

**Entwurf des IDW Prüfungsstandard „Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen“**

Sehr geehrte Damen und Herren,

zu dem von Ihnen jüngst veröffentlichten Entwurf des o. a. Prüfungsstandard möchte ich auf Folgendes hinweisen:

1. Die deutschen Unternehmen richten sich bei Ihren Compliance-Programmen regelmäßig an der Compliance-Definition des deutschen Corporate Governance Kodex aus. Danach ist Compliance die Sorge um die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien. Es wäre sinnvoll, wenn sich der Prüfungsstandard hieran anschließen könnte und nicht – wie etwa in Tz 1 und 5 – vage von „Regeln“ sprechen würde.
2. Hinzu kommt, dass in Tz 5 als Beispiele für „Regeln“ genannt sind „Gesetze, vertragliche Verpflichtungen und interne Regelungen oder Richtlinien“. Die Beispielhaftigkeit dieser Aufzählung lässt offen, was sonst noch nach dem Standard unter „Regeln“ zu verstehen ist. Im Übrigen sind vertragliche Verpflichtungen schon dem Begriff nach keine Regeln. Die Ausdehnung von Compliance auf die Überprüfung der Einhaltung vertraglicher Bestimmungen würde zudem jeden Rahmen sprengen. Es geht vielmehr um die Überprüfung der Einhaltung der unternehmensinternen Richtlinien, mit denen eine korrekte Vertragsabwicklung sichergestellt wird (organisatorische Zuweisungen, Führung eines Fristenbuchs etc.). Die Sorge um die Einhaltung der Vertragsverpflichtungen selbst kann getrost den Vertragspartnern überlassen bleiben.
3. In Tz 7 definieren Sie die „Aussagen der gesetzlichen Vertreter“ zu wesentlichen Teilen der CMS-Beschreibung. Es klingt dann etwas merkwürdig, wenn Sie in Tz 13 die

Verantwortung für die CMS-Beschreibung nochmals ausdrücklich den gesetzlichen Vertretern des Unternehmens auferlegen. Wer sonst als sie selbst sollte für ihre Aussagen verantwortlich sein?!

Die Verantwortung der gesetzlichen Vertreter ist zwar richtig, von ihnen konkrete Aussagen abzufordern, erscheint dagegen überzogen. Die Regel ist vielmehr, dass auf Weisung der gesetzlichen Vertreter im Unternehmen ein CMS erarbeitet und umgesetzt wird, wobei die gesetzlichen Vertreter die „Initialzündung“ setzen (Tone from the Top). Diese enthält aber kaum die von Ihnen erwarteten detaillierten „Aussagen der gesetzlichen Vertreter“.

Nach Tz 7 gehören zu den Aussagen der gesetzlichen Vertreter „Erklärungen zur Konzeption“ des CMS, zu den Grundelementen des CMS sowie zur Angemessenheit, Implementierung und Wirksamkeit des CMS. Zur Konzeption des CMS nach Tz 10 gehören aber bereits die Festlegung der Compliance-Ziele, der Aufbau der Compliance-Organisation, der Prozess der Feststellung und Analyse der Compliance-Risiken, der Prozess der Erstellung des Compliance-Programms, Verfahren zur Überwachung und Verbesserung des Compliance-Programms und ähnliches. All dies sind Grundelemente des CMS bzw. betreffen die Angemessenheit, Implementierung und Wirksamkeit des CMS. Dies in Tz 7 neben der Erklärung zur Konzeption des CMS nochmals gesondert zu verlangen ist „doppelt gemoppelt“. Tz 7 und die wiederholten Hinweise auf die „Aussagen der gesetzlichen Vertreter“ im Entwurf sollten deshalb entfallen.

4. Dies würde auch Tz 11 wesentlich vereinfachen, wonach die CMS-Beschreibung Aussagen der gesetzlichen Vertreter zu Art, Umfang und Zeitpunkt der Konzeption beinhaltet. Der Satz könnte, wenn Tz 7 gestrichen wird, ebenfalls entfallen. Im Übrigen ist unerfindlich, warum hier die Aussagen der gesetzlichen Vertreter speziell zu „Art, Umfang und Zeitpunkt“ der Konzeption verlangt werden, während die (bislang vorgesehene) Definition dieser Aussagen in Tz 7 hierauf nicht eingeht, sondern nur „Erklärungen zur Konzeption“ verlangt.
5. Auch Tz 14 a – c könnten durch die Streichung von Tz 7 und die „Aussagen der gesetzlichen Vertreter“ wesentlich vereinfacht werden. Tatsächlich geht es auch hier nicht um die Aussagen der gesetzlichen Vertreter, sondern um die Prüfung, ob die CMS-Beschreibung zutrifft.

6. In Tz 14 b und c beschreiben Sie u. a. als Ziel der CMS-Prüfung festzustellen, ob die angewandten CMS-Grundsätze „geeignet (sind), ... Verstöße zu verhindern ...“. Dies entspricht Tz 65 j. Dagegen formulieren Sie in Tz 19 (Compliance Programm) weicher, dass das Programm „auf die Vermeidung von Compliance-Verstößen ausgerichtet“ sein soll. Nach Tz 16 ist allerdings ein CMS nur angemessen, „wenn ... Verstöße verhindert werden“. Entsprechend formulieren Sie in Tz 41. Abgesehen davon, dass die von Ihnen gewählten Formulierungen inhaltlich beachtliche Abweichungen aufweisen, geht es an der Wirklichkeit vorbei, von einem CMS die generelle Verhinderung von Verstößen zu erwarten. Entsprechend ist ein solches Programm auch niemals wirklich geeignet, Verstöße zu verhindern. Was erwartet werden kann ist, dass das Programm das Ziel verfolgt, Verstöße zurückzudrängen und hierfür die richtigen Mittel einzusetzen. Ich schlage deshalb vor, in dem Entwurf grundsätzlich den von Ihnen in Tz 19 verwendeten Textbaustein zu vermeiden, dass das Compliance Programm auf die Vermeidung von Compliance-Verstößen ausgerichtet sein muss.
7. Nach Tz 19 (Compliance-Ziele) legen die gesetzlichen Vertreter (richtiger: das Unternehmen) die Ziele fest, die mit dem CMS erreicht werden sollen. Weiter heißt es, „dies umfasst insbesondere die Festlegung der relevanten Teilbereiche und der in den einzelnen Teilbereichen einzuhaltenden Regeln“. Auf Grundlage der Compliance-Definition des DCGK ist Compliance unteilbar und umfasst generell die Einhaltung der Gesetze und unternehmensinternen Richtlinien. Eine Segmentierung in Teilbereiche und eine besondere Festlegung der in einzelnen Teilbereichen gültigen Regeln setzt sich mit dieser Allgemeindefinition in Widerspruch und sollte deshalb entfallen. Dies schließt nicht aus, die Prüfung des CMS auf Teilbereiche zu beschränken. Möglich erscheint auch bei der Beschreibung der Compliance-Ziele besondere Risiko-Felder und hierfür vorgesehene besondere Sicherungsmaßnahmen zusätzlich hervorzuheben.
8. Nach Tz 19 (Compliance-Risiken) ist ein Verfahren zur systematischen Risiko-Erkennung und Risikoberichterstattung einzuführen. In den meisten Unternehmen liegt ein solches Verfahren bereits im Rahmen des allgemeinen Risk Management vor. Für die Aktiengesellschaften ist dies mittlerweile vorgeschrieben. Hierin werden regelmäßig auch Compliance-Risiken erfasst. Ein gesondertes Verfahren zur Erkennung von und Berichterstattung über Compliance-Risiken erscheint daneben nicht erforderlich.
9. Nach Tz 38 hat der CMS-Prüfer beim Auftragsstyp 1 zu beurteilen „ob die Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung ... zutreffend sind“. Nach Tz 14 a geht es allerdings vielmehr darum zu prüfen, ob die Aussagen der gesetzlichen Vertreter in

Seite 4

der CMS-Beschreibung „zutreffend dargestellt“ sind. Das ist durchaus ein Unterschied. Verbleibt es beim Wortlaut der Tz 38 wäre zu klären, was denn den Vergleichsmaßstab bildet um festzustellen, ob die Aussagen zutreffen oder nicht.

10. Bezüglich der Tz 40 - 43 sollte klargestellt werden, welche der dort dargestellten Prüfungshandlungen nur für Auftragsstyp 3 und welche auch für Auftragsstyp 2 einschlägig sind.
11. Nach Tz 44 liegt es in der Verantwortung der gesetzlichen Vertreter (besser: des Unternehmens) zu untersuchen, welche Umstände zu dem Verstoß geführt haben und warum das CMS den Verstoß nicht verhindert hat. Ersteres ist sicher richtig, Letzteres ist dagegen nachrangig zu der umfassenderen Frage, wie das CMS besser darauf ausgerichtet werden kann, zukünftig entsprechende Verstöße zu verhindern. Erste Pflicht des Unternehmens dürfte im Übrigen sein, den Verstoß, sofern er noch fort dauert, zu unterbinden.

Mit freundlichen Grüßen

Sünner