

Funktionen der internen Revision im CMS sind noch zu definieren

Die Rolle der internen Revision im Compliance Management System

| von Matthias Schenkel und Jochen Ball |

Compliance Management Systeme „CMS“ sind dem Grunde nach nichts Neues, allerdings gewinnen sie mit Recht immer mehr an Bedeutung. Dies liegt zum einen an der gestiegenen Sensibilität im Zusammenhang mit der Unternehmensreputation und zum anderen an den nun durch Gesetz und Rechtsprechung konkreter gewordenen Anforderungen. Dass sich die interne Revision hier mehr oder weniger selbst als die Verantwortliche ins Spiel bringt ist vordergründig verständlich, trifft die Sache aber nur bedingt. Vielmehr ist es von zentraler Bedeutung, dass sich die Unternehmensführer ihrer Verantwortung selbst bewusst werden, um dann unter Hinzuziehung zum Beispiel der internen Revision ihrer Aufgabe – der verantwortungsvollen und sorgfältigen Unternehmensführung – gerecht zu werden.

Aufgaben des CMS

CMS sind grundsätzlich Systeme, die gewährleisten sollen, dass die für ein Unternehmen relevanten gesetzlichen und ggf. unternehmensindividuellen Regeln eingehalten werden. Auch die *Corporate Governance* – im Sinne von guter Unternehmensführung – spielt hierbei eine Rolle; denn die Anwendung des Corporate Governance Kodex für die Geschäftsführung eines Unternehmens kann abgesehen von finanzwirtschaftlichen und strategischen Gründen auch deshalb empfehlenswert sein, weil sich durch dessen Beachtung die *Unternehmensleitung* und *-kontrolle*, die *Krisenprävention* und seine *Exkulpationsmöglichkeiten* verbessern lassen. „Compliance ist Bestandteil des strategischen und operativen Managements und zielt auf die nachhaltige, legale, ökonomische und gesellschaftliche Sicherung der Existenz und der Zielerreichung einer Organisation“ (IDW EPS 980) ab.

Folgt man dieser Zielsetzung von Compliance, wird deutlich, dass die Aufgaben eines CMS weit über eine rein rechtliche oder prozessorientierte Betrachtung hinaus gehen. Das Management von Compliance ist mehr als das Her- und Sicherstellen von regelkonformen Verhalten und ist daher sicher nicht „nur“ Ergebnis der Arbeit der Rechtsabteilung, des Compliance Officers oder der *internen Revi-*

sion, sondern *integraler Bestandteil der Geschäftsführung*. Es bedarf einer im Organisationsermessen der gesetzlichen Vertreter liegenden entsprechenden Koordination bei der Entwicklung, Ausgestaltung und Überwachung des CMS.

Der Vollständigkeit halber sei ausdrücklich darauf hingewiesen, dass „ein ggf. vorhandenes Aufsichtsorgan über die Maßnahmen zur Überwachung und Verbesserung des CMS informiert werden sollte, soweit es der Erfüllung der eigenen Überwachungsfunktion des Aufsichtsorgans dient, z.B. § 107 Abs. 3 AktG“ (IDW PS 980, S. 217, A 20). Die Kenntnis darüber allein reicht allerdings nicht aus, um die eigenen Überwachungsaufgaben des Aufsichtsorgans insgesamt als erfüllt anzusehen.

Bestandteile eines CMS

Das IDW *Institut der Wirtschaftsprüfer* hat im Prüfungsstandard PS 980 dezidierte Angaben über die Bestandteile eines CMS gemacht. Danach sind wesentliche Bestandteile einer CMS-Beschreibung nachfolgende Grundelemente:

1. **Compliance Kultur**
Verhalten des Managements
2. **Compliance Ziele**
Regelranking in Abhängigkeit von Unternehmensanalyse und-zielen
3. **Compliance Organisation**
Aufbau- und Ablauforganisation
4. **Compliance Risiken**
Verfahren zur systematischen Risikoerkennung und –berichterstattung
5. **Compliance Programm**
Grundsätze und Maßnahmen zur Risiken- und Verstoßvermeidung
6. **Compliance Kommunikation**
Nutzungskonzept und Hinweisgebersystem
7. **Compliance Überwachung und Verbesserung**
Eskalationsbeschreibung

Ausgangspunkt für diesen Prüfungsstandard war die von der Praxis an das Institut herangetragene Bitte den Berufsstand der Wirtschaftsprüfer für die Prüfung derartiger Systeme zu sensibilisieren und einen Maßstab an die Hand zu geben, anhand dieser eine Beurteilung des CMS möglich ist. Die Prüfung eines CMS kann gemäß IDW PS 980 je nach Zielsetzung als Konzeptions-, Angemessenheits- oder Wirksamkeitsprüfung ausgestaltet sein.

Naturgemäß sehen sich die *internen Revisoren* als diejenigen, welche zur *Prüfung* eines CMS prädestiniert sind, so zumindest der Sprecher des Vorstandes des Deutschen Instituts für Interne Revision e.V. (DIIR), Herr Bernd Schartmann. Diese hätte ganz und gar „...die Verantwortung, diese Systeme auf ihre Angemessenheit und Funktionsfähigkeit zu überprüfen“. Dies ist umso erstaunlicher, als der BGH die strafrechtliche Haftung der CO Compliance Officer betont hat, Urteil vom 17.07.2009 – Az.: 9 StR 394/08. Im entschiedenen Fall war der Angeklagte kein CO, sondern Leiter der internen Revision, der sich dem Vorwurf der Beihilfe zum Betrug gegenüber sah. Das Gericht nahm auch für ihn eine sogenannte Garantstellung im Sinne des § 13 StGB an, welche eine besondere Verpflichtung dahin gehend begründet, dass ein aktives Tun zur Verhinderung von Straftaten nötig ist. Sollte fahrlässig unterlassen werden, ein effektives Compliance System aufzubauen, könnten sich daraus potentielle zivilrechtliche Ansprüche gegen den Angestellten ergeben.

Wer auch immer ein CMS prüft, fest steht, es kommen – wenn auch freiwillig – wieder neue Prüfungen auf die Unternehmen zu. Es ist aus Effektivitäts- und Effizienzgründen für alle Beteiligten (Prüfer, zu prüfende Stelle und Geschäftsführung) zielführend, wenn für sämtliche Prüfungen auf eine Unternehmens(prozess-)darstellung zugegriffen werden kann. Dabei ist es von zentraler Bedeutung, dass möglichst für alle Blickrichtungen auf ein Unternehmen die gleichen Begrifflichkeiten verwendet werden.

MOFIS-Methode als Clusterhilfe

Auf Basis dieser Überlegung hat sich in der Praxis der Autoren als Cluster (Einteilungs-) Hilfe für ein Unternehmen die sogenannte *MOFIS Methode* bewährt. Dabei steht MOFIS für die grundsätzliche Einteilung eines Unternehmens in Management (M), Operational (O), Financial (F), IT (I) und Specifics (S). Diese Methodik stellt eine Weiterentwicklung der, aus der internen Revision bekannten Clusterung von

sogenannten *Hauptprüffeldern* dar. Basis dieser Betrachtung sind die im Unternehmen vorhandenen Prozesse. Auf die MOFIS Matrix wird dann zum Beispiel das Risikomanagement und das interne Kontrollsystem oder auch das Anti-Fraud Management gelegt. Dadurch ist die Anwendung von einheitlichen Begriffsdefinitionen möglich.

In einem Unternehmen beruhen grundsätzlich alle Tätigkeiten auf Prozessen. Diese müssen erhoben werden, damit alle Unternehmensbeteiligten und etwaige Prüfer einen Überblick über die tatsächlichen Geschehnisse im Unternehmen erhalten. Als Ordnungskriterium (Clusterhilfe) bietet sich u. a. die oben beschriebene MOFIS Methode an. *Fraud* (Entdeckung und Prävention) und *Datenschutz* sind Themengebiete die bei einer Prozessbetrachtung immer eine Rolle spielen sollten, auch und gerade im Zusammenhang mit einem CMS. Nach der Erhebung sind die Prozesse im Rahmen des *Risikomanagements* zu bewerten. Dabei geht es um die Identifizierung von Risiken (Risikoanalyse) und die Bewertung in Geldbeträgen, wobei zwischen Bruttoisiken (ohne bewertete Gegenmaßnahmen) und Nettoisiken zu unterscheiden ist. Schließlich kann/sollten die Systeme wie Prozess- und Risikomanagement, internes Kontrollsystem und Anti-Fraudsystem, einer *Prüfung durch eine externe oder interne Revision* unterzogen werden.

Dies basiert auch auf der Erkenntnis, dass jeder Prozess sein Risiko hat und umgekehrt. Das heißt, dass es einer Abstimmung zwischen dem Prozessmanagement und dem Risikomanagement bedarf. In der Praxis zeigt sich, dass eine eingängige Prozessdarstellung die Grundlage für Redundanzvermeidungen bei sämtlichen auf ein Unternehmen zukommenden Prüfungen darstellt.

Da in der Unternehmenspraxis aber die Geschäftsprozesse regelmäßig nicht schriftlich niederlegt sind, kommt der Prozessaufnahme eine besondere Bedeutung zu. Vielfach wird die *Erhebung der Prozesse* in der Praxis durch die *interne Revision* durchgeführt, die diese dann *in einem zweiten Schritt auch prüft*. Ob dies der Zweckbestimmung eines Revisors entspricht, halten wir für zweifelhaft. Vielmehr sollten die Geschäftsprozesse durch von der internen Revision unabhängige Personen - nämlich die Prozessbeteiligten - aufgenommen werden, da andernfalls im Grunde die Prüfbereitschaft nicht vorhanden ist und so die nötige Distanz die sich auch im Vier-Augen-Prinzip manifestiert, nicht gegeben sein könnte.

Rolle der internen Revision im CMS

Das Management von Compliance bedarf einer im Organisationsermessen der gesetzlichen Vertreter liegenden Koordination bei der Entwicklung, Ausgestaltung und Überwachung des CMS. Die Unternehmensführung kann sich durch den Einsatz eines Compliance Officers unterstützen lassen. Compliance Management ist aber letztlich Chefsache. Neben der Unterstützung durch die Rechtsabteilung oder durch den Firmenanwalt (Compliance i. e. S.), kann die Unternehmensleitung auf bewährte in der Regel betriebswirtschaftlich geprägte Unternehmenssteuerungsinstrumente zwecks Sicherstellung von Compliance (Compliance i. w. S.) wie RMS *Risikomanagementsystem*, IKS *internes Kontrollsystem*, IR *interne Revision* etc. zurückgreifen. Selbstverständlich kommt hier der *internen Revision* eine herausragende Stellung zu, denn diese ist für nachfolgend dargestellte Aufgaben zuständig:

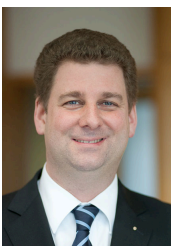
- a) Aufdeckung von Prozess- und Kontrollschwächen
- b) Kontinuierliche Unterstützung für die Optimierung von Geschäftsprozessen
- c) Überwachungsfunktion
- d) Kontinuierliche Berichterstattung

Zweifelsohne können als spezielle Beiträge der internen Revision zu mehr Compliance, deren prozessunabhängige Prüfung des IKS beitragen; denn in Bezug auf Compliance

untersucht sie das Prozessdesign und die Einrichtung der internen Kontrollen auf Sicherstellung der Einhaltung der relevanten Regeln. Das gilt entsprechend für das RMS; denn hier werden Konzeption und Organisation desselben, vollständige Erfassung der Risiken, Beurteilung der Risikoanalyse und -bewertung, sowie die resultierenden Maßnahmen und die Kommunikation in die Prüfung mit einbezogen. Mit den oben erwähnten Einschränkungen kann die interne Revision für die Prüfung des CMS zuständig sein. Ob sie tatsächlich wie von Schartmann/Büchner gefordert, die ersten Ansprechpartner bei eventuellen Verstößen sein sollten, ist doch eher zweifelhaft. Hier empfiehlt sich die Einführung eines *Hinweisgebersystems*, zum Beispiel unter Hinzuziehung eines externen Ombudsmannes, der unter Umständen eine juristische Ausbildung, insbesondere im Strafrecht, mitbringt. Dessen Aufgabe ist es dann, die Hinweise auf ihre rechtliche Relevanz hin zu prüfen, um so auch neutral Denunziantentum auszufiltern.

Fazit Die Verantwortung für ein wirksames und angemessenes CMS trägt allein die Geschäftsführung. Sie kann sich selbstverständlich durch andere – wie die interne Revision – unterstützen lassen. Aber es bleibt eine nicht delegierbare Vorbehaltsaufgabe. Das gilt gleichermaßen für den Aufsichtsrat, der sicherlich auf die Prüfungsergebnisse einer Prüfung nach PS 980 zurückgreifen kann, dennoch hat er eine originäre Prüfungspflicht mit der Einführung des §107 Abs. 3 AktG aufgetragen bekommen.

* * *



Autor

Wirtschaftsprüfer, Steuerberater Matthias Schenkel ist Gesellschafter-Geschäftsführer der Dr. Dornbach & Partner GmbH in Koblenz. Seine Tätigkeitsschwerpunkte liegen in der Beratung von mittelständischen Mandanten, Familienunternehmen und deren Gesellschaftern in steuerrechtlichen Fragen. Er hat sich auf die Gebiete Konzernrechnungslegung, Compliance Management und interne Revision spezialisiert. Der Autor ist Mitglied des European Executive Committee sowie des International Executive Committee von GMN International.

eMail mschenke@dornbach.de



Autor

Wirtschaftsprüfer, Steuerberater Jochen Ball ist geschäftsführender Gesellschafter der Dr. Dornbach Treuhand GmbH in Bad Homburg v.d.H. und betreut vor allem Mandanten der Branchen Finanzdienstleister, Real Estate und Health Care. Seine Tätigkeitsschwerpunkte liegen in der Compliance Management-Beratung, betriebswirtschaftlichen und Sanierungsberatung sowie bei IFRS. Der Autor hat umfangreich hierzu publiziert.

eMail jball@dornbach-rheinmain.de