COMPLIANCE - ABSTÜTZUNG DURCH RECHNUNGSWESEN, IKS UND RISK MANAGEMENT

Autor: **Jossy Gellis**

Inhaltsverzeichnis

I. Risk Management – kein isoliertes System

Eine zentrale Komponente für den Erfolg oder Misserfolg eines jeden Unternehmens ist ein funktionierendes Risk Management. Die gegenwärtige amerikanische Hypothekarkrise hat anschaulich vorgeführt, dass dieser vermeintlichen Binsenwahrheit wieder vermehrt Beachtung zu schenken ist. Der *„credit crunch"* anfangs 2008 hat massgeblich Schwachstellen aufgedeckt und gezeigt, dass ein funktionierendes Risk Management und insbesondere eine effiziente Risikokontrolle noch immer keine Selbstverständlichkeiten sind.

Die rechtlichen Grundlagen des Risk Managements und die Aufteilung der Kompetenzen zwischen Verwaltungsrat und Geschäftsleitung sind hiernach auszuführen. Es soll zudem aufgezeigt werden, dass ein sorgfältig ausgestaltetes Risk Management auch im Eigeninteresse der Verwaltungsräte und Manager liegt.

Die Ausgangslage scheint banal[1]: Jede unternehmerische Tätigkeit eröffnet Chancen und birgt Risiken. Dabei wird Risiko definiert als *„the possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood"*.[2] Letztlich handelt es sich um Chancen, Geld zu verdienen und Risiken, Geld zu verlieren.

Auf den ersten Blick könnte man versucht sein, zu behaupten, erfolgreiches Risk Management bestünde darin, die Risiken zu minimieren und die Chancen zu maximieren. In der Regel verhalten sich Chancen und Risiken aber gleichlaufend, sodass höheres Risiko grössere Chancen verspricht. Aufgabe des Risk Managements ist es somit nicht, die Risiken zu minimieren, sondern zu *optimieren*. Mit anderen Worten muss sich der Verwaltungsrat[3] die Frage stellen, wie viel Risiko das Unternehmen tragen kann und soll, um so erfolgreich wie möglich wirtschaften zu können, ohne aber seine Existenz zu gefährden.[4]

---

* Der Autor bedankt sich herzlich bei seinen geschätzten Kollegen Dr. Herbert Wohlmann und Dr. Alexander Fischer für den kritischen Input.

1 Vgl. WOHLMANN HERBERT, Risikomanagement und Corporate Governance in Risiko und Recht, Basel 2004, S. 214, mit dem Hinweis, dass bereits die biblischen Gestalten Adam und Noah Risk Management betrieben haben, ersterer mit weniger, letzterer mit mehr Erfolg.

2 International Standards for the Professional Practice of Internal Auditing, im Glossar; einzusehen unter <http://www.theiia.org>.

3 S.u. III.1.

4 Grundlegend zum Risk Management: Committee of Sponsoring Organizations of the Treadway Commission (COSO), Enterprise Risk Management – Integrated Framework (2004) – Executive Summary, zu finden unter <http://www.coso.org>; s. auch Enterprise Risk Management – Das COSO-ERM-Framework, FLEMMING T. RUUD/SOMMER KATERINA, ST 2006, S. 126 ff.

Ein international anerkanntes Konzept zum Risk Management wurde durch das Committee of Sponsoring Organizations of the Treadway Commission (COSO) entwickelt. In dem mittlerweile bekannten COSO-Würfel werden die Ziele eines jeden Unternehmens in vier Kategorien zusammengefasst:

- *Strategische Ziele* beinhalten die „Vision" des Unternehmens und definieren, worauf das Unternehmen hinarbeitet;
- *operative Ziele* definieren die Mittel, die dem Unternehmen zur Verfügung stehen sollen;
- *Reporting* zielt ab auf die funktionierende Berichterstattung innerhalb des Unternehmens;
- *Compliance* will die Einhaltung der anwendbaren Normen gewährleisten. [5]

Risiken können und werden sich in allen Zielkategorien materialisieren. Deshalb definiert das COSO-Modell acht Komponenten, wie mit Risiken umzugehen ist und wie sie sich steuern lassen: Internes Umfeld, Zielfestlegung, Ereignisidentifikation, Risikobeurteilung, Risikosteuerung, Kontrolle, Information, Kommunikation und Überwachung.[6] Es soll hier nicht im Detail auf diese Komponenten eingegangen werden. Zentral ist, dass Risk Management *kein isoliertes System* darstellt. Die verschiedenen Komponenten bedingen und beeinflussen sich gegenseitig und sind teilweise ineinander verwoben.

Während die zwei erstgenannten Zielkategorien, Strategie und Operations, auch von äusseren Umständen abhängen, die durch das Unternehmen nicht restlos kontrolliert werden können, liegt es bei den zwei letztgenannten Kategorien, Reporting und Compliance, in der Hand des Unternehmens, ob die Ziele erreicht werden.[7]

Im vorliegenden Artikel liegt der Fokus auf der Zielkategorie Compliance und deren Einordnung in das Risk Management des Unternehmens.

---

5 COSO (FN 4), 3 ff.

6 A.a.O.

7 A.a.O.

II. Die Verantwortung des Verwaltungsrates im Bereich von Compliance, Rechnungswesen, IKS und Risk Management

1. Compliance und Aufsicht

Unter Compliance[8] ist ein Organisationskonzept zu verstehen, welches gewährleisten soll, dass sich das Unternehmen sowie dessen Leitung und Mitarbeiter an die auf das Unternehmen anwendbaren Regeln halten. Es geht dabei primär um die Einhaltung von Vorschriften wie Gesetzen, internen Weisungen, Standesregeln und Geschäftsgrundsätzen, aber auch um die Einhaltung von gewissen ethischen Standards, sowie um die Vermeidung von Interessenskonflikten.[9]

Dem Konzept der Compliance trägt auch der schweizerische Gesetzgeber Rechnung, indem er dem Verwaltungsrat in Art. 716a Abs. 1 Ziff. 5 OR die *Oberaufsicht* über die mit der Geschäftsführung betrauten Personen zwingend auferlegt. Damit verbunden ist namentlich die Pflicht dafür zu sorgen, dass diese die anwendbaren staatlichen Vorschriften sowie auch die Reglemente der Gesellschaft und die Weisungen des Verwaltungsrates einhalten.[10]

Die Pflicht zur Oberaufsicht ist, wie die meisten Pflichten gemäss Art. 716a Abs. 1 Ziff. 2 - 6 OR, eine Konkretisierung der Oberleitungspflicht gemäss Art. 716a Abs. 1 Ziff. 1 OR.[11] Letztere beinhaltet im Wesentlichen die Festlegung der Unternehmensstrategie, die Definition der Mittel zum Erreichen der unternehmerischen Ziele, sowie die Kontrolle der Durchsetzung dieser Vorgaben.[12] Auch die Pflicht, die Organisation der Gesellschaft festzulegen (Art. 716a Abs. 1 Ziff. 2 OR), ergäbe sich ohne weiteres aus der Oberleitungspflicht. Denn ohne Implementierung einer klaren Hierarchie mit eindeutig definierten Dienstwegen liesse sich kein Unternehmen leiten.

Aufgrund der genannten Bestimmungen des Obligationenrechts trägt der Verwaltungsrat die Verantwortung dafür, dass sich nicht nur die Geschäftsleitung, sondern auch die ihr unterstellten Personen regelkonform

---

8 Auch dezidierte Gegner von Anglizismen können sich der Übernahme gewisser termini technici aus dem angelsächsischen Rechtsbereich nicht verwehren. Compliance tönt – das lässt sich kaum abstreiten – einfach eleganter als „Normeneinhaltung".

9 Grundlegend hierzu die Dissertation von BUFF HERBERT, Compliance, Zürich 2000; zum Begriff: BACHMANN DANIEL, Compliance – Rechtliche Grundlagen und Risiken, ST 2007, S. 93f.; BUFF, N 4 ff.; HOFSTETTER BRIGITTE, Das Compliance-Konzept zur Verhinderung von Interessenkonflikten innerhalb von Universalbanken, AJP 2002, S. 27 f.

10 BaK-WATTER, Art. 716a OR, N 19.

11 BÖCKLI PETER; Schweizer Aktienrecht, 3. Aufl., Zürich 2004, §13 N 308; BUFF (FN 9), N 116.

12 Botschaft des Bundesrates vom 23. Februar 1983 über die Revision des Aktienrechts, BBI 1983 745, 921; FORSTMOSER PETER/MEIER-HAYOZ ARTHUR/NOBEL PETER, Schweizerisches Aktienrecht, Bern 1996, § 30 N 31; BaK-WATTER, Art. 716a OR, N 6.

verhalten. Damit obliegt es dem Verwaltungsrat im Rahmen seiner Aufsichtspflicht, für die Einrichtung eines dem Unternehmen angepassten Compliance-Systems zu sorgen, welches sicherstellt, dass die im Unternehmen tätigen Personen die für ihre geschäftliche Tätigkeit massgebenden Normen und Regeln einhalten.[13]

Mit dem Gesagten zeigt sich die Wechselwirkung der Compliance mit den anderen Zielkategorien und dem Risk Management: Die Unternehmensstrategie nimmt Einfluss auf die Definition der Normen, die (im Rahmen der Compliance) einzuhalten sind. Mittels Risk Management sind die Risiken, welche die Compliance des Unternehmens bedrohen, aufzuspüren und zu bewältigen, wobei die daraus gewonnenen Erkenntnisse wiederum die Unternehmensstrategie beeinflussen. Mit Hilfe des internen Kontrollsystems (IKS) ist schliesslich festzustellen, ob die relevanten Risiken identifiziert, klassifiziert und angemessen behandelt werden.

2. Rechnungswesen, Finanzkontrolle und IKS[14]

Gemäss Art. 716a Abs. 1 Ziff. 3 OR obliegt dem Verwaltungsrat die Ausgestaltung des Rechnungswesens, der Finanzkontrolle sowie der Finanzplanung. Der Verwaltungsrat muss aufgrund dieser Bestimmung zwar nicht selbst das Rechnungswesen führen, er muss aber die organisatorischen Anordnungen treffen, die zur Einrichtung und Ausgestaltung eines dem Unternehmen angemessenen Rechnungswesens, einschliesslich Finanzkontrolle und Finanzplanung, notwendig sind.[15]

Die undelegierbare Pflicht des Verwaltungsrats zur Kontrolle ist nur für den Finanzbereich explizit erwähnt (Art. 716a Abs. 1 Ziff. 3 OR).[16] Die Finanzkontrolle gehört zum „ureigensten Aufgabenbereich“ des Verwaltungsrates.[17] Die Finanzen eines Unternehmens verdienen selbstredend höchste Aufmerksamkeit, da sie die finanzielle und somit die in erster Linie interessierende Verfassung des Unternehmens präsentieren.

Für die wirksame Durchführung der Finanzkontrolle ist ein der Gesellschaft angepasstes internes Kontrollsystem zu implementieren. Die von der

---

13 Swiss Code of Best Practice for Corporate Governance (Swiss Code), Rz. 20; BUFF (FN 9), N 190.

14 Im vorliegenden Artikel wird für das interne Kontrollsystem betreffend den Bereich der Rechnungslegung der Term „IKS“ verwendet, für das interne Kontrollsystem betreffend weitere Bereiche innerhalb des Unternehmens der Term „IKS im weiteren Sinne“, so auch BÖCKLI PETER, Revisionsstelle und Abschlussprüfung nach neuem Recht, Zürich/Basel/Genf 2007, N. 263ff und 292 ff.

15 BÖCKLI (FN 11), §13 N 342; FORSTMOSER et al. (FN 12), § 30, N 40 sowie Rz. 19 des Swiss Code (FN 13).

16 Zur verwaltungsrätlichen Pflicht der Kontrolle in anderen Bereichen, s.u. 2.3.

17 BBI 1983, 922 (FN 12).

Führungsebene des Unternehmens angeordneten Vorgänge, Methoden und Massnahmen, die dazu dienen, den ordnungsgemässen Ablauf des betrieblichen Geschehens sicherzustellen und das betriebliche Vermögen zu schützen, bilden das IKS.[18] Das IKS bezieht sich also auf *innerbetriebliche Prozesse*.

Faktoren, welche die Ausgestaltung und den Umfang des internen Kontrollsystems beeinflussen, sind die Grösse des Unternehmens, die Komplexität der Geschäftstätigkeit und die Art der Finanzierung (z.B. Familienholding vs. Publikumsgesellschaft).[19] Um die Kontrolle wirksam auszugestalten, ist die organisatorische Unabhängigkeit der Internen Revision und klares Reporting (unter Umständen an ein eingesetztes Audit Committee) zu gewährleisten.[20] Zudem sollte die Kontrolle auf wesentliche Vorgänge beschränkt sein, die ebenfalls für jedes Unternehmen individuell zu definieren sind. Schliesslich ist das Kontrollsystem so einzurichten, dass es sich in den operativen Betrieb des Unternehmens eingliedert.

Die Pflicht, ein Kontrollsystem einzurichten, wird durch den neuen Art. 728a Abs. 1 Ziff. 3 OR akzentuiert, wonach die Revisionsstelle bei der ordentlichen Revision auch die Existenz des Kontrollsystems prüfen muss. Diese Prüfungspflicht erstreckt sich allerdings lediglich auf das für die Rechnungslegung relevante interne Kontrollsystem.[21] Selbstverständlich entlässt die Prüfung des IKS durch die Revisionsstelle den Verwaltungsrat nicht aus seiner Verantwortlichkeit.[22]

Damit eine sinnvolle Prüfung möglich ist, muss das Kontrollsystem dokumentiert und den Mitarbeitern bekannt sein; es muss an das Unternehmen angepasst und innerhalb desselben angewendet werden; sodann muss im Unternehmen ein „Kontrollbewusstsein“ vorhanden sein.[23]

Die Existenz eines internen Kontrollsystems wird nur im Rahmen der ordentlichen Revision geprüft, nicht jedoch beim so genannten Review gemäss Art. 729 ff. OR. Dies bedeutet selbstverständlich nicht, dass Gesellschaften, die nicht der ordentlichen Prüfung unterliegen, von der Einführung eines angemessenen internen Kontrollsystems befreit wären. Es bedeutet lediglich,

---

18 IKS- Positionspapier der Treuhand-Kammer, ST 2006, S. 362.

19 A.a.O., S. 365.

20 BÖCKLI (FN 11), §13, N 349 f.

21 BACHMANN (FN 9), S. 95; BÖCKLI, Revisionsstelle (FN 14), N 274ff., insbes. N 279; IKS-Positionspapier (FN 18), S. 364; NADIG LINARD/MARTI SIMON/SCHMID MICHAEL, Interne Kontrolle in mittelgrossen Schweizer Unternehmen, ST 2006, S. 112; **a.M.** wohl WYSS LUKAS; Das IKS und die Bedeutung des (Legal) Risk Management für VR und Geschäftsleitung im Lichte der Aktienrechtsreform 2007, SZW 2007, S. 38.

22 Vgl. die neuen Art. 728a Abs. 3 und 729a Abs. 3 OR. Auf die Kontroverse über das Verhältnis der Veranwortlichkeit von Verwaltungsrat und Revisionsstelle soll hier nicht eingegangen werden. Eine Übersicht zur aktuellen Literatur ist bei BÖCKLI, Revisionsstelle (FN 14), N 44 zu finden.

23 IKS-Positionspapier (FN 18), S. 365.

dass das IKS dieser Gesellschaften von der *Überprüfung* durch die Revisionsstelle befreit ist. Ebenso wenig bedeutet die Beschränkung der Prüfung auf das die Rechnungslegung betreffende IKS, dass die restlichen Bereiche eines Unternehmens nicht kontrolliert werden müssen.[24]

3. Risk Management

Risk Management kann umschrieben werden als die Erfassung, Beurteilung und Bewältigung von geschäftlichen Risiken im Unternehmen.[25] Bei der Risikobewältigung stehen grundsätzlich vier Alternativen zur Verfügung:

1. Gewisse Risiken sind schlicht zu *vermeiden*, indem das Unternehmen auf die betreffende Tätigkeit verzichtet, da die damit verbundenen Risiken entweder zu gross sind oder keine, bzw. im Vergleich zum Risiko nur ungenügende, Chancen eröffnen, die Unternehmensziele zu erreichen.
2. Andere Risiken können *reduziert* werden, indem die Eintretenswahrscheinlichkeit oder die Auswirkung vermindert werden.
3. Risiken, die nicht vermieden oder reduziert werden können, lassen sich oft *überwälzen* (z.B. durch Versicherungen, Hedging etc.).
4. Schliesslich existieren Risiken, die von der Gesellschaft *getragen* werden müssen.

Das Risk Management ist darauf ausgelegt, das Erreichen der Unternehmensziele zu ermöglichen.[26] Der Verwaltungsrat trägt folglich auch hierfür die Verantwortung, was sich aus seiner Aufsichtskompetenz gemäss Art. 716a Abs. 1 Ziff. 5 und seiner Kompetenz zur Strategieentwicklung gemäss Art. 716a Abs. 1 Ziff. 1 OR ergibt. Die Bewältigung von Risiken ist letztlich unabdingbare Voraussetzung für die Entwicklung und Umsetzung der Unternehmensstrategie und stellt somit ein wesentliches Element der Aufsicht über die Geschäftstätigkeit dar.

Im neuen Art. 663b Ziff. 12 OR wird vom Verwaltungsrat daher auch ausdrücklich verlangt, dass er im Anhang zur Jahresrechnung Angaben über die Durchführung der Risikobeurteilung macht, welche von der Revisionsstelle im Rahmen des Audits zu prüfen sind (Art. 662 Abs. 2 OR).[27]

---

24 S.u. II.3.

25 Vgl. BÖCKLI Revisionsstelle (FN 14), N 194 ff. und detaillierter COSO, (FN 4), S. 3 f.; RUUD/SOMMER, S. 128; sowie oben I.

26 COSO (FN 4), S. 3.

27 Damit obliegt dem Verwaltungsrat formell auch über den Umweg von Art. 716a Abs. 1 Ziffer 3 OR die Pflicht zum Risk Management.

Zentrale Komponenten des erfolgreichen Risk Managements sind die Kontrolle der Risikobewältigung und die Überwachung des gesamten Risk Management-Systems. Es leuchtet ein, dass jedes Konzept und System, das auf Dauer implementiert wird, laufend überwacht werden muss. Nur so kann gewährleistet werden, dass dem System nachgelebt wird und nur so können allfällige Mängel im System erfasst und behoben werden.
Deshalb kann festgehalten werden, dass eine unübertragbare Kontrollpflicht des Verwaltungsrates in allen Bereichen besteht, für welche ihm gemäss Art. 716a Abs. 1 OR eine unübertragbare Kompetenz eingeräumt wurde. Daraus ergibt sich die Pflicht des Verwaltungsrates, ein an das Unternehmen angepasstes internes Kontrollsystem (IKS im weiteren Sinne) auch ausserhalb des Finanzbereiches zu implementieren. So heisst es in Randziffer 19 des Swiss Codes: „Das interne Kontrollsystem deckt, je nach den Besonderheiten der Gesellschaft, auch das Risk Management ab; dieses bezieht sich sowohl auf finanzielle wie auf operative Risiken".

Wie oben gesehen, bildet das IKS im weiteren Sinne einen Teil des umfassenden Risk Managements, wobei dessen Ausprägung selbstverständlich auf das Unternehmen abzustimmen ist. Alle Bereiche[28], in denen Risiken auftreten können, müssen mittels Risk Management erfasst und folglich auch mittels IKS im weiteren Sinne kontrolliert werden.[29] Das IKS im weiteren Sinne bildet, im Gegensatz zum IKS im Bereich der Rechnungslegung, nicht Prüfungsgegenstand der Revision. Jedoch ist auch das IKS im weiteren Sinne von der Revisionsstelle gemäss Art. 728a Abs. 2 OR zu „berücksichtigen".[30]

III. Die konkrete Aufgabenstellung von Verwaltungsrat und Geschäftsleitung

1. Systemverantwortung des Verwaltungsrates – Umsetzung durch die Geschäftsleitung

Der Verwaltungsrat muss die Aufgaben, die sich bei den oben erwähnten Kernkompetenzen stellen, nicht selber erfüllen, d.h. er muss weder die Buchhaltung noch die Finanzkontrolle selbst führen und muss auch nicht jedes Risiko begutachten bzw. im Bereich der Compliance selbst die Tätigkeit von Geschäftsleitung und Angestellten prüfen. Der Verwaltungsrat ist aber verpflichtet, die notwendigen *Systeme* zur Erfüllung dieser Aufgaben einzurichten. Er muss in diesem Sinne Ziele formulieren, die grundlegenden organisatorischen Anordnungen treffen, die für die Ausführung seiner Anordnungen verantwortlichen Personen bestimmen und die zur Erfüllung

---

28 Das sind gemäss dem COSO-Schema die Kategorien Strategy, Operations, Reporting und Compliance.

29 BÖCKLI (FN 11), §14, N 292; NADIG/MARTI/SCHMID (FN 21), S. 113; WYSS (FN 21), S. 40 f.

30 Diese Berücksichtigung beeinflusst das Vorgehen der Revisionsstelle bei der Prüfung, s. ausführlicher BÖCKLI, Revisionsstelle (FN 14), N 263 ff.

dieser Aufgaben notwendigen Ressourcen zur Verfügung stellen. Schliesslich trägt der Verwaltungsrat die Verantwortung, dass die Systeme funktionieren.[31] Der Verwaltungsrat hat also die Geschäftleitung zu beaufsichtigen, wozu er ein Reporting- und Management Information System einrichten muss.

Systemverantwortung bedeutet für den *Bereich der Compliance* die Ausarbeitung von klaren Leitplanken für das Compliance-System. Dessen konkrete Umsetzung kann der Verwaltungsrat der Geschäftsführung übertragen.[32] Die Geschäftsleitung sollte, zumindest bei grösseren und komplexeren Unternehmen, einen oder mehrere Compliance Officer(s) ernennen, die ihr direkt unterstellt sind. Organisatorisch wird der Compliance Officer mit Vorteil – aber nicht zwingend – der Rechts- (und Compliance-) Abteilung zugewiesen.[33] Für die Überwachung des Compliance-Systems zeichnet wiederum der Verwaltungsrat verantwortlich.[34] Selbst wenn der Verwaltungsrat ein Audit Committee eingesetzt hat, welches vornehmlich die Überwachung der Compliance übernimmt[35], verbleibt die Systemverantwortung beim Gesamtverwaltungsrat.[36] Durch die dargestellten und noch darzustellenden Massnahmen in den Bereichen Compliance, Reporting und IKS können Risiken bereits erheblich reduziert werden, sodass der Verwaltungsrat vor allem noch die verbleibenden Risiken und die Funktionsfähigkeit der Systeme beurteilen muss.

Im *Bereich der internen (Finanz-)Kontrolle* ist der Verwaltungsrat für die zweckmässige Organisation verantwortlich, sodass er sich jederzeit ein vollständiges Bild über das Unternehmen machen und die richtigen Schlüsse ziehen kann. Hierzu ist ein effizientes Reporting unabdingbar. Auch in diesem Bereich bleibt die konkrete Ausgestaltung delegierbar.[37]

Im *Bereich des Risk Managements* hat der Verwaltungsrat ebenfalls die Pflicht zur Einrichtung eines zweckmässigen Systems, um das Risiko in allen Bereichen des Unternehmens zu erfassen, zu beurteilen und zu bewältigen. Ein bedeutender Anteil des Risk Managments betrifft operative Bereiche, was die Federführung der Geschäftsführung rechtfertigt. Dennoch muss der Verwaltungsrat auch über diese Risiken informiert sein, um seine Erkenntnisse bei strategischen Entscheiden einfliessen lassen zu können. Der Verwaltungsrat

---

31 Ausführlicher zur Verantwortlichkeit des Verwaltungsrates, BACHMANN (FN 9), S. 95 f.

32 BACHMANN (FN 9), S. 94; Swiss Code (FN 13) Rz. 20.

33 Ausführlich zum Compliance Officer, BUFF (FN 9), N 41 ff.

34 BÖCKLI PETER, Audit Committee, Zürich/Basel/Genf 2005, N 21 und oben II.3.

35 Vgl. Swiss Code (FN 13), Rz. 24.

36 BÖCKLI, Audit Committee (FN 34), N 21; BUFF (FN 9), N 121.

37 BÖCKLI (FN 11), § 13, N 343 f.; BaK-WATTER, Art. 716a OR, N 13.

ist also dafür verantwortlich, die Gesamtrisikosituation zu kennen, richtig einzuschätzen und geeignete Massnahmen zu treffen.

Die Geschäftsleitung hat die Aufgabe, im Rahmen der Grundsatzentscheide und der Weisungen des Verwaltungsrates Compliance, Rechnungswesen, internes Kontrollsystem und Risk Management zu realisieren.[38] Nur die Geschäftsleitung, die sich täglich mit den genannten Bereichen auseinandersetzt, kann für die Durchsetzung des vom Verwaltungsrat definierten Rahmens in Frage kommen. Die Geschäftsleitung trägt damit auch die Verantwortung im Sinne von Art. 754 Abs. 1 OR für die richtige Umsetzung dieser Systeme und muss selbst im Rahmen dieser Kontrollaufgaben übernehmen.

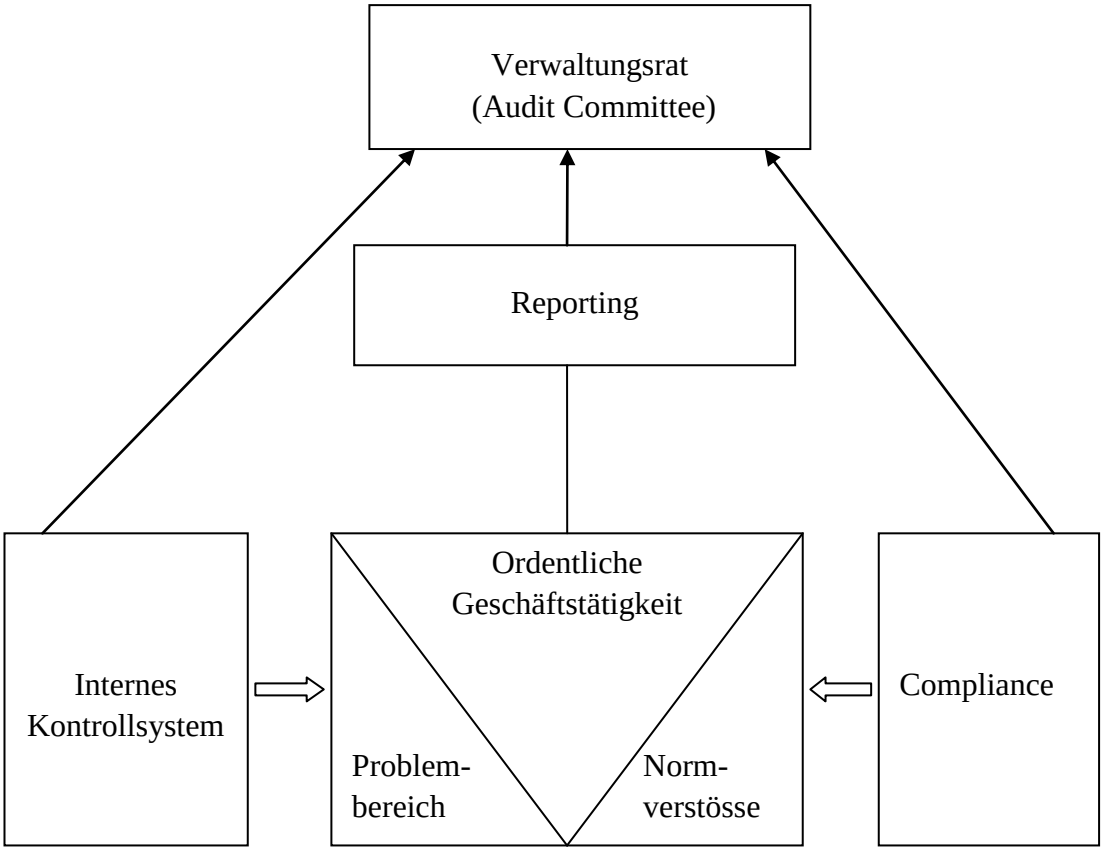
2. Integration

Verwaltungsrat und Geschäftsleitung sollten die oben erwähnten Aufgaben und zu implementierenden Systeme nicht isoliert betrachten, sondern im Sinne einer ganzheitlichen Sicht *zu einem einheitlichen System integrieren.*[39] Dadurch erhält der Verwaltungsrat ein wichtiges Führungsinstrument. Dieses System ermöglicht es ausserdem, die Qualität der einzelnen Entscheide des Verwaltungsrates zu verbessern, da sich dieser auf gut aufbereitete Daten und auf eine klare Risikoeinschätzung abstützen kann. Nur ein integriertes Gesamtsystem von Compliance, Rechnungswesen, interner Kontrolle und Risk Management gibt Verwaltungsrat und Geschäftsleitung die notwendige Übersicht über das Unternehmen und nützt die Ressourcen der Gesellschaft optimal.

---

38 BÖCKLI (FN 11), §14, N 291.

39 Zum Compliance-System im Besonderen, s. IV.1 hiernach.



3. Dokumentation

Von wesentlicher Bedeutung für die Praxis ist die sorgfältige Dokumentation, welche alle Komponenten des integrierten Systems umfassen sollte. Es ist dabei beispielsweise an Leitfäden zu denken, an Systeme, in denen Ereignisse als (potentielle) Risiken erfasst werden können, an die Aufbereitung von Informationen zur Beurteilung und Steuerung der Risiken, an das Rechnungswesen, an die Dokumentation der Prozesse, der Kommunikationswege und der vorgenommenen Kontrollen. Die Dokumentation betreffend die Durchführung einer Risikobeurteilung ist neu in Art. 663b Ziff. 12 OR gesetzlich vorgeschrieben.

Die Dokumentation hat eine interne und eine externe Komponente. Die *interne Komponente* ermöglicht erst das Funktionieren des Systems. Insbesondere Compliance aber auch Risk Management und IKS im weiteren Sinne beschlägt das gesamte Unternehmen. Jeder Mitarbeiter muss sensibilisiert sein und wissen, welche Tätigkeiten er zu unterlassen hat oder wie Ereignisse zu

identifizieren und zu handhaben sind, die mit den unternehmerischen Zielen im Konflikt stehen. Die schriftliche und systematische Dokumentation ist die einzige Möglichkeit, die Vollständigkeit von Informationen und den ungehinderten Informationsfluss und somit die effiziente Zusammenarbeit zu gewährleisten. Es ist auch zu bedenken, dass wesentliche Teile des Risk Managements heute durch spezialisierte Computersoftware vorgenommen werden. Dies erfordert wiederum die Prüfung und Kontrolle dieser IT-Systeme sowohl in technischer als auch in materieller Hinsicht. Auch hierfür ist eine möglichst lückenlose Dokumentation erforderlich.

Allerdings wird auch immer wieder der erhebliche Mehraufwand beklagt, der sich insbesondere bei KMU ergeben kann. Die Dokumentation erfüllt jedoch bei KMU andere Bedürfnisse als etwa bei Publikumsgesellschaften, da schriftliche Kommunikation aufgrund der geringeren Mitarbeiterzahl und der direkten Involvierung von Geschäftsleitung und Verwaltungsrat ins Tagesgeschäft sowie geringerer Mitarbeiterfluktuation nicht zwingend die Regel ist. Es sollte deshalb pragmatisch vorgegangen werden: Wo Dokumentation quasi inexistent war, ist diese einzuführen. Hingegen darf diese weit schlanker ausgestaltet sein als in grossen Unternehmen, um unnötigen Aufwand und Doppelspurigkeiten zu vermeiden.[40]

Auch (oder vielleicht ganz besonders) bei grossen Unternehmen und Publikumsgesellschaften sollte periodisch geprüft werden, ob der Systemaufwand und -nutzen in einem sinnvollen Verhältnis zueinander stehen.

Eine adäquate Dokumentation ist also Voraussetzung für das Funktionieren eines integrierten Systems von Risk Management, Compliance, Rechnungswesen und IKS im weiteren Sinne.

Die *externe Komponente* der Dokumentation hat zwei Wirkungen: Zum einen bildet die Dokumentation die Grundlage für die Prüfung durch die Revisionsstelle. Der Prüfer muss sich ein „Verständnis des Rechnungswesen-Systems und der internen Kontrolle“ erarbeiten[41], was nur bei genügender Dokumentation von Seiten des Unternehmens möglich ist. Zum anderen kann die Dokumentation (sofern sie adäquat und vollständig ist!) dem Verwaltungsrat als Nachweis dienen, dass er alle notwendigen Vorkehrungen getroffen hat, die ihm von Gesetz und Statuten auferlegt wurden und eine allfällige Verantwortlichkeitsklage deshalb unbegründet ist. Mit der Implementierung einer guten Dokumentation im Gebiet der Compliance, des Risk Managements,

---

40 Vgl. auch NADIG/MARTI/SCHMID (FN 21), S. 115 f. sowie PFÄFFLI WERNER, Internes Kontrollsystem als Reizwort für KMU, NZZ vom 8.1.2008, S. 25.

41 Schweizer Prüfungsstandards der Treuhandkammer 2004, PS 400, Rz. 2.

der Rechnungslegung und des IKS handelt der Verwaltungsrat im Interesse der Gesellschaft und nicht zuletzt auch im eigenen Interesse.

IV. Der Beitrag von Rechnungswesen, IKS und Risk Management zur Compliance

1. Das Compliance-Konzept

Die auf ein Unternehmen anwendbaren Normen, deren Einhaltung im Rahmen der Compliance sicherzustellen ist, sind von Fall zu Fall unterschiedlich. Aufgrund der bestehenden – und wohl weiter zunehmenden – Regulationsdichte kann nur systematische und vorausschauende Compliance wirksam sein. Der Verwaltungsrat muss folglich ein dem Unternehmen angepasstes Compliance-Konzept einrichten.

Voraussetzung für den erfolgreichen Aufbau eines solchen Compliance-Konzeptes ist die Identifikation der Mitarbeiter mit der Idee der Compliance und dem implementierten Konzept.[42] Die Mitarbeiter müssen für die relevanten Normen sensibilisiert werden. Klassische Compliance-Bereiche sind etwa das Insider- und Korruptionsstrafrecht, das auf die Gesellschaft anwendbare Aufsichtsrecht, Geldwäscherei, Umweltrecht, Kartellrecht, Interessenkonflikte, Arbeitsumfeld (d.h. sexuelle Belästigung, Mobbing, Diskriminierung etc.) sowie der Umgang mit Daten (Datenschutz und Vertraulichkeit), Kommunikation und IT-Mitteln.

Die Bausteine des Compliance-Konzeptes reichen von Regeln und Richtlinien über Ausbildung, organisatorischen Massnahmen und Kontrolle bis zu konkreten Verboten.[43] Säule des Compliance-Konzeptes sollte ein Code of Conduct darstellen, der sich an der jeweiligen Unternehmenskultur orientiert (also auch ethische Normen enthält) und die Grundsätze für die Handhabung der klassischen Compliance-Bereichen festlegt. In gewissen Branchen ist auch die Einführung eines Whistle-Blowing-Mechanismus gerechtfertigt. Dabei muss jedoch die Verhältnismässigkeit beachtet werden. Das Compliance-Konzept ist auf die Kooperation der Mitarbeiter angewiesen und bedingt deren Vertrauen, dass nicht jede kleinere Verfehlung hart geahndet wird.[44]

Das Compliance-Konzept muss in allen Hierarchiestufen der Gesellschaft verwirklicht werden. Die Mitarbeiter können die Compliance-Bemühungen einer Gesellschaft allerdings nur wirksam tragen, wenn sie durch entsprechende Weisungen dazu angehalten werden, auf konkrete Compliance-Fragen zu achten

---

42 BUFF (FN 9), N 72 ff.

43 BUFF (FN 9), N 308; HOFSTETTER (FN 9), S. 33.

44 WOHLMANN (FN 1), S. 222.

und allfällige Probleme der Compliance-Organisation zu melden. Die Erfahrung zeigt, dass blosse Richtlinien und Weisungen ohne ergänzende Ausbildung meist wirkungslos sind.[45] Ausserdem ist der Code of Conduct laufend zu aktualisieren und bei Bedarf mit einzelnen Weisungen und Richtlinien zu ergänzen.[46]

Das Compliance-Konzept darf also weder Damoklesschwert noch Papiertiger sein, weshalb es durch Unternehmensführung äusserst sorgfältig ausgearbeitet und implementiert werden muss.

2. Rechnungswesen und Compliance

Primäres Ziel des Rechnungswesens ist es, wirtschaftliche Vorgänge und insbesondere Geldflüsse zwischen dem Unternehmen und Dritten genau zu erfassen und abzubilden. Dementsprechend muss in diesem Bereich eine Organisation geschaffen werden, welche sicherstellt, dass alle buchungspflichtigen Vorgänge prompt erfasst und in den Büchern des Unternehmens korrekt verbucht werden.

Das Rechnungswesen ist für die Unternehmensführung zentral und untersteht grundsätzlich der gesetzlichen Prüfungspflicht, sodass die Compliance-Funktion praktisch ohne Zusatzaufwand wirkungsvoll unterstützt werden kann. Eine wesentliche Voraussetzung ist dabei, dass das Rechnungswesen tatsächlich sämtliche Mittel der Gesellschaft erfasst und so die Existenz „schwarzer Kassen“ ausgeschlossen wird. Weiter muss sichergestellt werden, dass sämtliche Ausgaben mit Belegen dokumentiert werden, wodurch ungesetzliche Zahlungen leicht erkennbar werden und besser vermieden werden können.

Die Mitarbeiter des Rechnungswesens müssen dazu ausgebildet werden, problematische Zahlungen zu erkennen und rechtzeitig zu melden.

3. IKS und Compliance

Das IKS dient zur Qualitätssicherung des Rechnungswesens. In der Praxis haben sich die folgenden Kernelemente des internen Kontrollsystems ausgebildet:

a) Kompetenzregelungen und organisatorische Massnahmen

---

45 BUFF (FN 9), N 603 f.

46 BUFF (FN 9), N 305 ff.

Die Kompetenzregelungen in der Buchhaltung und die Unterschriftenregelung für den Zahlungsverkehr müssen so gestaltet werden, dass Manipulationen ausgeschlossen sind. Dabei sollte vor allem das Vier-Augen-Prinzip möglichst lückenlos verwirklicht werden, da dieses erfahrungsgemäss bereits einen grossen Teil der möglichen Fehler und Manipulationen verhindert.

Der Zugriff auf Vermögenswerte und Daten des Unternehmens ist ab einer gewissen Wesentlichkeitsgrenze zu beschränken und der Bewilligung zu unterstellen.

Wesentlich ist auch der Systemschutz durch personelle Trennung von Transaktionen und Verbuchungen sowie durch restriktive Zugangsberechtigungen bei EDV-Systemen.

b) Kontrollmassnahmen

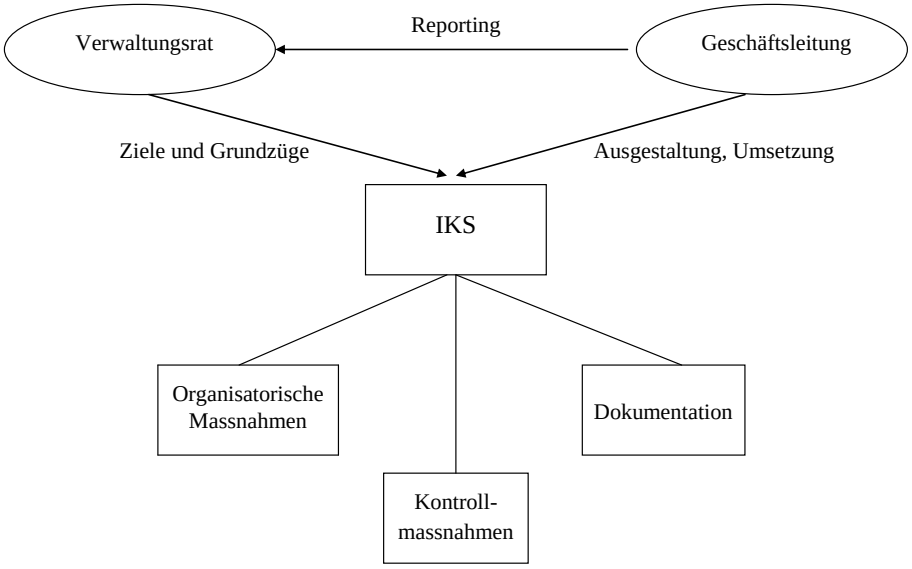
Zur Qualitätssicherung und Kontrolle sollte der regelmässige Vergleich von Kontoauszügen und Verbuchungen sowie von Belegen und Buchungen vorgesehen werden. Auch der Vergleich der ausgewiesenen Ergebnisse mit dem Budget und allenfalls die physische Bestandesaufnahme zum Vergleich mit den erfassten Vermögenswerten können aufschlussreich sein. Überdies muss auch die Einhaltung des Bewilligungs- und Entscheidungsverfahrens regelmässig geprüft werden, um zu verhindern, dass Zahlungen von Personen ausgelöst werden, die keine entsprechende Kompetenz haben. Die Kontrolle sollte nicht bloss detektiv, sondern auch präventiv (z.B. durch Passwörter, Chinese Walls) ausgestaltet sein. Meist ist es allerdings nicht möglich, eine lückenlose Kontrolle bzw. Überprüfung zu garantieren.[47] Stichproben haben aber schon eine stark präventive Wirkung und vermögen bereits einen grossen Teil der möglichen Manipulationen zu verhindern.

c) Dokumentation

Das interne Kontrollsystem muss so dokumentiert sein, dass organisatorische Massnahmen und Kontrollvorgänge für Verwaltungsrat, Geschäftsleitung und für alle mit der Umsetzung betrauten Personen nachvollziehbar sind. Auf diese Weise ist auch sichergestellt, dass die Revisionsstelle die Existenz des internen Kontrollsystems in einfacher Weise durch Kontrolle der entsprechenden Dokumentation feststellen und so auch den entsprechenden Bericht abgeben kann.

---

[47] Beispielsweise werden innerhalb eines Unternehmens Passwörter relativ schnell ausgetauscht (insbesondere zwischen Vorgesetzen und Assistenten aus Praktikabilitätsgründen).



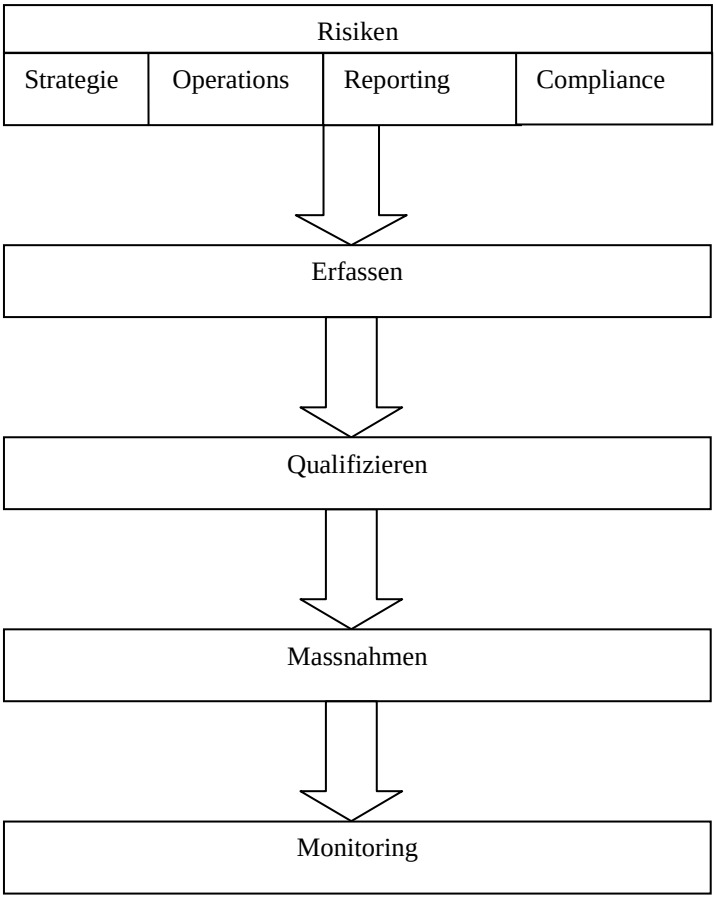
4. Risk Management und Compliance

Wie erwähnt kann und soll eine Gesellschaft Risiken nicht völlig vermeiden. Risiken sind letztlich unabdingbarer Teil jeder unternehmerischen Tätigkeit, und die Bereitschaft, Risiken zu tragen, ist häufig auch Basis des unternehmerischen Erfolges. Der Verwaltungsrat muss aber dafür sorgen, dass die im Unternehmen auftretenden Risiken erfasst und identifiziert werden. Auf dieser Basis können Verwaltungsrat bzw. vor allem auch die Geschäftsleitung Massnahmen ergreifen, um die Wahrscheinlichkeit des Schadenseintrittes zu reduzieren oder um Risiken auf Dritte zu transferieren.[48] Die Wirksamkeit dieser Massnahmen und die Entwicklung der betreffenden Risiken müssen als Teil des Risk Management-Prozesses in einem konsequenten Monitoring laufend überprüft werden.

Der Prozess der Risikoerfassung und des Risikomanagements kann wie folgt dargestellt werden:

---

[48] Durch Versicherungsdeckung, Alternative Risk Transfer, Hedging etc.



Risk Management und Compliance haben folgende wesentliche Berührungspunkte:

– Eine sorgfältige Risikoanalyse zeigt, wo im Unternehmen Compliance-Probleme auftreten können. Dies ermöglicht es, Compliance-Bemühungen und Kontrollmassnahmen gezielt einzusetzen, um Probleme zu verhindern. Hierbei ist zu beachten, dass die Risikoanalyse naturgemäss zukunftsgerichtet ist. Deshalb sind die Entwicklungen in den verschiedenen Risikobereichen so gut wie möglich einzuschätzen. In der Praxis beschlägt die Risikoerfassung insbesondere bekannte Risiken. Dies ist zwar notwendig, aber nicht ausreichend. Die Analyse sollte so aufgebaut werden, dass Risiken antizipiert werden, die zur Zeit der Erfassung noch nicht manifest sind, aber mit einer gewissen Wahrscheinlichkeit in Zukunft entstehen könnten.[49] Risikoanalyse ist deshalb ein Vorgang, der viel Sorgfalt, Phantasie und Kreativität erfordert.

[49] Wie zum Beispiel die passive Privatbestechung gemäss Art. 4a UWG, die erst seit dem 1. Juli 2006 in Kraft ist. Eine gute Risikoanalyse hätte jedoch in der Privatkorruption schon vor In-Kraft-Treten dieser Bestimmung ein Risiko erkannt.

– Umgekehrt sorgt eine funktionierende Compliance für die Verminderung der Risiken, die sich für die Gesellschaft aus der Verletzung anwendbarer Normen durch die Mitarbeiter ergeben. Selbst ein noch so ausgeklügelter Compliance-Prozess vermag jedoch nicht sämtliche Verletzungen von Normen zu verhindern. Dem Unternehmen verbleibt immer ein Restrisiko. Dieses muss im Rahmen des Risk Managements eingeschätzt und mit der Fähigkeit des Unternehmens, Risiken zu tragen (*„risk bearing capacity“*), abgestimmt werden. Ist es einem Unternehmen nicht möglich, diese Restrisiken zu tragen, so muss letztlich das Business Modell so geändert werden, dass die Compliance-gefährdende Tätigkeit vermieden wird.

Wie ausgeführt, tragen Rechnungswesen, IKS und Risk Management nachhaltig zur Erreichung des Unternehmensziels Compliance bei. Es liegt also im Interesse des Unternehmens wie auch des Verwaltungsrates und der Geschäftsführung, diesen Bereichen höchste Aufmerksamkeit zu schenken.

Zum Schluss sei aber noch folgende kritische Bemerkung erlaubt: IKS, Risk Management und Compliance sind – trotz ihrer Wichtigkeit – letztlich Hilfsmittel, welche darauf abzielen, die Gefährdung des wirtschaftlichen Erfolgs des Unternehmens zu minimieren bzw. auszuschliessen. Der hierzu notwendige bürokratische Apparat muss dem Unternehmen immer wieder angepasst werden und darf nie derart aufgeblasen sein, dass der personelle, kostenmässige und verfahrensmässige Aufwand das Erreichen der strategischen und operativen Unternehmensziele unnötig erschwert.