

Michael Beyer | Reinhard Heyd

Compliance für Aufsichtsräte

Rechtliche und fachliche Anforderungen
an die Finanzexpertise



SCHÄFFER
POESCHEL

Hinweis zum Urheberrecht:

Alle Inhalte dieses eBooks sind urheberrechtlich geschützt.

Bitte respektieren Sie die Rechte der Autorinnen und Autoren, indem sie keine ungenehmigten Kopien in Umlauf bringen.

Dafür vielen Dank!

Compliance für Aufsichtsräte

Michael Beyer/Reinhard Heyd

Compliance für Aufsichtsräte

Rechtliche und fachliche Anforderungen an die Finanzexpertise

1. Auflage

Schäffer-Poeschel Verlag Stuttgart

Bibliografische Information der Deutschen Nationalbibliothek

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

Print: ISBN 978-3-7910-4962-5 Bestell-Nr. 17208-0001

ePub: ISBN 978-3-7910-4963-2 Bestell-Nr. 17208-0100

ePDF: ISBN 978-3-7910-4964-9 Bestell-Nr. 17208-0150

Michael Beyer/Reinhard Heyd

Compliance für Aufsichtsräte

1. Auflage, Juni 2021

© 2021 Schäffer-Poeschel Verlag für Wirtschaft · Steuern · Recht GmbH

www.schaeffer-poeschel.de

service@schaeffer-poeschel.de

Bildnachweis (Cover): © EtiAmmos, AdobeStock

Produktmanagement: Kühn, Alexander

Lektorat: Susanne Mall | www.conscripto.de

Dieses Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Alle Rechte, insbesondere die der Vervielfältigung, des auszugsweisen Nachdrucks, der Übersetzung und der Einspeicherung und Verarbeitung in elektronischen Systemen, vorbehalten. Alle Angaben/Daten nach bestem Wissen, jedoch ohne Gewähr für Vollständigkeit und Richtigkeit.

Schäffer-Poeschel Verlag Stuttgart

Ein Unternehmen der Haufe Group

Vorwort

Sehr geehrte Leserinnen und Leser,

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

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

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

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

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

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

Inhaltsverzeichnis

Vorwort	5
Abbildungsverzeichnis	13
Tabellenverzeichnis	19
1 Grundlagen	21
1.1 Begriffsdefinitionen	21
1.2 Stellung in der Governance	23
1.3 Finanz-Compliance	27
1.4 Aktuelle rechtliche Entwicklungen (ARUG II, FISG, neuer DCGK etc.)	30
2 Stellung und Aufgaben des Aufsichtsrats	37
2.1 Überwachung und Beratung	37
2.2 Zusammenarbeit von Aufsichtsrat und Vorstand im Rahmen von Finanz-Compliance (Finanzberichterstattung und Finanzrevision)	39
2.3 Sonderstellung des Financial Experts und des Prüfungsausschusses	43
2.4 Zusammenarbeit von Prüfungsausschuss, Aufsichtsrat, Finanzvorstand und Abschlussprüfer	60
2.5 Aufsichtsratsreporting	64
2.5.1 Rechtliche Regelungen und Best-Practice-Normen (Bring- und Holschuld)	64
2.5.2 Regelkommunikation und Ad-hoc-Berichtspflichten	71
2.5.2.1 Sonderberichtspflichten auf Initiative des Vorstands gegenüber dem Aufsichtsrat(svorsitzenden)	71
2.5.2.2 Sonderberichtspflichten des Vorstands auf Initiative des Aufsichtsrats bzw. seiner Mitglieder	72
2.5.3 Bilaterale Kommunikationswege im Überblick	74
2.5.3.1 Kommunikation zwischen Prüfungsausschuss und Gesamtaufichtsrat	74
2.5.3.2 Kommunikation zwischen Aufsichtsrat/Prüfungsausschuss und Abschlussprüfer	74
2.5.3.3 Kommunikation zwischen Aufsichtsrat und Hauptversammlung	76
3 Zur Abgrenzung von Compliance und Compliance-Management	77
3.1 Notwendigkeit eines Compliance-Management-Systems	77
3.1.1 Rechtsgrundlagen von Compliance-Management-Systemen	77
3.1.1.1 Einführung	77
3.1.1.2 Informationsgegenstand für den Aufsichtsrat	78
3.1.1.3 Erfolgsfaktoren eines Compliance-Management-Systems	82
3.1.1.4 Compliance-Maßnahmen	83

3.1.1.5	Compliance-Regelungen	83
3.1.1.6	Compliance-Dokumentation	84
3.1.1.7	Elemente einer Compliance-Organisation	85
3.1.1.8	Compliance-Reporting	86
3.1.1.9	Meldestellen für Compliance-Verstöße	86
3.1.1.10	Geschäftspartner-Checks	87
3.1.1.11	Notfallpläne	88
3.1.2	Auswirkungen von Compliance-Verstößen	89
3.1.3	Zuständigkeiten	91
3.1.3.1	Einrichtung und Anwendung von Finanz-Compliance-Systemen durch den Vorstand, Überwachung durch den Aufsichtsrat	91
3.1.3.2	Haftung bei Compliance-Verstößen	94
3.1.3.3	Haftung bei Verletzung der Überwachungspflicht über das Compliance-Management-System	97
3.1.3.3.1	Haftung bei Compliance-Pflichtverletzungen des Vorstands	97
3.1.3.3.2	Haftung der Aufsichtsräte bei Verletzungen ihrer Überwachungspflicht	100
3.2	Elemente der Unternehmensüberwachung	103
3.2.1	Vorbemerkungen	103
3.2.2	Controlling	106
3.2.3	Risikomanagement	108
3.2.4	Compliance-Management	116
3.2.5	Innenrevision	123
3.2.6	Bestandteile des Finanz-Compliance-Management-Systems und seine Überwachung nach anerkannten Compliance-Standards	126
3.2.6.1	IDW PS 980	126
3.2.6.2	ISO 19600	130
3.2.6.3	Weitere Compliance-Standards im Überblick	132
3.3	Überwachung des Compliance-Management-Systems durch den Aufsichtsrat	133
3.3.1	Gegenstand der Überwachung des Compliance-Management-Systems durch den Aufsichtsrat	133
3.3.1.1	Einführung eines Compliance-Management-Systems	133
3.3.1.2	Laufende Überwachung eines Compliance-Management-Systems	135
3.3.1.2.1	Vom Vorstand veranlasste Überwachungsmaßnahmen	135
3.3.1.2.2	Vom Aufsichtsrat veranlasste Überwachungsmaßnahmen	136
3.3.2	Integration des Compliance-Management-Systems in das Überwachungsportfolio des Aufsichtsrats	140
3.3.2.1	Strategische Überwachung der Finanz-Compliance	140
3.3.2.2	Operative Überwachung der Finanz-Compliance	142

3.3.3	Organisation der Finanz-Compliance	144
3.3.3.1	Vorbemerkungen	144
3.3.3.2	Compliance Board, Compliance Committee	146
3.3.3.3	Chief Compliance Officer	148
3.3.3.4	Interne und externe Spezialisten für Finanz-Compliance	150
3.3.3.4.1	Organisatorische Eingliederung der Finanz-Compliance	150
3.3.3.4.2	Outsourcing der Finanzrevision	152
3.3.3.5	Schnittstellen von operativen Fachabteilungen, Management und Finanz-Compliance	153
3.3.3.6	Informations- und Kommunikationskanäle über Themen der Finanz-Compliance	154
3.3.3.6.1	Bringschuld- bzw. Bottom-up-Konzept	155
3.3.3.6.2	Holschuld- oder Top-down-Konzept	156
3.3.4	Maßnahmen des Aufsichtsrats zur Überwachung des Finanz-Compliance-Systems im Unternehmen	159
3.3.4.1	Sanktionsmöglichkeiten des Aufsichtsrats zur Einhaltung der Compliance-Normen im Unternehmen	159
3.3.4.1.1	Meinungsbeschlüsse	160
3.3.4.1.2	Änderung der Geschäftsordnung des Vorstands	161
3.3.4.1.3	Bestimmung zustimmungspflichtiger Geschäfte	162
3.3.4.1.4	Abberufung einzelner Vorstandsmitglieder wegen Compliance-Verstößen	163
3.3.4.1.5	Einberufung einer außerordentlichen Hauptversammlung	164
3.3.4.2	Sonderfragen der Überwachung des Finanz-Compliance- Management-Systems im Unternehmen	165
3.3.4.3	Beispiele zur Umsetzung der Finanz-Compliance-Maßnahmen	166
3.3.4.3.1	Finanz-Compliance-Maßnahmen bei der Erstellung eines Konzernabschlusses	166
3.3.4.3.2	Finanz-Compliance-Maßnahmen in Bezug auf die Abläufe bei der Planung und Durchführung eines Investitionsprojektes, z. B. dem Bau eines Zweigwerkes	169
3.3.5	Überwachung von Compliance-Management-Maßnahmen in der Unternehmenskrise	172
3.4	Aufgaben des Aufsichtsrats im Rahmen der Finanzberichterstattung	178
3.4.1	Grundverständnis des Aufsichtsrats vom Geschäftsmodell und den Finanzprozessen	178
3.4.2	Rechtsform, Unternehmensgröße und Geschäftsmodell als Risikofaktoren für die Finanzberichterstattung	186

3.4.3	Auswahl des Abschlussprüfers, Beauftragung und Honorarvereinbarung	188
3.4.3.1	Definition und Vorbemerkungen	188
3.4.3.2	Externe Pflichtrotation und interne Rotation innerhalb der Führungspersonen im Prüfungsteam	189
3.4.3.3	Auswahl des Abschlussprüfers: Auswahlverfahren bei Neuausschreibungen des Prüfungsauftrags	190
3.4.3.4	Überwachung des Abschlussprüfers und Funktion des Abschlussprüfers als Sparringspartner des Aufsichtsrats bzw. Prüfungsausschusses	191
3.4.3.5	Verlautbarungen des Abschlussprüfers	194
3.4.4	Prüfungsschwerpunkte, Erweiterung des Prüfungsauftrags, Sonderprüfungen	201
3.4.5	Prüfung und Billigung des Jahresabschlusses	207
3.4.6	Prüfungsausschuss als Sparringspartner des Abschlussprüfers während der Prüfung	209
3.5	Aufgaben des Aufsichtsrats im Rahmen der Finanzrevision	217
3.5.1	Sonderprüfungen	217
3.5.2	Verhalten bei aufgedeckten Compliance-Verstößen	219
3.5.3	Whistleblower-System	225
3.5.4	Kommunikation des Aufsichtsrats mit vorstandsnachgelagerten Abteilungen	232
3.6	Ausgewählte Risiken der Finanz-Compliance	234
3.6.1	Konzernabschlusserstellung	234
3.6.1.1	Vorbemerkung	234
3.6.1.2	Einzelverrichtungen bei der Konzernabschlusserstellung und mögliche Compliance-Risiken	235
3.6.1.2.1	Einzelverrichtungen bei der Konzernabschlusserstellung	235
3.6.1.2.2	Mögliche Compliance-Risiken bei der Konzernabschlusserstellung	239
3.6.1.3	Ziele und Maßnahmen im Rahmen eines Compliance-Management-Systems im Konzernrechnungswesen	242
3.6.1.3.1	Überblick	242
3.6.1.3.2	Identifikation von Compliance-Risiken	242
3.6.1.3.3	Reaktion auf eingetretene Compliance-Verstöße	244
3.6.1.3.4	Prävention für künftige Compliance-Verstöße	245
3.6.2	Shared-Service-Center	247
3.6.3	Verrechnungspreisgestaltung	252
3.6.3.1	Überblick	252
3.6.3.2	Gesetze, Vorschriften und Rechtsprechung	252

3.6.3.3	Vergleichbarkeitsanalyse als Ausgangspunkt jedes Fremdvergleichs	254
3.6.3.4	Methoden der Verrechnungspreisermittlung	255
3.6.3.4.1	Vorbemerkungen	255
3.6.3.4.2	Transaktionsbezogene Methoden der Verrechnungspreise	256
3.6.3.4.3	Gewinnorientierte Methoden der Verrechnungspreisermittlung	259
3.6.3.4.4	Steuerliche Sanktionen für unzureichende Verrechnungspreisdokumentationen	260
4	Sonderfragen der Überwachung des Finanz-Compliance-Systems durch den Aufsichtsrat	263
4.1	Konzernrelevante Überwachungskriterien des Finanz-Compliance-Systems	263
4.2	Internationalität des Geschäftsmodells und der Organisationsstruktur als Finanz-Compliance-Risiken	268
4.3	Tax Compliance	271
4.4	Finanz-Compliance im Mittelstand und in KMU	278
4.5	Finanz-Compliance entlang der Wertschöpfungskette	280
4.6	M&A-Compliance	281
4.7	IT-Compliance	287
4.8	Arbeitsrechtliche Fragen der Finanz-Compliance	289
5	Fazit: Compliance-Assessment	291
	Literaturverzeichnis	295
	Stichwortverzeichnis	297
	Zu den Autoren	305

Abbildungsverzeichnis

Abb. 1-1:	Begriffsklärung	21
Abb. 1-2:	Was meint Compliance?	23
Abb. 1-3:	Abgrenzung des Compliance-Managements gegenüber anderen Aufgaben in der Unternehmensüberwachung	25
Abb. 1-4:	Überblick zu einem vereinfachten Rechnungslegungsprozess	27
Abb. 1-5:	Zweck eines Tax-CMS	29
Abb. 1-6:	Wesentliche Änderungen durch das ARUG II	31
Abb. 1-7:	Wesentliche Änderungen des Deutschen Corporate Governance Kodex (DCGK) ...	32
Abb. 1-8:	Entwurf »Verbandssanktionengesetz« (VerSanG-E)	34
Abb. 2-1:	Wesentliche Pflichten des Aufsichtsrats	38
Abb. 2-2:	Wesentliche Abgrenzung der Organe Aufsichtsrat und Geschäftsleitung I/II	39
Abb. 2-3:	Wesentliche Abgrenzung der Organe Aufsichtsrat und Geschäftsleitung II/II	41
Abb. 2-4:	Möglichkeit der Bestellung eines Prüfungsausschusses sowie diesbezügliche Änderungen durch das FISG	43
Abb. 2-5:	Anforderungen an den Financial Expert nach § 100 Abs. 5 AktG und dessen Überarbeitung durch das FISG	45
Abb. 2-6:	Möglichkeiten der Delegation von Compliance-Aufgaben und -Verantwortlichkeiten	47
Abb. 2-7:	Arbeitsgebiete des Prüfungsausschusses und deren Ausweitung durch das FISG	49
Abb. 2-8:	Wesentliche Informationsflüsse in und um den Prüfungsausschuss	51
Abb. 2-9:	Prüfungsausschuss versus Aufsichtsrat	53
Abb. 2-10:	Pflichtverletzungen nach § 334 Abs. 2a HGB	55
Abb. 2-11:	Wahl der Mitglieder des Prüfungsausschusses	57
Abb. 2-12:	Erfolgsfaktoren für eine effiziente Unternehmensüberwachung durch den Finanzexperten	58
Abb. 2-13:	Zusammenarbeit von Aufsichtsrat/Prüfungsausschuss mit dem Abschlussprüfer	60
Abb. 2-14:	Festzulegende Themen der Zusammenarbeit von Prüfungsausschuss, Aufsichtsrat, Finanzvorstand und Abschlussprüfer	63
Abb. 2-15:	Zweck der Berichterstattung	64
Abb. 2-16:	Rechtliche Grundlagen des Aufsichtsratsreportings	66
Abb. 2-17:	Inhalte der Berichterstattung nach § 90 Abs. 1 AktG	67
Abb. 2-18:	Vorgaben des DCGK zum Aufsichtsratsreporting	70
Abb. 2-19:	Berichtsarten – Compliance-Berichterstattung	71
Abb. 2-20:	Compliance-Reporting als wichtiges (und oft unterschätztes) Instrument für das Überwachungsorgan	73
Abb. 2-21:	Berichtsinhalte der Kommunikation zwischen Aufsichtsrat/ Prüfungsausschuss und Abschlussprüfer	75

Abb. 3-1:	Gesetzliche Compliance-Vorgaben	77
Abb. 3-2:	Rechtliche Grundlagen für das Compliance-Management	79
Abb. 3-3:	Einfluss von Rechtsform, Größe und Risikoneigung des Unternehmens auf Compliance-Anforderungen	81
Abb. 3-4:	Compliance-Anforderungen der Rechtsprechung – LG München, Urteil vom 10.12.2013, 5 HK O 1387 / 10 – Siemens / Neubürger	83
Abb. 3-5:	Welche Ressourcen und Organisationsstrukturen/Berichtslinien sind erforderlich?	85
Abb. 3-6:	Organisationsformen	87
Abb. 3-7:	Beispiel einer Compliance-Landkarte	88
Abb. 3-8:	Erforderlichkeit von internen Ermittlungen	89
Abb. 3-9:	Interne Ermittlungen	91
Abb. 3-10:	Unterscheidung bei Einrichtung und laufender Anwendung eines CMS	94
Abb. 3-11:	Haftung der Geschäftsleitungsmitglieder (Überblick)	94
Abb. 3-12:	Business Judgement Rule	96
Abb. 3-13:	Zivilrechtliche Haftung von Aufsichtsratsmitgliedern I/II	98
Abb. 3-14:	Zivilrechtliche Haftung von Aufsichtsratsmitgliedern II/II	100
Abb. 3-15:	Strafrechtliche Haftung von Aufsichtsratsmitgliedern	102
Abb. 3-16:	»Three Lines of Defence«	103
Abb. 3-17:	Risikomanagement, Compliance-Management, Internes Kontrollsystem, Interne Revision	105
Abb. 3-18:	Controlling, Risikocontrolling	107
Abb. 3-19:	Risikomanagement und Risikomanagementsystem	109
Abb. 3-20:	Grundelemente eines internen Risikomanagementsystems	111
Abb. 3-21:	Gesetzliche Grundlagen des Risikomanagements sowie künftige Verpflichtung zum IKS und RMS nach dem FISG	113
Abb. 3-22:	Risikoberichterstattung des Vorstandes	115
Abb. 3-23:	Vergleich Risikomanagement und Compliance-Management	117
Abb. 3-24:	Folgen von Compliance-Verstößen für das Unternehmen	118
Abb. 3-25:	Elemente einer Compliance-Organisation	120
Abb. 3-26:	Compliance-Reporting	121
Abb. 3-27:	Funktionen des Vorstands im Zusammenhang mit der Einrichtung und Funktionsfähigkeit der Internen Revision	123
Abb. 3-28:	Verantwortung des Vorstandes im Rahmen der Einbeziehung von Mitarbeitern in die Wahrnehmung der Internen Kontrolle	125
Abb. 3-29:	Implementierungsmöglichkeiten eines Compliance-Management-Systems	126
Abb. 3-30:	Bestandteile eines Compliance-Management-Systems I/II	128
Abb. 3-31:	Bestandteile eines Compliance-Management-Systems II/II	129
Abb. 3-32:	ISO 19600 – Das Fünf-Säulen-Modell	131
Abb. 3-33:	Überwachung des Compliance-Management-Systems durch den Aufsichtsrat I/IV	133

Abb. 3-34:	Überwachung des Compliance-Management-Systems durch den Aufsichtsrat II/IV	135
Abb. 3-35:	Überwachung des Compliance-Management-Systems durch den Aufsichtsrat III/IV	136
Abb. 3-36:	Überwachung des Compliance-Management-Systems durch den Aufsichtsrat IV/IV	138
Abb. 3-37:	Beispiele für Projekte, bei denen die Normkonformität durch den Vorstand bestätigt und vom Aufsichtsrat geprüft werden sollte	140
Abb. 3-38:	Punkte im Rahmen der operativen Überwachung, auf die besonderes Augenmerk zu legen ist	142
Abb. 3-39:	Delegation der Compliance-Verantwortung	144
Abb. 3-40:	Mitglieder des Compliance Committee	146
Abb. 3-41:	Chief Compliance Officer (CCO)	148
Abb. 3-42:	Zu beachtende Besonderheiten der Finanz-Compliance	150
Abb. 3-43:	Organisationsformen der Finanz-Compliance	154
Abb. 3-44:	Compliance-Reporting	156
Abb. 3-45:	Möglichkeiten der Bildung eines Compliance-Ausschusses	157
Abb. 3-46:	Beispielhafte Aufgaben, die dem Compliance-Ausschuss übertragen werden können	159
Abb. 3-47:	Sanktionsmöglichkeiten des Aufsichtsrats I/III	160
Abb. 3-48:	Sanktionsmöglichkeiten des Aufsichtsrats II/III	163
Abb. 3-49:	Sanktionsmöglichkeiten des Aufsichtsrats III/III	164
Abb. 3-50:	Finanz-Compliance-Maßnahmen bei der Planung und Durchführung eines Investitionsprojektes, z. B. dem Bau eines Zweigwerkes I/II	166
Abb. 3-51:	Finanz-Compliance-Maßnahmen bei der Planung und Durchführung eines Investitionsprojektes, z. B. dem Bau eines Zweigwerkes II/II	169
Abb. 3-52:	Phasen der Unternehmenskrise	172
Abb. 3-53:	Besondere Aufgaben des Aufsichtsrats/Sanierungsausschusses in der Krise im Zusammenhang mit der Überwachung der Finanzberichterstattung I/II	174
Abb. 3-54:	Besondere Aufgaben des Aufsichtsrats/Sanierungsausschusses in der Krise im Zusammenhang mit der Überwachung der Finanzberichterstattung II/II	176
Abb. 3-55:	Grundverständnis des Aufsichtsrats vom Geschäftsmodell und den Finanzprozessen I/II	178
Abb. 3-56:	Grundverständnis des Aufsichtsrats vom Geschäftsmodell und den Finanzprozessen II/II	180
Abb. 3-57:	Erstellung eines Konzernabschlusses	182
Abb. 3-58:	Konsolidierung	184
Abb. 3-59:	Risikofaktoren für die Finanzberichterstattung	186
Abb. 3-60:	Aufgaben des Aufsichtsrats bzw. des Prüfungsausschusses im Rahmen der Prüfung des Unternehmens	188

Abb. 3-61:	Arten der Rotation	190
Abb. 3-62:	Externe Rotation	191
Abb. 3-63:	Interne Rotation	193
Abb. 3-64:	Nichtprüfungsleistungen	195
Abb. 3-65:	Inhalt des Prüfungsberichts	196
Abb. 3-66:	Bestätigungsvermerk	198
Abb. 3-67:	Erteilung des Prüfungsauftrags	200
Abb. 3-68:	Honorarvereinbarung	201
Abb. 3-69:	Inhalte der Prüfung	203
Abb. 3-70:	Prüfungsschwerpunkte	205
Abb. 3-71:	Erweiterungen und Ergänzungen des Prüfungsauftrags	207
Abb. 3-72:	Feststellung des Jahresabschlusses in einer AG	208
Abb. 3-73:	Ebenen der Zusammenarbeit mit dem Abschlussprüfer	209
Abb. 3-74:	Prüfungsplanung	211
Abb. 3-75:	Prüfungsgegenstände/-maßstäbe des Aufsichtsrats und des Abschlussprüfers	213
Abb. 3-76:	Beispiel zu den Prüfungsmaßstäben von Aufsichtsrat und Abschlussprüfer	215
Abb. 3-77:	Unterscheidung von Sonderprüfungen	217
Abb. 3-78:	Umgang des Vorstandes mit Compliance-Verstößen sowie interne Untersuchungen und Krisenmanagement (Aufgaben des Aufsichtsrats)	219
Abb. 3-79:	Wann und wie muss der Aufsichtsrat initiativ tätig werden?	221
Abb. 3-80:	Compliance-Pflichten des Aufsichtsrats bei mutmaßlichen Compliance-Verstößen von Vorstandsmitgliedern I/II	223
Abb. 3-81:	Compliance-Pflichten des Aufsichtsrats bei mutmaßlichen Compliance-Verstößen von Vorstandsmitgliedern II/II	225
Abb. 3-82:	EU-Hinweisgeberrichtlinie (EU) 2019/1937 I/III	226
Abb. 3-83:	EU-Hinweisgeberrichtlinie (EU) 2019/1937 II/III	228
Abb. 3-84:	EU-Hinweisgeberrichtlinie (EU) 2019/1937 III/III	230
Abb. 3-85:	Befugnisse des Aufsichtsrats beim Zugriff auf unternehmensinterne Personen und anstehende Änderungen durch das FISG	232
Abb. 3-86:	Konzernabschluss	234
Abb. 3-87:	Einzelverrichtungen bei der Konzernabschlusserstellung	236
Abb. 3-88:	Qualitätssicherungsmaßnahmen des Vorstandes für die Bewältigung des Gesamtprojekts »Konzernabschlusserstellung«	238
Abb. 3-89:	Mögliche Compliance-Risiken bei der Konzernabschlusserstellung I/II	239
Abb. 3-90:	Mögliche Compliance-Risiken bei der Konzernabschlusserstellung II/II	241
Abb. 3-91:	Ziele und Maßnahmen im Rahmen eines Compliance-Management-Systems im Konzernrechnungswesen I/II	244
Abb. 3-92:	Ziele und Maßnahmen im Rahmen eines Compliance-Management-Systems im Konzernrechnungswesen II/II	246
Abb. 3-93:	Gründe für und Vorteile von Shared-Service-Centern	247
Abb. 3-94:	Zu beachtende Aspekte bei der erfolgreichen Einführung und dem Betrieb von Shared-Service-Centern	249

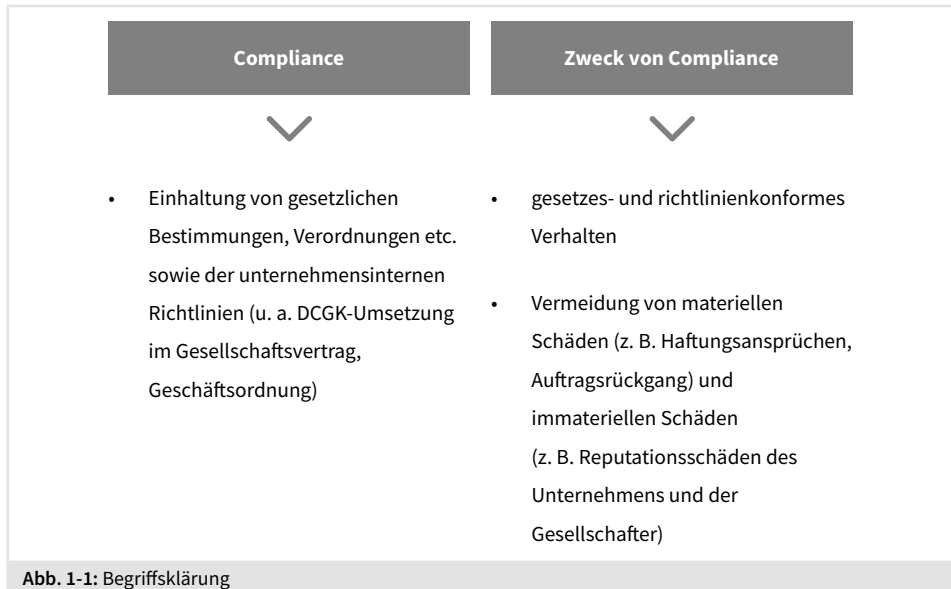
Abb. 3-95:	Herausforderungen an die Finanz-Compliance-Überwachung durch den Aufsichtsrat/Prüfungsausschuss im Zusammenhang mit Shared-Service-Centern	251
Abb. 3-96:	Gründe, warum die Gewinnverlagerung mittels Verrechnungspreisen in der Praxis nur eingeschränkt möglich ist	253
Abb. 3-97:	Methoden, die für die Fremdvergleichsermittlung grundsätzlich zur Verfügung stehen	255
Abb. 3-98:	Einteilung der Dokumentationspflichten für Verrechnungspreise	257
Abb. 3-99:	Grundsätze für die Dokumentationspflichten für Verrechnungspreise sowie der Funktions- und Risikoanalyse	259
Abb. 3-100:	Compliance-relevante Überwachung der Verrechnungspreisgestaltung durch den Aufsichtsrat bzw. Prüfungsausschuss	261
Abb. 4-1:	Beispiel zur Delegation von Aufgaben und Kompetenzen an die dezentralen Konzerneinheiten	264
Abb. 4-2:	Beispiele für compliance-relevante konzernumfassende Berichtsinhalte bezüglich rechtlicher Besonderheiten	266
Abb. 4-3:	Beispielhafte Gründe für verstärkte Compliance-Risiken in international tätigen Unternehmen und Konzernen I/II	268
Abb. 4-4:	Beispielhafte Gründe für verstärkte Compliance-Risiken in international tätigen Unternehmen und Konzernen II/II	270
Abb. 4-5:	Meist vorliegende Problemfelder für das Unternehmen und die Unternehmensorganisation im Rahmen der Tax Compliance	272
Abb. 4-6:	Maßnahmen zur Risikominimierung	274
Abb. 4-7:	Überwachungsaufgaben des Prüfungsausschusses im Zusammenhang mit dem Tax-CMS	276
Abb. 4-8:	Aufgaben des Aufsichtsrats in Bezug auf die Finanz-Compliance bei KMU	278
Abb. 4-9:	Einzelschritte bezüglich der Finanz-Compliance entlang der Wertschöpfungskette	280
Abb. 4-10:	Definition von Mergers and Acquisitions	281
Abb. 4-11:	Gliederung des typischen Ablaufs einer M&A-Transaktion	283
Abb. 4-12:	Typische Fehler einer M&A-Transaktion	285
Abb. 4-13:	Funktion des Prüfungsausschusses bei M&A-Transaktionen	286
Abb. 4-14:	Verpflichtung zur Einrichtung eines Datenschutzmanagementsystems	288
Abb. 4-15:	Themen der arbeitsrechtlichen Finanz-Compliance	290
Abb. 5-1:	Inhalte des Finanz-Compliance-Assessments	291
Abb. 5-2:	Anhaltspunkt für ein Compliance-Assessment	293

Tabellenverzeichnis

Tab. 2-1: Kompetenzen im Prüfungsausschuss nach Rechtsquellen	54
Tab. 3-1: Three Lines of Defence	104
Tab. 3-2: Anforderungen an die Ausgestaltung eines CMS nach dem IDW PS 980	127
Tab. 3-3: Abweichungen in Bilanzposten	243
Tab. 3-4: Zu analysierende komparative Kompetenzen, bevor das Shared-Service-Center ausgelagert wird	249
Tab. 4-1: Übliche Inhalte eines Verkaufsmemorandums	284
Tab. 4-2: Risiken und Erfolgsfaktoren einer M&A-Transaktion	287

1 Grundlagen

1.1 Begriffsdefinitionen



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

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

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

Zu den externen Bestimmungen zählen gesetzliche Regelungen. Hierbei können beispielsweise folgende angeführt werden:

- Gesetze,
- Verordnungen,
- etc.

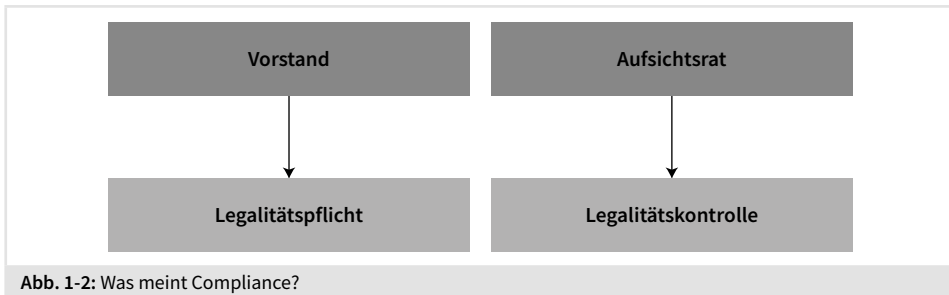
Demgegenüber können sich bei Gesellschaften unternehmensinterne Richtlinien u. a. aus der Umsetzung des Deutschen Corporate Governance Kodex (DCGK) im Gesellschaftsvertrag, der Geschäftsordnung, dem Organisationshandbuch oder aus sonstigen unternehmensinternen Richtlinien sowohl für den Aufsichtsrat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

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

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

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

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



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

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

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

1.2 Stellung in der Governance

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

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

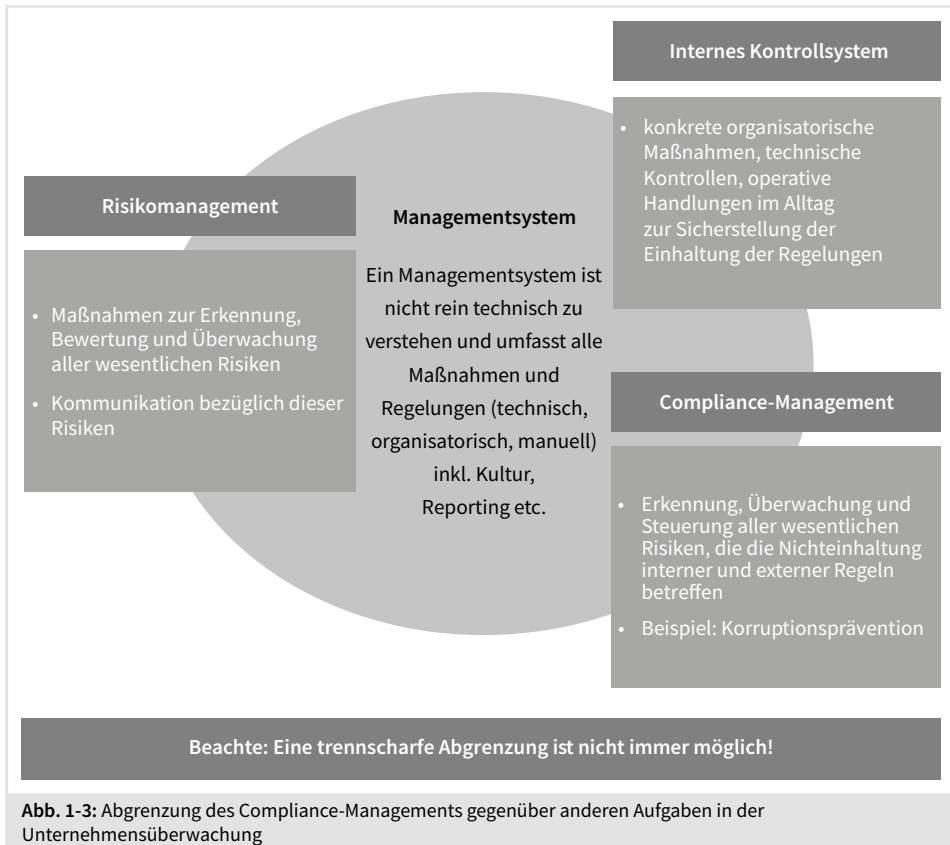
Unterschieden werden sollen im Folgenden:

- das Compliance-Management,
- das Risikomanagement und
- das Interne Kontrollsystem.

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

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

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



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

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

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

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

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

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

- etwaige Haftungsansprüche,
- Bußgelder,
- Strafverfahren.

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

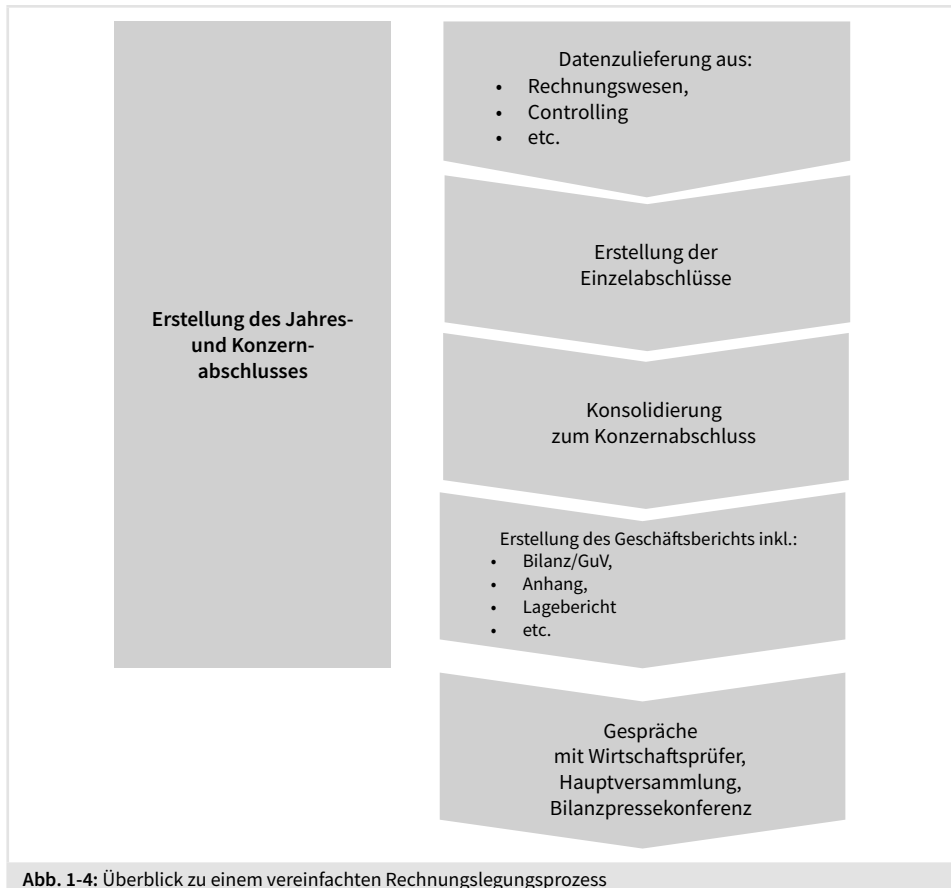
Bezogen auf die Zielsetzung des Compliance-Managements und des Risikomanagements haben beide zunächst die gemeinsame Intention, etwaige Schäden der Gesellschaft abzuwenden. Das Compliance-Management geht jedoch über das Risikomanagement dahingehend hinaus, dass es nicht bei der Erkennung, Bewertung,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

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

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

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

1.3 Finanz-Compliance



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

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

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

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

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

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

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

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

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

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