Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Open C³S
Open Competence Center for Cyber Security

Master IT GRC Management

Grundlagen IT Governance, Risk and Compliance Management

Autoren:
Prof. Dr. Nils Herda
Prof. Dr. Stefan Ruf
M. Eng. Christoph Wabersich

Hochschule Albstadt-Sigmaringen

Modul 102

Grundlagen IT Governance, Risk and Compliance Management

Studienbrief 1: Bedeutung und Motivation

Studienbrief 2: Corporate Governance

Studienbrief 3: Risikomanagement

Studienbrief 4: Compliance

Studienbrief 5: IT-GRC

Autoren:

Prof. Dr. Nils Herda

Prof. Dr. Stefan Ruf

M. Eng. Christoph Wabersich

---

1. Auflage

Hochschule Albstadt-Sigmaringen

Bundesministerium
für Bildung
und Forschung

AUFSTIEG DURCH BILDUNG >>
OFFENE HOCHSCHULEN

Institut für Wissenschaftliche Weiterbildung
Studiengang IT Governance, Risk and Compliance Management
Steinachstraße 11
72336 Balingen

1. Auflage (01. März 2015; aktualisiert)

Didaktische und redaktionelle Bearbeitung:
Bärbel Wolf-Gellatly

Um die Lesbarkeit zu vereinfachen, wird auf die zusätzliche Formulierung der weiblichen Form bei Personenbezeichnungen verzichtet. Wir weisen deshalb darauf hin, dass die Verwendung der männlichen Form explizit als geschlechtsunabhängig verstanden werden soll.

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung, und Forschung unter dem Förderkennzeichen 16OH11066 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

Inhaltsverzeichnis

Einleitung zu den Studienbriefen

I. Abkürzungen der Randsymbole und Farbkodierungen

Beispiel	B
Definition	D
Exkurs	E
Kontrollaufgabe	K
Merksatz	M
Quelltext	Q
Übung	Ü

II. Zu den Autoren

Prof. Dr. Nils Herda, Dozent | Autor
verfügt über mehr als 15 Jahre aktive Management-Erfahrung in der IT. Er begann seine Laufbahn als Unternehmensberater für SAP-Standard-Software und war nach seiner Promotion in Software-Engineering Vorstandsassistenz der Landesbank Baden-Württemberg (LBBW). Anschließend wechselte er zur Excelsis Business Technology AG und war zuletzt Geschäftsführer der deutschen und der schweizerischen Gesellschaft.
Seit 2013 ist er Professor für Wirtschaftsinformatik, insbesondere ERP-Systeme und unternehmensübergreifende Geschäftsprozesse, an der Hochschule Albstadt-Sigmaringen. Professor Herda ist zudem als internationaler Gutachter tätig und veröffentlicht auch regelmäßig zu den Themen ERP, IT-GRC, IT-Management und Mobile Business.

Prof. Dr. Stefan Ruf, Dozent | Autor
studierte Wirtschaftsinformatik in Göttingen und absolvierte seine Promotion in Tübingen. Der Schwerpunkt seiner Forschungsarbeit lag dort in der Konzeption eines prozessorientierten Referenzmodells für das Risikomanagement.
Gegenwärtiger Forschungsschwerpunkt von Prof. Ruf ist die Analyse von Sicherheit und Risiko in Cloud-Architekturen unter Beachtung relevanter gesetzlicher Bestimmungen.
Prof. Ruf begann seine berufliche Laufbahn bei der Boston Consulting Group in Frankfurt und war vor seiner Berufung zehn Jahre lang mit der Konzeption und Leitung elektronischer Vertriebswege bei einem großen Finanzdienstleister betraut.
Seit 2010 ist Stefan Ruf Professor an der Hochschule Albstadt-Sigmaringen, berufen für das Lehrgebiet Informationsmanagement. Prof. Ruf leitet seit 2012 als Studiendekan das Masterprogramm „IT Governance, Risk and Compliance Management“.

M. Eng. Christoph Wabersich | Autor
hat an der Hochschule Albstadt-Sigmaringen den Bachelor-Studiengang „Kommunikations- und Softwaretechnik“ und den Master-Studiengang „Systems Engineering“ abgeschlossen. Im Rahmen seiner Master-Thesis definierte und realisierte er die Systemüberwachung des Rechenzentrums der Firma Geberit.
Seine berufliche Laufbahn begann Christoph Wabersich bei der Firma Intec International GmbH, wobei seine Schwerpunkte im Bereich des Systemmonitorings und der Softwareentwicklung lagen.
Seit 2012 ist Christoph Wabersich für das Open Competence Center for Cyber Security als Modulentwickler tätig sowie für die Betreuung der Module in den Fachgebieten Informatik und Informationstechnik des Masterstudiengangs „IT Governance, Risk and Compliance Management“, verantwortlich.

III. Modullehrziele

Das Modul „Grundlagen IT Governance, Risk and Compliance Management“ vermittelt eine Einführung und die Grundlagen der Corporate Governance, des Risikomanagements und der Compliance. Die Begrifflichkeiten, grundlegenden Konzepte, Aufgaben und Ziele der drei Themenbereiche werden ausführlich erläutert.

Der erste Studienbrief „Bedeutung und Motivation“ legt die Gründe für die immer größere Bedeutung der drei Themenbereiche Governance, Risikomanagement und Compliance (kurz: GRC) dar und verdeutlicht die Notwendigkeit für Unternehmen, sich mit GRC auseinanderzusetzen. Weiterhin gibt dieser erste Studienbrief einen kurzen Überblick über bedeutsame Meilensteine, die in der historischen Entwicklung und für den starken Bedeutungsgewinn von GRC ausschlaggebend waren.

Der zweite Studienbrief „Corporate Governance“ vermittelt die Grundlagen im Bereich der Governance. Begrifflichkeit, Bedeutung, Aufgaben, Anforderungen und Ziele einer unternehmensweiten Governance sowie die Notwendigkeit zur Etablierung einer qualitativen Corporate Governance in der betrieblichen Praxis werden erläutert. Weiterhin werden die Prinzipien der Corporate Governance und die wichtigsten Elemente einer angemessenen Aufbauorganisation dargestellt. Ein kurzer Überblick über die relevanten Aufgaben zur Etablierung der Corporate Governance im Unternehmen sowie die grundlegenden Aspekte der Prüfung der Corporate Governance bildet den Abschluss des Studienbriefs.

Der dritte Studienbrief „Risikomanagement“ vermittelt die Grundlagen im Bereich des Risikomanagements. Die Begriffe Risiko und Risikomanagement, dessen Bedeutung, Aufgaben und Ziele werden ausführlich erläutert. Aufbau- und Ablauforganisation des Risikomanagements in der betrieblichen Praxis werden sowohl auf strategischer als auch auf operativer Ebene dargestellt. Weiterhin folgt die Vermittlung der Grundlagen zur Einführung eines effektiven Risikomanagementsystems im Unternehmen und zu dessen Prüfung.

Der vierte Studienbrief „Compliance“ vermittelt die Bedeutung, Aufgaben, Anforderungen und Ziele des Compliance-Managements. Die Anwendungsfelder in der betrieblichen Praxis werden dargelegt und ein Überblick über die Aufbau- und Ablauforganisation des Compliance-Managements im Unternehmen gegeben. Abschließend folgt die Vermittlung der notwendigen Kenntnisse zur betrieblichen Einführung eines effektiven Compliance-Managementsystems und der Grundlagen zur Prüfung des Compliance-Managements.

Der letzte Studienbrief „IT-GRC“ verdeutlicht den Zusammenhang aller drei Themenbereiche unter einer ganzheitlichen Betrachtung. Daneben wird die Rolle und Bedeutung der IT für alle drei Themenbereiche erläutert.

Nach dem Abschluss dieses Moduls kennen Sie alle wichtigen Grundlagen der drei Themenbereiche Governance, Risikomanagement und Compliance. Sie können die Begrifflichkeiten definieren und verstehen ihren Zusammenhang. Weiterhin sind Sie in der Lage, Managementsysteme für alle drei Themenbereiche zu konzipieren, im Unternehmen einzuführen und diese auf Korrektheit, Vollständigkeit und Effektivität zu prüfen.

Studienbrief 1 Bedeutung und Motivation

1.1 Einführung

1.1.1 Lernergebnisse

- Sie haben die Motivatoren und Treiber für die drei Themenbereiche Governance, Risikomanagement und Compliance erfasst und können diese wiedergeben.
- Sie haben die Bedeutung von Governance, Risikomanagement und Compliance für Unternehmen und die Notwendigkeit für die Auseinandersetzung mit den Themenbereichen erfasst und können diese erläutern.
- Sie sind in der Lage, die Notwendigkeit und Erfordernisse zur Einführung und Ergreifung geeigneter Mechanismen, Maßnahmen und Vorkehrungen zu erläutern sowie dessen Nutzen zu bewerten.

1.1.2 Advance Organizer

Vorkenntnisse

Für den ersten Studienbrief „Bedeutung und Motivation“ sind keine Vorkenntnisse erforderlich. Dieser Studienbrief bietet für Einsteiger und Neulinge in dieser Thematik genügend Materialien in Form von Hinweisen, Übungen und Grafiken, um einen grundlegenden Wissensstand zu schaffen und soll alle Teilnehmer auf einen einheitlichen Wissensstand bringen.

Einordnung

Die behandelten Themen stellen die Notwendigkeit und Bedeutung von Governance, Risikomanagement und Compliance im unternehmerischen Kontext dar und sind für das Verständnis der Bedeutung der nachfolgenden Module wichtig: Welche Bedeutung haben die Themen Governance, Risikomanagement und Compliance und warum erfuhren sie in den letzten Jahre diesen enormen Bedeutungszuwachs? Welche Gründe gibt es für Unternehmen sich damit auseinanderzusetzen?

1.1.3 Überblick

Motivation und Entwicklung

Der erste Teil dieses Studienbriefs erläutert die Motivatoren für Governance, Risikomanagement und Compliance im Unternehmen. Verschiedene Fallbeispiele verdeutlichen die Notwendigkeit für die Auseinandersetzung mit GRC. Nachfolgend wird ein kurzer Überblick über wichtige Meilensteine gegeben, die für die historische Entwicklung und den starken Bedeutungszuwachs von Governance, Risikomanagement und Compliance ausschlaggebend waren.

Einordnung und Bedeutung

Der zweite Teil setzt sich mit der Einordnung der drei Themenbereiche Governance, Risikomanagement und Compliance in den unternehmerischen Kontext auseinander. Die Bedeutung von Governance, Risikomanagement und Compliance für Unternehmen wird erläutert.

Ausblick Studienbrief 2 „Corporate Governance“ bietet mit seiner Einführung einen Überblick über die Grundlagen einer qualitativen Governance im Unternehmen.

1.2 Einleitung

In jedem Unternehmen gibt es Situationen und Umstände, die Gefahren bergen und verheerende Folgen nach sich ziehen können. Die Anzahl an Krisen, Insolvenzen und Zusammenbrüchen von Unternehmen ist hoch. Vor diesem Hintergrund ist für Unternehmen und Regierungen die Beschäftigung und Auseinandersetzung mit potenziellen Krisen und Risiken sowie deren Prävention unausweichlich. Sie müssen sich an die Entwicklung von Bedrohungen anpassen und sich ihnen an jedem möglichen Eintrittspunkt stellen.

Aus diesen Gründen werden seit einiger Zeit jedes Jahr eine Vielzahl an neuen Vorgaben und Regelungen (Gesetze, Vorschriften, Verordnungen, Normen, Standards, Richtlinien, Best Practices und Empfehlungen) zur Verbesserung und Gewährleistung einer ordnungsgemäßen Unternehmensführung und -kontrolle erlassen. Inzwischen ist jedes Unternehmen und jeglicher Bereich der unternehmerischen Aktivitäten von Vorgaben und Regelungen betroffen; von der Finanzberichterstattung, der Kontrolle der Materialverwendung, der Qualität der Produkte und Dienstleistungen, der Vertraulichkeit und Integrität wichtiger Daten und Informationen, der Unversehrtheit der Mitarbeiter bis zur langfristigen Speicherung von Geschäftskorrespondenzen.

Aus der Nichtbeachtung von oder potenziellen Verstößen gegen geltende Vorgaben und Regelungen resultieren Risiken, die zu schwerwiegenden Folgeschäden für ein Unternehmen führen können. Vorgaben und Regelungen einzuhalten und Gefahren in Bezug auf Risiken, Regelverstöße oder Missmanagement rechtzeitig zu erkennen, um gegebenenfalls zeitnah und zielgerichtet handeln zu können, ist eine Notwendigkeit zur Sicherung des Unternehmenswohls.

Durch die zunehmende Internationalisierung der Unternehmen stellt die Wahrung des Überblicks über und die Einhaltung aller relevanten Vorgaben und Regelungen, die stetig zunehmen und häufig permanenten Änderungen unterliegen, eine komplexe Herausforderung dar. Die Erkennung und Beherrschung von Risiken, die Einhaltung aller relevanter Vorgaben und Regelungen sowie ein ordnungsgemäßes, ethisch und moralisch vertretbares Verhalten müssen Teil und Zielsetzung eines modernen Führungssystems zur Leitung und Überwachung eines Unternehmens sein.

Ein effektives Compliance- und Risikomanagement ist Voraussetzung für eine gute Governance, welche wiederum der Compliance und dem Risikomanagement dient. Dementsprechend sind die Führungsstrukturen und -systeme im Unternehmen so zu gestalten, dass eine erfolgreiche Berücksichtigung und effektive Verwirklichung der verflochtenen Bereiche der Corporate Governance, des Risikomanagements und der Compliance (kurz: GRC) erzielt respektive unterstützt wird.

1.3 Motivation für Governance, Risikomanagement und Compliance

Im Zuge einer Vielzahl an Unternehmensskandalen und -zusammenbrüchen, die weltweites Aufsehen erregten, rückten die drei Themenbereiche Governance, Risikomanagement und Compliance immer stärker in den Fokus der Öffentlichkeit. Spätestens die von den USA ausgehende Wirtschafts- und Finanzkrise 2007 machte die Notwendigkeit einer ordnungsgemäßen Unternehmensführung sowie von mehr Transparenz und Kontrolle für Unternehmen deutlich.

B

Beispiel 1.1: Auswirkungen einiger Unternehmensskandale

Insbesondere einige Skandale größerer Unternehmen (wie bspw. Enron und WorldCom) lenkten die öffentliche Aufmerksamkeit auf das Missmanagement vieler Unternehmen und lösten eine Kettenreaktion an aufgedeckten Unternehmensskandalen und -zusammenbrüchen aus.

Nicht weniger als 158 Unternehmen, deren Aktien an der Börse gehandelt wurden, mussten im Jahr 2002 ihre Zahlen für das vergangene Geschäftsjahr korrigieren. Die Börse erlitt, durch die Enttäuschungen der Aktionäre und den entstandenen Vertrauensverlust einen enormen Wertverlust. Der teils enorme Kurssturz vieler Aktien vernichtete rund 8 000 Milliarden US-Dollar. Auch ausländische Investoren, die zuvor auf die Stärke der US-Währung vertrauten, zogen innerhalb weniger Wochen über 37 Milliarden US-Dollar ab.[1]

Viele Skandale, wie Bestechungen, Betrugsfälle, Bilanzmanipulationen oder risikoreiche Spekulationsgeschäfte, die dem Finanzmarkt erheblich zusetzten, wurden durch fehlende Vorgaben und Regelungen sowie eine mangelhafte Kontrolle ermöglicht. Aus einer Vielzahl an zumindest bedenklichen Entscheidungen und Handlungen, denen fehlende soziale Verantwortung unterstellt werden kann, resultierte die Forderung nach einer besseren Unternehmensführung, rechtskonformen Verhalten sowie ethisch und moralisch vertretbarem Handeln, kontrolliert durch fest definierte und bindende Vorgaben und Regelungen und unter einem vernünftigen Risikomanagement.

Die weltweit stark zunehmende Wirtschafts- und Computerkriminalität ist ein weiterer Treiber für die Auseinandersetzung mit GRC. Durch die Optimierung und Überwachung von Arbeits- und Geschäftsprozessen sowie eine höhere Transparenz können Betrugsfälle reduziert und gegebenenfalls schneller respektive leichter aufgedeckt werden.

Die Bedeutung von GRC hat sich in den letzten Jahren stark erhöht. GRC-Anforderungen sind heute durch eine Vielzahl an Vorgaben und Regelungen bindend und sollen Risiken, grobes Missmanagement oder gezielte Manipulationen

[1] [vgl. Ogger, 2003]

einschränken sowie frühzeitig aufzeigen, um durch entsprechende Maßnahmen angemessen und schnellstmöglich reagieren zu können.

Die Verwirklichung eines effizienten GRC-Managements unterstützt sowohl eine langfristig wertorientierte Perspektive zur Vermeidung größerer Schäden im respektive für Unternehmen, als auch eine direkte Wertsteigerung für das Unternehmen selbst.

B

Beispiel 1.2: Unternehmensskandale in Deutschland

Einige der größten Unternehmensskandale[2] der letzten Jahre in Deutschland waren beispielsweise:

- Telekom (2008): Bespitzelung der eigenen Manager und Aufsichtsräte; der Leiter der Konzernsicherheit wurde zu über drei Jahren Haft verurteilt
- Volkswagen (2005): Bestechungsskandal (Firmenleitung besticht Betriebsrat); Haftstrafen bis zu 2 Jahren
- Daimler (2010): Bestechungsskandal (Geschenke und Bestechungsgelder an Regierungsbeamte für Aufträge); 185 Millionen US-Dollar Strafe in den USA
- Deutsche Bank (2011): Verkauf riskanter Produkte ohne Aufklärung über deren Risiken; 145 Millionen US-Dollar Strafe in den USA
- Eon und Gaz de France: Illegale Absprache beim Bau einer Pipeline (1975); Kartellstrafe von jeweils über 550 Millionen Euro
- Heidelberg Cement (2003): Künstliche Preistreiberei; 170 Millionen Euro Bußgeld
- Henkel AG (2011): Absprachen mit Wettbewerber; 92 Millionen Euro Strafe
- Infineon (2005): Bestechlichkeit, Untreue, Korruption; Auflösung des Vorstandes
- MAN (2009): Bestechungsskandal (Bestechungsgelder an Kunden für Aufträge); 150 Millionen Euro Bußgeld
- Siemens (2008): Korruptionsskandal (über 4 000 Schmiergeld-Zahlungen); ca. 1 Milliarde US-Dollar Strafe (600 Millionen Euro Strafe in den USA, 395 Millionen Euro Strafe in Europa)

[2] vgl. http://www.handelsblatt.com/unternehmen/buero-special/compliance-die-groessten-skandale-in-deutsch
6641352.html (Zugriff 2014-09-23)

1.3.1 Fallbeispiel 1: Der Enron-Skandal

Ende 2001 erreichte eine Reihe von Unternehmensskandalen mit dem Konkurs der Enron Corporation einen Höhepunkt. Der Enron-Skandal gehört zu den bekanntesten Fällen des Wirtschaftsbetrugs und Missmanagements und versetzte dem Finanzmarkt in den USA einen schweren Treffer. US-Aktien verzeichneten im ersten Halbjahr 2002 ihren schärfsten Rückgang seit 30 Jahren.

Im Jahr 2000 gehörte Enron mit über 20.000 Mitarbeitern zu den 10 größten Unternehmen der USA und war mit einem Umsatz von mehr als 100 Milliarden US-Dollar sowie einem Gewinn von einer Milliarde einer der erfolgreichsten Energiekonzernen in den USA.[3] 2001 erfolgte der erschreckende Absturz. Die Enron-Aktie fiel von 79,88 US-Dollar (2. Januar 2001) auf 67 Cent (10. Januar 2002). Am 2. Dezember 2001 meldete Enron Konkurs an.[4] Tausende verloren ihre Anstellung, ihre Altersvorsorge und ihre Einlagen. Zugleich wurden einige Topmanager und Vorstandsmitglieder reich, genehmigten sich Abfindungen von 50 Millionen US-Dollar.

Heute ist Enron vor allem bekannt durch „zweifelhafte Geschäftspraktiken, Selbstbereicherung von Angestellten, unzureichende interne Kontrollen, gleichgültige Aufsichtsbehörden, Fehler bei der Wirtschaftsprüfung, eine Firmenkultur, die jeden Mitarbeiter aufforderte, Grenzen zu testen, und dabei über ihr Ziel hinausschoss“.[5]

Durch Buchalter-, Bilanzierungs- und Finanztricks hielt Enron seinen Aktienkurs künstlich hoch. Enron brach jegliche Integritätsgrenzen mit dem Ziel, den Wert des Unternehmens zu steigern und Geld zu machen. Die Ertragslage von Enron erschien durch viele Manipulationen und Tricks hervorragend.

Enron gründete unzählige Tochter- und Partnerunternehmen (z. B. Chewca, Jedi, LJM Cayman, LJM2, Raptor, Talon oder Marlin), die zwar von Enron kontrolliert wurden, doch auf dem Papier nicht dem Konzern zugeordnet waren und in den Konzernberichten bloß als Fußnoten erwähnt wurden. Laut geltendem Gesetz war es dafür lediglich notwendig, dass Enron nicht mehr als 97 Prozent an einer Firma besaß. So kauften die eigenen Manager geringe Anteile von 3 Prozent der Tochter- oder Partnerfirma und ließen diese damit aus den Büchern von Enron verschwinden. Schulden und Verluste konnten nun den Tochter- und Partnerunternehmen zugeschrieben werden. Gewinne verbuchte Enron.

Weitere ethisch kaum vertretbare Tricks waren der Verkauf von Unmengen an Strom an die eigenen Tochter- und Partnerunternehmen, um die Preise künstlich in die Höhe zu treiben oder die aggressive Nutzung des „mark-to-market accounting“. Dabei wurden die Erträge aus mehrjährigen Geschäften unmittelbar gutgeschrieben.[6]

[3] [vgl. Fischermann and Kleine-Brockhoff, 2002]
[4] [vgl. Schramm, 2005, S. 2]
[5] [vgl. Fischermann and Kleine-Brockhoff, 2002]
[6] [vgl. Schramm, 2005, S. 3]

Studienbrief 2 Corporate Governance

2.1 Einführung

2.1.1 Lernergebnisse

- Sie haben die relevanten Grundlagen im Themenbereich des Corporate Governance erfasst und können diese wiedergeben.
- Sie sind in der Lage, den Begriff Corporate Governance zu erklären.
- Sie haben die Aufgaben, Anforderungen und Zielen einer unternehmensweiten Governance erfasst und können diese darlegen.
- Sie können die Notwendigkeiten und Erfordernisse zur Verwirklichung einer qualitativen Corporate Governance im Unternehmen verdeutlichen.
- Sie sind imstande, die Prinzipien einer guten Corporate Governance anzuwenden.
- Die wichtigsten Elemente eines effektiven Corporate Governance-Systems können Sie benennen.
- Sie können ein Corporate Governance-System konzipieren.
- Sie sind in der Lage ein Corporate Governance-System in die betriebliche Praxis einführen.
- Sie sind in der Lage, eine Prüfung der unternehmensweiten Governance durchzuführen.

2.1.2 Advance Organizer

Vorkenntnisse

Für den Studienbrief „Corporate Governance“ sind keine Vorkenntnisse erforderlich. Dieser Studienbrief bietet für Einsteiger und Neulinge in dieser Thematik genügend Materialien in Form von Hinweisen, Übungen und Grafiken, um einen grundlegenden Wissensstand zu schaffen und soll alle Teilnehmer auf einen einheitlichen Wissensstand bringen.

Einordnung

Die behandelten Themen stellen die Bedeutung, Funktion und Funktionsweise einer qualitativen Governance im Unternehmen dar und sind für das Verständnis der Bedeutung der nachfolgenden Module wichtig.

2.1.3 Überblick

Motivation, Zielsetzung, Definition

Der erste Teil dieses Studienbrief erläutert die Bedeutung, Funktion und Zielsetzung einer qualitativen Governance im Unternehmen. Es folgt eine ausführliche Definition des Begriffs „Corporate Governance“.

Corporate Governance-System

Der zweite Teil setzt sich mit der Corporate Governance in der betrieblichen Praxis auseinander. Aufbau- und Ablauforganisation, sowie die Prinzipien und wichtigen Elemente eines Corporate Governance-Systems werden erläutert.

Regelbetrieb

Der dritte Teil dieses Studienbriefs beschreibt die betriebliche Einführung eines Corporate Governance-Systems bis hin zum Regelbetrieb. Eine Erläuterung wichtiger Grundlagen für die Prüfung von Corporate Governance-Systemen rundet diesen Studienbrief ab.

Ausblick

Der nächste Studienbrief „Risikomanagement“ bietet eine Einführung in und einen Überblick über die Grundlagen des Risikomanagements im Unternehmen.

2.2 Einleitung

Der Wert eines Unternehmens wird in der Regel am wirtschaftlichen Erfolg gemessen. Doch nicht nur die Höhe des Umsatzes und des Gewinns sind von zentraler Bedeutung, auch die Art und Weise der Unternehmensführung sowie das Unternehmensimage sind in heutiger Zeit ausschlaggebende Faktoren für den Unternehmenserfolg. Seit einigen Jahren rücken insbesondere Prinzipien guter Unternehmensführung, wie ethische und moralische Werte, ein verantwortungsvolles und risikobewusstes Handeln oder die Motivation der Angestellten immer stärker in den Vordergrund.

Vor allem in Folge von Börsen- und Unternehmensskandalen, mit teilweise milliardenschweren Schäden, gewann das Thema Corporate Governance stark an Bedeutung. Als deren Ursache werden eine von Management- und Eigeninteressen getriebene Unternehmensführung, in Kombination mit mangelhafter Aufsicht und Kontrolle, identifiziert.

2.3 Motivation und Zielsetzung

Motivation

Eine hohe Qualität der Corporate Governance gewinnt für Unternehmen zunehmend an Wichtigkeit. Effiziente und transparente Corporate Governance Maßnahmen und Strukturen werden bei Anlageentscheidungen oft die gleiche Bedeutung wie finanziellen Kennzahlen beigemessen, institutionelle Investoren zahlen häufig Prämien für Unternehmen mit hohen Standards in der Unternehmensführung, -kontrolle und -überwachung. Zusätzlich fordert die Öffentlichkeit von Unternehmen die bewusste Wahrnehmung ihrer gesellschaftlichen Verantwortung sowie moralisch und ethisch vertretbare Handlungen.

Ziele der Corporate Governance

Corporate Governance soll eine

- verantwortungsvolle,
- qualifizierte,
- transparente und

- auf den nachhaltigen Erfolg ausgerichtete

Führung des Unternehmens nach langfristigen Zielen und Strategien gewährleisten. Dabei nimmt die Corporate Governance ebenfalls eine Überwachungs- und Kontrollfunktion für die Gewährleistung der Leistungsfähigkeit und des Unternehmenswohls sowie eine Beratungsfunktion für die Verbesserung und Professionalisierung der Unternehmensführung, -kontrolle und -überwachung ein (Abbildung 2.1).

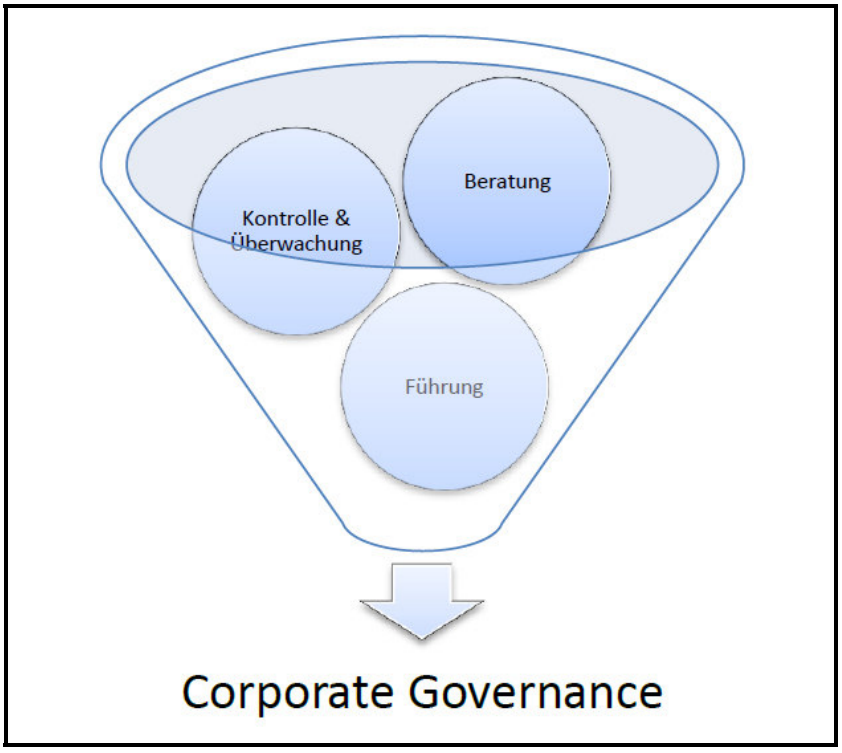

Abb. 2.1: Corporate Governance

Eine gute Corporate Governance verhilft Unternehmen zu einer hohen Reputation, positiveren Einschätzungen und Bewertungen, mindert Risiken und Schäden durch ungewollte Sachverhalte oder Handlungen, fördert ein höheres Vertrauen (z. B. von Anlegern, Kreditgeber oder Mitarbeitern) und erzielt letztendlich eine direkte als auch indirekte Wertsteigerung sowie Unternehmenssicherung.

2.4 Begriffssystem

Problemstellung

Aus der Trennung von Eigentum, Leitung und Kontrolle resultieren unterschiedliche Interessenlagen für die verschiedenen Stakeholder (Interessengruppen) eines Unternehmens.[1] Um ein Unternehmen sowie alle Stakeholder vor Schäden durch Handlungen einzelner Interessengruppen im Eigeninteresse zu schützen und zu gewährleisten, dass alle Handlungen und Entscheidungen die Unternehmensziele und -strategie unterstützen, muss der Handlungsspielraum einzelner Interessengruppen durch Vorgaben und Maßnahmen eingeschränkt und kontrolliert werden.

[1] [vgl. Zöllner, 2007, S. 9]

Aufgabe der Corporate Governance

Dies ist Aufgabe der Corporate Governance. Dabei unterliegt sie den ständig zunehmenden rechtlichen, gesellschaftlichen, geschäftlichen, qualitativen und regulatorischen Anforderungen, Vorgaben und Regelungen und umfasst alle nationalen und internationalen Gesetze, Vorschriften, Verordnungen, Normen, Richtlinien, Standards und Grundsätze für eine verantwortungsvolle, qualifizierte, transparente und auf den langfristigen Erfolg ausgerichtete Unternehmensführung. Eine erfolgreiche Corporate Governance dient dem Unternehmen selbst, als auch sämtlichen Stakeholdern wie Teilhabern, Aktionären, Kreditgebern, Mitarbeitern, Kunden und Lieferanten sowie der Gesellschaft und dem Staat.

Hauptinteressenten

Damit betrifft Corporate Governance vor allem die Unternehmen, bei denen mehrere Stakeholder mit eigenen Interessen existieren. Für börsennotierte Unternehmen ist das Thema Corporate Governance von besonderer Wichtigkeit, da hier die Trennung zwischen Eigentum, Leitung und Kontrolle sehr ausgeprägt ist.[2] Allerdings sind zunehmend auch andere Rechtsformen, kleine und mittlere oder öffentliche Unternehmen respektive Organisationen von der Thematik betroffen und werden unter dem Blickwinkel ihrer spezifischen Anforderungen an die Corporate Governance analysiert.[3]

Verschiedene Definitionsansätze

Eine allgemeingültige, weltweit einheitliche Definition für den angelsächsischen Begriff Corporate Governance existiert nicht. Die verschiedenen Definitionsansätze unterscheiden sich hauptsächlich in der Ausdehnung des Begriffs und somit der Berücksichtigung der Anforderungen und Interessengruppen bzw. deren Ansprüche[4]:

- Shareholder-orientierte Definitionsansätze stellen die Beziehung zwischen Eigentümern und Kapitalgebern in den Vordergrund (ursprüngliches, angloamerikanisches Corporate Governance-System).
- Stakeholder-orientierte Definitionsansätze weiten die berücksichtigten Anforderungen aus und beziehen die Interessen aller Stakeholder mit ein.
- Ressourcenorientierte Definitionsansätze stellen das Unternehmen selbst, die Gewährleistung der Wettbewerbsfähigkeit und die Maximierung der Überschüsse durch eine effiziente Unternehmensführung und -kontrolle in den Vordergrund.

Abgrenzung

Corporate Governance weist weitgehende Überscheidungen mit dem deutschen Begriff Unternehmensverfassung auf. Die Unternehmensverfassung bezeichnet die Gesamtheit der (langfristig) festgelegten Vorgaben und Regelungen für ein Unternehmen. Sie umfasst jedoch hauptsächlich die innere Ordnung eines Unternehmens (Festlegung verschiedener Informations- und Entscheidungsrechte unterschiedlicher Interessengruppen), Corporate Governance beschäftigt sich dagegen auch mit der (rechtlichen und faktischen) Einbindung des Unternehmens in dessen Umfeld. Weiterhin wird Corporate Governance häufig mit den Begriffen

[2] [vgl. Zöllner, 2007, S. 9]
[3] [vgl. Werder, 2008, S. 2f.]
[4] [vgl. Zöllner, 2007, S. 8ff.]

Unternehmensführung und -kontrolle gleichgesetzt, was aber ebenfalls keiner vollständigen Übereinstimmung entspricht.[5]

Interne & externe Corporate Governance

Es kann zwischen einer internen und externen Corporate Governance unterschieden werden. Die interne Sicht bezieht sich auf das Zusammenwirken der Unternehmensorgane wie Vorstand, Aufsichtsrat und Hauptversammlung. Die externe Sicht beschäftigt sich mit dem Verhältnis der Unternehmensleitung zu den wesentlichen Interessengruppen (Stakeholdern), wobei den Anteilseignern (Shareholder) oft eine stärkere Bedeutung zugemessen wird und der Eingliederung des Unternehmens in dessen Umfeld.[6]

Corporate Governance umfasst sowohl obligatorische Maßnahmen, wie die Einhaltung von Gesetzen, als auch freiwillige Maßnahmen, wie die Verwendung anerkannter Standards. Als wichtiger Bestandteil der Unternehmensführung liegt die Verantwortung für die Corporate Governance beim Vorstand und dem Management. Des Weiteren ist Corporate Governance als Prozess zu sehen, der an die sich ständig ändernden Anforderungen und Rahmenbedingungen angepasst werden muss.

D

Definition 2.1: Corporate Governance

Generell bezeichnet Corporate Governance den rechtlichen und faktischen Ordnungsrahmen für die Unternehmensleitung und -kontrolle.[7]. Corporate Governance besteht aus Organisationsstrukturen und Prozessen, die eine effiziente Führung und Überwachung zur Unterstützung der Unternehmensziele und -strategie gewährleisten sollen, und die Interessen aller am Unternehmen und damit an den Entscheidungsprozessen beteiligter bzw. von diesen betroffener Gruppen auszugleichen. Die Corporate Governance eines Unternehmens muss sowohl länderspezifische, als auch länderübergreifende Maßnahmen umfassen.

K

Kontrollaufgabe 2.1

Worin liegt der Unterschied zwischen Corporate Governance und Unternehmensführung?

[5] [vgl. Werder, 2008, S. 1]
[6] [vgl. Werder, 2008, S. 2]
[7] [vgl. Werder, 2008, S. 1f.]

Studienbrief 4 Compliance

4.1 Einführung

4.1.1 Lernergebnisse

- Sie haben die relevanten Grundlagen im Themenbereich der Compliance erfasst und können diese wiedergeben.
- Sie sind in der Lage, Compliance zu definieren und zu erläutern.
- Sie haben die Aufgaben, Anforderungen und Ziele eines unternehmensweiten Compliance-Managements erfasst und können diese beschreiben.
- Sie können die Notwendigkeit und Erfordernisse zur Verwirklichung eines effektiven Compliance-Managementsystems im Unternehmen erkennen und präzisieren.
- Sie sind imstande, die wichtigsten Elemente eines effektiven Compliance-Managementsystems wiederzugeben und zu erklären.
- Sie können ein Compliance-Managementsystem konzipieren.
- Sie sind in der Lage, ein Compliance-Managementsystem in die betriebliche Praxis einführen.
- Sie haben die Grundlagen der Prüfung des Compliance-Managements erfasst und sind in der Lage, eine Prüfung des Compliance-Managementsystems durchzuführen.

4.1.2 Advance Organizer

Vorkenntnisse

Für den Studienbrief „Compliance“ sind keine Vorkenntnisse erforderlich. Dieser Studienbrief bietet für Einsteiger und Neulinge in dieser Thematik genügend Materialien in Form von Hinweisen, Übungen und Grafiken um einen grundlegenden Wissensstand zu schaffen und soll alle Teilnehmer auf einen einheitlichen Wissensstand bringen.

Einordnung

Die behandelten Themen stellen die Bedeutung, Funktion und Funktionsweise eines effizienten Compliance-Managements im Unternehmen dar und sind für das Verständnis der Bedeutung der nachfolgenden Module wichtig.

4.1.3 Überblick

Motivation, Zielsetzung, Definition

Der erste Teil dieses Studienbriefs erläutert die Bedeutung, Funktion und Zielsetzung eines effektiven Compliance-Managements im Unternehmen. Es folgt eine ausführliche Definition des Begriffs „Compliance“.

Corporate Governance-System

Der zweite Teil setzt mit dem Compliance-Management in der betrieblichen Praxis auseinander. Die grundlegenden Elemente eines Compliance-Managementsystems sowie die Durchführung des Compliance-Managements werden erläutert.

Regelbetrieb

Der dritte Teil dieses Studienbriefs beschreibt die betriebliche Einführung eines Compliance-Managementsystems bis hin zum Regelbetrieb. Eine Erläuterung wichtiger Grundlagen für die Prüfung von Compliance-Managementsystemen rundet diesen Studienbrief ab.

Ausblick

Der nächste Studienbrief „IT-GRC“ erläutert den Zusammenhang der drei Themenbereiche und die Rolle der IT.

4.2 Einleitung

In der heutigen Zeit müssen sich Unternehmen mit einer Vielzahl an Vorgaben und Regelungen (insbesondere Gesetze) auseinandersetzen und stehen vielen rechtlichen Risiken gegenüber. Diese Risiken, die aus Rechtsverstößen oder sonstigen Missständen bei der Berücksichtigung von Vorgaben, Regelungen und Verhaltensstandards resultieren, können für ein Unternehmen gravierende Folgeschäden mit sich bringen. Rechtsverstöße, bspw. im Bereich der Wirtschaftskriminalität, des Datenschutzes und der Korruption finden eine immer größere Aufmerksamkeit.

B

Beispiel 4.1: Prozentuale Umsetzung des Compliance-Managements in Unternehmen

Laut einer Studie der PricewaterhouseCoopers AG berichteten im Jahr 2009 61 Prozent der befragten Unternehmen von mindestens einem Schadensfall durch Wirtschaftskriminalität. Bis 2013 lies sich diese Zahl auf 45 Prozent reduzieren, was auf die Anzahl der bis dahin eingeführten Compliance-Maßnahmen zurückzuführen ist. Demnach verfügten 2013 74 Prozent der befragten Unternehmen über ein Compliance-Management.[1]

Die Folgen von Rechtsverstößen oder Missständen, die auf mangelhafte oder fehlende Sicherstellung der Compliance zurückzuführen sind, können mittelbare als auch unmittelbare finanzielle Schäden verursachen. Sie reichen vom Reputationsverlust (wie bspw. dem öffentlichen Ansehen des Unternehmens oder die Akzeptanz der Produkte am Markt), Einbußen bei der Motivation der Mitarbeiter, dem Ausschluss von öffentlichen und privaten Auftragsvergaben über erhebliche finanzielle Geldstrafen bis hin zu straf- und zivilrechtlichen Maßnahmen gegen Management und Mitarbeiter und wirken sich letztendlich auf die wirtschaftliche Situation des Unternehmens sowie dessen Erfolg aus.

Unternehmensleitung und Vorstände tragen die Verantwortung für das Unternehmen und sind somit für die Gewährleistung der Gesetzeskonformität und eines

[1] [vgl. Bussmann et al., 2013, S. 3f.]

ordnungsgemäßen Verhaltens verantwortlich.[2] Dies bedeutet, jedes Mitglied der Unternehmensleitung bzw. des Vorstandes ist für Regelverstöße im Unternehmen haftbar und einem Schadenersatzanspruch der Gesellschaft oder dem Staat ausgesetzt, sollte keine angemessene Sicherstellung der Compliance veranlasst worden sein.

Daneben sind ebenfalls Aufsichtsräte gesetzlich (bspw. AktG § 91 (2), GmbHG § 43) für Verstöße persönlich haftbar, falls ihnen eine Vernachlässigung ihrer Pflichten nachgewiesen werden kann.[3] Um dieser Verantwortung nachzukommen, Compliance-Anforderungen zu erfüllen und Compliance-Risiken zu minimieren, muss das Management proaktiv tätig werden und präventive Mechanismen und Maßnahmen zur Sicherstellung der Compliance einführen.

B

Beispiel 4.2: Folgeschäden aus Compliance-Missständen

Beispielhaft lassen sich die folgenden Konsequenzen nennen:[4]

- Gefährdung des Unternehmens durch negative Berichte in den Medien über Missstände im Unternehmen
- Werteverfall für die Shareholder
- Beeinträchtigung der Beziehungen zu Aufsichtsbehörden
- Vergabesperre und Ausschluss („Blacklisting“) von künftigen Aufträgen
- Betriebsstilllegung
- Unternehmenskrise, Gefährdung der Arbeitsplätze
- Bußgelder und Geldstrafen für Management und Unternehmen
- Verfall des mit inkriminierten Geschäften erzielten Gewinns an die Staatskasse
- Untersuchungshaft und Freiheitsstrafe für Manager
- Einstweilige Verfügung gegen die Durchführung einzelner Geschäftsaktivitäten
- Pfändung von Bankkonten
- Schadensersatzforderungen durch Kunden, Wettbewerber und Verbraucher
- Aufwändige Beschäftigung des Managements mit Verteidigungsaktivitäten zu Lasten der Konzentration auf das Geschäft

[2] [vgl. Pütz, 2011, S. 11]
[3] [vgl. Meyer, 2010]

- Bedrohung der beruflichen Existenz der Organmitglieder

4.3 Motivation und Zielsetzung

Motivation

Compliance-Maßnahmen dienen der Prävention gegenüber Risiken aus Rechtsverstößen und schützen ein Unternehmen und dessen Stakeholder, wie Eigentümer, Manager, Mitarbeiter und Geschäftspartner, vor Folgeschäden und Strafverfolgung. Ein erfolgreiches Compliance-Management dient aber nicht nur der Vermeidung von Schäden und Haftungsrisiken, sondern stellt vielmehr auch einen strategischen Vorteil gegenüber dem Wettbewerb dar.

Die Zunahme der strategischen Bedeutung begründet sich auch durch den Bedeutungsgewinn einer erfolgreichen Corporate Governance. Vor allem bei der Auswahl eines Geschäftspartners werden Unternehmen zunehmend nach ihrer Corporate Governance (Verhaltensleitlinien und dem Umgang mit Risiken) bewertet. Geschäftsbeziehungen werden nur mit Unternehmen aufgenommen bei denen nicht befürchtet werden muss, dass negative Ereignisse (wie Rechtsverstöße) auftreten und sich möglicherweise auf das eigene Unternehmen durchschlagen können. Neben der Risikovorbeugung und Schadensabwehr ist ein effektives Compliance-Management sowohl ein wichtiger Bestandteil einer erfolgreichen Corporate Governance als auch ein Marketing-Faktor.[5]

Zielsetzung

Compliance-Management soll systematisch die Voraussetzungen schaffen,

- Verstöße gegen Compliance-Anforderungen zu verhindern sowie
- eingetretene Verstöße schnellstmöglich zu erkennen und behandeln zu können

mit dem Ziel,

- eine erfolgreiche Corporate Governance und ordnungsgemäße Unternehmensführung zu unterstützen,
- Risiken und mögliche Schäden, wie Negativschlagzeilen durch Rechtsverstöße, zu minimieren,
- Haftungsrisiken vorzubeugen sowie Schadensansprüche abzuwehren,
- präventiv gegen Wirtschaftskriminalität und Korruption zu wirken sowie
- die Integrität des Unternehmens zu stärken und sicherzustellen.

4.4 Begriffssystem

Compliance

Der Begriff Compliance stammt ursprünglich aus dem Gesundheitswesen und

[4] [vgl. Vetter, 2013, S. 9f.]
[5] [vgl. Vetter, 2013, S. 2]

4.10 Übungen

Übung 4.1

Ordnen Sie die Schritte zur Einführung eines Compliance-Managementsystems den Grundelementen des Compliance-Managementsystems zu.

Ü

Übung 4.2

Konzipieren Sie einen Compliance-Managementprozess (siehe Abbildung 4.2) inklusive der Elemente Berichtwesen, Dokumentationsmanagement, Änderungsmanagement und Überwachungsorgan.

Ü

Übung 4.3

Erläutern Sie die Bedeutung des Risk-Assessments für das Compliance-Management. Gehen Sie dabei sowohl auf die Identifikation, Analyse sowie Bewertung von Compliance-Risiken ein.

Welche Faktoren beeinflussen das Ausmaß der Identifikation?
Was wird bei der Analyse untersucht?
Welche Kriterien sind für die Bewertung ausschlaggebend?

Ü

Übung 4.4

Erläutern Sie den Begriff Whistleblower (Hinweisgeber) -Hotline im Kontext der Compliance-Organisation und des Compliance-Programms.

Ü