Kapitel 1
Unternehmensorganisation, Risikomanagement, Compliance-Management

Die Idee, die zur Entstehung dieses Buches geführt hat, resultiert im Wesentlichen aus Beratungen mittelständischer (Versorgungs-)Unternehmen, bei denen Consultants, Wirtschaftsprüfer und Juristen gemeinsam an einer Aufgabenstellung gearbeitet haben. Im Rahmen dieser Zusammenarbeit wurde deutlich, dass zwischen den genannten Funktionen vielfältige Schnittstellen und Wechselbeziehungen bestehen. 1

Diese Erkenntnis überrascht zumindest dann nicht, wenn man die genannten Funktionalitäten – ggf. unter Einbeziehung der Internen Revision – als Teilelemente eines umfassenden „**Internen Kontrollsystems**“ (IKS) versteht. 2

Unter einem IKS soll an dieser Stelle die Gesamtheit aller von der Unternehmensleitung angeordneten Vorgänge, Methoden und Maßnahmen (Kontrollmaßnahmen) verstanden werden, die dazu dienen, einen ordnungsgemäßen Ablauf des betrieblichen Geschehens sicherzustellen.[1] Die Errichtung eines solchen Systems ist Ausdruck der sog. **Corporate Governance**, also der Gesamtheit aller rechtlichen und faktischen Aktivitäten der Unternehmensleitung, die auf die Führung, Kontrolle und Steuerung des Unternehmens abzielen.[2] Bei Verwendung eines weiten IKS-Verständnisses wird man mit Recht (auch) die Unternehmensorganisation, das Risiko- und Compliance-Management sowie die Interne Revision als Teil eines (integrierten) IKS verstehen dürfen. 3

In diesem Kontext bildet die Unternehmensorganisation die formale Grundlage für das Risiko- und Compliance-Management im Unternehmen. Die Aufgabe der **Unternehmensorganisation** ist es, die Verantwortlichkeiten der einzelnen Unternehmenseinheiten und dort tätigen Beschäftigten präzise festzulegen und die Ablauf- sowie die Zusammenarbeitsprozesse in und zwischen den Einheiten festzulegen.[3] 4

Diese Festlegungen bilden den Anknüpfungspunkt für das Rechts- und Compliance-Management. Beide Funktionen weisen ebenfalls diverse Schnittstellen/Wech- 5

---

1 Vgl. statt vieler: PricewaterhouseCoopers (PwC), Internes Kontrollsystem – Führungsinstrument im Wandel, S. 4, abrufbar unter http://www.pwc.ch/user_content/editor/files/publ_ass/pwc_iks_fuehrungsinstrument_wandel_06_d.pdf; IDW Prüfungsstandard 261 n.F. (IDW PS 261 n.F.), Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken, 13.3.2013, Nr. 3.1.2.1.

2 Vgl. *Marekfia/Nissen*, Strategisches GRC-Management – Grundzüge eines konzeptionellen Bezugsrahmens (Forschungsbericht), November 2009, S. 3, abrufbar unter http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-18915/FUB-2009-2.pdf; Gabler Wirtschaftslexikon, Corporate Governance abrufbar unter http://wirtschaftslexikon.gabler.de/Archiv/55268/corporate-governance-v7.html.

3 Vgl. auch Gabler Wirtschaftslexikon, Organisation, abrufbar unter http://wirtschaftslexikon.gabler.de/Archiv/773/organisation-v6.html.

selwirkungen auf. Das **Risikomanagement** zielt bekanntlich darauf ab, die **ökonomischen Risiken** einer Organisation (frühzeitig) zu erkennen, zu analysieren und zu bewerten, um daran anknüpfend die erforderlichen Maßnahmen zu treffen, um die Realisierung dieser Risiken möglichst zu verhindern bzw. die daraus resultierenden Nachteile soweit wie möglich zu minimieren (**Risikosteuerung**) sowie entsprechende Risiken künftig zu vermeiden. Daneben sind Risikokontrolle und Risikowälzung im Auge zu behalten.[4] Das **Compliance-Management** versucht mit ähnlichen Mitteln die **rechtlichen Risiken** eines Unternehmens (rechtzeitig) zu erkennen, zu analysieren und zu bewerten, um deren Eintritt soweit wie möglich zu verhindern bzw. etwaige Nachteile aufgrund von Rechts- und Regelverletzungen so gering wie möglich zu halten.[5] Da Rechtsrisiken sich nicht selten in ökonomischen Risiken realisieren, ist Compliance-Management letztlich als eigenständiger Teil eines umfassenden Risikomanagements und damit eines (weit verstandenen) IKS eines Unternehmens zu begreifen.[6]

6 Dieser Befund ist wiederum der maßgebliche Grund für die integrierte Behandlung von Unternehmensorganisation, Risiko- und Compliance-Management in diesem Buch. Die gewählte Darstellungsweise soll dazu beitragen, der Komplexität eines umfassend verstandenen Risikomanagements in der täglichen unternehmerischen Praxis sowie in der Unternehmensberatung besser gerecht zu werden.

7 Wer sich im Unternehmen – sei es als Führungskraft, sei es als externer Berater – mit Fragestellungen der Unternehmensorganisation, des Risiko- oder des Compliance-Managements befasst, wird – wie bereits eingangs angemerkt – feststellen, dass Problemlösungen in einem der genannten Bereiche sehr oft die Beantwortung von Fragestellungen aus dem einen oder anderen Bereich erfordern. Wer dann erwartet, für diese „interdisziplinäre" Fragestellung unschwer Hilfestellung in entsprechend angelegter Fachliteratur zu finden, wird erstaunt feststellen, dass das Angebot insoweit nicht übermäßig breit ist. Grundlegende und eingehende Darstellungen finden sich zwar mittlerweile zu allen genannten Bereichen[7] ebenso wie zu den angrenzenden Themen IKS und interne Revision.[8] Literatur, die die vorstehenden Disziplinen in

4 Vgl. statt vieler nur Gabler Wirtschaftslexikon, Risikomanagement, abrufbar unter http://wirtschaftslexikon.gabler.de/Archiv/7669/risikomanagement-v10; IDW Prüfungsstandard 340 (IDW PS 340), Die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB, 11.9.2000, Nr. 2; vgl. näher Kap. 3.

5 Vgl. dazu nur IDW Prüfungsstandard 980 (IDW PS 980), Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen, 11.3.2011, Rn 6, sowie näher ab Kap. 4.

6 Vgl. nur Hauschka/*Bürkle*, Corporate Compliance, § 8 Rn 52; *Gold/Schäfer/Bußmann*, ET 6/2011, 71, 72; Hauschka/*Paupel/Glage*, Corporate Compliance, § 5 Rn 13 ff.

7 Vgl. z.B. *Hauschka*, Corporate Compliance; *Diederichs*, Risikomanagement und Risikocontrolling; *Schreyögg*, Organisation.

8 Vgl. z.B. *Böhmer/Hengst/Hofmann/Müller/Puchta*, Interne Revision.

Bezug auf ihre Schnittstellen, Wechselwirkungen und Abhängigkeiten eingehender beschreibt, ist dagegen weniger häufig anzutreffen.[9]

Eine integrierte Betrachtung von Unternehmensorganisation, Risikomanagement und Compliance und daran anknüpfend ein holistisches Management dieser Funktionalitäten ist jedoch (auch) bei mittelständischen Unternehmen nicht bloß ein „Kostenverursacher",[10] sondern schafft nicht unerheblichen (Mehr-)Wert, wie folgende Überlegungen zeigen: **8**

Die Existenz von Unternehmensorganisation, Risiko- und Compliance-Management ebenso wie die Einrichtung einer internen Revision werden zunehmend auch in mittelständischen Unternehmen zum „Stand der Technik".[11] Grund dafür dürften diverse gesetzliche Vorschriften[12] sein ebenso wie vielfältige untergesetzliche Regelwerke von Behörden und Organisationen.[13] Zu erwähnen ist auch das Urteil des Landgerichts München I vom 10.12.2013,[14] das eine Reihe von konkreten Vorgaben für ein Compliance-Management macht, damit es den gesetzlichen Vorschriften entspricht.[15] **9**

Diese aus volkswirtschaftlicher Sicht an sich begrüßenswerte Institutionalisierung und Strukturierung des Managements operativer und rechtlicher Risiken hat allerdings noch gewisse Schwächen bzw. Nachteile. Diese resultieren primär daraus, dass sämtliche genannten Funktionen, sofern implementiert, parallel vorgehalten werden und mehr oder weniger isoliert in ihrem jeweiligen „Zuständigkeitsbereich" arbeiten. Zumindest in Teilbereichen kommt es auf diese Weise zu inhaltlichen und/oder funktionalen Überschneidungen.[16] Entweder werden Sachverhalte mehrfach bearbeitet oder es kommt zu Diskussionen über die „Bearbeitungszuständigkeit" oder – noch schlimmer – zu beiden Effekten. **10**

9 Vgl. z.B. *Laue/Mohr*, CB 2014, 334 ff.; *Marekfia/Nissen*, Strategisches GRC-Management, S. 5 ff., abrufbar unter http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-18915/FUB-2009-2.pdf.

10 Vgl. auch *Marekfia/Nissen*, Strategisches GRC-Management, S. 2 f., abrufbar unter http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-18915/FUB-2009-2.pdf.

11 Zur zunehmenden Verbreitung von Compliance-Management seit 2009 vgl. etwa PwC, Wirtschaftskriminalität-Studie 2013, S. 26 f., bestellbar unter http://www.pwc.de/de/risiko-management/wirtschaftskriminalitaet-2013.jhtml.

12 Zu denken ist vor allem an § 93 Abs. 1 S. 1, 2 AktG (Aktiengesetz (AktG) v. 6.9.1965 (BGBl. I S. 1089), zuletzt geändert durch Gesetz v. 23.7.2013 (BGBl. I S. 2586)), §§ 30, 130 OWiG (Gesetz über Ordnungswidrigkeiten (OWiG) v. 19.2.1987 (BGBl. I S. 602), zuletzt geändert durch Gesetz v. 10.10.2013 (BGBl. I S. 3786)); vgl. dazu näher Kap. 5.

13 Vgl. dazu im Einzelnen näher Kap. 5, 7, 9, 18; Stichworte sind hier insbesondere: Deutscher Corporate Governance Kodex, MaRisk, MaComp, ONR 192050, ISO 19600, sowie die Prüfungsstandards 261, 340, 980 des IDW.

14 Vgl. LG München I, Urt. v. 10.12.2013 – 5 HK O 1387/10 – DB 2014, 766.

15 Dies gilt ungeachtet der Tatsache, dass die Vorgaben des LG München I aus Verfahrensgründen nicht mehr einer Validierung durch das OLG München oder den BGH unterzogen werden.

16 Vgl. *Laue/Mohr*, CB 2014, 335, 336.

11 Diese unbefriedigende Ineffizienz kann auch nicht immer auf Ebene der Geschäftsleitung vermieden werden, da die beteiligten Funktionalitäten nicht durchweg auf Geschäftsleitungsebene in einem Ressort/einer Person verbunden sind.[17] Auch unterhalb der Geschäftsleitung sehen die derzeit gängigen Organisationsmodelle in der Regel keine „Personalunion" hinsichtlich der in Rede stehenden Funktionen vor.

12 Durch die Fragmentierung, in Bezug auf die Gesamtrisikosituation, entstehen vielfach nur Teilbilder, die wiederum nur Teillösungen von Problemen ermöglichen. Daneben kommt es durch die angesprochene Mehrfachbearbeitung zu redundanten Abfragen mit entsprechender „bürokratischer" Belastung bei den operativen Bereichen und anschließend zu Mehrfachberichterstattungen an die Geschäftsleitung und/oder einzelne Mitglieder des Gremiums.

13 Trotzdem – oder gerade deswegen – entstehen auf diese Weise unerwünschte Informationslücken in Bezug auf die Risikosituation.[18] Fehlende Abstimmung und asymmetrische Informationen in Bezug auf eine Risikosituation können unvernetzte (Ad-hoc-)Aktivitäten einzelner Führungsverantwortlicher im Krisenfall erzeugen, die nicht zwingend die für das Gesamtunternehmen beste Lösung darstellen. Es fehlt mit anderen Worten eine optimale Gestaltung der relevanten Geschäftsprozesse.[19]

14 Eine faktisch-wissenschaftlich fundierte Aufarbeitung der vorstehenden Problematik steht – soweit ersichtlich – derzeit noch weitgehend aus. Aktuell finden sich diverse Ansätze für Verbesserungsvorschläge, ohne dass sich bisher ein allgemein akzeptierter Lösungsansatz durchgesetzt hätte.[20]

15 Zunehmend diskutiert wird in jüngster Zeit ein sog. **GRC-Ansatz**, wobei „GRC" für Governance Risk und Compliance steht. Darunter wird ein integrierter, holistischer Ansatz verstanden, der auf unternehmensweit angelegte Organisationssteuerung (Governance) unter Einschluss des Risiko- und Compliance-Managements abzielt und der gewährleisten soll, dass sich das Unternehmen insgesamt entsprechend dem festgelegten Risikoappetit unter Beachtung rechtlicher und ethischer Vorgaben verhält. Dies soll durch eine Abstimmung von Organisation, Prozessen und Strategien erreicht werden, die auf der integrierten Praktizierung der genannten Funktionalitäten beruht.[21]

---

17 Vgl. *Laue/Mohr*, CB 2014, 334, 335; *Dederichs/Fricke/Macke*, DB 2011, 1461 ff.

18 Ähnlich auch *Laue/Mohr*, CB 2014, 334, 336.

19 Vgl. auch *Marekfia/Nissen*, Strategisches GRC-Management, S. 5, abrufbar unter http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-18915/FUB-2009-2.pdf.

20 Vgl. *Laue/Mohr*, CB 2014, 334, 335.

21 Vgl. *Marekfia/Nissen*, Strategisches GRC-Management, S. 4 ff., abrufbar unter http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-18915/FUB-2009-2.pdf; De Decker/Schaumüller-Bichl/*Racz/Weippel/Seufert*, Communications and Multimedia Security, S. 106 ff.

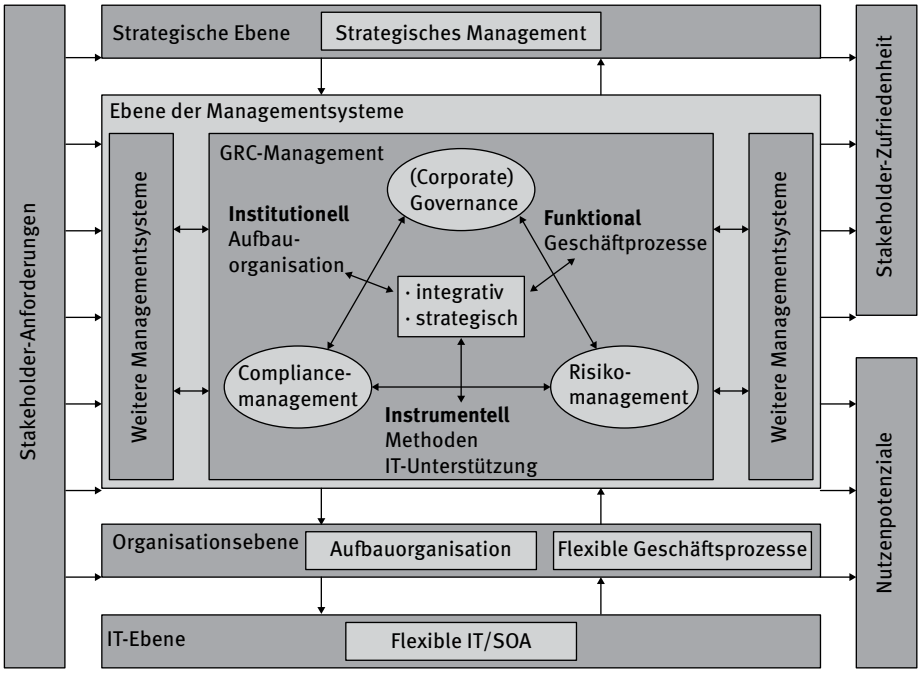

Abb. 1: GRC-Ansatz[22]

Auf dieser Basis werden zunehmend die Einführung eines „Chief Governance Officers" (CGO) bzw. eines „GRC-Officers" oder auch eines „GRC-Komitees" vorgeschlagen.[23] **16**

Der CGO bzw. das GRC-Office sollen als Stabstelle bei der Geschäftsleitung bzw. deren Vorsitzendem eingerichtet werden und unmittelbar an diese(n) berichten. Dabei wird eine Zusammenlegung mit der Funktion des Chief Compliance Officers oder des Leiters der Rechtsabteilung erwogen. **17**

Der Aufgabenumfang des CGO soll neben der Entwicklung von unternehmensinternen Richtlinien, der Schulung des Aufsichtsrats, der Beratung der Geschäftsleitung (insbesondere auch im Zusammenhang mit der Besetzung von Schlüsselpositionen im Unternehmen) sowie die Berichterstattung über die einzelnen Teilsysteme des GRC-Komplexes umfassen.[24] **18**

22 *Marekfia/Nissen*, Strategisches GRC-Management, S. 8, abrufbar unter http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-18915/FUB-2009-2.pdf.

23 Vgl. etwa *Laue/Mohr*, CB 2014, 334, 336; *Marekfia/Nissen*, Strategisches GRC-Management, S. 9 f., abrufbar unter http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-18915/FUB-2009-2.pdf.

24 Vgl. anschaulich *Laue/Mohr*, CB 2014, 334, 337.

19 Diese Vorschläge dürften für große börsennotierte Unternehmen zweifellos eine angemessene Lösung darstellen und werden deshalb dort auch schon zum Teil praktiziert.[25] In Bezug auf mittelständische Unternehmen wird man dagegen genau überlegen müssen, welche Lösung hier das relative Optimum zwischen Kosten und Nutzen eines GRC-Ansatzes bieten kann.

20 Vor diesem Hintergrund ist es Ziel des vorliegenden Werkes, einen Beitrag zur integrierten Darstellung und Handhabung von Unternehmensorganisation, Risiko- und Compliance-Management zu leisten. Der Fokus liegt dabei weniger auf der wissenschaftlichen Aufbereitung der einzelnen Gebiete als vielmehr auf dem Nutzen der gebotenen Informationen und Überlegungen für die tägliche Praxis in mittelständischen Unternehmen. Das Buch richtet sich deshalb vornehmlich an Vorstände, Geschäftsführer und Aufsichtsräte in mittelständischen Unternehmen sowie an Leiter Risikomanagement, Risikocontrolling, interne Revision, Compliance und deren Mitarbeiter. Ebenso angesprochen werden die Leitungsebene und die Beschäftigten der öffentlichen Verwaltung und der Gerichtsbarkeit, die Organisationsverantwortung tragen. Allen Adressaten soll die Thematik des Werks praxisnah und anwenderfreundlich aufbereitet und vermittelt werden.

25 Vgl. die Nachweise *Laue/Mohr*, CB 2014, 334, 337, Fn 15 ff.