Sarbanes-Oxley und Corporate Compliance

Nachhaltigkeit, Optimierung, Integration

Bearbeitet von
Christof Menzies

1. Auflage 2009 2006. Buch. XXIV, 506 S. Hardcover
ISBN 978 3 7910 2490 5
Format (B x L): 17 x 24 cm
Gewicht: 1103 g

I Corporate Compliance in einem dynamischen Umfeld

Das Thema »Compliance« besitzt in der heutigen Unternehmenswelt große Bedeutung und genießt hohe Aufmerksamkeit. Die Einhaltung von Gesetzen, von regulatorischen Vorgaben oder auch von freiwilligen Verpflichtungen gegenüber den Stakeholdern hat nicht zuletzt nach der Verabschiedung des Sarbanes-Oxley Act deutlich an Bedeutung gewonnen. Unternehmen erkennen zunehmend, dass die Sicherstellung von Compliance nicht nur von den verschiedensten Anspruchsgruppen erwartet wird und eine Voraussetzung für die Geschäftstätigkeit bildet. Abhängig von den Anforderungen kann die Erfüllung von Regeln und Standards gegenüber der Öffentlichkeit als ein Qualitätsmerkmal des Unternehmens demonstriert werden. Darüber hinaus unterstützen erfolgreich eingerichtete Verfahren zur Sicherstellung von Compliance ein Unternehmen dabei, zielgerichtet zu handeln und die Interessen der verschiedensten Anspruchsgruppen ausreichend zu berücksichtigen.[1]

Das Ziel der nachfolgenden Kapitel ist es, den Begriff »Compliance« näher zu untersuchen und dessen Stellenwert und Tragweite anhand von verschiedenen, derzeit relevanten Regeln und Standards aufzuzeigen. Bereits bei der Definition und Abgrenzung des Begriffs in Kapitel I.1 wird deutlich, welche vielschichtigen Themengebiete im Zusammenhang mit »Compliance« stehen und für Unternehmen als »Corporate Compliance« von Bedeutung sind.

Ab Kapitel I.2 werden einige der verschiedenen Regeln und Standards beschrieben, die vor allem für börsennotierte Unternehmen gegenwärtig von Bedeutung sind bzw. zukünftig sein werden. Neben global anerkannten Standards, wie beispielsweise den OECD Corporate Governance Principles, werden auch Auswirkungen und Entwicklungen des Sarbanes-Oxley Act betrachtet. Ein weiterer Schwerpunkt der Ausführungen liegt auf EU-Initiativen und der Umsetzung spezifischer EU-Standards in Deutschland. Deutlich wird auch, dass viele der aufgeführten Regeln und Standards einer kontinuierlichen Veränderung unterworfen sind.

Compliance in einem dynamischen Umfeld stellt deshalb hohe Anforderungen an die Organisation, die Prozesse, die Systeme und die Mitarbeiter im Unternehmen. Die Komplexität und Vielzahl der Anforderungen in Verbindung mit den kontinuierlichen Veränderungen stellen Unternehmen zunächst vor die wichtige Aufgabe, alle relevanten Regeln und Standards zielgerichtet zu identifizieren. Die Identifikation ist eine Voraussetzung, um geeignete Maßnahmen festlegen und umsetzen zu können. Eine weitere Herausforderung für die Unternehmen besteht darin, sich den andauernden und häufigen Veränderungen der als relevant identifizierten Regeln und Standards möglichst effektiv und auch effizient sowie in Übereinstimmung mit den Unternehmenszielen anzupassen. Effektiv und wirtschaftlich effizient ist eine Umsetzung neuer Standards und Regeln erfahrungsgemäß dann, wenn die erforderlichen Maßnahmen frühzeitig geplant und umgesetzt werden.

---

1 Anm.: Der Nutzen von Compliance für Unternehmen wird u. a. in Kapitel II.1 nochmals ausführlicher diskutiert.

Kapitel I bietet nicht nur einen Überblick über verschiedene, aktuell relevante Regeln und Standards. Es verdeutlicht zusätzlich, welchen Stellenwert und Umfang die Erfüllung von Anforderungen der verschiedenen Anspruchsgruppen einnimmt. Das Kapitel schafft gleichzeitig eine Basis für die Ausführungen in späteren Kapiteln. Maßnahmen, um eine Anforderung nachhaltig über einen längeren Zeitraum sicherzustellen, werden in den Folgekapiteln ebenso diskutiert wie die Integration verschiedenster Compliance-Anforderungen in einem ganzheitlichen Ansatz.

Wie bereits angemerkt, sind die beschriebenen Regeln und Standards häufigen Änderungen unterworfen. Die nachfolgenden Ausführungen beziehen sich auf den Stand im Februar 2006.

1 Der Compliance-Begriff

Das allgemeine Verständnis des Begriffs »Compliance« ist heterogen – eine anerkannte disziplinenübergreifende Definition für Compliance besteht in der Praxis häufig nicht. Der Begriff und die Funktion »Compliance« haben ihren Ursprung in der Bankenwelt.[2]

Aus juristischer Sicht ließe sich Compliance frei mit »Handeln in Übereinstimmung mit geltendem Recht« übersetzen. Für das »Committee of Sponsoring Organizations of the Treadway Commission« (COSO) bezieht sich »Compliance« auf die Einhaltung von Gesetzen und Regeln, von denen Unternehmen betroffen sind.[3] Für die Betriebswirtschaftslehre war der Begriff »Compliance« bis zum Inkrafttreten des Sarbanes-Oxley Act im Jahr 2002 unscharf und in der täglichen Arbeit kaum von Bedeutung. Insbesondere Section 404 des Sarbanes-Oxley Act hat diesen Sachverhalt geändert. Umfangreiche »SOA 404 Compliance-Projekte« haben dazu geführt, dass der Begriff »Compliance« im Sprachgebrauch der Unternehmenswelt heute einen sehr viel größeren Stellenwert einnimmt als noch vor wenigen Jahren. Section 404 des Sarbanes-Oxley Act hat insoweit zu einer starken Sensibilisierung in Bezug auf das Thema »Compliance« geführt.

Als Basis für die nachfolgenden Kapitel des Buchs wird an dieser Stelle eine **Abgrenzung des Compliance-Begriffs** vorgenommen:

Compliance steht in diesem Buch für die Einhaltung von gesetzlichen Bestimmungen, regulatorischen Standards und die Erfüllung weiterer wesentlicher Anforderungen der Stakeholder.[4] Compliance trägt dazu bei, die Beständigkeit des Geschäftsmodells, das Ansehen in der Öffentlichkeit und die finanzielle Situation eines Unternehmens zu verbessern. Compliance umfasst die Einrichtung geeigneter Organisationsstrukturen, Prozesse und Systeme im Unternehmen.[5]

Die Bezeichnung **Corporate Compliance** erweitert den oben beschriebenen Compliance-Begriff um einen unternehmensweiten, integrativen Ansatz zur effektiven und effizienten Erfüllung der wesentlichen Stakeholder-Anforderungen. Corporate Compliance wird hierdurch zu einer Voraussetzung für eine nachhaltige, risiko- und wertorientierte, ethische und regelkonforme Unternehmensführung.[6]

---

2 Vgl. Buff (2000), S. 10 ff.
3 Vgl. COSO (2004), S. 121.
4 Anm.: Stakeholder sind Personen oder Gruppen aus dem gesamten sozioökonomischen Unternehmensumfeld, die (berechtigte) Ansprüche und Anforderungen an das Unternehmen richten.
5 Vgl. PwC (2005d), S. 3.
6 Anm.: Integrierende Maßnahmen werden u. a. in Kapitel II.1 und II.5 ausführlicher vorgestellt.

Kapitel I betrachtet, welche verschiedenen Arten von Stakeholder-Anforderungen in Form von gesetzlichen oder freiwillig zu erfüllenden Anforderungen existieren. Ein Schwerpunkt der Betrachtung liegt hierbei auf den Anforderungen, die im Zusammenhang mit der Finanzberichterstattung stehen. Kapitel II und die jeweiligen Unterkapitel beschreiben, welche Maßnahmen notwendig sind, um ein geeignetes Organisationsmodell zur Erfüllung der Anforderungen mit Prozessen und Systemen einzurichten.

Compliance mit globalen Regeln und Standards
Das Einhalten von globalen Regeln und Standards ist heute eine Grundvoraussetzung dafür, dass Unternehmen Geschäfte betreiben und am Markt auftreten dürfen. Andauernde Änderungen des regulatorischen Umfelds aufgrund gesellschaftlicher, ökonomischer, ökologischer und technologischer Fortschritte stellen hohe Anforderungen an die Fähigkeit der betroffenen Unternehmen, sich neuen Regeln und Standards möglichst effektiv und effizient anzupassen. Unternehmen, die sich frühzeitig auf neue Regeln und Standards einstellen und vorbereiten, haben gegenüber ihren Wettbewerbern Vorteile, weil deren Implementierung erfahrungsgemäß wirksamer und auch kostengünstiger ist, je eher mit der Umsetzung begonnen wird. Globale Regeln und Standards, wie beispielsweise Transparenz- und Publizitätsstandards, Sozial- und Umweltstandards oder Standards für gute Unternehmensführung und Unternehmensüberwachung werden von internationalen Standardsettern und Institutionen, wie beispielsweise der Organisation für Wirtschaftliche Zusammenarbeit und Entwicklung (OECD), entwickelt. Sie sind nicht rechtsverbindlich, gelten aber regelmäßig als Vorgabe bzw. Rahmen, an dem sich andere Regulatoren und Standardsetter, aber auch Unternehmen orientieren.

Compliance mit Regeln und Standards zur Unternehmenspublizität
Unternehmen haben vielfältige Verpflichtungen im Hinblick auf die Veröffentlichung von Informationen finanzieller und nicht-finanzieller Art. Diese Informationen dienen den Investoren und anderen Stakeholdern dazu, sich ein faires, richtiges und vollständiges Bild von der Vermögens-, Finanz- und Ertragslage des Unternehmens zu machen. Grundsätzlich sollen die Informationen zuverlässig, entscheidungsrelevant, zeitgerecht, verständlich und im Hinblick auf vorherige Perioden vergleichbar sein. Informationen finanzieller Art beinhalten in erster Linie den Jahresabschluss eines Unternehmens. Der Anhang als Bestandteil des Jahresabschlusses enthält neben finanziellen Informationen auch nicht-finanzielle Informationen. Erst mit Hilfe der nicht-finanziellen Informationen kann sich der Empfänger der Informationen ein vollständiges Bild von der wirtschaftlichen Lage der Gesellschaft machen.

Börsennotierte Gesellschaften in den USA müssen umfangreiche Publizitätspflichten erfüllen, die unter anderem aus dem Sarbanes-Oxley Act resultieren. So definiert Section 302 die Verantwortung der Unternehmen für die vierteljährlichen und jährlichen Finanzberichte, die durch den CEO und CFO geprüft, kontrolliert, unterschrieben und mit diesbezüglichen Hinweisen veröffentlicht werden müssen. Die Erklärung nach Section 302 durch den CEO und den CFO enthält weiterhin Aussagen zum Publizitätskontrollsystem (Disclosure Controls and Procedures). Section 404 verpflichtet das Management, einmal im Jahr eine Beurteilung der internen Kontrollen vorzunehmen und im Rahmen der jährlichen Unternehmensberichterstattung in dem »Internal Control Report« dazu Stellung zu nehmen. Wesentliche Informationspflichten für Gesellschaften, die in Deutschland börsennotiert sind, ergeben sich aus dem Wertpapierhandelsgesetz, dem Handelsgesetzbuch und dem Aktiengesetz. Compliance mit Regeln und Standards

in Bezug auf die Veröffentlichung finanzieller und nicht-finanzieller Unternehmensinformationen bedeutet, dass das Ziel einer effektiven und effizienten Kapitalmarktkommunikation erreicht wird.

Compliance mit Regeln und Standards zur Unternehmensführung und Unternehmensüberwachung

In den vergangenen Jahrhunderten ist es immer wieder zu Unternehmenskrisen mit weit reichenden Auswirkungen gekommen.[7] Hauptursache für die meisten Unternehmenskrisen waren damals wie heute Fehler des Managements, das im Auftrag der Eigentümer die Geschäfte der Gesellschaft führt und ihr Vermögen verwaltet. Nach herrschender Meinung war und ist das Auseinanderfallen von Eigentum und Kontrolle das Kernproblem von Corporate Governance.[8] In der Folge wurde das Geschäftsleben nach und nach stärker reguliert, um existenzbedrohende Krisen von Unternehmen zu vermeiden bzw. zu verhindern. Diese Entwicklung hält bis heute an.

Vor dem Hintergrund diverser Initiativen zur Regulierung und Standardisierung der Unternehmensführung und -überwachung werden die fachlichen und persönlichen Anforderungen an die geschäftsführenden Direktoren und die nicht-geschäftsführenden Direktoren weiter steigen. Gute Corporate Governance sichert die Existenz von Unternehmen und wirkt sich positiv auf den Unternehmenswert aus.[9] Corporate-Governance-Codes existieren mittlerweile in nahezu allen wirtschaftlich entwickelten Ländern.[10]

Im Fall der Nichteinhaltung der Kodizes drohen den Unternehmen der Verlust des Vertrauens der Kapitalmarktteilnehmer und verschlechterte Finanzierungskonditionen. Die verantwortlichen Mitglieder der Verwaltung[11] selbst sind hohen persönlichen Haftungsrisiken ausgesetzt.

Compliance mit den Regeln und Standards zur Unternehmensführung dient der Existenzsicherung, steigert den Wert des Unternehmens,[12] minimiert das Risiko unternehmerischer Fehlentscheidungen und reduziert zugleich die persönlichen Haftungsrisiken für die Mitglieder der Verwaltung.

Compliance mit den Regeln und Standards der Börsen

Alle bedeutenden Börsenplätze, wie zum Beispiel die New York Stock Exchange (NYSE), die London Stock Exchange (LSE) oder die Frankfurter Wertpapierbörse (FWB), geben Regeln und Standards vor, die von den Gesellschaften zu erfüllen und einzuhalten sind, wenn sie ihre Aktien an der Börse handeln lassen wollen.

Compliance mit den Regeln und Standards der Börsen ermöglicht den Zugang zum Kapitalmarkt und sichert damit die Finanzierung der Geschäftstätigkeit.

Compliance mit Rechnungslegungsstandards

Regeln und Standards in Bezug auf die Rechnungslegung, wie die International Financial Reporting Standards (IFRS) oder die US-amerikanischen Generally Accepted Accounting

---

7 Vgl. Hopt/Leyens (2004), S. 135-138.
8 Vgl. Hopt/Leyens (2004), S. 135 f.
9 Vgl. McKinsey (2002), S. 1 ff.
10 Vgl. ECGI, http://www.ecgi.org/codes/all_codes.php für eine Übersicht zu Corporate-Governance-Codes.
11 Vgl. § 120 Absatz 2 Satz 1 AktG – In Deutschland erfolgt die Verwaltung der Aktiengesellschaft durch Vorstand und Aufsichtsrat. Die Mitglieder der Verwaltung sind demnach dem Vorstand oder dem Aufsichtsrat zuzuordnen.
12 Vgl. McKinsey (2002), S. 1 ff.

Standards (US-GAAP), geben einen konkreten Rahmen vor, in dem sich insbesondere börsennotierte Unternehmen gegenüber ihren Anteilseignern präsentieren müssen.

Compliance mit den gängigen internationalen Rechnungslegungsstandards bedeutet, dass der Hauptzweck der Finanzberichterstattung, eine möglichst zuverlässige und faire Darstellung der wirtschaftlichen Lage des Unternehmens sicherzustellen, erreicht wird.

Compliance in Bezug auf Business Judgement Rules

Der Grundgedanke der aus dem angelsächsischen Rechtskreis stammenden Business Judgement Rules besteht darin, dass die Mitglieder der Verwaltung dann nicht persönlich haften, wenn sie zum Wohle der Gesellschaft auf der Grundlage angemessener Information handeln und entscheiden.[13]

Entscheidungen auf der Grundlage angemessener Informationen erfordern interne Kontroll- und Risikomanagementsysteme, die wesentlich dazu beitragen können, die unternehmerische Entscheidung zu fundieren und ein Abwägen von Chancen und Risiken basierend auf einer geeigneten Informationsbasis zu ermöglichen.

In Deutschland findet das Prinzip der Business Judgement Rules Parallelen in der neueren höchstrichterlichen Rechtsprechung des Bundesgerichtshofs,[14] und bedingt durch das Gesetz zur Unternehmensintegrität und Verbesserung des Anfechtungsrechts (UMAG), erstmals Eingang in das Aktienrecht.[15]

Compliance mit Business Judgement Rules bedeutet, dass die Verwaltung der Gesellschaft Entscheidungen im Rahmen ihres unternehmerischen Ermessens zum Wohle der Gesellschaft trifft.

Compliance mit Regeln und Standards in Bezug auf interne Kontroll- und Risikomanagementsysteme

Innerhalb der betriebswirtschaftlichen Praxis findet Compliance generell Niederschlag in den Bereichen des internen Kontrollsystems und des Risikomanagements, beides originäre Aufgaben des Vorstands bzw. des Aufsichtsrats. Während der Vorstand für die eigentliche Umsetzung verantwortlich ist, hat der Aufsichtsrat die relevanten Prozesse und Systeme unabhängig zu überwachen. Wirksame und effiziente interne Kontroll- und Risikomanagementprozesse sind erfahrungsgemäß Katalysatoren für eine gute Unternehmensführung und -überwachung. Beispiele für betriebswirtschaftlich geprägte Standards für diesen Teil der Unternehmensführung und -überwachung sind das Internal Control – Integrated Framework oder das Enterprise Risk Management – Integrated Framework.[16] Die beiden Rahmenwerke werden in der Praxis häufig mit »COSO I« (Internal Control) und »COSO II« (Enterprise Risk Management) bezeichnet.

Exkurs: Das interne Kontrollsystem nach COSO I

Gemäß dem Rahmenwerk von COSO ist das interne Kontrollsystem ein Prozess, der von Aufsichtsgremien, dem Management und den Mitarbeitern ausgeführt wird und das Erreichen der festgelegten Unternehmensziele gewährleistet. Für die Zielsetzung unterscheidet das COSO I-Rahmenwerk die folgenden Zielkategorien:[17]

13 Vgl. Hillebrand (2005), S. 136-147; Hopt/Leyens (2004), S. 142.
14 Vgl. BGH (1997).
15 Vgl. § 93 Abs. 1 Satz 2 AktG.
16 Vgl. COSO (1992); COSO (2004); Kapitel II.5.1.2.
17 Vgl. Menzies (2004), S. 76 ff. für weitere Erläuterungen zur Definition des IKS nach COSO.

- Sicherung der Wirksamkeit und der Wirtschaftlichkeit der Geschäftstätigkeit **(Operations),**
- Ordnungsmäßigkeit und Verlässlichkeit der Finanzberichterstattung **(Financial Reporting)** und
- Einhaltung von maßgeblichen Gesetzen und Vorschriften **(Compliance).**

Kontrollen müssen fortlaufend ausgeführt werden, um die ordnungsgemäße Funktion des Systems und das Erreichen der Ziele mit hinreichender Sicherheit zu gewährleisten. Daher ist es notwendig, das interne Kontrollsystem fest in die Geschäftsprozesse des Unternehmens einzubinden. Der Aufbau des COSO-Rahmenwerks ist in Form eines Würfels dargestellt (vgl. Abb. 1).

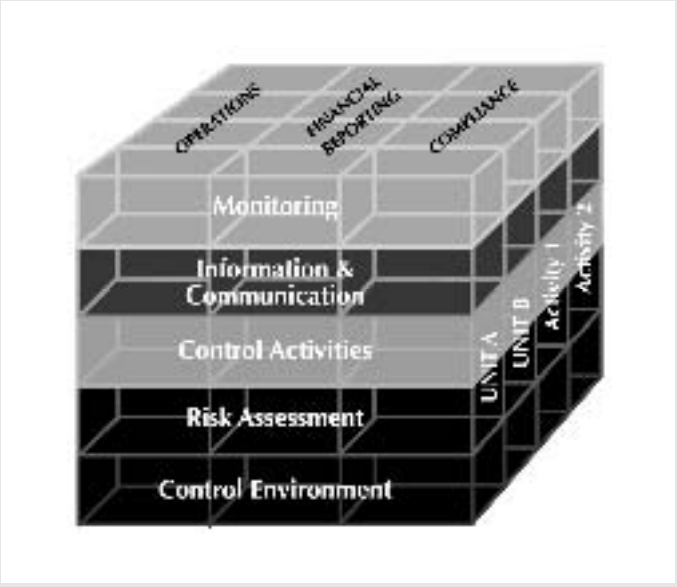

Abb. 1: Der COSO-Würfel[18]

Jede einzelne der fünf Komponenten (Control Environment, Risk Assessment, Control Activities, Information & Communication, Monitoring) trägt zum Erreichen der Ziele bei. Die Komponenten stehen in einer Wechselbeziehung zueinander und betreffen sowohl die Gesamtorganisation als auch einzelne Unternehmenseinheiten und Prozesse. Alle fünf Komponenten sind erforderlich, um ein wirksames internes Kontrollsystem zu gewährleisten.
Abhängig von der Struktur, Größe und Komplexität der Organisation können die Komponenten unterschiedlich stark ausgeprägt sein.[19] Zur Verdeutlichung des Aufbaus des internen Kontrollsystems unterscheidet COSO zwischen fünf Komponenten:

18 Vgl. Menzies (2004), S. 75 ff. zu den unterschiedlichen Dimensiionen des COSO-Rahmenswerks.
19 Vgl. COSO (1992), S. 15; Menzies (2004), S. 77.

- Das **Kontrollumfeld** (Control Environment) bildet das Fundament für die anderen vier Komponenten und bestimmt das Kontrollbewusstsein in einem Unternehmen. Es umfasst die im Unternehmen vermittelte Unternehmenskultur und den Führungsstil des Managements, wie zum Beispiel den »Tone at the Top«[20], die Bedeutung von Integrität und ethischen Werten.
- Ein kontinuierlicher Prozess der **Risikobeurteilung** (Risk Assessment) stellt sicher, dass Risiken erkannt und bewertet werden, die ein Erreichen der Unternehmensziele beeinträchtigen können.
- **Kontrollaktivitäten** (Control Activities) müssen (z. B. als Richtlinien und Verfahren) eingerichtet und ausgeführt werden. Die Aktivitäten dienen dazu, die gesetzten Unternehmensziele zu erreichen.
- Die **Informations- und Kommunikationskomponente** (Information & Communication) des COSO-Würfels soll verdeutlichen, dass Informationen so identifiziert, erfasst und kommuniziert werden, dass Mitarbeiterinnen und Mitarbeiter in der Lage sind, ihrer Verantwortung gerecht zu werden.
- Die **Überwachung** (Monitoring) des internen Kontrollsystems ist erforderlich, um die Effektivität des Systems kontinuierlich zu gewährleisten und flexibel auf Veränderungen reagieren zu können.

Für jede der genannten Komponenten muss das Vorhandensein wirksamer Kontrollen sichergestellt sein. Kontrollen der Komponente »Kontrollaktivitäten« sind überwiegend auf Prozessebene implementiert und besitzen in der Regel den größten Anteil an den insgesamt im Unternehmen vorhandenen Kontrollen. Kontrollen der übrigen vier Komponenten sind häufig komponentenübergreifend (beispielsweise auf Unternehmensebene) eingerichtet. Die vier Komponenten werden in der Praxis auch als »**Softer COSO-Components**« bezeichnet.

Die Securities and Exchange Commission (SEC) empfiehlt das COSO I-Rahmenwerk als Referenz zur Evaluierung des internen Kontrollsystems der Finanzberichterstattung nach SOA Section 404. Allerdings handelt es sich lediglich um eine Empfehlung der SEC, so dass auch andere Konzepte, wie zum Beispiel die Turnbull Guidance oder der Leitfaden des Canadian Institute of Chartered Accountants, zu Risikomanagement und Corporate Governance verwendet werden können.[21,22] Der im Rahmen der Jahresberichterstattung durch das Management abzugebende Internal Control Report gemäß Section 404 hat unter anderem einen Hinweis darauf zu enthalten, welches Framework im Rahmen des Assessments genutzt wurde.

In Europa existiert eine Vielzahl einzelstaatlicher, zum Teil gesetzlicher Regelungen in Bezug auf interne Kontrollen und Risikomanagement.[23] In Deutschland zum Beispiel verpflichtet § 91 Absatz 2 des Aktiengesetzes (AktG) Vorstände börsennotierter Gesellschaften, ein Risikofrüherkennungssystem einzurichten. In einem dualistischen System der Unternehmensführung und Unternehmensüberwachung obliegt es dem Aufsichtsrat der Aktiengesellschaft, das Risikomanagementsystem in Bezug auf die

20 Anm.: Die Bedeutung des »Tone at the Top« wird u.a. in Kapitel II.5.1.1. diskutiert.
21 Vgl. SEC (2003), Fn. 67.
22 Vgl. PCAOB (2004), Section 13 für Kriterien, die ein geeignetes Rahmenwerk erfüllen muss (u. a. das Durchlaufen eines »Due-Process«).
23 Vgl. FEE (2005), S. 39 ff.

Wirksamkeit und Wirtschaftlichkeit zu überwachen.[24] Im Handelsgesetzbuch schreibt § 317 HGB außerdem die Prüfungspflicht des Risikofrüherkennungssystems durch den Abschlussprüfer vor. Diese Regelungen gelten bereits seit dem Inkrafttreten des seinerzeit richtungsweisenden Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) aus dem Jahr 1998.

Mit dem Enterprise Risk Management – Integrated Framework ist ein weiteres modernes Rahmenwerk (COSO II) entstanden, das auch im Hinblick auf die praktische Umsetzung und Interpretation der unbestimmten Rechtsbegriffe in § 91 Absatz 2 des Aktiengesetzes wichtige Impulse liefern kann. Kleineren an den Börsen notierten Gesellschaften wird darüber hinaus ein auf ihre Bedürfnisse zugeschnittener Leitfaden, die Guidance for Smaller Public Companies Reporting on Internal Controls over Financial Reporting, an die Hand gegeben.[25] Diese Guidance wurde von COSO entwickelt. Das Framework ist zwar in erster Linie für kleinere börsennotierte Gesellschaften gedacht, es kann aber auch großen Gesellschaften Anhaltspunkte für eine kosteneffiziente Gestaltung ihres unternehmensweiten internen Kontrollsystems liefern. Die SEC unterstützt die COSO-Initiative: »… this guidance is an important step forward in helping smaller businesses understand and apply COSO's internal control framework in connection with implementing Section 404 of the Sarbanes-Oxley Act.«[26]

Compliance mit den betriebswirtschaftlich geprägten Standards, wie zum Beispiel dem Internal Control – Integrated Framework (COSO I), bedeutet, dass ein Unternehmen sein internes Kontrollsystem nach anerkannten Best Practice-Standards eingerichtet hat und damit beispielsweise das Ziel einer zuverlässigen Finanzberichterstattung unterstützt wird.

Corporate Compliance

Die bisherigen Ausführungen geben einen ersten Überblick darüber, für welche Bereiche mit Standards und Regeln die Einhaltung von Compliance bzw. Corporate Compliance zur Erfüllung der Stakeholder-Anforderungen unter anderem von Bedeutung ist. In den nachfolgenden Kapiteln werden Standards und Regeln aus den folgenden Themengebieten nochmals ausführlicher betrachtet:

- weltweit geltende Industrie-, Sozial- und Umweltstandards,
- Standards und Regeln zur Veröffentlichung finanzieller und nicht-finanzieller Unternehmensinformationen,
- Corporate-Governance-Praktiken,
- Zulassungsbedingungen bestimmter Börsen,
- international akzeptierte Rechnungslegungsstandards, wie IFRS oder US-GAAP,
- Business Judgement Rules sowie
- betriebswirtschaftliche Standards zu internen Kontrollen und Risikomanagementsystemen.

24 Vgl. Schichold (2001), S. 397-422.
25 Vgl. COSO (2005), S. 1 ff.
26 SEC (2005).

2 Bedeutende globale Regeln und Standards

Globale Regeln und Standards haben eine große Bedeutung für Unternehmen und deren Einhaltung ist in vielen Fällen die Voraussetzung für eine erfolgreiche Geschäftstätigkeit. Aus diesem Grund gibt der folgende Abschnitt einen Überblick über internationale und nationale Entwicklungen zum Thema Compliance. Dabei werden bedeutende Anforderungen wie z. B. die Corporate-Governance-Grundsätze der OECD, industriespezifische Standards oder die Neugestaltung von Eigenkapitalvorschriften für Kreditinstitute (Basel II) eingehend erläutert. Die Ausführungen verdeutlichen auch Zusammenhänge zwischen den Regeln und Standards und den Auswirkungen auf das Risikomanagement sowie das interne Kontrollsystem eines Unternehmens.

2.1 OECD Principles of Corporate Governance

Die Corporate-Governance-Grundsätze der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung wurden erstmals im Jahr 1999 vom Rat der OECD auf Ministerebene gebilligt. Im Jahr 2004 wurde eine überarbeitete Fassung der Grundsätze veröffentlicht. Die Corporate-Governance-Grundsätze der OECD sind weltweit zu einer internationalen Richtschnur für Anleger, börsennotierte Unternehmen, politische Entscheidungsträger und sonstige Stakeholder geworden.[27]

Die Corporate-Governance-Grundsätze der OECD beinhalten nicht-rechtsverbindliche Standards, Leitlinien, empfehlenswerte Praktiken und Orientierungshilfen, die so definiert sind, dass sie den spezifischen Gegebenheiten in den einzelnen Ländern und Regionen angepasst werden können.[28] Sie werden als Orientierungshilfe für Gesetzes- und Regulierungsinitiativen von den OECD-Mitglieds- wie auch Nicht-Mitgliedsländern verwendet.

Die OECD hat einen auf Prinzipien basierenden Ansatz gewählt, bei dem angemessene Corporate-Governance-Praktiken im Zentrum stehen. Die Prinzipien nehmen konkret Bezug auf

- die Sicherung der Grundlagen eines wirksamen Rahmens für Corporate Governance,
- Aktionärsrechte und Schlüsselfunktionen der Kapitaleigner,
- die Gleichbehandlung der Aktionäre,
- die Rolle der verschiedenen Stakeholder,
- die Offenlegung und Transparenz finanzieller und nicht-finanzieller Informationen sowie
- die Aufgaben und Pflichten des Aufsichtsorgans.

Informationen zu den Themen interne Kontrollen und Risikomanagement finden sich insbesondere in den Abschnitten über die Offenlegung und die Aufgaben des Verwal-

27 Vgl. OECD (2004), S. 3 ff.
28 Vgl. OECD (2004), S. 4.

tungsorgans. Die OECD weist beispielsweise darauf hin, dass die Offenlegung von Informationen über die Risikoüberwachungs- und -managementsysteme zunehmend als empfehlenswerte Praxis angesehen wird.[29] Wesentliche von den Unternehmen offen zu legende Informationen über Risiken werden in den Corporate-Governance-Grundsätzen der OECD exemplarisch aufgelistet. So sollte das Unternehmen alle vorhersehbaren wesentlichen Risikofaktoren in einer präzisen Form publizieren[30] und im Einzelnen berichten über

- branchenspezifische Risiken,
- regional bedingte Risiken,
- das Risiko der Abhängigkeit von bestimmten Rohstoffen,
- Risiken des Finanzmarkts einschließlich der Zins- und Währungsrisiken,
- Risken im Hinblick auf Finanzderivate,
- Risiken nicht bilanzwirksamer Transaktionen sowie
- umweltbezogene Haftungsrisiken.

Weiterhin sehen die OECD-Prinzipien die Einrichtung von Ausschüssen, wie zum Beispiel eines Audit Committees, vor. Deren Mandat, Zusammensetzung und die festgelegten Arbeitsverfahren sind zu veröffentlichen, wobei sich die Offenlegung nicht auf solche Ausschüsse erstrecken sollte, die zur Abwicklung vertraulicher Geschäfte eingerichtet wurden.[31] Eine exakte Definition des Begriffs »vertrauliche Geschäfte« wird jedoch nicht vorgenommen.

Die Corporate-Governance-Grundsätze der OECD benennen bestimmte Schlüsselfunktionen, die unbedingt durch das Aufsichtsorgan ausgeübt werden sollten. Auch an dieser Stelle wird die Bedeutung interner Kontroll- und Risikomanagementprozesse als Treiber für eine gute Unternehmensführung und Unternehmensüberwachung hervorgehoben. Zu den Schlüsselfunktionen, die durch das Aufsichtsorgan wahrgenommen werden sollten, zählen die

- Überprüfung der Unternehmensstrategie, der operativen Pläne und der Risikopolitik,
- Überwachung der Wirksamkeit der von dem Unternehmen angewandten Corporate-Governance-Praktiken,
- Bestellung, Vergütung, Kontrolle sowie gegebenenfalls Auswechselung von Mitgliedern der Geschäftsführung und Überwachung der Nachfolgeplanung,
- Anpassung des Vergütungssystems für die Geschäftsführung an die längerfristigen Interessen des Unternehmens und der Aktionäre,
- Verfolgung potentieller Interessenkonflikte,
- Gewährleistung der Integrität der Rechnungslegungs- und Buchführungssysteme, einschließlich der Initiierung unabhängiger Prüfungen durch die Abschlussprüfer sowie
- Sicherstellung angemessener interner Kontrollen im Hinblick auf das Risikomanagement, die Finanzen, die operativen Geschäftsaktivitäten sowie die Einhaltung gültiger Gesetze und relevanter Standards.

29 Vgl. OECD (2004), S. 65.
30 Vgl. OECD (2004), S. 65.
31 Vgl. OECD (2004), S. 83.

2.2 Industriespezifische Regeln und Standards

Die Beachtung industriespezifischer Regeln und Standards ist heute Grundvoraussetzung für einen erfolgreichen Marktauftritt. Diese Regelwerke bilden ebenfalls die Grundlage für die Implementierung von Managementsystemen.

Bei Qualitätsmanagementsystemen handelt es sich um strukturierte Modellbeschreibungen, bei denen die Qualität als Teil der Gesamtführungsaufgabe eines Unternehmens wahrgenommen wird.[32] Gerade unter dem Eindruck gesättigter und teilweise krisengeschüttelter, konkurrenzintensiver Märkte kommt dem Standard »Qualität« besondere Bedeutung zu.

Alle relevanten Managementelemente einer Organisation und auch deren Beziehungen zu Geschäftspartnern und der gesellschaftlichen Umwelt berücksichtigt das Model for Business Excellence der European Foundation for Quality Management (EFQM-Standard).[33] Die produktionslastige Analyse und Beschreibung von Prozessen nach ISO 9000[34] wird durch EFQM überwunden. Die Weiterentwicklung einer Organisation aus Kunden- und Mitarbeitersicht ist eine der wesentlichen Zielsetzungen des EFQM-Standards. Das EFQM-Modell basiert auf der Grundphilosophie der Selbstbewertung betrieblicher Prozesse. Stärken und Verbesserungspotentiale können daher klar identifiziert und geplant werden.[35] Die Kriterien des EFQM sind bereits heute Basis für Standards und Regeln des Qualitätsmanagements in Krankenhäusern. Im Sinne einer sich entwickelnden Qualitätspolitik von Kommunen und öffentlichen Trägern werden sie zunehmend auch für die Felder sozialer und gesundheitlicher Arbeit allgemein eingeführt. EFQM-Standards stellen eine wichtige Beurteilungsbasis für die notwendige Prioritätensetzung der Ressourcen im Gesundheitswesen dar.

Auch die Telekommunikationsindustrie hat erkannt, dass Unternehmen, die sich frühzeitig und effektiv an neue Standards und Regeln anpassen, Wettbewerbsvorteile haben. Die internationale Telekommunikationsindustrie hat daher mit dem Standard TL 9000 ein zukunftsweisendes Qualitätsmanagementmodell geschaffen, das Regeln und Standards der ISO 9000 an die Erfordernisse dieses Industriezweigs anpasst.[36] Der TL 9000-Standard wird von dem QuEST-Forum (Quality Excellence for Suppliers of Telecommunication) erarbeitet und verwaltet. Das Forum wurde von der University of Texas in Dallas gegründet. Ihm gehören nahezu alle Telekommunikationsausrüster und -dienstleister an.

Als festgelegter Industriestandard integriert der TL 9000 spezifische Anforderungen der Branche mit Messgrößen in ein industriespezifisches Managementsystem. Eine regelmäßige Berichterstattung über Kennzahlen und Messgrößen ermöglicht den Vergleich mit Konkurrenzdaten und gewährleistet damit ein echtes Benchmarking. Industrieübergreifend berichten auch bestimmte große deutsche Unternehmen insbesondere über gesellschaftliche Aspekte ihres unternehmerischen Handelns und erfüllen damit relevante Standards des Total Quality Management (TQM). Auch wird in Nachhaltigkeitsberichten über Interessen der Mitarbeiter, soziale Verantwortung im Umfeld der Unternehmen oder ökologische Aspekte der Produktion berichtet.

---

32 Vgl. IHK (2003), S. 10 ff.
33 Vgl. EFQM (2003), S. 1 ff.
34 Anm.: ISO 9000 wird im weiteren Verlauf als Synonym für ISO 9001:2000 bzw. ISO 9004:2000 verwendet.
35 Vgl z. B. IHK (2003), S. 16.
36 Vgl z. B. IHK (2003), S. 11.