Aleksandra Sowa
Peter Duscha
Sebastian Schreiber

IT-Revision, IT-Audit und IT-Compliance

Neue Ansätze für die IT-Prüfung

Springer Vieweg

IT-Revision, IT-Audit und IT-Compliance

Lizenz zum Wissen.

Sichern Sie sich umfassendes Technikwissen mit Sofortzugriff auf tausende Fachbücher und Fachzeitschriften aus den Bereichen: Automobiltechnik, Maschinenbau, Energie + Umwelt, E-Technik, Informatik + IT und Bauwesen.

Exklusiv für Leser von Springer-Fachbüchern: Testen Sie Springer für Professionals 30 Tage unverbindlich. Nutzen Sie dazu im Bestellverlauf Ihren persönlichen Aktionscode **C0005406** auf *www.springerprofessional.de/buchaktion/*

Jetzt 30 Tage testen!

Springer für Professionals.
Digitale Fachbibliothek. Themen-Scout. Knowledge-Manager.

- Zugriff auf tausende von Fachbüchern und Fachzeitschriften
- Selektion, Komprimierung und Verknüpfung relevanter Themen durch Fachredaktionen
- Tools zur persönlichen Wissensorganisation und Vernetzung

www.entschieden-intelligenter.de

Springer für Professionals

Springer

Aleksandra Sowa • Peter Duscha
Sebastian Schreiber

IT-Revision, IT-Audit und IT-Compliance

Neue Ansätze für die IT-Prüfung

Springer Vieweg

Aleksandra Sowa
Bonn, Deutschland

Peter Duscha
Frankfurt, Deutschland

Sebastian Schreiber
Syss GmbH
Tübingen, Deutschland

ISBN 978-3-658-02807-7 ISBN 978-3-658-02808-4 (eBook)
DOI 10.1007/978-3-658-02808-4

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 Fachmedien Wiesbaden 2015
Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.
Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.
Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen.

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Fachmedien Wiesbaden GmbH ist Teil der Fachverlagsgruppe Springer Science+Business Media (www.springer.com)

Inhalt

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)

„Ihr Fortdauern", schrieb der polnische Philosoph Leszek Kolakowski, der u. a. an den Universitäten in Warschau und Oxford lehrte, in seinem Buch *Zweifel an der Methode*, „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", vermutet er, „dieses schlechte Gewissen scheint immerhin fast ebenso alt zu sein wie die Philosophie selber." Philosophie bedürfe jedoch, so Kolakowski, vielleicht genau dieser „Unsicherheit ihres Legitimationsprinzips", um weiterzubestehen.

Der Beruf des Revisors besteht nach historischen Übermittlungen vermutlich nicht so lange wie der des Philosophen, doch lange genug, um auf eine reiche Tradition und zahlreiche Vorbilder zurückzugreifen. Auf eines dieser berühmten Vorbilder, oder besser

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

© Springer Fachmedien Wiesbaden 2015

A. Sowa et al., *IT-Revision, IT-Audit und IT-Compliance*,
DOI 10.1007/978-3-658-02808-4_1

gesagt „Anti-Vorbilder“, aus dem bekannten Stück Nikolay Gogols *Der Revisor* wird in diesem Buch häufig zurückgegriffen.

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.

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.

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 die Best Practices und erprobte Verfahren zurückzugreifen und so das Handwerk des Revisors zu lernen – 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 Überwacher – des internen Kontroll- und Überwachungssystem geworden ist, avancierte die Revision schnell zum sprichwörtlichen „Hexenhammer“ der Compliance-Organisation im Kampf gegen die 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 Business-Security-Verantwortliche, externe Dritte, Forensik-Firmen 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), 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. In diesem Werk werden sowohl die weibliche als auch die männliche Form von Berufsbezeichnungen verwendet. In jedem Fall ist damit auch das andere Geschlecht mit einbezogen.

1.1 Buchinhalte

Im vorliegenden Buch werden die modernen Grundlagen der Revisionsarbeit systematisiert, erklärt und erläutert. Basierend auf den Best Practices und erprobten Traditionen der Revisionsarbeit, 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, Datenschutzaudit 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.[2] 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. 3 durch die schier unendliche Wüste von Revisionsstandards zweier für die IT-Revision 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. 2, 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.

In den Kapiteln Kap. 4 bis Kap. 6 werden die neuen Arbeitsansätze der Revisionsarbeit dem Status quo entsprechend systematisiert. Dr. Aleksandra Sowa, Expertin und

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

Prüfungsleiterin für Informationssicherheit und Datenschutz, systematisiert das Datenschutzaudit als Prüfung der Ordnungsmäßigkeit und Wirksamkeit der organisatorischen und technischen Maßnahmen gemäß den Vorgaben in der Anlage zu § 9 des Bundesdatenschutzgesetzes (BDSG) durch die Interne Revision. Investigationen als originäre Aufgabe der Revision werden heute zunehmend an spezialisierte Kanzleien und Drittanbieter delegiert. Der Revision kann jedoch im Rahmen einer Unterschlagungsprüfung beim konkreten Verdachtsfall 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 Sicherheitsattacken oder Cyberthreats. Ähnlich den Prüfungen der Notallsysteme und insbesondere der Notfallübungen etabliert sich eine neue Prüfungsart, welche die Ordnungsmäßigkeit und Wirksamkeit der kartellrechtlichen Compliance ermöglicht. Mock Down Raids haben sich als eine sinnvolle Ergänzung der Ordnungsmäßigkeitsprüfung des Compliancemanagements gemäß Prüfungsstandard des Instituts der Wirtschaftsprüfer, IDW PS 980, erwiesen.

Sebastian Schrieber, 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. 7 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.

Im letzten Kapitel wird der Versuch unternommen, die Zulässigkeit bzw. die Nichtzulässigkeit von Auswertungen personenbezogener Daten, hier insbesondere der E-Mail-Korrespondenz, anhand der aktuellen Rechtsprechung zu diskutieren. Anstelle des angekündigten Beschäftigtendatenschutzgesetzes wurde im Rahmen der Novellierung des Bundesdatenschutzgesetzes (BDSG) dieses um § 32 über den Beschäftigtendatenschutz ergänzt. Dies, so die Meinung der Experten, führt lediglich dazu, dass viele Aspekte des Umgangs mit personenbezogenen Daten der Mitarbeiter erst durch die Gerichtsurteile/Rechtsprechung explizit geregelt werden. In dem Kapitel erfolgen eine Bestandsaufnahme aktuell bekannter Urteile und eine Einschätzung der Zulässigkeit einer Auswertung anhand verschiedener denkbarer Szenarien.

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.[3]

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: „Worüber lacht ihr denn? Ihr lacht über euch selbst!“

Auszüge aus dem Stück dienen als Motto für die einzelnen Kapitel des Buches. Also Vorlage für die Zitate dient die Ausgabe *Der Revisor* der Reclams Universal-Bibliothek Nr. 837 aus dem Jahr 1996.

[3] Aus dem Kapitel „Zeitdokumente und Entstehung, Aufführung und Rezeption des Revisor“ in: Gogol, N. (1996). *Der Revisio*r. Reclams Universal-Bibliothek Nr. 837. S. 141.

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)

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 muss aber ein gemeinsames Verständnis für die später verwendeten Begriffe und Definitionen erzeugt werden.

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

© Springer Fachmedien Wiesbaden 2015

A. Sowa et al., *IT-Revision, IT-Audit und IT-Compliance*,
DOI 10.1007/978-3-658-02808-4_2

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 Standard Nr. 2 („Prüfung des Risikomanagements durch die Interne Revision“) des Deutschen Instituts für Interne Revision (DIIR) bezieht sich zur Begriffsbestimmung auch auf die eben genannte Gesetzesbegründung.

Im Gesetz über das Kreditwesen (KWG) schreibt der Gesetzgeber in § 25a Abs. 1 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 Anhang V der Bankenrichtlinie [der Europäischen Union] 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). In den MaRisk wird zudem auch die Ausgestaltung einer Internen Revision konkretisiert (vgl. [1]).

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.

2.2 3LoD: Three Lines of Defence

Diese Überlegungen bringen uns direkt zum „Three-Lines-of-Defence“-Modell (3LoD-Modell[1]). Nach derzeit herrschender Meinung (vgl. [3]) verkörpert das 3LoD-Modell die Grundlage für ein funktionierendes Corporate-Governance-System, bestehend aus

- internem Kontrollsystem (1st Line),
- Risikomanagement (2nd Line) und
- Interner 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

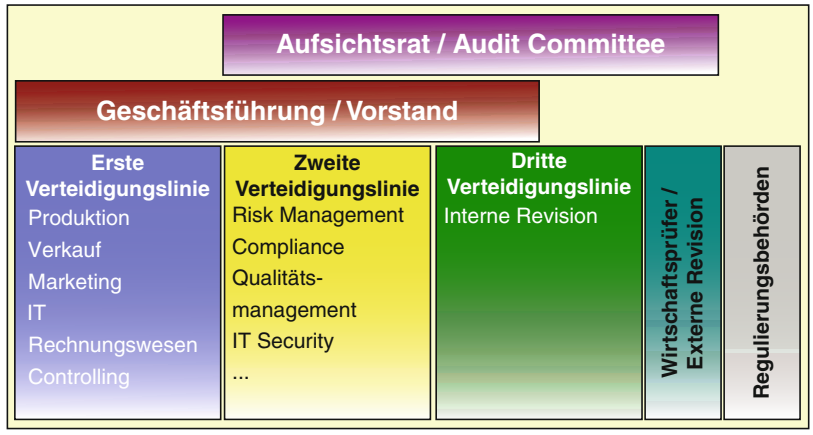

Abb. 2.1 Three-Lines-of-Defence-Modell

[1] Eine gute Zusammenfassung des 3LoD-Modells aus Sicht der IT-Revision bietet auch der Artikel von Ken Doughty (vgl. [2]).

Geschäftsführung regelmäßig unabhängig Bericht erstatten. Insbesondere validiert 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 ist unabhängig von den beiden vorhergehenden und 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 (vgl. [1]). 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) (vgl. [1]). 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 (stetige) Überwachung der Risiken des Unternehmens 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 zweite Verteidigungslinie Abschn. 2.2.

Gemäß dieser Auslegung des Begriffs wird klar, dass die Interne Revision gerade nicht Teil des Monitorings ist. Vielmehr kommt zum Ausdruck, dass sie insbesondere das Monitoring prüfen soll. Die geforderte Unabhängigkeit bedeutet u. a. auch, dass sich die Interne Revision nicht selbst prüfen darf, also nicht selbstreferenziell ist. Dabei wird sprachlich klar zwischen Überwachen/Monitoren und Prüfen getrennt. Ersteres ist, wie zuvor dargelegt, eine stetige, prozessabhängige Tätigkeit. Prüfen als Haupttätigkeitsbereich der Internen Revision findet außerhalb des Monitorings statt und ist daher eben nicht stetig, sondern diskret. In den Begriffen des 3LoD-Modells ist dies die dritte Verteidigungslinie Abschn. 2.2.

Hintergrundinformation
In dem Bereich Informationstechnologie und Informationssicherheit liegen Monitoring und Audit oft sehr nah beieinander.

[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.

Mit dem **Monitoring** ist die permanente Überwachung der Performance der IT, der Informationssicherheit und/oder der Compliance mittels Indikatoren (Metriken) und Reports gemeint. Dabei handelt es sich um die unmittelbare und systematische Erfassung, Beobachtung bzw. Überwachung eines Prozesses mittels technischer Hilfsmittel oder anderer Beobachtungssysteme (vgl. [4]).

Audit steht hingegen für die periodische Überprüfung der Wirksamkeit der implementierten Kontrollen in der IT.

Gemäß National Institute of Standards and Technology, Special Publication NIST PS 800–14, „Generally Accepted Principles and Practices for Securing Information Technology Systems" wird festgestellt: Je mehr eine Auditaktivität in Echtzeit, also Realtime, erfolgt, desto mehr fällt sie in die Kategorie „Monitoring". Dementsprechend wird Audit als eine einmalige oder periodische Bewertung bzw. Prüfung definiert, während sich Monitoring auf eine fortlaufende Aktivität bezieht, die die Überprüfung von Systemen oder ihrer Nutzer zum Ziel hat (vgl. [5]).

2.5 Exkurs: Jahresabschlussprüfung

Der Fokus des Buches liegt zwar auf der (Internen) IT-Revision. Gleichwohl lohnt sich der Blick über den Tellerrand auf die Wirtschaftsprüfung. Nach § 317 Abs. 4 Handelsgesetzbuch (HGB) ist der Wirtschaftsprüfer verpflichtet, die Funktionsfähigkeit des Überwachungssystems nach § 91 Abs. 2 AktG und dabei insbesondere auch die Funktionsfähigkeit der Internen Revision zu beurteilen. Dies gilt zwar laut Gesetz nur für Aktiengesellschaften, jedoch kann man die bereits erwähnte Ausstrahlungswirkung der Regelungen im Aktiengesetz auf diese Regelung erweitern.

Damit wird es natürlich interessant, die Beurteilungsmaßstäbe der Wirtschaftsprüfer genauer zu betrachten. Zum einen die Maßstäbe zur Beurteilung der Internen Revision selbst, aber auch die Maßstäbe zur Beurteilung der restlichen Unternehmung (erste und zweite Verteidigungslinie der 3LoD Abschn. 2.2). Diese haben sicherlich auch eine Wirkung auf die Beurteilung der Prüfungstätigkeit und der Beurteilungen der Internen Revision. Die bereits genannte EU-Richtlinie 2006/43/EC verpflichtet den Wirtschaftsprüfer, die Jahresabschlussprüfung unter Verwendung nationaler oder internationaler Prüfungsstandards durchzuführen.

EU-Richtlinie 2006/43/EC, Artikel 26, Abs. 2

„Die Mitgliedstaaten verpflichten die Abschlussprüfer und Prüfungsgesellschaften, Abschlussprüfungen unter Beachtung der von der Kommission nach dem in Artikel 48 Absatz 2 genannten Verfahren angenommenen internationalen Prüfungsstandards durchzuführen. Die Mitgliedstaaten können einen nationalen Prüfungsstandard so lange anwenden, wie die Kommission keinen internationalen Prüfungsstandard, der für denselben Bereich gilt, angenommen hat."

Für Deutschland sind dies die Prüfungsstandards des Instituts der Wirtschaftsprüfer in Deutschland e. V. (IDW), die sich stark an die internationalen Prüfungsstandards, nämlich den „International Standards on Auditing (ISA)" des International Auditing and Assurance Standards Board (IAASB) anlehnen.

Interessant sind u. a. die Prüfungsstandards:

- „Interne Revision und Abschlussprüfung (IDW PS 321)“,
- „Abschlussprüfung bei Einsatz von Informationstechnologie (IDW PS 330)“;
- „Die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB (IDW PS 340)“ und über die Ausstrahlungswirkung über das Finanzgewerbe hinaus auch noch
- „Die Beurteilung des Risikomanagements von Kreditinstituten im Rahmen der Abschlussprüfung (IDW PS 525)“.

Vor allen Dingen die letzten drei genannten Prüfungsstandards bilden durch die Verpflichtung ihrer Anwendung durch den Wirtschaftsprüfer eine gute Grundlage für die Arbeit der Internen Revision, auf die wir später noch zurückgreifen werden.

2.6 Continuous Auditing

Bereits in den 1980er-Jahren waren weitgehend alle Geschäftsprozesse größerer Unternehmen computerunterstützt. Die Revision, intern und extern, war zu dieser Zeit noch hauptsächlich finanzorientiert und technisch oft nicht auf dem gleichen Stand wie die geschäftstreibenden Unternehmensbereiche. Das hatte vor allen Dingen den Grund, dass bis in die 1990er-Jahre hinein Revision rein rückblickend (wie der Name auch sagt: Re – zurück, Vision – Sicht) tätig war. Für die Beurteilung der finanziellen Daten eines Unternehmens einerseits und die Aufdeckung unerlaubter Handlungen andererseits ist dies auch völlig ausreichend.

Ausgehend von den USA rückte eine Reihe von Unternehmensskandalen zu Anfang dieses Jahrtausends die Corporate Governance, also das System der Unternehmensführung, in den Fokus der Gesetzgeber (zur weiteren Lektüre z. B. [6] und [7]). In den USA kam dies durch den Sarbanes-Oxley-Act (SOX) [8] bereits 2002 zur Geltung und in Europa letztendlich durch die 8. EU-Direktive (2006/43/EC) 2006, die hier nun bereits zum dritten Mal erwähnt wird. In diesen Regelwerken wird das Augenmerk verstärkt auf das Management und dessen Verantwortung für das interne Überwachungssystem gelegt. Des Weiteren wird besonders die unabhängige Prüfung dieser Verantwortung hervorgehoben. Spätestens seitdem diese gesetzlichen Anforderungen eingeführt wurden, ist klar, dass sich die Externe und Interne Revision nicht mehr auf die Prüfung allein der finanziellen Situation beschränken können. Diese Entwicklung setzte tatsächlich schon früher ein, wie man auch an der Entwicklung der verschiedenen Standards der Verbände für Interne Revision und IT-Revision erkennen kann (Beispiele: Institute for Internal Auditors [IIA] mit den „Professional Standards for Internal Auditing“ und ISACA mit den „Control Objectives for Information and related Technology, CObIT“).

Mit dieser Entwicklung rückte auch der Begriff des Continuous Auditing mehr und mehr in den Vordergrund. Eine Methode mit dieser Bezeichnung wurde bereits 1989 bei AT & T Bell Laboratories eingesetzt (vgl. [9]) und diente der Überwachung und Prüfung