

# COSO “Enterprise Risk Management – Integrated Framework“ als internationale Benchmark für Risikomanagementsysteme

Das Enterprise Risk Management – Integrated Framework des Committee of Sponsoring Organizations of the Treadway Commission (COSO) wurde im September 2004 veröffentlicht und stellt den international anerkannten Standard für ein umfassendes, unternehmensweites Risikomanagement dar. Der Inhalt des COSO-Frameworks sowie die einzelnen Bestandteile eines Risikomanagementsystems nach COSO bilden den Gegenstand der folgenden Ausführungen.

## Enterprise Risk Management – Integrated Framework als Benchmark

In Anbetracht der steigenden Komplexität der Umwelt und den Herausforderungen durch Globalisierung und Internationalisierung auf der einen und den gestiegenen Anforderungen der Stakeholder an die Führungsebene der Unternehmen auf der anderen Seite entscheiden sich immer mehr Unternehmen ein umfassendes Risikomanagement einzuführen. Die Ansätze der Einführung und der Umfang eines Risikomanagements unterscheiden sich ebenso voneinander wie das Verständnis von Chancen und Risiken.

**Bisherige Risikomanagementsysteme** beschäftigten sich vor allem mit finanziellen Aspekten, wie bspw Währungsrisiken, Kreditrisiken und Liquiditätsrisiken, oder mit Versicherungsaspekten, bspw hinsichtlich der Versicherung gegenüber Elementarereignissen oder Betriebsunterbrechungen. Ein umfassendes Risikomanagement geht jedoch über den Finanz- und Versicherungsbereich hinaus und inkludiert sämtliche Unternehmensbereiche.

Das “**Enterprise Risk Management – Integrated Framework**“ des „Committee of Sponsoring Organizations of the Treadway Commission“, kurz COSO, kann als international anerkannte Richtschnur für die Elemente eines umfassenden Risikomanagements genannt werden. Mit der Veröffentlichung des Frameworks für

Enterprise Risk Management hat COSO ca. zehn Jahre nach dem Framework für Internal Controls einen weiteren Meilenstein gesetzt. Im Blickpunkt sind die Gewissheit der strategischen und operativen Zielerreichung und dadurch die erleichterte Steuerbarkeit des Unternehmens. Aus einem funktionierenden Enterprise Risk Management zieht vor allem der Vorstand bzw. die Geschäftsführung ihren Nutzen. Aber auch sämtliche Stakeholder, wie bspw Aktionäre, Geschäftspartner, die interessierte Öffentlichkeit, profitieren von der Einführung eines Risikomanagements, da die unsichere Zukunft berechenbarer wird. Ähnlich wie das Framework zu internen Kontrollen gewinnt das Enterprise Risk Management Framework international zunehmend an Bedeutung. Es dient mittlerweile als eine international anerkannte **Benchmark für unternehmensweite Risikomanagementsysteme** und findet bei der Einführung und Evaluierung von Risikomanagementsystemen Verwendung.

Im Folgenden werden, in enger Anlehnung an das “Enterprise Risk Management – Integrated Framework“, die einzelnen Komponenten und Elemente eines COSO-Compliant Risikomanagements dargestellt.

## Bestandteile des Enterprise Risk Management nach COSO

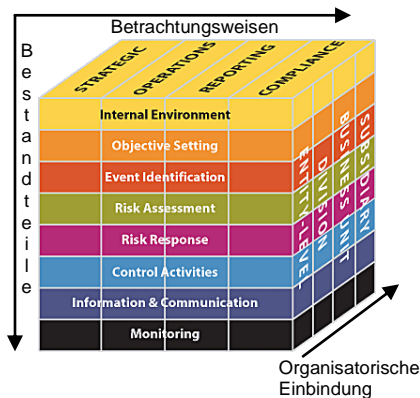
Die **Definition** eines Enterprise Risk Managements nach COSO spiegelt die einzelnen Elemente eines Risikomanagements wider:

***Enterprise Risk Management ist ein Prozess, der vom Vorstand, dem Management und definierten anderen Mitarbeitern eines Unternehmens getragen wird, als Inputfaktor bei der Strategisierung dient und unternehmensweit einheitlich gestaltet ist, sodass potenzielle positive wie negative Ereignisse, die sich auf das Unternehmen auswirken, gleichermaßen erkannt werden, um die Risiken im Rahmen des Risikoappetits zu steuern, damit die Gewissheit erhöht wird, die gesetzten Unternehmensziele zu erreichen.***

Betrachtungsmittelpunkt des COSO-Frameworks sind **Ereignisse**. Diese können sowohl negative wie positive Auswirkungen auf die Zielerreichung eines Unternehmens haben. Negative Auswirkungen verhindern Wertschaffung oder vernichten Werte und stellen somit **Risiken** dar. Positive Auswirkungen schaffen Werte oder dienen der Werterhaltung und sind als **Chancen** zu klassifizieren.

## Der COSO-Würfel

Die Bestandteile eines umfassenden Risikomanagements nach COSO können über den COSO-Würfel visualisiert werden (siehe Abbildung 1). Dieser beinhaltet die einzelnen Elemente eines Risikomanagementsystems (Vorderseite), die möglichen Betrachtungsweisen und Zielsetzungen (Oberseite) sowie die organisatorische Einbindung (Rechte Seite).



**Abbildung 1: Der COSO-Würfel visualisiert die Zusammenhänge zwischen den Elementen eines Risikomanagements, den Perspektiven und den Unternehmenseinheiten**

Sämtliche Wertungen beziehen sich auf die durch das Unternehmen festgelegte **Ziele**. Ein Enterprise Risk Management unterstützt die Erreichung dieser Unternehmensziele in vier unterschiedlichen Kategorien:

- **Strategic** - High-level Ziele, abgestimmt auf die Mission des Unternehmens
- **Operations** - Wirksamer und effizienter Umgang mit Ressourcen
- **Reporting** - Zuverlässigkeit des Reportings
- **Compliance** - Einhaltung der gesetzlichen und regulatorischen Rahmenbedingungen

Durch die Dimensionen wird die Möglichkeit geschaffen, unterschiedliche Erwartungen der jeweiligen Ziele der Kategorie zu verdeutlichen und die verschiedenen Aspekte des Risikomanagements unter diesem Blickwinkel näher zu betrachten.

Neben den unterschiedlichen Betrachtungsweisen können noch **organisatorische Aspekte** als weitere Gliederungsebene herangezogen werden.

Ein Risikomanagement kann auf vier organisatorischen Ebenen betrachtet werden:

- **Gesamtsicht**
- **Divisionsebene**
- **Business Units**
- **Niederlassungsebene**

Die Betrachtungsebenen ermöglichen somit das Risikomanagement oder seine einzelnen Bestandteile aus verschiedenen Blickwinkeln für das gesamte Unternehmen oder auch nur Teile davon zu betrachten.

Als Bestandteile eines Enterprise Risk Managements nach COSO führt das Enterprise Risk Management Framework folgende acht Komponenten an:

### Internal Environment Innerbetriebliche Umwelt

Die innerbetriebliche Umwelt stellt den **Rahmen für die weiteren Komponenten** des Risikomanagements dar. Ihre Ausprägung beeinflusst die Strategie- und Zielfindung, die Einstellung zum Risiko, die Elemente des Risikomanagementprozesses - Identifizierung, Bewertung und Umgang mit Risiko - sowie die Gestaltung und das Funktionieren der Kontrollaktivitäten und der Informations- und Kommunikationssysteme.

Wesentliche Elemente der innerbetrieblichen Umwelt sind unter anderem die **Risikomanagement-Philosophie** und das im Unternehmen etablierte **Wertesystem**. Die **Kompetenzverteilung** und das Zusammenspiel der Verantwortungsträger sind ebenso relevant wie die Kompetenzen der Mitarbeiter und die Organisation des Unternehmens.

Die Etablierung einer geeigneten innerbetrieblichen Umwelt erfolgt über eigene Maßnahmen bspw die **Ausformulierung von Risikomanagement-Philosophie** und Risikoappetit sowie die **Integration** der Risikoaspekte in das **Werte-, Normen- und Zielsystem** des Unternehmens. Hierzu eignet sich ein von der Geschäftsführung veröffentlichtes **Risikomanagement-Grundsatzdokument**. Neben der Unterstützung durch die Geschäftsführung wird so dem Risikomanagement im Unternehmen ein neuer Stellenwert verliehen und die Bedeutung für das Unternehmen herausgestrichen. Ein derartiges Dokument eignet sich auch, um die Verantwortung jedes einzelnen Mitarbeiters zu verdeutlichen und festzuschreiben.

Zusätzlich zu den formellen Dokumenten können noch risikobezogene Verhaltensregeln, bspw direkt in Prozessabläufen, implementiert oder das Chancen- und Risikobewusstsein der Mitarbeiter über Schulungen gesteigert werden.

Objective Setting

### Festlegung von Zielen

Chancen und Risiken lassen sich nur im Verhältnis zu einem Bezugspunkt definieren. Für ein Unternehmen stellt dieser Bezugspunkt die **Planung** bzw. die festgelegten **Ziele** dar. Die Auswirkung von Ereignissen – und somit die Klassifikation als Chance oder als Risiko – lassen sich nur unter Bezugnahme auf die Unternehmensziele und Planung feststellen. Die Dimensionen des Risikos müssen in sämtlichen Kategorien, ausgehend von den strategischen Zielen, bis hin zu den operativen Zielen, berücksichtigt werden. Dies gilt auch bei einer Veränderung der Ziele oder ihrer Schwerpunkte bzw. Kategorien. Ebenso gilt es die Risikokomponenten bei der Priorisierung der Ziele und der Messung der Zielerreichung ausreichend zu berücksichtigen.

Eine gangbare Methode Chancen und Risiken explizit in den Zielfindungsprozess zu integrieren, stellt die Definition eines entsprechenden **Risikoappetits** für das Unternehmen dar. Der Risikoappetit eines Unternehmens gibt an, wie viel Risiko die Führungsebene zur Erreichung der Unternehmensziele einzugehen gewillt ist. Die Visualisierung des Risikoappetits kann durch Verwendung von **Risks Maps** für das Unternehmen oder einzelne Bereiche erreicht werden.

Aus sämtlichen möglichen Handlungsalternativen zur Zielerreichung werden jene herausgefiltert, die im Einklang mit dem Risikoappetit stehen. Hierbei dienen Verfahren der Szenarioanalyse, Stress Tests etc. - immer unter Einbezug von Risikogesichtspunkten wie bspw Risikoverteilung oder der Art des Risikos.

Neben der Definition des Risikoappetits werden für sämtliche Ziele so genannte Risikotoleranzen festgelegt. Diese stellen die von der Unternehmensführung akzeptierte Bandbreite bei der Über- oder Unterschreitung von Zielgrößen dar und geben indirekt Auskunft über die Priorisierung der Ziele.

Event Identification

### Ereignisidentifikation

Eines der Kernelemente eines Risikomanagements stellt die Identifikation möglicher Ereignisse mit Auswirkung auf die Zielerreichung des Unternehmens dar. Die Ergebnisse der Ereignisidentifikation bilden die **Basis für sämtliche weitere Schritte**. Es gilt somit eine möglichst große Anzahl an Ereignissen zu erfassen. Als beeinflussende Faktoren kommen sowohl interne wie externe Faktoren in Betracht. Politische, ökonomische, ökologische, soziale, technische und natürliche Einflussfaktoren müssen ebenso Beachtung finden, wie die Aufbau- und Ablauforganisation des Unternehmens samt den internen Prozessen.

Die **Verfahren** zur Ereignisidentifikation sind vielfältig und können bzw sollen beliebig kombiniert werden. Grundsätzlich besteht die Möglichkeit über Brainstorming und Brainwriting unterschiedlichste Chancen und Risiken zu sammeln. Auch die Veranstaltung von Ereignisidentifikations-Workshops oder die gezielte Befragung von Entscheidungsträgern sind gängige Methoden der Ereignisidentifikation. Um Ereignisse aus allen Bereichen zu identifizieren, ist aber stets auf die Heterogenität der befragten Gruppe zu achten.

Sind die **Chancen und Risiken**

können auch externe Ereignislisten herangezogen und im Zuge der Identifikation an die Spezifika des jeweiligen Unternehmens angepasst werden.

Risk Assessment

### Risikobewertung

Nach der Identifikation der Ereignisse müssen diese entsprechend bewertet werden. Die Einschätzung der Chancen und Risiken ist wiederum von den unternehmensspezifischen Faktoren wie bspw Vision, Unternehmenskultur und Unternehmensgröße, Komplexität der Organisation etc. abhängig.

**Ausgangspunkt** für die Bewertung der einzelnen Ereignisse sind die Ziele und die **Planung** des Unternehmens. Der Zeithorizont der Betrachtung der Chancen und Risiken ist mit jenem der Planung abzustimmen. Die Teilnehmer der Bewertung müssen bei ihren Überlegungen sowohl inhärente Risiken als auch Restrisiken berücksichtigen. Das **inhärente Risiko** stellt jenes Risiko dar, welches ohne den Einbezug bestehender Maßnahmen bestehen würde. Berücksichtigt man in einem nächsten Schritt die bereits getroffenen Maßnahmen, so bleibt ein **Restrisiko** bestehen. Sowohl inhärentes Risiko als auch Restrisiko geben wesentliche Anhaltspunkte und Interpretationshilfen

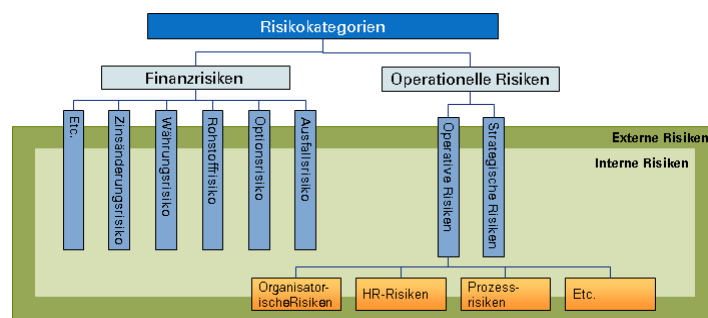


Abbildung 2: Die Abbildung zeigt eine beispielhafte Risikokategorisierung

erfasst, sollten diese **systematisiert** werden. Zum einen erleichtert dies die weiteren Schritte, zum anderen kann so eine Überprüfung auf Vollständigkeit durch Vergleich mit bereits bestehenden Risikosammlungen oder Ereignislisten erreicht werden. Weiters

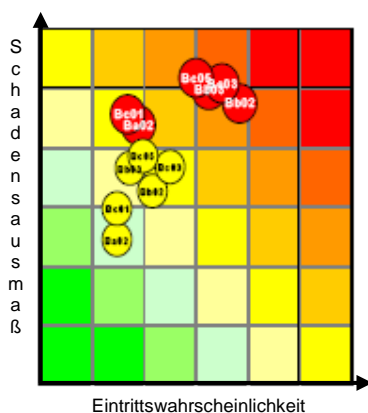
für die anschließende Analyse und Priorisierung der Risiken.

Eine Bewertung der Risiken erfolgt über **Beurteilung der Eintrittswahrscheinlichkeit und der Auswirkungen**. Über Kombinati-

on der Eintrittswahrscheinlichkeit und der Auswirkung gelangt man zum bestehenden Risiko und in weiterer Folge zum Handlungsbedarf. Ein Risiko mit hoher Eintrittswahrscheinlichkeit und großen Auswirkungen schafft akuten **Handlungsbedarf**, ein Risiko mit niedriger Eintrittswahrscheinlichkeit und geringen Auswirkungen bedingt hingegen keinen unmittelbaren Handlungsbedarf.

Die konkreten Methoden der Bewertung differieren je nach betrachtetem Risiko. Qualitative als auch quantitative Bewertungsverfahren kommen regelmäßig zum Einsatz. **Qualitative Verfahren** bieten den Vorteil, dass nicht auf umfangreiches und schwer verfügbares Datenmaterial zurückgegriffen werden muss. Zudem können alle Risiken beurteilt und die Einschätzung der Entscheidungsträger entsprechend berücksichtigt werden.

Übliche qualitative Methoden sind Expertenbefragungen oder die Schätzung von Risiken durch die Verantwortlichen. Verbreitete quantitative Methoden der Risikomessung sind bspw der Value-at-Risk (VaR)-Ansatz, Cash-Flow at Risk, die Heranziehung des EBITs als Bezugsgröße für den Verlust/die Chance von Ereignissen, die Bewertung von „loss events“ und Back Testing-Verfahren. Daneben kommen noch Techniken der Szenarioanalyse, der Sensitivitätsanalyse, Benchmarking oder des Stress Testings zum Einsatz.



**Abbildung 3: Visualisierung der Risiken durch Risk Maps**

Die **Visualisierung** der Risiken erfolgt oftmals über Risikolandkar-

ten („Risk maps“) oder Prozess-Charts. Hierbei wird auf der y-Achse das Schadensausmaß abgebildet, auf der x-Achse die Eintrittswahrscheinlichkeit. Das Risiko selbst ergibt sich dann aus der Kombination beider Größen. Quantitative Ergebnisse werden oftmals in Prozent einer Zielgröße oder als Wahrscheinlichkeitsverteilungen mit Intervallen dargestellt.

### Risk Response Reaktion auf Risiken

Den identifizierten und bewerteten Risiken kann das Unternehmen auf unterschiedlichen Wegen begegnen. Zum einen kann eine Strategie der **Risikovermeidung** durch Unterlassung der risikoverursachenden Aktivitäten verfolgt werden. Zum anderen kann eine **Reduktion des Risikos** durch Implementierung von Maßnahmen zur Verringerung der Auswirkungen und / oder der Eintrittswahrscheinlichkeit angestrebt werden. Als weitere Alternative steht die **Risikoteilung** durch Übertragung auf oder Teilung der Risiken mit Dritten zur Verfügung. Zu guter letzt kann ein Unternehmen auch entscheiden, das Risiko zu **akzeptieren**.



#### Vier Möglichkeiten zum Umgang mit Risiko

Ziel der Reaktionen ist nicht, das Risiko auf Null zu reduzieren, sondern das **Restrisiko innerhalb** der definierten **Risikotoleranzen** zu halten. Dies gilt für das einzelne Risiko ebenso wie für die Einhaltung des gesamten Risikoappetits.

Die Reaktionen werden für **jedes Risiko getrennt**, aber in Abhängigkeit von dem Risikopotenzial, dem Restrisiko und dem angestrebten Zielrisiko betrachtet. Die **Maßnahmen** selbst sind hinsichtlich ihrer Auswirkung auf Eintrittswahrscheinlichkeit und Schadensausmaß zu bewerten und ihre Wechselwirkungen untereinander

sind ebenfalls zu berücksichtigen. Hilfe bei der Bewertung können wiederum vergangenheitsbezogene Daten, Trends oder Zukunftsszenarien bieten.

Stets ist aber immer die Kosten-Nutzen Relation der Maßnahmen zu beachten – eine Abwägung zwischen den Kosten der Implementierung der Maßnahmen samt den laufenden Kosten versus dem Nutzen aus der Reduktion des Risikos ist zweckmäßig.

Zur Erleichterung der Setzung von Reaktionen können wiederum Risikokategorien gebildet und diese mit den Zielen, Ereignissen und ausgewählten Maßnahmen bspw tabellarisch verknüpft werden.

### Control Activities Kontrollmaßnahmen

Die Umsetzung der Reaktionen auf die Risiken muss entsprechend gewährleistet werden. Hierbei kommen unterschiedliche Kontrollmaßnahmen zum Einsatz. Kontrollaktivitäten finden sowohl auf strategischer als auch operativer Ebene statt. Überwacht wird, ob die beschlossenen Reaktionen in der vorgesehenen Art und Weise von den verantwortlichen Personen zeitgerecht umgesetzt und gegebenenfalls auch berichtet werden.

Wie bei allen Kontrollen empfiehlt es sich auch hier die notwendigen Kontrollschritte bereits in den umzusetzenden Reaktionen selbst vorzusehen und in die Arbeitsabläufe zu integrieren. Das Kosten-Nutzen-Verhältnis ist zu beachten. Die ausgewählten Kontrollmaßnahmen sollten in einem angemessenen Verhältnis zum Risiko bzw zum Nutzen der jeweiligen Reaktionen auf das Risiko stehen. Art und Umfang der Maßnahmen variieren somit von Risiko zu Risiko.

Übliche Maßnahmen sind Top-Level-Reviews, Performance-Berichte und Performance Indikatoren, Informationschecks oder Verteilung der Kompetenzen und Funktionstrennung sowie die Definition von geregelten Abläufen. Sicherheitsmanagement, Plausibilitätsüberlegungen und logische



Tests kommen ebenfalls zum Einsatz. Bei der Definition der Maßnahmen muss aber stets das Ziel der Reaktionen und somit der Maßnahmen Beachtung finden.

#### Information & Communication

### Information und Kommunikation

Mit dem Terminus Information verdeutlicht das Enterprise Risk Management Framework den Stellenwert des Informationsverarbeitungsprozesses für das Risikomanagement. Es gilt, sämtliche verfügbare Informationen in verwertbares Wissen zu transformieren. Hierzu muss der Informationsverarbeitungsprozess in der Lage sein die verfügbaren Informationen zu sammeln, systematisch aufzubereiten und zu analysieren und schließlich die derart aufbereitete Information den jeweiligen Empfängern gemäß ihrem Informationsbedarf zur rechten Zeit zur Verfügung zu stellen.

Zur Unterstützung des Informationsverarbeitungsprozesses kommen regelmäßig unterschiedliche IT-Systeme zum Einsatz. Aufgrund der gestiegenen Komplexität der Entscheidungen und Aufgaben muss bei der Auswahl und Gestaltung der Struktur auf eine entsprechende Flexibilität geachtet werden.

Ähnlich wie bei den Kontrollmaßnahmen ist die Integration des Informationsverarbeitungsprozesses in die standardisierten Abläufe des Unternehmens von besonderer Bedeutung. Über die Integration kann einerseits die Aktualität und Verfügbarkeit der Daten gewährleistet werden, andererseits verstärkt die Angabe von risikospezifischer Information im Rahmen der Alltagsaktivitäten das Risikobewusstsein und -verständnis im gesamten Unternehmen und unterstützt dadurch die Einhaltung der jeweiligen Risikotoleranzen.

Im Rahmen der Kommunikation widmet sich COSO der Übertragung von Informationen zwischen Personen. Hierbei ist sowohl die interne wie auch externe Kommunikation zu beachten.

Interne risikospezifische Kommunikation beinhaltet die Kommunikation der Bedeutung des Risikomanagements, der Ziele desselben, des Risikoappetits und der Risikotoleranzen, der Risikosprache und der Rollen und Verantwortlichkeiten. Hierbei sind entsprechende Informationskanäle aber auch Eskalationswege vorzusehen.

Die externe Kommunikation beinhaltet die Informationsweitergabe an Adressaten außerhalb des Unternehmens – somit an sämtliche Stakeholder. Auch bei diesem Kreis gilt es die Sensibilität der Informationsempfänger für die unternehmensspezifischen Risiken zu fördern und ein Verständnis für die Chancen- und Risikosituation des Unternehmens zu schaffen.

#### Monitoring

### Überwachung

Das Monitoring beschäftigt sich mit der Prüfung der Effektivität und der Funktionsfähigkeit des Risikomanagementprozesses und der implementierten Kontrollen im Zeitablauf. Nur durch eine Überprüfung des Risikomanagements an sich, kann der Nutzen des Konzeptes verwirklicht werden. Prüfungen können als eine ständige Überwachung oder eigene Prüfung konzipiert sein. Zum Einsatz kommen unter anderem Checklisten, Fragebögen, Benchmarks, peer reviews, interne Audits oder externe Evaluierungen.

Die Evaluierung selbst ist ein Prozess. Ausgehend vom Verständnis des Risikomanagements, seiner Komponenten und ihres Zusammenspiels werden die implementierten Prozesse auf ihre Aktualität, Effizienz und Effektivität sowie ihre Fähigkeit Abweichungen zu identifizieren überprüft. Die Ergebnisse der Evaluierung werden ebenso wie die Ergebnisse des Risikomanagementprozesses entsprechend dokumentiert. Sie dienen wiederum der Kommunikation des Risikomanagements nach innen wie nach außen.

### Inhalt einer Dokumentation

Eine mögliche Dokumentation könnte folgende Elemente beinhalten:

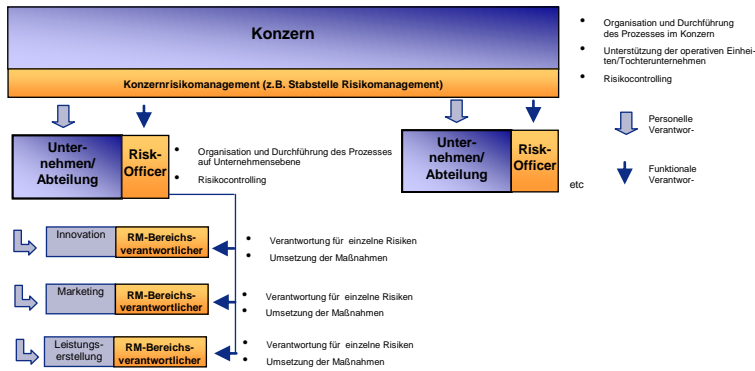
- Organigramm
- Schlüsselrollen, Autoritäten und Verantwortlichkeiten
- Grundsätze
- Betriebsverfahren
- Prozessflussdiagramme
- Relevante Kontrollen und zusammenhängende Verantwortlichkeiten
- Schlüsselindikatoren
- Top-Risiken
- Top-Risiken-Kennzahlen

### Rollen und Verantwortlichkeiten

Die Definition der Verantwortlichkeiten für das Risikomanagement im Unternehmen muss sich selbstverständlich an der internen Kompetenzverteilung orientieren.

Die Gesamtverantwortung für das Risikomanagement liegt stets bei der Geschäftsführung des Unternehmens. Ihr Commitment ist für ein funktionierendes Risikomanagement unabdingbare Voraussetzung. Weiters obliegt der Geschäftsführung die Führung und Richtungsbestimmung des gesamten Unternehmens, die Formulierung der Strategie und der high-level Ziele sowie des Risikoappetits. Ebenfalls ist ein entsprechendes internes Umfeld zu schaffen. Die Geschäftsführung ist stets über die wesentlichen Risiken und die Risk Response-Aktivitäten des Unternehmens informiert. CEO und die Financial Executives sind in der Regel erste Ansprechpersonen für das Risikomanagement.

Meistens wird in Unternehmen die Funktion eines Risk Officers eingerichtet. Dieser unterstützt und betreut die anderen Manager bei der Implementierung und der Umsetzung des Risikomanagements. Die konkrete Ausgestaltung der Position und Umfang der Weisungsbefugnisse und Kompe-



### Beispiel einer organisatorischen Eingliederung des Risikomanagements

tenzen variiert je nach Unternehmen.

Den internen Audit-Abteilungen kommt auch in Zusammenhang mit dem Risikomanagement große Bedeutung zu. Zusätzlich zu ihren bisherigen Aufgaben – Prüfung der Verlässlichkeit, Effektivität und Effizienz der Abläufe und des Berichtssystems – treten risikomanagementspezifische Aspekte in den genannten Bereichen hinzu.

Sämtliche weitere Mitglieder des Unternehmens werden durch ein umfassendes Risikomanagement im Rahmen ihrer Kompetenzbereiche integriert und sind dementsprechend für die sie betreffenden Risiken verantwortlich.

Die Ansprüche der externen Stakeholder sind im Rahmen eines umfassenden Risikomanagements ebenfalls zu berücksichtigen. Die grundlegenden Treiber für ein Risikomanagement und Erwartungen von externen

Stakeholdern, wie Aktionären oder Behörden etc., wurden im vorigen Beitrag bereits dargestellt und werden daher an dieser Stelle nicht nochmals erläutert.

### Grenzen des Risikomanagements

Das Ziel des Risikomanagements ist es, dem gesamten Management einen Überblick über bestehende Chancen und Risiken zu verschaffen und das Bewusstsein für die Chancen- und Risiko-Problematik zu schärfen. Aufgrund von Unsicherheit der Zukunft, von möglichen Fehlinterpretation der Informationen oder dem Versagen des Systems kann ein Risikomanagement das Erreichen der Unternehmensziele zwar niemals hundertprozentig garantieren, es kann jedoch trotzdem ohne Zweifel eine wertvolle Hilfestellung für die im Unternehmen ablaufenden Entscheidungsprozesse bieten.