Michael Beyer | Reinhard Heyd

Compliance für Aufsichtsräte

Rechtliche und fachliche Anforderungen an die Finanzexpertise

SCHÄFFER
POESCHEL

Compliance für Aufsichtsräte

Michael Beyer/Reinhard Heyd

Compliance für Aufsichtsräte

Rechtliche und fachliche Anforderungen an die Finanzexpertise

1. Auflage

Schäffer-Poeschel Verlag Stuttgart

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de/ abrufbar.

Print: ISBN 978-3-7910-4962-5 Bestell-Nr. 17208-0001
ePub: ISBN 978-3-7910-4963-2 Bestell-Nr. 17208-0100
ePDF: ISBN 978-3-7910-4964-9 Bestell-Nr. 17208-0150

Michael Beyer/Reinhard Heyd
Compliance für Aufsichtsräte
1. Auflage, Juni 2021

www.schaeffer-poeschel.de
service@schaeffer-poeschel.de

Bildnachweis (Cover): © EtiAmmos, AdobeStock

Produktmanagement: Kühn, Alexander
Lektorat: Susanne Mall | www.conscripto.de

Schäffer-Poeschel Verlag Stuttgart
Ein Unternehmen der Haufe Group

Vorwort

Sehr geehrte Leserinnen und Leser,

das Gesetz zur Umsetzung der zweiten Aktionärsrechterichtlinie (ARUG II), das Gesetz zur Stärkung der Finanzmarktintegrität (FISG), das Verbandssanktionengesetz sowie die EU-Hinweisgeberrichtlinie und viele weitere in Umsetzung befindliche oder sich bereits abzeichnende Vorgaben rücken Compliance immer mehr in den Fokus der guten Unternehmensführung durch das Management sowie der Überwachung und Beratung durch die Aufsichts-, Verwaltungs- und Beiräte der betroffenen Unternehmen.

Längst bilden sich auch innerhalb der Compliance verschiedene Schwerpunkte heraus, die unterschiedlichste Kompetenzen erfordern. Der Umgang mit dem Thema Korruption von der initialen Vermeidung bis hin zur Verknüpfung in die Managementsysteme der Organisation stellt an die verantwortlichen und handelnden Personen ganz andere Anforderungen als beispielsweise die Implementierung eines angemessenen Datenschutzmanagementsystems oder eines Tax-CMS. Dennoch sollte das Zielbild bei allen genannten Themen identisch sein: nämlich, »compliant« zu sein.

Vor dem Hintergrund dieser Compliance-Disziplinen und Anregungen aus unserer beruflichen Praxis sind die Idee und das Anliegen entstanden, eine weitere Disziplin zu benennen, abzugrenzen und den Leserinnen und Lesern mittels verständlicher Darstellungen und vieler Schaubilder zugänglich zu machen. Es geht um die **Finanz-Compliance**, welche ein Kernthema für die Überwachungsorgane sein sollte.

Wir würden uns freuen, wenn »Compliance für Aufsichtsräte« mit diesem speziellen Fokus auf die Finanzthemen eine wertvolle Hilfe für Ihre Mandatsarbeit wird und auch den sonstigen interessierten Leserinnen und Lesern neue Erkenntnisse bringt sowie als Nachschlagewerk dient.

Sehr herzlich möchten wir uns bei Herrn Markus Mai für die Unterstützung bedanken sowie beim Schäffer-Poeschel Verlag, insbesondere bei Frau Marita Mollenhauer, und allen involvierten Kolleginnen und Kollegen.

Berlin/Ulm, im Mai 2021
Michael Beyer und Reinhard Heyd

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Grundlagen

1.1 Begriffsdefinitionen

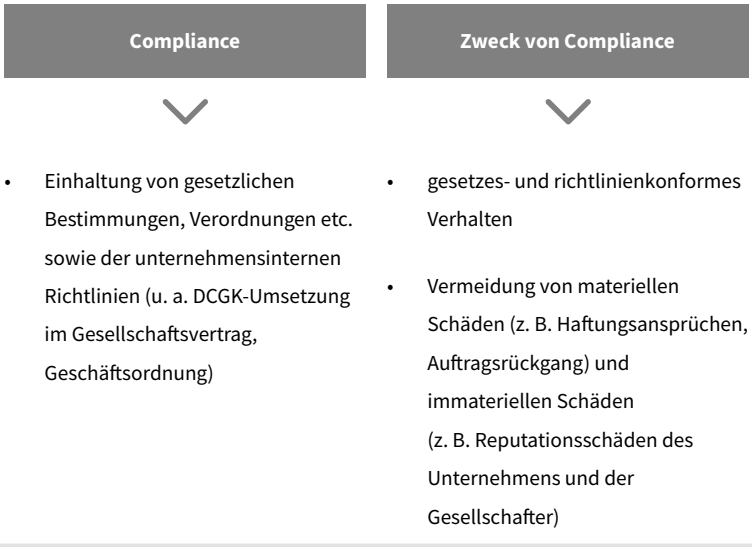

Abb. 1-1: Begriffsklärung

Der Begriff der »Compliance« wird derzeit zunehmend breiter verwendet und ist insbesondere aufgrund der medialen Aufmerksamkeit der letzten Jahre von besonderer Relevanz.

Dies liegt u. a. an den zahlreichen Fällen von Korruption, kartellrechtswidrigen Absprachen und sonstigen Regelverstößen, welche teils auf der Ebene des Topmanagements der Unternehmen begangen oder zumindest von ihm geduldet wurden. Das zeigt, dass »Compliance« ein Kernthema der Aufsichtsratsarbeit darstellt und dass das Überwachungsorgan die Entscheidungen des Vorstandes auf Rechtmäßigkeit prüfen und beurteilen sowie sich mit den Compliance-Risiken des Unternehmens beschäftigen muss.

Oftmals wird »Compliance« mit dem Begriff der »Haftungsvermeidung« übersetzt und beide werden als Synonyme erachtet. Das ist jedoch nicht zutreffend, da »Compliance« die Einhaltung von Regelungen, welche sich aus externen und internen Vorgaben ergeben, meint.

Zu den externen Bestimmungen zählen gesetzliche Regelungen. Hierbei können beispielsweise folgende angeführt werden:
- Gesetze,
- Verordnungen,
- etc.

Demgegenüber können sich bei Gesellschaften unternehmensinterne Richtlinien u. a. aus der Umsetzung des Deutschen Corporate Governance Kodex (DCGK) im Gesellschaftsvertrag, der Geschäftsordnung, dem Organisationshandbuch oder aus sonstigen unternehmensinternen Richtlinien sowohl für den Aufsichtsrat als auch für den Vorstand und die Belegschaft ergeben.

Folglich besteht der Zweck der Compliance darin, einerseits ein rechtswidriges Verhalten (z. B. Missachtung von Regelungen) zu verhindern und andererseits ein rechtmäßiges Verhalten (z. B. interne Meldung von möglichen Compliance-Verstößen) zu fördern. Hierdurch werden in dem Unternehmen Rahmenbedingungen geschaffen, durch die die einschlägigen Gesetze und Richtlinien eingehalten und mögliche Schäden vermieden werden (sollen). Als Schäden sind hierbei sowohl Schäden materieller als auch immaterieller Art zu nennen. Schäden von materieller Art, d. h. Schäden, die in Geld messbar sind, können in diesem Zusammenhang in der Durchsetzung von möglichen Haftungsansprüchen gegen das Unternehmen oder seine Organe bestehen. Denkbar sind auch ein möglicher Auftragsrückgang und daraus folgende Umsatz- und Gewinneinbrüche. Bei den immateriellen Schäden können zunächst mögliche Reputationsschäden bzw. Imageschäden des Unternehmens eintreten. Diese können wiederum materielle Schäden, wie den bereits benannten Auftragsrückgang, zur Folge haben. Bei den immateriellen Schäden kann es sehr herausfordernd sein, nach einem Compliance-Verstoß die vorher gute Reputation wieder aufzubauen. Da die Bußgelder für Compliance-Verstöße sehr hoch sein können und teils auch umsatzbezogen berechnet werden (z. B. bei illegalen Preisabsprachen), kann es dazu kommen, dass sie sich existenzbedrohend auf das Unternehmen auswirken.

Dies verdeutlicht, wie wichtig die Überwachung der Einhaltung der geltenden Regelungen sein kann.

Compliance meint somit zum einen die Legalitätspflicht des Vorstandes und zum anderen die Legalitätskontrolle durch den Aufsichtsrat.

Der Vorstand ist im Rahmen seiner Legalitätspflicht zum einen dazu verpflichtet, selbst keine Gesetzesverstöße zu begehen oder anzuordnen. Zum anderen hat er dafür Sorge zu tragen, dass das Unternehmen so organisiert ist und so beaufsichtigt wird, dass es zu keinen derartigen Gesetzesverletzungen in der Organisation (z. B. durch nachgeordnete Mitarbeiter) kommt. Dies ergibt sich nach der h. M. aus der Leitungs- und Organisationspflicht des Leitungsorgans, welche aus den §§ 76, 93 AktG folgt. Eine Konkretisierung der genannten Verpflichtung erfolgt durch § 91 Abs. 2 AktG, welcher den Vorstand dazu verpflichtet, ein Risikofrüherkennungssystem einzurichten, welches bestandsgefährdende Entwicklungen frühzeitig erkennt. Zu den bestandsgefährdenden Entwicklungen können auch mögliche Verstöße gegen gesetzliche Vorschriften gehören, wenn diese bestandsgefährdende Auswirkungen haben können.

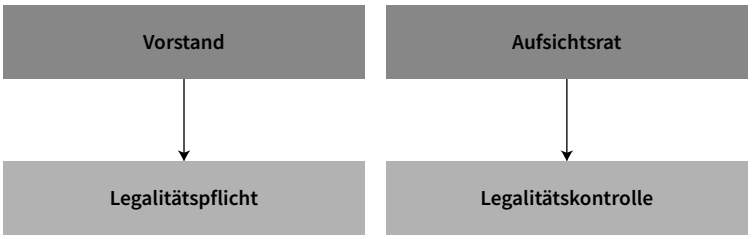

Abb. 1-2: Was meint Compliance?

Die Sicherstellung der Legalitätspflicht liegt in der Gesamtverantwortung des Vorstandes. Hieran ändert eine Delegation nichts.

Die Aufgabe des Aufsichtsrats ist nicht auf die Überwachung des Vorstandes hinsichtlich Zweckmäßigkeit und Wirtschaftlichkeit des Handelns beschränkt, sondern umfasst auch die Kontrolle der Rechtmäßigkeit des Handelns (sog. Rechtmäßigkeitskontrolle oder auch Legalitätskontrolle).

Der Aufsichtsrat hat im Hinblick auf die Compliance zu überprüfen, ob die von dem Vorstand eingeleiteten Compliance-Maßnahmen angemessen, effizient und effektiv sind. Ist dies nicht der Fall, so muss der Aufsichtsrat entsprechende Maßnahmen von dem Vorstand fordern. Weiterhin erstreckt sich die Überwachungspflicht des Gremiums auf die Überwachung, Steuerung, Pflege und Weiterentwicklung der genannten Maßnahmen durch das Leitungsorgan. Bestehen diesbezüglich Bedenken aufseiten des Aufsichtsrats, so sind diese darzulegen und mit dem Vorstand zu erörtern. Gegebenenfalls ist zu überlegen, ob Zustimmungsvorbehalte in Bezug auf bestimmte Compliance-Maßnahmen einzuführen sind, damit der Aufsichtsrat hierdurch seine Vorstellungen durchsetzen kann. Sollte es dazu kommen, dass die regelmäßigen Berichte des Vorstandes unzureichend sind oder Zweifelsfragen aufwerfen, hat der Aufsichtsrat von seinem Recht auf Erstellung eines Sonderberichts (§ 90 Abs. 3 AktG) bzw. auf Einsicht oder Prüfung (§ 111 Abs. 2 Sätze 1 und 2 AktG) Gebrauch zu machen. Kommt es zu möglichen Compliance-Verstößen in dem Unternehmen, so ist es die Aufgabe des Aufsichtsrats, sich regelmäßig über den aktuellen Stand der von dem Vorstand eingeleiteten Ermittlungen informieren zu lassen sowie dessen Vorgehen zu überwachen. Die Kontrolldichte bzw. die Intensität der Überwachung ist hierbei vom konkreten Fall abhängig.

1.2 Stellung in der Governance

Um den Begriff der »Compliance« bzw. des »Compliance-Managements« einzuordnen, ist eine Abgrenzung zu den anderen Governance-Bereichen vorzunehmen. Hierbei ist jedoch zu erwähnen, dass eine trennscharfe Abgrenzung nicht immer möglich ist.

Ein Beispiel hierfür ist ein Compliance-Verstoß, da er ein Risiko (beispielsweise Verhängung hoher Bußgelder) darstellt und somit auch der Behandlung im Risikomanagement zuzuordnen ist.

Unterschieden werden sollen im Folgenden:
- das Compliance-Management,
- das Risikomanagement und
- das Interne Kontrollsystem.

Die Aufgabe des *Compliance-Managements* besteht in der Erkennung, Überwachung und Steuerung aller wesentlichen Risiken, die die Nichteinhaltung interner und externer Regeln betreffen. Hiervon abzugrenzen ist das Compliance-Management-**System**, welches nicht rein technisch zu verstehen ist und alle Maßnahmen und Regelungen (technisch, organisatorisch, manuell) inklusive Kultur, Reporting etc. umfasst.

Eine Verpflichtung zur Einrichtung eines solchen Systems kann sich zum einen aus den individuellen Risikoparametern der Gesellschaft, wie z. B. der Größe und Organisation des Unternehmens, der Branchenzugehörigkeit und den Compliance-Verstößen in der Vergangenheit, und zum anderen aus unternehmensinternen Regelungen, wie beispielsweise der verpflichtenden Umsetzung des DCGK in der Satzung der Gesellschaft, ergeben.

Das *Risikomanagement* im Unternehmen ist für jegliche Maßnahmen zur Erkennung, Bewertung und Überwachung aller wesentlichen Risiken sowie die diesbezügliche Kommunikation verantwortlich. Von besonderer Bedeutung sind hierbei wirtschaftliche Risiken (wie z. B. die Wettbewerbsfähigkeit des Unternehmens oder Prozessrisiken). Die gesetzliche Mindestanforderung ist hierbei, dass Gesellschaften in Form der Aktiengesellschaft, der Gesellschaft mit beschränkter Haftung, der Kommanditgesellschaft auf Aktien sowie diesen gleichgestellte Gesellschaftsformen ein Risikofrüherkennungssystem einzurichten haben, welches bestandsgefährdende Entwicklungen erkennt und es möglich macht, Abwehrmaßnahmen einzuleiten. Darüber hinaus kann sich aus der Unternehmensgröße und -komplexität sowie aus Spezialgesetzen (z. B. gem. § 25a Abs. 1 Satz 3 KWG) eine Verpflichtung zur Einrichtung eines umfassenden Risikomanagementsystems ergeben, welches für Risikoinventur, -klassifizierung, -steuerung, -controlling und -reporting verantwortlich ist.

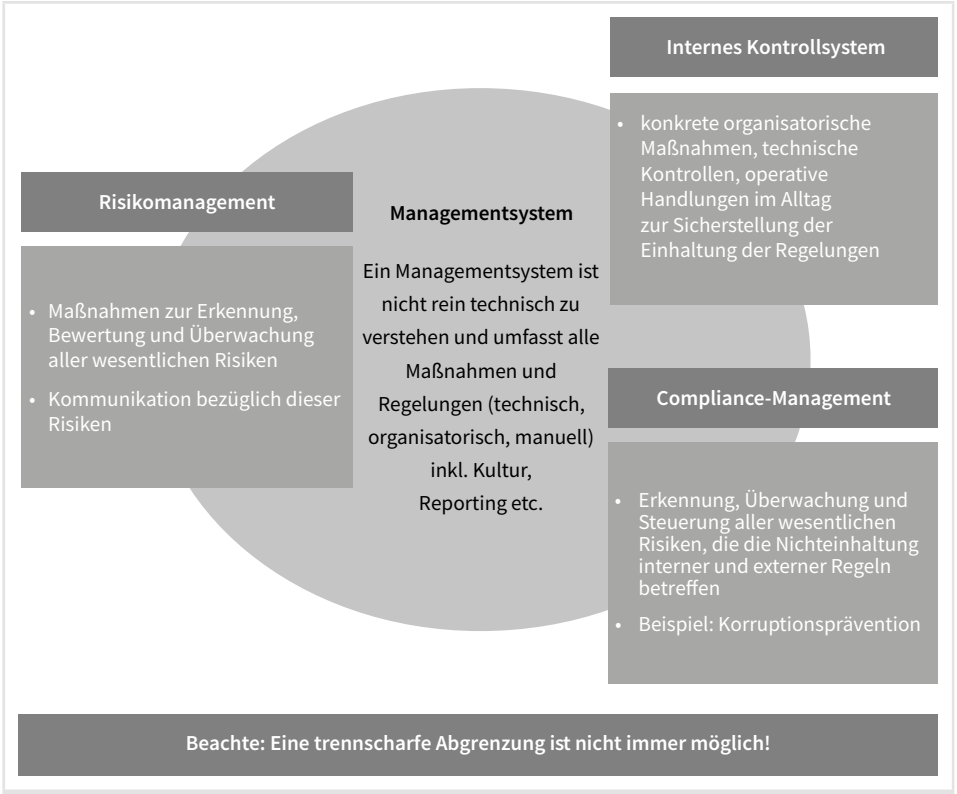

Abb. 1-3: Abgrenzung des Compliance-Managements gegenüber anderen Aufgaben in der Unternehmensüberwachung

Das *Interne Kontrollsystem* beinhaltet als Oberbegriff der Steuerungs- und Überwachungssysteme des Unternehmens alle prozessimmanenten und prozessunabhängigen Aktivitäten zur Erfassung, Analyse, Bewertung, Überwachung und Kontrolle operativer und strategischer Prozesse, der Wirtschaftlichkeit, der Rechnungslegung und der Compliance.

Dazu zählen beispielsweise Zutrittskontrollen oder das »Vier-Augen-Prinzip« bei Zahlungsfreigaben.

Da das Compliance-Management und das Risikomanagement einander im Kern sehr stark ähneln, weil sich beide Bereiche mit der Vermeidung und Steuerung von Risiken auseinandersetzen, sind sie nochmals in drei Punkten voneinander abzugrenzen, und zwar auf der organisatorischen und der inhaltlichen Ebene sowie bei der Zielsetzung.

In organisatorischer Hinsicht sind beide Bereiche in der Regel in zwei unterschiedlichen Abteilungen o. Ä. angesiedelt.

So wird es meist einen Compliance- und einen hiervon getrennten Risikomanager im Unternehmen geben. Weiterhin sind häufig die Anforderungen an die zu besetzenden Positionen andere. So wird der Compliance-Manager für gewöhnlich einen juristischen Hintergrund und der Risikomanager einen betriebswirtschaftlichen Background haben.

Beide setzen sich mit der Risikoprävention, -steuerung und -verhinderung auseinander. Bei dem Compliance-Management liegt der Fokus jedoch auf den Risiken, die aus Regelbrüchen resultieren. Zu diesen gehören beispielsweise:

- etwaige Haftungsansprüche,
- Bußgelder,
- Strafverfahren.

Demgegenüber geht es beim Risikomanagement z. B. auch um Marktpreis-, Finanz- oder Liquiditätsrisiken. Weiterhin liegt der Fokus beim Risikomanagement auf den wirtschaftlichen Risiken sowie der Gesamtrisikosteuerung und -berichterstattung.

Bezogen auf die Zielsetzung des Compliance-Managements und des Risikomanagements haben beide zunächst die gemeinsame Intention, etwaige Schäden der Gesellschaft abzuwenden. Das Compliance-Management geht jedoch über das Risikomanagement dahingehend hinaus, dass es nicht bei der Erkennung, Bewertung, Überwachung und Kommunikation der Risiken bleibt. Es strebt vielmehr danach, zusätzlich in dem Unternehmen eine gewisse Compliance-Kultur zu schaffen, interne Meldekanäle einzurichten und Compliance-Verstöße unternehmensintern angemessen zu sanktionieren (z. B. durch Kündigung des betreffenden Mitarbeiters).

In der Praxis liefert das Compliance-Management oft dem Risikomanagement zu. Angemerkt sei allerdings, dass auch die Risiken, die beim Risikomanagement im Fokus stehen, im Risikohandbuch und in Risikorichtlinien niedergelegt sind, sodass sie ihrerseits Teil von »verbindlichen Vorgaben« sind. Hieraus folgt, dass Verstöße gegen das Risikohandbuch und gegen die Risikorichtlinie zugleich Compliance-Verstöße darstellen.

Es zeigt sich somit, dass, wie bereits eingangs dargestellt, eine strikte Trennung zwischen den einzelnen Funktionsbereichen nicht möglich ist.

Dies führt u. a. dazu, dass es mittlerweile viele integrierte Ansätze gibt, bei denen das Compliance-Management-System, das Risikomanagement und das Interne Kontrollsystem auf der System- und/oder auf der Reportingebene einen gemeinsamen Output haben. Hierdurch sollen Redundanzen vermieden werden.

1.3 Finanz-Compliance

Abb. 1-4: Überblick zu einem vereinfachten Rechnungslegungsprozess

Im Bereich der Finance-Compliance sind insbesondere folgende Themenbereiche für den Aufsichtsrat bedeutsam:

- Jahresabschluss,
- Überwachung des Rechnungslegungsprozesses,
- Tax Compliance.

Alle Kaufleute nach §§ 1 ff. HGB haben einen Jahresabschluss, bestehend aus einer Bilanz und einer Gewinn- und Verlustrechnung, zu erstellen (vgl. § 242 Abs. 3 HGB). Kapitalgesellschaften haben diesen um einen Anhang zu erweitern. Die Bilanz, die Gewinn- und Verlustrechnung und der Anhang bilden als Einheit den »Jahresabschluss der Kapitalgesellschaften« (§ 264 Abs. 1 Satz 1 HGB). Mittelgroße und große Kapitalgesellschaften haben den »Jahresab-

schluss der Kapitalgesellschaften« um den Lagebericht zu erweitern, der ein eigenständiges Rechnungslegungsinstrument darstellt (§ 264 Abs. 1 Satz 1 HGB). Kapitalmarktorientierte Kapitalgesellschaften haben zusätzlich einen Eigenkapitalspiegel und eine Kapitalflussrechnung aufzustellen. Sie können den Jahresabschluss um einen Segmentbericht erweitern (§ 264 Abs. 1 Satz 2 HGB), wobei zu berücksichtigen ist, dass die vorgenannte Verpflichtung nur für kapitalmarktorientierte Kapitalgesellschaften gilt, die nicht zur Aufstellung eines Konzernabschlusses verpflichtet sind.

Der Aufsichtsrat hat den Jahresabschluss, den Lagebericht sowie den Vorschlag für die Verwendung des Bilanzgewinns zu prüfen und den Jahresabschluss festzustellen (§§ 171, 172 AktG). Prüfungsgegenstand sind die entsprechenden Vorlagen des Vorstandes nach § 170 Abs. 1 und 2 AktG. Ergänzend steht dem Aufsichtsrat das Einsichts- und Prüfungsrecht des § 111 Abs. 2 AktG zu Gebote. Das Überwachungsorgan ist stets berechtigt und bei Verdacht auf Unregelmäßigkeiten auch verpflichtet, von diesen Befugnissen Gebrauch zu machen. Ist die Gesellschaft zur Aufstellung eines Konzernabschlusses verpflichtet (§ 290 Abs. 1 und 2 HGB), so erstreckt sich die Prüfungspflicht auch auf den Konzernabschluss (§ 297 HGB) und den Konzernlagebericht (§ 315 HGB).

Im Hinblick auf die Prüfungsmaßstäbe hat das Überwachungsorgan den Jahresabschluss, den Lagebericht und den Gewinnverwendungsvorschlag auf Rechtmäßigkeit und Ordnungsmäßigkeit sowie auf Wirtschaftlichkeit und Zweckmäßigkeit zu prüfen. Weiterhin ist der Aufsichtsrat einer AG für die Billigung des Jahresabschlusses zuständig, es sei denn, es greift eine der Ausnahmen nach §§ 173, 234 Abs. 2, 270 AktG.

In Bezug auf die Überwachung des Rechnungslegungsprozesses (siehe Abbildung 1-4 für einen vereinfachten Rechnungslegungsprozess) hat der Aufsichtsrat im Rahmen seiner Überwachungspflicht zu prüfen, ob der Rechnungslegungsprozess von dem Vorstand pflichtgemäß eingerichtet wurde und die Wirksamkeit gegeben ist. Ist dies nicht der Fall, so hat der Aufsichtsrat entsprechende Anpassungen einzufordern (§ 107 Abs. 3 Sätze 2 und 3 AktG).

Das Tax-Compliance-Management-System ist der Bereich eines Compliance-Management-Systems (CMS), welcher sich mit der regelkonformen Behandlung von sämtlichen Steuern befasst, wie z. B. der Körperschaftssteuer, der Gewerbesteuer etc. (einschließlich sämtlicher steuerlicher Nebenleistungen, beispielsweise Verspätungszuschlägen).

Zweck ist es, dass dadurch alle steuerrechtlichen Pflichten der Gesellschaft auf allen Ebenen der Organisation ordnungsgemäß erfüllt werden und mögliche Risiken wie z. B. Strafverfahren vermieden werden. Unter die zu erfüllenden Pflichten der Gesellschaft kann u. a. die fristgerechte und inhaltlich korrekte Abgabe der Steuererklärung subsumiert werden.

Als weiterer Zweck des Tax-CMS kann genannt werden, dass durch es ermöglicht werden soll, die gesetzlich eingeräumten Möglichkeiten zur Verringerung der Steuerlast zu nutzen und somit auf legale Weise einen höheren Gewinn (nach Abzug der Steuern) zu realisieren.