügen und die zeitliche Beanspruchung nicht unterschätzt werden darf. Mit einem pragmatischen Ansatz kann das Unternehmen jedoch schrittweise an den Prozess herangehen. Als Orientierungshilfe erweist sich dabei das COSO-ERM-Framework. Besonderes Augenmerk ist dabei auf folgende Punkte zu legen:

- Mit der Durchführung erster Risiko- und Chancen-Assessments wird das nötige Bewusstsein auf der Stufe des Verwaltungsrats und des Managements geschaffen.
- Grundsätze und Ziele bilden die Grundlage für das Risikomanagement-System.
- Auf Unternehmensbereiche heruntergebrochen wird die operative Ausgestaltung des Risikomanagement-Systems definiert.
- Parallel wird definiert, welche risikorelevanten Informationen in welcher Form und zu welchem Zeitpunkt benötigt werden (Reporting).

Die Autoren hoffen, mit der vorliegenden Analyse des Status quo in der Schweizer Wirtschaft einen Beitrag zum besseren Verständnis des Risikomanagements zu leisten und umfassenden Systemen zum Durchbruch zu verhelfen. Die Spezialisten von KPMG stehen allen Unternehmen gerne für ein unverbindliches Gespräch über ihr Risikomanagement- System und Assurance-Konzept zur Verfügung.

Haben Sie Fragen zur Studie oder möchten Sie ein vertiefendes Gespräch führen?

Bitte wenden Sie sich an die KPMG Lokale Niederlassung oder an:

Audit Comitee Institute:
Günter Haag, Partner, dipl. Wirtschaftsprüfer
Telefon: +41 1 249 20 46, ghaag@kpmg.com

Assurance Concept:
Dieter Widmer, Partner, dipl. Wirtschaftsprüfer
Telefon: +41 1 249 21 01, dwidmer@kpmg.com

Risk Management/ Interne Revision:
Hans Ulrich Pfyffer, Partner, dipl. Wirtschaftsprüfer, CIA
Telefon: +41 1 249 27 77, hpfyffer@kpmg.com

Fragen zur Studie:
Sandra Heimüller, Marketing
Telefon +41 1 249 47 83, sheimueller@kpmg.com

Herausgeber:
KPMG's Audit Committee Institute
Badenerstrasse 172
Postfach
8026 Zürich 4
Tel +41 1 249 22 22
Fax +41 1 249 21 66

An dieser Studie haben mitgewirkt:
Dieter Widmer,
Leiter Risk Advisory Services
Mitglied der Geschäftsleitung

Hans Ulrich Pfyffer,
Leiter Internal Audit Services

André Wyss,
Manager, Internal Audit Services

Ghislain de Kerviler,
Leiter Marketing

Bestell-Nr. xxx
Tel +41 1 249 31 31
Fax +41 1 249 25 92
www.kpmg.ch
www.auditcommittee.ch

«Risiko Management 2004»
erscheint in Deutsch und Französisch.