KONSTANZ INSTITUT FÜR CORPORATE GOVERNANCE

Compliance-Prüfung nach dem IDW EPS 980 – Pflicht oder Kür für den Aufsichtsrat?

Stephan Grüninger

KICG – Forschungspapiere
Nr. 1 (2010)
ISSN 2198-4913

Konstanz Institut für
Corporate Governance

Hochschule Konstanz
Brauneggerstraße 55
78462 Konstanz

www.kicg.htwg-konstanz.de

KICG-Forschungspapier Nr. 1 (2010)

Compliance-Prüfung nach dem IDW EPS 980 – Pflicht oder Kür für den Aufsichtsrat?

Stephan Grüninger

Der folgende Artikel ist in der Ausgabe 10/2010 (S. 141-142) der Zeitschrift „Der Aufsichtsrat" in einer gekürzten Fassung erschienen.

Das KICG ist ein Forschungsinstitut der HTWG Konstanz, Brauneggerstr. 55, 78462 Konstanz.

Kontakt

Konstanz Institut für
Corporate Governance
Hochschule Konstanz
Brauneggerstraße 55
78462 Konstanz
www.kicg.htwg-konstanz.de

„Der Aufsichtsrat legt selbst fest, wie er sich über die Corporate Compliance informiert."

Compliance ist originär Managementaufgabe und liegt damit in der Verantwortung des Vorstandes bzw. der Geschäftsführung. Naheliegend ist, dass dem Aufsichtsrat als Überwachungsorgan eine Rolle im Rahmen der Compliance-Prüfung zukommt. Anlässlich der Veröffentlichung des Entwurfs für einen Prüfungsstandard – Grundsätze ordnungsgemäßer Prüfung von Compliance Management Systemen (IDW EPS 980) – des Instituts der Wirtschaftsprüfer sollen in diesem Beitrag drei Aspekte dieses Themas erörtert werden. Erstens soll das Verhältnis von Leitung und Überwachung im Compliance-Management behandelt und dabei auch die Rolle des Aufsichtsrates geklärt werden. Zweitens wird das Thema der Compliance-Prüfung in Grundzügen diskutiert und drittens der neue Prüfungsstandard des IDW knapp vorgestellt und wesentliche Anforderungen einer kritischen Beurteilung unterzogen.

1 Leitung und Überwachung im Compliance-Management

Das Thema Compliance-Management ist in aller Munde, insbesondere aufgrund vieler Fälle von Korruption und kartellrechtswidrigen Absprachen in den letzten Jahren und aktuell – gelegentlich auch unter direkter Mitwirkung oder Duldung des Top-Managements. Ein vom Verfasser in 2010 mit herausgegebenes Werk zum Thema Compliance fokussiert auf den Aspekt des Managements dieser Organisationspflicht.[1] Diese Betonung als *Management*aufgabe signalisiert erstens, dass der Vorstand die Verantwortung für das rechtmäßige Verhalten der AG trägt (Legalitätspflicht) – was die Entscheidung einschließt, ob er dazu ein Compliance-Management-System (CMS) einrichten muss – und unterstreicht zweitens gleichzeitig, dass Compliance eine dauerhafte Aufgabe im Rahmen der strategischen und operativen Unternehmensführung darstellt, mit anderen Worten, eine Aufgabe, die in die Geschäftsprozesse und -routinen integriert werden muss, die unabweisbares Kriterium in Entscheidungsfindungsprozessen zu sein hat und die als Bestandteil der Geschäftskultur zum Verhaltens- und Erfolgsmaßstab von Organmitgliedern und Mitarbeitern gemacht werden muss. Die Abteilung bzw. Funktion „Corporate Compliance", der Compliance-Beauftragte oder Chief Compliance Officer (CCO) im Unternehmen hat dann die Aufgabe, Programme und Maßnahmen zur Unterstützung der Sicherstellung der Einhaltung der Compliance zu entwickeln, zu implementieren und hat deren Durchsetzung zu überwachen und berichtet hierüber dem Vorstand.

Compliance selbst bleibt Aufgabe des Linienmanagements: diejenigen also, die die unternehmerischen – strategischen und operativen – Entscheidungen treffen, müssen auch für das Compliance-gerechte Handeln und Verhalten bei der Anbahnung und Abwicklung der Geschäfte eines Unternehmens verantwortlich sein. Dies bleibt im Übrigen auch nach dem viel beachteten BGH-Urteil vom 17.7.2009 – 5 StR 394 richtig, bei dem sich das Gericht nebenbei zur strafrechtlichen Garantenstellung des Compliance Officers geäußert und dabei allerdings festgestellt hat, dass ein für Compliance verantwortlicher Mitarbeiter in der Regel dazu ver-

[1] Vgl. Wieland, J./Steinmeyer, R./Grüninger, S.: Handbuch Compliance-Management. Berlin: Erich Schmidt 2010.

pflichtet ist, Straftaten von Unternehmensangehörigen gegen Dritte, die aus dem Unternehmen heraus begangen werden, zu verhindern.[2] So wichtig nach diesem Urteil die exakte Beschreibung der Aufgaben und Verantwortungen des Compliance Officers – einschließlich der expliziten Nennung von Bereichen, die nicht zu dessen Aufgabengebiet gehören – auch ist, hinzu kommen muss die Erkenntnis, dass nur eine gewollte und top-down konsequent durchgesetzte Compliance-Kultur die notwendige präventive Wirkung entfalten kann. Die Compliance-Maßnahmen sind in der Literatur bereits umfassend beschrieben[3] und werden auch vom IDW EPS 980 wieder aufgegriffen (s.u.). Deren Definition und Entwicklung, praktische Implementierung und Durchsetzung sowie die Überprüfung der Funktionsfähigkeit des CMS ist Obliegenheit des Vorstandes – diese Aufgaben kann er (an einen Compliance Officer) delegieren, die Verantwortlichkeit für Compliance indes nicht.

Den Aufsichtsrat einer AG trifft gemäß § 111 AktG bekanntermaßen die Pflicht, den Vorstand zu überwachen. Diese Überwachungspflicht erstreckt sich neben der Prüfung von Jahresabschluss Lagebericht, Gewinnverwendungsvorschlag etc. auch auf das Risikofrüherkennungssystem (das der Vorstand nach § 91, Abs 2 AktG einzurichten hat). Im Zuge der Einführung des BilMoG wurde klargestellt, dass der Aufsichtsrat bzw. der Prüfungsausschuss sich u.a. auch mit der Überwachung der Wirksamkeit des Internen Kontrollsystems, des Risikomanagementsystems sowie des Internen Revisionssystems zu befassen hat. Nach allgemeiner Auffassung gehören hierzu auch die Compliance-Maßnahmen des Unternehmens;[4] dies sieht auch der Deutschen Corporate Governance Kodex so vor (Tz. 5.3.2. in Verbindung mit Tz. 3.4. und Tz. 4.1.3.).

Als zweite Säule der Compliance-Prüfung und zusätzlich zur durch die Unternehmensleitung (Vorstand) obligatorisch vorzunehmenden Überprüfung der Funktionsfähigkeit des CMS (durch Compliance Office, Interne Revision) prüft der Aufsichtsrat die Compliance im Rahmen seiner Tätigkeit der Überwachung des Vorstandes. Auf dem Prüfstand steht hier also praktisch immer die Arbeit des Vorstandes in Sachen Compliance und damit auch die Arbeit des CCO. Nach allgemeiner Auffassung bleibt es im Benehmen des Aufsichtsrats festzulegen, wie er sich über die Corporate Compliance informiert. Er kann dies mittels der Berichterstattung des Vorstandes tun oder aber er greift zusätzlich auf unabhängige, externe Dienstleister (z.B. Wirtschaftsprüfer) zurück, die in seinem Auftrag eine Prüfung durchführen bzw. ein Gutachten erstellen. Damit ist die im Titel des Beitrags gestellte Frage bereits beantwortet: die Prüfung eines CMS nach dem IDW EPS 980 ist für den Aufsichtsrat alles andere als zwingend. Es ist vielmehr so, dass der Aufsichtsrat sich auch mit einem unabhängigen, externen Prüfungsunternehmen auf vertraglich abgestimmte Prüfverfahren bzw. Untersuchungshandlungen und Gegenstandsbereiche der Prüfung verständigen kann (sog. „Agreed Upon Procedures“). Darüber hinaus besteht selbstverständlich die Möglichkeit, dass der Aufsichtsrat die Beurteilung der Corporate Compliance entlang eigener Prüfungshandlungen (Besprechung mit Vorstand, Analyse der

[2] Vgl. dazu Rotsch, T.: Entscheidungsbesprechung – Garantenpflicht aufgrund dienstlicher Stellung, in: ZJS 6/2009, 712ff. Den Compliance Officer trifft die Garantenstellung zur Verhinderung von unternehmensbezogenen Straftaten gegen Dritte aber nur dann, wenn ihm diese Aufgabe zugewiesen ist (z.B. durch Arbeitsvertrag). Zur rechtsdogmatischen Analyse und kritischen Würdigung des erwähnten BGH-Urteils vgl. ebd. sowie Wybitul, T.: Strafbarkeitsrisiken für Compliance-Verantwortliche, in BB 2009, 2590 ff.

[3] Vgl. z.B. Grüninger, S.: Werteorientiertes Compliance-Management-System, in: Wieland, J./Steinmeyer, R./Grüninger, S. (Hrsg.): Handbuch Compliance-Management (a.a.O.), 39ff. sowie Wieland, J./Grüninger, S.: Die 10 Bausteine des Compliance-Managements, in: ebd., 111 ff.

[4] Vgl. z.B. Steinmeyer, R./Späth, P.: Rechtliche Grundlagen und Rahmenbedingungen der Legal Compliance, in:, Wieland, J./Steinmeyer, R./Grüninger, S. (Hrsg.): Handbuch Compliance-Management (a.a.O.), 198.

internen Compliance-Berichterstattung etc.) vornehmen und darauf beschränken kann. In diesem Zusammenhang stellt sich immer auch die Frage, inwieweit der Aufsichtsrat einen direkten Kontakt zum Leiter Interne Revision bzw. Chief Compliance Officer haben sollte, nicht zuletzt aufgrund der Möglichkeit doloser Handlungen durch den Vorstand selbst. Entgegen der gesetzlichen Regelung zur alleinigen Verantwortung für die Führung der Geschäfte in § 76 Abs. 1 AktG wird in der Literatur neuerdings teilweise empfohlen, dass eine solche Möglichkeit der unter Abwesenheit des Vorstandes durchgeführten Befragung der genannten Fachleiter durch den Aufsichtsrat oder Prüfungsausschuss gegeben sein sollte.[5] Diese Möglichkeit sollte am besten durch Aufnahme in eine Geschäftsordnung institutionalisiert werden, womit bei den zuständigen Fachleitern Handlungssicherheit geschaffen und gleichzeitig die Glaubwürdigkeit des gesamten Compliance-Managements nach innen und außen gesteigert wird.

2 Prüfung von Compliance-Management-Systemen

Die Praxis der CMS-Prüfung reicht in Deutschland weit über eine Dekade zurück.[6] In Deutschland wurden in diesem Zeitraum verschiedene Standards geschaffen, die in den Kontext der CMS-Prüfung gehören. Zunächst das System der Bayerischen Bauwirtschaft (EMB-Wertemanagement Bau e.V.) im Jahre 1996, danach das WerteManagementSystem^{ZfW}, das im Anwenderrat für Wertemanagement (AfW) – einem Zusammenschluss von Unternehmen (siehe www.dnwe.de/fci.html) – im Jahre 2000 veröffentlicht wurde, bald darauf die Initiative Corporate Governance der deutschen Immobilienwirtschaft e.V., die 2002 gegründet wurde und sich in 2008 eine Auditierungs- und Zertifizierungsordnung für CMS (diese wird im IDW EPS 980 als Referenzstandard erwähnt) nach dem Vorbild der Bauwirtschaft gegeben hat und schließlich der im AfW beratene und vom Zentrum für Wirtschaftsethik unter Mitwirkung des Verfassers herausgegebene ComplianceProgramMonitor^{ZfW}, ein Leitfaden für die Entwicklung, Implementierung und Überprüfung von CMS.

In diese Dekade fallen auch einige der schwerwiegenden Korruptionsskandale in Unternehmen, die – nicht zuletzt aufgrund der für sie relevanten US-amerikanischen Jurisdiktion – großangelegte und konsequent durchgesetzte CMS zur Folge hatten. In diesen Unternehmen war es dann auch wesentlich, die implementierten CMS einer objektiven und unabhängigen Überprüfung zu unterziehen, die jeweils durch Wirtschaftsprüfungsgesellschaften erfolgte. Zu den in dieser Zeit verfügbaren Quellen gehörten neben den genannten deutschen Referenzstandards insbesondere das COSO-Rahmenwerk, die US Sentencing Guidelines for Organizations, das Redbook der Open Compliance and Ethics Group (OCEG) sowie themenspezifische Guidance-Dokumente, wie etwa im Bereich der Korruptionsprävention die ICC Rules of Conduct oder die Business Principles for Countering Bribery.[7]

Referenzstandards können bei der CMS-Prüfung allerdings immer nur eine Quelle der Information für die Erarbeitung eines Prüfprogramms für das CMS eines Unternehmens

[5] Vgl. Nonnenmacher, R./Pohle, K./ von Werder, A.: Aktuelle Anforderungen an Prüfungsausschüsse, in: DB 60. Jg. (2007), 2412).
[6] Vgl. Wieland, J/Grüninger, S.: Ethikmanagement-Systeme und ihre Auditierung, in: Wieland, J. (Hrsg.): Dezentralisierung und weltweite Kooperationen – Die moralische Herausforderung der Unternehmen. Marburg: Metropolis 2000, 123-164.
[7] Eine Liste mit Referenzstandards findet sich im o.g. Handbuch Compliance-Management, 115f.

darstellen, schon aufgrund unterschiedlicher „Compliance-Komplexitätsstufen“, in denen sich Unternehmen befinden und die durch den Internationalisierungsgrad des Geschäfts (unterschiedliche Jurisdiktionen, spezifische Länderrisiken), die Umsatzhöhe, die Vertiebsstrukturen, die Mitarbeiterzahl und vieles andere mehr gegeben ist. Diese Beurteilung vorzunehmen bleibt Aufgabe des CMS-Prüfers, der darum über das entsprechende Fachwissen und die Erfahrung in der Prüfung solcher Systeme verfügen muss.

3 IDW EPS 980: Vorstellung und Möglichkeiten zur Verbesserung

Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) legt in dem neuen Prüfungsstandard (lediglich) seine Berufsauffassung zu CMS-Prüfungen dar. Eine gesetzliche Pflicht zur Prüfung von CMS gibt es offenkundig nicht, es handelt sich um freiwillige Prüfungen von CMS, auf die sich der Standard bezieht. Dennoch ist die Etablierung eines „Standards“ bekanntermaßen stets mit einer gewissen Festlegung von Qualitätsnormen verbunden, auf die sich Dritte (z.B. Gutachter, Gerichte) im Zweifel berufen werden. Der „IDW Prüfungsstandard: Grundsätze ordnungsgemäßer Prüfung von Compliance Management Systemen (IDW EPS 980)“, der als Entwurf vom Hauptausschuss (HFA) zum 11.03.2010 vorgelegt wurde, soll dabei angewendet werden für entsprechende Prüfungen, die nach dem 30.06.2011 durchgeführt werden.

Es ist zunächst hervorzuheben, dass die Erarbeitung des IDW EPS 980 zu tun hat mit den o.g. Anlässen und in diesem Zuge mit der Einrichtung von CMS in Unternehmen und der damit verbundenen Nachfrage nach unabhängiger Prüfung dieser Systeme. Die Darlegung der Berufsauffassung des IDW zu diesem Thema ist damit vor allem zu begrüßen – auch weil sie einen weiteren Schritt zur nachgefragten Konkretisierung der Anforderungen an ein CMS darstellt.

Der folgende Überblick über den neuen „Compliance-Standard“ fasst nur die wichtigsten Grundelemente und -ausrichtungen zusammen und muss aufgrund des Umfangs des IDW EPS 980 von 45 Seiten hier unvollständig bleiben.

Als Grundelemente eines CMS werden die Compliance-Kultur (1), Compliance-Ziele (2), Compliance-Organisation (3), Compliance-Risiken (4), Compliance-Programm (5), Compliance-Kommunikation (6) Compliance-Überwachung und Verbesserung (7) beschrieben. Der Standard sieht drei unterschiedliche Auftragstypen von CMS-Prüfungen vor. In Typ 1 ist Gegenstand der Prüfung die Konzeption des CMS, in Auftragstyp 2 die Angemessenheit und Implementierung des CMS und in Typ 3 die Angemessenheit, Implementierung und Wirksamkeit des CMS. Ein CMS kann sich nach IDW auf „abgegrenzte Teilbereiche“ (Geschäftsbereiche, operative Prozesse, bestimmte Rechtsgebiete) beziehen und die Prüfung auf diese beschränkt sein. Darüber hinaus beinhaltet der Standard Ausführungen zu Begriffsbestimmungen und Prüfungsanforderungen (v.a. Prüfungsplanung, Prüfungshandlungen, Berichterstattung).

Insgesamt ist dem IDW m.E. ein guter Entwurf für einen CMS-Prüfungsstandard gelungen, auch wenn er sich weitgehend auf den formalen Prüfprozess beschränkt und für die inhaltlichen Beschreibungen der Anforderungen auf „anerkannte CMS-Rahmenkonzepte“ verweist. Die folgenden Anregungen sind daher nur zur weiteren Verbesserung seiner Anwendbarkeit in der Praxis zu verstehen. Zunächst sollte darauf verzichtet werden, „vertragliche Verpflichtungen“ per se in den Fokus eines CMS zu nehmen, die Durchsetzung deren Einhaltung sollte bei den

Vertragpartnern verbleiben. Dass Elemente und Regeln des CMS zu Bestandteilen von Verträgen mit Lieferanten, Auftragsmittlern etc. gemacht werden ist ein davon zu unterscheidender Sachverhalt.

Zudem bleiben die Forderungen im Grundelement „Compliance-Ziele" zu unbestimmt und sind wenig nachvollziehbar. So fordert der Standard, dass „[d]ie gesetzlichen Vertreter […] auf der Grundlage der allgemeinen Unternehmensziele und einer Analyse und Gewichtung der für das Unternehmen bedeutsamen Regeln die Ziele fest[legen], die mit dem CMS erreicht werden sollen. […] Die Compliance-Ziele stellen die Grundlage für die Beurteilung von Compliance-Risiken dar." Zunächst ist dazu festzustellen, dass die gesetzlichen Vertreter immer die Verantwortung für die Inhalte und Aussagen der zu einem CMS gehörenden Dokumente tragen. Die gewählte Formulierung des IDW würde praktisch aber bedeuten, dass „die gesetzlichen Vertreter" nochmals separat Aussagen treffen müssten zum CMS, seinen Regeln und Zielen. Aus prüferischer Sicht ist dieser Wunsch nachzuvollziehen, da dies die Prüfungsdurchführung operativ erleichtert und die Prüfschritte scheinbar (!) objektiviert. Es würde aber lediglich den Fehler der formalistischen Herangehensweise aus der Prüfungsära in Sachen SOX 404 (Funktionsfähigkeit und Wirksamkeit des IKS) wiederholen. Dieser Formalismus bestand und besteht ja gerade darin, ein Kontrollziel zu formulieren, das Risiko zu beschreiben, das das Kontrollziel gefährdet und eine zugehörige Kontrollaktivität zu entwickeln. Wenn der Prüfer zu dem Urteil gelangt, dass das Risiko durch die Kontrollaktivität ausreichend mitigiert wird, ist das Kontrollziel erreicht. Dies führt dann praktisch z. B. im Bereich der Compliance-Schulung zu der Kuriosität, dass mit der richtigen Beantwortung der Frage des Prüfers, ob der Mitarbeiter 10.000 Euro zahlen würde, um einen Auftrag zu akquirieren (die richtige Antwort lautet im Übrigen „Nein"), das Risiko der Bestechungshandlung ausreichend mitigiert ist, damit das Kontrollziel des rechtskonformen Handelns im Vertriebsprozess erreicht ist: so geht es nicht!

Diese kausale Ableitung bringt den Prüfer insofern auf „die sichere Seite", weil diese so genannten „Control Sets" im Einvernehmen mit dem Mandanten entwickelt werden und so quasi eine allgemeine Akzeptanz über die Kausalität von Kontrollaktivität, Kontrollrisiko und Kontrollziel geschaffen wird. So wird überhaupt erst verständlich, warum „der Sicherheitsgrad festgelegt [wird], mit dem das CMS Regelverstöße verhindern soll." Diese Organisierung einer scheinbaren Sicherheit ist letztlich nur dem Umstand geschuldet, dass – wie bei SOX 404 – die *Wirksamkeit* des CMS bescheinigt werden können soll, die nach IDW EPS 980 dann gegeben ist, „wenn die Grundsätze und Maßnahmen von den hiervon Betroffenen nach Maßgabe ihrer Verantwortung zur Kenntnis genommen und bei der täglichen Arbeit *beachtet werden*. (Herv. d. V.)" Wenig überrascht, dass diese Definition von Wirksamkeit an anderer Stelle – realistischer Weise! – relativiert wird, wenn u.a. menschliche Fehlleistungen, Missbrauch oder Vernachlässigung der Verantwortung oder die Umgehung und Außerkraftsetzung von Kontrollen durch das Management als Gründe angeführt werden, die „ein ansonsten wirksam erscheinendes CMS" außer Gefecht setzen.

All diesen Problemen könnte man sich weitgehend entledigen, würde man den Anspruch an die Prüfungsaussage an die Möglichkeiten der CMS-Prüfung anpassen und nicht, wie im vorliegenden Fall, nachgerade anders herum vorgehen. Der o.g. CompliceProgramMonitor[ZfW] arbeitet daher auch mit einer entsprechend realistischeren Definition von Wirksamkeit, die dann gegeben ist, wenn das jeweilige Compliance-Instrument mindestens einmal in der Praxis angewendet wurde. Wirksamkeit bedeutet damit, dass die Umsetzung des CMS tatsächlich

erfolgt, nicht dass das CMS Fehlverhalten bzw. Straftaten verhindert. Auch hier versteigt sich der IDW EPS 980 zu der Aussage, dass ein CMS dann angemessen ist, „wenn es mit hinreichender Sicherheit [die definiert ist mit den o.g. Relativierungen!; Anm. d. .V.)] gewährleistet (sic!), dass Risiken für wesentliche Verstöße gegen die betreffenden Regeln rechtzeitig erkannt und Verstöße verhindert werden." Jeder, der die Praxis kennt, kann wissen, dass dies eine systematische Überforderung eines CMS darstellt.

Das CMS muss darauf ausgerichtet sein und geeignet sein, Verstöße aufzudecken und zu verhindern, mehr kann im Übrigen auch nicht geprüft werden, zumindest dann nicht, wenn man auf den eigentümlichen und im Übrigen kostentreibenden Dreischritt (s.o.) verzichten möchte.

Bisher sind in der Reihe der KICG-Forschungspapiere erschienen:

- Grüninger, S. „Compliance-Prüfung nach dem IDW EPS 980 – Pflicht oder Kür für den Aufsichtsrat?“ (KICG-Forschungspapier Nr. 1/2010)