ESV ERICH SCHMIDT VERLAG

Handbücher der Revisionspraxis

Band 2

Herausgeber

Prof. Dr. Volker H. Peemöller und
Joachim Kregel

Operational Auditing

Revision von IT, Marketing, Produktion und Einkauf

von

Joachim Kregel

ERICH SCHMIDT VERLAG

Bibliografische Information der Deutschen Nationalibliothek
Die Deutsche Nationalibliothek 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 15466 1

Gedrucktes Werk: ISBN 978 3 503 15466 1
eBook: ISBN 978 3 503 15467 8
ISSN 1867 6146

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: Schwarz auf Weiss, Berlin
Druck und Bindung: Druckerei Strauss, Mörlenbach

Geleitwort der Herausgeber

Die Buchreihe „Handbücher der Revisionspraxis“ wird für die Praxis der Internen Revision geschrieben und entsteht aus der Praxis. Mit dem Operational Auditing liegt nun der zweite Band der Reihe vor, der in die Prüfungspraxis einsteigt. Erstmals wird in einer Publikation die Prüfung der Geschäftsprozesse von Unternehmen geschlossen behandelt. Bislang fanden sich nur kurze Abgrenzungen und theoretische Anmerkungen zum Operational Auditing in der Literatur. Dieser Band konfrontiert den Leser mit der Praxis der Prüfung von Prozessen, die anschaulich aufbereitet und mit einer Fülle von Checklisten hinterlegt sind. Der Autor gibt seinen Erfahrungsschatz in strukturierter und fundierter Form an den Leser weiter.

Erfreulicherweise ist die Interne Revision in letzter Zeit häufig Gegenstand von Publikationen, insbesondere auch von Dissertationen. Damit zeigt sich, dass die Interne Revision verstärkt Eingang in die wissenschaftliche Literatur gefunden hat. Was aber nach wie vor als Veröffentlichung fehlt, ist die praktische, anwendungsbezogene Sicht der Arbeit der Internen Revision. Dies ist nun mit diesem Werk gelungen. Das COSO Enterprise Risk Model bildet die Basis der Beschreibung der Prüfungen. Ausgangspunkt für die Geschäftsprozesse ist das generische Prozessmodell mit Marketing-, Kern- und Supportprozessen. Damit wird sehr anschaulich die Neuausrichtung der Internen Revision in der heutigen Zeit vorgestellt. In den einzelnen Passagen seiner Ausführungen macht der Verfasser die veränderten Anforderungen im Umfeld der Internen Revision deutlich. Breiten Raum im Rahmen dieser Arbeit nimmt Marketing und Marketingrevision ein. Hier werden die einzelnen Bestandteile dieser Prozesse umfangreich gewürdigt und hinsichtlich Zweckmäßigkeit, Wirtschaftlichkeit und Ordnungsmäßigkeit analysiert. Dabei fließen die neueren psychologischen wie neurowissenschaftlichen Erkenntnisse ein.

Die Kernprozesse umfassen den Verkaufsprozess, das Operational Planning, die Produktentwicklung und das Innovationsmanagement sowie die Produktion und die Produktionsprüfungen. Damit sind alle Prozesse eines Produktionsbetriebes abgebildet. Es gibt sicherlich eine Vielzahl an unterschiedlichen Ausprägungen von Prozessen in den verschiedenen Branchen. Mit dieser Untergliederung gelingt es dem Verfasser, aber die bedeutsamen Prozesse herauszustellen, die in allen Unternehmen vorzufinden sind.

Bei den Support-Prozessen sind an erster Stelle der IT-Prozess und die IT-Prüfungen zu nennen. Sie werden umfangreich und detailliert vorgestellt. Auch hier findet sich ein Abschnitt, der sich ausschließlich mit den Prüfertools beschäftigt. Weitere Themen dieses Kapitels sind SAP, Continuous Auditing und die Zukunft der IT-Revision. Als zweiter Support-Prozess wird der Einkauf beleuchtet. Auch hier werden wieder alle bedeutsamen Probleme und Fragen aufgeworfen und außerdem Outsourcing, IT-Prüfung im Einkauf und Einkaufs-Compliance, jeweils in eigenen Abschnitten gewürdigt.

Dieses Buch wendet sich an Revisoren, aber auch an das Management und die Aufsichtsorgane der Unternehmen. Den Internen und Externen Revisoren werden Hinweise und Ratschläge für die Durchführung von Prüfungen an die Hand gegeben. Die Vorstände und Geschäftsführer erhalten einen Einblick in die Arbeit der Internen Revision und damit eine Vorstellung, was von der Internen Revision verlangt und geleistet werden kann. Die Aufsichtsräte, Beiräte und Mitglieder von Prüfungs- oder Compliance-Ausschüssen erhalten einen Eindruck, welche Anregungen sie der Internen Revision hinsichtlich der Planung und Berichterstattung von Prüfungen geben können.

Das vorliegende Werk unterstützt die Kandidaten für das CIA-Examen und das Examen zum Internen Revisor^{DIIR}, da in einer Synopse die Gliederung des vorliegenden Buches mit den Examensfeldern vernetzt wird, sodass ein gezieltes Lernen für die einzelnen Examensbestandteile möglich ist.

Für Studierende des Faches Prüfungswesen ist dieses Buch eine wertvolle Hilfe, weil es einführt in die Prozess- und Risikoorientierung von Prüfungen. Damit wird ein Gesamtzusammenhang für die Prüfungsüberlegungen hergestellt, der eine nützliche Ergänzung zu rein theoretischen Abhandlungen des Stoffes bildet.

Das Buch hat sein Ziel erreicht, wenn es die Leser mit den Fragen der Internen Revision vertraut macht, die Qualität der Internen Revision fördert und sichert, Impulse für die Prüfungsarbeit liefert und fester Bestandteil der beruflichen Praxis wird. Das wünschen sich Herausgeber, Autor und Verlag.

Herausgeber

Volker H. Peemöller
Nürnberg

Joachim Kregel
Köln

Geleitwort

Die Interne Revision ist nunmehr als ein zentraler Bestandteil der Corporate Governance anerkannt und erfährt seit Jahren eine kontinuierliche Aufwertung. Gesetzliche Regelungen im Aktiengesetz, Kreditwesengesetz, Versicherungsaufsichtsgesetz und Haushaltsgrundsätzegesetz lenken den Fokus verstärkt auf die Interne Revision und sind ein Zeichen für deren gestiegene Bedeutung.

In Deutschland wird die Entwicklung der Internen Revision durch das DIIR – Deutsches Institut für Interne Revision e.V. getragen und durch vielfältige Aktivitäten vorangetrieben. Das DIIR bietet umfassende Aus- und Weiterbildungsmöglichkeiten in Form von Seminaren und Tagungen an und pflegt intensive Kontakte zu Hochschulen, auch mit dem Ziel, das Thema Interne Revision in die Hochschulausbildung zu integrieren. An der Universität Duisburg-Essen hat das DIIR einen Stiftungslehrstuhl „Interne Revision und Corporate Governance" gegründet. Das DIIR bietet mit der weltweit einheitlichen Zertifizierung zum Certified Internal Auditor (CIA) und zum Internen Revisor^{DIIR} stark nachgefragte Qualifikationen an, die genauso wie das weltweit einheitliche Regelwerk der Berufsstandards dabei helfen, das Profil der Internen Revision und ihrer Mitarbeiter deutlich zu schärfen. In über 30 Arbeitskreisen des DIIR tauschen darüber hinaus engagierte Fach- und Führungskräfte der Internen Revision praktische Erfahrungen aus und erarbeiten fachliche Hilfestellungen für die vielfältigen, anspruchsvollen und in ihrer Komplexität stetig steigenden Anforderungen der Internen Revision.

Auch die Reihe „Handbücher der Revisionspraxis" will für die Praxis und die Ausbildung in der Internen Revision Hinweise geben, die helfen, die gestiegenen Anforderungen zu bewältigen. Der nun vorliegende, zweite Band der Reihe ist ein umfassendes Werk zu den Ansätzen des Operational Auditing. Das Aufgabengebiet der Internen Revision hat sich in den letzten Jahrzehnten vom Financial Auditing, also der Prüfung des Finanz- und Rechnungswesens, stark zum Operational Auditing hin verändert. Wir verstehen darunter vielfältige Prüfungsthemen der Internen Revision, die die Verbesserung der Aufbau- und Ablauforganisation, der Wirtschaftlichkeit, Zweckmäßigkeit und Sicherheit von Prozessen einer Organisation zum Ziel haben. Diese Prüfungen sind – anders als Financial Audits – in erster Linie gegenwarts- und zukunftsorientiert und werden unter Risikogesichtspunkten ausgewählt und durchgeführt. Operational Audits verdeutlichen noch einmal mehr den Mehrwert der Internen Revision.

Das vorliegende Werk zum Operational Auditing bietet eine Fülle von Anregungen für die Prüfungspraxis und schlägt einen weiten Bogen über die verschiedensten Kern- und Unterstützungsprozesse wie Produktion, Marketing, IT und Einkauf. Es berücksichtigt viele aktuelle Entwicklungen wie COSO ERM, COBIT 5.0 und auch aktuelle Marktstudien wie die viel beachtete „Enquête 2014", die vom DIIR gemeinsam mit den österreichischen und schweizerischen Instituten herausgegeben wird.

Das Wissen über die aktuellen Erkenntnisse ist für die Internen Revisoren von hoher Wichtigkeit. Das DIIR begrüßt daher die Reihe „Handbücher der Revisionspraxis" und begleitet sie mit Interesse.

Frankfurt am Main, Februar 2015

Bernd Schartmann, CIA, CRMA
Sprecher des Vorstands
DIIR – Deutsches Institut für Interne Revision e.V.

Vorwort des Autors

„Was lange währt, wird endlich gut (hoffentlich)!"

Viel später als angedacht, jedoch dadurch umso aktueller, kommt der zweite Band der Schriftenreihe Interne Revision aus dem Erich Schmidt Verlag mit dem Titel Operational Auditing auf den Markt.

Mangels Vorlagen ist dieser Band in seiner Form und Darstellungsweise einzigartig. Er weist eine Spannbreite der Prüfungen von Einkaufs- über Verkaufsprozessen bis hin zur Produktion auf. Der Prüfung der Marketingprozesse und des Supportprozesses Informations- und Telekommunikationstechnologie wird mit jeweils mit über 25 % des Gesamttextanteils ein breiter Raum gewidmet. Damit soll dieses Buch dem Leser für die nach Auffasssung des Autors wichtigsten Trends der aktuellen Wirtschaft, der Digitalisierung und der gleichzeitigen Kundenorientierung, Stichwort Social Media, die Prüfungsgrundlagen legen.

Auch die Prüfungen im Baubereich bzw. die Prozessprüfungen um die Immobilien werden aus Sicht des Bauherrn diskutiert. Branchenbesonderheiten wird nach Möglichkeit Rechnung getragen.

Viele praktische Beispiele aus dem Handel, der IT- und Telekommunikationsindustrie, aber auch der Automobilindustrie und der Lebensmittelindustrie unterstreichen die besonders praktische Bedeutung dieses Bandes.

Aus der Kaufmannsbrille gesehen, erlebt und geschrieben, soll er Kaufleuten die Angst vor einem engen Kontakt mit Naturwissenschaftlern und den MINT (Mathematik, Informatik, Naturwissenschaft, Technik)-Welten nehmen. Im Gegenteil können sich beide Seiten bei gegenseitiger offener Kommunikation „befruchten", ganz im Sinne eines interdisziplinären Ansatzes. Die Begeisterung des Naturwissenschaftlers mit zu nehmen, der nach vielen Versuchen endlich Lösungen gefunden hat, immer steht für ihn das Werk im Mittelpunkt. Diese Sichtweise des Kreativen oder Innovators gilt für den Maschinenbau in der Konstruktion, beim Design eines Softwareprodukts in der Informatik oder einer durchgängigen Strategie des Marketings, die dann alle anderen Unternehmensbereiche zum Aufbau der Marke mitreißt. Diese andere Sichtweise kann uns manchmal sehr nüchtern daherkommende, an Zahlen orientierte RevisorInnen[1] viel Freude bereiten. Denn aus dem anderen Betrachtungswinkel sehen wir die Produkte hinter den Zahlen und finden bei all dem notwendigen abstrakten Oberbau aus COSO (Committee of Sposoring Organizations of the Treadway Commission), IIA (Institute of Internal Auditors)-Anforderungen, IFRS (International Financial Reporting Standards)-Regularien dann die wertvolle Essenz des Geschaffe-

1 Im Folgenden wird jeweils die männliche Schreibweise gewählt. Der Autor ist sich bewusst, dass dieses Buch auch von vielen Kolleginnen gelesen werden wird. Trotzdem ist er nach einigen Gesprächen mit Frauen aus seinem eh. Mitarbeiterkreis der Überzeugung, der Lesbarkeit gegenüber einer nur oberflächlichen „Political Correctness" den Vorzug zu geben.

nen/der Werke der realen analogen und auch digitalen Welt, die unsere Welt der Zahlen und Fakten erst möglich macht.

Unsere betriebwirtschaftliche und unternehmerische Sichtweise des Geschäftsmodells, des „Es muss sich aber irgendwann rechnen", unsere Einforderung von operativer Verantwortung nicht nur für das Schöne, sondern auch für die Einhaltung von Plänen und Budgets, die Bewältigung von Risiken, die Implementierung notwendiger Kontrollschritte öffnet wiederum die operative Seite für unternehmerische Gesamtverantwortung.

In diesem Sinne sollen auch einige kritische Ansätze zu Reputationsrisiken, zum echten Wahrnehmen von CSR (Corporate Social Responsibility), also Nachhaltigkeit im wirtschaftlichen Denken und Handeln, verstanden werden. Sie sollen nicht als Systemkritik, sondern als notwendige Reformschritte für einen Erhalt und Ausbau der sozialen Marktwirtschaft in den Unternehmen angesehen werden. In Zeiten der Globalisierung können sich Unternehmen den Konsequenzen ihrer Entscheidungen sowohl in der Lieferkette wie auch in der Produkt- und Servicekette zum Kunden hin nach Meinung des Autors nicht in ihr Unternehmen zurückziehen.

Die zwei privat geführten Unternehmen (Otto und Kaufhof/Metro-Gruppe), in denen der Autor die große Freude hatte, zum Wohl dieser Unternehmen einen Beitrag zu leisten, sahen und sehen sich immer auch als Teil der Gesellschaft. Die beiden anderen, Unilever und Deutsche Telekom AG, haben dies aus ihrer Kundenorientierung und ihrem Marketing schnell gelernt und sich entsprechend angepasst und neu ausgerichtet.

Das Buch Operational Auditing wendet sich sowohl an den erfahrenen, aufgeschlossenen als auch an den jungen, wissbegierigen Revisor. Beide sollen ein wenig Grundlagenwissen erhalten, wenn sie sich mit den für Kaufleute manchmal fremden Gebieten der MINT-Welten beschäftigen. Das Buch ist nicht bewusst für den CIA- und Interner Revisor (DIIR)-Kandidaten geschrieben worden, obwohl es gerade in den Management- und IT-Teilen dieser Examina hilfreich sein wird. In der Vorbereitung dieser Examina wünscht der Autor, selbst CIA, allen Kandidaten viel Erfolg und Nutzen beim Durcharbeiten des Materials aus diesem Buch.

Der neue PS 261, der seit 2012 den alten IKS-Standard PS 260 abgelöst hat, ermöglicht es den Kollegen aus der Abschlussprüfung, nicht nur nach den Posten der Abschlussrechnungen, sondern auch nach Geschäftsprozessen und Funktionen ihre risikoorientierte Prüfung zu orientieren. Der Autor hofft, in den angesprochenen Themengebieten, insbesondere in den Kapiteln 5: Marketing und Marketingrevision, 9: Produktion und Produktionsprüfungen, 10: IT-Prozesse und IT-Prüfungen und 11: Einkauf/Sourcing und Beschaffungsprüfungen einige Anregungen geben zu können.

Darüberhinaus wendet sich das Buch an Manager der Internen und Externen Revision, die sich inhaltlich mit der Grundlage operationeller Risiken beschäftigen wollen und nicht beim Prozess des Risikomanagements stehen bleiben möchten. Insofern sind nicht nur Kollegen aus dem Handel, der Dienstleistungsbranche und der Industrie angesprochen, sondern auch die Kollegen aus Banken und Versicherungen, die

sich mit operationellen Risiken beschäftigen, in ihrem eigenen Unternehmen oder Unternehmen von Kredit- und Versicherungsnehmern.

Nachdem im ersten Kapitel die Voraussetzungen für Operational Auditing in der Internen Revision, ein adäquater Geschäftsauftrag, entsprechend qualifizierte Mitarbeiter und Interesse an der Auseinandersetzung mit dem Geschäftsmodell ihres Unternehmens geklärt werden, geht es im zweiten Kapitel um COSO ERM (Enterprise Risk Management) oder COSO II. COSO ERM legt mit seinen 8 Prozessen zum Risikomanagement in einem Unternehmen den generischen Ansatz, um komplizierte Risiko-Sachverhalte vollständig und anschaulich zu beschreiben und abzubilden. Das gilt für die Konzernebene für Unternehmen wie auch für einzelne Geschäfts- oder Funktionsbereiche. Der Autor verbindet in den einzelnen Kapiteln den COSO ERM-Ansatz mit dem Revisions-Ziel „Zweckmäßigkeit von Prüfungen". Die Ziele Ordnungsmäßigkeit, Wirtschaftlichkeit und Compliance werden separat beschrieben. In den Kapiteln Einkauf, Marketing, Produktion und ITK erfolgt auch jeweils eine Einführung in die Grundlagen dieses Themengebiets. Diese Einführung ist nicht als betriebswirtschaftliche Einführung in die Themengebiete gedacht, darüber gibt es ausreichend Fachliteratur. Es werden nur die Fachbegriffe und -hintergründe erörtert, die wichtig sind, um die danach folgenden Prüfungsaussagen zu verstehen.

Im dritten Kapitel wird ein generisches Prozessmodell mit Management-, Support- und operativen Prozessen vorgestellt und die wichtigsten Prozesse, die in diesem Band nicht abgehandelt werden, z. B. alle Finanz- und Führungsprozesse, kurz aus Revisionssicht angerissen[2].

Ein kurzes Tool-Kapitel beschäftigt sich mit einigen bekannten Analysewerkzeugen, wie der GWA (Gemeinkostenwertananalyse), dem Zero-Base-Budgeting und der Balanced Scorecard als Führungsinstrument, um nur einige zu benennen.

Einen weiteren Schwerpunkt sieht der Autor in der Beschäftigung mit dem Marketing eines Unternehmens. Dieser Bereich wird in seinen Grundlagen der 7P (Product, Pricing, Promotion, Placement, People, Process und Provision of Service) vorgestellt. Dabei wird auch der SWOT (Strengths Weaknesses Opportunities Threads)-Ansatz zur Unternehmensanalyse sowie das BCG (Boston Consulting Group)-Modell eines generischen Produktportfolios diskutiert. Ein Modell für Kundenmanagement mit Bezug zu CRM (Customer Relationsship Management) sowie der TRI:M-Ansatz von TNS Infratest/Burke zur Kundenzufriedenheit vervollständigt die Grundlagen.

Alle Ziele einer Prüfung werden im Einzelnen beschrieben. Hierbei sollte, wie in den anderen Kapiteln auch, immer wieder beachtet werden, dass der Autor dem Full Audit vor einem Spezial Audit den Vorzug gibt[3].

Sonderthemen in diesem Kapitel sind Erkenntnisse der Neurowissenschaften, die teilweise schon sehr professionellen Einzug ins Marketing gefunden haben, das quan-

2 Eine vertiefte Abhandlung ist im Band Financial Auditing geplant.

3 Auch hier ist dem Autor bewusst, dass bei Prüfungen, die sich mit dolosen Handlungen beschäftigen, zunächst das Compliance-Ziel im Vordergrund stehen muss. Nach seiner Erfahrung sollten trotzdem das Ziel der Wirtschaftlichkeit und Zweckmäßigkeit hinzukommen, um zu einer Gesamtbeurteilung des Falls zu gelangen.

titative Marketing mit Big-Data-Analysen und Online-Marketing mit seinen unterschiedlichen Spielarten.

Die Graubereiche, die in der Praxis häufig schwer zu trennen sind, werden im Compliance-Ansatz zusammen mit Red Flags dargestellt. Zu den Graubereichen gehören im Einzelnen Einladungen zu Events, Preisausschreiben und Gewinnspiele, Zugaben und Auslobungen bei Treueprämien u. a. m.

Auch im Einkaufskapitel wird der COSO ERM-Ansatz umgesetzt. Zuvor folgen Hinweise zum Chief Buyer Konzept, der Internationalisierung der Beschaffungsmärkte mit Darstellung der Incoterms für die internationale Logistik und unterschiedliche Beschaffungformen entsprechend der Güterarten. Risiken aus der internationalen Beschaffung mit Warentermin und Devisengeschäften, Beachtung der Corporate Global Citizenship, heruntergebrochen auf die Lieferantenkette, und eine Vielzahl von IT-gestützten SCM-Prüfungsansätzen runden dieses Kapitel ab.

Im Produktionskapitel werden die Planungsgrundlagen, basierend auf den Marketing- und Unternehmensplänen dargestellt. Entwicklungsprozesse und Innovationsmanagement werden erörtert und an Beispielen aus der Telekommunikation und dem Handel diskutiert. Im Vergleich der Wertschöpfungsquoten am Umsatz können viele Non-Food-Handelsunternehmen mit denen von Industrieunternehmen, z. B. der Stahl- oder Automobilindustrie mithalten. In der Telekommunikation wird das Modell einer vollautomatischen Produktion mit eingebauter Fehlerkorrektur sichtbar, das ein wenig über die unterschiedlichen Protokoll- bzw. Layerebenen im IT-Kapitel vertieft wird. Diese Vertiefung erscheint dem Autor sinnvoll, um die vielfachen Angriffen, der sich eine ITK-Infrastruktur ausgesetzt ist, in ihren Grundlagen zu verstehen.

Über ein abstraktes Modell von Fehl-, Blind-, Schein- und Wirkleistung aus der Elektrotechnik wird versucht, dem Leser ein Gefühl für mögliche Prüfungsansätze zu geben und ihn zu ermutigen, zusammen mit dem operativen Management dafür zu sorgen, dass der Anteil der Wirkleistung seines Unternehmens an der Gesamtleistung immer höher wird.

Risiken der Produktion, die allein schon durch die Standortwahl oder Verzögerungen in der Lieferkette verursacht sein könnten, werden angesprochen und im Einzelnen diskutiert. Die möglichen Implikationen von Industrie 4.0 oder dem Internet der Dinge werden angerissen.

Bei all dem ist zu beachten, dass es unmöglich ist, über die unterschiedlichen Spielformen von Branchen einen allgemeinen, jedoch in der Praxis sofort umsetzbaren Prüfungsansatz zu finden. Der Autor hat versucht, aus seiner Erfahrung von vier sehr unterschiedlichen Branchen allgemeinere Ansätze zu formulieren, die einem Revisor einen ersten Einstieg in die Prüfung von Produktionsprozessen seines Unternehmens erleichtern soll.

In dem anderen Schwerpunktkapitel IT, das in seinen größten Teilen kurz vor der Snowden-NSA (National Security Agency)-Affäre geschrieben wurde, wird der Darstellung der Grundlagen der ITK großer Raum gewidmet. Hardware-, Netz- und Softwarekomponenten werden im Einzelnen dargestellt und im Zusammenspiel ge-

schildert. Eine Vielzahl von Fachbegriffen und Abkürzungen wird u. a. im Glossar erläutert und mit ihren Implikationen auf eine IT-Prüfung dargestellt. Die verschiedenen Software- Entwicklungs- und Vorgehensweise-Modelle werden präsentiert, ebenso die große Bandbreite von internationalen Qualitätsnormen. Zusätzlich zu COBIT (Control Objectives for Information and Related Technology) gehören das CMMI (Capability Maturity Model Integration), ITIL (Information Technology Infrastructure Library), eTOM (Enhanced Telecom Operations Map) und SPICE (Software Process Improvement and Capability Determination) sowie TOGAF (The Open Group Architecture Framework) und eine Vielzahl von ISO-Normen zur IT, z. B. die ISO 27.000 für IT-Sicherheit[4].

Detailliert und mit vielen Grafiken hinterlegt wird die IT-Sicherheit dargestellt, den unterschiedlichen Angriffsformen wie u. a. bot-Netze, DoS, Viren, Würmern und Trojanern werden Verteidigungsformen wie Honeypot, Firewalls, Virenscanner und VPN (Virtual Private Network) entgegengesetzt. Auch das hochaktuelle Thema BYOD (Bring Your Own Device) wird bzgl. seiner Prüfungsimplikation dargestellt.

Nicht fehlen darf natürlich der Prüfungansatz mit IDEA (Interactive Data Extraction and Analysis) oder ACL (Audit Command Language) sowie die Erläuterung der Begriffe von CM (Continuous Monitoring) und CA (Continuous Auditing).

Last, but not least wurden auch die 17 GTAG des IIA mit eingearbeitet, die für die IT-Revision ebenso eine gewisse Relevanz aufweisen.

Dank zu sagen hat der Autor einer Vielzahl von kompetenten, professionell arbeitenden und immer Auskunft gebenden Kollegen aus den Unternehmen Deutsche Unilever, Otto Group, Kaufhof/Metro und der Deutschen Telekom. Weiterer Dank gebührt auch vielen Kollegen aus den Unternehmen, die dem Autor während seiner Zeit im DIIR-Programmausschuss vertiefende Blicke in ihr Unternehmen gewährt haben.

Besonders hervorheben möchte ich Wolfgang Jess, Vorsitzender der Geschäftsführung Witt Weiden und Dr. Christoph Stege, Partner bei Knapp Stege Marketing Solutions GmbH und Herrn Barthel Roitzsch, Vertriebsleiter bonprix, denen ich viele Ideen zur Vereinfachung und Fokussierung des Marketingkapitels verdanke.

Beim IT-Kapitel habe ich zu danken Herrn Frank Becker, Deutsche Telekom AG, und Herrn Kai-Uwe Ruhse, Protiviti GmbH, für ihre instruktive Kritik, die immer wieder versuchten, den Bogen von der Präzision zur Allgemeinverständlichkeit zu schlagen.

Großen Dank schulde ich meiner Tochter Alessandra Kregel, die es erst möglich gemacht hat, dass das Buch verständlich und klar formuliert wurde. Weiter verdanke ich ihr wertvolle Hinweise aus ihrem Wirtschafts- als auch aus ihrem Psychologiestudium zum Marketingkapitel, insbesondere dem Thema Neurowissenschaften.

4 Die Vielzahl der Abkürzungen mag auf den ersten Blick verwirrend sein, es soll jedoch genau das Gegenteil erreicht werden, eine Ent-Mystifizierung der IT, um auf Augenhöhe miteinander (Fachseite und IR) ins Gespräch zu kommen. Für ein Gespräch ist es wichtig, sog. Termini Technici schon einmal gehört zu haben und ein grobes Verständnis für den Hintergrund dieses Rahmenwerks zu entwickeln.

Last, but not least schulde ich sehr großen Dank Prof. Volker Peemöller, der mich immer wieder ermutigte, diesen Band fertigzustellen und ohne den der Full Audit-Ansatz bei den operativen Prozessen zulasten einer allein begrenzten wirtschaftlichen Sichtweise nicht verwirklicht worden wäre, sowie Herrn Winfried Schnitzler von der Versatel AG, der mir überhaupt die Idee zu dieser Revisionreihe gab und mich bei der Strukturierung der Kapitel unterstützt hatte.

Dank zu sagen habe ich letztlich dem Erich Schmidt Verlag, der mir dabei geholfen hat, meine Idee von einer professionell gemachten Unterstützung der Internen Revision umzusetzen und die vorliegenden Werke in einer hervorragenden Form für den interessierten Leser erstellt hat.

Etwaige Fehler, irrtümliche Schlussfolgerungen und fehlleitende Darstellungen sind allein dem Autor anzulasten.

Der Text ist bewusst mit einer Vielzahl von Beispielen und Namensnennungen von Unternehmen belegt, um dem Leser die Möglichkeit des eigenen Urteils und eigener Schlussfolgerungen zu überlassen. Es stand und steht dahinter immer die Absicht, „Lessons learnt“ oder „Best Practices“ zu beschreiben, nie, einem Unternehmen zu schaden oder es zu brandmarken.

Ich wünsche allen Lesern bei diesem von der Praxis für die Praxis entwickelten Buch viel Freude beim Lesen und Nachschlagen und viele Ideen für ihre Revisions- und Managementpraxis.

Joachim Kregel Köln

Synopse OA und CIA-Exam (Syllabus 2013, Part 3 – Internal Audit Elements)

Kapitel-Nr.	Thema	Unter-Nr.	Unterthema	Beispiel	OA-Nr.	Beispiele
I.	***Governance/Business Ethics***			***5–15 %***		
A.	*Corporate/Organizational Governance Principles – Proficiency Level (P)*				5.4.1 10.2.1 10.2.6 10.4.1	COSO ERM COBIT 5.0. ISO 38.500 Three Lines of Defense
B.	*Environmental and Social Safeguards*				9.2 9.1	Better Coal B.U.N.D Umweltbundes-amt
C.	*Corporate Social Responsibility*				5.1.1.1	Textilfabrik Bangladesh
II.	**Risk Management**			**10–20 % (Proficiency Level (P)**		
A.	*A. Risk Management Techniques*				5.4.4 9.2.4 10.3 11.2.4	Porter; Sensitivitätsanalyse, Value at Risk, Stresstest, Benchmarking, Ampelliste; Verwundbarkeitsanalyse (GTAG 6); Wasserfallmodell; Lieferantenbeurteilung; Risikostrategie: Vermeiden-Überwälzen-Versichern-Selbst Tragen;
B.	*B. Organizational Use of Risk Frameworks*				2; 5.2.5; 10.3	COSO ERM
III.	***Organizational Structure/Business Processes and Risks***			***15–25 %***		
A.	*Risk/Control Implications of Different Organizational Structures*				5, 9, 10, 11	COSO ERM im Marketing, Produktion, IT und Einkauf
B.	*Structure*			*centralized/ decentralized*	2,3	
C.	*Typical Schemes in Various Business Cycles*			*procurement, sales, knowledge, supply-chain management*	5, 11,	 Logistikbranche IT-Branche Preispolitik

Kapitel-Nr.	Thema	Unter-Nr.	Unterthema	Beispiel	OA-Nr.	Beispiele
D.	*Business Process Analysis*			*workflow analysis and bottleneck management, theory of constraints*	5.1.6, 5.2.3 9.2.4	SWOT Szenariotechnik, Sensitivitäts analyse
E.	*Inventory Management Techniques and Concepts*				*Offen: Financial Auditing*	
F.	*Electronic Funds Transfer (EFT)/Electronic Data Interchange (EDI)/E-commerce*				6.1, 6.2, 6.3, 10.1.2.6	B2B, B2C, EDI
G.	*Business Development Life Cycles*				10.2.7.1	CMMI
H.	*The International Organization for Standardization (ISO) Framework*				9.2.5 10.2.6	TQM, KVP ISO-Normen für IT
I.	*Outsourcing Business Processes*				11.3.3	ITK, Facility Management
IV.	***Communication***			***5–10_%***	5.1.5; 5.1.8	
A.	*Communication*			*the process, organizational dynamics, impact of computerization*	5.4.7.2; 9.2.7.2; 11.2.7	COSO ERM, Prozess 7: Information & Communication;
B.	*Stakeholder Relationships*					
V.	***Management/Leadership Principles***			**10–20 %**		
A.	*Strategic Management*					Porter, Disruptive Technologies am Beispiel des IT-Marktes
1.	Global analytical technique	1.	Structural Analysis of industries		5.2.4	
		2.	Competitive strategies		5.2.4	
		3.	Competive analysis		5.2.4	
		4.	Market signals		5.1.6, 5.2.4	
		5.	Industry evolution		5.2.4	
2.	Industry environments	1.	Competive strategies related to	1.Fragmented industries 2. Emerging industries 3. Declining industries	5.1.1.2	BCG Portfolio-Modell: Stars-Cash Cows-Dogs-Questions Marks
		2.	Competition in global industries	1. Sources/impediments 2.Evolution of global markets 3. Strategic alternatives 4. Trends affecting competition	5.2.4	Porter, Disruptive Technologies am

Kapitel-Nr.	Thema	Unter-Nr.	Unterthema	Beispiel	OA-Nr.	Beispiele
						Beispiel des IT-Marktes
3.	Strategic decisions	1.	Analysis of integration strategies		5.4.1	
		2.	Capacity expansion			McKinsey 7S
		3.	Entry in new businesses		3.2.1	M&A
4.	Forecasting				7	
5.	Quality Management			TQM, Six Sigma	Band 1	
6.	Decision Analysis				5, 9., 10, 11	COSO ERM im Marketing, Produktion, IT und Einkauf
B.	*Organizational Behaviour*					
1.	Organizational theory			Structures & configurations		
2.	Organizational behaviour			Motivation, impact of job design, rewards, schedules		
3.	Group dynamics			Traits, development stages, organizational politics, effectiveness	Band 1	
4.	Knowledge of human resources processes			Individual performance management, supervision, personnel sourcing/staffing, staff development	3.2.2	TRI:M, MOP (Mitarbeiterorientierter Prozess)
5.	Risk/control implications of different leadership styles				5.4.1; 9.2.1, 10.4.1; 11.2.1	
6.	Performance			Productivity, effectiveness	Über 200 konkrete Ersparnisvorschläge im gesamten Buch inkl. der Checklisten	
C.	*Management Skills/Leadership Styles*				5.1.5; 9.1.5	
1.	Lead, inspire, mentor, and guide people, building organizational commitment and entrepreneurial orientation				5.4.1	
2.	Create group synergy in pursuing collective goals				5.4.1	
3.	Team building and assessing team performance				5.4.1	
D.	*Conflict Management*				5.4.1	
1.	Conflict resolution			Competitive, cooperative, and compromise		McKinsey 7S
2.	Negotiation skills					

Kapitel-Nr.	Thema	Unter-Nr.	Unterthema	Beispiel	OA-Nr.	Beispiele
3.	Conflict Management				Band 1	
4.	Added value negotiating					
E.	*Project Management/Change Management*				4.3, 8.2	Modell des Macht-, Fach- und Prozesspromotor,
1.	Change Management					
2.	Project Management techniques				4.3.1/ 10.7.1	GANNT und PERT
VI.	***IT/Business Security***			**15–25 % der Examensfragen**		
A.	*Security*				10.6	Hackerangriffe, DoS-Attacken, Flooding, Spoofing, Viren, Trojaner, Pharming, Bot-Netze Phishing
1.	Physical/System Security			Firewalls, access control	10.6.6.1	
2.	Information protection			Viruses, privacy	10.6.6	
3.	Application authentication				10.6.2.1	Password und PIN
4.	Encryption				10.6.2.2	Kryptoverfahren
B.	*Application Development*				10.2.4	
1.	End-user Computing				10.5.2.2;10.6.2;	Password, SSO
2.	Change control				10.6.3;10.6.4	Password, SSO, back doors
3.	System development methodology				10.5.2; 10.6.5	Betriebs-, Administrations- und Benutzerhandbücher
4.	Application development				10.2.4, 10.2.5	ITIL, PRINCE II; V-Modell, RUP-Modell, Wasserfall-Modell, agile Softwareentwicklung
5.	Information systems development				10.2.1; 10.2.6; 10.3.3.	COBIT; ISO 15.504, 12.207, 20.000
C.	*System Infrastructure*					
1.	Workstations				10.1.1	RAM, ROM, Cache; CPU; Flashspeicher, USB-Sticks; SSD-Karten; NAS
2.	Databases				10.1.4	Relationale DB, NF-DB, XML-DB
3.	IT Control Frameworks			eSAC, CobiT	10.2	COBIT, ISO, COSO, ITIL PS und ISA, BSI, CMMI, Spice, TOGAF, eTOM
4.	Functional areas of IT operations			Data center operations	10.4.3	Audit Trail, CA, CM
5.	ERP Planning			SAP R3	7.1, 9.2.7, 10.1.3.3	ERP, SCM und CRM, MES

Kapitel-Nr.	Thema	Unter-Nr.	Unterthema	Beispiel	OA-Nr.	Beispiele
6.	Data, voice, and network communications/connections			LAN, VAN, WAN	10.1.2	TCP/IP, OSI: 7 Schichten Modell, Ethernet, Token-Ring; Cloud, Bridges, Hubs, Router; LAN, VAN, MAN, VAN, VPN; SAN, VSAN, NAS, DAS
7.	Server				10.1.1; 10.1.2	Web-Server, Client-Server-Architektur, Thin/O-Client
8.	Software Licensing				10.7.3	Software Lizenzen
9.	Mainframe				10.1.1	RAM, ROM, Cache; CPU; Flashspeicher, USB-Sticks; SSD-Karten; NAS
10.	Operating Systems				10.1.3.1	I:OS, Linux, Unix, Windows
11.	Web Infrastructure				10.1.2	OSI: 7 Schichten-Modell, TCP/IP
D.	Business Continuity				10.3; 10.6.1	Business Impact Analysis; Szenariotechnik nach BSI: Force Majeur, Technisches Versagen, Organisatorisches Versagen, Menschliches Fehlverhalten Dolose Handlungen
1.	IT Contingency Planning					
VII.	***Financial Management***			***13–23 %***	***Offen, Band Financial Auditing***	

Nr.	Gruppe	Kurztext	Kapitel	TAB	BPI	BPA	CLN	LVN
1	**Organisation**	Schriftliche Regelung **(Mindeststandard 1)**	1.3./ 7.1.	1.2.		7.9.4.1.	I7.1.	II7.1.
2		Aktuelle Regelung	1.3./ 7.1.			7.9.4.1.	I7.1.	II7.1.
3		Aufgaben sind: IKS, GO (Governance), RM; Antifraudmanagement	1.3./ 2.2./ 5.4.1,/ 7.1.2./ 7.7./ 8.2.5./8.2.6.	1.3./ 2.2./ 5.4./ 5.9./ 7.1./ 7.2./ 7.5./ 10.6.	7.9.3.3.	7.9.4.1.	I7.1.	II7.1./ II7.2.
4		Vollständiger Scope	1.3./ 7.1.3./8.1.	1.4. 1.7./ 5.9./ 7.1./ 7.3./ 10.6.	7.9.3.1.	7.9.4.2.	I.8.1.	II8.2.
5		Unabhängigkeit **(Mindeststandard 2)**	7.1.1.3.				I7.1.5.	II7.5.
6		Rev. unabhängig	7.1.3.				I7.1.5.	
7		Unternehmens.-Info erhalten	8.4./ 9.2.5.	8.7.			I.8.1./ I8.2.	
8		RHB vorhanden	7.6./7.7.	7.13./ 7.15.	7.9.3.4./ 11.8.3.		I7.4.	II7.9.
9		RHB angewandt und aktuell	7.6./7.7.	7.13./ 7.15.	7.9.3.4./ 11.8.3		I7.4.	II7.9.
10	**Budget/ Ressourcen**	Personalbudget angemessen **(NEU: Mindeststandard 3)**	7.1.5.	1.8.	7.9.3.5.	7.9.4.2.	I7.3.	
11		Personalbudget geeignet für Mitarbeiterqualifikation	7.1.5.	1.8.	7.9.3.5.	7.9.4.2.	I7.3.	
12		IT-Ausstattung intern	7.6.1./ 7.6.2./ 8.8.	7.13./8.11.	7.9.3.4./ 10.7.3	8.10.4./ 9.9.4.	I7.4./ I.8.1./ I.10.1.3	
13		IT-Ausstattung extern	7.6.3.	7.14.				
		Sachbudget	7.1.5.			7.9.4.2.	I7.3.	
		Risikoorientierte Planung	5.4./ 8.1.	5.7./ 5.8./ 8.1./ 8.3./ 8.6./ 8.8./ 8.10./ 10.6.	8.10.3.	8.10.4.	I8.2.	II8.1./ II8.2./ II9.1.
14		Jahresrevisionsplanung	8.5./ 8.6./ 8.7./	7.9./ 8.10.	8.10.3.	8.10.4.	I.8.1.	

*) Die Nummerierung der ersten Spalte entspricht dem Leitfaden zum DIIR-Standard Nr.3, Stand 1.7.2012, (3. überarbeitete und ergänzte Aufl.) TAB: Tabellen-Nummer, BPI: Best Practise International, BPA: Best Practise Autoren, CLN: Checkliste-Nummer, LVN: Lösungsvorschlag-Nummer, RO: Revisionsobjekt = einzelne Prüfung

Nr.	Gruppe	Kurztext	Kapitel	TAB	BPI	BPA	CLN	LVN
15	**Planung**	Risikoorientierter Planungsprozess **(Mindeststandard 4)**	8.	8.1.-8.11.		8.10.4.	I8.2.	II8.4.
16		Genehmigung und Bewertung	8.6.3.	8.2.			I8.2.	
17		Client-Wünsche zur Planung	8.6.	8.9.	8.10.3.	8.10.4.	I8.2.	
18		Audit Universe vollständig	8.1.	8.1.			I.8.1.	II8.3.
19		Risikoorierentierte. Revisionsobjekte (RO)	9.1.	8.6./ 8.11.		8.10.4.	I8.2.	II8.4.
20		Audit Universe aktuell	8.1.	8.1./ 8.7.			I.8.1.	II8.3
21		Risikobewertung	8.3./ 9.1.3.	8.4.				
22		Adhoc-Themen	8.7.			8.10.4.	I8.2.	
23		Review unterjährig und Kommunikation	8.7.				I8.2.	
24	**Vorbereitung**	RO-Projektplanung	9.1.	9.2./ 9.3.			I.8.1.	
25		Voranalyse	9.1.1.				I9.1.	
26		RO-Projektplanung	9.1.2.	9.2./ 9.3./ 10.7.			I9.1.	II9.3.
27		Ankündigung	9.3.1.			9.9.4.	I9.1.	
28		Kickoff	9.3.2.					
29		Ziele des RO	9.1.3.				I9.1.	
30		Arbeitsprogramm des RO	9.1.1./ 9.1.3.	9.1.		9.9.4.	I9.1.	
31	**Prüfung**	Prozess des RO		2.1./ 9.6.			I9.1.	
32		FA	9.6.1.					
33		OA, RM, CO	9.6.2./ 9.6.3./ 9.6.4.					
34		Maßnahmenvorschläge	9.6.5.	9.7.		9.9.4.	I9.2.	
35		Abstimmung Feststellung	9.5.2.	9.7./ 10.3.		9.9.4.	I9.2.	
36		RO: Plan-Ist-Abgleich	10.4.4.				I9.2./ I10.1.2.	
37		RO: Dokumentation	9.7.			9.9.4.	I9.2.	

Nr.	Gruppe	Kurztext	Kapitel	TAB	BPI	BPA	CLN	LVN
		(Mindeststandard 5)						
38		Einheitliche Bewertung	5.3.	5.6./ 10.1.				
39		Referenzierung Arbeitspapiere und Bericht	9.7.1.			9.9.4.	I9.2.	
40		Zweckmäßige Methodenwahl	5.5./ 9.2.	9.4./ 9.7./ 10.3.		9.9.4.	I9.2.	
41		Schlussbesprechung	10.4.	10.7./ 10.8.	9.5.	10.7.4.1.	110.1.2.	
42		Massnahmenkatalog	10.2.2.3.				I9.2.	
43		Alternative zur Schlussbesprechung	10.2.1./ 10.2.5.	10.2.				
44	**Berichterstattung**	Zusammenfassung +.-Detailbericht	10.2.2./ 10.2.3.	10.2.			I10.1.1.	II10.1.-3.
45		Standardisierung des RB	10.1.	10.1.			I10.1.1.	II10.1.
46		Vorabstimmung Feststellungen mit geprüften Bereich	9.5.2.	10.2.			I9.2.	
47		Stellungnahme zum RB vom geprüften Bereich	10.2.3.				I10.1.2./ I10.1.3.	II10.4.
48		Zeitnahe Veröffentlichung RB	10.1.2.	10.2.	10.7.3.		I10.1.3.	
49		Genehmigung RB		10.1.				
50		RB-Verteiler	10.2.2.1.	10.1.		10.7.4.1.		II10.1.
51		Schriftlicher Nachweis der Prüfung	10.2.5				I10.1.3.	
52		Kommunikation	10.2.4./10.2.5					
53	**Prüfungsnach-arbeit**	Feedback Team	10.4.4.	10.8.		10.7.4.2.	I10.3.	
54		Konsequenzen Feedback	7.4.5./ 10.4.4.			10.7.4.2.	I10.3.	
55		Wissensmanagement	9.7.4.		10.7.3.	10.7.4.2.	I10.3.	
56		Archivierung	9.7.5.				I10.3.	
57	**Follow-up**	Etablierter Prozess	10.5.	10.9.		10.7.4.3.	I10.2.	

Nr.	Gruppe	Kurztext	Kapitel	TAB	BPI	BPA	CLN	LVN
58		Fristverlängerungen	10.5.1./ 10.5.2.	10.9.			I10.2.	
59		Info über Follow-up an Leitung		10.9.		10.7.4.3.	I10.2.	
60		Regelung über Follow-up-Prüfung vorhanden	10.5.3.			10.7.4.3.	I10.2.	
61	**MA-Auswahl**	Personalplanungsprozess	7.4.5.			7.9.4.3.		
62		Stellen-, Aufgabenbeschreibungen vorhanden	7.4.2					
63		Stellen-, Aufgabenbeschreibungen angewandt	7.4.2					
64		Mitarbeiterqualifikation	1.3./ 7.4.5/ 7.5.2	1.4.-1.7./7.3/ 7.12				II7.7.
65		Nutzung von Expertenwissen	7.4.6					
66	**Entwicklung/ Fortbildung**	Schulungen	7.4.5.	7.12.	7.9.3.7.	7.9.4.4.	I7.3.	
67		Schulungen für Sozialkompetenz	7.4.5.	7.12./ 10.8.			I.7.3.	
68		Zertifizierungen	1.4./7.4.5.					
69		Beurteilungen		7.12.	7.9.3.1./ 7.9.3.6.		I7.3.	
70		Mitarbeiter-Initiativen für Fortbildung	7.4.5.	7.12.			I7.3.	
71	**Führung**	Zweckmäßige Revisions-Leiter (RL)-Qualifikation	7.5.1.		11.8.3.	7.9.4.5.		II7.8.
72		Akzeptanz des RL	7.5.2./ 11.4.3.	7.11./ 11.9.				
73		Zweckmäßige QA-Standards	4.2./ 11.1.	11.1./ 11.3./ 11.5./ 11.6./ 11.8./ 11.9.	11.8.3.		I11.1.	II11.1.-2.
74		QA-Programme laufen im Tagesgeschäft		11.2./ 11.4.	7.9.3.8./ 8.10.3./11.8.3.	8.10.4.	I11.1.-5	II11.1.-2.

Nr.	Gruppe	Kurztext	Kapitel	TAB	BPI	BPA	CLN	LVN
75		JRB	10.2.4.					
76		KVP	11.1./ 11.6.	11.2./ 11.7.	10.7.3./ 11.8.3.		I7.4.	II11.1.-2.
77		Feedbackgespräche intern FirstLine	7.5/ 8.6.2/8.6.3/ 12.1.6	12.5				
78		Beachtung Gesetze	3./ 7.2.1.					
79		Gespräche mit AP	12.1.1./ 12.1.6	12.5		8.10.4.	I7.3.	
80		Feedbackgespräche intern Second Line	12.1.2/ 12.1.3/ 12.1.5/ 12.1.6	12.5				

Inhaltsverzeichnis