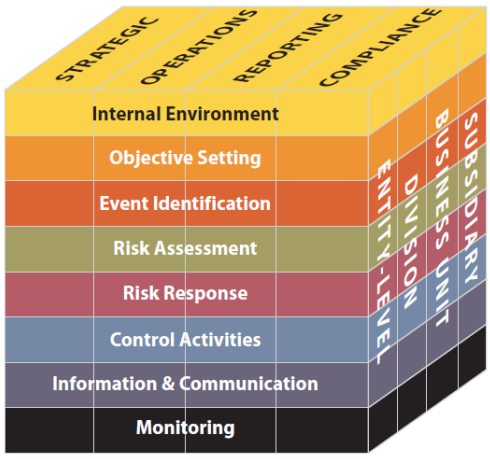
Management Service zu Themen, die wichtig sind, aber immer wieder dem Eiligen weichen müssen. Kurz und knapp angerissen – in einer »**EXECUTIVE SUMMARY**«, die an ein solches wichtiges Thema erinnert und das Wesentliche dieses Themas zusammenzufasst.

Risikomanagement

Klassische Organisations- und Kontrollthemen und der neue deutsche Nachhaltigkeitskodex waren bisher die Themen der »EXECUTIVE SUMMARY« – auch diesmal geht es wieder um einen Baustein der Organisation eines Unternehmens. Das Risikomanagement ist spätestens seit 1998 durch das »Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)« in Deutschland zu einem festen Bestandteil der Organisation geworden. Das Gesetz verlangt im Aktienrecht ein Überwachungssystem, das bestandsgefährdende Risiken frühzeitig erkennen lässt. Mit dem »Bilanzrechtsmodernisierungsgesetz«, das die Forderung nach einem Risikomanagementsystem verstärkt, fand der Begriff auch Aufnahme in den Gesetzestext. Auch wenn die genannten gesetzlichen Vorschriften sich nicht ausdrücklich auf alle Unternehmen beziehen, wird ein solches System heute in einem für das jeweilige Unternehmen angemessenem Umfang als Teil ordnungsgemäßer Geschäftsführung gesehen.

COSO ERM

International galt lange das amerikanische Rahmenmodell »COSO ERM« (Enterprise Risk Management – Integrated Framework) als führendes Referenzmodell für Wirtschaftsprüfer. Die Buchstaben »C O S O« stehen für das »Committee of Sponsoring Organizations of the Treadway Commission. Das Komitee beschäftigte sich zunächst mit der Wirksamkeit der internen Kontrollsysteme in Betrieben und veröffentlichte eine Anleitung für Unternehmensleiter zur Strukturierung und Einführung interner Kontrollen, um die Unternehmensziele in Bezug auf Operations, Reporting und Compliance zur erreichen. Diese wurde 2002 mit Section 404 des Sarbanes / Oxley Act (nachfolgend »SOx 404«) zur festen Größe in amerikanischen Unternehmen. Als Weiterentwicklung wurde 2004 »COSO ERM« als Risikomanagement-Rahmenmodell veröffentlicht und bildet den wesentlichen Teil der Corporate Governance:



ERM-Würfel aus: Enterprise Risk Management — Integrated Framework; Executive Summary; PWC für COSO; Jersey City, NJ 2004
als Download im Internet unter: http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf

ISO 31000:2009 Risikomanagement – Grundsätze und Leitlinien

Die International Organization for Standardization (**»ISO«**) in Genf hat 2009 den internationalen Standard ISO 31000 veröffentlicht. Das Ziel ist die Harmonisierung von Risikomanagementprozessen weltweit. Die ISO 31000 wird inzwischen als einziger international anerkannter Risikomanagement-Standard angesehen, von den meisten G20-Staaten als nationaler Standard anerkannt (so G31000, die neue Globale Risikomanagement Plattform im Internet bei der Ankündigung der ersten internationalen Konferenz zur ISO 31000). Sie ist ausdrücklich nicht als Grundlage für eine Zertifizierung vorgesehen.

Die ISO 31000 definiert in ihren ersten vier Abschnitten ihren Anwendungsbereich, die verwendeten Begriffe, die Grundsätze des Risikomanagements und seinen Rahmen. Der fünfte und letzte Abschnitt enthält die Vorgaben für den Prozess. Dieser muss ein wesentlicher Teil der Unternehmensführung sein und in die Unternehmenskultur und –praxis fest eingebunden sein sowie auf die Geschäftsprozesse des Unternehmens abgestimmt sein.

Der Prozess kann mit den Abschnittsüberschriften der ISO 31000 wie folgt dargestellt werden:

Die Abschnitte 5.4. (Risikobeurteilung), 5.5 (Risikobewältigung) und 5.6 (Überwachung und Überprüfung) finden sich im COSO-Würfel in den Schichten Event Identification, Risk Assesment, Risk Response und Control Activities wieder. Der Kernprozess enthält das klassische Repertoire des Risiko Reporting nach KonTraG und BilMoG, was die Voraussetzung für ein effektives Risikomanagement ist. Hier wird also alter Wein in neuen Schläuchen angeboten. Risikomanagement war immer schon eine Aufgabe der gesamten Organisation, die in der Gesamtverantwortung der obersten Unternehmensleitung liegt. Bis zu einem gewissen Grad muss jede Mitarbeiterin und jeder Mitarbeiter Risikomanagement als einen Teil ihrer/seiner Aufgaben verstehen. Die Einordnung der identifizierten Ereignisse als Chancen oder Risiken und die Bewertung der Auswirkungen und Eintrittswahrscheinlichkeiten der Risiken ist ureigenste Aufgabe des Unternehmens und kann nicht ausgelagert werden.

Risikoinventar

Haben Unternehmen bestimmte Größen erreicht, werden üblicherweise unternehmensspezifische Risikoinventare, aus denen sich Eintrittswahrscheinlichkeit und potentielle Schadenshöhen (monetär oder qualitativ) und der Aufwand für die Bewältigung des jeweiligen Risikos ergeben, geführt und vierteljährlich oder halbjährlich aktualisiert. Dabei empfiehlt es sich für KMUs, bei der Risikobeurteilung nur wenige Optionen anzubieten – jeweils drei Stufen sollten hier reichen:

Eintrittswahrscheinlichkeit	Potentieller Schaden	Bewältigungsaufwand
hohe Wahrscheinlichkeit (> 50% oder weniger als einmal in zwei Jahren)	**kritisch** (> 50% des durchschnittlichen Gewinns der letzten 3 Jahre oder des EK)	**herausfordernd** und schwierig
mittlere Wahrscheinlichkeit (zwischen 5% und 50%)	**deutlich** (zwischen 5% und 50% des durchschn. Gewinns der letzten 3 J.)	**möglich** bei fehlerfreier Abwicklung
niedrige Wahrscheinlichkeit (< 5% oder weniger als einmal in zwanzig Jahren)	**gering** (< 5% des durchschnittlichen Gewinns der letzten 3 Jahre)	**einfach** abzuwickeln

Ist das erste Risikoinventar mit seinen Teilinventaren aus allen Unternehmensbereichen erst einmal aufgestellt, sind die erforderlichen Ressourcen für die periodischen Aktualisierungen überschaubar und auf viele Schultern verteilt. Letztlich hat dabei jede Führungskraft für ihren Bereich alle Vorgänge, die Risiken in sich tragen, in das jeweilige Teilinventar aufzunehmen.

Unternehmenssteuerung

Das Risikoinventar ist für die Unternehmensleitung und die Teilinventare sind für die einzelnen Organisationseinheiten des Unternehmens formalisierte Übersichten auf einheitlicher Grundlage. So können bewusst akzeptierte Risiken und Maßnahmen zur Risikobewältigung gezielt überwacht werden. Die Teilinventare dienen so der bewussten Steuerung der organisatorischen Einheiten; das unternehmensweite Risikoinventar dient der Gesamtsteuerung und der Weiterentwicklung von Strategie und Businessplänen. Es empfiehlt sich, im Prozess den Abgleich mit der Internen Revision (in beiden Richtungen) vorzusehen.

Bei Fragen zu dieser »**EXECUTIVE SUMMARY**« wenden Sie sich bitte an:

Dr. Frank Herdmann, Auxilium Management Service
Gluckweg 10 | 12247 Berlin
Tel.: +49 30 – 771 90 321
Fax: +49 30 – 771 90 322
Mobil: +49 172 – 301 91 24
Mail: **auxilium@herdmann.de**
Internet: **http://herdmann.de**