Compliance im Mittelstand: Die Rolle des Aufsichtsrats

Meinhard Remberg*

Obwohl im Mittelstand auch in risikobehafteten Branchen das Compliance Management häufig nicht so ausgeprägt ist wie in Groß-, insbesondere in DAX-Unternehmen, hat der (Pflicht-)Aufsichtsrat hier die gleichen Überwachungsaufgaben wahrzunehmen. Hierzu muss er sich mit den „Compliance-Besonderheiten" des jeweiligen mittelständischen Unternehmens auseinandersetzen, die Risikoanalyse einer Prüfung unterziehen und dann vor allem den offenen Dialog mit der Unternehmensführung suchen.

I. Begriff Mittelstand

Bei dem Begriff bzw. dem Phänomen Mittelstand handelt es sich um eine deutsche Besonderheit. In keinem anderen europäischen Land spielen die kleinen und mittelgroßen Unternehmen eine derartige Rolle wie in Deutschland. Einerseits sind sie ein Synonym für die wirtschaftliche Leistungsfähigkeit und die Innovationskraft der deutschen Wirtschaft; andererseits finden sie Beachtung durch eine Vielzahl von Gruppen und Verbänden, die sich ihrer speziellen Interessen annehmen. Beispielhaft seien hier nur die Stiftung Familienunternehmen und das Institut für Mittelstandsforschung genannt.

Eine einheitliche Definition für den Begriff Mittelstand liegt nicht vor. Den folgenden Ausführungen wird der Mittelstandsbegriff des Deutschen Instituts für Compliance (DICO) zugrunde gelegt. Hiernach ist ein Unternehmen einerseits dem Mittelstand zuzurechnen, wenn es bis zu 3.000 Mitarbeiter hat oder einen Umsatz bis zu 600 Mio. Euro realisiert. Andererseits kann aber auch das qualitative Merkmal herangezogen werden, demzufolge es sich um ein mittelständisches Unternehmen handelt, wenn Eigentum, Leitung, Haftung und Risiko in einer Hand liegen. Dies ist typischerweise bei den Familienunternehmen der Fall. Es ist offensichtlich, dass bei Zugrundelegung der angeführten Definition in vielen Fällen ein Aufsichtsrat zwingend vorgeschrieben ist.

II. Verantwortung

Welche Verantwortung kommt nun auf diesen Aufsichtsrat im Hinblick auf das Thema Compliance zu und welchen „Mittelstands-Besonderheiten" begegnet er hierbei? Die Etablierung eines funktionierenden Compliance-Management-Systems (CMS) ist eine originäre Aufgabe des Vorstands bzw. der Geschäftsführung. Der Aufsichtsrat muss überwachen, ob dies ordnungsgemäß erfolgt ist und dabei insbesondere auf Konzeption, Angemessenheit und Wirksamkeit des CMS achten. Er muss Maßnahmen ergreifen, falls Schwächen festgestellt werden.

Verschiedene Studien zum Thema Compliance im Mittelstand und auch die Erfahrungen, die in den Verbänden gesammelt werden, zeigen, dass die Compliance-Strukturen im Mittelstand in der Regel nicht mit denen der DAX-Unternehmen vergleichbar sind. Während insbesondere DAX-Unternehmen nicht zuletzt auch vor dem Hintergrund bekannt gewordener „Compliance-Unfälle" sowie des immer größer werdenden Drucks der Öffentlichkeit und hier vor allem der Medien ausgefeilte und somit personal- und damit auch kostenintensive CMS aufgebaut haben, lässt sich dies für die mittleren und größeren Mittelständler eher nicht behaupten. Häufig mangelt es dort bereits an einer professionell durchgeführten und dokumentierten Risikoanalyse. Es fehlt hier manchmal an einer gelebten Unternehmenskultur, die es ermöglicht, die Risiken des Unternehmens offen und ehrlich anzusprechen. Verständlich ist dies insbesondere deshalb, da mit dem Benennen der Problembereiche – zum Beispiel der Korruption im Vertrieb – häufig eine gravierende Verhaltensänderung einhergehen muss.

Anders als die DAX-Unternehmen neigen mittelständische Unternehmen häufig zu Einzelfalllösungen und nicht zu der Etablierung institutionalisierter Vorgehensweisen. Auch ist der Weg von der Erkenntnis – aufgrund konkret identifizierter Risiken etwas tun zu müssen – bis zum konkreten Handeln manchmal sehr lang. Compliance-Maßnahmen werden schließlich vor allem aus Angst – vor Strafen und Reputationsverlust – und weniger aus Überzeugung ergriffen. Schließlich unterliegen Mittelständler oft auch sehr großem Wettbewerbsdruck, der dazu führt, dass viele Entscheidungen unter Kostengesichtspunkten gefällt werden; dem Einsatz teurer externer Berater steht man eher kritisch gegenüber. Nicht selten fehlt es an unterstützenden Einrichtungen wie einer Internen Revision oder einem Risikomanagementsystem; gerade Letzteres ist oft nur fragmentarisch entwickelt.

III. Handlungspflichten

Wie sieht nun vor diesem Hintergrund die konkrete Überwachungspflicht des Aufsichtsrats aus und wer kann ihn dabei

unterstützen, das CMS zu überwachen? Der Aufsichtsrat muss sich zunächst mit den Kriterien für ein ordnungsgemäßes bzw. angemessenes CMS beschäftigen. Leider kann er sich hierbei nicht an einem allgemeingültigen, in allen Unternehmen praktisch umsetzbaren Mindeststandard orientieren. Wertvolle Hilfestellungen geben jedoch der IDW-Prüfungsstandard „Grundsätze ordnungsmäßiger Prüfung von Compliance-Management-Systemen", der Standard für Compliance-Management-Systeme des TÜV Rheinland sowie der Ende 2014 veröffentlichte ISO Standard 19600 für Compliance-Management-Systeme. Gerade Mittelständler sind jedoch häufig mit den hier vorgefundenen Anforderungen überfordert bzw. finden ihre Unternehmensrealität nicht hinreichend berücksichtigt. Nicht nur in der mittelständischen Praxis haben sich folgende Grundelemente eines effektiven CMS herauskristallisiert, von deren Existenz sich der Aufsichtsrat ggf. durch aktives Nachfragen überzeugen sollte:

» Kontrolliert der Aufsichtsrat das Compliance-Management-System oder unterliegt er einer Illusion? «

- Sorgfältige Auswahl eines „Kümmerers" – in größeren Unternehmen auch Compliance Officer genannt –, der sich des Themas Compliance im Unternehmen annimmt. Hier ist auf ausreichende Kenntnisse, Befugnisse und eine professionelle Berichtslinie zu achten.
- Regelmäßige Feststellung und Bewertung der mit der Geschäftstätigkeit einhergehenden rechtlichen Risiken (Risikoanalyse).
- Schulung von Mitarbeitern zwecks Verhinderung von Straftaten oder Ordnungswidrigkeiten; geeignete Kommunikation in Form von Richtlinien und Anweisungen.
- Professionelle Verfolgung von anonymen und nichtanonymen Hinweisen.
- Systematische Aufklärung von Verdachtshinweisen sowie konsequente Ahndung von Fehlverhalten.

Dabei ist darauf zu achten, dass die Maßnahmen in einem angemessenen Verhältnis zur Größe des Unternehmens und zu den Erkenntnissen der jedem CMS zugrunde liegenden Risikoanalyse stehen müssen. Sollte der Aufsichtsrat Zweifel an der Existenz, Angemessenheit oder Wirksamkeit des CMS hegen und lassen sich diese auch nach Gesprächen mit der Unternehmensführung nicht ausräumen, ist es empfehlenswert, eine externe Prüfung des CMS zu veranlassen. Dies muss nicht zwingend eine Prüfung nach dem o.g. IDW-Prüfungsstandard sein; oft ist es ratsam, zunächst einen beratenden Ansatz zu wählen, um mit dem externen Prüfer das CMS zu entwickeln oder zu verbessern.

Grundsätzlich sollte der Aufsichtsrat seine Überwachungstätigkeit jedoch zunächst an dem Bericht des Vorstands bzw. der Geschäftsführung ausrichten. Dieser erfolgt normalerweise im Rahmen der turnusmäßigen Aufsichtsratssitzungen, die in der Regel viermal im Jahr stattfinden. Wesentliche Schwerpunkte der Aufsichtsratssitzungen sind die Erläuterung der Geschäftslage sowie strategischer Themen. Compliance rückt gerade im Mittelstand eher dann auf die Tagesordnung, wenn es einen „Compliance-Unfall" gegeben hat, weniger um auf der Grundlage der dem Aufsichtsrat häufig nicht bekannten Risikoanalyse Präventivmaßnahmen zu diskutieren. Bei der Berichterstattung des Vorstands an den Aufsichtsrat wird immer wieder auch die Vertrauenskultur im Unternehmen und den Gremien zitiert. Nicht nur die Presseberichte zu den Compliance-Verstößen in der jüngsten Vergangenheit zeigen, dass Vertrauenswürdigkeit veränderlich und immer abhängig vom Kontext ist. Über die Berichte der Unternehmensleitung hinaus kann sich der Aufsichtsrat bei seiner Überwachungsaufgabe auch auf Berichte ggf. der Wirtschaftsprüfer oder der Internen Revision stützen.

Nachdenklich sollte ein Aufsichtsrat werden, wenn ihm auf der Basis glattpolierter PowerPoint-Präsentationen suggeriert wird, dass man die branchentypischen Risiken aufgrund etablierter Compliance-Maßnahmen jederzeit im Griff habe oder behauptet wird, zukünftige Verfehlungen ausschließen zu können. Selbst das beste CMS kann Compliance-Verstöße nicht ausschließen. Entscheidend ist, dass das Unternehmen alles getan hat, um diese zu verhindern. Die Compliance-Berichterstattung des Vorstands ist häufig gerade dann glaubwürdig, wenn deutlich gemacht wird, dass viele Compliance-Themen Fähigkeiten hinsichtlich des Handelns in Grauzonen und in Dilemma-Situationen verlangen. Offene Fragen und auch Widersprüche können hier das Kennzeichen dafür sein, dass jemand von der Wirklichkeit spricht. Hinterfragen sollte der Aufsichtsrat auch die häufig üblichen Compliance-Schulungen. Die Verbreitung juristischer Erkenntnisse per PowerPoint oder E-Mail bedeutet nicht zwingend, dass Menschen die Botschaft auch verstanden haben und ihr Verhalten ändern. Die entscheidende Frage lautet: Woran können Unternehmensleitung und Aufsichtsrat erkennen, dass die Verankerung der kommunizierten Verhaltensregeln in den betrieblichen Alltag tatsächlich gelungen ist? Man stellt dann fest, dass sich beim Thema Compliance nicht alles mit den üblichen „Tools" – Richtlinien, Hinweisgebersystem, Schulungen etc. – „managen" lässt. Was wirklich bei den Mitarbeitern ankommt und überzeugend zu Verhaltensänderungen führt, ist vor allem abhängig von der Unternehmenskultur und der glaubwürdigen Vorbildfunktion der Unternehmensleitung und der Führungskräfte auf der mittleren Ebene.

IV. Aktives Compliance Management

In jedem Fall empfiehlt es sich, dass der Aufsichtsrat, bevor er sich mit der Überwachung des CMS beschäftigt, mit dem Vorstand die zugrunde liegende Risikoanalyse diskutiert. Der Aufsichtsrat sollte sich auch davon überzeugen, dass das CMS nicht nur im deutschen Stammhaus etabliert wurde, sondern in sämtlichen relevanten in- und ausländischen Tochtergesellschaften: Umsetzungslücken können hier erhebliche Konsequenzen haben. Abschließend bleibt festzuhalten, dass nicht zuletzt vor dem Hintergrund der deutlich ausgeweiteten Haftung die Überwachung der Compliance-Aktivitäten eines Unternehmens durch den Aufsichtsrat nicht zu unterschätzen ist. Es ist daher notwendig, dass der Aufsichtsrat bzw. einzelne Aufsichtsratsmitglieder über hinreichende Kenntnisse verfügen, ihre Rolle aktiv wahrnehmen und sich nicht einer Illusion von Kontrolle hingeben. So lautet eine Standardfrage bei Compliance-Verstößen immer häufiger: Hätte dies der Aufsichtsrat erkennen können?

* *Dipl.-Kfm. Meinhard Remberg, Generalbevollmächtigter der SMS GmbH; seit 2013 Vorstandsmitglied des Deutschen Instituts für Compliance e.V. (DICO); Mitherausgeber der CCZ.*