

Michael Beyer | Reinhard Heyd

Compliance für Aufsichtsräte

Rechtliche und fachliche Anforderungen
an die Finanzexpertise



SCHÄFFER
POESCHEL

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