Interne Revision und Compliance

Jörg Berwanger • Ulrich Hahn

Interne Revision und Compliance

Operative Grundlagen und Recht

Springer Gabler

Jörg Berwanger
Neunkirchen, Deutschland

Ulrich Hahn
Frankfurt am Main, Deutschland

ISBN 978-3-658-31806-2 ISBN 978-3-658-31807-9 (eBook)
https://doi.org/10.1007/978-3-658-31807-9

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

Springer Gabler

Springer Gabler ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Geleitwort Prof. Gerrit Horstmeier

Dieses Werk beschäftigt sich mit den Risiken der eigenen (Unternehmens-) Organisation, insbesondere im privatwirtschaftlichen Kontext. Diese Risiken zu kennen und zu steuern ist eine Grundvoraussetzung für das Fortbestehen des Unternehmens – ein „Muss" für jede Führungskraft, ohne die eine funktionierende Unternehmensleitung nicht denkbar ist. Dieses Buch beschreibt praxisnah die Grundlagen und Instrumentarien des komplexen internen Risikomanagements, die sich daraus ergebenden Haftungsrisiken sowie die erforderlichen Umsetzungsschritte. Es zeigt die Wege auf, wie ein effizientes und dauerhaftes Frühwarnsystem im Unternehmen etabliert wird und funktioniert. Dabei wird nicht nur die unternehmerische Sicht, sondern auch der entsprechende juristische Hintergrund in für Nicht-Juristen verständlicher, auch unterhaltender Form ausgeleuchtet, denn juristische Aspekte werden durch gesetzgeberische Impulse national wie international immer wichtiger. Darüber hinaus zeigt das Buch Wege auf, wie Prüfungs- und Beratungsleistungen der Internen Revision und wie ein zeitgemäßes Compliance-Management-System Unternehmensprozesse optimieren können.

Schwerpunkte des Buches sind:

- Corporate Governance
- Rechtsgrundlagen für die Interne Revision und für die Compliance
- Revisionsmanagement
- Grundlagen zu einem Compliance-Management-System
- Durchführung von internen Prüfungs- und Beratungsaufträgen
- Spezielle Prüffelder der Internen Revision

Ein Glossar mit den wesentlichen Fachbegriffen zu Interner Revision und zu Compliance rundet das Werk ab. Es erleichtert auch Nicht-Fachleuten den Überblick über und den Einstieg in die Materie ganz wesentlich. Zahlreiche Beispiele helfen bei der praktischen Anwendung und Umsetzung. Mit diesem Buch sollte Ihnen die Beherrschung dieses komplexen Themas gut gelingen!

Vorwort

„Change“ ist heutzutage ein in der Managementsprache beinahe schon inflationär gebrauchter Begriff. Beschwörend soll er die Mitarbeiter dazu motivieren, Veränderungsprozesse im Unternehmen aktiv und konstruktiv mit zu gestalten.

Change sollte nie einem reinen Selbstzweck dienen – ein Irrtum, dem manches auf Trial and Error angelegte Management unterliegen kann. Die beiden Autoren wollen jedenfalls diesen Fehler vermeiden. Dies gilt vor allem für den juristischen Ko-Autor, der mit einschlägiger literarischer Vergangenheit ausgestattet ist. Dieses Buch soll seine geschätzten Leserinnen und Leser in komprimierter Form zu den wesentlichen Themen der Internen Revision und der Compliance, als Teile im Wimmelbild eines Unternehmens, hinführen. Über den soziologisch-rechtlichen Tellerrand hinaus wird das soziale Biotop „Unternehmen“ und seine Rolle im Globalisierungswettbewerb betrachtet. Auch wenn in den vergangenen Jahren, nicht zuletzt wegen des verstärkten Aufkommens der Compliance, einige einschlägige Werke auf dem Fachbuchmarkt erschienen sind, der hier präsentierte Mix aus Operativem und Recht – „Recht“ seinerseits auch operativ angelegt – bietet ein Alleinstellungsmerkmal der gewählten Konzeption.

Die letzten Arbeiten an diesem Buch wurden unter dem Eindruck der weltweiten Corona-Krise, ja auch eine globale Wirtschafts- und Unternehmenskrise, erledigt. Mit Bezug auf die Rollen von Interner Revision und Compliance: Gerade in Krisenzeiten sind Unternehmensleitungen auf die Funktions- und Leistungsfähigkeit von Interner Revision und Compliance angewiesen. Interne Revision hat schon in den vergangenen Jahrzehnten eine deutliche Aufwertung erlebt – trotz der Konkurrenz durch Risikomanagement- und Compliance-Funktionen. Wiederholte Aussetzer von Leitungsmechanismen (neudeutsch „Governance-Strukturen“) im privatwirtschaftlichen, aber auch im öffentlichen Bereich fordern immer neue gesetzgeberisch-regulatorische Initiativen heraus. Interne Kontroll-, Risiko- und auch Compliance-Managementsysteme sind zu implementieren. Diese stellen immer wieder die hergebrachte Revisionsrolle in Frage, schlussendlich geht aber die Interne Revision daraus gestärkt hervor, nämlich indem ihre Rolle klarer bestimmt und der Berufsstand im Wettbewerb mit der ebenfalls gut aufgestellten „Konkurrenz“ weiter professionalisiert wird.

Der rechtliche Teil des Buches behandelt wesentliche und grundlegende Rechtsfragen rund um die Interne Revision und die Compliance. So viel wie notwendig, so wenig wie möglich, Leserinnen und Leser sollen nicht mit allzu vielen rechtlichen Abstraktheiten und Dogmatiken befrachtet werden. Immerhin war es an der einen oder anderen Stelle schon notwendig, rechtliche Wegmarken etwas vertieft zu platzieren – auch als Versuch der Belebung der Diskussion innerhalb der rechtlichen Community. Wie auch andere Passagen des Buches sind die rechtlichen Ausführungen im Übrigen deduktiv angelegt. Die geschätzte Leserschaft wird, ausgehend von allgemeinen Grundlagen, systematisch aufbauend peu à peu an spezielle Materien herangeführt.

Die Themen betreffen rechtliche Statusfragen der beiden Funktionen im Unternehmen und befassen sich mit dessen Stellung im Rechtsverkehr. Auch werden wesentliche praktische Rechtsfragen (etwa zur Haftung), denen sich die beiden Funktionen und ihre Berufsträger stellen müssen, beleuchtet und anhand der aktuellen Rechtsprechung und anderer Meinungen in der juristischen Literatur gespiegelt. Fast durchgängig wurde im Rechtsteil auch die „Geschichte hinter der Geschichte" erzählt, um rechtliche Themen nicht nur anhand von Rechtsvorschriften und derer Vorgaben zu deklinieren. Das gilt z. B. für die soziologischen Zusammenhänge zur Wirtschaftskriminalität. Eine strenge nüchtern-technokratische Sprachwahl, die sich für ein wissenschaftliches Fachbuch grundsätzlich geziemt, wurde, wenn es um Kernthemen des Buches kritisch bestellt ist, auch einmal abgelegt. Die Autoren konnten sich einige deutliche Worte zum Verhalten mancher Unternehmen und von Führungskräften im Zusammenhang mit den jüngsten Skandalen nicht ersparen. Geradezu wie eine Bombe eingeschlagen ist (nicht nur) in der deutschen Öffentlichkeit der Fall Wirecard. Unmittelbar vor Redaktionsschluss konnte er von den Autoren nicht mehr verarbeitet werden – er bietet aber sicherlich reichlich „Futter" für die folgende Auflage!

Der operative Teil des Buches zur Internen Revision orientiert sich an den typischen Revisionsaufgaben und Revisionsprozessen, sowohl im privatwirtschaftlichen als auch im öffentlichen Kontext. Dabei wird besonders Wert auf die pragmatisch-praxistaugliche Umsetzung der Berufsgrundlagen der Internen Revision gelegt, abgestimmt mit aktuellen Entwicklungen und Erkenntnissen. Dieser Teil des Werks ist als Basis für die Grundausbildung in der Internen Revision, den schnellen Zugriff auf die grundlegenden Instrumente des Revisionsmanagements sowie die Vorbereitung der Zertifizierungen Qualification in Internal Audit Leadership (QIAL), Certified Internal Auditor (CIA), Interner Revisor (DIIR) und anderer IIA-Zertifizierungen (CRMA, CIAP etc.) geeignet. Analog dazu werden die Anbindung an die Compliance und ihre Strukturen skizziert.

Zusätzlich bietet das Werk Risikomanagern, Compliance-Beauftragten, Aufsichtsräten, Externen Revisoren und anderen Governance-Funktionen einen verständlichen Zugang zu den praktischen und konstitutiv-juristischen Aspekten der Internen Revision und der Compliance. Ein Glossar mit wesentlichen Fachbegriffen führt rasch auf den Punkt.

Dem vorstehend skizzierten Programm folgen auch die konkrete Sachbearbeitung und die Arbeitsteilung hinsichtlich der einzelnen Kapitel dieses Buches. Gemeinsam bearbeitet wurden Kap. 7 (Glossar) und Kap. 8 (Zusammenfassung). Von Berwanger allein stam-

men die Unterkapitel 1.1-1.4 und 2.1 sowie das gesamte rechtlich orientierte Kapitel 3. Von Hahn allein erstellt wurden die revisionsbezogenen Unterkapitel 1.5 und 2.2-2.5 sowie die Kapitel 4-6 und das Kapitel 9.

Die Autoren haben sich um eine leicht verständliche Darstellungsweise bemüht. Ein zuweilen bewusst gewählter locker-lässiger Schreibstil, der selbstverständlich nicht in die Nachlässigkeit abdriften darf, wurde gewählt. Er will auch mal zum Nachdenken und Schmunzeln anregen und soll dazu führen, die zum Teil schwierigen Sachthemen möglichst leicht bekömmlich zu servieren, um so ihre gedankliche Aufnahme und Verarbeitung zu erleichtern.

Konstruktive Kritik ist den Autoren stets willkommen.

Neunkirchen (Saar), Deutschland — Jörg Berwanger
Frankfurt am Main, Deutschland — Ulrich Hahn
Dezember 2020

Inhaltsverzeichnis

1 Corporate Governance 1
1.1 Einleitung: Ankerplätze 1
1.2 Determinanten der Corporate Governance 4
1.2.1 Bestandsaufnahme: Globalisierung 4
1.2.2 Kleines soziologisches Einmaleins – Soziologische Systemtheorie 7
1.2.3 „Governance-Ethik“ und eine Entgegnung 11
1.2.4 Wertedilemmata in Unternehmen 14
1.3 Prinzipien für die Corporate Governance 18
1.3.1 Supranationale Prinzipien – G20/OECD 18
1.3.2 Regionale Regelungen – EU 19
1.3.3 Deutscher Corporate Governance Kodex 20
1.4 Managementmodelle und -theorien 22
1.4.1 Grundlagen 22
1.4.2 Principal-Agent-Theorie (Agenturtheorie) 23
1.4.3 Stewardship-Theorie 25
1.4.4 Sicht der Verfasser 26
1.5 Interne Revision und Compliance 28
Literatur 30

2 Die Revisionsfunktion 33
2.1 Historische Entwicklung von Interner Revision und Compliance 33
2.1.1 Interne Revision 33
2.1.2 Compliance 35
2.2 Kontext der Revisionsfunktion 36
2.2.1 Interne Revision und Compliance im GRC-System 37
2.2.2 Die Rollenverteilung in der Unternehmenswirklichkeit 39
2.3 Institutionen der Internen Revision 41
2.3.1 Deutsches Institut für Interne Revision e.V. 41
2.3.2 IIA Switzerland und IIA Austria 43
2.3.3 Institute of Internal Auditors 45

2.3.4 European Confederation of Institutes of Internal Auditing 46
2.3.5 Weitere Institutionen mit Bezug zur Internen Revision 46
2.4 Berufsgrundlagen 47
2.4.1 Komponenten der Berufsgrundlagen des IIA (IPPF) 47
2.4.2 Ziel und Zweck der Revisionsfunktion 52
2.4.3 Nutzenbeitrag der Internen Revision 55
2.4.4 Abgrenzung zu anderen Funktionen 56
2.5 Revisionsorganisation und Standards 56
2.5.1 Positionierung und Ressourcen – Attribut-Standards 56
2.5.2 Revisionsmanagement und Auftragsdurchführung – Performance-Standards 57
2.5.3 Auftragsabwicklung – Prüfungsprozess und Standards 58
Literatur 59

3 Rechtsgrundlagen für die Interne Revision und für die Compliance 63
3.1 Allgemein: Rechtsquellen/Differenzierungen 63
3.1.1 Recht 63
3.1.2 „Außenrecht“ und „Innenrecht“ 64
3.1.3 Statusrecht 66
3.1.4 Operatives Recht 66
3.2 Erste statusrechtliche Befundungen – Juristisches Arbeitsprogramm dieses Buches 67
3.2.1 Keine wirtschaftsrechtliche Einrichtungspflicht – Überblick 67
3.2.2 Juristisches Sachthementableau 71
3.3 Staatliche Statusregeln für die Interne Revision und ein CMS 72
3.3.1 Vorstellung einschlägiger aktienrechtlicher Vorschriften 72
3.3.2 Begründungen der Verfasser: Keine allgemeine Rechtspflicht zur Schaffung einer Internen Revision und eines CMS 77
3.4 Deutscher Corporate Governance Kodex als Statusnorm? 88
3.5 Recht: International/Supranational 91
3.5.1 SOX 91
3.5.2 EU 92
3.5.3 UK Bribery Act 93
3.6 Innenrecht als Statusgrundlage für die Interne Revision und für ein CMS 94
3.6.1 Interne Revision 94
3.6.2 CMS 95
3.7 Interne Revision und CMS in besonderen Branchen – Kurzüberblick 97
3.8 Abweichendes Verhalten – Wirtschaftskriminalität im Unternehmen 98
3.8.1 Kriminalsoziologischer Rahmen 98
3.8.2 Wirtschaftskriminalität allgemein, insbesondere Korruption 108

3.8.3 Korruptionsursachen – Mitarbeiter und (Top-) Management 110
3.8.4 Staatliche Antworten gegen Wirtschaftskriminalität in Form von Korruption u. a. Missständen 113
3.8.5 Bekämpfung von Korruption durch die Unternehmen. 120
3.9 Haftungsrecht 125
3.9.1 Haftung allgemein 125
3.9.2 Öffentliches Recht 127
3.9.3 Zivilrecht 139
Literatur. 146

4 Revisionsmanagement 149
4.1 Organisationsmodelle der Internen Revision 149
4.1.1 Vierstufige Managementpyramide der Internen Revision 150
4.1.2 Siebenteiliges Komponenten-Modell der Revisionsorganisation 151
4.1.3 Umsetzung in den Berufsgrundlagen. 152
4.2 Aufgaben und Positionierung 153
4.2.1 Ausrichtung: Art der Arbeiten 153
4.2.2 Strategie 157
4.2.3 Geschäftsordnung 158
4.2.4 Rechte und Pflichten 159
4.3 Aufbauorganisation 160
4.3.1 Strukturmodelle 160
4.3.2 Unabhängigkeit und Objektivität 163
4.3.3 Sachkunde und Sorgfaltspflicht 167
4.4 Ressourcenausstattung 170
4.4.1 Finanzmittel 170
4.4.2 Sourcing-Strategien 171
4.4.3 Personal 173
4.4.4 IT-Infrastruktur. 175
4.5 Planung 177
4.5.1 Audit Universe 178
4.5.2 Risikobeurteilung. 179
4.5.3 Periodenplanung 182
4.5.4 Abstimmung mit anderen Assurance-Funktionen 185
4.6 Qualitätsmanagement der Internen Revision 187
4.6.1 Programm zur Qualitätssicherung und -verbesserung 187
4.6.2 Interne und externe Beurteilungen. 190
4.6.3 Laufende Überwachung und regelmäßige interne Beurteilungen . . . 191
4.6.4 Unabhängige, externe Beurteilungen – Quality Assessments 192
4.6.5 Beurteilungsverfahren und -instrumente 193
4.6.6 Revisions-Kennzahlen und Benchmarks 195

4.7 Revisionsorganisation 197
4.7.1 Richtlinien und Verfahren 198
4.7.2 Die Bedeutung des Formalisierungsgrads – Revision 9.0 200
4.7.3 Überwachen der Auftragsdurchführung 201
4.8 Funktionsbezogene Berichterstattung, Tätigkeitsbericht 201
Literatur 203

5 Durchführung von Prüfungs- und Beratungsaufträgen 207
5.1 Der Revisionsprozess 207
5.1.1 Der Revisionsprozess in den Berufsgrundlagen 208
5.1.2 Good Practices und Varianten 210
5.2 Prüfungsvorbereitung 210
5.2.1 Disposition der (Prüfungs-) Aufträge 211
5.2.2 Prüfungsauftrag und Prüfungsankündigung 211
5.2.3 Voruntersuchung 212
5.2.4 Aktivitäten – Prüfungsvorbereitung und Vorerhebung 213
5.2.5 Werkzeuge für die Vorbereitungsphase 227
5.2.6 Prüfungsvorbereitung – Good Practices und Varianten 227
5.3 Auftragsdurchführung 228
5.3.1 Prüfungsdurchführung – Informationssammlung 231
5.3.2 Informationssammlung – Good Practices und Varianten 234
5.3.3 Prüfungsdurchführung – Analyse und Beurteilung 235
5.3.4 Analyse und Beurteilung – Good Practices und Varianten 240
5.3.5 Prüfungsdurchführung – Dokumentation 242
5.3.6 Dokumentation – Good Practices und Varianten 249
5.3.7 Überwachen der Auftragsdurchführung 250
5.3.8 Überwachen der Auftragsdurchführung – Good Practices und Varianten 251
5.4 Auftragsberichterstattung und Auftragsabschluss 252
5.4.1 Auftragsberichterstattung 253
5.4.2 Auftragsberichterstattung – Good Practices und Varianten 268
5.4.3 Auftragsabschluss 269
5.4.4 Auftragsabschluss – Good Practices und Varianten 273
5.5 Follow-up und Übernahme der Verantwortung 274
5.5.1 Aktivitäten 275
5.5.2 Administrativer Follow-up 276
5.5.3 Follow-up im Rahmen von Folgeprüfungen 277
5.5.4 Gezielte Follow-up-Prüfungen 278
5.5.5 Risikoübernahme 278
5.5.6 Werkzeuge 278
5.5.7 Follow-up – Good Practices und Varianten 279

5.6 Beratungsaufträge 280
5.6.1 Aktivitäten 280
5.6.2 Umfang, Objektivität und Sorgfalt 283
5.6.3 Revisionsplan, Risikoorientierung und IKS 285
5.6.4 Durchführung von Beratungsaufträgen 287
5.6.5 Maßnahmenüberwachung 290
5.6.6 Beratungsaufträge – Good Practices und Varianten 291
Literatur 292

6 Spezielle Auftragstypen und besondere Prüffelder 295
6.1 IKS und Risikomanagement 295
6.1.1 GRC-Funktionen in den COSO-Modellen 295
6.1.2 GRC-Prüfstandards der Abschlussprüfung 297
6.1.3 Beurteilungskriterien für Compliance-Managementsysteme 297
6.2 Die COSO-Leitfäden 299
6.2.1 Übersicht und Hintergründe 299
6.2.2 Die ersten COSO-Modelle 300
6.2.3 Ergänzung und Überarbeitung der COSO-Modelle 302
6.2.4 COSO für Prüfung und Nachweis 303
6.2.5 COSO für die Organisationsentwicklung 303
6.3 COSO Internal Control – Integrated Framework 304
6.3.1 Aufbau 304
6.3.2 Kontrollziele im COSO-IKS 305
6.3.3 IKS-Kontrollkomponenten 306
6.3.4 IKS-Prinzipien und -Attribute 306
6.3.5 Umsetzungshilfen und Anwendung 307
6.4 COSO Enterprise Risk Management Framework 310
6.4.1 COSO ERM 2004 – Bauplan für unternehmensweites Risikomanagement 310
6.4.2 Grundbausteine des unternehmensweiten Risikomanagementsystems 311
6.4.3 COSO ERM 2017 – Fokus Strategie und Wertbeitrag 316
6.4.4 Risikomanagement-Komponenten des COSO ERM 2017 318
6.4.5 Risikomanagement-Prinzipien des COSO ERM 2017 318
6.5 Informationstechnologie und -systeme 319
6.5.1 IT-Prüfung: Ziele, Möglichkeiten, Rahmen 321
6.5.2 Berufsständische Grundlagen für IT-Prüfer 322
6.5.3 IT-Prüflandkarte 325
6.5.4 Beurteilungs- und Organisationsmodelle 328
6.5.5 IT-Organisation 332
6.5.6 IT-Prozesse und IT-Services 333
6.5.7 Ansatzpunkte für die Prüfung der IT 333

6.6 Weitere Prüffelder 335
6.6.1 Sonderprüfungen 335
6.6.2 Projekte 336
6.6.3 Betriebliche Kernprozesse – Zyklenmodell 339
Literatur 339

7 Fachwissen/Glossar 343

8 Zusammenfassung mit Thesen und Resümee 383

9 Gesamtanhang zum Buch 389
9.1 Mission, Grundprinzipien und Definition der Internen Revision 389
9.2 Ethikkodex der Internen Revision 390
9.3 Verbindliche Berufsstandards der Internen Revision mit Erläuterungen 392
9.3.1 Attributstandards 392
9.3.2 Ausführungsstandards 400
9.4 IIA Switzerland Quality Self Assessment Tool (Q-SAT) 412

Stichwortverzeichnis 429

Abkürzungsverzeichnis

a. a. O.	am anderen Ort
a. F.	alte Fassung
ABl.	Amtsblatt
Abs.	Absatz
abzgl.	Abzüglich
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Aktiengesellschaft
AGG	Allgemeines Gleichbehandlungsgesetz
AktG	Aktiengesetz
AO	Abgabenordnung
Aufl.	Auflage
AWG	Außenwirtschaftsgesetz
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAG	Bundesarbeitsgericht
BB	Betriebsberater
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Entscheidungen des Bundesgerichtshofs in Strafsachen
BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen
BilMoG	Bilanzrechtsmodernisierungsgesetz
BIZ	Bank für Internationalen Zahlungsausgleich
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgericht Entscheidung Band
bzw.	Beziehungsweise
CAE	Chief Audit Executive

CEO	Chief Executive Officer
CFE	Certified Fraud Examiner
CGAP	Certified Government Auditing Professional
CIA	Certified Internal Auditor
CISA	Certified Information Systems Auditor
CMA	Certified Management Accountant
CMS	Compliance Management System
CPA	Certified Public Accountant
d. h.	das heißt
DB	Der Betrieb
DCGK	Deutscher Corporate Governance Kodex
DIIR	Deutsches Institut für Interne Revision e. V.
DSGVO	Datenschutzgrundverordnung
ECIIA	European Confederation of Institutes of Internal Auditing
ECIIA	European Confederation of Institutes of Internal Auditors
ECODA	European Confederation of Directors Associations
EG	Europäische Gemeinschaft
ENISA	European Network and Information Security Agency
ERP	Enterprise Resource Planning
ESt	Einkommensteuer
EStG	Einkommensteuergesetz
etc.	et cetera
ETF	Exchange Traded Fonds
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EUR	Euro
EURIBOR	European Interbank Offered Rate
EWG	Europäische Wirtschaftsgemeinschaft
f.	Folgende
FA	Finanzamt
FCPA	Foreign Corrupt Practices Act
FERMA	Federation of European Risk Management Associations
ff.	Fortfolgende
FG	Finanzgericht
gem.	Gemäß
GenG	Genossenschaftsgesetz
GeschGehG	Geschäftsgeheimnisgesetz
GG	Grundgesetz
ggf.	Gegebenenfalls
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GWB	Gesetz gegen Wettbewerbsbeschränkungen

GwG	Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten, Geldwäschegesetz
h. M.	Herrschende Meinung
HaftPflG	Haftpflichtgesetz
HGB	Handelsgesetzbuch
Hrsg.	Herausgeber
i. d. F.	in der Fassung
i. d. R.	in der Regel
i. S. d.	im Sinne des
i. Ü.	im Übrigen
i. V. m.	in Verbindung mit
i. w. S.	im weitesten Sinne
IAASB	International Auditing and Assurance Standards Board
ICEFR	Internal Control over External Financial Reporting (COSO)
ICFR	Internal Control over Financial Reporting (PCAOB)
ICoFR	Internal Control over Financial Reporting
IDW	Institut der Wirtschaftsprüfer in Deutschland e. V.
IDW PS	IDW Prüfungsstandard
IFAC	International Federation of Accountants
IFRS	International Financial Reporting Standards
IIA	The Institute of Internal Auditors Inc.
IIA CoE	IIA Ethikkodex (Code of Ethics)
IIA IG	IIA Implementierungsleitlinie (Implementation Guide)
IIAS	IIA-Standard
IKS	Internes Kontrollsystem
InsO	Insolvenzordnung
InvG	Investmentgesetz
ISA	International Standards on Auditing
ISA	International Standards on Auditing
ISACA	Information Systems Audit and Control Association
ISAE	International Standards on Assurance Engagements
ISAE	International Standard on Assurance Engagements
ISO	International Organization for Standardization
ITAF	ISACA IS Audit/Assurance Framework
ITIL	IT Infrastructure Library
JZ	Juristenzeitung
KAGB	Kapitalanlagegesetz
Komm.	Kommentar
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KPI	Key Performance Indicator
KWG	Kreditwesengesetz
KZfSS	Kölner Zeitschrift für Soziologie und Sozialpsychologie

LFGB	Lebensmittel-, Bedarfsgegenstände- und Futtermittelgesetzbuch
m. w. N.	mit weiteren Nachweisen
MaComp	Mindestanforderungen Compliance, Rundschreiben der BaFin
MaRisk	Mindestanforderungen Risikomanagement, Rundschreiben der BaFin
MarkenG	Markengesetz
Mio.	Millionen
NCFFR	U.S. National Commission on Fraudulent Financial Reporting
NIST	U.S. National Institute of Standards and Technology
NJOZ	Neue Juristische Online-Zeitschrift
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NZA	Neue Zeitschrift für Arbeitsrecht
NZG	Neue Zeitschrift für Gesellschaftsrecht
o. ä.	oder ähnlich
OECD	Organization for Economic Cooperation and Development
OLG	Oberlandesgericht
OWi	Ordnungswidrigkeit
OWiG	Gesetz über Ordnungswidrigkeiten
PatG	Patentgesetz
PCAOB	Public Company Accounting Oversight Board
PDCA	Plan-Do-Check-Act
PMI	Project Management Institute
PS	IDW Prüfungsstandard
resp.	respektive
RL	Richtlinie
RMS	Risikomanagement-System
Rn.	Randnummer
S.	Seite
SAP	Systemanalyse und Programmentwicklung
SEC	Securities and Exchange Commission
Sec.	Section
sog.	so genannte
SOX	Sarbanes-Oxley-Act
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TLoD	Three Lines of Defence-Model
TransPuG	Gesetz zur weiteren Reform des Aktien- und Bilanzrechts, zu Transparenz und Publizität
u. a.	unter anderem
u. E.	unseres Erachtens
u. U.	unter Umständen
UK	United Kingdom

UmwHG	Umwelthaftungsgesetz
US-GAAP	U.S. Generally Accepted Accounting Principles
usw.	und so weiter
UWG	Gesetz gegen den unlauteren Wettbewerb
v. a.	vor allem
VermAnlG	Gesetz über Vermögensanlagen
VerSanG	Verbandssanktionengesetz
VersR	Zeitschrift für Versicherungsrecht
VG	Verwaltungsgericht
vgl.	vergleiche
VorstOG	Vorstandsvergütungs-Offenlegungsgesetz
WHG	Wasserhaushaltsgesetz
WpDVerOV	Verordnung zur Konkretisierung der Verhaltensregeln und Organisationsanforderungen für Wertpapierdienstleistungsunternehmen
WPg	Die Wirtschaftsprüfung (Zeitschrift)
WpHG	Wertpapierhandelsgesetz
z. B.	zum Beispiel
z. T.	zum Teil
ZfRSoz	Zeitschrift für Rechtssoziologie
ZGR	Zeitschrift für Unternehmens- und Gesellschaftsrecht
ZIR	Zeitschrift Interne Revision
ZRFG	Zeitschrift für Risk, Fraud & Governance
zzgl.	zuzüglich
ZfRSoz	Zeitschrift für Rechtssoziologie

Über die Autoren

Dr. iur. Dr. phil. Jörg Berwanger, Neunkirchen/Saar, Jahrgang 1959, Assessorexamen 1989, Promotionen 2000 und 2004, arbeitet seit 2013 als Commercial Project Manager bei der STEAG New Energies GmbH (Saarbrücken). Hier übt er auch eine Compliancefunktion aus. Nach einer vorherigen Geschäftsführertätigkeit bei einem Arbeitgeberverband war er seit 1995 als Justiziar im Saarbergwerke AG-Konzern, später bei RAG Saarberg AG (beide Saarbrücken) tätig. Von 2002 bis 2004 war er Leiter Umweltschutz und leitender Justiziar bei der Saar Energie GmbH. Ende 2004 war er in Führungsfunktionen in Sachen Interne Revision und als Datenschutzbeauftragter tätig: Er war Leiter des Regionalbüros Saar der RAG Revisions-GmbH, 2008 übernahm er für Evonik Services GmbH die Leitung des Büros der Internen Revision in Saarbrücken. Nach einer zwischenzeitlichen Referententätigkeit für die Rechtsabteilung der STEAG GmbH übernahm er die derzeitige Position bei STEAG New Energies GmbH. Fachlich setzt er seine Akzente im Wirtschaftsrecht (incl. Arbeitsrecht und einschlägigem öffentlichen Recht), Strafrecht und Unternehmensrecht. Es gibt zahlreiche Veröffentlichungen, auch zu anderen Rechtsgebieten und zum Teil mit soziologischen Anklängen. Siehe dazu seine Autorenseite im elektronischen Gablerwirtschaftslexikon, wo auch sonstige Aktivitäten, wie z. B. Dozententätigkeiten an Hochschulen, aufgeführt sind.

Dr. Ulrich Hahn, Frankfurt am Main, ist langjähriges Mitglied der Fachverbände für Interne und IT-Revision und dort in vielen Gremien und Arbeitskreisen aktiv. Er war unter anderem Chairman der European Confederation of Institutes of Internal Auditing (ECIIA), Mitglied im Board of Trustees des Institute of Internal Auditors (IIA), Vorstandsmitglied im Deutschen Institut für Interne Revision (DIIR) sowie im ISACA Germany Chapter. Seine berufliche Laufbahn bei internationalen Prüfungsgesellschaften, führenden Technologieunternehmen und IT-Dienstleistern im In- und Ausland hat es ihm ermöglicht, ein sehr breites Spektrum an Governance-, Organisations- und Assurancepraktiken kennenzulernen. Seit langem engagiert er sich für die fachliche Aus- und Weiterbildung; heute primär durch Fortbildungen für Zertifikatsanwärter, Workshops sowie persönliche fachlich-organisatorische Unterstützung von Führungskräften und Teams in Governance-, Audit- und IT-Funktionen.