

Handbücher der Revisionspraxis

Band 1

Herausgeber

Prof. Dr. Volker H. Peemöller und
Joachim Kregel

Grundlagen der Internen Revision

Standards, Aufbau und Führung

Von
Prof. Dr. Volker H. Peemöller
und
Joachim Kregel

3., neu bearbeitete Auflage

ERICH SCHMIDT VERLAG

Bibliografische Information der Deutschen Nationalbibliothek

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

Weitere Informationen zu diesem Titel finden Sie im Internet unter

ESV.info/978-3-503-20088-7

1. Auflage 2010
2. Auflage 2014
3. Auflage 2022

Gedrucktes Werk: ISBN 978-3-503-20088-7

eBook: ISBN 978-3-503-20089-4

ISSN 1867 6146

Alle Rechte vorbehalten

© Erich Schmidt Verlag GmbH & Co. KG, Berlin 2022

www.ESV.info

Dieses Papier erfüllt die Frankfurter Forderungen der Deutschen Bibliothek und der Gesellschaft für das Buch bezüglich der Alterungsbeständigkeit und entspricht sowohl den strengen Bestimmungen der US Norm Ansi/Niso Z 39.48-1992 als auch der ISO-Norm 9706.

Satz: L101 Mediengestaltung, Fürstenwalde
Druck und Bindung: Kösel, Altusried-Krugzell

Geleitwort

Die Interne Revision ist inzwischen ein zentraler Bestandteil der Corporate Governance im Unternehmen geworden und erfährt im Wirtschaftsleben eine kontinuierliche Aufwertung.

Im § 107, Abs. 3 Satz 2 AktG wird vom Prüfungsausschuss verlangt, dass er sich mit der Wirksamkeit des Internen Revisionssystems beschäftigt. § 25a KWG und § 64a VAG verlangen seit längerem die Einrichtung einer Internen Revision. Die BaFin geht in den MaRisk sehr intensiv und detailliert auf die Aufgabenstellung der Internen Revision ein. Auch für öffentliche Unternehmen ergibt sich aus § 53, Abs. 1 Ziffer 1 des Haushaltsgrundsätzegesetz mittelbar die Notwendigkeit der Einrichtung eines Internen Revisionssystems.

Aber nicht nur die gesetzliche Verankerung führt zu einem verstärkten Fokus auf die Interne Revision, sondern auch die Aus- und Weiterbildung. Dieser Trend schlägt sich nieder in der Hochschulausbildung, sowie der berufsbegleitenden Ausbildung zum CIA mit einer 15-jährigen Erfolgsgeschichte in Deutschland sowie mit der relativ neuen Ausbildung zum Internen Revisor^{DIIR}, die ebenfalls sehr gut angenommen wird.

Diese Entwicklung fußt maßgeblich auf den Internationalen Grundlagen für die berufliche Praxis, die vom IIA und dem DIIR veröffentlicht wurden und zu einer Festigung des Berufsbildes beigetragen haben. Sie bilden einen Kristallisationspunkt des Berufsstands, der für High Potentials immer attraktiver wird, denn in der heutigen Zeit und unter den heutigen Gegebenheiten sind viele Vorteile für die persönliche Karriere erkennbar. In Deutschland wird die Entwicklung der Internen Revision getragen und vorangetrieben durch das DIIR, das gerade wieder in seinem Kongress in Dresden 2013 mit rund 830 Teilnehmern einen kraftvollen Akzent gesetzt hat.

Mit der verstärkten Wahrnehmung in der Öffentlichkeit sind auch weitere Anforderungen an die Berufsträger verbunden. Die Kenntnis der gesetzlichen Vorschriften, der Standards der Berufsausbildung, der Prozesse und Geschäftsmodelle im Unternehmen sind nur einige Aspekte, die von den Angehörigen des Berufsstandes beherrscht werden müssen.

Diese umfangreiche Palette anspruchsvoller Aufgaben kann ein einzelnes Lehrbuch kaum erschöpfend behandeln. Mit der vorliegenden, neu bearbeiteten zweiten Auflage des ersten Bandes einer umfassenden Buchreihe setzen die Autoren Volker H. Peemöller und Joachim Kregel eine Publikationsreihe für die Praxis und die Ausbildung der Internen Revision fort, die wir, das Deutsche Institut für Interne Revision, begrüßen und mit Interesse begleiten.

Frankfurt am Main, Oktober 2013

Bernd Schartmann, CIA, CRMA

Sprecher des Vorstands, Deutsches Institut für Interne Revision e. V.

Executive Vice President, Corporate Internal Audit & Security, Deutsche Post DHL

Vorwort zur dritten Auflage

Die Autoren freuen sich, mit dieser dritten Auflage die Erfolgsgeschichte des Grundlagenbuchs weiter schreiben zu dürfen. Das Buch wendet sich weiter an Einsteiger in die Interne Revision und will ihnen Grundlagenwissen vermitteln. Auch für das CIA-Examen und die Prüfung zum Internen Revisor DIIR soll es seinen Beitrag leisten. Letztlich dient es dem erfahrenen Praktiker als Nachschlagewerk, um bestimmte Themen vertiefen zu können.

Auch in der Internen Revision hat sich seit 2013 eine Menge getan.

Zu nennen sind hier die Abschlussprüfer-Verordnung der EU von 2014, die u. a. klarstellt, dass Abschlussprüfung und Interne Revisionsleistungen nicht von ein und derselben Organisation für dasselbe Unternehmen erbracht werden dürfen. Die Änderungen im Zuge des Wirecard-Skandals bei den öffentlichen und privaten Prüforganisationen EBA, BaFin/DPR und APAS sind momentan in 3/2021 nicht ganz absehbar. Es wird jedoch auf einige Verschärfungen und Klarstellungen von Ausnahmeregelungen hinauslaufen.

Das IIA hat mit den IPPF ab 2019 ein wenig Ordnung in die praktischen Hinweise gebracht. Wiewohl die verpflichtenden Grundsätze mit dem Code of Ethics und den Standards im Wesentlichen gleichgeblieben sind, wird zukünftig unterschieden in Implementing Guidance, Supplementing Guidance und Positions Papers. Während die Implementing Guidance die Standards näher erläutern, geben die Supplementing Guidance Hilfestellung bei der Weiterentwicklung der Internen Revision (General und IA Strategy Best Practises), die GTAG streben dasselbe Ziel im IT-Bereich an.

Das international sehr bedeutsame Rahmenwerk COSO ERM hat sich 2017 neu strukturiert. Der Teil Internal Control wurde als separates Rahmenwerk aus ERM herausgelöst, ERM selbst erhebt den Anspruch, in allen Managementprozessen eines Unternehmens anwendbar zu sein und nicht nur als „5. Rad am Unternehmenswagen“ den Risikoaspekt einzubringen. Vielmehr soll schon bei der Unternehmenskultur (Risikoappetit des Unternehmens geprägt durch die Unternehmensspitze) angesetzt werden, auch die Strategieformulierung kommt zukünftig ohne gleichzeitige Risikoszenarien nicht mehr aus.

Insgesamt hat CoViD 19 uns alle einem Stresstest unterzogen, inwieweit die Unternehmensprozesse und die Unternehmensorganisation resilient, also widerstandsfähig ist oder inwieweit aus operativer Optimierung heraus Klumpenrisiken in Kauf genommen wurden. Es wäre uns allen zu wünschen, wenn bei Erscheinen dieser Neuauflage dieses Thema mehr oder weniger ein Thema der Vergangenheitsbewältigung geworden ist.

Das Prüfungsspektrum der Internen Revision dürfte sich in den nächsten Jahren bedingt durch die ESG-Berichtspflichten der großen Kapitalgesellschaften und das Lieferkettengesetz erweitern. Sind durch US-GAAP und IFRS im finanziellen Berichtserstattungsteil die Normen klar festgelegt, so muss sich die Standardisierung der ESG-Normen erst noch durchsetzen. Klar ist, dass Unternehmen ihre Anstrengungen

zu den Bereichen Umweltschutz, Mitarbeiterbelange und Corporate Governance vergrößern werden. Die Anforderungen an Zertifizierungen dieser gemachten Anstrengungen werden wachsen und last, but not least die Interne Revision wird von der Unternehmensführung beauftragt werden, zu unterstützen. Sie wird ihren Beitrag leisten, dass interne und externe Normen von ESG auch tatsächlich in der Praxis dann gelebt werden.

Die Professionalisierung wird ebenfalls weitergehen. Der Bereich IT wird zunehmend nicht nur wie in der Vergangenheit Prüfungsgegenstand sein, um als Third Line of Defense das Unternehmen u. a. vor Cyberangriffen zu schützen, die IT wird im Sinne von Continuous Auditing in eine IR Data Base kontinuierlich „Ereignisse einspeisen“, die ganz im Sinne von Soll-Ist-Abweichungen vorab als berichtenswert qualifiziert wurden und so dann eine noch fundiertere Basis für Prüfungen darstellen.

Die letzt verfügbare Enquete hat u. a. deutlich gemacht, dass der Prozentsatz externer Validierungen durch Assessments noch stark steigerbar ist. Die Autoren wünschen hier ihren Kollegen Mut, diesen Weg weiter zu beschreiten. Das DIIR steht hier mit einer Vielzahl von Angeboten zur Hilfe und Schulung gerne zur Verfügung. Letztendlich hilft eine externe Zertifizierung im Sinne eines kontinuierlichen Verbesserungsprozesses dem Zertifizierten ähnlich weiter wie auch er seine Unternehmens-Kollegen mit seiner Revisionstätigkeit tatkräftig unterstützen möchte.

Die Autoren, Juni 2021

*Volker H. Peemöller
Nürnberg*

*Joachim Kregel
Köln*

Vorwort zur zweiten Auflage

Vom Erfolg der ersten Auflage ein klein wenig überrascht, freuen sich die Autoren, dem Leser nun in der zweiten, neu bearbeiteten Auflage ein Buch vorzustellen, das sich als Nachschlagewerk in der Praxis weiter bewähren wird und Einsteigern in die Interne Revision kompakt das Grundlagenwissen vermitteln hilft.

Seit der ersten Auflage ist viel Positives in Richtung Interne Revision bewegt worden. Der Gesetzgeber hat im § 107 des Aktiengesetzes dem Prüfungsausschuss aufgetragen, das System der Internen Revision (IRS) zusätzlich zum System der Internal Controls und des Risikomanagements einer Beurteilung auf Zweckmäßigkeit und Funktionsfähigkeit zu unterziehen. Der Deutsche Juristentag hat 2012 dieses Thema zum Anlass genommen, eine breite Diskussion darüber zu führen, inwieweit sich der Prüfungsausschuss als Teil des Aufsichtsrats ein unabhängiges Urteil über das IRS im dualen System der Unternehmensüberwachung bilden kann. Denn er ist darauf angewiesen, dass der zuständige Vorstand dem Revisionsleiter offenes Rederecht einräumt, und zwar auch, ohne dass er als zuständiger Vorstand selbst zugegen ist. Ob sich hier gelebte gute Praxis gegen die Theorie einer grundsätzlich nicht unabhängigen Internen Revision, soweit sie funktional und disziplinarisch an einen Vorstand berichtet, durchsetzt, bleibt abzuwarten.

Auch die BaFin hat in ihren MaRisk die Rolle der Internen Revision weiter gestärkt.

Inzwischen gibt es auch das Three-Lines-of-Defense-Modell, das jedem Dritten eindrucksvoll die Bedeutung der Internen Revision in der letzten, d. h. dritten Verteidigungslinie zeigt. Jedoch besteht eine Tendenz in kleineren und mittleren Unternehmen, die Interne Revision mit Teilen der zweiten zusätzlich zur dritten Linie zu betrauen, also z. B. Compliance- und Risikomanagement. Die Unabhängigkeit des Urteils ist nur dann nicht gefährdet, wenn die Interne Revision in einer derartigen Zuständigkeit die Prüfung des Compliance- und des Risikomanagementsystems durch Dritte durchführen lässt.

Auch die Entwicklung auf dem Markt für hochkomplexe Software wie GRC (Governance, Risk Management und Compliance) hat die Tendenz in angloamerikanischen Unternehmen aufgegriffen, das Aufsichtsgremium integriert und einheitlich informieren zu lassen. Dokumentation von Kontrollen inkl. deren täglicher Anwendung, Reportingtools, SoD (Segregation of Duties)-Themen und Regulierungsthemen sind hier meist in einem Tool integriert. Für die Interne Revision ist manchmal auch eine Prozessunterstützung des Revisionsprozesses vorhanden. Auch hier bleibt abzuwarten, ob sich die Vereinheitlichung gegen die „Funktionstrennung in drei Linien“ durchsetzen wird.

Die Gruppe „Cauers“ hat sich inzwischen die Mühe gemacht, den Leitfaden zum 3. Revisionsstandard QA (Quality Assessment) zu überarbeiten. Die aktualisierte Version aus 2012 ist in die Aktualisierung dieses Buchs mit eingeflossen. Mutig finden es die Autoren, dass mit neuem Selbstbewusstsein gefordert wird, die Personalausstattung der Internen Revision im Hinblick auf ihre Aufgaben und die Risikosituation auf Ange-

messenheit zu überprüfen. Es ist als neues, sechstes K.o.-Kriterium bei einem externen QA bestimmt worden. Eine externe Beurteilung auf Nicht-Angemessenheit der Personalausstattung führt also automatisch zur Nicht-Zertifizierung beim QA. Auch hier wird die Zukunft entscheiden, wie weise Revisionsleiter und Externe Assessoren mit diesem neuen „Tool(Schwert)“ umgehen werden, um die Qualität und nicht nur die Quantität der IR zu verbessern.

Die Wertediskussion in den Unternehmen verbunden mit dem Code of Ethics hat ein altes Thema wieder mehr in den Vordergrund geschoben, nämlich den kompletten Menschen in seinem Erleben und seinem Verhalten, und nicht nur den rationalen Teil, den homo oeconomicus, zu betrachten, Stichwort Revisionspsychologie. Der Leser findet zu diesem Thema in den Kapiteln 3, 6, 7, 9 und 10 gezielte Hinweise. Fast immer geht es um das Verhalten von Menschen, ob nun im Kapitel 3, in dem die Verhaltensgrundsätze eingehend besprochen werden, oder im Kapitel 6, in dem das Thema Wertewandel praxisnah veranschaulicht wird. Kapitel 7 beschäftigt sich u. a. mit der Rolle des Revisors und der des Revisionsleiters, mit den Erwartungen und den Voraussetzungen, die in ein ideales Jobprofil münden, mit der Mitarbeiterbefragung anhand von TRI:M des Instituts tns-infratest sowie mit den 4 Intelligenzen des Menschen. Im Kapitel 9 sind Hintergründe einer „quadratischen“ Kommunikation am Beispiel des Eröffnungsgesprächs einer Prüfung erläutert. Kapitel 10 geht ausführlich auf die Revisionspsychologie im Rahmen eines Schlussgesprächs ein und veranschaulicht anhand des sozialpsychologischen Modells TZI (Themenzentrierte Interaktion), wie sich scheinbar ohne Anlass Barrieren, Hemmnisse aufbauen und gibt Hilfen, wie man vermeidet, in solche Situationen hinein zu geraten und wie man sich im worst case wieder daraus „befreien“ kann.

Beide Autoren hoffen und wünschen dem Leser, dass er auf möglichst viele Fragen Hinweise findet, um selbst zu den richtigen Antworten zu gelangen. Das Buch möge dazu beitragen, die Qualität und Akzeptanz der Internen Revision innerhalb und außerhalb der Unternehmen und Organisationen nachhaltig zu steigern.

Die Autoren, Oktober 2013

*Volker H. Peemöller
Nürnberg*

*Joachim Kregel
Köln*

Vorwort zur ersten Auflage

Die Verfasser freuen sich, dem interessierten Leser zum ersten Mal in Deutschland eine Buchreihe vorstellen zu können, die von der Praxis für die Praxis der Internen Revision entwickelt wurde.

Der erste jetzt vorliegende Band enthält die Grundlagen der Arbeit der Internen Revision.

Ausgehend von einer Analyse der Überwachungsaufgaben eines Unternehmens wird insbesondere den Entscheidern an der Unternehmensspitze eine Hilfe geboten, welche Kriterien notwendig sind, den Aufbau und Ausbau der Internen Revision voranzutreiben. Gerade kleine und mittlere Unternehmen erfahren, wie sie kostengünstig, z. B. durch Pooling der Internen Revision, die Prüfungsaufgabe organisieren können.

Weiter werden, beginnend mit der klassischen Prüfungsfunktion, Ziele und Aufgaben diskutiert, die zu einer modernen, zukunftsgerichteten Revisionsfunktion gehören. Die Aufgaben Beratung und Innovation werden in die Diskussion eingebracht, weil sie nach Auffassung der Autoren in besonderem Maße eine Unterstützungsfunktion für das Top Management darstellen. Parallel dazu wird besonderer Wert auch auf Tätigkeitsfelder gelegt, die die Unabhängigkeit der Internen Revision gefährden können. Insgesamt bleiben mit den Aufgabengebieten Financial, Operational, Management Auditing und Compliance genügend Gestaltungsräume für eine wertschaffende und werterhaltende prüferische Tätigkeit.

Einen breiten Raum nimmt dann die Ethikdiskussion ein, die nach der Vielzahl der Unternehmensskandale jetzt auch in den Unternehmen zu einer neuen Ausrichtung auf akzeptierte Werte geführt hat. Die Interne Revision hat ja ihren Code of Ethics schon seit langem als Basis ihres Handelns verabschiedet. Sie kann daher in Unternehmen quasi eine Leuchtturmfunktion bilden.

Eine fundierte Analyse der nationalen und internationalen Richtlinien und Regelungen, die gerade in 2008 und 2009 mit vielen neuen Anforderungen aufwarten konnten, bilden das Fundament dieses Buches. Sie werden dann herangezogen, wenn es zum Verständnis der entsprechenden Inhalte notwendig erscheint, jedoch immer im Bezug zur Praxis. Insbesondere das Verständnis der Rahmenkonzepte Corporate Governance, Internal Control und Risk Management wird durch eine ausführliche Erläuterung anhand der IIA-Standards verdeutlicht. Auch das Zusammenspiel dieser Rahmenwerke im Rahmen von COSO ERM wird dargestellt, um dem Leser einen praktischen Leitfaden zu vermitteln.

Die Prozesswelt hat seit einiger Zeit Einzug in den Revisionsalltag gehalten. Deshalb nimmt die Diskussion der Kernprozesse

- Risikoorientierte Revisionsplanung,
- Revisionsobjektplanung, Vor-Ort-Arbeiten und
- Berichterstattung mit Follow-up

einen breiten Raum ein. Das zunehmend eingeforderte Qualitätsmanagement macht auch vor den Toren der Internen Revision nicht Halt. Anhand der Standards zeigen die

Autoren, welche Faktoren für eine effektive und ordnungsgemäße Revisionsarbeit notwendig sind. In diesem Zusammenhang werden auch die 5 K.O.-Kriterien besprochen, deren Beachtung für eine Zertifizierung unbedingt erforderlich ist. In den Best Practices werden darauf aufbauend viele Hinweise gegeben, wie die Arbeit kontinuierlich verbessert werden kann. Ein Revisionsleiter erhält also über die geforderten Standards hinaus wertvolle Anregungen, wie und in welchen Themenbereichen er seine Abteilung in Richtung Best-in-Class weiterentwickeln kann.

Das frühere „Angst“-Thema Outsourcing und Teiloutsourcing wird plakativ und aktuell dargestellt. Hier geht es im Wesentlichen um die Themen Fachkompetenz, Komplexität und Größe des Unternehmens, die die Mitarbeiterzahl und Ausrichtung der Internen Revision gerade in kleineren und mittleren Unternehmen bestimmen. Anhand dieser Kriterien kann dann sehr nüchtern ein möglicher Sourcingbedarf ermittelt werden.

Die Themen Risikomanagement und Risikofrühwarnsysteme schärfen den Blick des Lesers für Indikatoren, die substantiellen Problemen vorangehen können. Sie bieten anhand der vorgestellten Risikokataloge eine Fülle von Material, die richtigen Dinge zu tun. Die Herausforderung in der Revisionsplanung, die in der gleichzeitigen Forderung „Keine revisionsfreien Räume“ und „Fokussierung auf substanzgefährdende Risiken“ besteht, wird ausführlich besprochen.

Die Diskussion der Führungsprozesse der Internen Revision kommt auch nicht zu kurz. Es werden die organisatorischen Voraussetzungen der Internen Revision beschrieben und mögliche Strategieansätze thematisiert.

Die zunehmende Internationalisierung der Unternehmen, der gerade in der Wirtschaftskrise verschärfte Kostendruck und die erforderliche Spezialisierung und Fokussierung bleibt nicht ohne Folgen für die Ausrichtung der Internen Revision. Mit dem Versuch einer Antwort auf die Frage „Generalist oder Spezialist“ wird hierzu ein Weg aufgezeigt.

Die Forderung nach besserer Überwachung in den Unternehmen, wie z. B. in der 8. EU-Richtlinie gefordert, hat zu einem Trend geführt, Prüfungsausschüsse oder Audit Committees einzurichten und professionell auszugestalten. Wie sich hier die Interne Revision aufstellen kann, wird anhand der monalen und dualen Unternehmensverfassungen diskutiert.

Zur zunehmenden Professionalisierung der Internen Revision gehört inzwischen mehr als ein nur theoretisches Verständnis für die IT. Die Erleichterung der Arbeit mit IT und die Prüfung von IT gehören inzwischen zum Rüstzeug eines Revisors. Es werden deshalb einige Empfehlungen zum internen Gebrauch von IT als Unterstützung aller Prozesse der Internen Revision, zum Nutzen der IT als Prüfungstool und der IT als eigener Prüfungsgegenstand im Rahmen der Diskussion von Kontrollen gegeben.

Gespickt mit zahlreichen Beispielen, Abbildungen und Grafiken werden aktuelle Informationen aus dem Revisionsalltag, die Ihre Arbeit erleichtern sollen, vorgestellt. Zusammen mit

- den umfangreichen Checklisten des Anhangs,
- den ins Deutsche übersetzten IIA-Standards,

- den 81 Fragen des deutschen Leitfadens des Quality Assessments und
- den Best Practices aus dem internationalen Bereich (GAIN: Global Auditor Information Network) und dem nationalen Bereich

werden Ratschläge und Hintergrundinformationen für fast jede kritische Situation im Revisionsalltag angeboten. Ein umfangreiches Glossar rundet den Band ab.

Die neuen IIA-Standards, die Anfang 2009 veröffentlicht wurden, sind in die entsprechenden Abschnitte des Buches eingearbeitet worden. Sie erhöhen durch das oligatorische „must“ statt früher „should“ den Grad der Verbindlichkeit. Viele Definitionen von Begrifflichkeiten sind jetzt in die Standards integriert worden. Dies soll die Lesbarkeit und das Sachverständnis erhöhen.

In 2008 wurde eine Befragung der Revisionsleiter in Deutschland, Österreich und der Schweiz durchgeführt und in 2009 veröffentlicht. Die Ergebnisse sind jeweils in den entsprechenden Kapiteln summarisch berücksichtigt worden. Ziele und Aufgaben der IR sind im Vergleich zu früheren Befragungen in etwa stabil geblieben. Jedoch ist eine Tendenz zu stärkerer Risikoorientierung und Prüfung der Geschäftsprozesse festzustellen.

Unterschiede in der Ausrichtung der Arbeit ergeben sich je nach Zuordnungs-Cluster des eigenen Unternehmens in Industrie, Dienstleistungen, Banken und öffentlichen Institutionen.

Auch die dazugehörigen Practical Advisories (PA) sind, soweit sie bis Juli 2009 überarbeitet und veröffentlicht wurden, berücksichtigt worden. Im Zuge der Neuausrichtung der Veröffentlichungspraxis des IIA muss hier festgestellt werden, dass sich die noch heute gültigen PA gegenüber dem letzten Jahr mehr als halbiert haben. Der Grund ist in der stärkeren Verbindlichkeit der heute gültigen PA zu sehen. Das hat natürlich zur Folge, dass wertvolle Praxistipps der anderen, heute nicht mehr verbindlichen PA aus dem Blickfeld verschwinden könnten.

Auch für die neue MA (Mindestanforderung) Risk (Risikomanagement) der BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht), die am 14.8.2009 veröffentlicht wurde, wurde in die entsprechenden Kapitel Erläuterungen mit aufgenommen. Herauszustellen ist die Berichtspflicht der IR (Interne Revision) an den AR (Aufsichtsrat)-Vorsitzenden oder Vorsitzenden des Prüfungsausschusses, die die Unabhängigkeit der IR stärken sollte. Auch die Prüfungsplanung kann jetzt noch risikoorientierter angesetzt werden, da die starre Regel der 3 Jahre für alle Elemente eines Audit Universe abgemildert wurde.

Die Buchreihe gliedert sich zunächst in den jetzt vorliegenden Einführungsband „Grundlagen der Internen Revision“ und in vier weitere Bände „Financial Auditing (FA)“, „Operational Auditing (OA)“, „Compliance (CO)“ und „Management Auditing (MA)“. Die Herausgeber wollen dem interessierten Leser für die jeweiligen Fachgebiete in der IR vertiefte Einblicke in das Revisionsgeschäft geben.

Die Autoren bedanken sich bei dem DIIR (Deutsches Institut für Interne Revision e. V.), dem IIA (Institute for Internal Auditors) und dem IIA Austria für die gute Unterstützung, insbesondere für die freundlichen Genehmigungen, die neuen IIA-Standards und die 81 Fragen des QA (Quality Assessment) abdrucken zu dürfen.

Ein herzlicher Dank geht an den Vorstand des DIIR, ohne dessen Unterstützung der Erfolg dieser Buchreihe nicht denkbar wäre, an eine Vielzahl von Kollegen und Mitarbeitern, die wertvolle praxisorientierte Hinweise zur Verbesserung der Buchreihe gegeben haben und dem Erich Schmidt Verlag, ohne dessen Weitblick dieses Werk nie einem breiten Fachpublikum zugänglich gemacht werden könnte.

Insbesondere sei Dank ausgesprochen Frau Inge Molkenthin, Frau Alessandra Kregel und Herrn Winfried Schnitzler, die substantiell durch ihre vielfältigen Anregungen und Verbesserungsvorschläge zum Gelingen eines lesbaren und verständlichen Buches beigetragen haben.

Diese Buchreihe wird dem interessierten Leser aus der Internen und Externen Revision, dem Management und den Aufsichtsorganen der Unternehmen ein täglicher Ratgeber in Fragen rund um die Interne Revision sein. Vorstände, Geschäftsführer und Aufsichtsorgane, die zurzeit noch überlegen, eine Interne Revision einzurichten, erhalten praktische Entscheidungshilfen.

Revisoren, die anstreben, das CIA-Examen abzulegen, gibt das Buch wertvolle praktische Hinweise und ein umfassendes theoretisches Gerüst. Auch den Studierenden und den Lehrenden wird diese Buchreihe empfohlen, enthält sie doch durch ihr umfangreiches Praxiswissen, dokumentiert im Textteil und dem ausführlichen Anhang, genügend Ansatzpunkte für weitere Forschungsarbeiten und Ausarbeitungen für die theoretische Basis der Internen Revision.

Möge der Vergleich eines CEO einer ausländischen Tochtergesellschaft allen Revisoren nachhaltig in den Ohren klingen: CEO und Revisor haben ähnlich hohe Freiheitsgrade in ihrer täglichen Arbeit, sodass es ein ganzes Arbeitsleben dauern kann, bis sich ein Arbeitstag wiederholt.

Nutzen wir diese Freiheit zum Wohle unserer Unternehmen!

Autoren

Volker H. Peemöller
Nürnberg

Joachim Kregel
Köln

Inhaltsverzeichnis

Geleitwort	V
Vorwort zur dritten Auflage	VII
Vorwort zur zweiten Auflage	IX
Vorwort zur ersten Auflage	XI
Schnellorientierung	XV
Inhaltsverzeichnis	XXIII
Abbildungsverzeichnis	XXXIII
Tabellenverzeichnis	XXXV
Abkürzungsverzeichnis	XXXVII
1 Gründe für die Einrichtung einer Internen Revision	1
1.1 Prüfungsfunktion im Unternehmen	1
1.2 Prüfung als Aufgabe der Unternehmensführung	2
1.3 Einrichtung einer Internen Revision	3
1.3.1 Voraussetzungen	3
1.3.2 Maßnahmen zur Einführung	6
1.3.3 Interne Revision in der Praxis (Erhebung der Institute)	13
1.3.4 Überwachung der Internen Revision	14
1.4 Ausbildung zum Internen Revisor in Deutschland	15
1.4.1 Das CIA-Examen	15
1.4.2 Interner Revisor ^{DIIR}	17
1.5. Kernthesen	18
2 Abgrenzung der Internen Revision	21
2.1 Definition der Internen Revision nach IIA und DIIR	21
2.2 Ziele und Aufgaben der Internen Revision	22
2.2.1 Ziele der Internen Revision	22
2.2.2 Prüfung als Aufgabe der Internen Revision	23
2.2.3 Vorgehensweise der Prüfung	25
2.2.4 Zeitaspekt der Prüfung	26
2.2.5 Beratung als Aufgabe der Internen Revision	27
2.2.5.1 Ziel der Beratungsfunktion	27
2.2.5.2 Prüfungsnahe Beratung	28
2.2.5.3 Prüfungsunabhängige Beratung	29
2.2.6 Innovation als Aufgabe der Internen Revision	30
2.2.6.1 Begründung der Aufgabe	30
2.2.6.2 Aufgabenstellungen	30
2.2.7 Weitere Aufgaben der Internen Revision	32
2.3 Rechte und Pflichten der Internen Revision	33
2.4 Kernthesen	34

3	Verhaltensgrundsätze (Code of Ethics) der IR	37
3.1	Zielsetzung und Bedeutung des Code of Ethics	37
3.1.1	Inhalt und Bedeutung einer Berufsethik	37
3.1.2	Zielsetzung des Code of Ethics des IIA	38
3.2	Bestandteile des Code of Ehtics	39
3.2.1	Rechtschaffenheit	39
3.2.2	Objektivität	40
3.2.3	Vertraulichkeit	40
3.2.4	Fachkompetenz	41
3.3	Kernthesen	41
4	Standards bzw. Grundsätze des IIA und DIIR	43
4.1	Zweck und Bedeutung der Grundsätze	43
4.2	Attribute Standards	45
4.3	Ausführungsstandards	53
4.4	Kernthesen	61
5	Regelungen zur Internen Revision	63
5.1	Regelungen in Deutschland	63
5.1.1	Einrichtung eines Überwachungssystems nach AktG	63
5.1.2	Einrichtung eines Prüfungsausschusses nach DCGK	65
5.1.3	MaRisk des Bundesamtes für Finanzdienstleistungsaufsicht	68
5.2	Europäische Regelungen	71
5.2.1	8. EU-Richtlinie	71
5.2.2	Umsetzung von Basel III	72
5.3	US-amerikanische Regelungen	74
5.3.1	Foreign Corruption Practices Act	74
5.3.2	Sarbanes Oxley Act (SOX)	76
5.3.2.1	Einleitung	76
5.3.2.2	Sarbanes-Oxley Act von 2002	76
5.3.2.3	Internes Kontrollsystem nach SEC 404	79
5.3.2.4	COSO I als Grundlage des Internal Control des SOX	81
5.3.2.5	Audit Committee (SEC 204, 301, 407 SOX)	82
5.3.2.6	Schutz von Whistle Blowers (SEC. 806, 1107 SOX)	82
5.3.2.7	Aufgaben der Internen Revision im Zusammenhang mit SOX	83
5.3.2.8	Testdurchführung und Berichterstattung über die Ergebnisse des SOX 404	83
5.3.2.9	Schlussbetrachtung	88
5.4	Internationale Initiativen	88
5.4.1	COSO und Risikomanagementsystem	88
5.4.1.1	Auslöser für die Initiativen zum Risikomanagementsystem	88

5.4.1.2	Begründung für die Risikomanagementsysteme	88
5.4.1.3	Bestandteile eines Risikomanagementsystems	89
5.4.1.4	Risikomanagementsystem nach COSO	91
5.4.1.5	Das Risikomanagementsystems nach COSO 2017	95
5.4.1.6	Problembereiche von Risikomanagementsystemen	101
5.4.2	OECD und Corporate Governance	101
5.4.3	Transparency International und Fraud	103
5.5	Kernthesen	104
6	Entwicklungstendenzen der Internen Revision	107
6.1	Entwicklungstendenzen im Unternehmen	107
6.1.1	Wissensmanagement im Unternehmen	107
6.1.2	Flexible Organisation	108
6.1.3	Shareholder Value-Denken	109
6.1.4	Diversity Management	110
6.2	Entwicklungstendenzen im Umfeld des Unternehmen	111
6.2.1	Internationalisierung/Globalisierung	111
6.2.2	Wettbewerbsdruck	112
6.2.3	Wertewandel	113
6.2.4	Technologische Entwicklung	113
6.2.5	Nationale und internationale Regulierung	114
6.2.6	Soziale und politische Konflikte	115
6.3	Die Interne Revision der Zukunft	116
6.4	Kernthesen	117
7	Strategie und Organisation der Internen Revision	119
7.1	Geschäftsordnung/Geschäftsauftrag der IR	119
7.1.1	Die Einbettung der IR im Unternehmen	120
7.1.1.1	Die IR im dualen System von Aufsichtsrat und Vorstand	120
7.1.1.2	Interne Revision und amerikanische Gesetzgebung	122
7.1.1.3	Stellung des Revisionsleiters im Unternehmen	123
7.1.1.4	Rollen und Aufgaben der Internen Revision zu den Leitungsebenen im Unternehmen	126
7.1.2	Ziele und Aufgaben der Revision	127
7.1.3	Informationszugang, -zutritt, -zugriff	135
7.1.4	Berichtspflichten, Verschwiegenheitspflichten, berufsständische Pflichten	136
7.1.5	Budget	138
7.2	Strategie der IR	141
7.2.1	Vision und Mission	141
7.2.2	Der Strategiebegriff	143
7.2.3	Umsetzung des Strategiebegriffs in die IR-Welt	144

7.2.3.1	Wie „wir“ gewinnen	144
7.2.3.2	Was wir sagen	146
7.2.3.3	Was wir können	146
7.2.3.4	Was wir tun	147
7.2.3.5	Kommunikation der Strategie	148
7.2.4	Umsetzung der Strategie: Beispiel Internationalisierung der IR ..	150
7.3	Aufbauorganisation der IR	153
7.3.1	Generelle Ordnungsprinzipien	153
7.3.1.1	Zentral/dezentral	154
7.3.1.2	Zentral/regional	154
7.3.1.3	Funktional/divisional	155
7.3.2	Führungsebenen in der IR	158
7.3.3	Produktive und administrative Zeiten in der IR	159
7.4	Der Mitarbeiter in der IR	161
7.4.1	Berufsrevisor oder Revisor auf Zeit	162
7.4.2	Anforderungsprofil für Revisoren	162
7.4.3	IR als Teil des Führungsnachwuchspools in einem Unternehmen	165
7.4.4	Mitarbeiterbefragung als Start eines mitarbeiterorientierten Dialog in der IR	166
7.4.5	Die Instrumente des mitarbeiterorientierten Prozesses	168
7.4.6	Job Rotation und das Modell Gastrevisor	170
7.5	Der Revisionsleiter	170
7.5.1	Die Anforderungen an einen Revisionsleiter	170
7.5.2	Der Revisionsleiter und sein Umfeld	172
7.5.2.1	Erwartungen des Topmanagements an die IR	172
7.5.2.2	Erwartungen der geprüften Bereiche an die IR	173
7.5.3	Erwartungsdiskrepanzen an die IR zwischen geprüftem Bereich und Unternehmensleitung	174
7.6	Revisionstools zur Unterstützung der Arbeit der IR	176
7.6.1	Anforderungen an ein Revisionstool	176
7.6.2	Standardsoftware für den internen Revisionsprozess	178
7.6.3	Dateianalysertools	181
7.6.4	Continuous Auditing (CA)	183
7.7	Kern-Prozesse der IR	185
7.8	Kernthesen	188
Kapitelanhang 7	190
IIA-Standards	190
DIIR-Standards	199
A: Best Practices GAIN (IIA)	202
B: Best Practices National	203

8 Risikoorientierte Revisionsplanung	205
8.1 Das Audit Universe	205
8.1.1 Funktionsprüfungen	206
8.1.2 Prozessprüfungen	207
8.1.3 Prüfung von Geschäftseinheiten	211
8.1.4 Prüfung von Gesellschaften	212
8.1.5 Projektprüfungen im Unternehmen	213
8.2 Risikoklassifizierungen und Risikomodelle	215
8.2.1 Risiko und Chance	215
8.2.2 Problem-Risiko-Substanzgefährdendes Risiko-Systemrisiko	217
8.2.3 Risikoursache und Risikowirkung	219
8.2.4 Risiko-Faktoren nach COSO II sowie nach DIIR und DRS 20 ..	221
8.2.5 Risikomanagementsysteme	224
8.2.6 Risikofrühwarnsysteme	227
8.3 Risikoklassifizierung im Audit Universe	231
8.3.1 Risikomatrix zur Jahresplanung	231
8.3.2 Risiko revisionsfreier Räume bei Unternehmensteilen geringerer Bedeutung	233
8.4 Informationsquellen für eine risikoorientierte Prüfungsplanung	234
8.4.1 Interne Quellen	234
8.4.2 Externe Quellen	235
8.5 Ideenspeicher: Sammlung von möglichen Handlungsfeldern aus Erkenntnissen von Prüfungen des laufenden Jahres	237
8.5.1 Strategiediskussion	237
8.5.2 Detailplanung möglicher Themen	238
8.6 Einbindung des Top-Managements in die Jahresrevisionsplanung	240
8.6.1 Diskussion von Eckpunkten für die Planung	240
8.6.2 Roadshow	240
8.6.3 Einbindung von Gesamt-Vorstand und Aufsichtsrat	241
8.7 Ressourcenplanung und Teambildungsprozess	242
8.7.1 Planung der internen und externen Ressourcen	242
8.7.2 Teambildungsprozess	243
8.8 IT-Tools zur Unterstützung des Planungsprozesses	246
8.8.1 Informationstool für das Audit Universe: Datenbank	246
8.8.2 Prozessbegleitende Revisionssoftware	247
8.9 Kernthesen	248
Kapitelanhang 8	250
A: IIA Standards	250
B: DIIR Standards	252
C: Best Practices GAIN (IIA)	253
D: Best Practices National	253

9	Revisionsobjekt-(RO)-planung und Prüfungsarbeiten vor Ort	255
9.1	Revisionsobjekt-(RO)-planung	255
9.1.1	Briefing und Vorrecherche möglicher Inhalte	256
9.1.2	Planung von Zeit, Kosten und speziellen Anforderungen des RO	258
9.1.3	Interne Genehmigungsprozesse mit RO-Zielplanung	261
9.2	Prüfungsmethoden	262
9.2.1	Prüfungsverfahren	263
9.2.2	Prüfungszeitraum	266
9.2.3	Prüfungsort	267
9.2.4	Prüfungsart	268
9.2.5	Auswahl der benötigten Informationsquellen	269
9.3	Prüfungsarbeiten vor Ort	270
9.3.1	Anschreiben und Anforderung von vorbereitenden Informationen	272
9.3.2	Das Eröffnungsgespräch	273
9.3.2.1	Emotionale Ebene	274
9.3.2.2	Selbstdarstellung	274
9.3.2.3	Sachebene	275
9.3.2.4	Appell	275
9.4	Schwachstellenanalyse	277
9.4.1	Die sechs Zustände von SOLL und IST	277
9.4.2	Kontrollen	280
9.4.3	Die Ist-Soll-Analyse	285
9.5	Feststellungen	286
9.5.1	α - und β -Fehler: Schlussfolgerungen	286
9.5.2	Abstimmung mit der Fachseite	288
9.6	Verbesserungsvorschläge	289
9.6.1	Verbesserungsvorschläge im FA	291
9.6.2	Verbesserungsvorschläge im OA	292
9.6.3	Verbesserungsvorschläge im CO	294
9.6.4	Verbesserungsvorschläge im MA	296
9.6.5	Generelle Merkmale von Verbesserungsvorschlägen	297
9.7	Dokumentation	297
9.7.1	Formalisierung und Referenzierung	298
9.7.2	Prüfungsdokumentation	298
9.7.3	Berichtsdokumentation	298
9.7.4	Systemdokumentation, Dauerakte/Permanent File und Wissensmanagement	298
9.7.5	Archivierung	299
9.8	Kernthesen	300

Kapitelanhang 9	301
A: IIA Standards	301
B: DIIR Standards	305
C: Best Practices National	306
10 Berichterstattung	307
10.1 Anforderungen an eine professionelle Berichterstattung	307
10.1.1 Detaillierungsgrad von Revisionsinformationen in Abhängigkeit vom Empfänger	308
10.1.2 Zeitnah und aktuell	310
10.1.3 Klar, wahr, konkret und vollständig	311
10.1.4 Objektiv und konstruktiv	313
10.1.5 Schwerpunktsetzung	315
10.2 Prüfungsergebnisse und Maßnahmenempfehlungen zielgruppen- orientiert aufbereiten und berichten	318
10.2.1 Mündliche versus/und schriftliche Berichterstattung im Revisionsprozess	319
10.2.2 Der Kurzbericht	322
10.2.2.1 Das Deckblatt	322
10.2.2.2 Die Zusammenfassung	324
10.2.2.3 Der Maßnahmenkatalog	326
10.2.3 Die Langversion mit Detailbericht und Anlagen	328
10.2.4 Monatsberichte, Jahresberichte und Berichterstattung vor dem Prüfungsausschuss	332
10.2.5 Sonderberichte	333
10.3 Präsentationstechniken	334
10.3.1 Visualisierung	335
10.3.2 Formalanforderungen	337
10.3.3 Techniken	338
10.4 Revisionspsychologie: Revisionsgespräche erfolgreich führen	339
10.4.1 Vorbereitung einer Schlussbesprechung	340
10.4.2 Vorbereitung der Unterlagen	343
10.4.3 Gruppendynamik (TZI: Themenzentrierte Interaktion) in den Schlussbesprechungen	344
10.4.4 Debriefing/Prüfungsnachbereitung	347
10.5 Überwachung von Prüfungsergebnissen	349
10.5.1 Terminüberwachung	350
10.5.2 Eskalationsprozess	351
10.5.3 Follow-Up-Prüfungen	352
10.6 Kernthesen	354

Kapitelanhang 10	356
A. IIA – Standards zur Berichterstattung und zum Follow-Up:	356
B. Auszug aus dem Leitfaden zum DIIR-Standard Nr. 3 „Qualitätsmanagement in der Internen Revision“ zum Thema Berichterstattung, Prüfungsnacharbeit und Follow-Up	360
C: Best Practices GAIN (IIA)	361
D: Best Practices National	361
a. Berichterstattung	361
b. Prüfungsnacharbeit	362
c. Follow-Up	362
11 Qualitätsmanagement in der IR	363
11.1 Qualitätsstandards	363
11.1.1 ISO-Normen	365
11.1.2 DIN-Normen	366
11.1.3 Total Quality Management (TQM)	367
11.1.4 European Foundation on Quality Management (EFQM)	368
11.2 Die IIA-Standards für Qualitätsmanagement in der IR	370
11.2.1 Hintergrund	370
11.2.2 Formen der Zertifizierung	371
11.3 Das deutsche Quality Assessment nach DIIR-Norm	372
11.3.1 Die 6 K.O.-Kriterien	372
11.3.2 Die 11 Hauptkapitel des QA	374
11.3.3 Die Bewertungssystematik	375
11.4 Die Vorbereitung und Durchführung eines QA	376
11.4.1 Vorbereitung eines QA durch den Auftraggeber mittels einer Selbstbewertung	378
11.4.2 Mittlere und größere Revisionsabteilungen/Externes QA	378
11.4.2.1 Strategie	378
11.4.2.2 Planung des QA	379
11.4.2.3 Zusammenstellung des Teams	380
11.4.2.4 Teambildungsprozess im QA-Team	381
11.4.3 Exkurs: Das „360° Feedback“ als Management-Tool im QA-Prozess	381
11.4.4 Selbstbewertung mit externer Validierung	383
11.5 Gemeinsamkeiten und Unterschiede von IIA und DIIR beim Quality Assessment	383
11.6 Kosten und Nutzen eines Qualitätsmanagement in der IR	385
11.7 Kernthesen	386
Kapitelanhang 11	388
A: IIA Standards	388
B: DIIR-Standards	390
C: Best Practices (GAIN)	391

12 Die Interne Revision in ihrer Außenansicht, national und international	393
12.1 Zusammenarbeit der Internen Revision mit verwandten Bereichen	393
12.1.1 Zusammenarbeit mit dem Abschlussprüfer	393
12.1.1.1 Gründe für die Zusammenarbeit zwischen Interner Revision und Abschlussprüfer	393
12.1.1.2 Regelungen zur Zusammenarbeit zwischen Interner Revision und Abschlussprüfer	394
12.1.1.3 Ausprägungen der Zusammenarbeit in der Praxis	397
12.1.2 Zusammenarbeit mit dem Controlling	399
12.1.2.1 Gemeinsamkeiten zwischen Interner Revision und Controlling	399
12.1.2.2 Unterschiede zwischen Interner Revision und Controlling	401
12.1.2.3 Formen der Zusammenarbeit	401
12.1.3 Zusammenarbeit mit den Bereichen Sicherheit/Compliance	404
12.1.4 Zusammenarbeit mit Strafverfolgungsbehörden	406
12.1.5 Zusammenarbeit mit dem Bereich Risikomanagement	411
12.1.5.1 Organisation des Risikomanagements	411
12.1.5.2 Zusammenarbeit mit der Internen Revision	412
12.1.6 Gefüge der Überwachung: Das Three-Lines-of-Defense-Modell/ Das Drei-Linien-Modell.	414
12.2 Branchenspezifische Besonderheiten der IR in Deutschland	417
12.2.1 Interne Revision in Banken und Versicherungen	417
12.2.2 Interne Revision in öffentlichen Unternehmen und Verwaltungen	419
12.2.3 Interne Revision bei den Wirtschaftsprüfungsgesellschaften	422
12.2.4 Interne Revision im Mittelstand	425
12.3 Internationale und nationale Berufsorganisationen der Internen Revision	428
12.3.1 Deutsches Institut für Interne Revision e. V. (DIIR)	428
12.3.2 Institut für Interne Revision Österreich und Schweizerischer Verband für Interne Revision	429
12.3.3 The Institute of Internal Auditors (IIA)	430
12.3.4 European Confederation of Institutes of Internal Auditing (ECIIA)	432
12.4 Kernthesen	433
Ausblick	435
Anhang	437
Literaturverzeichnis	447
Internetlinks: Große Organisationen national und international von A–Z	460
Stichwortverzeichnis	461