KONSTANZ INSTITUT FÜR CORPORATE GOVERNANCE

Prüfung von Compliance-Management-Systemen

Maximilian Jantz, Stephan Grüninger

KICG – Forschungspapiere
Nr. 7 (2013)
ISSN 2198-4913

Konstanz Institut für
Corporate Governance

Hochschule Konstanz
Brauneggerstraße 55
78462 Konstanz

www.kicg.htwg-konstanz.de

KICG-Forschungspapier Nr. 7 (2013)

Prüfung von Compliance-Management-Systemen

Maximilian Jantz, Stephan Grüninger

Der folgende Artikel wurde im Rahmen der Aktivitäten der Arbeitsgruppe 2 „Monitoring & Review" des Forum Compliance & Integrity verfasst. Weitere Informationen zum Forum Compliance & Integrity: http://www.dnwe.de/fci.html

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

1 Über das Forum Compliance & Integrity

Das „Forum Compliance & Integrity ist ein freiwilliger Zusammenschluss von Unternehmen und Verbänden, die werteorientierte Compliance-Management-Systeme betreiben sowie die im WerteManagementSystem^{ZfW}[1] und ComplianceProgramMonitor^{ZfW}[2] erarbeiteten Ansätze des Werte- und Compliance-Managements unterstützen. Das Forum hat sich die Förderung, Weiterentwicklung und Qualitätssicherung von Compliance- und Integrity-Maßnahmen zum Ziel gesetzt und bietet darüber hinaus seinen Mitgliedern eine Plattform für kontinuierlichen Erfahrungsaustausch und gegenseitige Beratung.

Das FCI hat drei Arbeitsgruppen gebildet, in denen aktuelle und offene Themenstellungen aus dem Spektrum des Compliance- und Integritätsmanagements erörtert, Stellungnahmen und Studien erarbeitet sowie deren Veröffentlichung vorbereitet werden.

Die Arbeitsgruppe 2 „Monitoring & Review“[3] beschäftigt sich hierbei u.a. mit der Angemessenheit und Wirksamkeit von Compliance-Management-Systemen (CMS) und wird geleitet von Manuela Mackert, Chief Compliance Officer der Deutschen Telekom AG, und Prof. Dr. Stephan Grüninger, Direktor des Forum Compliance & Integrity.

2 Gründe für die Überwachung und Überprüfung von CMS

Die Gründe für eine Überwachung und Überprüfung von CMS können mannigfaltig sein:

- Unternehmen und Geschäftsleitung beabsichtigen die Minderung des Haftungsrisikos (vgl. z.B. USSG, wonach der Nachweis eines „Effective Program to Detect and Prevent Violations of Law“ einen Strafmilderungsgrund darstellen kann)
- Die Geschäftsleitung möchte sich nach erstmaliger Implementierung eines CMS dessen Effektivität versichern lassen
- Aufsichtsrat/Prüfungsausschuss kommen ihrer Pflicht gem. §§ 111 Abs. 1, 107 Abs. 3 AktG sowie den Empfehlungen des Deutschen Corporate Governance Kodex (vgl. Ziff. 5.3.2 des DCGK) nach, die Wirksamkeit eines eingerichteten internen Kontrollsystems zu überwachen. Dies umfasst auch die Überwachung der Angemessenheits- und Funktionsfähigkeit des CMS[4]
- Prüfung im Rahmen der gesetzlichen bzw. freiwilligen Abschlussprüfung
- Nachweis eines durch eine unabhängige Instanz geprüften CMS im Rahmen von M&A Transaktionen
- Überprüfung des CMS nach einem erheblichen Compliance-Verstoß

[1] Abrufbar unter: http://www.dnwe.de/tl_files/ZfW/wms.pdf (21.11.2012).
[2] Abrufbar unter: abrufbar unter: http://www.dnwe.de/tl_files/ZfW/cpm.pdf (21.11.2012).
[3] Das FCI hat insgesamt 3 Arbeitsgruppen gegründet. Neben der Arbeitsgruppe 2 bestehen bislang die Arbeitsgruppe 1 „Values & Integrity“ sowie die Arbeitsgruppe 3 „Best Practice Benchmarking“ (http://www.dnwe.de/fci-arbeitsgruppen.html).
[4] Hüffer, Aktiengesetz, 9. Auflage 2010, §107, Rn. 17c.

- Einsetzung eines sog. „Compliance Monitors“ nach US-amerikanischer Rechtspraxis, der auf Grundlage einer Vereinbarung mit US Behörden das Unternehmen einige Jahre dahingehend kontrolliert, ob die eingerichteten Compliance-Maßnahmen auch greifen.[5]

Kommt es zu der Überprüfung des CMS, so dürfte für die Unternehmen primäres Ziel der Überprüfung die Feststellung sein, inwieweit die implementierten Compliance-Maßnahmen angemessen und wirksam sind.

3 Allgemeine Definition von Angemessenheit und Wirksamkeit

Der Begriff Angemessenheit steht für „Adäquanz, Adäquatheit, Eignung, Verhältnismäßigkeit, Zweck-Mittel-Relation“.[6] In diesem Sinne sind Compliance-Maßnahmen dann angemessen, wenn sie generell geeignet sind, das Ziel – nämlich die Vermeidung bzw. „wesentliche Erschwerung“ (vgl. § 130 OWiG) von Compliance-Verstößen – erreichen zu können.

Wirksamkeit bedeutet: „Ausmaß, in dem geplante Tätigkeiten verwirklicht und geplante Ergebnisse erreicht werden.“[7] Die Beurteilung der Wirksamkeit eines CMS hängt somit von der Erreichung der gesteckten Ziele ab. Werden die mit einem CMS verfolgten Ziele – nämlich Prävention und Detektion von Fehlverhalten – durch die zugeordneten Compliance-Maßnahmen mit hinreichender Sicherheit erreicht, so könnte man das CMS als *wirksam* bezeichnen. Sollten einzelne Ziele hingegen nicht erreicht werden, sei es weil die Compliance-Maßnahmen nicht angemessen sind oder weil durchgeführte aufdeckende Kontrollen zu keiner lückenlosen Entdeckung von Verstößen führen, könnte die Beurteilung zur *Wirksamkeit* des Gesamtsystems CMS sehr schnell angreifbar werden.

Entsprechend der eingangs dargelegten allgemeinen Definition von Wirksamkeit kann das CMS eines Unternehmens dann als wirksam bezeichnet werden, wenn die Maßnahmen/Elemente tatsächlich implementiert wurden (*..geplante Tätigkeiten verwirklicht..)* und zu einer Prävention und Detektion (*..geplante Ergebnisse erreicht werden..)* – z.B. im Wege der Aufdeckung von erfolgten Verstößen durch Kontrollverantwortliche in den Geschäftsprozessen– führen.

Unternehmen sehen sich allerdings der nicht leicht zu beantwortenden Frage ausgesetzt, wie die Prüfung von CMS im Detail zu erfolgen hat, um die Angemessenheit und Wirksamkeit der CMS tatsächlich beurteilen zu können.

4 Definition unterschiedlicher Prüfungshandlungen

Prüfungshandlungen können unterschiedlich ausgerichtet sein – nämlich zur Beurteilung der Angemessenheit, der Funktionsfähigkeit und Wirksamkeit.

---

[5] Vgl. Siemens: Einsetzung des ehemaligen Bundesfinanzministers Dr. Theo Waigel (vgl. http://www.siemens.com/press/de/pressemitteilungen/?press=/de/pressemitteilungen/2008/corporate_communication/axx20081220.html) oder Daimler: Einsetzung des ehemaligen US-Richters Louis Freeh (vgl. http://www.daimler.com/dccom/0-5-7171-49-1285922-1-0-0-0-0-1-8-7164-0-0-0-0-0-0-0.html, 18.05.2012).

[6] Abrufbar unter: http://www.enzyklo.de/Begriff/Angemessenheit (17.02.2012).

[7] ENZYKLO- Online Enzyklopädie http://www.enzyklo.de/Begriff/Wirksamkeit%28effectiveness%29 (17.02.2012).

Im Rahmen der Angemessenheitsprüfung wird überprüft, ob bei der Ausgestaltung des Compliance-Programms die für das Unternehmen relevanten Referenzstandards berücksichtigt wurden und die getroffenen Compliance-Maßnahmen für die Organisation angemessen ausgestaltet sind.[8] Dieser „Design Check" beinhaltet eine inhaltliche Prüfung (z.B. ist die Regel richtig, sind die Maßnahmen sinnvoll bzw. notwendig aufgrund bestehender externer Benchmarks oder Standards) sowie eine strukturelle Prüfung (passen die Regeln und Maßnahmen für die Organisation und sind sie so aufgestellt, dass sie innerhalb der Organisation funktionieren können).

Bei der Überprüfung der Funktionsfähigkeit ist zu prüfen, ob eine Compliance-Maßnahme implementiert, also verabschiedet und in Kraft getreten ist, alle zugehörigen Instrumente (wie Formulare, technischen Systeme etc.) vorhanden sind und die Compliance-Maßnahme den ihr zugedachten Zweck – nämlich das definierte Ziel - erfüllen kann.[9]

Bei der Wirksamkeitsprüfung des Compliance-Systems hingegen ist durch eine Überprüfung der dezentralen Implementierung von Compliance-Maßnahmen bzw. –Kontrollen im Wege von Stichproben (i.S.v. prozessualen Vor-Ort-Prüfungen) zu überprüfen, ob die Elemente des CMS (die Compliance-Grundsätze und Compliance-Maßnahmen) wirksam implementiert worden sind und im Geschäftsalltag tatsächlich angewendet werden. Im Rahmen der Wirksamkeitsprüfung kommt es also darauf an, ob die Compliance-Maßnahme im Unternehmensalltag „gelebt" wird. Dabei ist bei der Beurteilung der wirksamen Implementierung zu unterscheiden, ob es um Compliance-Grundsätze oder Compliance-Maßnahmen geht. Bei der Überprüfung der wirksamen Implementierung von Compliance-Maßnahmen wird, wie zuvor ausgeführt, über prozessuale Vor-Ort-Prüfungen (Stichproben) geprüft, ob diese Maßnahmen in den Geschäftsprozessen tatsächlich angewendet werden.

Compliance-Grundsätze hingegen können dann als wirksam implementiert betrachtet werden, wenn sie von den jeweils zuständigen Organen/Gremien unter Wahrung der Beteiligungsrechte der Arbeitnehmervertreter beschlossen und an den Adressatenkreis der Richtlinie bekanntgemacht worden sind. Sofern die Compliance-Grundsätze auch Regularien mit prozessualen Komponenten enthalten, wäre unserer Auffassung nach im Rahmen einer Wirksamkeitsprüfung ebenso die Implementierung dieser prozessualen Komponenten zu prüfen.

Von diesen prozessualen Vor-Ort-Prüfungen sind jedoch sowohl Prozessanalysen, die auf die Prozessstabilität gegen Non-Compliance/ Fraud abzielen, als auch Compliance-Audits streng zu unterscheiden.

Prozessanalysen erfordern einen erheblich hohen Aufwand, da diese in der Regel Untersuchungshandlungen wie Ist-Aufnahmen von Geschäfts-(teil)prozessen, „Walk-throughs" (Beobachtung und Dokumentation der Ist-Prozesse), die Identifikation von Kontrolllücken und das Testen von Kontrollen auf Wirksamkeit beinhalten können. Noch umfassender können sog. Compliance-Audits ausfallen, die weit über den Umfang von prozessualen Vor-Ort-Prüfungen hinausgehen. Compliance-Audits bedeuten die Überprüfung der Regeleinhaltung bezogen auf bestimmte Prüfungsgegenstände (z.B. Anti-Bribery, Illegal Price Fixing) und –Zeiträume. Die Analyse zielt daher auf Geschäftsvorfälle, entweder mit relativ hoher Stichprobe oder aber

[8] Vgl. CPM[ZfW].
[9] Vgl. CPM[ZfW].

mittels einer Vollerfassung bezogen auf einen bestimmten Prüfungszeitraum, ab. - Das Compliance-Audit ist damit von der Herangehensweise der forensischen Untersuchung ähnlich, ohne dass jedoch ein konkreter Verdachtsfall in der zu untersuchenden Entität vorliegt.

5 Prüfung nach IDW PS 980

Mit dem PS 980 wurde seitens der Wirtschaftsprüfer ein Prüfungsstandard geschaffen, der drei unterschiedliche Prüfungsvarianten aufweist. Im Weiteren soll auf die folgenden Punkte näher eingegangen werden:

- Wirksamkeitsprüfung nach dem PS 980
- Ist einer externen Prüfung nach PS 980 gegenüber einer internen Prüfung der Vorrang einzuräumen?
- Möglichkeit der Enthaftung durch ein Testat/Bericht nach dem PS 980?
- Grenzen der Wirksamkeitsprüfung (Management Override u.a.)

5.1 Wirksamkeitsprüfung nach IDW PS 980

Bei der CMS-Prüfung wird zwischen den drei Kategorien – Konzeptionsprüfung (1), Angemessenheitsprüfung (2) sowie Wirksamkeitsprüfung (3) – unterschieden.

Im Rahmen der Angemessenheitsprüfung nach Kategorie 2 des PS 980, die auch die Implementierungsprüfung umfasst, wird festgestellt, ob die Aussagen in der CMS-Beschreibung, d.h. dem Prüfungsgegenstand – SOLL-Objekt – angemessen dargestellt und grundsätzlich geeignet sind, wesentliche Regelverstöße rechtzeitig zu erkennen und zu verhindern und ob die Maßnahmen zu einem bestimmten Zeitpunkt implementiert waren. Eine Richtlinie kann beispielsweise dann als umgesetzt gelten, wenn die Voraussetzungen, nämlich die Beschlussfassung durch das jeweils zuständige Organ/Gremium, Wahrung der Beteiligungsrechte der Arbeitnehmervertreter und Bekanntmachung an den Adressatenkreis der Richtlinie, erfüllt sind. Die Feststellung, ob die Maßnahmen formell implementiert sind kann somit nach unserer Ansicht im Regelfall durch Dokumentenreview erfolgen (z.B. Implementierungsbeschlüsse, Kommunikationsnachweise etc.). Die Wirksamkeit des CMS ist nach IDW PS 980 dann gegeben „wenn die Grundsätze und Maßnahmen in den laufenden Geschäftsprozessen von den hiervon Betroffenen nach Maßgabe ihrer Verantwortung zur Kenntnis genommen und **beachtet** werden (vgl. Tz. A12 f.)“. Nach dem IDW PS 980 handelt es sich bei den Grundsätzen um „Regelungen, mit denen die Mitarbeiter und ggfs. Dritte zu regelkonformem Verhalten angehalten werden.“ (Tz. A17). Nach dieser Definition dürften unter die Grundsätze sowohl der Code of Conduct/ Code of Ethics – oder wie auch immer die firmenspezifische Bezeichnung der Unternehmensleitlinie lautet – sowie die darauf abgeleiteten weiteren internen (Bereichs-)Richtlinien fallen. Wie der PS 980 allerdings die Feststellung treffen will, dass der Code of Conduct von den betroffenen Mitarbeitern während eines bestimmten Zeitraumes **beachtet** wurde, bleibt fraglich. Dies wäre nach unserer Ansicht letztendlich nur durch eine umfassende forensische Überprüfung möglich, die systematisch und strukturiert nach Anhaltspunkten für wirtschaftskriminelle Handlungen sucht und dabei prüft, ob sämtliche Geschäftsvorgänge im Einklang mit dem Code of Conduct und allen weiteren Betriebsrichtlinien stehen (s.o.). Dies wird

jedoch von den Wirtschaftsprüfern im Rahmen der Wirksamkeitsprüfung nach IDW PS 980 so nicht vorgenommen, welcher im Einklang mit dem International Framework for Assurance Engagements (ISAE) 3000 ein Prüfungsauftrag zur Erlangung „hinreichender Sicherheit" ist[10] (siehe Tz. A12). Dementsprechend wird der Wirksamkeitsbegriff (Tz. 21) an zwei Stellen im IDW PS 980 schließlich wieder eingeschränkt. So wird in Tz. A12 klarstellt, dass auch ein ansonsten wirksames CMS systemimmanenten Grenzen unterliegt, sodass möglicherweise auch wesentliche Regelverstöße auftreten können, ohne systemseitig verhindert oder aufgedeckt zu werden. Dies wird dann in Tz. 18 nochmals verdeutlicht: „Die Zielsetzung einer nach diesem IDW Prüfungsstandard durchgeführten Prüfung liegt als Systemprüfung nicht in dem Erkennen von einzelnen Regelverstößen. Sie ist daher nicht darauf ausgerichtet, Prüfungssicherheit über die **tatsächliche Einhaltung von Regeln zu erlangen** (vgl. Tz. 30 und A12)."

Diese Systematik kann nach unserer Ansicht zu Fehlinterpretationen bzgl. der nach dem PS 980 zu erbringenden Leistung bei der Wirksamkeitsprüfung führen, da die Definition von „Wirksamkeit" (in Tz. 21) zu weitgehend gefasst ist, weil sie die Möglichkeit der Überprüfung der Regeleinhaltung durch die betroffenen Mitarbeiter an dieser Stelle suggeriert. Zur Vermeidung von Missverständnissen sollte unserer Ansicht nach die Wirksamkeitsdefinition im PS 980 entsprechend angepasst werden, indem z.B. diese beiden Einschränkungen (Tz. 12A und Tz. 18) auch unmittelbar nach der Definition der Wirksamkeitsprüfung in Tz. 21 angeführt werden.

Der Begriff „beachtet" im Rahmen der Wirksamkeitsdefinition kann zu einem weiteren Missverständnis bzgl. der Leistung der Wirksamkeitsprüfung führen, nämlich dass die Wirksamkeitsprüfung gem. IDW PS 980 eine Inhaltsprüfung dahingehend beinhaltet, ob z.B. Richtlinien und Fallbearbeitung *inhaltlich* korrekt und/oder Compliance-Risiken *inhaltlich* korrekt erfasst sind. Eine derartige Leistung wird allerdings von der Wirksamkeitsprüfung nicht umfasst. Ein Grund dafür ist, dass Wirtschaftsprüfern in aller Regel hierfür eine ausreichende Kenntnis des Unternehmens fehlt oder diese nur mit sehr hohen Kosten erlangt werden kann. Denn eine Wirksamkeitsprüfung kann nur im Wege einer stichprobenartigen Systemprüfung erfolgen, die auch eine Aussage darüber enthält, ob die betroffenen Personen die implementierten Maßnahmen im operativen Geschäft tatsächlich berücksichtigt und eingehalten haben.

Im PS 980 sollte deshalb erläutert werden, dass „Einhalten" und „Befolgen" sich auf die im Rahmen des CMS implementierten Maßnahmen und Grundsätze bezieht, die Wirksamkeitsprüfung jedoch nicht den Anspruch auf Aufdeckung von Einzelverstößen hat. Weiterhin könnte erläutert werden, dass die Prüfungshandlungen einer Wirksamkeitsprüfung („Einhalten" und „Befolgen") auf den Grad der „Prüfbarkeit" von CMS-Bestandteilen anzupassen sind, z. B. kann die „Befolgung" von Verhaltensgrundsätzen schwer direkt, jedoch aber indirekt

[10] Hinreichende Sicherheit bedeutet nicht absolute Sicherheit: Auch ein ansonsten wirksames CMS unterliegt systemimmanenten Grenzen, sodass möglicherweise auch wesentliche Regelverstöße auftreten können, ohne systemseitig verhindert oder aufgedeckt zu werden. Diese systemimmanenten Grenzen ergeben sich u.a. aus menschlichen Fehlleistungen (bspw. infolge von Nachlässigkeit, Ablenkungen, Beurteilungsfehlern und Missverstehen von Arbeitsanweisungen), Missbrauch oder Vernachlässigung der Verantwortung durch für bestimmte Maßnahmen verantwortliche Personen, der Umgehung oder Außerkraftsetzung von Kontrollen durch Zusammenarbeit zweier oder mehrerer Personen oder dem Verzicht des Managements auf bestimmte Maßnahmen, weil die Kosten dafür höher eingeschätzt werden als der erwartete Nutzen (A12).

beispielsweise durch Abfrage des Kenntnisstandes sowie durch Abfrage des „Wollens“, d.h. der Bereitschaft, die Regeln einzuhalten, geprüft werden.

Im Ergebnis kann damit festgehalten werden, dass es sich bei der Wirksamkeitsprüfung nach IDW PS 980 um eine *Implementierungsprüfung* handelt, die neben einer Überprüfung der dezentralen Implementierung von Compliance-Maßnahmen bzw. -Kontrollen auch eine Stichprobenprüfung dahingehend beinhaltet, ob die Richtlinien, Regularien von den Mitarbeitern gelebt werden. Basierend auf den obigen Ausführungen müsste aus unserer Sicht im PS 980 die Definition zur Wirksamkeitsprüfung klargestellt werden, da ansonsten weiterhin den Unternehmen eine Leistung suggeriert wird, die der PS 980 nicht erbringen kann und letztendlich auch nicht erbringen will.

Eine praxisnähere Definition zur Wirksamkeitsprüfung von CMS könnte in Anlehnung an den ComplianceProgramMonitor^{ZfW} (CPM)[11] wie folgt lauten:

„Im Rahmen der Wirksamkeitsprüfung wird überprüft, ob die für die Organisation angemessen ausgestalteten und implementierten Elemente des CMS im Geschäftsalltag angewendet werden (Effectiveness Check). Dazu muss die geprüfte Compliance-Maßnahme bereits mindestens einmal ausgeführt worden sein. Bei der Prüfung der wirksamen Umsetzung kommt es also darauf an, ob die Compliance-Maßnahme tatsächlich im Unternehmensalltag „gelebt“ wird. Dabei ist zu beachten, dass die Wirksamkeitsprüfung nicht für alle Compliance-Maßnahmen möglich ist. Z.B. ist ein Code of Conduct nur hinsichtlich der Angemessenheit und Implementierung überprüfbar, da im Rahmen eines Compliance-Monitorings nicht überprüft werden kann, ob sich Mitarbeiter an die inhaltlichen Vorgaben des Kodex halten.“ In diesen Fällen muss es für eine prozessuale Wirksamkeitsprüfung ausreichend sein, wenn die Verhaltensregeln von den jeweils zuständigen Organen/Gremien unter Wahrung der Beteiligungsrechte der Arbeitnehmervertreter beschlossen und an den Adressatenkreis der Richtlinie bekanntgemacht worden sind und die von der Richtlinie betroffenen Mitarbeiter entsprechend geschult wurden. Weiter heißt es im CPM *„Demgegenüber ist die Integration von Compliance in Zielvereinbarungen und Leistungsbewertungen erst dann „effektiv“, wenn dieses Instrument einmal angewendet wurde, nicht, wenn dessen Planung abgeschlossen und das Prozedere vollständig beschrieben ist.“* An diesem Beispiel der Integration von Compliance in die HR-/Vergütungssysteme wird sehr deutlich, dass eine Wirksamkeitsprüfung durch Wirtschaftsprüfer sich nur auf die Anwendung bzw. Nichtanwendung des unternehmensindividuell erarbeiteten Instruments beziehen kann, nicht aber auf die Frage, ob das angewendete Instrument „qualitativ gut“ ist. Die spezifische Kompetenz von Wirtschaftsprüfern im Allgemeinen macht eine solche „Qualitätsprüfung“ schlicht unmöglich! Bei Verhaltensrichtlinien, die auch Regularien mit prozessualen Komponenten enthalten, wäre auch hier unserer Auffassung nach im Rahmen der Wirksamkeitsprüfung die Implementierung dieser prozessualen Komponenten zu prüfen. Die folgenden Beispiele sollen den Gegenstand einer solchen dezentralen Implementierungsprüfung (prozessuale Vor-Ort-Prüfung) ohne Inhaltsprüfung weiter veranschaulichen:

- Prozess „Geschäftspartnerscreening“: Dieser Prozess kann eine Stichprobenprüfung beinhalten, ob das Ausfüllen der Selbstauskunft durch die Mitarbeiter eingehalten

[11] Abrufbar unter: http://www.dnwe.de/complianceprogrammonitor.html (20.02.2012).

wurde und die Mitarbeiter das Verfahren korrekt und im Einklang mit der zugrundeliegenden Policy und der dort festgelegten Grundsätzen durchgeführt haben ohne dabei die Richtigkeit des Ausfüllens zu überprüfen.

- Prozess „Aufnahme bestimmter Vertragsklauseln in Verträgen“: Dieser Prozess könnte beispielsweise die prozessuale Stichprobenprüfung vorsehen, Einblick in die relevanten Verträge zu nehmen, um festzustellen, ob die Regelung – nämlich die Aufnahme von Anti-Korruptions-Vertragsklauseln in den Verträgen – auch tatsächlich beachtet wurde. Eine inhaltliche Prüfung der Verträge findet dabei im Rahmen der IDW PS 980 Prüfung nicht statt.
- Prozess „Tell me / Case Management“: Anhand einer Stichprobenprüfung kann die Anwendung der implementierten Prozesse zur Prüfung der eingehenden Hinweise auf Compliance-Verstöße und Fallbearbeitung (bei hinreichendem Anfangsverdacht) durchgeführt werden, wobei keine inhaltliche Prüfung (Fallbearbeitung korrekt, angemessene Sanktionierung etc.) stattfindet.
- Prozess „Compliance Risk Assessment:“ Anhand einer Stichprobenprüfung kann die Anwendung der implementierten Prozesse zur Durchführung von Compliance Risk Assessments (CRA) (z.B. Prozessdarstellung, Schulung der Prozessteilnehmer, Durchführung des CRA auf Gesellschaftsebene, Berichterstattung der Ergebnisse an die vorab definierten Gremien) geprüft werden. Eine Prüfung, ob die Gesellschaft die richtigen Risiken im Rahmen des CRA benannt hat, ist allerdings nicht Gegenstand einer IDW PS 980-Prüfung.
- Sollten diese Prüfungen in den genannten Beispielen allerdings bereits durch die lokale Revision oder Compliance-Abteilung durchgeführt worden sein, so kann auf dieses Ergebnis Bezug genommen werden, wodurch eine zusätzliche dezentrale Implementierungsprüfung im Rahmen der IDW Prüfung entbehrlich wäre.

5.2 Interne Prüfung vs. externe Prüfung nach PS 980

Die Überprüfung erfolgt in der Praxis durch eine „neutrale“ Stelle. Dabei kann die Überprüfung sowohl durch eine interne als auch externe Prüfungsinstanz erfolgen. Intern wird die Prüfung üblicherweise durch die Innenrevision vorgenommen.

Als externe Experten kommen insbesondere Anwaltskanzleien, Wirtschaftsprüfer sowie im Bereich Compliance & Integrity erfahrene Experten in Betracht. Eine solche externe Prüfung wird vor allem dann erforderlich sein, wenn es der Innenrevision eines Unternehmens an der notwendigen Fachkompetenz zur Durchführung der Prüfungen fehlt bzw. der Aufbau einer solchen Fachkompetenz wirtschaftlich mit unverhältnismäßig hohen Kosten verbunden wäre.[12]

Da Compliance-Verstöße Schadensersatzforderungen, Strafverfahren, Geldbußen und Reputationsschäden nach sich ziehen können, ist das Ansinnen von Vorstand und Aufsichtsrat, sich im Falle eines Compliance-Vorfalles, vor Gericht enthaften zu können, gegeben. Nach unserer Erfahrung ist dies für manch Unternehmen Anlass, eine Überprüfung seitens einer externen Stelle durchführen zu lassen.

[12] Moosmayer, Compliance, 2. Auflage 2012, S.90.

Als Argument für ein von einer neutralen Instanz erarbeitetes Gutachten könnte weiter angeführt werden, dass durch ein unabhängiges Gutachten/Zertifizierung der Bericht des Vorstandes/Aufsichtsrates zur Wirksamkeit des CMS an Glaubwürdigkeit gewinnt. Die Glaubwürdigkeit kann aber nur dann nachhaltig sichergestellt werden, wenn Transparenz über Prüfungshandlungen und Prüfungsaussagen besteht und keine falschen Vorstellungen seitens Kapitalmarktteilnehmern und anderen Stakeholdern zu überzogenen Erwartungen an die Prüfungssicherheit führen.[13]

Eine 2004 durchgeführte Befragung im Rahmen einer internationalen Analyse des Nutzens von Testaten in Nachhaltigkeitsberichten hat ergeben, dass nur etwas mehr als die Hälfte der Befragten eine unabhängige Begutachtung für ein hilfreiches Mittel zur Steigerung der Glaubwürdigkeit hielten.[14] Im Ergebnis ihrer Untersuchung halten die Autoren allerdings fest, dass die Testierung von Nachhaltigkeitsberichten als eine wichtige Option zur Förderung der Glaubwürdigkeit von Unternehmen und ihrer Sustainable Corporate Governance angesehen werden kann.[15] Wohlgemerkt ist zu betonen, dass die Testierung als *eine* Option zu sehen ist, die aber nicht unbedingt genutzt werden muss, um Glaubwürdigkeit zu erlangen.[16]

Interne und externe Prüfungen sind gleichermaßen geeignet, ein CMS auf Angemessenheit und Wirksamkeit hin zu prüfen. Aus diesem Grund sollte sich nach unserer Ansicht keine „Best Practice" dahingehend entwickeln, dass einer externen Prüfung ein höherer Stellenwert als einer internen Prüfung eingeräumt wird mit der Folge, dass Unternehmen sich künftig gezwungen sehen könnten, sich für die externe Prüfung zu entscheiden, um der „Best Practice" gerecht zu werden.

Vor allem sollten die Unternehmen nicht aus den Augen verlieren, dass in vielen Fällen eine tatsächlich unabhängige, mit den Prozessen und der Kultur des Unternehmens vertraute interne Audit-Abteilung wertvollere Erkenntnisse und Ergebnisse bringen kann als eine Überprüfung durch externe Berater.

5.3 Möglichkeit der Enthaftung durch eine Zertifizierung/Bericht nach dem PS 980?

Eine externe Bescheinigung der Wirksamkeit eines CMS von einer anerkannten unabhängigen Stelle kann u.U. zu einer Haftungsentlastung des Unternehmens und seiner Organe beitragen. Inwieweit im Einzelfall tatsächlich eine Zertifizierung/Zertifikat einer unabhängigen Stelle, das die Wirksamkeit eines CMS bescheinigt, haftungsentlastend wirken kann, bleibt offen. Nach Ansicht von Prof. Dr. Wulf Goette – bis September 2010 Vorsitzender Richter am BGH – helfe das

---

[13] Zum Problem überzogener Erwartungen an die Leistungsfähigkeit von Wirtschaftsprüfung im allgemeinen um CMS-Prüfungen im besonderen vgl. Grüninger „Wirtschaftsprüfung und Prüfung von Compliance-Management-Systemen im Spannungsfeld von Kontrolle und Vertrauen", Wieland (Hrsg.): Die Zukunft der Firma (Studien zur Governanceethik Band 10, 2011), S. 131 – 166.

[14] Clausen/Loew: „Mehr Glaubwürdigkeit durch Testate: Internationale Analyse des Nutzens von Testaten in der Umwelt- und Nachhaltigkeitsberichterstattung"; IÖW (Hrsg.) 2005, S. 75(abrufbar unter: http://www.bmu.de/wirtschaft_und_umwelt/ unternehmensverantwortung_csr/nachhaltigkeitsmanagement/doc/37054.php,17.02.2012).

[15] Clausen/Loew: „Mehr Glaubwürdigkeit durch Testate: Internationale Analyse des Nutzens von Testaten in der Umwelt- und Nachhaltigkeitsberichterstattung"; IÖW (Hrsg.) 2005, S. 80.

[16] Clausen/Loew: „Mehr Glaubwürdigkeit durch Testate: Internationale Analyse des Nutzens von Testaten in der Umwelt- und Nachhaltigkeitsberichterstattung"; IÖW (Hrsg.) 2005, S. 77.

Testat vor Gericht nichts, wenn die Risikoanalyse, die das Unternehmen selbst vornimmt und auf der die Prüfung durch die Wirtschaftsprüfer basiert, nicht stimmt.[17]

5.4 Grenzen der Wirksamkeitsprüfung

Eine hundertprozentige Compliance lässt sich weder durch interne noch externe unabhängige Prüfungshandlungen erzielen. Diese systemimmanenten Grenzen ergeben sich u.a. durch bewusste Außerkraftsetzung interner Kontrollen seitens des Managements („management override"), fehlendem Tone from the Top, falscher Vorbilder oder durch Umgehung im Wege kollusiver Zusammenarbeit zweier oder mehrerer Personen. Diesen Umstand berücksichtigt auch der PS 980 (vgl. Tz. A12), was jedoch nach Ansicht von AG 2 des FCI in der Wirksamkeitsdefinition nicht deutlich genug gemacht wurde, so dass ein falscher Wirksamkeitsbegriff suggeriert wird.

Da Wirksamkeit nach dem PS 980 bedeutet, dass die Betroffenen die Maßnahmen kennen und beachten, so dürfte nach dem PS 980 eine Aussage zur inhaltlichen Wirksamkeit letztendlich nie möglich sein, da der PS 980 selbst davon ausgeht, dass es immer möglich sein wird, dass Mitarbeiter die implementierten Maßnahmen nicht einhalten , sei es intentional oder aufgrund fehlerhaften Verhaltens, weil sie z.B. die korrekte Anwendung in der konkreten Arbeitssituation nicht erkennen können (komplexe dynamische Arbeitswelt).

6 Anforderungen an die Prüfung

Aus den vorherigen Ausführungen lassen sich einige Anforderungen an eine Prüfung ableiten, damit diese die Angemessenheit und Effektivität des CMS realistisch beurteilen kann:

6.1 Unterschiedliche Arten der Prüfung

Unternehmen müssen unterschiedliche Arten der Wirksamkeitsprüfung zur Verfügung stehen:

- Interne Prüfung durch eine tatsächlich unabhängige, mit den Prozessen und der Kultur des Unternehmens vertraute interne Audit-Abteilung
- Externe Prüfung, falls intern die erforderliche Fachkompetenz nicht vorhanden ist oder das Unternehmen in bestimmten Situationen die „Neutralität" einer externen Stelle als eher gegeben sehen sollte
- Externe Prüfung nach IDW PS 980 weil z.B. Nachhaltigkeitsinvestoren hierauf Wert legen

6.2 Inhalt der Wirksamkeitsprüfung

Bei der Wirksamkeitsprüfung geht es darum zu überprüfen, ob die Elemente des Compliance-Management-Systems im Geschäftsalltag angewendet werden. Entsprechend den obigen Ausführungen hat nach unserer Ansicht bei der Wirksamkeitsprüfung von Verhaltens-

[17] Schlueter: „Persilschein vom Wirtschaftsprüfer" , COMPLIANCE Mai 2011, S. 2 (abrufbar unter: www.compliance-plattform.de, 18.05.2012).

vorschriften – wie beispielsweise dem CoC – allerdings lediglich eine Prüfung von Funktionsfähigkeit und Implementierung der CMS Maßnahmen stattzufinden und keinesfalls eine Überprüfung der ***Beachtung*** von Maßnahmen. Denn letztendlich findet seitens des PS 980 kein *Compliance Audit*[18] dergestalt statt, dass umfassende Kontrollen der Dokumentation und Stichprobenerhebungen bzgl. des Mitarbeiterverhaltens im Sinne einer forensischen Untersuchung vorgenommen werden. Z.B. mag es durchaus in bestimmten Situationen angebracht sein, eine derartig umfangreiche anlassbezogene Untersuchung oder ein nicht anlassbezogenes Detektion Audit auf Antrag des Unternehmens durchzuführen, wird aber auf Sonderfälle begrenzt sein. Im Ergebnis findet nach dem IDW PS 980 vielmehr ein *Compliance* ***Program*** *Audit (*bzw. *Compliance Monitoring)*[19] statt, nämlich eine Systemprüfung dahingehend, ob die Elemente des CMS implementiert, grundsätzlich funktionsfähig sind und wirksam in die Geschäftsprozesse des Unternehmens implementiert wurden. Hier sollte nach dem PS980 die Wirksamkeitsprüfung auf der Programmebene ansetzen, um so durch Stichproben die erfolgreiche Umsetzung der CMS-Maßnahme und Grundsätze zu beurteilen. Daher sollten im PS 980 Definitionen und Beschreibungen den tatsächlichen Begebenheiten nämlich dem, was letztendlich im Rahmen der PS 980 Prüfungen geleistet wird, auch entsprechend angepasst werden.

---

[18] Begriffsbestimmung *Compliance Audit* nach CPM^{ZfW}: „Ein Compliance Audit, hier die Überprüfung der Funktionsfähigkeit des Business Conduct Compliance-Programms, kann sowohl intern (z. B. durch die interne Revision) als auch extern (z. B. durch geeignete Beratungs- oder Wirtschaftsprüfungsgesellschaften) erfolgen. Der Begriff Audit soll im Rahmen dieses Leitfadens für die Fälle reserviert sein, in denen ein Compliance-Programm bereits vorhanden ist, d. h. eine Implementierung abgeschlossen ist. Das bedeutet nicht, dass bereits alle Compliance-Maßnahmen implementiert und umgesetzt sein müssen, die unter den Gesichtspunkten von Best-Practice und Angemessenheit für das Unternehmen notwendig sind. Es bedeutet lediglich, dass der interne oder externe Auditor bzw. das interne oder externe Audit-Team seine Aufgabe nach einem erfolgten Implementierungsprozess ausführt." (abrufbar unter http://www.dnwe.de/complianceprogrammonitor.html).

[19] Begriffsbestimmung *Compliance Program Audit* bzw. *Compliance Monitoring* nach CPM^{ZfW}: „Dahingegen soll mit Compliance Monitoring gemeint sein, dass der externe, unabhängige und objektive Compliance Monitor seine Aufgabe im Zuge der Implementierung des Compliance-Programms im Sinne einer prozessbegleitenden Prüfung wahrnimmt. Er agiert in diesem Zusammenhang ausdrücklich nicht als Berater oder Trainer, d. h. er trifft keine Entscheidungen hinsichtlich notwendiger Compliance-Maßnahmen oder gestaltet deren Implementierung und Umsetzung. Dagegen coacht er die Unternehmensleitung, die internen Compliance-Verantwortlichen (Compliance-Beauftragter, Compliance Committee etc.) und etwaige interne und externe Berater entlang von Best-Practice-Standards. Ein Best-Practice-Standard stellt beispielsweise die Gesamtheit der in der Compliance Checkliste (siehe D. III.) genannten Anforderungen dar. Compliance Monitoring kommt u.a. dann zur Anwendung, wenn private und insbesondere öffentliche Auftraggeber oder Finanzierungsinstitute (z. B. Weltbank, Europäische Bank für Wiederaufbau und Entwicklung) die Einrichtung oder Erneuerung/ Verbesserung eines Compliance Systems von einem Unternehmen verlangen. Der unabhängige Compliance Monitor berichtet in diesem Falle während der Entwicklung und Implementierung über die Fortschritte und den Status und erstellt einen Abschlussbericht nach erfolgter Einrichtung des Compliance Systems. In den folgenden Abschnitten wird der Begriff Compliance Monitoring auch für einer Compliance-Programm-Implementierung nachgelagerte Überprüfungsverfahren des Compliance Audits verwendet. Dies soll der besseren Lesbarkeit dienen. Umfang und Dauer eines Compliance Monitorings können nicht allgemeingültig definiert, sondern nur für den Einzelfall vom Compliance Monitor festgelegt werden. In jedem Falle sind die Unternehmensgröße (Umsatz, Anzahl der Mitarbeiter), die Komplexität der Organisation und das Geschäftsmodell wesentliche Kriterien für die Festlegung des Umfangs und der Dauer des Compliance Monitorings. Hinzu kommen ggf. Vorgaben externer Standards, die für das Compliance System zu beachten sind."(abrufbar unter http://www.dnwe.de/complianceprogrammonitor.html, 18.05.2012).

7 Zusammenfassung

Die Überprüfung der Wirksamkeit des CMS ist für Unternehmen von wesentlicher Bedeutung, um die Haftungsrisiken und die wirtschaftlichen Risiken – wie z.B. Reputationsschäden im Falle von Compliance-Verstößen – zu begrenzen. Dabei kann die Überprüfung der Wirksamkeit sowohl durch eine interne als auch eine externe Instanz erfolgen. Eine „Testierung" der Wirksamkeitsprüfung des CMS nach IDW PS 980 mag durchaus für manchen Stakeholder die Glaubwürdigkeit der Berichterstattung von Vorstand/Aufsichtsrat unterstreichen. Allerdings sollte nach Ansicht des FCI – auch im Hinblick darauf, dass es sich bei den Prüfungen nach IDW PS 980 und CPM um freiwillige Prüfungsmöglichkeiten handelt – die externe Testierung nur eine Option darstellen. Eine „Best-Practice" dahingehend, dass einer externen Prüfung gegenüber der internen Prüfung ein Vorrang einzuräumen ist, sollte sich nach unserer Ansicht nicht entwickeln. Es muss vielmehr den Unternehmen weiterhin selbst überlassen bleiben, ob sie die Wirksamkeitsprüfung ihrer CMS von externer oder interner Stelle vornehmen lassen.

Vorstand und Aufsichtsrat müssen sich bewusst sein, dass auch ein Testat von externer Stelle nach PS 980 nicht per se zu einer Enthaftung führt. Denn weder durch Beachtung der veröffentlichten Prüfungsstandards noch durch ein Testat über eine externe Wirksamkeitsprüfung werden Unternehmen automatisch von der Haftung befreit. Vielmehr müssen Vorstand und Aufsichtsrat weiterhin vor Gericht beweisen, dass sie den für den Einzelfall ihres Unternehmens erforderlichen Überwachungspflichten nachgekommen sind.[20]

Wirksamkeitsprüfung kann nach unserer Ansicht nur bedeuten, ob die für die Organisation angemessen ausgestalteten und implementierten Elemente des CMS im Geschäftsalltag angewendet werden (Effectiveness Check). Dazu muss die geprüfte Compliance-Maßnahme bereits mindestens einmal ausgeführt worden sein. Bei der Prüfung der wirksamen Umsetzung kommt es darauf an, ob die Compliance-Maßnahme tatsächlich im Unternehmensalltag „gelebt" wird. Keinesfalls kann die Wirksamkeitsprüfung die Überprüfung beinhalten, ob sich Mitarbeiter an die inhaltlichen Vorgaben eines Code of Conduct halten. Denn eine derartige Prüfung ist, wie oben ausgeführt wurde, nicht möglich.

Im Ergebnis ist daher eine realistischere Wirksamkeitsdefinition, wie beispielsweise unter 5.1 dargelegt, erforderlich. Andernfalls könnte bei dem ein oder anderen Vorstand/ Aufsichtsrat durchaus ein falsches Verständnis hinsichtlich der Wirksamkeitsprüfung suggeriert werden, die die Prüfung nach PS 980 letztendlich nicht leisten kann und nicht leisten will.

[20] Böttcher: „Compliance: Der IDW PS 980 – Keine Lösung für alle (Haftungs-)Fälle!", NZG 2011, 1054.

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)

Grüninger, S.; Jantz, M.; Schweikert, C.; Steinmeyer, R. „Sorgfaltsbegriff und Komplexitätsstufen im Compliance Management“ (KICG-Forschungspapier Nr. 2/2012)

Schweikert, C.; Jantz, M. „Corporate Governance in Abhängigkeit von Unternehmensstruktur und Unternehmensgröße - eine betriebswirtschaftlich-juristische Analyse“ (Studie 1 im Forschungsprojekt „Leitlinien für das Management von Organisations- und Aufsichtspflichten“) (KICG-Forschungspapier Nr. 3/2012)

Grüninger, S.; Jantz, M.; Schweikert, C.; Steinmeyer, R. „Organisationspflichten - eine Synopse zum Begriffsverständnis und den daraus abzuleitenden Anforderungen an Aufsichts- und Sorgfaltspflichten aus juristischer und betriebswirtschaftlicher Perspektive“ (Studie 2 im Forschungsprojekt „Leitlinien für das Management von Organisations- und Aufsichtspflichten“) (KICG-Forschungspapier Nr. 4/2012)

Grüninger, S.; Jantz, M.; Schweikert, C. „Risk-Governance-Cluster-Cube“ (KICG-Forschungspapier Nr. 5/2013)

Grüninger, S.; Jantz, M.; Schweikert, C. „Begründung für die Festlegung der Größengrenzen zur Einteilung von Unternehmen in die verschiedenen Leitfäden“ (KICG-Forschungspapier Nr. 6/2013)

Jantz, M.; Grüninger, S. „Prüfung von Compliance-Management-Systemen“ (KICG-Forschungspapier Nr. 7/2013)