

# 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
<b>1 Gründe für die Einrichtung einer Internen Revision .....</b>	<b>1</b>
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 <sup>DIIR</sup> .....	17
1.5. Kernthesen .....	18
<b>2 Abgrenzung der Internen Revision .....</b>	<b>21</b>
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

<b>3 Verhaltensgrundsätze (Code of Ethics) der IR</b>	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
<b>4 Standards bzw. Grundsätze des IIA und DIIR</b>	43
4.1 Zweck und Bedeutung der Grundsätze	43
4.2 Attribute Standards	45
4.3 Ausführungsstandards	53
4.4 Kernthesen	61
<b>5 Regelungen zur Internen Revision</b>	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	Problemgebiete von Risikomanagementsystemen .....	101
5.4.2	OECD und Corporate Governance .....	101
5.4.3	Transparency International und Fraud .....	103
5.5	Kernthesen .....	104
<b>6</b>	<b>Entwicklungstendenzen der Internen Revision .....</b>	<b>107</b>
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
<b>7</b>	<b>Strategie und Organisation der Internen Revision .....</b>	<b>119</b>
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	Dateianalysetools .....	181
7.6.4	Continuous Auditing (CA) .....	183
7.7	Kern-Prozesse der IR .....	185
7.8	Kernthesen .....	188
<b>Kapitelanhang 7</b>	.....	190
IIA-Standards	.....	190
DIIR-Standards	.....	199
A: Best Practices GAIN (IIA)	.....	202
B: Best Practices National	.....	203

<b>8 Risikoorientierte Revisionsplanung</b>	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
<b>Kapitelanhang 8</b>	250
A: IIA Standards	250
B: DIIR Standards	252
C: Best Practices GAIN (IIA)	253
D: Best Practices National	253

<b>9</b>	<b>Revisionsobjekt-(RO)-planung und Prüfungsarbeiten vor Ort</b>	<b>255</b>
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	$\alpha$ - und $\beta$ -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

<b>Kapitelanhang 9</b> .....	301
A: IIA Standards .....	301
B: DIIR Standards .....	305
C: Best Practices National .....	306
<b>10 Berichterstattung</b> .....	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

<b>Kapitelanhang 10</b> .....	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
<b>11 Qualitätsmanagement in der IR</b> .....	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
<b>Kapitelanhang 11</b> .....	388
A: IIA Standards .....	388
B: DIIR-Standards .....	390
C: Best Practices (GAIN) .....	391



<b>12 Die Interne Revision in ihrer Außenansicht, national und international</b>	<b>393</b>
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