

ESV ERICH
SCHMIDT
VERLAG

Handbücher der Revisionspraxis

Band 3

Management Auditing

Prüfung von Strategien, Systemen und Prozessen

Von

Prof. Dr. Volker H. Peemöller

Dipl.-Oek. Joachim Kregel

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.dnb.de> abrufbar.

Weitere Informationen zu diesem Titel finden Sie im Internet unter

<https://ESV.info/978-3-503-16325-0>

Zitiervorschlag:

Peemöller/Kregel, Management Auditing

ISBN 978-3-503-16325-0 (gedrucktes Werk)

ISBN 978-3-503-16326-7 (eBook)

ISSN 1867-6146

DOI <https://doi.org/10.37307/b.978-3-503-16326-7>

Alle Rechte vorbehalten.

© 2025 Erich Schmidt Verlag GmbH & Co. KG

Genthiner Straße 30 G, 10785 Berlin

info@ESVmedien.de, www.ESV.info

Die Nutzung für das Text und Data Mining ist ausschließlich dem Erich Schmidt Verlag GmbH & Co. KG vorbehalten. Der Verlag untersagt eine Vervielfältigung gemäß § 44b UrhG ausdrücklich.

Druck: C. H. Beck, Nördlingen

Vorwort der Autoren

Mit Management Auditing wird der dritte Band der Reihe „Handbücher der Revisionspraxis“ vorgelegt. Diese Prüfung gilt als Königsdisziplin der Internen Revision. Sie wird z.T. als Tabuthema gesehen unter dem Motto „Wessen Brot ich esse, dessen Lied ich singe“. Das ist aber zu kurz gesprungen. Management Auditing betrifft nicht nur das Topmanagement. Prüfung bedeutet verbessern, Management-Systeme sind nicht geschlossen vorgegeben, sind zeitlich versetzt entstanden und werden nicht immer so umgesetzt, wie sie geplant wurden. Insofern ist das Management Auditing heute eine Notwendigkeit.

Das vorliegende Buch umfasst das gesamte Management System in der Breite wie in der Tiefe. Zunächst werden die Voraussetzungen für MA kurz erläutert. Sehr ausführlich werden die verschiedenen Formen der Unternehmensüberwachung mit den bestehenden gesetzlichen und regulatorischen Anforderungen vorgestellt. COSO ERM und COSO ICS werden intensiv beleuchtet und mit vielen Beispielen angereichert. Die anschließenden Kapitel folgen dem Managementprozess über Aufsichtsratsprozesse, Strategieentwicklung, Planung, externe Berichterstattung, Führungsprozess, Fusionen, Topmanagement und Management-Fraud. Alle diese Themen werden unter dem Gesichtspunkt der Internen Revision betrachtet. Der gesamte Kreislauf des Management Prozesses ist damit eingebunden. Besondere Bedeutung hat dabei die Verbindung von Strategie und Risiko, wie sie im COSO ERM dargestellt wird und die Unterstützung der Leitungs- und Überwachungsorgane. Die neuen Themen und Herausforderungen der Internen Revision werden diskutiert, wie die Möglichkeiten und Grenzen der KI, die Bedeutung der ESG-Normen für die Interne Revision. Die Interne Revision dient damit als Vorbild für alle Supportfunktionen. Die abwechslungsreiche und anspruchsvolle Thematik des MA macht die Interne Revision zu einem gelungenen Sprungbrett für den Revisions-Nachwuchs.

Die bewährte Konzeption der Buchreihe wird auch in diesem Band beibehalten. Die neuen Standards IIA sind in den Abschnitten eingearbeitet. Wichtige und markante Stellen werden hervorgehoben. Viele Beispiele und Abbildungen veranschaulichen den Text. Im Vordergrund stehen Praxisbezug und Problemorientierung. Hinweise, Anleitungen und Anregungen machen das Buch zu einem Werkzeug des Internen Revisors, der sich mit dem Management Auditing vertraut machen will. Für den Revisor, der bereits Erfahrungen mit dem MA hat, enthält das Buch eine geschlossene Darstellung, viele spezielle Anregungen und gibt gezielte Unterstützung bei praktischen Aufgabenstellungen.

Die Autoren hoffen, dass die Leser auf viele Fragen Antworten finden und darüber hinaus Erkenntnisse gewinnen, die zur Förderung und Sicherung der Qualität der Internen Revision beitragen.

Köln, Nürnberg, September 2024

Joachim Kregel
Volker H. Peemöller

Vorwort

Joachim Kregel hat mit großem Einsatz die Veröffentlichung dieses Buches vorangetrieben und geprägt. Es enthält eine Vielzahl seiner persönlichen Erfahrungen zur Internen Revision, der er sich immer verbunden fühlte. Am Manuskript hat er bis zu seinem Tod gearbeitet und es mit abgeschlossen. Am 17. Oktober ist er verstorben. Die Interne Revision verliert einen Experten und kritischen Betrachter. Ich einen Partner, mit dem ich mich fachlich und menschlich über viele Jahre sehr verbunden fühlte.

Nürnberg, November 2024

Volker H. Peemöller

Inhaltsverzeichnis

Vorwort der Autoren	5
Vorwort	6
Abbildungsverzeichnis	17
Tabellenverzeichnis	19
Abkürzungsverzeichnis	23
Einführung	33
1. Voraussetzungen für MA	37
1.1 Die Prüfungsarten im Überblick	38
1.2 Der Revisor im Spannungsfeld zwischen geprüften Bereichen, Topmanagement und Aufsichtsrat (Serving two Masters)	41
1.2.1 Erwartungen des Topmanagements an die IR	42
1.2.2 Erwartungen des Aufsichtsrats/Prüfungsausschuss an die IR	45
1.2.3 Erwartungen der geprüften Bereiche an die IR	45
1.2.4 Erwartungsdiskrepanzen an die IR zwischen geprüfem Bereich und Unternehmensleitung	47
1.3 Mitarbeiterqualifikation	49
1.4 Kenntnisse des Geschäftsmodells	51
1.5 Kernthesen	53
Anhang	54
A. IIA Standards	54
B. Best Practises International	59
C. Best Practises National	60
2. Unternehmensüberwachung	63
2.1 Gesetzliche und regulatorische Grundlagen	63
2.1.1 Relevante aktienrechtliche Regelungen	63
2.1.2 Relevante Regelungen des OWiG	68
2.1.3 Relevante Regelungen des Sarbanes Oxley-Act	74
2.1.4 Organization for Economic Cooperation and Development (OECD)	81
2.1.5 Deutscher Corporate Governance Kodex (DCGK)	82
2.2 COSO ERM	83
2.2.1 Unternehmensführung und Kultur	85
2.2.2 Strategie und Zielvereinbarungen	93
2.2.3 Zielerreichung	106
2.2.4 Überprüfung und Korrektur	119
2.2.5 Information, Kommunikation und Berichterstattung	122

2.3.	COSO ICS	126
2.3.1.	Kontrollumfeld	128
2.3.2.	Risikoinventur	131
2.3.3.	Steuerungsaktivitäten	136
2.3.4.	Information und Kommunikation	139
2.3.5.	Monitoring-Aktivitäten	141
2.4.	Three Lines of Defense Model (TLoD) alt und Three Lines Model (TLM) neu	142
2.4.1.	High Level Controls der Unternehmensleitung	144
2.4.2.	First Line: operative Kontrollen	145
2.4.3.	Second Line: Risikomanagement, Compliance, Controlling, Qualitätssicherung, Unternehmenssicherheit, IT-Sicherheit	146
2.4.4.	Third Line: Interne Revision	149
2.4.5.	Abschlussprüfer	151
2.4.6.	Möglichkeiten und Grenzen des TLM-Modells	151
2.5.	Kernthesen	152
	Anhang	153
A.	IIA Standards	153
B.	DIIR: Standard	162
C.	Best Practises International	166
D.	Best Practises National	166
3.	Grundzüge der Unternehmensführung	167
3.1.	Leitbild des Unternehmens	167
3.1.1.	Vision	167
3.1.2.	Mission	167
3.1.3.	Code of Conduct	168
3.1.4.	Corporate Governance	169
3.1.5.	Social Responsibility	170
3.2.	Organisation/Organisationsentwicklung/Organisationsänderungen	172
3.2.1.	Organisation	172
3.2.2.	Zentral/Dezentral nach Funktionen, Objekten und Regionen	173
3.2.3.	Matrix-Organisation	175
3.2.4.	Prozess-Organisation	176
3.2.5.	Projektmanagement	181
3.3.	Outsourcing	189
3.3.1.	Grundlagen	189
3.3.2.	Phasen des Outsourcing-Prozesses	190
3.4.	Chancenmanagement	193
3.5.	Kernthesen	196
	Anhang	197
A.	IIA-Standards	197
B.	DIIR-Standards	198

4. Managementprozess I: Revision der Aufsichtsrats-Prozesse	199
4.1 DCGK und gesetzliche Grundlagen	202
4.2 Satzung und Grundsatzserklärungen des Unternehmens	203
4.3 Geschäftsordnung des Aufsichtsrats	205
4.3.1 Sitzungshäufigkeit und Anwesenheit	207
4.3.2 Bildung der Ausschüsse	208
4.3.3 Effizienzprüfung und Selbstbewertung AR/AR- Prozess 2	212
4.3.4 Auswahl und Benennung der Aufsichtsrats- mitglieder/AR-Prozess 1	217
4.4 Sonderthemen	222
4.4.1 Kapitalia	224
4.4.2 Directors Dealings, Insider-Geschäfte	227
4.4.3 D&O-Versicherung	228
4.4.4 Mitbestimmter Aufsichtsrat	228
4.5 Auswahl und Benennung der Vorstandsmitglieder/AR- Prozess 3	229
4.6 Geschäftsordnung des Vorstands inkl. zustimmungspflichtiger Geschäfte (TransPuG)	231
4.7 Festlegung des (max.) Risikoappetits im Unternehmen im Rahmen der Strategiediskussion mit dem Vorstand/auch AR-Prozess 6	234
4.8 Zielvereinbarungen mit dem Vorstand/auch AR-Prozess 4	236
4.9 Beauty Contest der Abschlussprüfer und Vorschlag für die Hauptversammlung/AR-Prozess 5	238
4.10 Berichterstattung des Vorstands vor dem Aufsichtsrat/AR- Prozess 7	241
4.10.1 Budget	243
4.10.2 Finanzieller und nicht-finanzieller Geschäftsbericht inkl. Zielerfüllungen und mit Diskussion des Abschlussprüfer- berichts, Bilanzzeit (Versicherung der gesetzlichen Vertreter), Entsprechenserklärung zum DCGK	243
4.10.3 Quartalsberichte	245
4.10.4 Bericht zum RFS und RMS	246
4.10.5 Sonderberichte zur Compliance	247
4.10.6 Berichterstattung über die IR und von der Internen Revision	249
4.11 Vor- und Nachbereitung der Hauptversammlung/AR- Prozess 8	250
4.12 Kernthesen	251
Anhang	252
A. IIA-Standards	252
B. DIIR-Standards	270
C. International Best Practices	271
D. Nationale Best Practices	272
E. Sonder-Fachthemen	274

5. Managementprozess 2: Revision der Strategieentwicklung	277
5.1 Bestandsaufnahme/SWOT-Analyse	280
5.1.1 Prüfung der Strengths und Weaknesses	283
5.1.2 Prüfung der Opportunities and Threats	285
5.1.3 Unternehmenskultur: Spiegelkabinett oder Klarheit und Wahrheit	288
5.1.4 Prüfung der notwendigen Funktionen und Einschätzung der Fähigkeiten der Funktionsinhaber (Management Audit)	291
5.2 Vorstandsklausur	294
5.2.1 Vorbereitung der „weichen“ Vorstands- oder Strate- gieklausur	295
5.2.2 Prüfung auf angemessene Moderation und Protokollführung	296
5.2.3 Nahtlose Überleitung zur „harten“ Vorstandsklausur/Budgetierung	298
5.3 Prüfung von Vorstandsvorlagen	299
5.3.1 Prüfung auf Relevanz	301
5.3.2 Prüfung auf Plausibilität	301
5.3.3 Prüfung auf Wahrheit und Klarheit	303
5.3.4 Prüfung auf SMART-Adäquatheit	304
5.4 Prüfung des Risk Managements	307
5.4.1 Tone at the Top/Gremienvorbehalte in der Geschäftsordnung des Vorstands	307
5.4.2 Risikoappetit	307
5.5 Prüfung des Risiko-Managementprozesses und eines adäquaten Risiko-Frühwarnsystems	309
5.5.1 Prüfung des Risikomodells	310
5.5.2 Prüfung des Meldesystems innerhalb der Gesellschaft	311
5.5.3 Prüfung der Aktualität der Risikomaßnahmen	315
5.5.4 Prüfung der Vollständigkeit der substanzgefährdenden Risiken bzw. Großrisiken	317
5.5.5 Prüfung des Risiko-Frühwarnsystems (RFS) und PS 340 n. F.	318
5.6 Kernthesen	319
Anhang	320
A. IIA Standards	320
B. DIIR Standards	321
C. Internationale Best Practises	322
D. Nationale Best Practises	323
6. Managementprozess 3: Revision der Planung	327
6.1 Anforderungen an ein Planungssystem	327
6.2 Mehrjahresplanung	328
6.3 Budgetabstimmung	331

6.4	Planungsmodelle	332
6.4.1	Balanced Scorecard (BSC)	332
6.4.2	Planung als Vorwärtsbuchhaltung	337
6.4.3	Hockeystick-Planung	338
6.4.4	Rasenmäher-Methode	339
6.4.5	Sunk-Cost-Effekt	340
6.4.6	Target Costing	341
6.4.7	Marktanteils-/Marktwachstumsportfolio zur Entwicklung von Normstrategien	344
6.5	Kernthesen	348
	Anhang	348
A.	IIA Standards	348
B.	Nationale Best Practises	348
7.	Managementprozess 4: Revision der externen Berichterstattung	351
7.1	Die Träger der externen Berichterstattung	351
7.1.1	Investor Relations	352
7.1.2	Public Relations	357
7.1.3	Human Relations	360
7.2.	Externe Berichterstattung	363
7.2.1	Disclosure Committee	363
7.2.2	Geschäftsberichtsprüfung	368
7.2.3	Sonderberichte	372
7.3	Besonderheiten der Unternehmens-Website	376
7.3.1	Satzung, DCGK, Code of Ethics, Vision und Mission Statement	376
7.3.2	Aufbau des Unternehmens und Vorstellung der Entscheidungsträger in Vorstand und Aufsichtsrat	379
7.3.3	Analystenkonferenzen-/Roadshow-Präsentations- unterlagen	380
7.3.4	Protokolle der Q&A-Sessions der Analystenkonferenzen/ Roadshows	380
7.4.	Sonderfälle interner Berichterstattung	381
7.4.1.	Whistle Blowing	381
7.4.2.	Notfall- und Katastrophen-Management	382
7.4.3.	Unter Kuratel der SEC: US-Börsenaufsicht in deutschen Unternehmen	383
7.4.4.	Unter Kuratel der BaFin	384
7.5	Kernthesen	384
	Anhang	385
A.	IIA-Standards	385
B.	DIIR Standards	386
C.	International Best Practises	387

8. NGO-Regelungen zum Berichtswesen ESG	389
8.1 Global Reporting Initiative (GRI)	395
8.2 UN Global Compact (10 Principles)	398
8.3 ISO 26.000	403
8.4 EFFAS	404
8.5 Greenhouse Gas Protocol	404
8.6 Versuch gemeinsamer weltweiter ESG-Standards unter Führung des ISSB	407
8.7 Kernthesen	408
Anhang	409
A. IIA Standards	409
B. DIIR Standards	409
C. International Best Practises	409
D. National Best Practises	410
9. Managementprozess 5: Revision des Operativen Führungs- prozesses	413
9.1 Bedeutung und Inhalte eines Ethikkodexes	413
9.1.1 Begriff und Gegenstand der Ethik	413
9.1.2 Inhalt und Bedeutung des Ethikkodexes	416
9.1.3 Bestandteile des Ethikkodexes	418
9.2 Führungsgrundsätze	420
9.2.1 Leadership	420
9.2.2 Commitment	421
9.2.3 Klarheit und Wahrheit	423
9.2.4 Mitarbeiterzufriedenheit und Mitarbeiterbefragungen	424
9.3 Führungspsychologie	427
9.3.1 Rollenmodelle	427
9.3.2 Einheit von Verantwortung, Kompetenz und Aufgabe	430
9.3.3 Supervision	432
9.4 Führungsmodelle und Motivation	434
9.4.1 Management by Objectives	434
9.4.2 Management by Exception	438
9.4.3 Management by Walking Around	441
9.4.4 Führungsstile	443
9.5 Einstellungsprozess Top Management	450
9.5.1 Anforderungsprofil	451
9.5.2 Personalberatung	453
9.5.3 Bewerberauswahl	457
9.5.4 Bewerbungsgespräche	459
9.5.5 Einstellungsgespräche	462
9.6 Mitarbeiterorientierter Prozess (MOP)	463
9.6.1 Zielvereinbarungsgespräch	464
9.6.2 Beurteilungsgespräch	465
9.6.3 Gehaltsgespräch	466

9.6.4	360-Grad-Feedback	468
9.6.5	Weiterbildung	470
9.7.	Entlassungen	471
9.7.1	Außerordentliche Kündigungen	472
9.7.2	Outplacement	473
9.8.	Karriere- und Nachfolgeplanung	474
9.8.1	Förderprogramme (Führung und Führungsnachwuchs)	475
9.8.2.	Beförderungen/Old Boys Network/Förderlisten Organisationsänderungen/	475
9.9	Altersversorgung Top Management	476
9.10	Kernthesen	477
	Anhang	479
A.	IIA-Standards	479
B.	DIIR-Standards	480
C.	International Best Practises	480
D.	National Best Practises	482
10.	Managementprozess 6: Fusionen, Übernahmen und Verkäufe	485
10.1	Kerngeschäftsfelder, Randgeschäftsfelder und Ergänzungsgeschäftsfelder	485
10.2	Externes und Internes Wachstum, Wachstumspfade	488
10.3	Zusammenarbeit mit Investmentbanken und Kanzleien	493
10.4	Due Diligence	497
10.4.1	Begriff und Bedeutung von Due Diligence	497
10.4.2	Ziele, Bedeutung und Inhalt der Financial Due Diligence	498
10.4.3	Ziele, Bedeutung und Inhalt der Legal Due Diligence	502
10.4.4	Ziele, Bedeutung und Inhalt der Environmental Due Diligence	504
10.4.5.	Ziele, Bedeutung und Inhalt der Tax Due Diligence	505
10.4.6	Ziele, Bedeutung und Inhalt der Cultural Due Diligence	506
10.4.7	Ziele, Bedeutung und Inhalt der Management Due Diligence	509
10.5.	Prüfung von besonderen Geschäftseinheiten	511
10.5.1	Prüfung von Minderheitsgesellschaften	511
10.5.2	Prüfung von Joint Venture	513
10.5.3	Prüfung von Minderheitsgesellschaftern	517
10.5.4	Prüfung von Assoziierten Gesellschaften	523
10.5.5	Prüfung von Kleinen Kapitalgesellschaften/Kleinstkapitalgesellschaften	528
10.5.6	Prüfung von Mantelgesellschaften ohne operatives Geschäft	532
10.6	Kernthesen	535

11. Revision im Top Management und bei der Geschäftsführung	537
11.1 Notwendigkeit von Assessment	537
11.2 Externe und interne Assessments	538
11.2.1 360 Grad im Top Management als internes AC	539
11.2.2 Assessment Center im Topmanagement bei Fusionen als externes AC	539
11.2.3 Objektivität versus „Wohlgefallen“ bei Personalent- scheidungen	541
11.3.1 Management Override	544
11.3.2 Principal-Agent-Dilemma bei AGs	546
11.3.3 Grauzone privat – dienstlich	549
11.4 Kernthesen	552
Anhang	553
A. IIA-Standards	553
12. Management-Fraud	555
12.1. Red Flags	556
12.1.1. Anonyme Schreiben	559
12.1.2. Whistle Blower Prozess	560
12.1.3 Sammlung von Red Flags	562
12.2. Gesetzliche Grundlagen	572
12.2.1 Untreue (§ 266 StGB-Untreue)	573
12.2.2 Kollusion	574
12.2.3. Diebstahl von materiellem und immateriellen Vermögen	575
12.2.4 Urkundenfälschung (§ 267 StGB) und schriftliche Lüge	576
12.2.5 Bestechung und Vorteilsannahme (§ 108e, 299, 300, 331, 333–335 StGB)	577
12.2.6 Geldwäsche (§ 261 StGB und GWG nach 5. EU-Geldwäsche-Richtlinie)	579
12.3 Der DIIR-Standard Nr. 5 Anti-Fraud-Management	581
12.4 Fraud-Prophylaxe	581
12.4.1 Offene Unternehmenskultur ohne Hidden Agenda	582
12.4.2 Mitarbeiterbefragung zur Compliance von Führungskräften	583
12.5 Repression von dolosen Handlungen	584
12.5.1 Profiling des oder der Täter	584
12.5.2 Ermittlung des Schadens	585
12.5.3 Zusammenarbeit mit den ermittelnden Behörden	586
12.5.4 Rechtliche Maßnahmen	588
12.5.5 Rückführung des Vermögens	592
12.6 Kernthesen	595
Anhang	596
A. IIA-Standards	596
B. DIIR Standard Nr. 5	596

C.	International Best Practises (Fraud Report)	597
D.	Nationale Best Practices (Hinweise zum DIIR Nr. 5, Auszüge, eigene Ergänzungen)	597
Ausblick	601
Literaturverzeichnis	605
Glossar	631
Namensregister	639
Stichwortverzeichnis	651