Aleksandra Sowa
Peter Duscha
Sebastian Schreiber

IT-Revision, IT-Audit und IT-Compliance

Neue Ansätze für die IT-Prüfung

2. Auflage

EBOOK INSIDE

Springer Vieweg

IT-Revision, IT-Audit und IT-Compliance

Aleksandra Sowa · Peter Duscha ·
Sebastian Schreiber

IT-Revision, IT-Audit und IT-Compliance

Neue Ansätze für die IT-Prüfung

2., aktualisierte Auflage

Springer Vieweg

Aleksandra Sowa
Deutsche Telekom AG, Bonn, Deutschland

Peter Duscha
Frankfurt, Deutschland

Sebastian Schreiber
Syss GmbH
Tübingen, Deutschland

ISBN 978-3-658-23764-6 ISBN 978-3-658-23765-3 (eBook)
https://doi.org/10.1007/978-3-658-23765-3

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

Springer Vieweg

Springer Vieweg 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

Inhaltsverzeichnis

Abkürzungsverzeichnis

ACH	Automated Clearing House
AktG	Aktiengesetz
APT	Advanced Persistent Threat
AV	Antiviren-Software, Antiviren-Programm (kurz: AV-Software)
BaFin	Bundesanstalt für Finanzaufsicht
BDSG	Bundesdatenschutzgesetz
BIA	Business Impact Analysis
BKA	Bundeskriminalamt
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz
bspw.	beispielsweise
bzw.	beziehungsweise
CEO	Chief Executive Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COO	Chief Operating Officer
CSO	Chief Security Officer
(D)DoS	(Distrubuted) Denial of Service Attack
d. h.	das heißt
DIIR	Deutsches Institut für Interne Revision e. V.
DSGVO	Datenschutzgrundverordnung (auch EU-DSGVO)
DSP	Digital Service Provider (Anbieter digitaler Dienste)
ENISA	European Network and Information Security Agency
EU	Europäische Union
EW	Eintrittswahrscheinlichkeit
ff.	folgende [Seiten]
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GSHB	IT-Grundschutzhandbuch des BSI (IT-Grundschutz ermöglicht es, notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen)
HGB	Handelsgesetzbuch

IAASB	International Auditing and Assurance Standards Board
i. d. R.	in der Regel
IDS	Intrusion-Detection-System
IDW	Institut der Wirtschaftsprüfer in Deutschland e. V.
IKS	Internes Kontrollsystem
IoT	Internet of Things (Internet der Dinge)
ISA	International Standards on Auditing
ISACA	Information Systems Audit and Control Association, internationaler Berufsverband der IT-Revisoren, Informationssicherheitsmanager und IT-Governance-Experten
ISM	Information Security Management (auch: IT-Sicherheitsmanagement)
ISMS	Information Security Management System
ISO	International Organization for Standardization (Internationale Organisation für Normung) internationale Vereinigung der Standardisierungsgremien, Herausgeber der ISO-Normen (z. B.: ISO/IEC 27001 ff)
ITIL ®	IT Infrastructure Library, eine Sammlung von Prozessen, Funktionen und Rollen, die typischerweise in einer IT-Infrastruktur von mittleren und großen Unternehmen vorkommen
ITSiG	IT-Sicherheitsgesetz, eigentlich: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme
KPI	Key Performance Indicator
KRITIS	Kritische Infrastrukturen
KWG	Kreditwesengesetz
MAD	Mean Absolute Deviation
Mio.	Millionen
Mrd.	Milliarden
NBL	Newcomb Benford Law
NGSOC	Next Generation SOC
NISD	Network and Information Security Directive (auch: NIS-Richtlinie, NIS-RL)
OWiG	Gesetz über Ordnungswidrigkeiten
PDCA	Plan-Do-Check-Act (Phasen des Informationssicherheitsmanagements)
PRAGMATIC	Akronym für Predictive, Relevant, Actionable, Genuine, Meaningful, Accurate, timely, Independent und Cheap – Prinzip für u. a. Kennzahlensysteme und Metriken
PS	Prüfungsstandard
RS	Stellungnahme zur Rechnungslegung
S.	Seite
SIEM	Security Information and Event Management, verbindet Security Information Management (SIM) und Security Event Manager (SEM)

SMART	Akronym für Specific, Measurable, Accepted, Relevant und Timely (oder: Tome Bound) – Prinzip für u. a. Kennzahlensysteme und Metriken (aber auch Projektmanagement)
sog.	sogenannte
StGB	Strafgesetzbuch
TKG	Telemediengesetz
TOM	technische und organisatorische Maßnahmen
u. a.	unter anderem
VAG	Versicherungsaufsichtsgesetz, Gesetz über die Beaufsichtigung der Versicherungsunternehmen
vgl.	vergleiche
WAF	Web Application Firewall
WS	Wahrscheinlichkeit
z. B.	zum Beispiel

Einleitung

1

STADTHAUPTMANN. Ich habe Sie hergebeten, meine Herren, um Ihnen eine äußerst unerfreuliche Mitteilung zu machen. Ein Revisor kommt in unsere Stadt.

AMMOS FJODOROWITSCH. Ein Revisor?

ARTEMIJ FILIPPOWITSCH. Ein Revisor?

STADTHAUPTMANN. Ja, ein Revisor aus Petersburg. Inkognito. Und in geheimer Mission.

AMMOS FJODOROWITSCH. Eine schöne Bescherung!

ARTEMIJ FILIPPOWITSCH. Das hat uns gerade noch gefehlt!

LUKA LUKITSCH. Mein Gott! Und auch noch in geheimer Mission!

Nikolaj Gogol, Der Revisor (I, 1).

Zusammenfassung

Die Methoden, Routinen und Standards in der Revisionsarbeit sind notwendig zur Legitimation ihrer Vorgehensweisen und Prüfungsergebnisse gegenüber den Geprüften, der Aufsicht, den Auftraggebern, den Kontrollgremien etc. Das Prüfungsergebnis muss plausibel, der Weg dorthin nachvollziehbar und repetierbar sein. Das „Sich-selbst-in-Frage-Stellen" ist in dem Sinne für die Revision von Relevanz, dass sie sich regelmäßig an die neuen Rahmenbedingungen, Normen und Anforderungen anpassen, modernisieren und ihre Methoden weiterentwickeln muss, um nicht obsolet zu werden. In diesem Kapitel werden die neuen Methoden kurz skizziert und erläutert. Der interessierte Prüfer wird in die Arkana der statistisch-mathematischen Methoden herangeführt, welche in der Form noch nicht in einem Werk für die Revision

A. Sowa et al., *IT-Revision, IT-Audit und IT-Compliance,*
https://doi.org/10.1007/978-3-658-23765-3_1

zusammengefasst wurden. Ebenfalls kann der Prüfer neue Themen, wie Mock Dawn Raid, Prüfung der Umsetzung von Meldepflichten oder interne Ermittlungen als systematische Revisionsprüfungen erfassen und umsetzen.

„Ihr Fortdauern", schrieb in dem Buch *Zweifel an der Methode* der Philosoph Leszek Kolakowski, „verdankt […] die Philosophie dem niemals endenden Sich-selbst-in-Frage-Stellen"[1]. Für die Suche nach dem Sinn würde in den Geisteswissenschaften seiner Meinung nach so etwas wie „die Methode" im besten Sinne des Wortes gar nicht existieren. „Vielleicht kommt in diesem Zweifel das schlechte Gewissen der Philosophie zum Ausdruck", vermutete er, „dieses schlechte Gewissen scheint immerhin fast ebenso alt zu sein wie die Philosophie selber." Philosophie bedürfe jedoch vielleicht genau dieser „Unsicherheit ihres Legitimationsprinzips", um weiter zu bestehen.

Der Beruf des Revisors/der Revisorin[2] besteht nach historischen Übermittlungen vermutlich nicht so lange wie der des Philosophen, doch lange genug, um auf eine reiche – gerade was Methoden betrifft – Tradition und zahlreiche Vorbilder zurückzugreifen. Auf eines dieser berühmten Vorbilder, oder besser gesagt „Anti-Vorbilder", aus dem bekannten Stück Nikolay Gogols *Der Revisor* wird in diesem Buch an einigen Stellen erinnert.

Und auch wenn sich heute die vorrangig praktische Philosophie zunehmend mathematischer Methoden, u. a. zur Beweisführung ihrer Hypothesen, bedient, so stützt sich die Arbeit des Revisors seit jeher auf Methoden, die sowohl Anwendung als auch Theorie der Mathematik und Statistik umfassen. Es ist das Praktische, das Systematische und das Strukturierte, was der Revisor für seine Arbeit benötigt. Erst dann sind Ergebnisse seiner Prüfungen nachvollziehbar: Die Transparenz ist die notwendige, wenn auch nicht hinreichende, Bedingung der Prüfbarkeit.

Die Methoden, Routinen und Standards in der Revisionsarbeit sind notwendig zur Legitimation ihrer Vorgehensweisen und Prüfungsergebnisse gegenüber den Geprüften, der Aufsicht, den Auftraggebern, den Kontrollgremien etc. Das Prüfungsergebnis muss plausibel, der Weg dorthin nachvollziehbar und repetierbar sein. Das „Sich-selbst-in-Frage-Stellen" ist in dem Sinne für die Revision von Relevanz, als dass sie sich regelmäßig an die neuen Rahmenbedingungen, Normen und Anforderungen anpassen, modernisieren und ihre Methoden weiterentwickeln muss, um nicht obsolet zu werden.

Über Jahrzehnte haben die Revisoren, die Auditoren und die internen Ermittler Methoden und Werkzeuge entwickelt, die zweierlei bewirken: Sie helfen einerseits dem Adepten der Prüfungskunst, auf Best Practices und erprobte Verfahren zurückzugreifen

[1] Kolakowski, L. (1977). *Zweifel an der Methode.* Stuttgart: Kohlhammer, S. 7.

[2] Aus Gründen der besseren Lesbarkeit wird in diesem Buch jeweils männliche Form verwendet, obwohl natürlich gleichermaßen Frauen wie Männer gemeint sind.

und so das Handwerk des Revisors zu erlernen – und machen andererseits die Methoden der Revisionsarbeit für die Geprüften und Dritte transparent und nachvollziehbar.

Gewiss erlangte der Revisor im Laufe der Jahre durch seine unabhängige Stellung, seine Objektivität, Unnachgiebigkeit und Unbestechlichkeit eine besondere Position und einen – oft wenig vorteilhaften – Ruf in der Gesellschaft, in den Unternehmen und Organisationen. Die Revision ist zum wichtigen Instrument der Geschäftsführung geworden, indem sie die Ordnungsmäßigkeit und Wirksamkeit des internen Kontrollsystems (IKS) bewertet und beurteilt, Vorfälle, Schwachstellen und Unregelmäßigkeiten lückenlos aufdeckt und aufklärt. Gerade seit sie nach den Wirtschaftsskandalen des Jahres 2002 zum Bestandteil – und Wächter – des internen Kontroll- und Überwachungssystems geworden ist, avancierte die Revision schnell zum sprichwörtlichen „Hexenhammer" der Compliance-Organisation im Kampf gegen Korruption oder Veruntreuung.

Die besondere Stellung der Revision im Unternehmen, insbesondere in den Banken und Kreditinstituten, weckt Begehrlichkeiten. Wurde in dem wegweisenden Compliance-Urteil aus dem Jahr 2009 noch der Revisionsleiter wegen Nichteinhaltung der Compliance im Unternehmen verurteilt, befassen sich heute immer mehr Abteilungen und Organisationseinheiten mit Aufgaben, die originär im Zuständigkeitsbereich der Revision lagen. Die Funktionstrennung zwischen Vorgabe und Kontrolle verwischt zunehmend, und Prüfungen bzw. Audits führen heute nicht nur die Interne Revision und Wirtschaftsprüfer durch, sondern auch Compliance-Abteilungen, Datenschutzbeauftragte, Sicherheitsbeauftragte, Chief Information Security Officer (CISOs) und IT-Sicherheitsverantwortliche, externe Dritte, Forensik-Unternehmen etc.

Dieses Buch richtet sich an alle, die Prüfungen durchführen oder sich auf die Durchführung solcher vorbereiten wollen. Der Fokus liegt auf den sogenannten IT-Prüfungen (Prüfungen der Informationstechnologie und ihrer Aspekte), die eine schnell wachsende Gruppe der Revisionsprüfungen umfassen, vorrangig durch die steigende Abhängigkeit der Ablauf- und Aufbauorganisation von der Informationstechnologie. Es gibt heute kaum noch einen Aspekt der Unternehmensarbeit, der nicht von der Informationstechnologie abhängig wäre. Deswegen nimmt die Prüfung der IT einen immer wesentlicheren Teil der „traditionellen" Revisionsprüfungen ein.

1.1 Buchinhalte

Im vorliegenden Buch werden die modernen Grundlagen der Revisionsarbeit systematisiert, erklärt und erläutert. Basierend auf den Best Practices und erprobten Traditionen, werden die Herangehensweisen aktualisiert und erweitert. Der interessierte Prüfer wird in die Arkana der statistisch-mathematischen Methoden herangeführt, welche in der Form noch nicht in einem Werk für die Revision zusammengefasst wurden. Ebenfalls kann der Prüfer neue Themen, wie Mock Dawn Raid, Prüfung der Umsetzung von

Meldepflichten oder interne Ermittlungen als systematische Revisionsprüfungen erfassen und umsetzen. IT-Forensik als Revisionsprüfung? Eine systematische Anleitung für die Revisoren wird erstmalig auf den Seiten dieses Buches vorgestellt, gleichwohl sich die Methodik – da es sich um relativ neue Phänomene handelt – stets weiterentwickelt.

Von „Theoriemüdigkeit" schreibt Roberto Simanowski in seinem Buch *Data Love* und meint damit die theoriefreien Auswertungen von Massendaten auf der Suche nach zufälligen und oft willkürlichen Zusammenhängen.[3] Peter Duscha, Mathematiker und erfahrener Prüfungsleiter in Finanzinstituten, zeigt auf, warum sich Prüfer auf Standards, Rahmenwerke und methodisch erprobte Verfahren stützen sollten. Peter Duscha lotst in Kap. 2 durch die schier unendliche Wüste von Revisionsstandards relevanter, normengebender Organisationen und vergleicht die Werke im Hinblick auf die Anwendbarkeit. Er systematisiert die Methoden der Prüfung und führt mit Hinweisen und Best Practices durch alle Phasen der Prüfung hindurch, von der Planung bis hin zur Berichterstellung und zum Follow-up. Vorab, in Kap. 3, wird der Versuch unternommen, die heute gängigen Begriffe und Bezeichnungen für die Revisionsarbeit, Audit, Prüfung und Monitoring gemäß dem aktuellen Verständnis der Begriffe zu definieren, zu systematisieren und zu differenzieren.

Sebastian Schreiber, Gründer und Geschäftsführer des IT-Sicherheitsunternehmens SySS GmbH, das Sicherheitsprüfungen bei einer Vielzahl von Firmen durchführt und der ein gefragter Experte für IT-Sicherheit in Printmedien, Fernsehen und Rundfunk ist (u. a. Tagesschau, Plusminus, Günther Jauch etc.), systematisiert in Kap. 5 Penetrationstests als Prüfungsform, die von der Revision im Rahmen von Security-Audits implementiert werden kann. Die Aufgabe von Penetrationstests ist es – wenn korrekt konzipiert und durchgeführt –, anhand von realen Prüfungen das Sicherheitsniveau der Zielsysteme zu ermitteln. Kurz: Es wird geprüft, ob Angriffe in der Realität erfolgreich durchgeführt werden können.

In Kap. 4, 6 und 7 werden die neuen Arbeitsansätze der Revisionsarbeit dem Status quo entsprechend systematisiert. Dr. Aleksandra Sowa, Expertin für Informationssicherheit, Datenschutzauditorin und Datenschutzbeauftragte, systematisiert Investigationen als originäre Aufgabe der Revision, die zunehmend an spezialisierte Kanzleien und Drittanbieter delegiert wird. Der Revision kann jedoch im Rahmen von z. B. Unterschlagungsprüfungen bei konkretem Verdacht eine interne Investigation übertragen werden. Die Methoden, auf welche die Revision zurückgreifen kann, unterscheiden sich, ob bei einem Verdacht auf Zahlenmanipulationen, bspw. im Transaktionsbereich, oder beim Verdacht auf Cyberattacken.

Sowohl bei Datenschutz- als auch bei Sicherheitsvorfällen kommen auf die Unternehmen Pflichten zur behördlichen Meldung des Vorfalls zu. In Kap. 6 werden Vorgaben zu den Meldepflichten aus BSIG und DSGVO zusammengefasst und Prüfungsansätze vorgeschlagen. Ähnlich den Prüfungen der Notallsysteme und insbesondere der

[3] Simanowski, R. (2014). *Data Love.* Berlin: Matthes & Seitz Berlin.

Notfallübungen etablierte sich eine neue Prüfungsart, welche die Ordnungsmäßigkeit und Wirksamkeit der kartellrechtlichen Compliance ermöglicht. Mock Down Raids, beschrieben in Kap. 7, haben sich als eine sinnvolle Ergänzung der Ordnungsmäßigkeitsprüfung des Compliancemanagements gemäß Prüfungsstandard des Instituts der Wirtschaftsprüfer, IDW PS 980, erwiesen.

1.2 Historisches

Dass die Revision – anders als die Philosophie – für ihr Fortbestehen gerade Regeln und Methoden braucht, zeigt ein Vorfall, der sich im Zarenrussland Ende des 19. Jahrhunderts ereignet haben soll. Im Gouvernement Nowgorod soll sich ein Durchreisender als Ministerialbeamter ausgegeben und die Bewohner der Stand Ustjushna um ihr Geld gebracht haben. Diese Geschichte hat Alexander Puschkin als ein „Sujet", eine Idee, für eine Komödie seinem Schriftstellerkollegen Nikolay Gogol gegeben. Puschkin erfuhr während seiner Reise nach Orenburg außerdem von einem geheimen Dokument, in dem die Obrigkeiten der Stadt gewarnt wurden, der Zweck seiner Reise sei nur ein Vorwand für seinen tatsächlichen Auftrag, nämlich die Beamten einer Überprüfung zu unterziehen.[4]

Nikolay Gogol verarbeitete die Geschichte in einem Theaterstück, *Der Revisor*, das inzwischen eine mehr oder minder gelungene Verfilmung und unzählige Theatervorführungen erfuhr. In den beinahe zwei Jahrhunderten seit ihrer Entstehung verlor die Komödie kaum an Aktualität, beeindruckt durch ihre frische und direkte Art, Korruption und Missbräuche aufzuzeigen. Auszüge aus dem Stück dienen als Motto für die einzelnen Kapitel des Buches. „Worüber lacht ihr denn? Ihr lacht über euch selbst!", urteilt unerbittlich Gogol.[5]

[4]Aus dem Kapitel „Zeitdokumente und Entstehung, Aufführung und Rezeption des Revisors" in: Gogol, N. (1996). *Der Revisior.* Reclams Universal-Bibliothek Nr. 837. S. 141.

[5]Gogol, N. (1996). *Der Revisior.* Reclams Universal-Bibliothek Nr. 837.

Audit, Continuous Audit, Monitoring und Revision

2

Peter Duscha

KAUFLEUTE (sich verneigend). Wir wünschen einen guten Tag, gnädiger Herr!

STADTHAUPTMANN. Na, ihr Lieben, wie geht es euch denn? Was machen die Geschäfte? Ihr Samowarhelden, ihr Falschmesser beschwert euch über mich? Ihr Erzgauner, Oberbestien, Halsabschneider führt Beschwerde? Und hat es sich für euch gelohnt? Ihr habt wohl gedacht, den bringen wir ins Gefängnis […] Sieben Teufel und eine Hexe sollen euch ins Gesicht springen. Wisst ihr nicht, dass […]

ANNA ANDREJEWNA. Mein Gott, Antoscha, was du wieder für Wörter benutzt!

STADTHAUPTMANN (ärgerlich). Hier geht es jetzt nicht um Wörter! Wisst ihr, dass derselbe Beamte, bei dem ihr euch beschwert habt, meine Tochter heiraten wird? NA? Was sagt ihr jetzt? Jetzt werde ich es euch zeigen […]

Nikolaj Gogol, Der Revisor (V, 2)

Zusammenfassung

In der Fachliteratur werden die Begriffe Prüfung (Auditing) und Überwachung (Monitoring) oft synonym verwendet. In diesem kurzen Kapitel wird der Versuch unternommen, diese wesentlichen Begriffe der Revisionswelt anhand der gesetzlichen Grundlagen und der berufsständischen Standards der Internen und Externen Revision zu differenzieren. Darüber hinaus werden die im direkten Zusammenhang stehenden Begriffe „Continuous Auditing“, „Continuous Monitoring“ und der ins Deutsche überführte Begriff „Audit“ näher beleuchtet und eine Differenzierung versucht.

A. Sowa et al., *IT-Revision, IT-Audit und IT-Compliance*,
https://doi.org/10.1007/978-3-658-23765-3_2

Dazu werden zuerst die wesentlichen gesetzlichen Grundlagen betrachtet. Dabei ist zu beachten, dass verschiedene Branchen besonderen Regeln zur Internen Revision unterliegen, die eine Ausstrahlung auf die gesamte Revisionswelt entwickeln. Die Finanzwirtschaft ist hier ein prominentes Beispiel.

In der relevanten Fachliteratur werden viele Begriffe unterschiedlich verwendet. Darunter natürlich auch Begriffe aus dem Umfeld der Internen Revision bzw. der IT-Revision. In diesem Kapitel geht es nicht darum, eventuelle Begriffsüberschneidungen generell aufzuklären. Es soll vielmehr ein gemeinsames Verständnis für die später verwendeten Begriffe und Definitionen erzeugt werden.

Zu diesem Zweck ist es sinnvoll, sich einen Überblick über die wesentlichen gesetzlichen Grundlagen zu verschaffen. Dabei unterliegen verschiedene Branchen besonderen Regeln für die Interne Revision. Die Finanzwirtschaft ist hier ein prominentes Beispiel. Auch existieren Unterschiede der gesetzlichen Regelungen im Verhältnis zu Unternehmensgröße und Gesellschaftsform, auf die im Folgenden nicht weiter eingegangen werden kann.

2.1 Allgemeine gesetzliche Grundlagen zur Internen Revision

Laut § 91 Abs. 2 des Aktiengesetzes (AktG) hat der Vorstand einer Aktiengesellschaft (AG) geeignete Maßnahmen zu treffen, um den Fortbestand der Gesellschaft gefährdende Entwicklungen frühzeitig zu erkennen.

Dabei soll er insbesondere ein Überwachungssystem einrichten. Wie dieses ausgestaltet sein sollte, ist im Gesetzestext nicht erläutert. Nun wurde der zweite Absatz des § 91 AktG durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) ergänzt. Dort steht in der Begründung des Gesetzentwurfs, dass der Vorstand für ein angemessenes Risikomanagement und eine angemessene Interne Revision zu sorgen hat. Damit wird klar, was der Gesetzgeber mit einem Überwachungssystem gemeint hat: Zumindest Risikomanagement und Interne Revision.

Im selben Abschnitt der Gesetzesbegründung findet sich ferner, dass von einer Ausstrahlungswirkung auf alle Unternehmen, abhängig von ihrer Größe und Komplexität, ausgegangen wird, obwohl dafür kein expliziter Gesetzesrahmen vorhanden ist. Der Revisionsstandard Nr. 2 („Prüfung des Risikomanagementsystems durch die Interne Revision“, Version 2.0, 2018) des Deutschen Instituts für Interne Revision (DIIR) bezieht sich bei den rechtlichen Grundlagen (Abschnitt 3, Textziffer 10) auch auf die eben genannte Gesetzesbegründung.

Im Gesetz über das Kreditwesen (KWG, Stand Januar 2017) schreibt der Gesetzgeber in § 25a Abs. 1 Nr. 3 noch deutlicher vor, dass ein Institut ein internes Kontrollsystem und eine Interne Revision einrichten muss. Dem Wortlaut nach besteht ein internes Kontrollsystem aus Prozessen zur Identifizierung, Beurteilung, Steuerung sowie Überwachung und Kommunikation der Risiken entsprechend den in Titel VII Kapitel 2 Abschnitt 2 Unterabschnitt II der EU-Bankenrichtlinie (Richtlinie 2013/36/EU) niedergelegten Kriterien. Diese wiederum werden von der deutschen Regulierungsbehörde, der

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) in regelmäßigen Rundschreiben für den deutschen Rechtsraum konkretisiert. Diese Rundschreiben sind bekannt als Mindestanforderungen an das Risikomanagement von Kreditinstituten (MaRisk, [1]). In den MaRisk wird zudem auch die Ausgestaltung einer Internen Revision konkretisiert.

Mittels der gleichen Schlussfolgerung wie zu § 91 AktG entwickelt auch § 25a KWG mitsamt seiner Konkretisierung durch die MaRisk eine Ausstrahlungswirkung auf Unternehmen außerhalb der Finanzbranche. Somit ist es für alle Unternehmen geraten, wenn auch für Unternehmen außerhalb der Finanzbranche nicht explizit gefordert, ihr Risikomanagement und ihre Interne Revision nach den Maßgaben der MaRisk aufzustellen.

Die seit 2011 fortschreitende Bankenunion der EU hat auch bei der Internen Revision nicht Halt gemacht. Die am 27. September 2011 von der European Banking Authority (EBA) herausgegebenen Leitlinien zur internen Governance (GL 44) sind seit dem 26. September 2017 aktualisiert [2]. Dort widmet sich der Abschnitt 22 der Internen Revision. Unter anderem wird in Textziffer 204 auf die Standards des **Institute of Internal Auditors** (IIA) hingewiesen. Diese werden uns in Abschn. 3.2 wieder begegnen.

2.2 3LoD: Three Lines of Defence

Die Überlegungen aus Abschn. 2.1 bringen uns zum „Three-Lines-of-Defence"-Modell (3LoD-Modell[1]). Nach Meinung der Europäischen Bankenaufsicht („European Banking Authority", EBA; vgl. [1]) verkörpert das 3LoD-Modell die Grundlage für ein funktionierendes Corporate Governance System, bestehend aus

- dem internem Kontrollsystem (1st Line),
- einer unabhängiger Risikomanagement- und Compliancefunktion (2nd Line) und
- der Internen Revision (3rd Line).

Diese Elemente sind demnach drei aufeinander aufbauende Verteidigungslinien, die unabhängig voneinander agieren und daher die Sicherheit der Unternehmung erhöhen bzw. das Risiko senken (siehe Abb. 2.1).

Die **erste Verteidigungslinie** besteht aus den Mitarbeitern, die direkt oder indirekt an den Prozessen beteiligt sind, welche die Unternehmung ihrem Geschäftszweck näherbringen (Geschäftsprozesse). Das schließt auch die Budgetierung, Planung und ggf. Forschung mit ein. Insbesondere betrifft dies das Linienmanagement, welches verantwortlich ist für die Planung, Implementierung und Überwachung der kontinuierlichen Steuerungs- und Kontrollaktivitäten.

Die **zweite Verteidigungslinie** besteht aus den Compliance-, Qualitäts- und Risikomanagementfunktionen, die das Linienmanagement beraten und beaufsichtigen sowie der Geschäftsführung regelmäßig unabhängig Bericht erstatten. Insbesondere validiert

[1]Eine gute Zusammenfassung des 3LoD-Modells aus Sicht der IT-Revision bietet auch der Artikel von Ken Doughty [3].

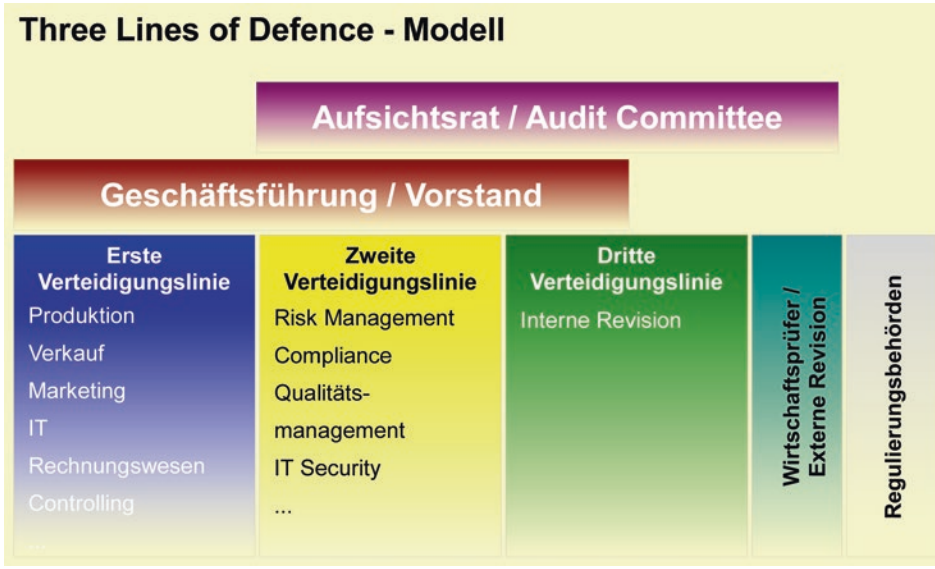

Abb. 2.1 Three-Lines-of-Defence-Modell

und überwacht die zweite Verteidigungslinie die Steuerungs- und Kontrollaktivitäten des Linienmanagements. Zur zweiten Verteidigungslinie gehören auch die IT-Sicherheit oder ähnliche Funktionen, die auf die allgemeine Sicherheit der Unternehmung und ihrer Mitarbeiter ausgerichtet sind.

Die **dritte Verteidigungslinie** setzt sich aus der Internen und im weiteren Sinne auch der Externen Revision zusammen. Im Folgenden wird der Begriff im engeren Sinn ausgelegt, weshalb lediglich die Interne Revision gemeint ist. Die dritte Verteidigungslinie soll als letzte Instanz innerhalb der Unternehmung deren Sicherheit und Risikolage ganzheitlich beurteilen, unabhängig von den zugrunde liegenden Geschäfts- und Risikomanagementprozessen.

2.3 Rolle der Internen Revision

Nach der Definition des **Institute for Internal Auditors** (IIA), welche vom DIIR übernommen wurde, erbringt die Interne Revision

> […] unabhängige und objektive Prüfungs- und Beratungsdienstleistungen, welche darauf ausgerichtet sind, Mehrwerte zu schaffen und die Geschäftsprozesse zu verbessern. Sie unterstützt die Organisation bei der Erreichung ihrer Ziele, indem sie mit einem systematischen und zielgerichteten Ansatz die Effektivität des Risikomanagements, der Kontrollen und der Führungs- und Überwachungsprozesse bewertet und diese verbessern hilft.

Diese Definition schließt im Wesentlichen auch die in den MaRisk genannten Aufgaben ein. Nach AT 4.4.3, Abs. 3 hat die Interne Revision

> […] risikoorientiert und prozessunabhängig die Wirksamkeit und Angemessenheit des Risikomanagements im Allgemeinen und des internen Kontrollsystems im Besonderen sowie die Ordnungsmäßigkeit grundsätzlich aller Aktivitäten und Prozesse zu prüfen und zu beurteilen, unabhängig davon, ob diese ausgelagert sind oder nicht.

2.4 Monitoring

Die Mindestanforderungen an das Risikomanagement der BaFin (MaRisk) unterscheiden in AT 4.4 besondere Funktionen zwischen Risikocontrolling (AT 4.4.1) und Interner Revision (AT 4.4.3). Dies entspricht zwar nicht dem Wortlaut aus der Gesetzesbegründung zu § 91 Abs. 2 AktG, jedoch kann man aus der gegenseitigen Ausstrahlungswirkung folgern, dass damit die gleichen Funktionen gemeint sind. Diese Sichtweise wird ebenfalls durch die weitgehende Übereinstimmung zwischen dem Standard Nr. 2 des DIIR und den in den MaRisk, AT 4.4.1 beschriebenen Aufgaben bestätigt. Danach sind im Wesentlichen folgende Elemente Teil des Risikomanagements bzw. -controllings:

- Unterstützung der Geschäftsleitung in allen risikopolitischen Fragen, insbesondere bei der Entwicklung und Umsetzung der Risikostrategie sowie bei der Ausgestaltung eines Systems zur Begrenzung der Risiken;
- Durchführung der Risikoinventur und Erstellung des Gesamtrisikoprofils;
- Unterstützung der Geschäftsleitung bei der Einrichtung und Weiterentwicklung der Risikosteuerungs- und -controllingprozesse;
- Einrichtung und Weiterentwicklung eines Systems von Risikokennzahlen und eines Risikofrüherkennungsverfahrens;
- laufende Überwachung der Risikosituation des Instituts und der Risikotragfähigkeit sowie der Einhaltung der eingerichteten Risikolimits;
- regelmäßige Erstellung der Risikoberichte für die Geschäftsleitung;
- Verantwortung für die Prozesse zur unverzüglichen Weitergabe von unter Risikogesichtspunkten wesentlichen Informationen an die Geschäftsleitung, die jeweiligen Verantwortlichen und ggf. die Interne Revision.

Insbesondere soll die oben beschriebene Funktion die laufende Überwachung der Risiken der Unternehmung für die Geschäftsführung sicherstellen (AT 4.4.1, Abs. 1). Diese Überwachung im engeren Sinne nennen wir im Folgenden *Monitoring*[2]. In den Begriffen des 3LoD-Modells ist dies die Aufgabe der zweiten Verteidigungslinie Abschn. 2.2.

[2]Dies sollte nicht mit dem Begriff *Monitoring* aus dem „Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management Framework"-Modell (COSO-ERM-Modell) verwechselt werden. COSO ERM versteht den Begriff als Überwachung im weiteren Sinne, also einschließlich der Internen Revision. Aus Sicht der Internen Revision ist diese Definition indes selbstreferenziell und daher nicht sinnvoll.