1. Grundlagen

1.1. Definitionen

Risiko: „Risiko" bezeichnet die Möglichkeit eines Schadens oder Verlustes als Konsequenz eines bestimmten Verhaltens oder Geschehens.

Risiken sind Bestandteil jeder unternehmerischen Tätigkeit. Risiken beinhalten die Gefahr, dass durch interne oder externe Ereignisse oder durch Handlungen – vornehmlich durch unternehmerische Entscheidungen – Unternehmensziele nicht oder nicht vollständig erreicht werden oder gar der Fortbestand des Unternehmens gefährdet wird.

Chance: Das begriffliche Pendant zum Risiko ist die „Chance". Chance ist im unternehmerischen Kontext die positive Auswirkung eines Ereignisses oder einer Entscheidung auf die Geschäftstätigkeit der Unternehmung bzw. die Übererfüllung von geplanten Unternehmenszielen.

Die Bewältigung und Steuerung von Risiken bzw. Chancen ist die Hauptaufgabe des Risikomanagements.

Risikomanagement: Das unternehmensweite Risikomanagement ist ein strukturierter, einheitlicher und schrittweiser Prozess zur Identifikation, Bewertung, Entscheidung, Reaktion und Berichterstattung hinsichtlich Chancen und Risiken, welche das Erreichen der Unternehmensziele beeinflussen können.[1]

Um das Ziel eines unternehmensweiten Risikomanagements zu erfüllen, nämlich die Risiken frühzeitig zu erkennen und gegebenenfalls geeignete Mittel zur Abwehr von internen und externen Entwicklungen zur Verfügung zu stellen, ist ein methodischer Ansatz – das Risikomanagementsystem – notwendig.

Das diesem Buch zu Grunde liegende Enterprise Risk Management ist jener Teil des Risikomanagementsystems, der sich unternehmensweit mit den bewerteten Risiken und Chancen auseinandersetzt, um durch ein planmäßiges, strategiekonformes Vorgehen den Unternehmenswert zu sichern.

Risikomanagementsystem: Unter Risikomanagementsystem werden alle organisatorischen, technischen, personellen und prozessualen Vorkehrungen verstanden, die ein Unternehmen zum professionellen Umgang mit Risiken (und Chancen) einsetzt.[2]

Das Risikomanagementsystem besteht aus:

- der Risikopolitik und -strategie
- der Risikomanagement-Aufbauorganisation und
- dem operativen Risikomanagementprozess

---

1 IIA Position Paper – The Role of Internal Audit in Enterprise-Wide Risk Management, 2009, S. 2.

2 *Wiederkehr*/*Züger*, Risikomanagementsystem im Unternehmen: Grundlagen mit zahlreichen Beispielen, Repetitionsfragen und Antworten, 2010, S. 18.

Das **Ziel** eines effektiven Risikomanagementsystems besteht im Wesentlichen in
- der Sicherung des Fortbestandes eines Unternehmens,
- der Absicherung der Unternehmensziele und
- der Erhöhung der Planungssicherheit.

Das Risikomanagementsystem unterstützt das Management, bei unternehmerischen Entscheidungen Chancen und Risiken gegeneinander abzuwägen.[3]

Risikopolitik: wesentlicher Teil der Geschäftspolitik; legt die Leitlinien im Umgang mit Risiken innerhalb der gesetzlichen und sonstigen Rahmenbedingungen fest.

Risikomanager: stellt in seiner Koordinationsfunktion sicher, dass das Risikomanagement im Unternehmen entsprechend den Vorgaben des Top Managements implementiert und gelebt wird (idealerweise als Stabsstelle der Geschäftsführung direkt unterstellt).

Risikoverantwortlicher (Risk Owner): Mitarbeiter – meist der operativ Verantwortliche –, der für die Beobachtung, Bewertung und Berichterstattung über die seinem Bereich zugeordneten Risiken, die Festlegung von geeigneten Maßnahmen zur Risikobewältigung sowie für deren Umsetzung persönlich bzw. gemeinsam mit dem Top Management verantwortlich ist.

1.2. Normative Vorgaben

1.2.1. Regelungen in Österreich

1.2.1.1. Gesetzliche Regelungen

Bei näherer Betrachtung der gesetzlichen Regelungen in Österreich zum Thema Risikomanagement wird schnell deutlich, dass es nur wenige Gesetzesstellen gibt, bei denen explizit auf das Thema Bezug genommen wird.

Konkrete Regelungen betreffen vornehmlich Unternehmen im öffentlichen Interesse, Banken, Versicherungen und den öffentlichen Sektor.

Mit dem Unternehmensrechts-Änderungsgesetz 2008 (URÄG 2008) hat der Gesetzgeber, zumindest bei Unternehmen im öffentlichen Interesse, der Überwachung des Risikomanagements mehr Gewicht eingeräumt.

Eine rechtliche Verpflichtung für die Einrichtung und in weiterer Folge auch Überwachung der Wirksamkeit des Risikomanagementsystems für **Kapitalgesellschaften** ergibt sich seit Inkrafttreten des URÄG 2008 aus folgenden Bestimmungen:

Bei **Unternehmen im öffentlichen Interesse**, das sind entweder
- börsennotierte Unternehmen oder (nur für GmbHs aufsichtsratspflichtige § 29 GmbHG) Gesellschaften mit Umsatzerlösen von mehr als 192,5 Millionen

[3] *Amling/Bantleon*, Handbuch der Internen Revision, Grundlagen, Standards, Berufsstand, 2007, S. 117.

Euro oder einer Bilanzsumme von mehr als 96,25 Millionen Euro, wenn eines der beiden Merkmale in zwei aufeinander folgenden Geschäftsjahren überschritten wurde (vgl. § 92 Abs. 4a AktG, § 30g Abs. 4a GmbHG, § 51 Abs. 3 SE-G, § 24c Abs. 6 Genossenschaftsgesetz); oder

- Kreditinstitute jedweder Rechtsform, deren Bilanzsumme eine Milliarde Euro übersteigt oder die übertragbare Wertpapiere ausgegeben haben, die zum Handel an einem geregelten Markt gemäß § 1 Abs. 2 Börsegesetz zugelassen sind (vgl. § 63 a Abs. 4 BWG); oder
- Versicherungsunternehmen jedweder Rechtsform, deren verrechnete Prämien des gesamten, auf Grund der Konzession betriebenen Geschäfts 750 Millionen Euro übersteigen oder die übertragbare Wertpapiere ausgegeben haben, die zum Handel an einem geregelten Markt gemäß § 1 Abs. 2 BörseG zugelassen sind (vgl. § 82b Abs. 4 VAG),

ist ein Prüfungsausschuss zu bestellen.

Zu den Aufgaben des Prüfungsausschusses zählt unter anderem:

Die Überwachung der Wirksamkeit des internen Kontrollsystems, gegebenenfalls des internen Revisionssystems, und des Risikomanagementsystems der Gesellschaft.

Inhaltliche Vorgaben, wie ein Risikomanagementsystem zu gestalten ist, finden sich vornehmlich in rechtlichen Vorgaben für Banken und Versicherungen (Details siehe Kap. 6.2 und 6.3).

Rechtliche Vorgaben, welche persönlichen Voraussetzungen im Bereich Risikomanagement tätige Mitarbeiter zu erfüllen haben, finden sich nur sehr eingeschränkt (z.B. § 25 Pensionskassengesetz).

Kapitalgesellschaften sind unter bestimmten Voraussetzungen verpflichtet, über ihr Risikomanagement zu berichten (vgl. Berichterstattung im Lagebericht § 243a Abs. 2 UGB und im Konzernlagebericht § 267 Abs. 1 UGB).

1.2.1.2. Österreichischer Corporate Governance Kodex

Mit dem Österreichischen Corporate Governance Kodex in der aktuellen Fassung vom Juli 2012[4] wird österreichischen (börsennotierten) Aktiengesellschaften ein Ordnungsrahmen für die Leitung und Überwachung des Unternehmens zur Verfügung gestellt. Durch die Verpflichtung zur Einhaltung des Corporate Governance Kodex soll das Vertrauen der Aktionäre durch Schaffung von Transparenz, durch Verbesserungen im Zusammenwirken zwischen Aufsichtsrat, Vorstand und den Aktionären sowie durch Orientierung an langfristiger Wertschaffung gefördert werden.

Seit dem URÄG 2008 haben alle österreichischen börsennotierten Unternehmen nach § 243b UGB einen Corporate Governance Bericht abzugeben.

[4] Siehe http://www.corporate-governance.at/.

Der Kodex selbst beinhaltet Regeln verschiedener Prioritätsstufen für Unternehmen, die sich durch drei definierte Regelkategorien ergeben, wie der folgende Auszug aus dem Kodex zeigt:

- Legal Requirement (L): Die Regel beruht auf zwingenden Rechtsvorschriften
- Comply or Explain (C): Die Regel soll eingehalten werden; eine Abweichung muss erklärt und begründet werden, um ein kodexkonformes Verhalten zu erreichen
- Recommendation (R): Regel mit Empfehlungscharakter; die Nichteinhaltung ist weder offenzulegen noch zu begründen

Der Code of Corporate Governance soll helfen, die Unternehmensüberwachung zu verbessern und gleichzeitig das Vertrauen in das Management zu stärken.

Im Detail setzt sich der Österreichische Corporate Governance Kodex in folgenden Regeln mit Risikomanagement auseinander:

Vorstand

L Regel 9 *„Der Vorstand informiert den Aufsichtsrat regelmäßig, zeitnah und umfassend über alle relevanten Fragen der Geschäftsentwicklung, einschließlich der Risikolage und des Risikomanagements der Gesellschaft und wesentlicher Konzernunternehmen. Bei wichtigem Anlass hat der Vorstand dem Vorsitzenden des Aufsichtsrats unverzüglich zu berichten ....“*

Aufsichtsrat

L Regel 40 *„Der Prüfungsausschuss hat […] die Wirksamkeit des unternehmensweiten internen Kontrollsystems, gegebenenfalls des internen Revisionssystems und des Risikomanagementsystems der Gesellschaft zu überwachen.“*

Berichtswesen

L Regel 69: *„Die Gesellschaft legt im Konzernlagebericht eine angemessene Analyse des Geschäftsverlaufes vor und beschreibt darin wesentliche finanzielle und nicht-finanzielle Risiken und Ungewissheiten, denen das Unternehmen ausgesetzt ist sowie die wichtigsten Merkmale des internen Kontrollsystems und des Risikomanagementsystems im Hinblick auf den Rechnungslegungsprozess.“*

C Regel 70: *„Die Gesellschaft beschreibt im Konzernlagebericht die wesentlichen eingesetzten Risikomanagement-Instrumente in Bezug auf nicht-finanzielle Risiken.“*

Abschlussprüfer

C Regel 83: *„Darüber hinaus hat der Abschlussprüfer auf Grundlage der vorgelegten Dokumente und der zur Verfügung gestellten Unterlagen die Funktionsfähigkeit des Risikomanagements zu beurteilen und dem Vorstand zu berichten. Dieser Bericht ist ebenfalls dem Vorsitzenden des Aufsichtsrats zur*

Kenntnis zu bringen. Dieser hat Sorge zu tragen, dass der Bericht im Prüfungsausschuss behandelt wird und im Aufsichtsrat darüber berichtet wird."

1.2.2. Regelungen in Deutschland

1.2.2.1. Gesetzliche Regelungen

Aufgrund der wirtschaftlichen und sozialen Verflechtung mit Deutschland ist aus österreichischer Sicht ein Blick in das Nachbarland besonders interessant.

Zum Thema Risikomanagementsystem ist die Regelung des § 91 Abs. 2 dAktG von Bedeutung, wonach „d*er Vorstand geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten hat, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden."*

Diese grundlegende Bestimmung zur Organisation einer Aktiengesellschaft verpflichtet den Vorstand, für ein angemessenes Risikomanagement und für eine angemessene Interne Revision im Unternehmen zu sorgen.

Es finden sich keine entsprechenden Bestimmungen zu § 91 dAktG im dGmbHG oder dPersonengesellschaftsG. Unter den allgemeinen Sorgfaltspflichten eines GmbH- Geschäftsführers nach § 43 Abs. 1 dGmbHG wird aber – nicht zuletzt als Folge der Bestimmungen des AktG – u.a. auch die Einrichtung eines Risikomanagementsystems subsumiert.

Kapitalgesellschaften, die nach § 137 dHGB zur Aufstellung eines Lageberichtes verpflichtet sind, müssen in diesem *die voraussichtliche Entwicklung mit ihren wesentlichen Chancen und Risiken beurteilen und erläutern; zugrunde liegende Annahmen sind anzugeben* (§ 289 Abs. 1 dHGB).

Kapitalmarktorientierte Kapitalgesellschaften haben nach § 324 dHGB einen Prüfungsausschuss einzurichten. Näher definiert § 107 Abs. 3 dAktG, dass sich der Prüfungsausschuss mit der *Überwachung des Rechnungslegungsprozesses, der Wirksamkeit des internen Kontrollsystems, des Risikomanagementsystems und des internen Revisionssystems sowie der Abschlussprüfung, hier insbesondere der Unabhängigkeit des Abschlussprüfers und der vom Abschlussprüfer zusätzlich erbrachten Leistungen, befasst.*

Der Wirtschaftsprüfer hat bei börsennotierten Aktiengesellschaften im Rahmen der Prüfung zu beurteilen, ob der Vorstand die ihm nach § 91 Abs. 2 dAktG obliegenden Maßnahmen in einer geeigneten Form getroffen hat und ob das danach einzurichtende Überwachungssystem seine Aufgaben erfüllen kann. Zudem ist zu prüfen, *ob der Lagebericht insgesamt eine zutreffende Vorstellung von der Lage des Unternehmens und der Konzernlagebericht insgesamt eine zutreffende Vorstellung von der Lage des Konzerns vermittelt. Dabei ist auch zu prüfen, ob die Chancen und Risiken der künftigen Entwicklung zutreffend dargestellt sind* (§ 317 Abs. 2 dHGB).

Der Wirtschaftsprüfer hat im Prüfbericht u.a. darzustellen, *ob Maßnahmen erforderlich sind, um das interne Überwachungssystem zu verbessern* (§ 321 Abs. 4 dHGB).

1.2.2.2. Deutscher Corporate Governance Kodex

Der von der Regierungskommission Deutscher Corporate Governance Kodex erarbeitete Deutsche Corporate Governance Kodex (DCGK) ist gesetzlich im § 161 dAktG für börsennotierte Unternehmen insoweit verankert, als jährlich ein Corporate Governance Bericht abzugeben ist.

Der aktuelle DCGK vom Mai 2013 sieht zum Thema Risikomanagement im Punkt 3.4. u.a. vor:

Der Vorstand informiert den Aufsichtsrat regelmäßig, zeitnah und umfassend über alle für das Unternehmen relevanten Fragen der Strategie, der Planung, der Geschäftsentwicklung, der Risikolage, des Risikomanagements und der Compliance. Er geht auf Abweichungen des Geschäftsverlaufs von den aufgestellten Plänen und Zielen unter Angabe von Gründen ein.

Zu den Aufgaben des Vorstandes zählt nach 4.1.4.:

Der Vorstand sorgt für ein angemessenes Risikomanagement und Risikocontrolling im Unternehmen.

Zu den Aufgaben des Aufsichtsrates zählt nach 5.2.:

Der Aufsichtsratsvorsitzende soll zwischen den Sitzungen mit dem Vorstand, insbesondere mit dem Vorsitzenden bzw. Sprecher des Vorstands, regelmäßig Kontakt halten und mit ihm Fragen der Strategie, der Planung, der Geschäftsentwicklung, der Risikolage, des Risikomanagements und der Compliance des Unternehmens beraten …

Der Prüfungsausschuss hat nach 5.3.2. u.a. folgende Aufgabe:

Der Aufsichtsrat soll einen Prüfungsausschuss (Audit Committee) einrichten, der sich insbesondere mit der Überwachung des Rechnungslegungsprozesses, der Wirksamkeit des internen Kontrollsystems, des Risikomanagementsystems und des internen Revisionssystems, der Abschlussprüfung, hier insbesondere der Unabhängigkeit des Abschlussprüfers, der vom Abschlussprüfer zusätzlich erbrachten Leistungen, der Erteilung des Prüfungsauftrags an den Abschlussprüfer, der Bestimmung von Prüfungsschwerpunkten und der Honorarvereinbarung sowie – falls kein anderer Ausschuss damit betraut ist – der Compliance, befasst.

1.2.3. Regelungen in der Schweiz

1.2.3.1. Gesetzliche Regelungen

Durch die Aufhebung des Artikels 663b Z 12 Obligationenrecht (chOR) durch das neue Buchführungs- und Rechnungslegungsrecht kam es mit Inkrafttreten per 1.1.2013 zu einer Entschärfung der Vorschriften im Zusammenhang mit Risikomanagement für Schweizer Unternehmen.