Axel P. Lehmann* / Katja Roth Pellanda**

Agenda für ein (besseres) Risikomanagement durch den Verwaltungsrat

Inhaltsübersicht

I. Einleitung

Die Anforderungen, welche an ein effektives Risikomanagement gestellt werden, sind in den letzten Jahren durch die zunehmende Internationalisierung und Globalisierung der Geschäftstätigkeiten und deren technologische Entwicklungen laufend gestiegen.[1] Zusätzlich hat die globale Finanzkrise das Vertrauen der Investoren in den Kapitalmarkt und den Finanzsektor erschüttert. Mit der gegenwärtigen Krise hat das Risikomanagement und die Frage nach einer Verantwortlichkeit für Missmanagement daher an zusätzlicher Bedeutung gewonnen und ist nun auch ins Bewusstsein einer breiteren Öffentlichkeit gedrungen. Neben einer hohen Medienaufmerksamkeit[2] und der Sensibilisierung der Investoren befassen sich nun auch der Gesetzgeber und die Regulatoren zunehmend mit dieser Thematik. Als aktuelle Beispiele kann aus Schweizer Sicht einerseits auf die seit dem 1. Januar 2008 geltende Pflicht zu Angaben über eine Risikobeurteilung in der Jahresrechnung durch den Verwaltungsrat (Art. 663b Ziff. 12 OR) und zur Überprüfung der Existenz eines internen Kontrollsystems (IKS) durch die Revisionsstelle (Art. 728a Abs. 1 Ziff. 3, Abs. 2 sowie Art. 728b Abs. 1 OR) bei Aktiengesellschaften sowie andererseits auf das von der Eidgenössischen Finanzmarktaufsicht (FINMA) geplante Rundschreiben zu den Vergütungssystemen von Finanzinstituten hingewiesen werden, welches insbesondere das Setzen von Anreizen für unangemessene Risiken durch solche Systeme verhindern soll[3]. Auf internationaler Ebene sind die Turnbull Guidance für interne Kontrolle durch den Verwaltungsrat (1999/2005)[4], der im März 2009 publizierte Turner Review[5] über die Möglichkeiten einer regulatorischen Antwort auf die globale Bankenkrise sowie der Mitte Juli 2009 veröffentlichte Walker Review[6] über Corporate Governance in englischen Banken und anderen Finanzinstituten hervorzuheben, welche sich alle mit Fragen des Risikomanagements befassen. Anfangs Mai 2008 hat überdies die Kreditratingagentur Standard & Poor's mitgeteilt, dass sie ab 2009 auch für Unternehmen ausserhalb des Finanzbereichs eine Beurteilung des Risikomanagements in ihre Bewertungen mit einbeziehen wird.[7] Insofern kommt dem Risikoma-

---

* Prof. Dr. oec., Mitglied des Group Executive Committee und Group Chief Risk Officer der Zurich Financial Services Group, Titularprofessor für Betriebswirtschaftslehre und Dienstleistungsmanagement an der Universität St. Gallen.

** Dr. iur., Rechtsanwältin, Bär & Karrer AG, Zürich; zur Zeit London School of Economics, London.

1 Ausführlich zur Bedeutung der Globalisierung für das Risikomanagement Wyss Lukas, Juristisches Risk Management und Hedging als Mittel zur Risikokontrolle, Diss. Bern 2005, 39 ff.

2 Siehe etwa folgende kürzlich in der Financial Times erschienenen Artikel: Grant Jeremy, Risk management: Blue-sky approach sought for improving early warning, 17. Juni 2009; Birkinshaw Julian/Jenkings Huw, Personalising risk management, 12. Februar 2009.

3 Siehe den Entwurf des Rundschreibens «Vergütungssysteme» der Eidgenössischen Finanzmarktaufsicht (FINMA), Juni 2009, <http://www.finma.ch/d/regulierung/anhoerungen/Documents/rs-verguetungssysteme-20090524-d.pdf>, nachfolgend «Entwurf Rundschreiben» sowie den Erläuterungsbericht zum Rundschreiben «Vergütungssysteme» der FINMA, Juni 2009, <http://www.finma.ch/d/regulierung/anhoerungen/Documents/bericht-verguetungssysteme20090602-d.pdf>.

4 Turnbull Guidance – Internal Control: Revised Guidance For Directors On the Combinded Code (Oktober 2005) des Financial Reporting Council, <http://www.frc.org.uk>.

5 Turner Review – A regulatory response to the global banking crisis, März 2009, <http://www.fsa.gov.uk/pubs/other/turner_review.pdf>, nachfolgend «Turner Review».

6 Walker Review – A review of corporate governance in UK banks and other financial industry entities, <http://www.hm-treasury.gov.uk/walker_review_information.htm>, nachfolgend «Walker Review»; siehe für erste Reaktionen den in der Financial Times erschienene Artikel: Jenkins Patrick/Parker George, Bankers hit back at Walker Review, 17. Juli 2009.

7 Siehe die Mitteilung von Standard & Poor's vom 7. Mai 2008, <http://www.towersperrin.com/tp/getwebcachedoc?webc=HRS/USA/2008/200805/ERM4Corp.pdf>.

nagement zunehmend auch eine Bedeutung für Unternehmen ausserhalb der Finanzbranche zu.

Risikomanagement ist aber bereits seit langem weit mehr als ein blosser Trendbegriff und stellt eine strategische Notwendigkeit für jedes Unternehmen dar. Unter Risikomanagement wird grundsätzlich der systematische Prozess des Umgangs mit (externen und internen) Unternehmensrisiken verstanden. Risiken für Unternehmen ergeben sich aus einer Vielzahl von Faktoren und können etwa in der Branchenzugehörigkeit, der Unternehmensgrösse, der technologischen Fortentwicklung, der Arbeitsmarktverhältnisse, der Finanzierungs- und Liquiditätslage, der internen Organisation, der Konkurrenzsituation und den externen Einflüssen von Stakeholdern oder der Umwelt bestehen.[8] Die Herausforderung des Risikomanagements liegt einerseits im Auffinden von sog. «Black Swans» (darunter sind positive, aber auch negative Zufallsereignisse mit grossen Auswirkungen zu verstehen, die mit auf historischen Daten basierenden Risikomodellen grundsätzlich nicht vorhersehbar und berechenbar sind)[9], andererseits aber auch im Herbeiführen einer optimalen Balance zwischen (notwendigem) Risiko und (erwünschtem) Ertrag und keineswegs in der Vermeidung sämtlicher potenzieller Risiken denn «without risk, there is no successfull business». Risikomanagement im umfassenden Sinne eines Enterprise Risk Management ist damit nicht nur auf die Vermeidung und Verringerung von Verlusten ausgerichtet. Das bewusste Eingehen von Risiken muss aus unternehmerischer Perspektive auch immer im Zusammenhang mit dem entsprechenden Chancen- und Ertragspotenzial gesehen werden. Das Eingehen grosser Risiken kann akzeptabel sein, wenn es für ein Unternehmen nachhaltige Werte schafft, indem diesen Risiken entsprechend grosse Ertragschancen gegenüberstehen (sog. risk/return Profil). Insofern gehört das bewusste Eingehen von Risiken zum integralen Bestandteil jeder Geschäftstätigkeit. Da in den meisten Risiken sowohl Chancen als auch Gefahren liegen, stellt sich jeweils die Frage, welche Risiken tragbar sind und durch welche Massnahmen unerwünschte Risiken vermieden oder zumindest auf ein annehmbares Mass reduziert werden können. Da sich Risiken letztlich aus einem Handeln unter unvollständiger Information ergeben, besteht die Kunst des Risikomanagements darin, den «Schleier der Ungewissheit» über die Wirkungen eigener (und fremder) Handlungen bzw. Unterlassungen so weit als möglich zu heben. Risikomanagement ist daher keine einmalige Aktion oder eine Art Krisenmanagement, sondern ein Instrument, zur nachhaltigen Erreichung der Geschäftsziele, das deshalb anhaltende Beachtung erfordert.

In der juristischen Literatur wurden die Aufgaben und Verantwortlichkeiten des Verwaltungsrates bezüglich des Risikomanagements lange stiefmütterlich behandelt.[10] Erst mit dem Inkrafttreten der neuen Art. 663b Ziff. 12, 728a und 728b OR auf den 1. Januar 2008 fand eine gewisse Annäherung an diese Thematik statt, wobei jedoch der interdisziplinäre Aspekt und damit die Verknüpfung mit wirtschaftlichen Überlegungen weitgehend vernachlässigt wurde. Nach wie vor herrscht sowohl über die materielle Tragweite dieser Bestimmungen als auch über die weiteren Pflichten des Verwaltungsrates im Bereich des Risikomanagements wenig Konsens. Unbestritten ist jedoch, dass das Risikomanagement der unternehmerischen Tätigkeit keine neue Aufgabe darstellt, sondern der Verwaltungsrat bereits vor Inkrafttreten dieser Gesetzesbestimmungen gehalten war, sich mit den unternehmensspezifischen Risiken auseinander zu setzen. Dies ergibt sich nicht nur aus der in Art. 716a OR verankerten Pflicht zur Oberaufsicht über die Geschäftsleitung und Festlegung der Organisation, sondern ein effektives und effizientes Risikomanagement wird auch verlangt, um den Ansprüchen einer *Good Corporate Governance* gerecht zu werden[11].[12] Für Finanzinstitute wird die Pflicht zur Etablierung eines Risikomanagements zudem explizit in der bankenrechtlichen Spezialgesetzgebung[13,14] statuiert, denn ein

---

8 Vgl. Botschaft zur Änderung des Obligationenrechts (Revisionspflicht im Gesellschaftsrecht) sowie zum Bundesgesetz über die Zulassung und Beaufsichtigung der Revisorinnen und Revisoren, BBl 2004, 4036 (nachfolgend «Botschaft Revisionspflicht», <http://www.admin.ch/ch/d/ff/2004/3969.pdf>).

9 Das Konzept und der Begriff «Black Swans» wurde von Taleb entwickelt: Taleb Nassim Nicholas, The Black Swan – The Impact of the Highly Improbable, London 2007.

10 Siehe aus betriebsökonomischer Sicht die empirische Studie von Kalia Vinay, Risk Management at Board and Management Levels, Diss. St. Gallen/Bamberg 2006.

11 Gemäss Ziff. 19 des Swiss Code of Best Practice for Corporate Governance (nachfolgend «SCBP») hat der Verwaltungsrat für ein dem Unternehmen angepasstes internes Kontrollsystem und Risikomanagement zu sorgen, wobei sich letzteres sowohl auf finanzielle als auch auf operationelle Risiken beziehen soll, <http://www.economiesuisse.ch/web/de/pdf%20download%20files/pospap_swiss-code_corp-govern_20080221_de.pdf>; siehe auch Ziff. 24 und 30 SCBP.

12 Ausführlich hierzu Crouhy Michel/Galai Dan/Mark Robert, The Essentials of Risk Management, New York 2006, 83 ff.; vgl. auch Coyle Brian, Risk Awareness and Corporate Governance, Canterbury 2002, 4.

13 Hervorzuheben ist hier insb. Art. 9 Abs. 2 BankV (SR 952.02), wonach eine Bank die Grundzüge des Risikomanagements sowie die Zuständigkeiten und das Verfahren für die Bewilligung von risikobehafteten Geschäften in einem Reglement oder in internen Richtlinien zu regeln und überdies insb. Markt-, Kredit-, Ausfall-, Abwicklungs-, Liquiditäts- und Imagerisiken sowie operationelle und rechtliche Risiken zu erfassen, zu begrenzen und zu überwachen hat. Zu berücksichtigen ist aber auch die Eigenmittelverordnung (SR 952.03) sowie die dazugehörigen Rundschreiben der FINMA zu den Eigenmittelanforderungen, (<http://www.finma.ch/d/regulierung/Seiten/rundschreiben.aspx>), und das Rundschreiben der FINMA «Überwachung und Interne Kontrolle bei Banken» vom 20. November 2008 (nachfolgend FINMA-RS 2008/24, <http://www.finma.ch/d/regulierung/Documents/finma-rs-2008-24.pdf>).

14 Ausführlich zu den gesetzlichen Vorschriften betreffend das Risikomanagement von Banken Othmar Strasser, Antwort einer

wirkungsvolles Risikomanagement stellt naturgemäss einen der bedeutungsvollsten strategischen Erfolgsfaktor eines Finanzinstitutes dar.[15] Ein aus der Realisierung eines Risikopotenzials entstandener Schaden kann nicht nur den Unternehmenserfolg behindern, sondern – insbesondere im Falle von Banken – auch die Funktionsfähigkeit von Finanzinfrastrukturen erheblich beeinträchtigen. Risikomanagement ist demzufolge nichts Neues, aber die Bedeutung des Risikomanagements wird in Zukunft für sämtliche Unternehmen, insbesondere aber für Finanzinstitute, weiter zunehmen und seine Angemessenheit wird vom Markt genau beobachtet und beurteilt werden.

Die nachfolgenden Ausführungen sollen namentlich aufzeigen, welche Aufgaben der Verwaltungsrat im Bereich des Risikomanagements zu übernehmen hat und wie er diesen nach Ansicht der Autoren am besten nachkommt. Schliesslich wird eine Agenda für ein besseres Risikomanagement durch den Verwaltungsrat vorgeschlagen.

II. Definition und Abgrenzung

Risikomanagement ist eine umfangreiche Aufgabe, welche verschiedene Tätigkeiten beinhaltet und von verschiedenen Funktionsträgern innerhalb eines Unternehmens wahrgenommen werden kann. Da die Abgrenzungen teilweise unklar sind, lohnt es sich, an dieser Stelle auf die gebräuchliche Terminologie einzugehen. Vorab sei festgehalten, dass unter Risiko grundsätzlich (Zufalls-)Ereignisse zu verstehen sind, die in ihrer Entstehung und Ausprägung schwer zu prognostizieren und zu beeinflussen sind. Als negatives Risiko gilt jedes Ereignis und/oder jede Handlung, welche die Gefahr einer negativen Abweichung von Erwartungen in sich birgt und dadurch ein Unternehmen daran hindern kann, seine Geschäftsziele zu erreichen bzw. die gewählte Strategie erfolgreich umzusetzen.[16] Ein positives Risiko wird zumeist in einem Unternehmenserfolg resultieren. Risiko beschreibt somit die Möglichkeit, dass sich die Ziele und Erwartungen eines Systems nicht erfüllen und es wird vielfach auch als Streuung um einen Erwartungswert definiert.

1. Internes Kontrollsystem (IKS)

Das IKS hat erst mit dem Inkrafttreten von Art. 728a und 728b OR explizit Einzug ins Aktienrecht[17] gehalten.[18] Diese Bestimmungen verlangen von der externen Revisionsstelle seit dem 1. Januar 2008 bei allen ordentlich revidierten Gesellschaften die Prüfung der Existenz eines IKS, die schriftliche Berichterstattung über das Ergebnis der Revision an die Generalversammlung sowie einen umfassenden Bericht mit Feststellungen über das IKS an den Verwaltungsrat.[19] Eine gesetzliche Definition sowie eine Umschreibung des materiellen Gehaltes dieses aus der US-amerikanischen betriebswirtschaftlichen Praxis stammenden Begriffs fehlen hingegen weiterhin. Die konkrete Ausgestaltung des IKS liegt damit im Ermessen der einzelnen Unternehmen und in der Verantwortung des Verwaltungsrates,[20] wobei den anerkannten Rahmenwerken[21] bei der Wahl der jeweiligen Massnahmen wesentliche Bedeutung zukommt. Nach der von der Treuhand-Kammer in ihrem Positionspapier von 2006 enthaltenen Definition ist das IKS ein Managementinstrument zur zweckmässigen Sicherstellung der Erreichung von Unternehmenszielen in den Bereichen «Prozesse», «Informationen», «Vermögensschutz» und «Compliance».[22] Gemäss dem US-amerikanischen Committee of Sponsoring Organization of the Treadway Commission (COSO), welches den Begriff international prägte, hat das IKS drei Ziele:

Bank auf die erhöhte Verantwortlichkeit im Unternehmen aus zivil-, straf- und verwaltungsrechtlicher Sicht – oder Management von Compliance Risiken als Aufgabe von Unternehmensjuristen, in: Niggli/Amstutz (Hrsg.), Verantwortlichkeit im Unternehmen – Zivil- und strafrechtliche Perspektiven, Basel 2007, 252 ff.

15 Ausführlich zum Risikomanagement bei Banken Emch Urs/Renz Hugo/Arpagaus Reto, Das Schweizerische Bankgeschäft, 6. Aufl., Zürich/Basel/Genf 2004, N 2823 ff.

16 Vgl. Wyss Hans-Peter, Integriertes Risikomanagement, ST 2000, 179; siehe auch Haller Matthias:«Je planmässiger die Menschen vorgehen, desto wirksamer vermag sie der Zufall zu treffen» (Friedrich Dürrenmatt), in: I.VW-Jahresbericht 2003, St. Gallen 2004, 4 ff. – Abschiedsvorlesung – St. Gallen.

17 Für Banken (Art. 9 Abs. 4 BankV) sowie Versicherungsunternehmen (Art. 96 Abs. 1 AVO, SR 961.011) war die Errichtung eines wirksamen internen Kontrollsystems bereits seit langem explizit gesetzlich vorgeschrieben.
Demgegenüber bestimmt Art. 9 Abs. 4 BankV, dass Banken für ein wirksames internes Kontrollsystem zu sorgen und insbesondere eine von der Geschäftsführung unabhängige interne Revision zu bestellen haben.

18 Im Vorentwurf zur Teilrevision des Aktienrechts war vorgesehen, in Art. 716a OR den Begriff «Finanzkontrolle» durch «interne Kontrolle» zu ersetzen (siehe Begleitbericht zum Vorentwurf zur Revision des Aktien- und Rechnungslegungsrechts im Obligationenrecht vom 2. Dezember 2005, 83, <http://www.ejpd.admin.ch/etc/medialib/data/wirtschaft/gesetzgebung/aktienrechtrevision.Par.0004.File.tmp/05-11-30%20defFassung-BegleitberichtVarianteEDA.pdf>; davon wurde im Entwurf zur Aktienrechtsrevision nun aber wieder abgesehen.

19 Ausführlich zum internen Kontrollsystem und dessen Prüfung durch die Revisionsstelle Böckli Peter, Schweizer Aktienrecht, 4. Aufl., Basel 2009, § 15 N 247 ff., N 331 ff.

20 Vgl. Böckli (FN 19), § 15 N 254.

21 Dazu gehören u.a. der in Zusammenarbeit zwischen dem «Institute of Risk Management» (IRM), der «Association of Insurance and Risk Managers» (AIRMIC) sowie dem «National Forum for Risk Management in the Public Sector» (ALARM) im Jahre 2002 veröffentlichte Risk Management Standard (<http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf>) und das vom «Committee of Sponsoring Organization of the Treadway Commission» (COSO) im Jahre 2004 erlassene Enterprise Risk Management Framework, <http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf>.

22 Vgl. IKS-Positionspapier der Treuhand-Kammer, Änderungen Obligationenrecht – Berücksichtigung des internen Kontrollsystems in der Abschlussprüfung, März 2006.

(1) Effektivität und Effizienz der Geschäftsprozesse,
(2) Zuverlässigkeit der Finanzberichterstattung und
(3) Einhaltung der anwendbaren Gesetze und Normen.[23]

Zur Erreichung dieser Ziele muss das IKS verschiedene untereinander vernetzte Elemente aufweisen. Dazu gehören: (i) Information und Kommunikation über die Geschäftsaktivitäten; (ii) Risikobeurteilung; (iii) Errichtung eines angemessenen Kontrollumfeldes; (iv) Massnahmen und Prozesse zur Kontrolle sowie (v) Überwachungsmassnahmen.[24] Ausgangspunkt des IKS ist die Risikobeurteilung des Unternehmens.[25] Das IKS umfasst die Gesamtheit der Kontrollstrukturen und -prozesse, welche auf allen Ebenen der Geschäftstätigkeit eines Unternehmens die Grundlage für die Erreichung der geschäftspolitischen Ziele und eines ordnungsgemässen Betriebs sowie für die Gewährleistung der Normeneinhaltung bilden.[26] Nicht zum IKS gehört dagegen die Reaktion auf festgestellte Risiken, dies ist Aufgabe des entsprechenden Risikomanagements.

Verschiedene Funktionen innerhalb eines Unternehmens tragen zur Erreichung der oben genannten Ziele bei; dazu gehören neben dem Risikomanagement, sowohl die interne Revision als auch die Compliance und das Controlling.[27] Das Aktienrecht verpflichtet auch heute nicht explizit zur Errichtung einer *internen Revision*; in grösseren Gesellschaften ist der Verwaltungsrat jedoch aufgrund seiner Pflicht zur Ausgestaltung der Finanzkontrolle auf eine interne Revision angewiesen.[28] In kleineren Gesellschaften kann es hingegen zweckmässig sein, die Aufgaben der internen Revision einem externen Berater oder gar einem einzelnen Verwaltungsratsmitglied zu übertragen.[29] Die interne Revision übernimmt als vom täglichen Geschäftsprozess unabhängige Institution – im Sinne der Gewaltenteilung – die eigentliche Kontrollfunktion der betrieblichen Geschäftsführung und die Prüfung des Finanz- und Rechnungswesens unter dem Gesichtspunkt der operativen und finanziellen Risiken[30].[31] Insofern entlasten die internen Revisoren den Verwaltungsrat in seiner Überwachungsfunktion und werden deshalb teilweise auch als «Statthalter des Verwaltungsrates» bezeichnet.[32] Zumeist wird die interne Revision dem Audit Committee unterstellt und hat direkt diesem zu berichten, wobei eine Aufsicht durch ein allfälliges Risk Committee ebenfalls denkbar ist. Nicht empfehlenswert ist hingegen eine Unterstellung unter die Geschäftsleitung, da dies mit der erwünschten Unabhängigkeit in Widerspruch steht[33].[34]

Demgegenüber ist das *Controlling* eine Steuerungshilfe für das Management und beinhaltet die andauernde, ergebnisbezogene Überwachung der Geschäftsaktivitäten im Hinblick auf die Erreichung der definierten Rentabilitäts-, Liquiditäts- und Wirtschaftlichkeitsziele und damit der finanziellen Auswirkungen der Unternehmensführung.[35] Als Teilfunktion der operativen Unternehmensführung obliegt das Controlling der Geschäftsleitung.[36]

Unter *Compliance* versteht man die Einhaltung von gesetzlichen, regulatorischen und innerbetrieblichen Vorschriften sowie die Beachtung von marktüblichen Standards und Standesregeln durch ein Unternehmen.[37] Auf diese Weise deckt die Compliance jenen Aspekt des Risikomanagements ab, der sich mit der Normeneinhaltung sowie den verbundenen Reputationsrisiken befasst.[38] Während die Sicherstellung der Compliance ein Tätigkeitsfeld der Geschäftsleitung darstellt, gehört die Oberaufsicht über die Compliance nach Art. 716a Abs. 1 Ziff. 5 OR zu den unübertragbaren und unentziehbaren Aufgaben des Verwaltungsrates.[39]

---

23 Siehe Internal Control over Financial Reporting – Guidance for Smaller Public Companies (2006), <www.coso.org/publications.htm>; vgl. auch FINMA-RS 2008/24 Rz. 2.

24 Ausführlich Böckli Peter, Revisionsstelle und Abschlussprüfung, Zürich/Basel/Genf 2007, N 248 ff.; siehe auch Pfiffner Daniel Christian, Revisionsstelle und Corporate Governance, Diss. Zürich 2008, N 137 ff.; Bachmann Daniel, Compliance – Rechtliche Grundlagen und Risiken, ST 2007, 94 f.

25 Böckli (FN 19), § 13 N 349.

26 Vgl. Bumbacher Robert-Jan/Hodel Beat, Risk Management und Interne Revision, ST 2000, 1056; Wyss Lukas, Das IKS und die Bedeutung des (Legal) Risk Management für VR und Geschäftsleitung im Lichte der Aktienrechtsreform 2007, SZW 2007, 33; siehe auch FINMA-RS 2008/4 Rz. 2.

27 Siehe Iseli Thomas, Führungsorganisation im Aktien-, Banken- und Versicherungsrecht, Diss. Zürich 2008, N 395; Pfiffner (FN 24), N 137 ff.; Wyss (FN 26), 32 ff.

28 Vgl. BSK OR II-Watter/Roth Pellanda, Art. 716a OR N 17; Böckli (FN 19), § 15 N 313.

29 Ebenso Böckli (FN 19), § 13 N 349, FN 961und § 15 N 317.

30 Gemäss der Formulierung des Instituts of Internal Auditors (IIA) wird unter interner Revision folgende Tätigkeit subsumiert: «Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes», <http://www.theiia.org/guidance/standards-and-guidance/ippf/definition-of-internal-auditing/?search=Definition%20internal%20audit>.

31 Ausführlich Pfiffner (FN 24), N 1178 ff.; sowie Böckli (FN 24), N 313 ff.

32 Pfiffner (FN 24), N 697; kritisch Böckli (FN 19), § 15 N 315.

33 Vgl. Böckli (FN 19), § 15 N 316, 319.

34 Bei Finanzinstituten ist gemäss FINMA RS 2008/24 Rz. 60 eine Unterstellung unter die Geschäftsleitung nicht zulässig.

35 Böckli (FN 24), N 319; Wyss (FN 26), 34.

36 Pfiffner (FN 24), N 148; Böckli (FN 19), § 15 N 319.

37 Vgl. Bachmann (FN 24), 93; Bühler Theodor, Corporate Governance und Compliance, in: von der Crone et al. (Hrsg.), Neuere Tendenzen im Gesellschaftsrecht, Festschrift für Peter Forstmoser, Zürich/Basel/Genf 2003, 211 f.; sowie ausführlich Buff Herbert, Compliance, Diss. Zürich 2000, N 4 ff.

38 Vgl. Bodenmann Jan Marc, Unternehmenssteuerung und –überwachung – Beitrag von Risikomanagement, interner und externer Revision zu einer effektiven Corporate Governance, Diss. St. Gallen/Bamberg 2005, 104 f.

39 Siehe in diesem Zusammenhang Ziff. 20 SCBP, nach welchem der Verwaltungsrat Massnahmen zur Einhaltung der anwendbaren

2. Risikomanagement

Das Risikomanagement im umfassenden Sinne besteht in der systematischen Erfassung, Bewertung, Steuerung, Kommunikation und Überwachung der Risiken eines Unternehmens. Das Ziel ist die gesamthafte Betrachtung von Risiken und die Einschätzung der gesamten Risikoposition des Unternehmens. Wie erwähnt können Risiken dabei positive (Chancen) als auch negative (Gefahren) Auswirkungen haben. Gleichzeitig müssen auch qualitative Aspekte des Risikos und der Risikoentwicklung in den systematischen Prozess des Risikomanagements miteinbezogen werden.[40] Obwohl, wie vorgehend aufgezeigt, verschiedene materielle Berührungspunkte bestehen, ist zum Zweck der «checks and balances» das *Risikomanagement* unabhängig vom IKS und seinen weiteren Bereichen aufzubauen, wobei es gleichzeitig in das IKS eingebettet werden muss.[41]

Ein integriertes Risikomanagement und eine klare Risiko-Governance können verantwortungsvolle Anreize schaffen. Dabei ist es wichtig, dass eine Trennung zwischen den Risikoverantwortlichen («Risk Owner») und den Risikokontrollen («Risk Controls») vorliegt, um allfällige Interessenkonflikte zu vermeiden. Darüber hinaus muss das Risiko-Berichtsystem zeitgerecht und entscheidungsorientiert aufgebaut sein. Konsistente Limiten müssen definiert, implementiert und Risikopositionen zeitnah beobachtet werden.[42]

Nach heutigem betriebswirtschaftlichen Verständnis umfasst das Risikomanagement vier Hauptelemente:

(i) *Strategisches Risikomanagement*: Definition der Risikotoleranz des Unternehmens und Integration von Risikoüberlegungen in die Geschäftsprozesse und strategische Planung, unter Berücksichtigung der Optimierung des Risiko-/Ertragsprofils des Unternehmens.[43]

(ii) *Risikodefinition*: Frühzeitige Erkennung und Systematisierung der konkret für ein Unternehmen vorhandenen Risiken (sog. Risikoinventar oder Risikolandschaft) und Definition einer Risikopolitik, welche die qualitativen und quantitativen risikopolitischen Ziele und Strategien aus der Perspektive des Gesamtunternehmens definiert. Dies erfordert ein integriertes Risikomanagement und damit eine Abkehr von einem isoliert auf einzelne Risikotypen oder einzelne Geschäftseinheiten getrennt vorgenommenen Risikomanagement (sog. «Silodenken»).[44]

(iii) *Risikoidentifikation und -analyse*: Identifikation konkreter Risiken sowie deren Bewertung und wenn möglich Quantifizierung.

(iv) *Risikobewältigung und -kontrolle*: Planung von Strategien und Massnahmen zur Reduktion von Eintrittswahrscheinlichkeit und/oder möglichen Auswirkungen der Risiken. Dazu gehört u.a. die Überwachung der Unternehmensrisiken und die Bereitstellung der hierfür notwendigen Instrumente.[45, 46]

Die Kategorisierung und Systematisierung von möglichen Unternehmensrisiken anhand verschiedener Kriterien spielt in der Praxis eine wichtige Rolle, da sich nur identifizierte Risiken kontrollieren lassen. Entsprechend bilden die einzelnen Risiken und Risikokategorien die Grundlage eines angemessenen Risikomanagements. Grundsätzlich wird in der Praxis unterschieden nach: (a) allg. Unternehmensrisiko (d.h. die Gefahr eines geschäftlichen Misserfolges bzw. Verlustes); (b) Liquiditätsrisiko; (c) Kredit- und Marktrisiko; (d) weitere Risiken (wie bspw. Reputationsrisiken und operationelle Risiken[47]).[48]

Da heute sämtliche externe und interne Unternehmensrisiken und nicht mehr nur Kreditrisiken oder Risiken aus dem operativen Geschäft durch das Risikomanagement erfasst werden müssen, und da Risiken zudem oft korrelieren, wird häufig von integriertem Risikomanagement oder eben Enterprise Risk Management[49]

Normen (Compliance) zu treffen hat und sich mind. einmal jährlich Rechenschaft zu geben hat, ob die für ihn und das Unternehmen anwendbaren Compliance-Grundsätze hinreichend bekannt sind und ihnen dauernd nachgelebt wird.

40 Lehmann Axel P., Riskantes Risikomanagement?!, in: Strebel-Aerni (Hrsg.), Standards für nachhaltige Finanzmärkte, Zürich/Basel/Genf 2008, 110 f.

41 Vgl. Wyss (FN 26), 35.

42 Lehmann (FN 40), 118.

43 Siehe hierzu Lehmann (FN 40), 120 f.

44 Siehe das Prinzip I.i des Final Report of the IIF Committee on Market Best Practices: Principles of Conduct and Best Practice Recommendations, July 2008, 31, <www.iif.com>; nachfolgend «IIF Final Report».

45 Vgl. Bumbacher/Hodel (FN 26), 1054; Amhof Roger/Schweizer Markus, Positives Risikomanagement, ST 2000, 713.

46 Siehe Böckli (FN 24), N 194 ff.; Wyss (FN 26), 36 f.

47 Ausführlich zur Bedeutung und Kontrolle von operativen Risiken Wyss (FN 16), 179 ff.

48 Siehe Lehmann (FN 40), 111 f.; sowie ausführlich zu den Risikokategorien im Bankgeschäft Emch/Renz/Arpagaus (FN 15), N 2858 ff.; vgl. auch Zobl Dieter/Blöchlinger Christoph, in: Weber/Zobl (Hrsg.), Risikomanagement durch Recht im Banken- und Versicherungsbereich, Zürich/Basel/Genf 2006, 15 ff.; Ströckli Beat, Die Organisation von Banken aus privat-, aufsichts-, straf- und standesrechtlicher Perspektive, Diss. St. Gallen/Zürich et. al. 2008, 97.

49 Nach der allgemein anerkannten Definition des US-amerikanischen Committee of Sponsoring Organization of the Treadway Commission (COSO) wird Enterprise Risk Management wie folgt definiert: *«Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives»* (siehe das Executive Summary des «Enterprise Risk Management – Integrated Framework (2004)», <http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf>).

gesprochen[50].[51] Die Herausforderung liegt darin, dass sich die Risiken in materieller Hinsicht durch neue Umfeldentwicklungen, veränderte Geschäftsmodelle oder Prozesse und Instrumente laufend verändern. Das Risikomanagement muss somit nicht statisch sondern proaktiv und dynamisch ausgestattet sein.

III. Der Verwaltungsrat als Träger des Risikomanagements

1. Umfang der Aufgaben

1.1 Im Allgemeinen

Risikomanagement ist eine grundlegende Aufgabe der Geschäftsführung, wobei es heute unbestritten ist, dass sämtliche Unternehmen über ein angemessenes Risikomanagement verfügen müssen. Aus der in Art. 716a OR verankerten Zuständigkeit des Verwaltungsrates zur Organisation des Unternehmens, zur strategischen Führung und zur Aufsicht über die Geschäftsleitung sowie zur Ausgestaltung des Rechnungswesens und der Finanzkontrolle ergibt sich eine rechtliche Pflicht des Verwaltungsrates zur materiellen Auseinandersetzung mit den Unternehmensrisiken. Risikomanagement gehört zur Unternehmensführung, da sich das Eintreten von Risiken im künftigen Ertragspotential niederschlagen kann, welches den Wert des Unternehmens bestimmt.[52] Umstritten ist hingegen, inwiefern der Verwaltungsrat selbst tätig werden muss oder ob er diese Aufgabe und die entsprechenden Verantwortlichkeiten delegieren kann. Häufig findet sich in der Literatur die nicht weiter differenzierte Aussage, dass es sich beim Risikomanagement um eine undelegierbare und unentziehbare Aufgabe des Verwaltungsrates handelt.[53]

Unseres Erachtens ist der Verwaltungsrat für die *Festlegung der allgemeinen Grundsätze im Bereich des Risikomanagements und deshalb für die Risikopolitik* verantwortlich, welche die Entscheidungsgrundlagen für die Risikobewirtschaftung und -überwachung mit Blick auf die individuellen Gegebenheiten (insb. Geschäftsbereiche) enthält.[54] Es handelt sich dabei um eine zentrale Führungsaufgabe. In der Praxis werden die Vorbereitungsarbeiten zumeist von der Geschäftsleitung gemeinsam mit dem Audit Committee[55] oder einem allfälligen Risk Committee vorgenommen und die Risikopolitik anschliessend vom Verwaltungsrat genehmigt sowie mindestens einmal jährlich auf deren Angemessenheit überprüft. Aus rechtlicher Sicht ist jedoch zu beachten, dass der Verwaltungsrat durch diese Vorbereitungsarbeiten nicht von seiner diesbezüglichen Verantwortlichkeit entlastet wird.

In materieller Hinsicht hat eine Risikopolitik, als Ordnungsrahmen für ein globales und integriertes Risikomanagement durch sämtliche Führungsebenen, die folgenden Bereiche zu umfassen:

(i) Ziele des Risikomanagements (u.a. Festlegung der Risikopolitik, Risikogovernance und Risikoprofil des Unternehmens);
(ii) Typologisierung der für das konkrete Unternehmen relevanten Risikotypen und -faktoren;
(iii) Entscheid über den Grad der Risikobereitschaft und der Risikotragfähigkeit («risk tolerance and risk appetite»);[56]
(iv) Grundsätze und Prinzipien bzgl. Identifikation, Messung, Bewirtschaftung und Überwachung der Risiken;
(v) Errichtung einer «risk culture» bzw. «risk awareness» und des Integritätsstandards;
(vi) Festlegung der Organisation (Bereitstellung der nötigen personellen und finanziellen Ressourcen zur effektiven und effizienten Aufgabenerfüllung) sowie der Kompetenzen und Verantwortlichkeiten;
(vii) Errichtung eines Reportingsystems;
(viii) Überwachungsprozess zur periodischen Prüfung und allfälligen Anpassung der Risikopolitik an neue Gegebenheiten (z.B. Entwicklungen im Markt, neue Finanzinstrumente, etc.).[57]

Für den Verwaltungsrat liegt die Schwierigkeit darin, dass die Grundlagen für ein effektives Risikomanagement zwar *top down* erlassen werden, aber gleichzeitig problemgetrieben und deshalb auch *bottom up* orientiert sein müssen, was nur dann möglich ist, wenn eine verlässliche Aufwärtskommunikation relevanter Informationen vorhanden ist.[58] Neben der Implementierung

---

50 Ausführlich Bodenmann (FN 38), 126 ff.; sowie Flemming Ruud T./Sommer Katerina, Enterprise Risk Management – Das COSO-ERM-Framework, 126 ff.

51 Vgl. Müller Roland, Risk Management auf VR-Ebene, in: Verwaltungsrat – New Corporate Governance, scorecard – das Themenmagazin für Führungskräfte, 39.

52 Vgl. Bodenmann (FN 38), 116.

53 So etwa Müller (FN 51), 39; Flemming Ruud T./Sommer Katerina, Internes Audit und Enterprise Risk Management, ST 2006, 253.

54 Ebenso Wyss, (FN 26), 37.

55 Siehe in diesem Zusammenhang auch Ziff. 24 SCBP, nach welchem der Prüfungsausschuss die Funktionsfähigkeit des internen Kontrollsystems mit Einbezug des Risikomanagements beurteilen soll.

56 Anders das FINMA-RS 2008/24 Rz. 122, nach welchem der Verwaltungsrat oder die Geschäftsleitung die Risikobereitschaft zu genehmigen haben.

57 Vgl. Emch/Renz/Arpagaus (FN 15), N 2841 f.; Stöckli (FN 48), 88 f.; Hauri Patrick/Carri Anna, Wie kann der Bank-Verwaltungsrat seine Verantwortung im Risikomanagement wahrnehmen?, ST 2000, 1242.

58 Die an der SIX kotierten Unternehmen sind gemäss Ziff. 3.6 des Anhangs zur Richtlinie betreffend Information zur Corporate

eines zeitnahen Informations- und Reportingsystems[59] kommt insbesondere der Definition und klaren Zuteilung der Verantwortlichkeiten für das Risikomanagement eine grosse Bedeutung zu, da ohne sie ein effektives und effizientes Kontrollsystem nicht möglich ist.[60] Insofern besitzt der Verwaltungsrat die Pflicht, für eine zweckmässige Organisation und Wahrnehmung des Risikomanagements zu sorgen. Auch wenn das Risikomanagement für sämtliche Unternehmen von wesentlicher und stets zunehmender Bedeutung ist, hatte es doch in formalisierter und strukturierter Form bisher vor allem für Finanzinstitute einen hohen Stellenwert. Ein angemessenes Risikomanagement stellt eine der Voraussetzungen für die Bewilligung zur Bankentätigkeit dar[61].[62] In der gesellschaftsinternen Normenhierarchie steht die Risikopolitik deshalb für Finanzinstitute nach den Statuten und dem Organisationsreglement sowie dem Code of Conduct an vorderster Stelle[63] und ist schriftlich in einem internen Reglement oder einer internen Richtlinie[64] festzuhalten, wobei das Erfordernis der Schriftlichkeit u.E. für sämtliche grösseren Unternehmen und insbesondere die Publikumsgesellschaften zu gelten hat.

Heute bildet die Risikopolitik für jedes Unternehmen das Grundgerüst und den Ordnungsrahmen, auf welchen das Risikomanagement durchgeführt und umgesetzt wird. Diese *Umsetzung und Durchführung des Risikomanagements* kann (und soll bei Einsetzung einer Geschäftsführung[65]) durch den Verwaltungsrat delegiert werden.[66] Zur Umsetzung und Durchführung gehört auch die Entwicklung geeigneter Strukturen und Prozesse für die Identifikation, Beurteilung sowie Überwachung der eingegangenen Risiken, wobei Massnahmen zur Früherkennung (im Sinne eines Frühwarnsystems) im Vordergrund stehen.[67] Delegationsempfänger ist grundsätzlich die Geschäftsleitung.

Die *Verantwortung für die zweckmässige Durchführung des Risikomanagements* (und insbesondere für die aus den Erkenntnissen zu ziehenden Schlüsse) verbleibt hingegen beim Verwaltungsrat[68], weshalb er gezwungen ist, sowohl ein Reportingsystem als auch Risikolimiten zu errichten, die es ihm insbesondere erlauben, dann einschreiten zu können, wenn ein Risiko eingegangen wird, welches sich auf die Strategie oder die Risikotoleranz und Risikotragfähigkeit des Unternehmens auswirken könnte. Grund hierfür ist, dass die strategische Führung eines Unternehmens nach Art. 716a Ziff. 1 OR zu den undelegierbaren und unentziehbaren Aufgaben eines Verwaltungsrates gehört. Entsprechend hat hier der Grundsatz zu gelten: «Boards have to keep their noses in and their hands out».[69]

Ferner ist der Verwaltungsrat für die *Errichtung eines IKS sowie die Risikobeurteilung* als Grundlage für strategische Entscheide verantwortlich.[70]

1.2 Risikobeurteilung gemäss Art. 663b Ziff. 12 OR

Seit dem 1. Januar 2008 ist der Verwaltungsrat sämtlicher Aktiengesellschaften – unabhängig von einer allfälligen Kotierung oder ihrer Grösse – gehalten, ab dem Geschäftsjahr 2008 im Anhang zur Jahresrechnung *«Angaben über die Durchführung einer Risikobeurteilung»* zu machen (Art. 663b Ziff. 12 OR), welche als Bilanzanhang von der Revisionsstelle auf ihre Richtigkeit zu prüfen sind.[71] Diese Bestimmung ist an Sec. 404 des Sarbanes-Oxley Act[72] angelehnt, welche von jeder in den USA kotierten Gesellschaft verlangt, einmal pro Jahr einen Bericht über die «effectiveness of the internal control structure and procedures of the issuer for financial reporting» abzugeben.[73] Sinn und Zweck ist ein Zweifaches: Einerseits zwingt diese Bestimmung den Verwaltungsrat, welcher die Verantwortung für

---

Governance verpflichtet, im Geschäftsbericht zum Thema «Verwaltungsrat» u.a. Auskünfte über die Ausgestaltung der Informations- und Kontrollinstrumente des Verwaltungsrates gegenüber der Geschäftsleitung des Emittenten wie z.B. interne Revision, Risikomanagement-System oder Management Informations System (MIS) zu geben, <http://www.six-exchange-regulation.com/admission_manual/06_14-DCG_de.pdf>.

59 Ausführlich Hauri/Carri (FN 57), 1243 ff.

60 Ebenso Wyss (FN 26), 38; vgl. auch Stöckli, (FN 48), 91, 95; Bachmann, (FN 24), 93.

61 Art. 3 Abs. 2 lit. a BankG.

62 Als praktisches Beispiel sei in diesem Zusammenhang auf den Fall der Bank Rinderknecht AG verwiesen, welcher u.a. aufgrund des Fehlens eines angemessenen Risikomanagements die Bewilligung zur Führung einer Bank entzogen wurde, EBK-Bulletin, 22/1997, 22 ff., 31.

63 Vgl. Emch/Renz/Arpagaus (FN 15), N 2840; siehe auch Emmenegger Susan/Geiger Hansueli, Bank-Aktiengesellschaften – Statuten und Reglemente mit Mustern, Zürich/Basel/Genf 2004, N 34.

64 Art. 9 Abs. 2 BankV.

65 Ausführlich Böckli, welcher darauf hinweist, dass die Durchführung und Umsetzung des Risikomanagements nicht dem Audit Committee übertragen werden darf, da dies zu einer gravierenden Verwischung der Verantwortlichkeitslinien führen würde, Böckli Peter, Audit Committee – Der Prüfungsausschuss des Verwaltungsrates auf Gratwanderung zwischen Übereifer und Unsorgfalt, Zürich 2005, N 115 f.

66 Vgl. Hauri Patrick, Pflichten und Verantwortlichkeiten des Bank-Verwaltungsrates, ST 1998, 29; Boutellier Roman/Fischer Adrian/Palazzesi Mauro/Buser Stefan, Ansatz zur Prüfung der Risikobeurteilung, ST 2006, 619; Pfiffner (FN 24), N 3873.

67 Vgl. Wyss (FN 26), 38.

68 Vgl. Böckli (FN 65), N 117.

69 So Müller Roland/Kalia Vinay, Risk Management at Board Level – A Practical Guide for Board Members, Bern 2007, 20.

70 Atteslander Jan/Cheetman Malcolm, Vorschläge der Unternehmen zum IKS, ST 2007, 30 ff.; vgl. auch Böckli (FN 24), N 192 und (FN 19), § 15 N 312.

71 Zum Umfang der Prüfung durch die Revisionsstelle siehe Böckli (FN 19), § 15 N 210.

72 Vgl. <http://www.sec.gov/about/laws/soa2002.pdf>.

73 Ausführlich Merkl Georg, Neue Vorschriften der SEC und des PCAOB zum IKS, ST 2007, 38.

die Risikobeurteilung trägt,[74] sich mit dieser Thematik auseinander zu setzen; andererseits wird die Pflicht zur Offenlegung zu einer diesbezüglichen Sensibilisierung der Investoren führen und die Wahrscheinlichkeit eines informierten Investitionsentscheides erhöhen[75].

Der äusserst knappen Formulierung des Gesetzesartikels, welche keine Angaben zu *Form und Inhalt der Offenlegung* macht, mangelt es jedoch an Konkretisierung, was dementsprechend viel Spielraum für Interpretationen lässt. Während sich aus der Botschaft des Bundesrates ergibt, dass diejenigen Risiken offen zu legen sind, welche «einen wesentlichen Einfluss auf die Beurteilung der Jahresrechnung haben können»[76], wurde in der Gesetzesdebatte des Ständerates ausgeführt, dass die Angabe eines Sitzungsdatums und die Aussage, man habe über die Risiken gesprochen (im Sinne einer Bestätigung), nicht genügen könne und der Gesetzgeber eine inhaltliche Auseinandersetzung mit dem Unternehmensrisiko erwarte[77]. Sicher ist, dass sich der Verwaltungsrat mit den strategischen Unternehmensrisiken auseinanderzusetzen und diese Risiken zu beurteilen hat. Indessen umfasst die Offenlegung in der Jahresrechnung nicht sämtliche Geschäftsrisiken, sondern *nur diejenigen Risiken, welche einen wesentlichen Einfluss auf die Jahresrechnung haben können*.[78] Dementsprechend müssen die bewerteten Risiken gemäss den Kategorien «wesentlich» und «unwesentlich» bezüglich ihres Einflusses auf die Jahresrechnung eingeordnet werden. Diese Einteilung hat unternehmensbezogen zu erfolgen, da jedes Unternehmen hinsichtlich des Geschäftsmodells, der Strategien und insbesondere der Werte und Risikotragfähigkeit verschieden ist. Es bedarf daher einer situations- und empfängergerechten Darlegung der Risikoanalyse, der Einschätzung der Risiken und der getroffenen Massnahmen.[79] Als Richtwert sollte jedoch ein Risiko, dessen maximal möglicher Schaden die Stellung einer Gesellschaft am Markt erheblich negativ beeinflusst, als wesentlich bewertet werden. In der Praxis betrachten viele Unternehmen einen Vorfall dann als wesentlich, wenn er die Börsenkapitalisierung um mehr als fünf Prozent tangieren kann.[80] Unklar ist überdies, ob es nur um Risiken geht, welche bereits einen Einfluss auf die *gegenwärtige Jahresrechnung* haben oder auch solche Risiken umfasst sind, die sich erst auf zukünftige Jahresrechnungen auswirken können, aber dem Verwaltungsrat bereits bekannt sind. Als Beispiel sei ein Pharmazie-Unternehmen angeführt, dessen Hauptrisiko darin besteht, dass seine Forschungspipeline nicht erfolgreich sein könnte. Auf die gegenwärtige Jahresrechnung wird dies keinen Einfluss haben, auf die nächstjährige vielleicht insoweit, als sich der Forschungsaufwand erhöht, und falls sich die Gefahr realisiert, wird sich dies in späteren Jahren in Form von sinkenden Umsätzen bemerkbar machen.

Bei der Offenlegung nach Art. 663b Ziff. 12 OR geht es mit anderen Worten vor allem um das *Risiko einer wesentlichen Fehlaussage in der Jahres- oder Konzernrechnung*[81], d.h. die prozedurale Gewährleistung der Qualität der Finanzberichterstattung.[82] Das allgemeinere Thema der strategischen Risiken des Unternehmens, aber auch die Markt- und Gegenparteirisiken sowie die operationellen Risiken, insoweit sie keinen wesentlichen Einfluss auf die Qualität und Beurteilung der Jahresrechnung haben, sind demgegenüber nicht Gegenstand der Offenlegungspflicht.[83] Insofern handelt es sich lediglich um einen rudimentären Überblick über die (finanzielle) Situation der Gesellschaft, der eher Finanzanalysten als Investoren und Aktionären eine Beurteilung ermöglicht. Eine zusätzliche Einschränkung bedeutet die Tatsache, dass es sich – wenn man davon ausgeht, dass lediglich Risiken erwähnt werden müssen, welche einen Einfluss auf die gegenwärtige Jahresrechnung haben – um eine jährliche Offenlegung in Retrospektive handelt und damit nicht zwingend die aktuelle Risikosituation des Unternehmens widerspiegelt.

Schliesslich sieht die *derzeitige Revision des Aktienrechts* vor, dass nur noch grössere Unternehmen Angaben zur Durchführung einer Risikobeurteilung machen müssen. Ausserdem werden diese Angaben nicht mehr im Anhang der Jahresrechnung, sondern lediglich im Jahresbericht (neu: Lagebericht) anzubringen sein und dadurch in Zukunft nicht mehr von der externen Revisionsstelle geprüft werden. In Art. 961c OR des Ent-

---

74 Vgl. BSK OR II-Neuhaus/Blättler, Art. 663b OR N 41a; Böckli (FN 19), § 15 N 192.

75 Vgl. hierzu Simkins Betty/Ramirez Steven A., Enterprise-Wide Risk Management and Corporate Governance, 39 Loyola University Chicago Law Journal, 571 ff.

76 Botschaft Revisionspflicht (FN 8), 4036.

77 AmtlBull StR 2005, 988; ausführlich zu den parlamentarischen Beratungen Moser Hans/Stenz Thomas, Angaben über die Durchführung einer Risikobeurteilung, ST 2007, 592 ff.

78 Böckli (FN 19), § 15 N 205.

79 Vgl. Boutellier/Fischer/Palazzesi/Buser (FN 66), 618; Böckli (FN 24), N 206; Neuhaus/Blättler, (FN 74), N 41c.

80 Boutellier/Fischer/Palazzesi/Buser (FN 66), 619.

81 Da Konzerne einen Anhang sowohl als Bestandteil der Jahresrechnung jeder einzelnen Konzerngesellschaft als auch der Konzernrechnung erstellen müssen, braucht es dementsprechend Aussagen zur Risikobeurteilung sowohl auf der Ebene der Einzelgesellschaften als auch auf konsolidierter Ebene (Neuhaus/Blättler (FN 74), N 41d; vgl. auch Atteslander/Cheetham (FN 70), 32). Dabei sind Grösse, Komplexität und Risikoprofil der einzelnen Konzerngesellschaften angemessen zu berücksichtigen (Moser/Stenz (FN 77), 599). Sofern die Tochtergesellschaft ausschliesslich konzernaktiv ist, ergibt sich ihr Risiko im Wesentlichen aus dieser Tatsache; tritt die Tochtergesellschaft hingegen eigenständig am Markt auf, so kommen sämtliche Risiken hinzu, welche sich aus der (relativen) Eigenständigkeit der Gesellschaft ergeben, so dass ein Verweis auf die Angaben im Anhang der Konzernrechnung der Muttergesellschaft nicht genügen kann.

82 Böckli (FN 24), N 205; Neuhaus/Blättler (FN 74), N 41a, 41d.

83 Vgl. Atteslander/Cheetham (FN 70), 31, 35; Böckli (FN 19), § 15 N 205.

wurfs zum neuen Aktienrecht wird zudem der Übergang von einer «ex-post» Rechenschaft im Jahresbericht zur Gegenwarts-Analyse und Antizipierung im Lagebericht stipuliert, was die Aktualität und Transparenz der Angaben erhöhen soll. In der Botschaft des Bundesrates wird empfohlen, dass kleinere Unternehmen in der Übergangszeit bis zum Inkrafttreten des Entwurfs einen Ansatz wählen, der langfristig nachwirkende einmalige Kosten vermeidet.[84] Insofern findet in gewissem Sinne eine Relativierung der Bedeutung von Art. 663b Ziff. 12 OR statt.[85]

2. Wahrnehmung der Aufgaben

Wie oben festgehalten, kann die *Umsetzung und Durchführung des Risikomanagements* delegiert werden. Da das Risikomanagement einen integralen Bestandteil der Unternehmensführung darstellt, muss ein entsprechender personeller und organisatorischer Rahmen dafür bereitgestellt werden.[86] Zumeist wird diese Aufgabe von der Geschäftsleitung (in grösseren Unternehmen grundsätzlich vom Chief Risk Officer[87]) unter der Aufsicht des Audit oder Risk Committee wahrgenommen, wobei sich letztere von der internen Revision unterstützen lassen.[88] Zunehmend wird gefordert, dass die für das Risikomanagement zuständigen Personen von den ertragsorientierten Geschäftseinheiten unabhängig sind.[89]

In *formeller Hinsicht* erfordert eine solche Delegation der Geschäftsführung durch den Verwaltungsrat neben einer statutarischen Ermächtigung der Generalversammlung einen entsprechenden Beschluss des Verwaltungsrates, welcher zumindest in einem Protokoll des Verwaltungsrates festgehalten werden muss[90], wobei in grösseren Gesellschaften ein sog. Organisationsreglement erlassen wird. Auch wenn in der Praxis davon ausgegangen werden kann, dass die Delegation der Geschäftsführung die Durchführung des Risikomanagements mit umfasst und deshalb an sich nicht ausdrücklich erwähnt werden muss, empfiehlt es sich, im Interesse einer klaren Aufteilung der Verantwortlichkeiten entsprechende Bestimmungen über die einzelnen Aufgaben und Entscheidungskompetenzen in ein Kompetenzreglement aufzunehmen. Andernfalls besteht eine gewisse Gefahr, dass der Verwaltungsrat trotz Delegation weiterhin für die Durchführung und Umsetzung des Risikomanagements in vollem Umfang haftbar bleibt.[91]

Eine *Subdelegation* von Aufgaben im Bereich des Risikomanagements durch die Geschäftsleitung ist immer dann möglich, wenn der Verwaltungsrat eine solche Delegation (ausdrücklich oder stillschweigend) als zulässig erklärt und die Grundzüge der Delegation durch die weiterdelegierende Person ebenfalls reglementarisch festgehalten werden.[92] Hingewiesen sei jedoch darauf, dass angesichts der Wichtigkeit der Thematik analog zur Situation beim Verwaltungsrat davon ausgegangen werden muss, dass es einen Kernbereich an Aufgaben gibt, welcher von der Geschäftsleitung nicht delegiert werden kann.

3. Konsequenzen eines mangelhaften Risikomanagements

Wie nachfolgend zu zeigen sein wird, kann sich eine Verantwortlichkeit des Verwaltungsrates (und der Geschäftsleitung) sowohl mangels Errichtung eines Systems des Risikomanagements oder aufgrund Lücken in demselben als auch aus dem Fehlen einer effektiven Umsetzung und einer ungenügenden Überwachung ergeben. Voraussetzung jeglicher Verantwortlichkeit aus Art. 754 OR ist eine Sorgfaltspflichtverletzung (Handeln oder Unterlassen) eines Organs, welche kausal für den Eintritt eines Schadens war. Eine detaillierte Auseinandersetzung mit den einzelnen Voraussetzungen würde den Rahmen dieses Artikels sprengen. Dennoch sei an dieser Stelle auf einige Aspekte hingewiesen, welche für das Risikomanagement von wesentlicher Bedeutung sind.

Sind die materiellen und formellen Voraussetzungen einer Delegation erfüllt, so kann sich der Verwaltungs-

---

84 Siehe Botschaft zur Änderung des Obligationenrechts (Aktienrecht und Rechnungslegungsrecht sowie Anpassungen im Recht der Kollektiv- und der Kommanditgesellschaft, im GmbH-Recht, Genossenschafts-, Handelsregister- sowie Firmenrecht) vom 21. Dezember 2007, BBl 2008, 1717 f., <http://www.admin.ch/ch/d/ff/2008/1589.pdf>.

85 Siehe in diesem Zusammenhang Böckli, welcher vorschlägt, dass sich kleinere und mittlere Unternehmen, welche der eingeschränkten Revision unterstehen, mit einer knappen Angabe begnügen können, dass und wie der Verwaltungsrat eine Risikobeurteilung durchgeführt hat. Ordentlich revidierte Gesellschaften, die sich ausserdem einer jährlichen Prüfung der Existenz ihres internen Kontrollsystems unterziehen müssen, sollen demgegenüber mindestens jene Angaben machen müssen, die mit dem IKS in einem funktionalen Zusammenhang stehen, Böckli (FN 19), § 15 N 206 ff..

86 Bodenmann (FN 38), 117; Böckli (FN 24), N 320.

87 Ausführlich zur Funktion des Chief Risk Officers Bodenmann (FN 38), 117 ff.

88 Vgl. Emch/Renz/Arpagaus (FN 15), N 2848; Stöckli (FN 48), 92.

89 So müssen etwa Finanzinstitute ihre Compliance und Risikokontrolle von den ertragsorientierten Geschäftsaktivitäten unabhängig in die Gesamtorganisation eingliedern (vgl. FINMA-RS 2008/24 Rz. 100, 113) und das Entschädigungssystem für die entsprechenden Mitarbeiter darf keine Anreize setzen, welche zu Interessenkonflikten führen (vgl. FINMA-RS 2008/24 Rz. 103, 117); siehe in diesem Zusammenhang auch Walker Review (FN 6), 15, 84 f.

90 Siehe auch BGE 4A.503/2005 v. 22.2.2008, E. 3.2.2; 4A.501/2007 vom 22.2.2008, E. 3.2.2.

91 Siehe BSK OR II-Watter/Roth Pellanda (FN 28), Art. 716b OR N 17.

92 Siehe BSK OR II-Watter/Roth Pellanda (FN 28), Art. 716b OR N 15; a.M. Ehrat Felix, Mehr Klarheit für den Verwaltungsrat, AJP 6/1992, 795.

rat (und die Geschäftsleitung) beim *Nachweis der gehörigen Auswahl, Unterrichtung und Überwachung* grundsätzlich *von der Haftung aus aktienrechtlicher Verantwortlichkeit nach Art. 754 OR* befreien.[93] Bei der *cura in eligendo* ist darauf zu achten, dass die Delegationsempfänger über die zur Erfüllung der Aufgaben notwendigen Fähigkeiten und fachlichen Qualifikationen verfügen. Dazu gehören Branchenkenntnisse ebenso wie Know-how im Bereich des Risikomanagements. Ebenso bedeutend ist die rechtzeitige Abberufung von Delegationsempfängern, sofern diese nicht (mehr) über die notwendigen Fähigkeiten verfügen sowie die Nachfolgeplanung. Letzterer wird in der Praxis auch heute noch häufig zu wenig Beachtung geschenkt. Die gehörige Unterrichtung verlangt, dass der Delegationsempfänger die Grundzüge seiner Aufgabe kennt, dazu gehört insbesondere die Kenntnis derjenigen Personen, an welche er zu rapportieren hat. Im Wesentlichen geht es somit bei der *cura in instruendo* um die Bekanntgabe der organisatorischen Regeln. Die eigentliche Krux des Entlastungsbeweises stellt aber die Überwachungspflicht dar. Zur Wahrnehmung der Überwachung ist in grösseren Verhältnissen die Errichtung eines Informations- und Reportingsystems erforderlich,[94] wobei insbesondere der Einrichtung eines Frühwarnsystems wesentliche Bedeutung zukommt, da eine reine Beurteilung zurückliegender Sachverhalte, d.h. eine ex post Überwachung den Anforderungen der *cura in custodiendo* nicht genügt. Um seiner Verantwortung gerecht zu werden, hat der Verwaltungsrat deshalb dafür zu sorgen, dass er regelmässig über die Risikosituation und –exposition des Unternehmens informiert wird. Dies bedingt, dass das Unternehmen ein effizientes und funktionsfähiges Informations- und Reportingsystem implementiert, welches periodisch aussagefähige, stufen- und zeitgerechte Risikoinformationen bereitstellt. Neben der Sicherstellung der Vollständigkeit der Berichterstattung gehört es zu den Aufgaben des Verwaltungsrates, in Ausnahmesituationen oder im Falle von Unklarheiten, Zusatzinformationen zu verlangen sowie bei Unregelmässigkeiten einzuschreiten.

In der Praxis dürfte sich der *Verwaltungsrat* im Falle einer befugten Delegation dennoch häufig von einer Verantwortlichkeit befreien können. Bei der *cura in eligendo* müsste dem Delegierenden vorgeworfen werden können, dass ihm bereits bei der Auswahl Verdachtsmomente bekannt waren oder hätten sein müssen, die gegen eine Delegation gesprochen hätten. Bei der *cura in instruendo* besteht das Problem häufig darin, dass die Delegierten gerade wegen ihrer grösseren Fachkenntnisse angestellt werden und somit den Delegierenden fachlich überlegen sind. Am ehesten vorstellbar ist eine Haftung aufgrund mangelhafter Wahrnehmung der *cura in custodiendo*, wenn der Verwaltungsrat es etwa unterlassen hat, für ausreichende und klare Kompetenzregelungen zu sorgen oder gegen Kompetenzüberschreitungen vorzugehen. Keine Exkulpationsgründe sind demgegenüber ein Zeitmangel oder das Fehlen von unternehmensspezifischen Branchen- und Fachkenntnissen bei den Verwaltungsratsmitgliedern.[95]

Im Falle einer *Subdelegation durch die Geschäftsführung* stellt sich die Frage, wer für wessen Verschulden haftet. Klarerweise haftet der Verwaltungsrat für eigenes Verschulden bei Auswahl, Instruktion und Überwachung der Geschäftsführung. Bei zulässiger Subdelegation durch die Geschäftsführung haftet der Verwaltungsrat hingegen nicht für Fehler, welche der Zweitdelegierte verursacht hat, da dieses schadensstiftende Verhalten für den Verwaltungsrat als Erstdelegierenden kaum erkennbar ist.[96] Im Rahmen seiner Überwachungsfunktion hat der Verwaltungsrat jedoch zu überprüfen, dass die Geschäftsleitung ihrerseits die drei curae im Falle einer Subdelegation wahrnimmt und die notwendigen Kontrollinstrumente und -organe geschaffen werden und funktionieren.[97]

Dem Risikomanagement kommt insofern eine wesentliche Bedeutung zu, als dass Geschäftsführungsentscheide, die sich in einem geschäftlichen Ermessensspielraum bewegen und nachträglich als unzweckmässig oder falsch betrachtet werden, auch in der Schweiz – ähnlich der im US-amerikanischen Recht entwickelten «Business Judgement Rule» – nur dann eine aktienrechtlich relevante Pflichtverletzung darstellen, wenn sie nicht auf einer sorgfältigen Entscheidfindung beruhen.[98] Es ist davon auszugehen, dass ein Gericht heute im *Falle eines mangelhaften Risikomanagements eine haftungsbegründende Unsorgfältigkeit* annehmen wird, aus welcher sich bei Vorliegen der weiteren Voraussetzungen eine aktienrechtliche Verantwortlichkeit ergeben kann.[99]

Denkbar ist zudem eine *strafrechtliche Verantwortlichkeit des Unternehmens* mangels sorgfältiger Organisation gemäss Art. 102 StGB.

---

93 Statt vieler Bärtschi Harald, Verantwortlichkeit im Aktienrecht, Diss. Zürich 2001, 253.

94 Siehe ausführlich Roth Pellanda Katja, Organisation des Verwaltungsrates – Zusammensetzung, Arbeitsteilung, Information und Verantwortlichkeit, Diss. Zürich 2007, N 679 ff.

95 Siehe Watter Rolf/Roth Pellanda Katja, Die «richtige» Zusammensetzung des Verwaltungsrates, in: Weber (Hrsg.), Verantwortlichkeit im Unternehmensrecht III, Zürich 2008, 78 ff.

96 Bertschinger Urs, Arbeitsteilung und aktienrechtliche Verantwortlichkeit, Zürich 1999, 60, 106.

97 Vgl. Horber Felix, Die Kompetenzdelegation beim Verwaltungsrat der AG und ihre Auswirkungen auf die aktienrechtliche Verantwortlichkeit, Diss. Zürich 1986, 133 f. mit weiteren Hinweisen.

98 Zur Business Judgement Rule ausführlich Grass Andrea R., Business Judgement Rule – Schranken der richterlichen Überprüfbarkeit von Management-Entscheidungen in aktienrechtlichen Verantwortlichkeits-prozessen, Diss. Zürich 1998, 5 ff.

99 Vgl. Wyss (FN 26), 30.

Abschliessend sei darauf hingewiesen, dass die *Genehmigung der Jahresrechnung durch die Generalversammlung*, welche auf diese Weise auch die Genehmigung der Angaben über die «Durchführung einer Risikobeurteilung» umfasst, nicht gleichzeitig einen Verzicht der Aktionäre auf allfällige Verantwortlichkeitsansprüche aus mangelhaftem Risikomanagement zur Folge hat. Eine solche Genehmigungswirkung würde nicht dem Sinn und Zweck der gesetzlichen Bestimmung von Art. 663b Ziff. 12 OR entsprechen. Andererseits ist fraglich, *welche Folgen eine Falsch- bzw. Nichtinformation durch den Verwaltungsrat nach sich ziehen wird*. Denkbar sind eine Verantwortlichkeit nach Art. 754 OR, eine ausservertragliche Haftung nach Art. 41 OR sowie, bei Vorliegen der entsprechenden Voraussetzungen, allenfalls eine Vertrauenshaftung.[100]

IV. Empfehlungen an den Verwaltungsrat

Bereits heute stellt ein effektives und effizientes Risikomanagement eine der wesentlichsten Faktoren für eine erfolgreiche Unternehmensführung und eine grosse Herausforderung an Unternehmen und ihre Verwaltungsräte dar. Durch die globale Wirtschafts- und Finanzkrise und das komplexer werdende gesetzliche und regulatorische Umfeld wird diese Thematik zusätzlich an Bedeutung gewinnen. Die nachfolgenden Ausführungen stellen – ohne den Anspruch der Vollständigkeit zu erheben – den Versuch einer Agenda dar, welche die Verwaltungsräte in ihrem Bestreben nach einer Optimierung des Risikomanagements unterstützen soll. Es versteht sich von selbst, dass es sich dabei um ein «abstraktes» Beispiel handelt, welches an das jeweilige Unternehmen anzupassen ist, wobei die konkrete Situation eines Unternehmens ein anderes Vorgehen verlangen kann.

(1) *Implementierung eines umfassenden Risikomanagement-Systems*
Das Risikomanagement-System hat auf Transparenz, klaren Verantwortlichkeiten und unabhängiger Kontrolle zu basieren. Auf der Grundlage der Unternehmensstrategie hat der Verwaltungsrat eine Risikopolitik auszuarbeiten, welche die qualitativen und quantitativen risikopolitischen Ziele und Strategien aus der Perspektive des Gesamtunternehmens definiert. Er hat dabei das Risikoprofil des Unternehmens, die Risikotoleranz und die Risikotragfähigkeit mit der Geschäftsleitung zu diskutieren und festzulegen. Darüber hinaus sind Prozesse zu implementieren, welche sicherstellen, dass die definierten Risiken frühzeitig identifiziert und die Massnahmen zur Risikobewältigung getroffen werden können. Weil ein angemessenes Risikomanagement in der Regel das Zusammenwirken mehrerer Funktionen und Entscheidungsträger erfordert, ist für eine optimale Aufgabenerfüllung und zur Vermeidung von Doppelspurigkeiten eine klare Organisation und Rollenverteilung zwischen Verwaltungsrat, Geschäftsleitung und dem Risiko Management-Verantwortlichen (vielfach der Chief Risk Officer)[101] erforderlich. Dazu gehört, dass für jedes identifizierte Risiko ein «Risk Owner» bestimmt wird, der das Risiko beobachten und allfällige Gegenmassnahmen vorschlagen muss. Es ist darauf zu achten, dass die für das «Risk Control» zuständigen Personen von den ertragsorientierten Geschäftseinheiten unabhängig sind.[102]

(2) *Besetzung des Verwaltungsrates und der Geschäftsleitung mit geeigneten Personen*
Die Implementierung eines angemessenen Risikomanagements erfordert eine Besetzung des Verwaltungsrates und der Geschäftsleitung mit Mitgliedern, welche sowohl über konkrete Wirtschafts-, Branchen- und Unternehmenskenntnisse als auch über Kenntnisse im Risikomanagement verfügen (z.B. einen Finanz- oder Strategieexperten, Risk Officer oder je nach Unternehmen etwa einen Umwelt-, Sicherheits- oder Informatikexperten)[103].[104] Es darf nicht vergessen werden, dass insbesondere auch die nicht-exekutiven Verwaltungsräte über entsprechendes Know-how oder die Fähigkeit, sich solches in Kürze aneignen zu können, verfügen müssen. Fehlt dem Verwaltungsrat als Gremium das notwendige Wissen, so wird er nicht in der Lage sein, die unternehmensspezifischen Risiken frühzeitig zu erkennen, zu beurteilen und in seine Strategieüberlegungen mit einzubeziehen. Während der Verwaltungsrat für die Wahl der Geschäftsleitung zuständig ist, erfolgt die Wahl der Verwaltungsratsmitglieder durch die Aktionäre (Art. 698 Abs. 2 OR). Dennoch kommt dem Verwaltungsrat in der Praxis durch

---

100 Ausführlich zur Frage einer Haftung für Information im Allgemeinen Marolda Martínez Larissa, Information der Aktionäre nach schweizerischem Aktien- und Kapitalmarktrecht, Diss. Zürich 2006, 353 ff.

101 Da ein integriertes Risikomanagement ein Verständnis sowohl für sämtliche Geschäftstätigkeiten als auch die Geschäftspolitik des konkreten Unternehmens voraussetzt, hat der Risiko-Verantwortliche grundsätzlich der Geschäftsleitungsebene anzugehören, vgl. Meulbroek Lisa K., A Senior Manager's Guide to Integrated Risk Management, in: Chew (Hrsg.), Corporate Risk Management, New York 2008, 85.

102 Vgl. Walker Review (FN 6), 15, 84 f.

103 Ausführlich zur Zusammensetzung des Verwaltungsrates Watter/Roth Pellanda (FN 95), 47 ff.

104 So auch Turner Review (FN 5), 93 sowie die Empfehlung I.2 des IIF Final Report (FN 44), 33.

sein Vorschlagsrecht an die Generalversammlung eine wichtige Initiativfunktion und ein erheblicher Einfluss zu. Auf diese Weise kann der Verwaltungsrat über seine Zusammensetzung zumindest mitbestimmen und dafür sorgen, dass inskünftig auch Mitglieder in dieses Gremium Einsitz nehmen, welche über Fähigkeiten und Kenntnisse im Bereich des Risikomanagements verfügen. Von ebenso grosser Bedeutung ist es, bei der Aus- und Weiterbildung von Verwaltungsrat und Geschäftsführung dafür zu sorgen, dass das Risikomanagement einen der Schwerpunkte bildet.

Neben den Fähigkeiten und Kenntnissen müssen die Mitglieder des Verwaltungsrates über genügend Zeit für die Ausübung ihres Mandates verfügen. Dieser Aspekt erhält insbesondere für die nicht-exekutiven Mitglieder zunehmende Bedeutung. So soll etwa ein Verwaltungsratsmitglied eines grossen Bankinstituts gemäss den Empfehlungen des Walker Review jährlich 30 bis 36 Tage für diese Tätigkeit zur Verfügung haben.[105]

(3) *Bildung eines Risk Committee*

In grösseren Unternehmen und insbesondere für Publikumsgesellschaften im Finanzbereich ist die Schaffung eines (separaten) Risk Committee zur Unterstützung des Verwaltungsrates im Bereich des Risikomanagements als notwendig zu erachten. Grund hierfür ist, dass das Audit Committee bereits einen umfangreichen Aufgabenbereich hat und insbesondere in Stress- und Krisenzeiten kaum genügend Zeit für das Risikomanagement vorhanden sein wird. Die Aufgabe eines solchen Risk Committee ist es, dem Verwaltungsrat in Bezug auf aktuelle Risiken und künftige Risikostrategien beratend zur Seite zu stehen, wobei die mikro-ökonomischen Entwicklungen ebenso zu berücksichtigen sind wie das gesamtwirtschaftliche, soziale und finanzielle Umfeld, in welchem sich das Unternehmen bewegt.[106]

Ein Risk Committee ist mit Personen zu besetzen, welche über die nötigen Fähigkeiten und Kenntnisse verfügen, um sich über die Risikosituation des Unternehmens ein angemessenes Bild zu machen und entsprechende Massnahmen zu ergreifen. Ausserdem sollte das Risk Committee im Interesse der Unabhängigkeit mehrheitlich aus nicht-exekutiven Verwaltungsratsmitgliedern bestehen. Wenn die Umsetzung und Durchführung des Risikomanagements von der Geschäftsleitung wahrgenommen wird, haben der Chief Executive Officer, der Chief Risk Officer, der Chief Financial Officer und der Leiter der internen Revision grundsätzlich an den Sitzungen des Risk Committee teilzunehmen.[107]

Nicht zu vergessen ist jedoch, dass das Risikomanagement nicht nur beim Verwaltungsrat, sondern – bezogen auf die jeweiligen (Spezial-) Aufgaben – auch bei sämtlichen Verwaltungsratsausschüssen weiterhin auf der Traktandenliste zu stehen hat (z.B. Risiken im Zusammenhang mit der Ausgestaltung der Entschädigung beim Compensation oder Remuneration Committee oder der Nachfolgeplanung beim Nomination Committee) und dem Risk Committee insofern grundsätzlich nur unterstützende Bedeutung zukommen kann.

(4) *Informations- und Reportingsystem*

Der Verwaltungsrat und die Geschäftsleitung können ihren Verantwortlichkeiten im Bereich des Risikomanagements nur dann nachkommen, wenn sie rechtzeitig und umfassend die notwendigen Informationen über die Risikosituation und -exposition des Unternehmens erhalten. Dabei muss insbesondere die aggregierte Gesamtsicht der Risiken im Auge behalten werden, denn die Identifikation und Analyse von Einzelrisiken oder -aspekten reicht nicht aus. Im Interesse eines bestmöglichen Informationsaustausches sind direkte Reporting- und Informationslinien zwischen dem Senior Management und dem zuständigem Mitglied der Geschäftsleitung (in der Regel wird dies der Chief Risk Officer sein) sowie zwischen letzterem und dem Verwaltungsrat (bzw. dem zuständigen Committee) zu errichten.[108] Ebenfalls ist sicherzustellen, dass periodisch Treffen zwischen den zuständigen Funktionen stattfinden, welche eine gute Zusammenarbeit ermöglichen sollen. Nur auf der Grundlage der notwendigen Information wird es dem Verwaltungsrat möglich sein, neue Risiken zeitgerecht zu identifizieren sowie seiner Überwachungsaufgabe nachzukommen.

(5) *Ausgestaltung des Vergütungssystems*

Heute stehen Vergütungssysteme aufgrund der teilweise als extensiv empfundenen Höhe der Bezüge in der Kritik, welche durch die Notwendigkeit einer staatlichen Unterstützung von einzelnen Finanzinstituten zusätzlich verstärkt wurde. Gewisse Vergütungssysteme sind aber nicht nur aus sozialpolitischer Sicht problematisch, sondern können insbesondere falsche

---

105 Vgl. Walker Review (FN 6), 10, 39 ff.

106 Vgl. Walker Review (FN 6), 81 f.

107 Vgl. Walker Review (FN 6), 82 f.

108 Siehe Prinzip I.iv des IIF Final Report (FN 44), 39 sowie Walker Review (FN 6), 15, 84 f.

Anreize setzen, was zur Übernahme exzessiver Risken durch die Leitungsorgane führen und den (langfristigen) Unternehmenserfolg gefährden.

Unternehmensstufen in die Entscheidfindungsprozesse einbezogen werden. Risikomanagement ist ein «team game». Voraussetzung für die Umsetzung einer solchen risikobewussten Corporate Culture ist die Definition einer Risikopolitik und eines entsprechenden Risikoprogramms, welche unter der Aufsicht der Geschäftsleitung respektive des Chief Risk Officer die vom Verwaltungsrat gewählte Risikostrategie umsetzen. Entscheidend für den Aufbau einer risikobewussten Unternehmenskultur sind jedoch letztlich der «tone from the top» sowie die Einstellung und das Verhalten des Chief Executive Officers sowie sämtlicher anderen Führungskräfte.

(7) *Anpassung des Risikomanagements*

Ein effektives Risikomanagement muss immer den sich laufend verändernden wirtschaftlichen, gesellschaftlichen und regulatorischen Gegebenheiten sowie den Besonderheiten des Unternehmens und damit dem jeweiligen Risikoprofil und den konkreten Unternehmenszielen angepasst werden. Der Grundsatz «one-size-fits-all» kann insofern hier keine Anwendung finden, da sich insbesondere Geschäftsmodelle, Prozesse und Systeme laufend und unternehmensspezifisch ändern.

Ebenso wesentlich wie die Anpassung an das Unternehmen und veränderte Umstände ist damit eine kontinuierliche Selbstbeurteilung durch die mit dem Risikomanagement befassten Personen und Organe zur Behebung von Schwachstellen und eine entsprechende Überprüfung und Beurteilung des Verwaltungsrates, z.B. im Rahmen eines jährliches Assessmentprozesses.

V. Schlussbemerkungen

Das bewusste Eingehen von Risiken gehört zum integralen Bestandteil jeglicher Geschäftstätigkeit. Ein mangelhaftes bzw. nicht vorhandenes Risikomanagement kann nicht nur erheblichen Einfluss auf den Wert des Unternehmens und seine finanzielle und operative Stabilität haben, sondern ebenso zu rechtlichen Verantwortlichkeiten der Führungsorgane sowie zu einem erheblichen Reputationsverlust des Unternehmens[113] führen, was sich sowohl auf ein allfälliges Kreditrating, den Aktienkurs als auch den Umgang mit Kunden, Mitarbeitern und anderen Stakeholdern negativ auswirken

[113] Ausführlich zu Reputationsrisiken bei Banken Schierenbeck Henner/Grüter Marc D./Kunz Michael J., Management von Reputationsrisiken in Banken, WWZ Discussion Paper, Juni 2004.

kann. Umgekehrt ist davon auszugehen, dass Investoren für Aktien von Unternehmen mit einem ausgezeichneten Risikomanagement einen höheren Preis zu bezahlen bereit sind.[114]

So oder anders ist es von höchster Priorität, dem Risikomanagement genügend Bedeutung zu schenken und diesen wesentlichen Aspekt der Unternehmungs- und Verwaltungsratstätigkeit nicht zu vernachlässigen, denn: «There are risks and costs to a program of action. But they are far less than the long-range risks and costs of comfortable inaction» (John F. Kennedy).

[114] Hingewiesen sei in diesem Zusammenhang auf die RiskMetrics Group (früher «Institutional Shareholder Services»), welche seit 2002 Corporate Governance Ratings von Unternehmen durchführt (für mehr Informationen siehe <www.riscmetrics.com>).