I. Einleitung

A. Was ist Compliance?

Gliederung **Seite**

Der Begriff Compliance ist in aller Munde. Die gegenwärtige Finanz- und Wirtschaftskrise hat erhebliche Mängel bisheriger Risikomanagementsysteme zu Tage gebracht und aufgezeigt, dass Unternehmen erhebliche Risiken in finanzieller, betrieblicher, operativer und rechtlicher Hinsicht falsch eingeschätzt hatten. Im Folgenden soll zunächst der Begriff Compliance näher bestimmt werden.

1. Etymologie, Historie und allgemeine Erklärung des Begriffes „Compliance“

Die heutige Verwendung des Begriffs Compliance entstammt ursprünglich der englischen Bankensprache und wurde aus der angelsächsischen Rechtsterminologie übernommen. Compliance leitet sich von dem Verb „to comply with“ (einhalten) ab und bedeutet aus juristischer Sicht frei übersetzt „das Verhalten in Übereinstimmung mit und das Einhalten von rechtlichen sowie regulativen Vorgaben“.[1]

Die US-Finanzbranche Ende der 1980er Jahre hat den Begriff Compliance maßgeblich geprägt. Die USA begannen schon sehr früh mit der Einführung von Compliance-Anforderungen an Unternehmen, die vor dem Hintergrund der strafrechtlichen Verantwortung von Kapitalgesellschaften für kriminelle Handlungen ihrer Angestellten entstanden. Die sogenannten Compliance-Codes, die eine Selbstverpflichtung der Unternehmen darstellen, dienten jedoch nicht nur als unternehmensseitige Präventivmaßnahmen, welche sicherstellen sollten, dass Gesetze und Regeln eingehalten werden, sondern ermöglichten auch ein teilweise milderes Strafmaß für das betroffene Unternehmen im Falle einer Verurteilung (1991 erfolgte eine Revision der „US Federal Sentencing Guidelines“:[2] Strafmilderung war möglich, wenn das Unternehmen nachweisen konnte, dass es den Mitarbeitern die wichtigsten Regeln zugänglich gemacht und deren Einhaltung überwacht hatte).[3] Die Einrichtung eines funktionierenden Compliance-Systems war die einzige Möglichkeit, das Risiko derart kostspieliger Prozesse zu reduzieren.[4]

1 *Menzies*, Sarbanes-Oxley und Corporate Compliance: Nachhaltigkeit, Optimierung, Integration (2006) 2.
2 Zu den US Federal Sentencing Guidelines siehe Punkt 6.1.2.1.
3 *Kampffmeyer*, Compliance (2004) 4.
4 *Geißler*, Compliance-Management, Havard Business Management (2004) 48.

In Deutschland begann 1992 die Deutsche Bank als eines der ersten Geldinstitute mit dem Aufbau einer eigenen Compliance-Organisation nach angelsächsischem Vorbild, um sicherzustellen, dass kapitalmarktrechtliche Verhaltensregeln eingehalten werden und die Marktintegrität gewahrt bleibt.[5]

Heute umschreibt Compliance die Erfüllung bzw Konformität mit staatlichen Restriktionen, Regeln und Spezifikationen sowie mit ethischen und moralischen Grundsätzen, aber auch mit Standards und Richtlinien wie beispielsweise die ISO-Standards (International Organization for Standards). Compliance kann zum einen auf Zwang, wie beispielsweise im Falle von gesetzlichen Vorgaben,[6] und zum anderen auf fakultativem Einhalten von Standards und anderen Bestimmungen beruhen.

Ausgehend von der deutschen Übersetzung, die Compliance als „Verhalten in Übereinstimmung mit und Einhalten von rechtlichen sowie regulativen Vorgaben" versteht, ist zu den verschiedenen Aspekten der Compliance-Anforderungen Folgendes festzuhalten:

Voraussetzung für die Übereinstimmung mit und die Einhaltung von rechtlichen sowie regulativen Vorgaben ist, dass schriftlich verfasste und nachlesbare Vorgaben existieren, die vonseiten der Unternehmensleitung oder der Gesetzgebung verabschiedet wurden. Diese Regeln enthalten allerdings meist keine „technische" Vorgaben, wie die Anforderungen der Compliance an eine Organisation umzusetzen sind, sondern stellen lediglich das Grundgerüst, also den statischen Aspekt von Compliance dar. Dem dynamischen Aspekt hingegen wird durch das Einhalten der Vorgaben auf zwei Ebenen Rechnung getragen. Zum einen sind die Anforderungen in tatsächlichen Problemlösungen im Unternehmen umzusetzen und zum anderen hat diese Umsetzung kontinuierlich im Rahmen eines organisatorisch definierten und verankerten Prozesses zu erfolgen. Da die Anforderungen an das Unternehmen von verschiedenen Institutionen und Organen formuliert werden, wird eine Unterscheidung zwischen „rechtlichen" und „regulativen" Vorgaben getroffen. Bei den rechtlichen Vorgaben handelt es sich um Gesetze, Richtlinien oder behördliche Verordnungen, „die bestimmte Unternehmen, Organisationen oder Personen verpflichten, die jeweils aufgeführten Regelungen einzuhalten."[7] Hier ist anzumerken, dass lediglich im Hinblick auf Auslegung, Umfang und Umsetzungsweise Handlungsspielraum besteht, nicht allerdings bei der Erfüllung der Anforderungen selbst. Im Gegensatz zu den rechtlichen Vorgaben beruhen regulative Vorgaben nicht auf Gesetzen oÄ, sondern werden vom Unternehmen selbst oder von Dritten formuliert (freiwillige Verhaltensvorschriften – „soft law"[8]). Beispiele dafür sind Verhaltensregeln, Normen, Codes of Best Practice oder unternehmensspezifische Standards. In manchen Fällen können diese Regularien allerdings aus gesetzlichen Vorgaben resultieren, um so Mindestanforderungen weiter gerecht zu werden. Speziell im Rahmen von Umweltauflagen oder in Bezug auf nicht diskriminierende Verhaltensregeln gegenüber Mitarbeitern leiten sich solche regulativen Vorgaben von Gesetzen ab und werden unter Umständen um unternehmensinterne Kriterien erweitert.

---

5 *oV*, Deutsche Bank, Anti-Geldwäsche Richtlinie: http://www.db.com/de/downloads/Deutsche_Bank_Konzern_-_Anti-Geldwaesche_Richtlinie.pdf 2009 (12. 12. 2009).

6 Inwieweit dieser Zwang aufgrund von gesetzlichen Vorgaben besteht, wird in weiterer Folge unter Punkt 6. noch erörtert werden.

7 *Kampffmeyer*, Compliance (2004) 3.

8 Zum Begriff „soft law" siehe unten Punkt 3.

Der bindende Charakter von Compliance-Anforderungen kann somit sehr unterschiedliche Hintergründe aufweisen.

Das folgende Kapitel stellt dar, wie der Begriff Compliance in verschiedenen Branchen und Wissenschaften verstanden wird.

2. Interpretation von Compliance in verschiedenen Branchen

So vielfältig die Ausprägungen von Compliance-Anforderungen in Unternehmen formuliert werden können, so stark differenzieren diese auch zwischen den Branchen. „Der Begriff der Compliance wird in der medizinischen, psychologischen und betriebswirtschaftlichen Literatur unterschiedlich interpretiert."[9]

2.1 Begriffsentwicklung in Medizin und Psychologie

Allgemein lässt sich in Medizin und Psychologie Compliance als die Bereitschaft eines Patienten zur Mitarbeit bei diagnostischen und therapeutischen Maßnahmen, dh als Kooperationsbereitschaft des Patienten definieren.[10] Darüber hinaus wird der Begriff im medizinischen Kontext noch differenzierter betrachtet. So bezeichnet der Begriff der „Patienten-Compliance" in der Medizin die Beachtung ärztlicher Anweisungen durch den Patienten, wohingegen die „Medikamenten-Compliance" das Befolgen ärztlicher Behandlungsempfehlungen mit regelmäßiger Einnahme der verordneten Medikamente in den Fokus stellt.[11] Im angelsächsischen Raum wird hier von der „Patient Medication Compliance" gesprochen. Vor diesem Hintergrund lässt sich der Begriff der Compliance einerseits als gegenseitiges Einverständnis bei Willensbekundungen interpretieren, andererseits impliziert Compliance aber zusätzlich die einseitige Bereitschaft, sich am Willen bzw an Empfehlungen der anderen Seite zu orientieren und sich entsprechend unterzuordnen. Wie bereits einleitend bemerkt, lässt sich Compliance in eine statische und in eine dynamische Komponente unterteilen. Im Rahmen der Medizin wird dies besonders deutlich, da das Interpretationsspektrum von Compliance von der reinen Befolgung der therapeutischen Maßnahmen bis hin zur aktiven Unterstützung der Therapien reicht. *Haynes* definiert dies genauer und versteht unter Compliance „den Grad, in dem das Verhalten einer Person (in Bezug [sic] auf die Einnahme eines Medikaments, das Befolgen einer Diät oder die Veränderung eines Lebensstils) mit dem ärztlichen oder gesundheitlichen Rat korrespondiert",[12] was die dynamische Komponente (im Sinne eines Prozesses) hervorhebt.

9 *Dullinger*, Compliance-abhängige Dienstleistungen. Konzeption und Anwendung am Beispiel der Gesundheitsleistungen (2001) 24.

10 *Pschyrembel*, Klinisches Wörterbuch[258], (1998) 296.

11 *Löster*, Compliance im Wertpapier-Dienstleistungskonzern (2003) 13; *Findl & Koller*, NÖ Gebietskrankenkasse (2001): http://www.google.de/url?url=http://www.noegkk.at/mediaDB/MMDB54643_11204.PDF&rct=j&ei=_UYnS6W3NYHuAbRj6ybDQ&sa=X&oi=spellmeleon_result&resnum=2&ct=result&ved=0CAwQhgIwAQ&q=medikamenten-compliance&usg=AFQjCNH6qSnZcEucn_SUGAg6s7_oH0E-N3A2001 (13. 12. 2009).

12 *Haynes* in *Haynes/Taylor/Sackett*, Compliance-Handbuch[2], (1986) 12.

Aufgrund der vielfältigen Betrachtungsmöglichkeiten der Compliance im medizinischen Kontext ist eine Vielzahl von Definitionen verfügbar, auf die im Folgenden nun nicht mehr dezidiert eingegangen wird.[13]

2.2 Cross-Compliance als Sonderform der Landwirtschaft

Die Europäische Union (EU) setzt insbesondere in den Bereichen des Umweltschutzes, bei der Lebensmittel- und Futtermittelsicherheit sowie bei Tiergesundheit und -schutz im internationalen Vergleich hohe Standards.

Durch die Umsetzung dieser Standards entstehen höhere Produktionskosten im Vergleich zu Landwirtschaftsbetrieben in Nicht-EU-Mitgliedstaaten. Damit einer Benachteiligung der EU-Betriebe im internationalen Wettbewerb entgegengewirkt werden kann, beschlossen die Regierungen der EU-Mitgliedstaaten, Agrarzahlungen an betroffene Betriebe zu tätigen. Um „dieser politischen Verknüpfung der Zahlungen mit Schutzstandards auch rechtlichen Nachdruck zu verleihen",[14] wurde eine sogenannte Auflagenbindung auf Vorschlag der EU-Kommission im Rahmen der Agrarreform von 2003 eingeführt.

Diese Abhängigkeit der Agrarzahlungen von der Einhaltung bestimmter Verpflichtungen durch die betroffenen Landwirtschaftsbetriebe wird als „Cross-Compliance" bezeichnet und von der Europäischen Kommission als „ein Mechanismus, mit dem Direktzahlungen an Landwirte an die Erfüllung von Auflagen im Bereich Umweltschutz, Lebensmittelsicherheit, Tier- und Pflanzengesundheit und Tierschutz sowie den Erhalt der landwirtschaftlichen Nutzfläche in gutem Bewirtschaftungs- und Umweltschutz gebunden sind"[15] definiert.

Cross-Compliance ist ein wichtiges Werkzeug zur Integration von Umweltanforderungen in die gemeinsame Agrarpolitik und umfasst in allen EU-Mitgliedstaaten „Grundanforderungen an die Betriebsführung" und die „Erhaltung landwirtschaftlicher Flächen in gutem landwirtschaftlichen und ökologischen Zustand" (GLÖZ). Unter den Begriff „GLÖZ" fallen Flächen, die nicht mehr für die Erzeugung genutzt werden, jedoch in gutem landwirtschaftlichen und ökologischen Zustand (GLÖZ) zu halten sind. Die Mindestanforderungen werden vom jeweiligen Mitgliedstaat festgelegt.[16] Besonders in Bezug auf GLÖZ werden acht verbindliche Standards (Richtlinien) und weitere freiwillig einzuhaltende Mindestanforderungen formuliert, die von den Mitgliedstaaten umzusetzen und von landwirtschaftlichen Betrieben einzuhalten sind. Die Kontrolle der Einhaltung dieser Auflagen erfolgt im Rahmen einer Stichprobe von in der Regel einem Prozent der Zahlungsempfänger durch die fachlich zuständigen Behörden, wie beispielsweise Naturschutzbehörden und Veterinärämter. Etwaige festgestellte Verstöße gegen

13 Der interessierte Leser sei an dieser Stelle insbesondere auf *Linden*, Definition of Compliance, International Journal of Clinical Pharmacology, Therapy and Toxicology (1981) 86 verwiesen.

14 *oV*, Cross-Compliance, deutsches Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz, 14. 6. 2009, http://www.bmelv.de/cln_182/sid_D06FFEF2474048E7C38A5FD0927F29CF/SharedDocs/Standardartikel/Landwirtschaft/Foerderung/Direktzahlungen/Cross-Compliance.html (12. 12. 2009).

15 *oV*, Cross-Compliance – Erfüllung von Umweltschutzauflagen, Europäische Kommission, Landwirtschaft und ländliche Entwicklung, 26. 3. 2009, http://ec.europa.eu/agriculture/envir/cross_com/index_de.htm (12. 12. 2009).

16 Diese Festlegung wurde in Österreich mit der INVEKOS-Umsetzungs-Verordnung, BGBl II 474 idF BGBl II 2009/492, durchgeführt.

die Vorgaben werden nach Schwere, Ausmaß und Dauer bewertet und Zahlungen entsprechend gekürzt oder im Extremfall sogar ausgesetzt.[17]

2.3 Einhaltung von (Sicherheits-)Standards: IT-Compliance

Entgegen dem eigentlichen Begriff und der häufig anzutreffenden Praxis im Umgang mit der Einhaltung von Vorgaben, ist die IT-Compliance keine Aufgabe, die allein von der IT-Abteilung oder der Rechtsabteilung zu bewältigen ist. Vielmehr ist die Unternehmensleitung einer Kapitalgesellschaft direkt davon betroffen, da sie persönlich für die Einhaltung der Vorgaben haftbar gemacht werden kann. Aus diesem Grund ist genau genommen von einem IT-Compliance-Management zu sprechen. „Angesichts der Bedeutung von IT für das Funktionieren und den Fortbestand des Unternehmens gehört es damit auch zu den Pflichten eines gewissenhaften Geschäftsführers, das Unternehmen vor erkennbaren Gefahren zu schützen. […] Das Management muss also nachweisen können, dass auch im Zusammenhang mit der IT die erforderliche Sorgfalt Anwendung gefunden hat."[18]

Die IT-Compliance umfasst somit die Einhaltung von sämtlichen gesetzlichen und vertraglichen Regelungen betreffend die Unternehmens-IT-Landschaft. Der Begriff kann definiert werden als die Überwachung und der dauerhafte Nachweis der Einhaltung von gesetzlichen Regelungen sowie selbst auferlegten Unternehmensprinzipien (analog zu der allgemeinen Definition von Compliance) hinsichtlich der IT-Anwendungen. So schreiben beispielsweise umfangreiche Vorschriften bereits heute vor, welche Sicherheitsstandards bei einem Serverbetrieb erfüllt werden müssen oder welche Daten langfristig gespeichert werden dürfen. Darüber hinaus ist beispielsweise auch geregelt, in welchen Situationen ein Datenschutzbeauftragter zu bestimmen ist und welche Dokumentationspflichten in einer IT-Abteilung bestehen. In vertraglicher Hinsicht geht es zudem um effektives Lizenzmanagement, um so zu vermeiden, dass einzelne Softwareprogramme ohne ausreichende Lizenz verwendet werden, was zu erheblichen Schadenersatzansprüchen des Lizenzgebers führen kann. Somit besteht IT-Compliance im Wesentlichen aus drei Komponenten: der Vorsorge gegen Gesetzesverstöße, der Einrichtung eines Risikomanagementsystems sowie der persönlichen Haftung des Managements bei der Verletzung der Compliance-Vorgaben.[19]

2.4 Bankwesen

Abseits der Medizin oder der Landwirtschaft haben sich sehr früh das Finanzwesen und daher auch das Bankwesen mit Compliance beschäftigt, diese als feststehenden Begriff eingeführt und in die Unternehmenskultur aufgenommen. Somit wird unter Compliance als Bestandteil des Kapitalmarktrechts die Gesamtheit der Präventivmaßnahmen in Unternehmen verstanden, welche neben der Überwachung von Gesetzen, Richtlinien und Regeln insbesondere die Vermeidung von Interessenkonflikten und die unlautere Verwendung von Insiderinformationen

17 *oV*, Cross-Compliance, deutsches Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz, 14. 6. 2009, http://www.bmelv.de/cln_182/sid_D06FFEF2474048E7C38A5FD0927F29CF/SharedDocs/Standardartikel/Landwirtschaft/Foerderung/Direktzahlungen/Cross-Compliance.html (12. 12. 2009).

18 *Rath*, Rechtliche Aspekte von IT-Compliance, in *Wecker/van Laak*, Compliance in der Unternehmenspraxis (2009) 150.

19 Vgl *Bachmann*, Rechtliche Rahmenbedingungen für das IT-Management in *Tiemeyer*, Handbuch IT-Management, Konzepte, Methoden, Lösungen und Arbeitshilfe für die Praxis[3] (2009) 666–706.

zum Gegenstand haben. „In diesem Verständnis beschreibt Compliance eine Managementfunktion, nämlich die bewusste Steuerung der sich aus dem Wertpapiergeschäft ergebenden Risiken."[20]

Aus dieser Risikosteuerungsfunktion erschließt sich die Schutzwirkung von Compliance. Sie soll bereits im Vorfeld ansetzen und beispielsweise Insidergeschäfte verhindern und dadurch dem Wertpapierdienstleistungsunternehmen bzw dem Kreditinstitut und dessen Mitarbeitern dienen. Durch die Einhaltung kapitalmarktrechtlicher Normen sollen allfällige Schadenersatzansprüche abgewehrt und die Organe sowie Mitarbeiter des Unternehmens vor strafrechtlichen Folgen geschützt werden (ähnlich der Einführung der Compliance in den USA). Es steht jedoch nicht nur der geschäftliche Erfolg im Vordergrund der Interessen der Kreditinstitute, sondern auch ihre Integrität und ihre Reputation in den „Augen der Öffentlichkeit".[21]

Die von einer Bank verfolgten Strategien für das ordnungsgemäße Verhalten der Bank im Einklang mit geltendem Recht sind somit ein wesentlicher Bestandteil der Compliance. Der Begriff beschreibt jedoch auch eine ethische Grundhaltung der Banken im Umgang mit ihren Kunden einerseits sowie andererseits die Lösung von Interessenkonflikten, die meist auf Informationsasymmetrien basieren.

Nach dieser begrifflichen Abgrenzung von Compliance im Hinblick auf die Unterscheidung nach verschiedenen Branchen folgt nun eine Erläuterung der Compliance im engeren Sinn als Teil der Corporate Governance. Hier dient Compliance als Oberbegriff für ein funktionierendes Gesamtkonzept aller aktiven Maßnahmen zur Einhaltung gesetzlicher und unternehmensinterner Vorgaben in der Unternehmensorganisation.

3. Corporate Governance und Compliance

Compliance und Corporate Governance sind verwandte Begriffe. Beide haben mit Standards für Unternehmensführung und -kontrolle zu tun.

Der angelsächsische Begriff Corporate Governance kann mit Unternehmensverfassung übersetzt werden und „bezeichnet einen Ordnungsrahmen für die Leitung und Überwachung eines Unternehmens."[22] Abgeleitet von „to govern/government" bezieht sich der Begriff ursprünglich auf das politische Herrschafts- und Steuerungsregime des Staates.[23]

Der Unterschied zwischen Corporate Governance und Compliance liegt in der Betrachtungsperspektive. Während Corporate Governance die Sichtweise der „Regulierer" prägt, umschreibt die Compliance den Blickwinkel der „Regulierten", also der betroffenen Unternehmen.[24] Corporate Governance-Grundsätze dienen der Verwirklichung einer verantwortlichen, auf Wertschöpfung ausgerichteten Leitung und Kontrolle von Unternehmen und Konzernen. Sie fördern und vertiefen das Vertrauen von Share- und Stakeholdern (gegenwärtigen und künftigen Aktionären,

20 Vgl *Löster*, Compliance im Wertpapier-Dienstleistungskonzern (2003) 11.
21 Vgl *Löster*, Compliance im Wertpapier-Dienstleistungskonzern (2003) 12.
22 Vgl dazu eingehender *Hauschka* in *Hauschka*, Corporate Compliance-Handbuch der Haftungsvermeidung im Unternehmen (2007) 2.
23 Vgl *Wieland*, Wertemanagement und Corporate Governance, Working Paper Nr 03/2002, KIeM (2002) 3.
24 Vgl dazu eingehender *Hauschka* in *Hauschka*, Corporate Compliance-Handbuch der Haftungsvermeidung im Unternehmen (2007) 2.

Fremdkapitalgebern, Mitarbeitern, Geschäftspartnern und der Öffentlichkeit auf den nationalen und internationalen Märkten). Aufsichtsrat, Vorstand und leitende Mitarbeiter des Unternehmens identifizieren sich mit ihnen und sind durch entsprechende Verpflichtungserklärungen an sie gebunden. Diese Bindung ist Teil der Verpflichtung, auch die anderen mit der unternehmerischen Tätigkeit verknüpften Interessen zu berücksichtigen.

Allgemein anerkannte Definitionen der Begriffe Compliance und Corporate Governance existieren bisher nicht.

Im Bereich der öffentlich-privaten Regulierung (dh Kodices und Standards, welche Ergebnis der Zusammenarbeit zwischen öffentlichen und privaten Akteuren sind)[25] wurde im Österreichischen Corporate Governance Kodex[26] (siehe Kapitel G.1.8, Abschnitt II) festgeschrieben, dass der Vorstand geeignete Vorkehrungen zur Sicherstellung der Einhaltung der für das Unternehmen relevanten Gesetze zu treffen hat.

Eine Reihe von weiteren OECD-Ländern verfolgt ähnliche Bemühungen, um „gute Regeln" in Form von allgemein akzeptierten Maßnahmen für die Wirtschaft politisch zu forcieren.

Der Deutsche Corporate Governance Kodex (DCGK) stellt eine kodifizierte Umschreibung des Begriffes Compliance zur Verfügung. Diese Definition richtet sich zwar in erster Linie an börsenotierte Aktiengesellschaften, kann aber durchaus als allgemeine Definition herangezogen werden. Sie besagt, dass der Vorstand für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen hat und auf deren Beachtung durch die Konzernunternehmen hinwirkt (Compliance).[27] Hinzuweisen ist darauf, dass die deutsche Kodex-Kommission die Pflicht zur Compliance (gem der eingangs präsentierten Definition) nicht nur auf die Beachtung der gesetzlichen Bestimmungen beschränken will, sondern auch die regulativen Vorgaben einbezogen hat, sodass sich die Compliance-Verantwortung vor allem auf die Bestimmungen von Satzung und Geschäftsordnung, aber darüber hinaus beispielsweise auch auf Ethikrichtlinien, Merk- und Informationsblätter, Arbeitsanweisungen und Konzernrundschreiben erstreckt.

Über die jeweiligen gesetzlichen Vorgaben hinausgehende Ergänzungen werden auch als „soft law" bezeichnet. Soft law ist definiert als von Vertragsparteien anerkannte und kodifizierte Regeln, die aber nicht durch dritte Parteien erzwungen werden können.[28] Ohne Loyalität, Integrität und Ehrlichkeit der Vertragspartner, hier also des Vorstandes, aber auch aller Mitarbeiter gegenüber dem Unternehmen ist dies nicht umzusetzen. Soft law als Selbstbindungsmechanismus setzt zu seiner Wirksamkeit die moralische Selbstbindung der involvierten organisationellen und individuellen Akteure voraus.[29]

Nach diesen begrifflichen Abgrenzungen und Einordnungen werden nun Maßnahmen zur Einhaltung rechtlicher und regulativer Vorgaben im Unternehmen vorgestellt. Zu diesem Zweck erfolgt im Folgenden eine kurze Darstellung der Ziele und Instrumente einer Compliance-Organisation.

---

25 *Wieland* in *Wieland/Steinmeyer/Grüninger*, Handbuch Compliance-Management, 16.

26 Österreichischer Corporate Governance Kodex Fassung Jänner 2010, Hrsg: *Österreichischer Arbeitskreis für Corporate Governance*, vgl dazu die Ausführungen unter Punkt 6.2.2.

27 Regierungskommission, Deutscher Corporate Governance, geltende Fassung vom 26. 5. 2010.

28 Vgl *Wieland*, Wertemanagement und Corporate Governance, Working Paper Nr 03/2002, KIeM (2002) 4.

29 Vgl *Wieland*, Wertemanagement und Corporate Governance, Working Paper Nr 03/2002, KIeM (2002) 4.

4. Ziele und Instrumente einer Compliance-Organisation

Um die Einhaltung der Compliance-Vorgaben auch organisatorisch im Unternehmen zu verankern und eine Umsetzung zu gewährleisten, übernimmt eine organisatorische Einheit bzw Stelle die Erfassung von möglichen Interessenkonflikten sowie die Anwendung und Koordinierung von Strategien der Konfliktbehandlung. „In einem funktionalen Zusammenhang wird von der Compliance-Organisation gesprochen, die als Teil der Unternehmensorganisation die Menge aller Compliance-Stellen[30] umfasst. Die Compliance-Organisation ist somit für die Umsetzung eines Compliance-Konzeptes und für die Erfüllung der Compliance-Aufgaben verantwortlich."[31]

In den folgenden Abschnitten werden die „Säulen" der Corporate Governance kurz vorgestellt: Risikomanagement, interne Kontrollsysteme und interne Revision.

4.1 Risikomanagement

Reduzierung oder gar Vermeidung von Risiken und die Einhaltung von Normen in einem Unternehmen beginnen mit der Organisation von Informationsflüssen. Die Risikohandhabung in der Unternehmensführung wird häufig einer spezifischen Funktion oder Institution zugeordnet: der des Risikomanagements. Dessen Hauptaufgaben sind der Schutz vor negativen Veränderungen der Rahmenbedingungen der unternehmerischen Tätigkeiten und die Erfassung und Beeinflussung der Risikoursachen.[32] Durch die Integration von Compliance in die Prozessmodelle wird Transparenz geschaffen und werden die Risiken reduziert: Neben den bekannten Risiken aus Geschäften und Prozessen auch Risiken aus Verhalten, auf die ein Risikomanagement sensibel und präventiv reagieren muss.[33]

Allgemein umfasst das Risikomanagement die systematische Erfassung und Bewertung von sowie die Steuerung von Reaktionen auf festgestellte Risiken. Hierbei ist der erste prozessuale Schritt die Identifikation von Risiken, welche durch verschiedene Methoden erfolgen kann. Darüber hinaus beinhaltet das Risikomanagement auch die Risikosteuerung, die wiederum die Risikovermeidung, -verminderung, -begrenzung, -überwälzung und -akzeptanz zum Gegenstand hat. Nach der Erfassung und der Steuerung der Risiken folgt als letzter Schritt idealtypisch die Kontrolle, die auch als Risiko-Monitoring bezeichnet wird.[34]

4.2 Interne Kontrollsysteme

Neben dem Risikomanagement dienen interne Kontrollsysteme als Maßnahmen zur Einhaltung gesetzlicher und unternehmensinterner Vorgaben sowie zur Abwehr von Schäden. Ein internes Kontrollsystem umfasst neben Weisungen (zB schriftliche Anordnungen zur Sicherheit, zur Geheimhaltung von Betriebsgeheimnissen und zur Kommunikation mit der Öffentlichkeit bzw Presse) auch Aktivitäten – wie beispielsweise Zutrittskontrollen – sowie Maßnahmen zum Schutz der materiellen und immateriellen Vermögenswerte. Weiters können Maßnahmen

30 Vgl hierzu Punkt 5.

31 *Ehrler*, Compliance in Universalbanken, Strategien für das Management von Interessenkonflikten (1997) 5.

32 *Mikus*, Risiken und Risikomanagement – ein Überblick in *Götz/Henselmann/Mikus*, Risiko-Management (2001) 9 f.

33 Vgl *Wieland*, Wertemanagement und Corporate Governance, Working Paper Nr 03/2002, KIeM (2002) 4.

34 *Wolke*, Risiko-Management[2] (2008) 4 f.