Compliance Management System (CMS)

Aus der Praxis

„Ausführungen zu einer CMS Studie und ein falsches Sicherheitsgefühl durch unterlassene Wirksamkeitsprüfung“

Februar 2014

Klaus-Dieter Krause

Dipl.-Inform., CISA, CISM, MBCI, ITILFZ, DSB, QAR-IT

compliance-net GmbH

An der Trift 65

63303 Dreieich

Inhaltsverzeichnis

Einleitung 3

Reaktive und Präventive Ausrichtung eines Compliance Management Systems 4

Ziele und Themengebiete eines Compliance Management Systems 8

Implementierung eines Compliance Management Systems.....10

Steuerung eines Compliance Management Systems.....11

Wirksamkeitsprüfung eines Compliance Management Systems 12

Prüfungsstandard des IDW zum Compliance Management.....14

Begutachtung eines Compliance Management Systems 16

Quellen.....18

Einleitung

Durch die immer weiter und schneller voranschreitende Globalisierung und die damit verbundene Vernetzung der Marktteilnehmer sind immer neue Fragestellungen und Herausforderungen in Bezug auf die Einhaltung gesetzlicher Massgaben sowie Unternehmensrichtlinien gesetzt, die es sowohl durch die Führung als auch durch die jeweiligen Aufsichtsorgane und Mitarbeiter einer Unternehmung zu erfüllen gilt.

Damit sowohl die Unternehmensführung als auch die Aufsichtsorgane diesen hohen Ansprüchen an ein Compliance Management System gerecht werden können, sollten die vielfältigen und häufig unternehmensspezifischen Konstellationen durch Ziele und Themengebiete strukturiert werden.

Damit einher sollte die Umsetzung eines den Anforderungen entsprechenden Berichtswesens sowie eine hinreichende Dokumentation, um den Nachweispflichten (vgl. u.a. IDW PS 980 [2]) gerecht zu werden, erfolgen.

Die nachfolgenden Ausführungen verdeutlichen sowohl die in einer Studie zum Thema Compliance Management System gewonnen Erkenntnisse als auch Beispiele für die fatalen Folgen ausgebliebener oder zu großmaschiger Wirksamkeitskontrollen im Zusammenhang mit einem Compliance Management System. Ferner werden Möglichkeiten aufgezeigt, wie diesen durch das Management eines Unternehmens entgegengewirkt werden kann.

Reaktive und Präventive Ausrichtung eines Compliance Management Systems

Grundsätzlich lassen sich zwei Arten der Ausrichtung eines Compliance Management Systems unterscheiden. Zum einen lässt sich das Handeln eines Unternehmens in Bezug auf ein Compliance Management durch eine vorbeugende (präventive) Ausrichtung definieren, zum anderen durch eine reaktive (abwartende) Ausrichtung.

Die präventive Ausrichtung eines Compliance Managements kann durch aktives Handeln der Beteiligten definiert werden. Das aktive Handeln soll dabei unterstützen, die Compliance Konzeption, Themen und Ziele wirksam in ein Unternehmen hinein zu tragen, das notwendige Bewusstsein zu generieren und damit eine nachhaltige Umsetzung zu gewährleisten.

Die reaktive Ausrichtung eines Compliance Management kann z.B. durch bedarfsorientiertes Handeln der Beteiligten definiert werden. Dabei werden auf Anfragen zu bestimmten Themen entsprechende Richtlinien ausgearbeitet und erlassen, in ein unternehmensinternes Intranet eingestellt und damit dem Mitarbeiter als bekannt gegeben betrachtet.

Der Mitarbeiter ist gefordert, sich selbständig über Neuerungen zu informieren (Holschuld). Einen Nachweis, dass der Mitarbeiter diese Richtlinien nicht kennen oder nicht verstanden haben, ist nicht gegeben – somit hat das Management im Zweifel Zeit gewonnen und muss nicht aufgrund von Fakten handeln. Das Handeln ist auf den Zeitpunkt verschoben, bis das Management durch Dritte dazu angehalten wird oder eine entsprechende Situation eingetreten ist.

Wenn ein aktives Compliance Management betrieben wird, muss sich das Management auch aktiv mit den Ergebnissen und Erkenntnissen auseinandersetzen. Das lässt sich ganz gut an einem Beispiel in Bezug auf die Verteilung und Bekanntmachung von neuen Richtlinien im Unternehmen verdeutlichen.

Setzt ein Unternehmen beispielsweise ein softwaregestütztes Tool zur Verteilung von neuen oder aktualisierten Richtlinien ein (z.B. das Produkt Policy Hub der Firma HiTec Laboratories, UK [10]), mit welchem, bei entsprechender Parametrisierung, sowohl die Kenntnisnahme als auch das Verständnis nachgewiesen werden kann, so ist möglicherweise damit auch die Notwendigkeit verbunden, sich mit den Personen auseinander zu setzen, welche die Richtlinien nicht gelesen oder verstanden haben.

Wird eine solche Software hingegen nicht eingesetzt, kann das Management des Unternehmens in erster Linie auf die Holschuld der Mitarbeiter verweisen (z.B. eingestellt im Intranet), hat aber keine tatsächlichen Nachweise über Kenntnisnahme und Verständnis der verabschiedeten Regelungen.

Der Nachweis in Bezug auf die Verteilung, zur Kenntnisnahme und dem Verständnis von Richtlinien und Weisungen wird durch die zuständigen Aufsichtsgremien immer weiter manifestiert und vorangetrieben, so dass die Vorgehensweise der reaktiven Verfahrensweise, zumindest in Bezug auf Finanzdienstleister und Versicherer, in Deutschland als auf dem Rückzug befindlich verstanden werden kann.

Grundsätzlich sollte ein Unternehmen auf ein aktives CMS abstellen. Aus der jüngeren Vergangenheit sind die nachfolgend aufgeführten Vorfälle als Beispiele für ein offensichtlich wenig aktiv ausgeprägtes CMS anzusehen, teilweise mit fatalen Folgen für die Gesellschaften, das Management und Einzelpersonen.

Hierbei ist insbesondere der Fall aus 2009 bei dem Nutzfahrzeughersteller MAN hervorzuheben, da in diesem Fall die Staatsanwaltschaft die offensichtlich zu lasche Auslegung des CMS als herausragenden Angriffspunkt gegen den Konzern nutzen konnte.

2003	**Heidelberg Cement, Zementkartell**	Sie trieben die Preise immer weiter künstlich in die Höhe: 2003 enttarnte das Bundeskartellamt das sogenannte Zementkartell. Heidelberg Cement muss die höchste Strafe zahlen – 170 Millionen Euro Bußgeld [13].
2005	**Infineon, Untreue-Skandal**	Bestechlichkeit, Untreue, Korruption: Im Juli 2005 erschüttert ein Skandal den Chip-Hersteller Infineon. Die Münchner Staatsanwaltschaft ermittelte gegen Infineon-Topmanager. Es kam zu Festnahmen, der zuständige Vorstand trat zurück [13].
2005	**Volkswagen, Bestechungsskandal**	Mit Reisen im Firmenjet und Luxus-Nutten brachte die Firmenleitung von Volkswagen seinen Betriebsrat auf Linie. 2005 wurde der Korruptionsskandal öffentlich, in dessen Folge auch der ehemalige Personalvorstand Peter Hartz, bekannt als der Namensgeber des Hartz-Konzept, zurücktrat. Auch gegen mehrere SPD-Politiker wurde Anklage erhoben [13].
2008	**Deutsche Telekom, Datenschutzskandal**	Eigene Manager, Aufsichtsräte, Journalisten– sie alle wurden von der Deutschen Telekom bespitzelt. 2008 flogen die illegalen Aktivitäten auf, eine hohe Geldbuße gab es für den ehemaligen Staatskonzern aber nicht. Dafür wurde der ehemalige Leiter der Abteilung Konzernsicherheit zu über drei Jahren Haft verurteilt [13].

2008	**Siemens, Schmiergeld-Skandal**	Es ging um über 4000 Schmiergeld-Zahlungen in fast alle Teile der Welt: Der Siemens-Konzern wurde nach seinem Korruptionsskandal 2008 in Europa und in den USA zu einer Strafe von insgesamt rund einer Milliarde Dollar verurteilt – die höchste Strafe, die es für einen Dax-Konzern jemals gab [13].
2009	**MAN, Korruptionsaffäre**	MAN musste 2009 wegen Bestechung ein Bußgeld von rund 150 Millionen Euro zahlen. Um beispielsweise an Aufträge für Busse zu kommen, hatte der Nutzfahrzeughersteller in Europa, Afrika und Asien Kunden bestochen. Bereits vor der Urteilsverkündung trat MAN-Vorstandschef Håkan Samuelsson zurück. Größter Angriffspunkt für die Staatsanwaltschaft: Die Compliance-Struktur in der Nutzfahrzeugsparte sei zu lasch gewesen [13].
2010:	**Daimler Benz, Bestechungsskandal**	Mal hat Daimler einem hohen Beamten in Turkmenistan eine gepanzerte S-Klasse im Wert von 300.000 Euro spendiert, mal Würdenträger in Indonesien in den Golfclub eingeladen. Als Strafe musste der Autohersteller 2010 in den USA insgesamt 185 Millionen Dollar zahlen. Über zehn Jahre wurden weltweit Regierungsbeamte mit Bargeld und Geschenken bestochen, um an lukrative Aufträge zu kommen - und das nicht nur im Ausland. Zum Zeitpunkt dieser Meldung in 2012 ermittelt die Staatsanwalt Stuttgart bereits wieder gegen Daimler-Mitarbeiter wegen Bestechung [13].
2011	**Deutsche Bank, Auslöser Finanzkrise**	Schauplatz New York: Wegen der Pleite von fünf US-Genossenschaftsbanken während der Finanzkrise musste die Deutsche Bank 145 Millionen Dollar zahlen. Das Finanzinstitut hat in einem außergerichtlichen Vergleich der Zahlung zugestimmt – für schuldig bekannte sich die Deutsche Bank allerdings nicht. (...). Nach einem Bericht des US-Senats soll die Bank auch wegen dieser Verkaufspraktiken neben Goldman Sachs und den Ratingagenturen einer der Hauptauslöser für die Finanzkrise gewesen sein. (…) [13].

2012	**ThyssenKrupp, Kartellverstöße**	Nach Skandalen um Luxusreisen mit Arbeitnehmervertretern und Journalisten, nach Kartellverstößen beim Handel mit Schienen und beim Aufzugsgeschäft gibt es nun einen neuen schwerwiegenden Verdacht: Der Stahlkonzern ThyssenKrupp,(…), soll auch bei seinem Brot- und Buttergeschäft, der Herstellung von Autoblechen im Stahlwerk in Duisburg-Bruckhausen gemogelt haben. Es lägen Hinweise auf wettbewerbswidrige Absprachen vor, heißt es 2013 bei den Ermittlungsbehörden [14]. Nachdem zuletzt der vormalige Chef des Bereiches Compliance bei TyssenKrupp, Jürgen Claasen, nach dem Skandal um die Luxusreisen mit Journalisten durch Heinrich Hiesinger (CEO) 2012 abberufen wurde, hat ThyssenKrupp seit Januar 2014 wieder einen neuen Compliance-Vorstand. Der Aufsichtsrat berief Herr Dr. Donatus Kaufmann zum neuen Leiter des Ressort „Recht & Compliance“ [15].
2014	**ADAC, Wahlfälschungen**	Als jüngstes Mitglied in diesem Kreis, verursacht durch Unregelmäßigkeiten bei der Leserwahl zum "Lieblingsauto 2014" hatten das Präsidium und der Verwaltungsrat des ADAC Ende Januar 2014 neben einer lückenlosen Aufklärung einen tiefgreifenden Reformprozess auf den Weg gebracht und die Geschäftsführung mit der Umsetzung beauftragt. Diese hat wiederum im Februar 2014 eine Anwaltskanzlei damit beauftragt, die bisherigen Compliance-Regelungen des ADAC umfassend zu überprüfen.

Diese Beispiele zeigen auf, warum ein präventives/aktives Vorgehen im Rahmen der Umsetzung und des „Lebens“ eines CMS der richtigere Weg zu einem nachhaltigen und Wirksamen CMS darstellt als ein reaktives Vorgehen.

Ziele und Themengebiete eines Compliance Management Systems

Als beiden Ansätzen gleich könnte ein einheitliches Verständnis über Ziele und Themengebiete des Compliance Managements in einem Unternehmen sein. Darauf verweist eine aktuelle Studie, die im Controller Magazin Jan./Febr. 2014 zu dem Thema veröffentlicht wurde [3].

Demnach sind sich 97% der befragten Unternehmen über die "Einhaltung relevanter regulatorischer Vorschriften" und die "Einhaltung interner Richtlinien" (87%) als Mittel zum Schutz der Unternehmensreputation (84%) als Ziel eines Compliance Managements einig.

Ziele des Compliance Managements *

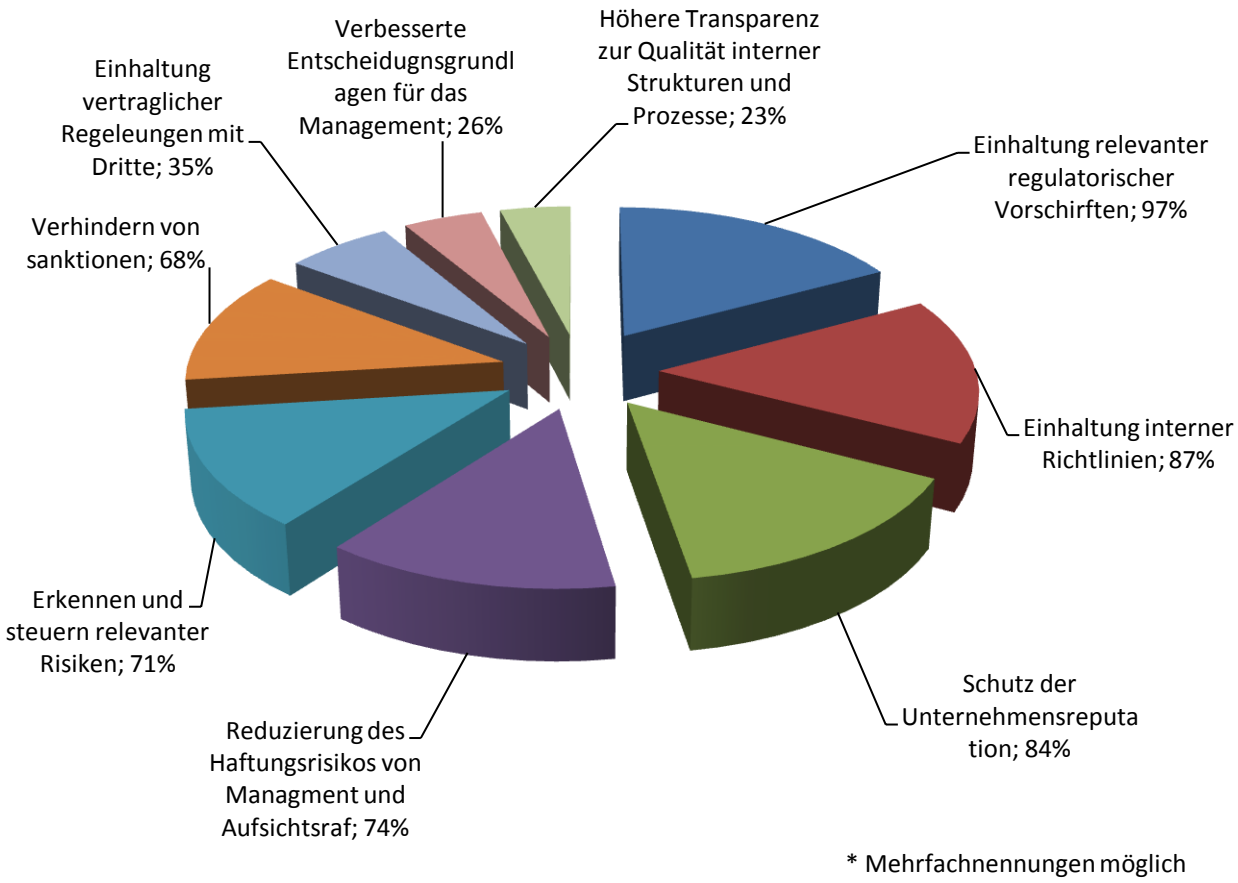


Abbildung 1 Ziele des Compliance-Management [1]

Erst an vierter Stelle, in Bezug auf die Ziele eine Compliance Managements wird mit 74% die "Reduktion des Haftungsrisikos von Management und Aufsichtsrat" genannt. Weitere

[1] Quelle: Vgl. Brühl, Kai und Humann, Nina; "Compliance Reporting – Ein Instrument der Unternehmenssteuerung?"; Controller Magazin Jan./Feb. 2014; Seite 13; 2014

wesentliche Triebfedern für ein Compliance Management sind das "Erkennen und steuern relevanter Risiken" (71%) sowie die "Vermeidung von Sanktionen" (68%).

Immerhin etwas mehr als 1/3 der antworteten Unternehmen haben angegeben, dass die Einhaltung vertraglicher Vereinbarungen zu den Zielsetzungen Ihres CMS gehört. In diesem Zusammenhang sei auf die Artikel „Prüfungsstandard für Outsourcing – Service Organization Control Report“[6], „Outsourcing: Berücksichtigung der Risiken und Kontrollen ausgelagerter Funktionen und Dienstleistungen im eigenen Governance – System“[7] , „Governance-System der Versicherungsunternehmen gemäß Solcency II“[8] und „Mindestanforderungen an das Risikomanagement für Investmentgesellschaften (InvMaRisk)“[9] verwiesen, die das Thema Outsourcing u.a. im Kontext zum Compliance Management weiter ausführen.

Die Themengebiete mit denen sich ein Compliance Management gemäss der Studie auseinandersetzt sind weit gestreut. Endend mit der "Unternehmenssicherheit" und "Produkthaftung", jeweils 19%, bis hin zu "Anti-Korruption (Bestechung und Bestechlichkeit)" mit 97% erstrecken sich die Anteile der einzelnen Themengebiete. Als zweithäufigstes Themengebiet wurde der Datenschutz mit 87% benannt. Mit fast 20% weniger folgt das "Wettbewerbsrecht & Verbandstätigkeit" [3]. Danach erst folgen Themen aus dem Finanzenbereich. Finanzberichterstattung / Steuerrecht / Bilanzpositionen (61%), Börden und Kapitalmarktrecht / Insiderhandel (52%) und Geldwäsche mit (48%). Interessanterweise ist das Themengebiet "IT Security" mit dem Themengebiet der "Geldwäsche" gleich häufig benannt worden [3].

Ebenfalls gleichauf mit jeweils 39% wurden die Themenbereiche "Vertragsmanagement" sowie "Aussenwirtschaftsrecht und Exportkontrolle" benannt [3]. Als weitere Themengebiete wurden genannt "Gesundheit, Sicherheit und Umwelt" (32%) sowie "Rollen und Berechtigungskonzept" (26%) und "Lizenzmanagement" mit 23% [3].

Normiert können die Themengebiete zusammengefasst und gefiltert werden, z.B. haben die stark IT-affinen Themengebiete (Datenschutz, IT Security, Rollen & Berechtigungsmanagement sowie Lizenzmanagement) einen Anteil von fast einem Drittel (27%). Gut die Hälfte der Themen (48%) lassen sich als Themen mit stark juristischer Ausprägung einstufen, wie z.B. Anti-Korruption, Wettbewerbsrecht & Verbandstätigkeit, Börsen und Kapitalmarktrecht / Insiderhandel, Vertragsmanagement, Aussenwirtschaftsrecht / Exportkontrolle und Produkthaftung. Themen aus dem Bereich Finanzberichterstattung / Steuerrecht / Bilanzmanipulation und Geldwäsche haben einen Anteil von 16%. Sonstigen Themen wie "Gesundheit, Sicherheit und Umwelt" sowie "Unternehmenssicherheit" schlagen mit 8% zu Buche, was sich durch die Struktur[2] der Befragungsteilnehmer erklären lässt.

[2] Studienteilnehmer nach Branchen: Manufacturing (35%), Financial Services (23%) sowie Telekom, Media, Utilities, Services & Logistics (42%)[3]
Studienteilnehmer nach Umsatz/Bilanzsumme: <= 1 Mrd. € (32%), <= 10 Mrd. € (48%), > 10 Mrd. € (20%)[3]

Implementierung eines Compliance Management Systems

Das nachfolgende Vorgehensmodell könnte Sie im Rahmen des Aufbaus bzw. der Implementierung eines CMS in Ihrem Unternehmen unterstützen bzw. Sie könnten dieses Vorgehensmodell mit Ihrem bestehenden abgleichen.

Das nachfolgend abgebildete Vorgehensmodell berücksichtigt die sieben grundlegenden Bausteine eines aus der Sicht des IDW angemessenen Compliance Management Systems und ist in den Artikeln „Das interne Kontrollsystem und das Risikomanagementsystem rücken durch das BilMoG stärker in den Blickpunkt“ [11] sowie „Implementierung eins Compliance-Management-Systems“ [4] näher beschrieben.

Abbildung 2 Prozessmodell zur Einführung eines CMS [4]

Weitere Literatur zu CMS Rahmenkonzepten finden Sie in dem Artikel „IDW PS 980: Linkliste zu den relevanten CMS Rahmenkonzepten“ [12] oder auf der Seite von zusammengestellten Rezensionen zu entsprechenden Büchern rund um das Thema Compliance. Die Aufstellung der Bücher finden sie hier und verschiedene Rezensionen zu den Themen finden Sie an dieser Stelle.

Steuerung eines Compliance Management Systems

Um ein Compliance Management in einem Unternehmen sachgerecht steuern zu können, ist neben einer sachgerechten Implementierung, umfassenden Befugnissen der Vertreter des CM und einer Kommunikationsstruktur sowohl ein entsprechendes Reporting als auch eine regelmäßige Wirksamkeitsprüfung der installierten Instrumentarien notwendig.

Gemäß der im Controller Magazin Jan/Feb 2014 [3] veröffentlichten Studie haben die Reportings an die Geschäftsführung, den Vorstand, den Aufsichtsrat, Prüfungsausschüsse und sonstige Gremien die in der nachfolgenden Grafik dargestellten Inhalte:

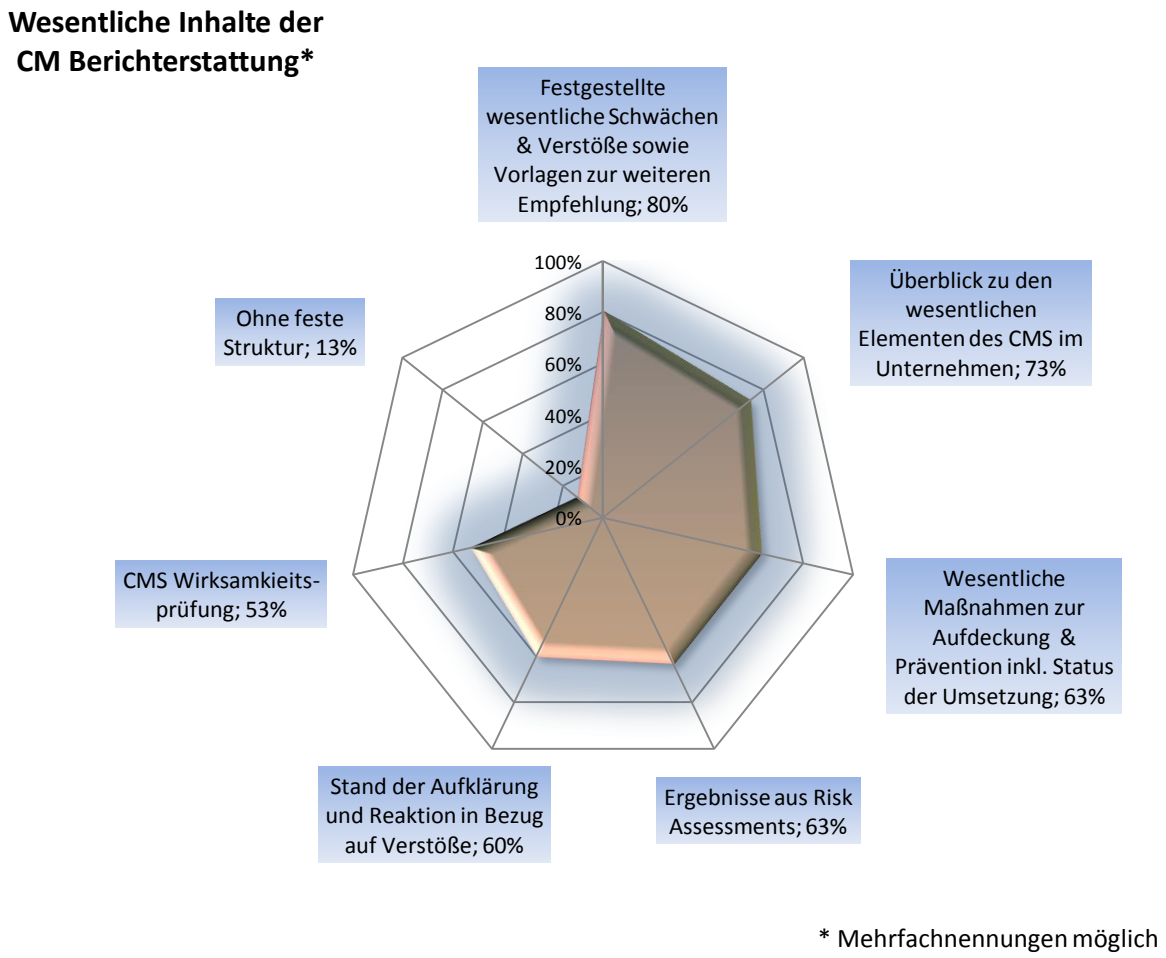


Abbildung 3 Wesentliche Berichtsbestandteile eines CMS [3]

[3] Quelle: Vgl. Brühl, Kai und Humann, Nina; "Compliance Reporting – Ein Instrument der Unternehmenssteuerung?"; Controller Magazin Jan./Feb. 2014; Seite 16; 2014

Wirksamkeitsprüfung eines Compliance Management Systems

Darüber hinaus kann auf Basis der zitierten Studie [4] festgehalten werden, dass nur bei 54% der befragten Unternehmen das Compliance Management vollumfänglich auf seine Wirksamkeit hin untersucht wird.

Bei 23% erfolgt dies nur teilweise und bei 23% der befragten Unternehmen überhaupt nicht. D.h. bei 23% der Unternehmen ist keine Aussage zur Handlungsfähigkeit beziehungsweise Effektivität des Compliance Managements möglich – es hat im schlimmsten Fall nur eine, meistens auch noch teure, Feigenblattfunktion.

Das bedeutet, dass Handlungsbedarf und Schwachstellen im Compliance Management unberücksichtigt und zumeist auch unbekannt bleiben.

Diese Erkenntnis lässt die These zu, dass sich die Unternehmensführungen von fast der Hälfte der an der Befragung teilgenommenen Unternehmen höchstwahrscheinlich in falscher Sicherheit wiegen, weil sie keine oder nur teileweise Wirksamkeitsüberprüfungen durchführen.

Diese These wird auch durch die im Kapitel *„Reaktive und Präventive Ausrichtung eines Compliance Management Systems“* angeführten Beispiele für die unzureichende Wirksamkeit von installierten Compliance Management Systemen als gestützt betrachtet werden. Hätten diese Unternehmen über ein wirksames Compliance Management Systemen verfügt, währe es vermeidlich nicht zu diesen Situationen bzw. in diesem beträchtlichen Ausmaß gekommen.

Von den Unternehmen, die sich mit der Frage der Wirksamkeit ihres Compliance Managements befassen, überprüfen 61% mindestens einmal pro Jahr die Wirksamkeit [3].

Von den 61% der Unternehmen wiederum, welche die Wirksamkeit jährlich überprüfen, tun dies 13% monatlich, 19% halbjährlich und 29 jährlich [3]. In wie weit hierbei durch die Unternehmen die Wirksamkeit des implementierten CMS geprüft wird (jeweils eine Vollprüfung oder die Prüfung von Teilbereichen) geht aus dem Veröffentlichten Sachverhalten der Studie nicht hervor.

16% der Unternehmen bevorzugen eine mehrjährig rotierende Prüfung der Wirksamkeit ihres Compliance Managements [3]. Dieser Zeitraum erscheint aufgrund der Schnelllebigkeit sowie der geforderten Reaktionszeiten des Managements eines Unternehmens als zu weit gefasst, um rechtzeitig steuernd durch das Compliance Management in die relevanten

[4] Quelle: Vgl. Brühl, Kai und Humann, Nina; "Compliance Reporting – Ein Instrument der Unternehmenssteuerung?"; Controller Magazin Jan./Feb. 2014; Seite 14; 2014

Geschäftsprozesse eingreifen zu können, wie es u.a. durch das AktG (§§ 93 und 107), GmbHG (§43) bzw. OWiG (§130), wenn teilweise auch nur indirekt, gefordert ist.

Wie Sie in Bezug auf Ihr Compliance Management System in Ihrem Unternehmen aufgestellt sind können Sie anhand einer kurzen, von der compliance-net GmbH, Dreieich erarbeiteten kostenlosen Diagnose in Bezug auf ihr Unternehmen ermitteln. Das Ergebnis erhalten Sie direkt nach Ihren Eingaben.

Prüfungsstandard des IDW zum Compliance Management

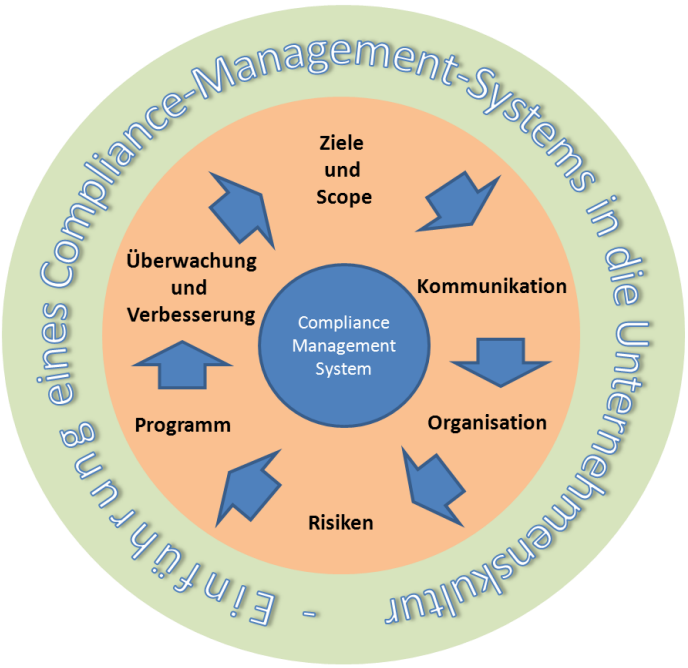
Der Prüfungsstandard des IDW PS 980 [2] benennt die nachfolgend genannten sieben grundlegenden Bausteine eines Compliance Management Systems

- Compliance-**Kultur** „Die Compliance-Kultur wird im Wesentlichen durch die Unternehmensleitung und das Management geprägt. Der sogenannte „tone at the top“ hat entscheidenden Einfluss auf die Wahrnehmung der Mitglieder einer Organisation im Hinblick auf das Thema Compliance. Wird das Thema offenkundig und erkennbar seitens des Managements nicht ernst genommen und Regelbruch nicht sanktioniert (gleich, auf welcher Hierarchieebene), dann ist eine hinreichende Akzeptanz kaum zu erwarten.“ [16]
- Compliance-**Ziele** „Ein CMS bezieht soll bestimmte Ziele erreichen, die vom verantwortlichen Management zu definieren sind. Ebenso ist zu definieren, welche Teile der Organisation vom CMS erfasst werden und welche Regeln im Fokus stehen. Diese Festlegungen korrespondieren mit den Risiken, die für die Einhaltung der entsprechenden Regeln bestehen und beziehen sich auf Regeln, die es je nach Einzelfall ebenfalls zu definieren gilt (s.u.).“ [16]
- Compliance-**Organisation** „Ein CMS wird durch eine zugehörige Organisation definiert und umgesetzt. Hierzu ist es erforderlich, die Definition von Rollen und Verantwortlichkeiten sowie der Aufbau- und Ablauforganisation vorzunehmen. Entsprechende Ressourcen sind erforderlich, um die Wirksamkeit zu gewährleisten.“ [16]
- Compliance-**Risiken** „Im Rahmen eines CMS werden die Risiken für die Erreichung der Ziele (s.o.) identifiziert und Maßnahmen zu deren angemessener Behandlung getroffen. Hierzu ist i.d.R. eine systematische Identifizierung und Beurteilung (Quantitativ und/oder Qualitativ) erforderlich.“ [16]
- Compliance-**Programm** „Das Compliance-Programm umfasst die Grundsätze und Maßnahmen, die die Begrenzung von Compliance-Risiken (und damit Regelverstöße) vermeiden sollen. Hierzu gehören auch die zu treffenden Maßnahmen bei festgestellten Verstößen.“ [16]

- Compliance-**Kommunikation** „Um eine erfolgreiche Implementierung des CMS sicherzustellen, ist eine sachgerechte Kommunikation an die betroffenen Personen (innerhalb und ggf. außerhalb der Organisation) erforderlich. Nur so können die im CMS und insbesondere im Compliance-Programm definierten Maßnahmen und Vorgehensweisen wirksam umgesetzt werden.“ [16]
- Compliance-**Überwachung und Verbesserung** „Um eine dauerhafte Eignung des Systems sicherzustellen und eventuelle Schwächen aufdecken zu können, erfolgt die Überwachung des CMS und die Umsetzung von identifiziertem Handlungsbedarf zu dessen Verbesserung. In der Praxis wird dies häufig durch eine interne Revision abgebildet, jedoch gibt es ggf. auch andere Informationsquellen zur Identifikation von Verbesserungsmöglichkeiten.“ [16]

als die wesentlichen, die im Sinne eines CMS definiert und implementiert sein müssen, damit ein CMS als angemessen gewertet werden kann.

Wie bei den meisten Standards lässt auch der Standard des IDW zum Compliance Management die hinreichende Freiheit zur individuellen Anpassung bzw. Ausgestaltung der einzelnen Bausteine in Bezug auf Ihr Unternehmen und lässt sich in einen Live Cycle einbinden.



CMS LifeCycle, © 2010 - compliance-net GmbH [4]

Begutachtung eines Compliance Management Systems

Die Fragen

- Wie gut ist mein Unternehmen in Bezug auf das CMS aufgestellt?
- Ist das CMS angemessen ausgestaltet?
- Ist das CMS in seiner Ausgestaltung wirksam?
- Wo weist das CMS noch Schwachstellen auf?

lassen sich in der Regel sowohl gegenüber unternehmensinternen als auch unternehmens-externen Aufsichtsorganen bzw. Investoren und Kunden durch eine externe Begutachtung glaubwürdig beantworten.

Darüber hinaus kann der Nachweis eines wirksamen und angemessenen CMS beispielsweise, wie auch der Nachweis eines entsprechend wirksamen Business Continuity Managements (BCM), im Rahmen von Geschäftsanbahnungen oder der Investorensuche den positiven Ausschlag für einen entsprechenden Abschluss geben.

Im Rahmen einer Begutachtung eines implementierten Compliance Management Systems stehen in der Regel die nachfolgenden drei Kernbereiche im Mittelpunkt:

- **Konzeption** Werden die sieben grundlegenden Bausteine des CMS Standards durch Ihr Unternehmen hinreichend ange-sprochen und sind die Aussagen des Unternehmens hierzu voll-ständig und auch zutreffend oder bestehen noch Lücken.
- **Angemessenheit** Ist die durch Ihr Unternehmen definierte Konzeption so in seinen Grundsätzen und Maßnahmen formuliert, geformt und imple-mentiert, dass Regelverstöße und Risiken rechtzeitig adressiert und daraus möglicherweise resultierende Verstöße vermieden werden.
- **Wirksamkeit** Wurde das CMS, basierend auf der Konzeption und der anschließenden Implementierung, so in Ihrem Unternehmen um-gesetzt, dass die Grundsätze und Maßnahmen hinreichende Beachtung durch die Mitarbeiter Ihres Unternehmens, im Rahmen des Durchlaufens Ihrer Geschäftsprozesse, erfahren. Hierbei sind unter andrem auch die Reaktionsfähigkeit sowie das Kommunikationsmanagement zu betrachten.

Im Innenverhältnis können Vorstände, Geschäftsführungen, Aufsichtsräte oder Beiräte eine Begutachtung ihres unternehmensbezogenen Compliance Management Systems gleichermaßen als Nachweis für die Implementierung ein vermeidlich effektiven CMS nutzen. Aufsichtsräte oder Beiräte einer Unternehmung können damit u.a. auch die Einhaltung ihrer Prüfungspflichten, vgl. z.B. §107 Abs. 3 AktG, darlegen.

Gerne können Sie den Autor oder seine Kollegen zu diesem Thema kontaktieren.

Klaus-Dieter Krause
Geschäftsführer
compliance-net GmbH

Kontaktdaten zum Download:
http://www.compliance-net.com/kontaktdaten

Quellen

[1] Aktiengesetz (AktG) in der Fassung vom 23.07.2013; http://www.gesetze-im-internet.de/bundesrecht/aktg/gesamt.pdf; 2013, Link zugegriffen am 19.2.2014

[2] IDW PS 980 „Prüfungsstandard, Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen“ (Quelle: WPg Supplement 2/2011, S. 78 ff., FN-IDW 4/2011, S. 203 ff.), vom 11.03.2011 (Stand), herausgegeben vom Institut der Wirtschaftsprüfer; http://www.idw.de/idw/portal/n281334/n281114/n302246/index.jsp; 2011, Link zugegriffen am 19.2.2014

[3] Brühl, Kai und Humann, Nina; "Compliance Reporting – Ein Instrument der Unternehmenssteuerung?"; Controller Magazin Jan./Feb. 2014; Seite 12 bis 17; 2014

[4] Krause, Klaus-Dieter; „Implementierung eines Compliance-Management-Systems“; www.compliance-net.de, ISSN 2192-3515; 2010, Link zugegriffen am 19.2.2014

[5] Krause, Klaus-Dieter; „Bücherauswahl rund um das Thema ‚Compliance‘“; www.compliance-net.de; ISSN 2192-3515; 2010, Link zugegriffen am 19.2.2014

[6] Bacht, Günter; “Prüfungsstandard für Outsourcing – Service Organization Control Report“, www.compliance-net.de; ISSN 2192-3515, 2012, Link zugegriffen am 19.2.2014

[7] Karamitros, Ioannis; „Outsourcing: Berücksichtigung der Risiken und Kontrollen ausgelagerter Funktionen und Dienstleistungen im eigenen Governance – System“, www.compliance-net.de; ISSN 2192-3515; 2012, Link zugegriffen am 19.2.2014

[8] Karamitros, Ioannis; „Governance-System der Versicherungsunternehmen gemäß Solcency II“; www.compliance-net.de; ISSN 2192-3515; 2012, Link zugegriffen am 19.2.2014

[9] Krause, Klaus-Dieter; „Mindestanforderungen an das Risikomanagement für Investmentgesellschaften (InvMaRisk)“; www.compliance-net.de; ISSN 2192-3515; 2010, Link zugegriffen am 19.2.2014

[10] ohne Angabe zum Verfasser; „Policy Management mit PolicyHub“; www.compliance-net.de; ISSN 2192-3515; 2013, Link zugegriffen am 19.2.2014

[11] Bartonitz, Dr. Martin; "Das interne Kontrollsystem und das Risikomanagementsystem rücken durch das BilMoG stärker in den Blickpunkt"; http://www.saperionblog.com/lang/de/das-interne-kontrollsystem-und-das-risikomanagementsystem-rucken-durch-das-bilmog-starker-in-den-blickpunkt/1989/; 2010, Link zugegriffen am 19.2.2014

[12] Meyer, Sören A.; „IDW PS 980: Linkliste zu den relevanten CMS Rahmenkonzepten“; www.compliance-net.de; ISSN 2192-3515; 2013, Link zugegriffen am 19.2.2014

[13] Handelsblatt;„Die größten Skandale in deutschen Konzernen. Korruption, Kartell, Datenmissbrauch: In den großen deutschen Unternehmen haben Ermittler und Journalisten in den vergangenen Jahren viele Verstöße entdeckt. Die zehn größten Skandale im Überblick“; 16.05.2012: Link zugegriffen am 20.02.2014

[14] Wirtschafts Woche;„Razzia bei ThyssenKrupp“; 28.02.2012, Link zugegriffen am 20.02.2014

[15] finance-magazin;„Donatus Kaufmann neuer Compliance-Chef bei ThyssenKrupp“; 20.01.2014; Link zugegriffen am 20.02.2014

[16] Hesselbach, Sven;„Elemente eines Compliance Management Systems“; www.compliance-net.de; ISSN 2192-3515; 2010, Link zugegriffen am 20.02.2014

[17] na presseportal;„Freshfields startet Überarbeitung der Compliance-Strukturen des ADAC“; 19.02.2014; Link zugegriffen am 20.02.2014