

Arbeitskreis Externe und Interne Überwachung der Unternehmung der Schmalenbach-Gesellschaft für Betriebswirtschaft e.V., Köln

Überwachung der Wirksamkeit des internen Kontrollsystems und des Risikomanagementsystems durch den Prüfungsausschuss – Best Practice

► DB0457885

I. Einleitung

Mit der Verabschiedung des Bilanzrechtsmodernisierungsgesetzes (BilMoG)¹ erhielt die Diskussion um die Corporate Governance in Deutschland neue Impulse. Der neu eingefügte § 107 Abs. 3 AktG setzt entsprechende europäische Vorgaben zur Unternehmensüberwachung um². Danach hat der Aufsichtsrat bzw. ein eingerichteter Prüfungsausschuss³ die Aufgabe, neben dem Rechnungslegungsprozess und der Abschlussprüfung die Wirksamkeit des internen Kontrollsystems, des Risikomanagementsystems und des internen Revisionssystems zu überwachen. Die aktienrechtliche Regelung konkretisiert die Pflichten des Prüfungsausschusses und definiert einen neuen Beurteilungsrahmen zur angemessenen Ausübung des Aufsichtsratsmandats.

Aus dem Gesetz und der Gesetzesbegründung geht nicht hervor, in welcher Art und Weise diese Überwachungsaufgabe wahrgenommen werden soll. Die Unternehmen und insbesondere deren Kontrollorgane stehen daher vor der Herausforderung, ihre bisherige Praxis der Überwachungstätigkeit zu überprüfen und ggf. an den konkretisierten Tatbestand des § 107 Abs. 3 Satz 2 AktG anzupassen.

In diesem Beitrag wird ein Ansatz zur Wahrnehmung der Überwachungstätigkeit in Thesenform vorgestellt, in den die Entwicklungen der Unternehmenspraxis eingeflossen sind. Der Fokus des Ansatzes liegt hierbei auf der Überwachung der Wirksamkeit des internen Kontrollsystems und des Risikomanagementsystems i. S. des § 107 Abs. 3 Satz 2 AktG.

Der Gesetzgeber gibt weder eine Legaldefinition der genannten Überwachungsgegenstände vor, noch liefert das Gesetz zusätzliche Erläuterungen zur hierarchischen Ordnung der Begriffe⁴. In der Literatur finden sich verschiedene Definitionen und Abgrenzungen, die einzelne Komponenten, verbunden, integriert oder unabhängig voneinander sehen. Im Folgenden soll unabhängig von sprachlichen Differenzierungen auf eine rein funktionale Betrachtung abgestellt werden. Dies hat den Vorteil, dass der entwickelte Ansatz unabhängig von organisatorischen Besonderheiten des jeweiligen Unternehmens umgesetzt werden kann.

Dem Ansatz liegt das Verständnis von Unternehmensüberwachung als ein systematischer, mehrstufiger Informations- und Entscheidungsprozess zugrunde, der alle Maßnahmen umfasst, mit denen Zustände oder Prozesse daraufhin überprüft werden, ob diese normgerecht und wirtschaftlich sind bzw. ablaufen⁵.

Die gesetzliche Mindestanforderung an die Ausgestaltung der Unternehmensüberwachung findet sich im § 91 Abs. 2 AktG, nach dem der Vorstand einer Aktiengesellschaft verpflichtet ist, „[...] geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“.

Grundsätzlich ist zwischen prozessintegrierten und prozessunabhängigen Überwachungsmaßnahmen zu unterscheiden. Ers-

tere umfassen sowohl organisatorische Sicherungsmaßnahmen, d. h. alle Überwachungsmaßnahmen, die Fehler verhindern sollen und damit der Erreichung einer vorgegebenen Sicherheit dienen, wie z. B. Funktionstrennungen, Zugriffsbeschränkungen, Organisationspläne, als auch Kontrollen, d. h. mit dem Arbeitsablauf unmittelbar gekoppelte Überwachungsmaßnahmen, die Fehler feststellen sollen, wie z. B. Kontenabstimmungen, Vollständigkeits- und Plausibilitätskontrollen. Prozessunabhängige Prüfungen stellen z. B. Überwachungsmaßnahmen durch Personen dar, die weder in den Arbeitsablauf eingebunden sind noch Verantwortung für den zu überwachenden Prozess tragen⁶.

Ein erfolgreicher Ansatz zur Überwachung der Wirksamkeit hinsichtlich des internen Kontrollsystems und Risikomanagementsystems beinhaltet folgende Aspekte:

- Beziehung von Risikomanagementsystem und internem Kontrollsystem,

Dem Arbeitskreis gehören folgende Mitglieder an:

Prof. Dr. Dr. h.c. Jörg Baetge (Universität Münster); **Prof. Dr. Alexander Bassen** (Universität Hamburg); **Dr. Roland Busch** (Deutsche Lufthansa AG); **Dipl.-Kfm. Lutz Cauers** (Deutsche Bahn AG); **Prof. Dr. Anne d'Arcy** (Universität Wien); **Dr. Mark-Ken Erdmann** (Bertelsmann AG); **Prof. Dr. Edgar Ernst** (DPR); **Dipl.-Kfm. Ulrich M. Harnacke** (Deloitte & Touche GmbH); **Prof. Dr. Michael Henke** (European Business School); **Dr. Frank M. Hülsberg** (KPMG Wirtschaftsprüfungsgesellschaft AG); **Prof. Dr. Anja Hucke** (Universität Rostock); **Frank Jasper** (Siemens AG); **Dr. Udo Jung** (The Boston Consulting Group GmbH); **Dipl.-Kfm. Ulf Kampruwen** (USG People Germany GmbH); **Prof. Dr. Hans-Jürgen Kirsch** (Universität Münster); **Dr. Thomas Knoll** (Deutsche Telekom AG); **Prof. Dr. Annette G. Köhler** (Universität Duisburg-Essen); **Dipl.-Ök. Wolf-Dieter Loos** (Loos & Co. KG); **Prof. (em.) Dr. Prof. h.c. Dr. h.c. Wolfgang Lück** (TU München); **Prof. Dr. Kai-Uwe Marten** (Universität Ulm); **Prof. Dr. Hanno Merkt** (Universität Freiburg); **Dipl.-Kfm. Peter Mißler** (Deutsche Post AG); **Prof. Dr. Ludwig Mochty** (Universität Duisburg-Essen); **Dr. Thomas Münzenberg** (Sozietät RAe Dr. Booz & Dr. Münzenberg); **Horst Piepenburg** (Piepenburg-Rechtsanwälte); **Prof. Dr. Jens Poll** (RÖVERBrönnner Rechtsanwälte); **Dr. Willi Schoppen** (Spencer Stuart); **Dr. Markus Warncke** (Villeroy & Boch AG); **Dipl.-Kfm. Andreas Wermelt** (PricewaterhouseCoopers AG).

1 BGBL I 2009 S. 1102 ff.

2 Vgl. Art. 41 der 8. EU-Richtlinie (2006/43/EG) über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen vom 17. 5. 2006, ABIEU Nr. L 157 vom 9. 6. 2006 S. 87.

3 Im Folgenden wird vereinfachend vom „Prüfungsausschuss“ gesprochen.

4 Die im BilMoG RefE aufgestellte These, dass das IKS Bestandteil des Risikomanagements sei, wurde im RegE nicht mehr weiterverfolgt, vgl. Referentenentwurf eines Gesetzes zur Modernisierung des Bilanzrechts (Bilanzrechtsmodernisierungsgesetz – BilMoG), S. 210.

5 Vgl. Lück, in: Lück, Lexikon der Internen Revision, 2001, S. 326.

6 Vgl. Freiling/Lück, zfbf 1986 S. 998.

- Konkretisierung des Überwachungsgegenstands und der Ziele der Überwachung,
- informatorische Voraussetzungen des Überwachungsprozesses,
- organisatorische Ausgestaltung der Steuerungs- und Kontrollsysteme.

II. Thesen

These 1: Das interne Kontrollsystem und das Risikomanagementsystem stehen in wechselseitiger Beziehung zueinander.

Unternehmerisches Handeln ist stets mit der Übernahme von Risiken verbunden. Als Risiko ist jedes Ereignis zu verstehen, das einen negativen Einfluss auf die wirtschaftliche Entwicklung des Unternehmens haben kann. Je nach Ursprung und Auswirkung kann es sich hierbei z. B. um Markt- und Umweltrisiken, rechtliche und operative Risiken oder Reputationsrisiken handeln. Diese Risiken sind zu identifizieren und zu bewerten (Bruttorisiken). Mithilfe geeigneter Maßnahmen können Risiken – in Abhängigkeit der jeweiligen Risikoneigung des Unternehmens – auf ein akzeptables Niveau reduziert werden (Nettorisiken)⁷.

Grundlage des Risikomanagementsystems (RMS) ist ein mehrstufiger Prozess, bei dem die Risikoidentifikation (frühzeitiges Erkennen bestandsgefährdender Entwicklungen), die Risikoanalyse und -bewertung (Einschätzung der Höhe und eventuelle Eintrittswahrscheinlichkeit des Schadens) das für Aktiengesellschaften gesetzlich geforderte Früherkennungssystem bilden⁸. Die Risikosteuerung umfasst die Festlegung eines akzeptablen Risikoniveaus sowie die Konzeption und Umsetzung der Aktivitäten zur Risikobegrenzung (vermeiden, vermindern, überwälzen)⁹. Die Risikokommunikation und die Risikouberwachung schließen den Prozess ab.

Als Best Practice orientiert sich das interne Kontrollsystem (IKS) u. a. an dem COSO-Internal Control-Framework¹⁰. Hier werden die Ziele des IKS (Wirtschaftlichkeit und Wirksamkeit der Geschäftstätigkeit, Ordnungsmäßigkeit und Verlässlichkeit der Finanzberichterstattung und Einhaltung von Gesetzen und Vorschriften) mit der Unternehmensorganisation (Unternehmensfunktionen und -prozesse bzw. Unternehmenseinheiten) und den Komponenten des IKS in Beziehung gesetzt¹¹. Diese Komponenten sind Kontrollumfeld, Risikobeurteilung, Kontrollaktivitäten, Information und Kommunikation sowie Überwachung¹².

Die Rolle beider Systeme im Rahmen der Unternehmensüberwachung wird durch die Regelungen des BilMoG deutlich. In § 107 Abs. 3 Satz 2 AktG sind als Aufgaben des Prüfungsausschusses die Überwachung des Rechnungslegungsprozesses, der Wirksamkeit des IKS, des RMS und des internen Revisionsystems sowie der Abschlussprüfung benannt. Während sich der Rechnungslegungsprozess ausschließlich auf die Verfahren und Funktionen zur zeitnahen Erfassung rechnungslegungsrelevanter Ereignisse sowie der Aufstellung, Verabschiedung und Veröffentlichung von Abschlüssen beschränkt, beziehen sich das IKS und RMS – als ebenfalls prozessintegrierte Überwachungselemente – auf alle Prozesse des Unternehmens. Interne Revision und Abschlussprüfer bilden dagegen die prozessunabhängigen Überwachungselemente, wobei letzterer Teil des externen Überwachungssystems ist.

IKS und RMS stehen also in einer engen Beziehung bzw. Wechselwirkung zueinander, da beide Systeme auf den Schutz des Unternehmens vor Risiken ausgerichtet sind: Das Kontrollumfeld als Fundament des IKS wird u. a. durch die Risikostrategie determiniert, die wiederum Teil des RMS ist. Die IKS-Komponenten Risikobeurteilung (Identifizierung und Bewer-

tung von Risiken), Kontrollaktivitäten (Grundsätze und Verfahren zum angemessenen Umgang mit Risiken) sowie Information und Kommunikation (Herstellen einer Entscheidungsgrundlage für die Unternehmensleitung) finden sich ebenfalls im RMS wieder; werden im IKS neue Risiken aufgedeckt, dann überschneiden sie sich sogar. Daher ist eine genaue Abgrenzung nicht immer möglich bzw. i. S. eines weitgehend integrierten Überwachungsansatzes auch nicht erforderlich bzw. notwendig.

Ein integrierter Ansatz von IKS und RMS findet sich beim COSO-Enterprise Risk Management-Modell (COSO-ERM)¹³. Hierbei wird das Internal Control Framework nicht durch COSO-ERM ersetzt, sondern in einen größeren Rahmen integriert. Die stärkere Differenzierung des Risikomanagementprozesses wird durch die Aufteilung der Risikobeurteilung in die vier Bereiche Zielsetzung (Vereinbarkeit der gewählten Unternehmensziele mit dem Unternehmensleitbild und der festgelegten Risikobereitschaft), Ereignisidentifikation (mögliche Einflüsse auf Strategieumsetzung und Zielerreichung), Risikobeurteilung und Risikosteuerung erreicht¹⁴. COSO-ERM bildet somit eine Grundlage für die Integration von IKS und RMS.

Während IKS und RMS in der operativen Verantwortung des Vorstands bzw. der Geschäftsleitung inzwischen integrale Bestandteile der Geschäftsprozesse sind, hat der Prüfungsausschuss infolge der aktienrechtlichen Änderungen durch das BilMoG deren Wirksamkeit zu überwachen. Zur Beurteilung der Wirksamkeit sind als notwendige Bedingungen die Angemessenheit (Entsprechen Aufbau und Umfang der Systeme der Risikoneigung des Unternehmens?) und die Funktionsfähigkeit (Können die Systeme den beabsichtigten Zweck erfüllen?) regelmäßig zu definierten Zeitpunkten zu prüfen. Der Prüfungsausschuss kann sich dabei der Ergebnisse von Interner Revision und externem Abschlussprüfer bedienen.

Hinreichende Bedingung für die Wirksamkeit der Systeme ist die kontinuierliche Prüfung ihrer Wirkung. Dazu ist in einem laufenden Prozess abzugleichen, ob

- eingetretene Risiken tatsächlich durch die Systeme erkannt und Maßnahmen zur Risikoreduzierung abgeleitet worden sind (1. Ebene),
- diese Maßnahmen auch umgesetzt worden sind (2. Ebene), und
- diese zudem geeignet sind, die Risiken zu reduzieren (3. Ebene).

These 2: Im Rahmen seiner Überwachungstätigkeit beurteilt der Prüfungsausschuss die Angemessenheit und Funktionsfähigkeit der Maßnahmen zur Erkennung und Steuerung der wesentlichen Unternehmensrisiken.

Ziel der Überwachungstätigkeit des Prüfungsausschusses ist es, Angemessenheit und Funktionsfähigkeit der identifizierten Maßnahmenbündel zur Erkennung und Steuerung der wesentli-

7 Zum Umgang mit den Herausforderungen im Risikomanagement von Unternehmen, vgl. AKEIÜ, DB 2010 S. 1245-1252.

8 Vgl. Buderath/Amling, in: Dörner/Horváth/Kagermann, Praxis des Risikomanagements – Grundlagen, Kategorien, branchenspezifische und strukturelle Aspekte, 2000, S. 127-152.

9 Vgl. Amling/Bantleon, Handbuch der Internen Revision – Grundlagen, Standards, Berufsstand, 2007, S. 126.

10 Vgl. COSO, Internal Control – Integrated Framework, abrufbar unter: www.coso.org/documents/VolumeII-Guidance.pdf (Abruf: 26. 7. 2011).

11 Zur Ausgestaltung von Compliance als Bestandteil des IKS, vgl. AKEIÜ, DB 2010 S. 1509-1518.

12 Vgl. Amling/Bantleon, a.a.O. (Fn. 9), S. 112 ff.

13 Vgl. COSO, Enterprise Risk Management – Integrated Framework. Eine Zusammenfassung in deutscher Sprache ist abrufbar unter: www.coso.org/documents/COSO_ERM_ExecutiveSummary_German.pdf (Abruf: 26. 7. 2011)

14 Vgl. Amling/Bantleon, a.a.O. (Fn. 9), S. 117 ff.

chen Unternehmensrisiken zu beurteilen. Dazu hat er ein Verständnis über die verlässliche Einschätzung und Steuerung wesentlicher Risiken zu erlangen, Steuerungslücken und -schwächen zu identifizieren sowie zu beurteilen, ob Ergänzungsbedarf oder Optimierungspotenzial besteht.

Im Sinne eines risikoorientierten Überwachungsansatzes¹⁵ muss der Prüfungsausschuss das zugrundeliegende Inventar wesentlicher Unternehmensrisiken hinterfragen und beurteilen. Da alle weiteren Aktivitäten zum Wirksamkeitsnachweis auf der initialen Risikobewertung aufbauen, kommt der Qualität dieses Risikoinventars eine besonders hohe Bedeutung zu. Dabei gilt es zu bewerten, ob alle wesentlichen Risiken erfasst wurden und ob die ausgewählten Risiken tatsächlich wesentlich sind. Damit der Prüfungsausschuss dieser Aufgabe nachkommen kann, müssen das Inventar und die Begründung für die Risikopriorisierung bzw. der Prozess der Risikoidentifikation als Bestandteil eines umfassenden Risikomanagements nachvollziehbar dokumentiert und transparent sein.

In einem zweiten Schritt erfolgt die Beurteilung der eingereichten Maßnahmen zur Steuerung der wesentlichen Unternehmensrisiken hinsichtlich deren Angemessenheit und Funktionsfähigkeit. Bezüglich der Angemessenheit gilt es zu beurteilen, ob die erfassten Maßnahmenbündel tatsächlich die Risiken adäquat adressieren. Die Bewertung der Funktionsfähigkeit umfasst die Feststellung, ob bzw. inwieweit das definierte Soll für einen bestimmten Zeitraum tatsächlich im Unternehmen gelebt wird und welche Verbesserungspotenziale bestehen.

Vor diesem Hintergrund kommt der Nachweisführung zur Wirksamkeit der relevanten Maßnahmen erhebliche Bedeutung zu. Hierzu bieten sich verschiedene Ansätze an. Die Selbsteinschätzung durch die für die Durchführung von Maßnahmen und Prozessen Verantwortlichen stellt die Basis der Nachweisführung dar. Hierbei werden die relevanten Maßnahmen hinsichtlich ihrer Angemessenheit und Funktionsfähigkeit durch die Maßnahmenverantwortlichen selbst beurteilt. Vorteile dieses Verfahrens bestehen in dem hohen Organisations- und Prozesswissen der Durchführenden. Dem gegenüber steht der Nachteil der fehlenden Unabhängigkeit der Maßnahmenverantwortlichen und damit einhergehend die eingeschränkte Verwertbarkeit entsprechender Aussagen für Überwachungszwecke.

Insofern wird die Selbsteinschätzung regelmäßig ergänzt durch eine systematische Einbindung der Internen Revision als prozessunabhängige Überwachungsinstanz. Grundsätzlich sollten die als relevant definierten Maßnahmen zur Steuerung der wesentlichen Unternehmensrisiken Bestandteil der Prüfungsplanung der Internen Revision sein und insofern im Rahmen einer rollierenden Prüfung regelmäßig durch diese berücksichtigt bzw. hinsichtlich ihrer Angemessenheit und Funktionsfähigkeit überprüft werden. Sofern über die Prozessunabhängigkeit hinausgehende Unabhängigkeitsanforderungen an die Nachweisführung bestehen, empfiehlt sich die Hinzuziehung externer bzw. unternehmensunabhängiger Experten (z. B. geeignete Beratungs- oder Wirtschaftsprüfungsgesellschaften).

In der Praxis bieten sich Kombinationen dieser Instrumente an. Hierbei ist festzustellen, dass sich der Einsatz prozess- und unternehmensunabhängiger Prüfungsinstanzen für die Nachweisführung umso mehr empfiehlt, je höher das angestrebte Sicherheitsniveau ist.

Prüfungen zur Angemessenheit und Wirksamkeit des rechnungslegungsbezogenen IKS sind grds. Gegenstand der regulären Jahresabschlussprüfung, über deren Ergebnisse der Abschlussprüfer gem. § 171 Abs. 1. Satz 2 AktG gegenüber dem Aufsichtsrat berichtet. Insofern empfiehlt es sich, hinsichtlich

der relevanten Maßnahmen zur Steuerung von wesentlichen Risiken in der Finanzberichterstattung, die Prüfungstätigkeit des Abschlussprüfers in dem Maße zu berücksichtigen, wie die relevanten Maßnahmen Gegenstand der Abschlussprüfung sind.

Die Ergebnisse der Nachweisführung zur Wirksamkeit sind zusammengeführt und in geeigneter Form aufbereitet an den Prüfungsausschuss zu berichten. Sie ergänzen das Inventar der wesentlichen Unternehmensrisiken und die relevanten Maßnahmen zur Steuerung dieser Risiken, um daraus schließlich Aussagen zur Wirksamkeit im Berichtszeitraum abzuleiten.

Angesichts der Anforderungen an die Überwachungsaktivitäten des Prüfungsausschusses kommt der nachweislichen Dokumentation des Inventars wesentlicher Unternehmensrisiken und der zugrundeliegenden Inventur, der Darstellung der relevanten Maßnahmen sowie den Aussagen zu deren Wirksamkeit eine hohe Bedeutung zu. Diese Dokumentation dient als Nachweis einer ordnungsmäßigen Unternehmensüberwachung. Dem Prüfungsausschuss ist i. d. R. ein sorgfältiges und pflichtgemäßes Handeln zu bestätigen, wenn er sich davon überzeugt hat, dass die Maßnahmen zur Steuerung der wesentlichen Unternehmensrisiken vorhanden und wirksam sind. Darüber hinaus hat er zu beurteilen, ob die Systeme in personeller und sachlicher Hinsicht angemessen ausgestattet sind und laufend an neue Risiken sowie Geschäftsentwicklungen angepasst werden.

These 3: Die Überwachungstätigkeit des Prüfungsausschusses ist fortlaufend angelegt und beruht auf Informationen, die im Rahmen eines Regelprozesses erhoben und zur Verfügung gestellt werden.

Die Überwachung der Wirksamkeit des IKS und RMS stellt hohe Anforderungen an die Informationsversorgung des Prüfungsausschusses. Voraussetzung für die Überwachungstätigkeit ist eine ausreichende Transparenz über das Überwachungsobjekt.

Der Aufsichtsrat hat gegenüber dem Vorstand einen systematischen Wissens- und Informationsnachteil, wodurch seine Überwachungsaufgabe erschwert wird. Aus diesem Grund hat das deutsche Aktienrecht dem Vorstand eine umfassende Informationspflicht gegenüber dem Aufsichtsrat auferlegt (§ 90 AktG). Zugleich verfügt der Aufsichtsrat über ein gesetzlich garantiertes Informationsrecht. Der Aufsichtsrat kann somit jederzeit detaillierte Informationen vom Vorstand verlangen (§ 90 Abs. 3 AktG) und sämtliche Unterlagen einsehen und prüfen (§ 111 AktG). Neben den Berichten des Vorstands kann der Aufsichtsrat auch den Abschlussprüfer sowie Sachverständige und weitere Auskunftspersonen als Informationsquellen nutzen.

Um sein Informationsrecht gegenüber dem Vorstand wirksam einsetzen zu können, hat der Prüfungsausschuss zunächst Überlegungen zu seiner optimalen Informationsversorgung anzustellen. Dazu empfiehlt sich der Erlass einer Informationsordnung, die regelt, über welche Sachverhalte, in welcher zeitlichen Frequenz und in welcher Form der Vorstand dem Aufsichtsrat zu berichten hat. In der Praxis großer Unternehmen hat sich eine Quartalsberichterstattung über die Funktionsfähigkeit und Wirksamkeit der Überwachungssysteme etabliert. Bei kleineren Unternehmen wird auch eine jährliche Berichterstattung durch den Vorstand noch angemessen sein, insbesondere wenn in der Vergangenheit keine gravierenden Schwachstellen hinsichtlich der eingerichteten Systeme festgestellt wurden.

¹⁵ In Rechtsprechung und der juristischen Fachliteratur wird von dem Aufsichtsrat eine Überwachungstätigkeit verlangt, die sich an die jeweilige Risikosituation und die Lage der Gesellschaft anzupassen hat und bei erkannten Mängeln oder Krisensituationen zu intensivieren ist; vgl. Habersack, in: Kropff, Münchener Kommentar zum AktG, 3. Aufl., § 111, Rdn. 46 und § 116, Rdn. 37, jeweils m. w. N.

Dem Vorstand obliegt die Verantwortung, dem Prüfungsausschuss die für dessen Überwachungsaufgabe erforderlichen Informationen bereitzustellen. Im Unternehmen beschäftigen sich i. d. R. sehr unterschiedliche Bereiche mit dem IKS und dem RMS. Neben dem Vorstand und den Leitern von operativen Einheiten bzw. Gesellschaften können das Controlling, das Rechnungswesen, die Interne Revision, die Rechtsabteilung bzw. eine eigene Compliance-Abteilung funktionale Verantwortung für Teilfunktionen tragen. Neben den Gefahren, die sich hieraus durch unterschiedliche inhaltliche Blickwinkel und Risikobeurteilungen ergeben können (vgl. These 4), führt diese gesplittete Verantwortung in der Praxis häufig auch zu nicht vergleichbaren Informations- und Berichtsstrukturen. Um den o. g. Anforderungen an Vorstandsberichte für den Prüfungsausschuss gerecht zu werden, ist es erforderlich, einen Regelprozess für die Erhebung und Zusammenstellung der relevanten Informationen zu etablieren sowie die Informations- und Berichtsstrukturen zu harmonisieren. Unabhängig von der formalen Berichterstattungspflicht durch den Gesamtvorstand sollte der Prüfungsausschuss im Grundsatz wissen, wie die Informationsbeschaffung und -aufbereitung organisiert ist, um die Qualität und Belastbarkeit der Informationen besser einschätzen zu können. Grundlage für die Informationsbeschaffung ist die Dokumentation des IKS und RMS, aus der die Risiken, die eingerichteten internen Kontrollen und die dahinter liegenden Prozesse sowie die Ergebnisse der Wirksamkeitsüberprüfung hervorgehen. Gerade in der Praxis zeigt sich aber, dass in der Dokumentation der relevanten Elemente des IKS und RMS Verbesserungsbedarf besteht¹⁶.

Die schriftlichen Berichte sollten im Umfang so gehalten sein, dass sie weder aufgrund ihrer Datenfülle die Bereitschaft zur Informationsaufnahme lähmen noch durch zu knappe Aussagen wichtige Hinweise verloren gehen. Weitere Anforderungen an die Berichte sind Aktualität, eine übersichtliche und geordnete Darstellung, die i. d. R. einem einheitlichen Schema folgen sollte, sowie die Vergleichbarkeit mit früheren Berichten.

Inhaltlich umfasst die Berichterstattung an den Prüfungsausschuss über die Wirksamkeit des IKS und RMS die folgenden Mindestbestandteile:

- Überblick über wesentliche Instrumente des IKS und RMS (umfassende Erstberichterstattung, Aktualisierung bei Änderungen): Themen und Verantwortlichkeiten, Risiken, wesentliche Prozesse und Maßnahmen, Implementierungsstand;
- Ergebnisse aus der Analyse der Angemessenheit und Funktionsfähigkeit der internen Steuerungs- und Kontrollsysteme;
- Festgestellte wesentliche Schwächen bzw. Verstöße und Vorschläge zum weiteren Vorgehen;
- Überblick über den Status der Beseitigung wesentlicher Schwächen und den Umsetzungsstand von Aufträgen des Prüfungsausschusses.

Sind die vorgelegten Informationen lückenhaft oder ergeben sich daraus Zweifel, trifft den Prüfungsausschuss die Pflicht, weitere Informationen beim Vorstand anzufordern. Dieses Nachfragen kann zunächst persönlich in der folgenden Sitzung des Prüfungsausschusses erfolgen. Daneben kann der Prüfungsausschuss dem Vorstand seine Fragen aber auch in schriftlicher Form vorlegen, auf die dieser bis zur nächsten Prüfungsausschusssitzung zu reagieren hat. Die Fragen des Prüfungsausschusses können von der Risikostrategie über die Risikobewertung bis hin zur Systemüberwachung reichen¹⁷.

Neben dem Vorstand kann der Prüfungsausschuss auf weitere Informationsquellen zurückgreifen, von denen der Abschluss-

prüfer den wichtigsten vom Vorstand unabhängigen Informationslieferanten darstellt. Bei der Wahrnehmung seiner Überwachungsaufgabe wird der Prüfungsausschuss durch den Abschlussprüfer unterstützt, da er in der Bilanzsitzung die wesentlichen Schwächen des IKS und des RMS bezogen auf den Rechnungslegungsprozess mündlich zu erläutern hat (§ 171 Abs. 1 Satz 2 AktG). Sofern keine Befangenheitsgründe dagegen sprechen, kann der Prüfungsausschuss den Abschlussprüfer auch mit Sonderprüfungen zu bestimmten Sachverhalten und Fragen zum IKS und RMS beauftragen.

Schließlich ist auch die Hinzuziehung von Sachverständigen und Auskunftspersonen zu den Sitzungen des Prüfungsausschusses eine weitere Möglichkeit, relevante Informationen über das IKS und RMS zu erhalten. Insbesondere Mitarbeiter des Unternehmens, z. B. die Leiter der Bereiche Controlling, Rechnungswesen, Interne Revision und Compliance sind hier wichtige zusätzliche Informationsquellen. Aufgrund des dualistischen Systems der deutschen Unternehmensverfassung hat der Prüfungsausschuss jedoch keinen unmittelbaren Zugriff auf Mitarbeiter des Unternehmens und ist diesen gegenüber auch nicht weisungsbefugt. Daher sollten Mitarbeiter grds. über den Vorstand geladen werden, um nicht dessen Leitungsautorität zu untergraben. Kommt der Vorstand dieser Aufforderung nicht nach, ist der Prüfungsausschuss jedoch nötigenfalls auch berechtigt, leitende Mitarbeiter direkt einzuladen, wenn dies z. B. in einer Informationsordnung geregelt ist.

Auf Basis der durch die unterschiedlichen Kanäle erhaltenen Informationen muss der Prüfungsausschuss sich ein eigenes Urteil über die Wirksamkeit des IKS und RMS bilden. Er muss hinterfragen, ob die aktuellen Systeme ausreichend sind oder ergänzt, erweitert bzw. verbessert werden müssen. Um seiner eigenen Sorgfaltspflicht Genüge zu tun, liegt es im Interesse des Prüfungsausschusses, den Vorstand zu veranlassen, ein umfassendes und wirksames IKS und RMS einzurichten bzw. zu betreiben.

These 4: Die umfassende Überwachungstätigkeit des Prüfungsausschusses basiert auf einem integrierten Steuerungs- und Kontrollsystem.

Die interne Unternehmenskontrolle mit den klassischen Funktionen Controlling und Interne Revision wurde in der Vergangenheit in vielen Unternehmen aufgrund von Trends und regulatorischen Anforderungen durch separate Teilfunktionen und -systeme, wie z. B. Risikomanagement, Compliance, IT-Sicherheit, Qualitätsmanagement, internes Kontrollsystem, Controls nach dem Sarbanes-Oxley Act etc. ergänzt. Diese Systeme operieren häufig ohne gegenseitige Abstimmung.

War ihre getrennte Einführung beim erstmaligen Aufbau i. d. R. sinnvoll, da dadurch die Komplexität verringert und die Implementierung beschleunigt wurde, so ist die Trennung aber durch Überschneidungen ineffizient und birgt die Gefahr, dass Risiken von keinem Teilsystem erfasst und berichtet werden. Zudem besteht das Risiko, die Berichtsadressaten mit inkonsistenten und inkohärenten Informationen zu überlasten, was dazu führen kann, dass diese sich nicht auf die Top-Prioritäten konzentrieren können. Daher besteht nicht nur hinsichtlich der Berichterstattung an den Prüfungsausschuss, sondern vielmehr aufgrund ökonomischen Kalküls die Notwendigkeit, Transparenz zu schaffen und Kontrolllücken zu schließen sowie Doppelarbeiten durch Mehrfachkontrolle zu vermeiden und Schnittstellen zu reduzieren.

16 Vgl. Wermelt/Saitz, ZCG 2011 S. 30 f.

17 Zu Vorschlägen für kritische Fragen des Aufsichtsrats zur Wirksamkeit eines RMS vgl. Withus, DB 2009 Beil. 5 S. 82 f.

Zur beschleunigten Umsetzung wird es sich häufig anbieten, die Integration der Kontrollsysteme zunächst mit der Einrichtung einer integrierten Berichterstattung zu beginnen. Die hierbei gewonnenen Erkenntnisse sind geeignet, die Umsetzung der weiteren Schritte zu unterstützen. Die Integration wird dadurch gefördert, dass die Kontrollsysteme mit Geschäftsleitung und Prüfungsausschuss den gleichen Adressatenkreis haben, häufig die gleichen Geschäftsprozesse in der Wertschöpfungskette betrachten und somit die Verantwortung beim Linienmanagement und häufig sogar bei den gleichen Managern oder Gremien liegt.

Die Integration der Berichterstattung soll durch Vorgaben der Berichtsempfänger oder durch eine von diesen beauftragte Stelle erfolgen. In der Praxis wird dies häufig durch ein Gremium vorgenommen, in dem Vertreter der betroffenen Kontrollsysteme sowie der Geschäftsfelder bzw. Unternehmensfunktionen vertreten sind. Zu entscheiden ist auch das Ausmaß der Integration, d. h. ob die Berichterstattung in erster Linie für die Geschäftsleitung und den Prüfungsausschuss integriert wird oder ob die Berichtsintegration bereits ab der untersten operativen Ebene beginnt.

Bei der Vereinheitlichung der Berichterstattung sind insbesondere die Datenaktualität und hier speziell die Angleichung der Berichtstermine, die Objektivität und Plausibilität sowie der Verdichtungsgrad zu berücksichtigen. Um die Konsistenz zwischen den Berichten der Teilsysteme sicherzustellen, sind ein übergreifender Risikokatalog zu erstellen und allgemeine Risikoprämissen, z. B. für die Risikobewertung, zu verwenden. Die Herausforderung bei der Verdichtung der Teilberichte besteht darin, die unterschiedlich quantifizierbaren und teilweise nur qualitativ bewertbaren Risiken so darzustellen, dass die Top-Risiken für den Adressaten sofort erkennbar sind und dennoch auch die notwendige Breite der Information zur Verfügung steht.

Die hier betrachteten Kontrollsysteme betreffen die Steuerung von Risiken im weiteren Sinne. Der Unterschied zwischen den Systemen liegt jedoch in der Praxis nicht nur in einem unterschiedlichen inhaltlichen Blickwinkel, sondern auch in verschiedenen methodischen Ansätzen, die zu inkonsistenten Risikobeurteilungen führen können.

Der Grad der organisatorischen Integration der Kontrollsysteme hängt von den unternehmensspezifischen Gegebenheiten des Einzelfalls ab. Sie kann zu Strukturveränderungen bis hin zu einer Zusammenlegung der die Kontrollsysteme betreibenden Funktionen in einer Abteilung reichen. Aber auch die Beibehaltung der bestehenden Aufbauorganisation kann aufgrund der

unterschiedlichen Aufgabenstellung der Teilsysteme sinnvoll sein. Aber auch in diesem Fall geht die Integration über eine reine Koordination hinaus, da neben dem bereits ausgeführten einheitlichen Berichtswesen und der Abstimmung der Prozesse und Instrumente ein widerspruchsfreies Rollen- und Aufgabenverständnis zwischen den Kontrollsystemen zu entwickeln ist. Dies ist die Basis für eine konsistente übergreifende Steuerung der Risiken im weiteren Sinne aus den einzelnen Bereichen Operations, Compliance und Rechnungslegung.

Im Ergebnis führt die Integration der Steuerungs- und Kontrollsysteme sowohl auf der Ebene der Organisation und der individuellen Prozesse als auch auf der Ebene der Berichterstattung zu einer erhöhten Überwachungseffizienz.

III. Zusammenfassung und Ausblick

Die vorliegenden Thesen zur Überwachung der Wirksamkeit des IKS und des RMS spiegeln die in den letzten zwei Jahren gemachten Erfahrungen mit dem BilMoG wider. Dabei stehen IKS und RMS in einer engen Wechselwirkung zueinander, da beide Kontrollsysteme auf den Schutz des Unternehmens vor Risiken ausgerichtet sind. Der Prüfungsausschuss hat sich bei seiner Überwachung auf die vom Vorstand eingeleiteten Maßnahmen zur Steuerung der wesentlichen Risiken zu konzentrieren.

Die konkrete Durchführung der Wirksamkeitsüberwachung stellt hohe Anforderungen an die Informationsversorgung des Prüfungsausschusses. Um eine ausreichende Transparenz der zu überwachenden Systeme herzustellen, sollten die regelmäßig zu erstattenden Berichte und die Möglichkeit zur Befragung von leitenden Mitarbeitern in einer Informationsordnung festgelegt werden. Angesichts der Vielfalt der zu überwachenden Systeme – neben dem IKS und RMS hat der Prüfungsausschuss das interne Revisionssystem und die Compliance (Tz. 5.3.2 DCGK) zu überwachen – ist eine stärkere Integration der im Unternehmen eingerichteten Kontrollsysteme notwendig, um inkonsistente Informationen zu vermeiden.

Die Konkretisierung der Überwachungspflichten durch den § 107 Abs. 3 Satz 2 AktG hat den Prüfungsausschuss vor neue Herausforderungen gestellt. Der Prozess der tatsächlichen Ausgestaltung dieser Verpflichtung ist noch nicht abgeschlossen. Die aus der Unternehmenspraxis entwickelten vier Thesen sollen einen Ansatz zur Überwachung der Wirksamkeit der Kontrollsysteme darstellen und so zur Bildung einer allgemein anerkannten Best Practice beitragen.

Dipl.-Kfm. Dr. Niko Frey / Dipl.-Kfm. David Rapp, beide Saarbrücken / StB/vBP Dr. Carl W. Barthel, Köln

Unternehmenswert: Das Problem der Scheingenauigkeit

– Erwiderung und Replik zu dem Beitrag von Barthel, DB 2010 S. 2236 ff. –

► DB0417021

A. Erwiderung von Dr. Niko Frey und David Rapp

I. Einleitung

In seinem Beitrag diskutiert *Barthel* Rahmenbedingungen, die seiner Meinung nach zu einer Nichtanwendbarkeit der Ertragswertmethode bei der Bewertung von Unternehmen führen. Er

Dipl.-Kfm. Dr. Niko Frey und Dipl.-Kfm. David Rapp sind als wissenschaftliche Mitarbeiter am Institut für Wirtschaftsprüfung an der Universität des Saarlandes tätig. Dr. Carl W. Barthel ist in eigener Praxis als Steuerberater und vereidigter Buchprüfer in Köln tätig.