

Risikomanagement-Standards und - Rahmenkonzepte – Die Qual der Wahl



Wer sich in diesem Jahr vorgenommen hat, ein Risikomanagement im Unternehmen zu implementieren, um der seit Jahresbeginn wirksamen Pflicht zur Beurteilung der Risiken im Anhang der Jahresrechnung nachkommen zu können, sieht sich vor die Wahl gestellt:

von Prof. Dr. Thomas Rautenstrauch und Stefan Hunziker

In vielen Ländern existieren bereits Standards und Rahmenwerke (engl. Framework), die als konzeptionelle Erklärungs- und Realisierungskonzepte dienen können. Allen gemeinsam ist dabei, dass Sie jeweils aus einer eigenen Perspektive die Bestandteile und das Verständnis von Risikomanagement beschreiben. Trotz mancher Unterschiede und Gemeinsamkeiten ist somit häufig die Frage, welches die vermeintlich beste «Richtschnur» für das eigene Vorgehen sei. Insbesondere für international orientierte Unternehmen ist dies keinesfalls einfach zu beantworten.

Neben Bestimmungen zur Organhaftung regeln das Obligationenrecht in der Schweiz, das KonTraG in Deutschland und das Verbandsverantwortlichkeitsgesetz in Österreich explizit die Verantwortung der Unternehmensführung für ein Risikomanagement im Unternehmen. Aus diesem Grund betreiben heute bereits zahlreiche Unternehmen ein Risikomanagement und sind zugleich damit befasst, ihr jeweiliges Risikomanagement-System (RMS) kontinuierlich zu verbessern. Demzufolge besteht ein hohes Interesse von Seiten der Unternehmen daran sicherzustellen, dass das eigene Risikomanagement konform zu den anerkannten internationalen bzw. nationalen Risikomanagement-Standards ist.

Die inhaltlichen Anforderungen, die ein wirksames RMS erfüllen muss, werden zum grossen Teil in Form international anerkannter Rahmenkonzepte und Regelwerke standardisiert, wobei die folgenden drei bislang hohe Akzeptanz erreicht haben:

- COSO Enterprise Risk Management Framework (COSO-ERM)
- ISO 31000 Guideline on Principles and Implementation of Riskmanagement
- ON-Regelwerk 49000 Risikomanagement für Organisationen und Systeme.

Im Hinblick auf die Anwendung der genannten Rahmenkonzepte für ein Risikomanagement gibt es bislang in der Schweiz keine Vorschrift, sich zwingend nach einem Standard zu richten. Dennoch sichern diese eine strukturierte Vorgehensweise und sind daher nur zu begrüssen. Im folgenden Beitrag soll daher ein Überblick zu den bestehenden Standards und Rahmenkonzepten im Kontext des Risikomanagements erfolgen.

Internationale Gesetzliche Normen zum Riskmanagement in Unternehmen

Ab Geschäftsjahr 2008 müssen Schweizer Unternehmen, die der ordentlichen bzw. eingeschränkten Revision unterliegen, im Anhang der Jahresrechnung Angaben zur Risikobeurteilung machen (Art. 663b Zif. 12 OR). Diese Neuregelung ist für alle Aktiengesellschaften und weitere Unternehmen (GmbH und gewerbetreibende Stiftungen), die einen Anhang gemäss Aktienrecht erstellen müssen, verbindlich. Daher müssen auch viele Kleingesellschaften in der Schweiz diese neue Forderung erfüllen. Die geforderte Risikobeurteilung ist Bestandteil des unternehmensweiten Risikomanagements, mit welchem die Risiken überwacht und gesteuert werden. Da der Anhang als Ganzes Prüfungsgegenstand darstellt, sind auch die Angaben zur Durchführung der Risikobeurteilung von der Revisionsstelle neu zu prüfen.

Es ist allerdings zu bemerken, dass aus methodischer Sicht noch viele Fragen offen bleiben, da es bisher an einer inhaltlichen Konkretisierung der Verpflichtung durch Art. 663b Ziffer 12. OR noch weitgehend fehlt (vgl. dazu Beitrag Rautenstrauch, T.; Hunziker, S.: «Grosser Handlungsspielraum für Risikobeurteilung im Anhang zur Jahresrechnung» im Praxisforum).

In Deutschland hingegen veröffentlichte die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) im Dezember 2005 die Endfassung der «Mindestanforderungen an das Risikomanagement» (MaRisk) für Kreditinstitute, welche alle früheren Regelungen ablöst und erweitert. Die MaRisk berücksichtigt die Anforderungen von Basel II und fordern von den Kreditinstituten unter anderem den Betrieb

- eines IKS (Internen Kontrollsystems) und eines integrierten Risikomanagements
- den Betrieb einer Internen Revision
- einer sicheren IT (IT Contingency, Continuity, Recovery Planning)
- eines Notfallmanagements

Weiter existiert in Deutschland das so genannte KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich), welches ein umfangreiches Artikelgesetz ist, das vom Deutschen Bundestag verabschiedet und am 1. Mai 1998 in Kraft trat. Das KonTraG verpflichtet explizit den Aufsichtsrat (Aufsichtsgremium) und den Vorstand einer Aktiengesellschaft, verlangt Risikotransparenz nach Aussen sowie den Betrieb eines Frühwarnsystems für den proaktiven und verantwortungsvollen Umgang mit Risiken.

In den USA wurde 2002 der Sarbanes-Oxley Act als Reaktion auf Fehler in den Finanzabschlüssen grosser Konzerne eingeführt. Das Gesetz (Act) enthält Bestimmungen, welche die Corporate Governance, die Finanzberichterstattung und die Kapitalmärkte stärken sollen und hat nicht lediglich nationale Bedeutung in den USA, sondern ist auch von internationaler Bedeutung. Der Sarbanes-Oxley Act gilt für alle Unternehmen, deren Wertpapiere an einer der SEC unterstehenden Börse gehandelt werden.

Als weiteres Regelwerk ist Basel II zu nennen. Basel II umfasst die Gesamtheit der Eigenkapitalvorschriften, die vom Basler Ausschuss für Bankenaufsicht in den letzten Jahren vorgeschlagen wurden. Die Regeln müssen seit dem 1. Januar 2007 in den Mitgliedsstaaten der Europäischen Union für alle Kreditinstitute und Finanzdienstleistungsinstitute angewendet werden. Basel II legt fest, wie Finanzinstitute zukünftig Ihre Risiken mit Eigenkapital hinterlegen sollen. Dabei kommen je nach Risikoinformationstransparenz unterschiedliche Bemessungsverfahren für die Bestimmung des Eigenkapitalbedarfs zum Einsatz. Es wird zwischen Kredit-, Markt-, und operationellen Risiken unterschieden. Basel II führt zu einer risikoadjustierten Verzinsung von Unternehmenskrediten und

ist somit für nahezu alle Marktteilnehmer von Bedeutung, weshalb es als ein wesentlicher Treiber für die Erhöhung der Risikotransparenz von Unternehmen gesehen werden kann.

Was für die Bankenwelt Basel II ist, ist für die Versicherungswelt Solvency II. Ziel von Solvency ist die zukünftige Zahlungsfähigkeit von Versicherungsgesellschaften zu gewährleisten. Dabei stellen die stark veränderten Risikoexpositionen infolge von Globalisierung, Erderwärmung, Demographische Entwicklung, Technologiewandel, Internationale Sicherheitspolitik und Terrorismus hohe Anforderungen an die Risikobemessung.

Ausgewählte internationale Rahmenkonzepte und Standards zum Risikomanagement

Das US-amerikanische Committee of Sponsoring Organizations of the Treadway Commission (CO-SO) erarbeitet Rahmenwerke für den Aufbau und Betrieb von wirksamen Internen Kontrollsystemen (IKS). Einer Risikoorientierung der «Internal Control» wurde bereits seit 1992 mit dem Rahmenkonzept COSO grosse Bedeutung beigemessen, welches heute als Quasi-Standard zur systematischen Einführung eines Internen Kontrollsystems gilt. In einem im September 2004 veröffentlichten erweiterten COSO-Konzept wird mit dem Enterprise Risk Management Framework (CO-SO-ERM) zusätzlich im Detail beschrieben, wie ein Unternehmensrisikomanagement aufgebaut und betrieben werden kann. Enterprise Risk Management wird als ein Prozess verstanden, der sowohl von den Führungsgremien des Unternehmens als auch von definierten anderen Mitarbeitern eines Unternehmens getragen wird, als Inputfaktor bei der Strategiesetzung dient und unternehmensweit einheitlich gestaltet ist, so dass potenzielle positive wie negative Ereignisse, die sich auf das Unternehmen auswirken, gleichermassen erkannt werden. Hierbei ist es das Ziel, die Risiken proaktiv zu steuern, um so die gesetzten Unternehmensziele erreichen zu können. Die internationale Anerkennung und Verbreitung dieses Konzepts ist vergleichsweise sehr hoch.

Neben COSO-ERM versteht sich ISO 31000 (Guideline on Principles and Implementation of Riskmanagement) als international abgestützter, umfassender, vielseitig anwendbarer und offener Risikomanagement-Standard. Die Normenentwürfe zur geplanten Norm ISO 31000 liegen in der Zwischenzeit in einer pre-finalen Form vor. Es ist geplant, dass die finale Fassung Anfang 2009 veröffentlicht wird. Der vorliegende Normenentwurf gliedert sich in vier wesentliche Teile:

- Begriffe und Definitionen
- Prinzipien und Grundsätze des Risikomanagements
- Das Risikomanagement-Framework
- Der Risikomanagementprozess

Die Begriffe und Definitionen stützen sich auf den ebenfalls in Überarbeitung begriffenen ISO Guide 73 ab. Die ISO-Norm 31000 ist generisch und allgemein formuliert, berücksichtigt keine branchenspezifischen Anforderungen an Risikomanagement-Systeme (z.B. im Bereich der Finanzdienstleister, Pharma oder Chemie) und regelt nur die generellen Anforderungen an den Risikomanagementprozess.

Schliesslich ist die ONR 49000 ff. (Risikomanagement für Organisationen und Systeme) zu nennen, welche das Österreichische Normungsinstitut gemeinsam mit deutschen und schweizerischen Spezialisten (Fachgruppe Risikomanagement der Schweizer Swiss Association for Quality), als einheitliches methodisches Rahmenkonzept für ein Riskmanagement entwickelt hat, das für Organisationen und Systeme zur Anwendung empfohlen wird. Auf dieser Grundlage sollen Unternehmen in die Lage versetzt werden, über verschiedene Unternehmensbereiche hinweg Risiken beurteilen, bewäl-

tigen und überwachen zu können. Die ONR 49000 ff beschreibt die Begriffe des Risikomanagements, umreißt die Elemente eines Risikomanagementsystems, definiert Methoden, teilt die Verantwortlichkeiten zu und definiert Anforderungen der beteiligten Mitarbeiter.

Insgesamt wird die Normenreihe ONR 49000 ff. vor allem wegen ihrer Praktikabilität gelobt, zumal sie weit über andere bestehende Standards zur Risikoberichterstattung und Prüfung von Risikomanagementsystemen hinaus geht. Die Integration in bestehende Managementsysteme nach ISO 9001, ISO/TS 16949, ISO 14001 und andere bietet nach Meinung von Experten auch die Chance, die häufig als unüberwindlich geltenden Hürden zwischen Technikern und Kaufleuten in einer Organisation bei der Bewältigung der Risiken einer Organisation zu nehmen.

Fazit

Es gibt zahlreiche Standards und Rahmenwerke, die für die Realisierung eines Risikomanagements als konzeptionelle Grundlage dienen können. Diese weisen als technische Normen (z.B. ISO 31000, ONR 49000) oder allgemein gehaltene Rahmenkonzepte (COSO-ERM) zahlreiche Unterschiede auf, so dass - je nach Hintergrund des Projektes - die Entscheidung für bzw. gegen ein bestimmtes Konzept ausfallen dürfte. Ein internationaler Harmonisierungsbedarf besteht jedoch in jedem Fall, da hierdurch mehr Entscheidungstransparenz gefördert würde. Die bestehende Konkurrenzsituation zwischen den verschiedenen Normen und Standards und deren häufig nationaler Ursprung lässt dies aber wohl nicht erwarten.

Prof. Dr. Thomas Rautenstrauch ist Dozent und Projektleiter am Institut für Finanzdienstleistungen Zug (IFZ) der Hochschule Luzern Wirtschaft und hat darüber hinaus Lehraufträge an der Universität Fribourg sowie weiteren Universitäten in Deutschland und Finnland. Seine Interessen- und Forschungsschwerpunkte liegen im Bereich IKS / Risikomanagement, International Accounting und Controlling. **Stefan Hunziker** ist Wissenschaftlicher Mitarbeiter und Doktorand am IFZ und verfügt zudem über Erfahrungen aus mehreren IKS-Projekten. Für weitere Informationen: www.interne-kontrolle.ch

Quelle: Praxisforum – www.weka-finanzen.ch