Stellungnahme

zum Entwurf IDW Prüfungsstandard: Grundsätze ordnungsgemäßer Prüfung von Compliance Management Systemen (IDW EPS 980)

Gesamtverband der Deutschen Versicherungswirtschaft e. V.

Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel.: +49 30 2020-5413
Fax: +49 30 2020-6000

60, avenue de Cortenbergh
B - 1000 Brüssel
Tel.: +32 2 28247-30
Fax: +32 2 28247-39

Ansprechpartner:
K. Bartel
Recht

E-Mail: K.Bartel@gdv.de

www.gdv.de

Zusammenfassung

Der Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV) bedankt sich für die Möglichkeit, zu dem Entwurf des IDW Standards „Grundsätze ordnungsgemäßer Prüfung von Compliance Management Systemen (IDW EPS 980)“ Stellung nehmen zu können. Compliance-Systeme sind unternehmensindividuell zu erarbeiten und den jeweiligen Gegebenheiten des Unternehmens anzupassen. Es ist daher auch zu begrüßen, dass der IDW Entwurf den Unternehmen die Wahlfreiheit bei der Auswahl der von Compliance erfassten Themen und der dafür erforderlichen Elemente eines Compliance-Management-Systems (CMS) gibt. Es wäre aus unserer Sicht aber wünschenswert, wenn noch deutlicher werden könnte, dass es keine gesetzlichen oder regulatorischen Vorgaben über die Organisationsform bzw. die konkreten Prozessabläufe der Compliance-Funktion gibt und die Anforderungen an die organisatorischen Maßnahmen wesentlich von der Größe sowie Art und Umfang der Geschäftstätigkeit abhängen.

Unabhängig hiervon bestehen zu einzelnen Punkten des Entwurfs noch Anmerkungen des GDV. So sollte insbesondere die Definition von Compliance bzw. Compliance Management den Vorgaben des Deutschen Corporate Governance Kodex angeglichen werden.

A. Einleitung

Wie in allen Wirtschaftszweigen gewinnt auch für die Versicherungswirtschaft das Thema Compliance zunehmend an Bedeutung. Mit Umsetzung der EU-Richtlinie 2009/138/EG (sog. Solvency II-Richtlinien) wird es für die Versicherungsunternehmen weitere rechtliche Konkretisierungen für Compliance geben.[1]

Unabhängig hiervon gibt es aber weder im Gesellschafts- noch im Aufsichtsrecht bisher gesetzliche oder regulatorische Vorgaben über die Organisationsform bzw. die konkreten Prozessabläufe der Compliance-Funktion. Der Gesetzgeber hat vielmehr bisher bewusst keinerlei Vorgaben zu konkreten Anforderungen an die Compliance Funktion oder zu deren organisatorischen Ausgestaltung im Rahmen des CMS aufgestellt. Selbst in den Bereichen, in denen der Gesetzgeber - wie z. B. in der Versicherungswirtschaft - weitergehende (aufsichtsrechtliche) Anforderungen normiert hat, beziehen sich diese ausschließlich auf die Compliance Funktion. Auch die spezialgesetzlichen Regelungen räumen den Unternehmen aber bewusst eine breite Gestaltungsfreiheit ein, wie die Compliance Funktion im Unternehmen umzusetzen ist. Dies ermöglicht es den Unternehmen, die jeweiligen Besonderheiten ihrer Unternehmen berücksichtigen zu können und "maßgeschneiderte Systeme" für die einzelnen Unternehmen einzurichten. Aus unserer Sicht besteht die Gefahr, dass diese gesetzgeberische Grundwertung durch die detaillierten Vorgaben des IDW Standards zu den Bestandteilen eines CMS in Frage gestellt werden könnte. Aus Sicht des GDV wäre es daher wünschenswert, wenn in dem Entwurf deutlicher als bisher werden könnte, dass es keine allgemein gültigen Vorgaben über die Organisationsform bzw. die konkreten Prozessabläufe der Compliance-Funktion gibt.

B. Einzelheiten

Dies vorausgeschickt bestehen folgende Anmerkungen zu den einzelnen Textstellen des Entwurfs:

Tz. 1

Ein Compliance Managementsystem (CMS) wird in Tz. 1 als Teilbereich des Risikomanagements definiert. Diese Definition ist so nicht zutreffend.

[1] vgl. Leitfaden des GDV „Compliance im Erst- und Rückversicherungsunternehmen“, abrufbar unter http://www.gdv.de/Themen/Vertrieb_Recht/Recht_Regulierung/inhaltsseite25721.html.

Sie steht vielmehr etwa den Vorgaben entgegen, die zukünftig für die Versicherungswirtschaft gelten werden. Compliance ist danach kein Teil des Risikomanagements, sondern neben dem Risikomanagement ein Teil des Governance-Systems. Innerhalb dieses Governance-Systems ist Compliance wiederum Teil des Internen Kontrollsystems (IKS), vgl. Art. 46 Abs.1 der Richtlinie 2009/138/EG.

Tz. 5

Laut Tz. 5 ist „unter dem Begriff Compliance allgemein die Einhaltung von Regeln zu verstehen, z. B. Gesetze, vertragliche Verpflichtungen und interne Regelungen oder neue Richtlinien." Diese Definition steht im Widerspruch zu der Definition im Deutschen Corporate Governance Kodex (DCGK). Danach umfasst der Begriff der Compliance die Einhaltung der gesetzlichen Bestimmungen und der unternehmensindividuellen Richtlinien. Im Sinne einer auch gesellschaftsrechtlich konsistenten Terminologie sollte dem IDW EPS 980 der DCGK-Begriff zugrunde gelegt werden.

In jedem Fall sollte die Einbeziehung von vertraglichen Verpflichtungen aus der Begriffsbestimmung gestrichen werden, da dies zu weitgehend ist. Im Rahmen der Compliance geht es vielmehr um die Einhaltung der unternehmensindividuellen Richtlinien, mit denen eine korrekte Vertragsabwicklung sichergestellt wird. Die Einhaltung der vertraglichen Verpflichtungen ist dagegen Sache der jeweiligen Vertragspartner. Darüber hinaus sollte auch der Teil der Regeln, den die Unternehmen im Wege der Selbstverpflichtung übernehmen (Corporate Social Responsibility), nicht vom Compliance-Management erfasst werden. Auch dies würde der Definition von Compliance im DCGK widersprechen.

Tz. 8 und A26

In diesen Tz. wird festgelegt, was unter CMS-Grundsätzen zu verstehen ist. CMS-Grundsätze sind danach allgemein anerkannte Rahmenkonzepte, andere angemessene Rahmenkonzepte oder vom Unternehmen selbst entwickelte Grundsätze. Damit werden zutreffend auch die von Unternehmen selbst entwickelten Grundsätze im Rahmen des IDW EPS 980 anerkannt. Wie oben ausgeführt, wäre es aber zu begrüßen, wenn hier noch deutlicher werden könnte, dass es allgemeingültige CMS-Grundsätze nicht gibt, sondern diese jeweils von den Gegebenheiten der einzelnen Unternehmen abhängen.

Tz. 6 und A9

Der Kreis der Betroffenen eines CMS „muss“ laut Tz. A9 nicht auf die vom Unternehmen beschäftigten Mitarbeiter begrenzt sein, sondern kann ggf. auch Dritte einbeziehen. Aus den bereits oben dargelegten Gründen (kein CMS für Corporate-Responsibility-Themen) erscheint es nicht gerechtfertigt, mit dem System auch Dritte, die dem Unternehmen nicht angehören und lediglich z. B. Kunde oder Zulieferer sind, erfassen zu wollen. Management-Systeme stoßen dort an ihre Grenzen, wo es an den Kontrollmöglichkeiten, wie gegenüber Dritten, fehlt. Dies hat nichts mehr mit Corporate Governance oder Compliance in dem Sinne des DCGK zu tun. Daher sollten in Tz. 6 „ggf. von Dritten“ und in Tz. A9 die letzten beiden Sätze gestrichen werden.

Tz. 14b, 14c, 16, 41 und A22

An verschiedenen Stellen im Entwurf wird auf die Eignung eines CMS zur Verhinderung von Verstößen Bezug genommen, vgl. Tz. 14b, 14c, 16 und 41. Laut Tz. 16 soll ein CMS angemessen sein, wenn es mit hinreichender Sicherheit gewährleistet, dass nicht nur Risiken für wesentliche Verstöße erkannt, sondern auch Verstöße verhindert werden. Es ist aber zu bezweifeln, dass mit der gleichen hinreichenden Sicherheit, wie Risiken erkannt werden können, die Verhinderung von Verstößen tatsächlich gewährleistet werden kann. Hier sind schon operationell Grenzen gesetzt, da etwa mit Blick auf den Datenschutz nicht jedes Mittel zur Verhinderung von Verstößen eingesetzt werden darf. Richtigerweise kann daher nur erwartet werden, dass das CMS das Ziel verfolgt, aufbauend auf der Risikoerkennung soweit als möglich Verstöße zu vermeiden.

Dies ergibt sich im Übrigen so auch aus Tz. A14, dritter Absatz. Dort heißt es, dass die Verhinderung von Regelverstößen „auch das rechtzeitige Erkennen von Risiken für Compliance-Verstöße und die Reaktionen auf die erkannten Risiken“ umfasse. Systematisch ist also die Verhinderung von Verstößen der Überbegriff; das rechtzeitige Erkennen von Risiken sowie die *angemessene* Reaktion auf die erkannten Risiken sind dahingegen konkrete Maßnahmen zur Prävention. Daher regen wir folgende Änderung in Tz. 16 an (Änderungen **fett**):

> *„Ein CMS ist angemessen, wenn es **zur Verhinderung von Verstößen** mit hinreichender Sicherheit gewährleistet, dass Risiken…... rechtzeitig erkannt **werden und auf die erkannten Risiken in angemessener Weise reagiert wird**.“*

Die anderen o. g. Tz. sollten analog angepasst werden.

Tz. A2
Unter A2 werden (beispielhaft) Bereiche genannt, die Gegenstand einer CMS-Prüfung sein können. Genannt wird dabei u. a. „Vorschriften zur Unternehmensführung und -überwachung (z. B. nach dem Deutschen Corporate Governance Kodex)“. Dies ist aus unserer Sicht kritisch zu beurteilen, weil sich die Frage stellt, ob die gesellschaftsrechtliche Corporate Governance (z. B. ordnungsgemäße Besetzung des Vorstandes und des Aufsichtsrates) tatsächlich einen abgegrenzten Teilbereich darstellt, der Gegenstand einer eigenständigen CMS-Prüfung sein kann. Außerdem sehen wir über die Entsprechenserklärung gem. § 161 AktG hinaus keinen weiteren Bedarf für zusätzliche Compliance-Maßnahmen. Die Kontrolle der DCGK-„Compliance“ zudem dürfte eher eine Frage der internen Kontrollen als die eines Compliance-Managements sein.

Auf der anderen Seite fehlt im Rahmen der Aufzählung derzeit noch das Aufsichtsrecht, und zwar sowohl das Banken- als auch das Versicherungsaufsichtsrecht. Für die beaufsichtigten Unternehmen sind dies sehr relevante Compliance-Bereiche, das erwähnte Geldwäschegesetz ist demgegenüber wiederum nur ein Teilausschnitt.

Tz. A6
Der Entwurf spricht in Satz 2 unter Tz. A6 von „Festlegung von Compliance-Risiken.“ Hierbei dürfte es sich aus unserer Sicht möglicherweise um ein Redaktionsversehen handeln, weil vermutlich die „Feststellung“ von Risiken gemeint ist.

Tz. A12
Der Begriff " Compliance Ziele" ist unklar und daher irreführend: Das Compliance Ziel ist in allen Unternehmensbereichen ein und dasselbe, nämlich die Einhaltung aller in dem betroffenen Bereich geltenden Regeln. Weshalb und in welcher Form zu diesem Ziel noch separate "Compliance Unterziele" festgelegt werden sollen, ist nicht nachvollziehbar, zumal diese schwer von den ohnehin zu definierenden Compliance-Maßnahmen und Compliance-Programmen abgegrenzt werden können.

Gem. Tz. 12 soll zudem ein „Sicherheitsgrad“ festgelegt werden, mit dem das CMS Regelverstöße verhindern soll. Aus unserer Sicht kann es, wie in Tz. 16 beschrieben, nur um eine „hinreichende“ Vermeidung von Verstößen gehen. Es ist nicht praktikabel, hierüber hinausgehend stets quantitative Sicherheitsziele zu definieren. Es sollte daher darauf verzichtet

werden, die Festlegung entsprechender „Sicherheitsgrade“ zu verlangen. Zumindest sollte deutlich werden, dass eine Quantifizierung der Ziele nicht erforderlich ist.

Berlin, den 30.09.2010