

Helfer/Geiersbach/Riediger/Hanenberg

# Interne Kontrollsysteme in Banken und Sparkassen

- Vorgaben & Erwartungen der Bankenaufsicht
- Schlüsselkontrollen implementieren & optimieren
- Kontrollrahmen & Risikoanalysen
- Prüfung & Kontrolltests

3. Auflage

Zitiervorschlag:

*Autor* in: Helfer/Geiersbach/Riediger/Hanenberg (Hrsg.), Interne  
Kontrollsysteme in Banken und Sparkassen, 3. Auflage, RdNr. XX.

ISBN: 978-3-943170-89-4  
© 2020 Finanz Colloquium Heidelberg GmbH  
Im Bosseldorn 30, 69126 Heidelberg  
[www.FCH-Gruppe.de](http://www.FCH-Gruppe.de)  
[info@FCH-Gruppe.de](mailto:info@FCH-Gruppe.de)  
Satz: MetaLexis, Niedernhausen  
Druck: VERLAGSDRUCKEREI SCHMIDT GMBH,  
Neustadt an der Aisch

Helfer/Geiersbach/Riediger/Hanenberg

# Interne Kontrollsysteme in Banken und Sparkassen

- **Vorgaben & Erwartungen der Bankenaufsicht**
- **Schlüsselkontrollen implementieren & optimieren**
- **Kontrollrahmen & Risikoanalysen**
- **Prüfung & Kontrolltests**

**3. Auflage**

**Ralf Barsch**

Geschäftsführer,  
Advanced Audit Solutions

**Dirk Bolte**

WP/StB, stv. Revisionsdirektor, Prüfungsstelle des  
Hanseatischen Sparkassen- und Giroverbandes, Hamburg

**Jürgen Büschelberger**

Leiter des Regionalbereichs Banken und Finanzaufsicht  
Hauptverwaltung Bayern, Deutsche Bundesbank

**Michael Claaßen**

Bereichsleiter Interne Revision,  
Volksbank Marl-Recklinghausen eG

**Dr. Karsten Geiersbach, CIA (Hrsg.)**

CIA, Bereichsleiter Interne Revision,  
Kasseler Sparkasse

**Ludger Hanenberg (Hrsg.)**

Abteilungsleiter Grundsatzabteilung der Versicherungsaufsicht,  
Bundesanstalt für Finanzdienstleistungsaufsicht

**Michael Helfer (Hrsg.)**

Geschäftsführer,  
FCH Consult GmbH

**Björn Reher**

Wirtschaftsprüfer/Steuerberater,  
Partner Financial Services/Gesellschafter,  
Mazars GmbH & Co. KG

**Henning Riediger (Hrsg.)**

Prüfungsleiter im Referat Bankgeschäftliche Prüfungen bei  
der Hauptverwaltung, Deutsche Bundesbank, Hannover

**Pascal Ritz**

Geschäftsführer,  
Justo Unternehmensberatung GmbH

**Dr. Stefan Scheve**

Sachgebietsleiter Laufende Aufsicht Sparkassen,  
Deutsche Bundesbank Hauptverwaltung  
Bremen, Niedersachsen und Sachsen-Anhalt

**Marc Stränger**

Sparkassenbetriebswirt, Abteilungsleiter Compliance,  
Sparkasse Krefeld

**Lukas Walla**

Mitarbeiter Regulatorik/Compliance in der  
Investitionsbank Schleswig-Holstein



## Inhaltsübersicht

<b>Vorwort der Herausgeber</b>	<b>1</b>
<b>A. Bedeutung des IKS für die Bankenaufsicht</b>	<b>5</b>
<b>B. Aktuelle Entwicklungstendenzen und Standardisierungsmodelle</b>	<b>229</b>
<b>C. Rollen im IKS (Aufgaben, Kompetenzen, Verantwortlichkeiten)</b>	<b>301</b>
<b>D. IKS-Anforderungen für die Bankprozesse</b>	<b>357</b>
<b>E. IKS als Kontrollrahmen für die Compliance-Funktion</b>	<b>731</b>
<b>F. IKS als zentrales Prüffeld für die Interne Revision</b>	<b>751</b>
<b>G. IKS aus Sicht des Dienstleisters in Auslagerungsunternehmen</b>	<b>887</b>
<b>H. Das Interne Kontrollsystem aus Sicht der Wirtschaftsprüfung</b>	<b>895</b>
<b>I. Autorenverzeichnis</b>	<b>1021</b>
<b>J. Literaturverzeichnis</b>	<b>1027</b>
<b>K. Abbildungsverzeichnis</b>	<b>1049</b>
<b>L. Stichwortverzeichnis</b>	<b>1057</b>





# Inhaltsverzeichnis

<b>Vorwort der Herausgeber</b>	<b>1</b>
<b>A. Bedeutung des IKS für die Bankenaufsicht</b>	<b>5</b>
I.    Europäische Bankenaufsicht – Umsetzung des SREP ( <i>Hanenberg</i> )	7
1.    Einführung	7
2.    EBA-Leitlinien über interne Unternehmensführung	8
a)    Internes Kontrollsystem (IKS), Kontrolleinheiten und Verantwortlichkeiten	8
b)    Umgang mit Risiken und Risikokonzentrationen	11
c)    Ausstattung der Leitung der Risikokontrollfunktion (CRO)	11
d)    Risikoberichterstattung	12
e)    Festlegung von Compliance-Richtlinien und Sicherstellung einer effektiven Compliance-Funktion	13
f)    Rolle der Risikokontrollfunktion im Neu-Produkt- Prozess	14
3.    Interne Revision im SREP	14
a)    Einrichtung gemäß den nationalen und internationalen berufsständischen Normen	14
b)    Revisions-Charta und Schutz der organisatorischen Unabhängigkeit und Objektivität der Revision	15
c)    Ressourcenmanagement der Internen Revision	16
d)    Risikoorientierte Prüfungsplanung	16
e)    Bestimmung der Einhaltung interner Vorschriften und externer Vorgaben sowie Maßnahmen zur Nachverfolgung bei Abweichungen	17
4.    Fazit	17
II.   IKS-Grundlagen im internationalen Kontext und Bedeutung des IKS für die Bankenaufsicht ( <i>Büschelberger</i> )	19
1.    IKS-Grundlagen im internationalen Kontext	19
2.    Bedeutung des IKS für die Bankenaufsicht	30

a)	Neue »Philosophie«: mehr qualitative und präventive Bankenaufsicht	30
b)	Internes Kontrollsystem als »Eckstein« der laufenden Beaufsichtigung der Institute	34
c)	Bankgeschäftliche Prüfungen	38
d)	Bankaufsichtliche Anforderungen an das IKS	40
III.	Aufsichtliche Anforderungen an das Interne Kontrollsystem im IT-Bereich ( <i>Riediger</i> )	43
1.	Vorbemerkungen zur Bedeutung des Internen Kontrollsystems bei IT-bezogenen Prozesskomponenten	43
2.	Grundsätzliche Überlegungen zum Management von IT-Risiken	45
a)	Strategische Vorgaben zum Umgang mit IT-Risiken	52
b)	Risikoinventur im IT-Bereich	53
c)	Informationsrisikomanagement	58
d)	Benutzerberechtigungen	84
e)	Individuelle Datenverarbeitung auf Trägersystemen	90
f)	Business Continuity-Maßnahmen	92
3.	Fazit und Ausblick	95
IV.	Performance-Anforderungen an die Interne Revision und Erkenntnisse aus externen Prüfungen ( <i>Reber</i> )	98
1.	Einbindung der Internen Revision in das interne Kontrollsystem	98
2.	Grundlage für die Einrichtung einer Internen Revision in Kreditinstituten	98
3.	Prüfungsmaßstab	99
4.	Aufgaben der Internen Revision	101
a)	Aufgabenspektrum	101
b)	Projektbegleitung	102
c)	Prüfungspflicht bei Auslagerungen	102
5.	Grundsätze der Internen Revision	103
a)	Rolle der Revision und internen Kommunikation	103
b)	Unabhängigkeit und Objektivität	103
c)	Persönliche Unabhängigkeit	104

d)	Geschäftsordnung und Revisionshandbuch	105
e)	Wertung der Prüfungsergebnisse und Berichterstattung	107
f)	Beeinträchtigung von Unabhängigkeit und Objektivität	107
g)	Fachkompetenz und berufliche Sorgfalt	108
6.	Prüfungsplanung und -durchführung	111
a)	Allgemeine Ausführungen	111
b)	Prozess der risikoorientierten Prüfungsplanung	112
c)	Kapazitätsplanung	114
d)	Prüfungsturnus	114
e)	Prüfungsmethoden und -arten	115
f)	Prüfungsprozess	115
7.	Überprüfung und Weiterentwicklung der Konzepte	120
a)	Überprüfung der Prüfungsplanung und -methoden	120
b)	Sicherstellung der Prüfungsqualität	121
8.	Berichtspflicht	124
a)	Schriftliche Fixierung und Vorlage der Prüfungsberichte	124
b)	Mängelkategorisierung	126
c)	Qualitative Beurteilung der Berichterstattung	126
d)	Zeitnahe Erstellung der Prüfungsberichte	126
9.	Reaktion auf festgestellte Mängel	127
V.	Vorgaben der MaRisk und Feststellungen im Rahmen von Prüfungen nach § 44 KWG zur Tätigkeit der Internen Revision ( <i>Scheve</i> )	129
1.	Grundlegende Bedeutung der Internen Revision	129
2.	Revisionsfunktion	131
3.	Prüfungsplanung und -durchführung der Internen Revision	140
4.	Berichtspflicht der Internen Revision	141
5.	Reaktion der Internen Revision auf festgestellte Mängel	143
6.	Schlusswort	145

VI.	Umsetzung der SREP-Leitlinie in der Internen Revision ( <i>Claaßen</i> )	147
1.	Einleitung	147
2.	Vergleich der SREP-Leitlinien	154
3.	Vergleich der Anforderungen an die Revision entsprechend der SREP-Leitlinien	158
4.	Internationale Standards zur Internen Revision	169
a)	IIA-Standards	169
b)	Implementierung der IIA-Standards in die Revisionsprozesse	171
c)	Umsetzungen zu den IIA-Standards	177
d)	Weitere Hinweise zur Aufbau- und Ablauforganisation	186
5.	Dokumentation im Rahmen der IIA-Standards	188
a)	Musterprüfungsbericht	188
b)	Arbeitspapiere	190
6.	Fazit	194
VII.	Risikokultur als zentrale Grundlage für das IKS ( <i>Ritz</i> )	196
1.	Die Risikokultur – eine lohnenswerte Herausforderung	196
2.	Abgrenzung Unternehmenskultur, Compliancekultur, Risikokultur	199
3.	Mehrwerte einer zielführenden Risikokultur	201
4.	Empfehlung für eine organisatorische Zuständigkeit	202
5.	Hilfsmittel für die Risikokultur	204
a)	Verhalten	204
b)	Kommunikation	205
c)	Anreizsysteme	207
d)	Nachhaltigkeit	207
6.	Auswirkung der Risikokultur auf die Prozessrisiken	208
a)	Steuerungsprozesse	209
b)	Geschäftsprozesse	210
c)	Unterstützungsprozesse	210
7.	Praxisumsetzung	210
a)	Entwicklung einer Risikokultur	210

b) Integration einer angemessenen Risikokultur	211
c) Förderung der Risikokultur	212
8. Bewertung der vorherrschenden Risikokultur	213
a) Internes Unternehmensumfeld	215
b) Information und Kommunikation	215
c) Zielsetzungsprozess	216
d) Ereignisinventur	217
e) Risikobeurteilung	217
f) Risikomaßnahmen	218
g) Kontroll- und Steuerungsaktivitäten	218
h) Überwachung	219
9. Fazit	219
VIII. Kontroll-, Unternehmens- und Risikokultur als Basis eines tragfähigen Geschäftsmodells ( <i>Barsch</i> )	221
1. Kontrollkultur	221
2. Unternehmens- und Risikokultur	222
3. »Lösungskultur« bzw. tragfähiges Geschäftsmodell	225
4. Fazit	226
<b>B. Aktuelle Entwicklungstendenzen und Standardisierungsmodelle (<i>Helper</i>)</b>	<b>229</b>
I. Bankaufsichtliche Anforderungen an das IKS	231
1. SREP – Supervisory Review and Evaluation Process (aufsichtlicher Überprüfungs- und Bewertungsprozess)	231
2. Bankaufsichtliche Anforderungen nach § 25a KWG	236
a) Einleitung	236
b) Anforderungen an das Risikomanagement	240
c) Anforderungen an eine angemessene personelle Ausstattung	245
d) Anforderungen an ein angemessenes, transparentes und nachhaltiges Vergütungssystem	247
e) Anforderungen an eine angemessene technisch-organisatorische Ausstattung sowie an das Notfallkonzept	249

f)	Anforderungen an die Dokumentation der Geschäftstätigkeit	254
II.	Anerkannte Standardisierungsmodelle	256
1.	SOX-Sarbanes-Oxley Act (SOA)	256
2.	COSO-Modell 1992/94 (COSO I)	259
3.	COSO ERM 2004 (COSO II)	264
4.	COSO Guidance on Monitoring IKS	268
5.	COSO Internal Control 2014	270
6.	COSO Enterprise Risk Management Integrating with Strategy and Performance (2017)	278
7.	COBIT	280
8.	Standardisierungshilfen für das IKS	283
a)	Darstellung von 8 Kontroll-Bausteinen als Strukturierungshilfe	283
b)	Bereichsübergreifende Kontroll-Bausteine	284
c)	Bereichsspezifische Kontroll-Bausteine	293
<b>C.</b>	<b>Rollen im IKS (Aufgaben, Kompetenzen, Verantwortlichkeiten)</b> <b>(Helfer)</b>	<b>301</b>
I.	Modell der 3 Verteidigungslinien (3 LoD bzw. TLoD)	303
II.	Geschäftsleitung	315
1.	Die ordnungsgemäße Geschäftsorganisation als zentraler Maßstab	315
2.	Wechselwirkungen mit den Strategien gemäß MaRisk	318
3.	Grundsätzliche Vorgaben in Bezug auf das Kontrollumfeld	320
4.	Aufgaben	321
5.	Kompetenzen	322
6.	Verantwortlichkeiten	322
III.	Aufsichts-/Verwaltungsrat	325
1.	Aufgaben	325
2.	Kompetenzen	327

3. Verantwortlichkeiten	328
IV. Prozessverantwortliche/Fachbereiche	329
V. MaRisk-Compliance	335
VI. WpHG-Compliance	340
VII. Geldwäschebeauftragter/Zentrale Stelle	345
VIII. Informationssicherheitsbeauftragter	347
IX. Datenschutzbeauftragter	348
X. Auslagerungsbeauftragter	349
XI. Risikocontrolling	350
XII. IKS-Evidenz	351
XIII. Interne Revision	354
<b>D. IKS-Anforderungen für die Bankprozesse</b>	<b>357</b>
I. Rahmenbedingungen für ein internes Kontrollsystem ( <i>Helfer</i> )	359
1. IKS-Ziele	359
2. IKS-Grundlagen	359
3. Ableitung der Kontrollanforderungen aus der Geschäftsstrategie und den Risikostrategien auf die Prozessebene	360
4. IKS-Management	361
a) Grundlagen IKS-Management und Übersicht der IKS-Management-Instrumente	361
b) IKS-Kontrollumfeld	364
c) IKS-Risikobewertung	371
d) IKS-Kontrollaktivitäten	372
e) IKS-Monitoring (Überwachungsaktivitäten)	377
f) Maßnahmenverfolgung	381
g) IKS-Berichterstattung	381
II. Kontrollen ( <i>Helfer</i> )	385
1. Vorbemerkung	385
2. Allgemeine Begriffsdefinition und Kontrollarten	389

3.	Wirkungsgrad von Kontrollen	390
4.	Kontrollziele	393
5.	Kontrollhandlungen und Festlegung der Kontrollspanne	394
6.	Schlüsselkontrollen	396
7.	Dokumentation der Kontrollen	398
	a) Dokumentation der implementierten Kontrollen	398
	b) Dokumentation der Kontrollhandlungen	400
8.	Reifegrad von Kontrollen	400
III.	Bewertung von Prozessen und Kontrollen ( <i>Helfer</i> )	405
1.	Prozesslandkarten	405
2.	Bewertungskriterien	407
3.	Risikoanalysen nach AT 8.2 MaRisk	417
IV.	Aufbauorganisatorische Schlüsselkontrollen ( <i>Helfer</i> )	426
V.	Ablauforganisatorische Schlüsselkontrollen	433
1.	Risikomanagement ( <i>Geiersbach</i> )	433
	a) Strategie	433
	b) Kapitalplanung	450
	c) Risikotragfähigkeit	455
	d) Adressenausfallrisiko	465
	e) Marktpreisrisiko, insbes. des Handelsbuches	472
	f) Liquiditätsrisiko	497
	g) Operationelles Risiko	519
	h) Stresstest	543
	i) Berichterstattung	550
2.	Unternehmenssteuerung ( <i>Helfer</i> )	560
	a) Prozesssteckbrief	560
	b) Regulatorische Anforderungen	561
	c) Inhärente Risiken	562
	d) Teilprozesse und Kontrollen	562
	e) Spezifische Risiken im Prozess	564
3.	IKS-Management ( <i>Helfer</i> )	565
	a) Prozesssteckbrief	565
	b) Regulatorische Anforderungen	566



c)	Inhärente Risiken	566
d)	Teilprozesse und Kontrollen	566
e)	Spezifische Risiken im Prozess	567
4.	Kreditgeschäft ( <i>Geiersbach</i> )	568
a)	Prozesssteckbrief	568
b)	Regulatorische Anforderungen	599
c)	Inhärente Risiken	600
d)	Teilprozesse und Kontrollen	600
e)	Spezifische Risiken im Prozess	602
5.	Wertpapiergeschäft ( <i>Helfer</i> )	606
a)	Prozesssteckbrief	606
b)	Regulatorische Anforderungen	609
c)	Inhärente Risiken	610
d)	Teilprozesse und Kontrollen	611
e)	Spezifische Risiken im Prozess	615
6.	Handelsgeschäft ( <i>Helfer</i> )	616
7.	Depotgeschäft ( <i>Helfer</i> )	616
a)	Prozesssteckbrief	616
b)	Regulatorische Anforderungen	618
c)	Inhärente Risiken	619
d)	Teilprozesse und Kontrollen	619
e)	Spezifische Risiken im Prozess	622
8.	Auslandsgeschäft ( <i>Helfer</i> )	625
a)	Prozesssteckbrief	625
b)	Regulatorische Anforderungen	626
c)	Inhärente Risiken	626
d)	Teilprozesse und Kontrollen	627
e)	Spezifische Risiken im Prozess	628
9.	Passivgeschäft ( <i>Helfer</i> )	630
a)	Prozesssteckbrief	630
b)	Regulatorische Anforderungen	631
c)	Inhärente Risiken	631
d)	Teilprozesse und Kontrollen	632
e)	Spezifische Risiken im Prozess	633

10. Zahlungsverkehr ( <i>Helfer</i> )	633
a) Prozesses Steckbrief	633
b) Regulatorische Anforderungen	636
c) Inhärente Risiken	637
d) Teilprozesse und Kontrollen	638
e) Spezifische Risiken im Prozess	641
11. Kassenverkehr ( <i>Helfer</i> )	641
a) Prozesses Steckbrief	641
b) Regulatorische Anforderungen	642
c) Inhärente Risiken	643
d) Teilprozesse und Kontrollen	643
e) Spezifische Risiken im Prozess	644
12. Personal ( <i>Helfer</i> )	644
a) Prozesses Steckbrief	644
b) Regulatorische Anforderungen	646
c) Inhärente Risiken	647
d) Teilprozesse und Kontrollen	647
e) Spezifische Risiken im Prozess	648
13. Rechnungswesen ( <i>Helfer</i> )	649
a) Prozesses Steckbrief	649
b) Regulatorische Anforderungen	663
c) Inhärente Risiken	663
d) Teilprozesse und Kontrollen	664
e) Spezifische Risiken im Prozess	665
14. Meldewesen ( <i>Helfer</i> )	666
a) Prozesses Steckbrief	666
b) Regulatorische Anforderungen	669
c) Inhärente Risiken	670
d) Teilprozesse und Kontrollen	670
e) Spezifische Risiken im Prozess	670
15. Informationstechnologie (IT) ( <i>Helfer</i> )	672
a) Prozesses Steckbrief	672
b) Regulatorische Anforderungen	673
c) Inhärente Risiken	674
d) Teilprozesse und Kontrollen	674
e) Spezifische Risiken im Prozess	681

16. Prozess Auslagerung ( <i>Walla</i> )	684
a) Prozesses Steckbrief	684
b) Regulatorische Anforderungen	685
c) Inhärente Risiken	685
d) Teilprozesse und Kontrollen	686
e) Spezifische Risiken im Prozess	688
17. Compliance ( <i>Helfer</i> )	697
b) Regulatorische Anforderungen	699
c) Inhärente Risiken	699
d) Teilprozesse und Kontrollen	700
e) Spezifische Risiken im Prozess	700
18. Geldwäsche-/Betrugspävention ( <i>Helfer</i> )	701
a) Prozesses Steckbrief	701
b) Regulatorische Anforderungen	703
c) Inhärente Risiken	704
d) Teilprozesse und Kontrollen	704
e) Spezifische Risiken im Prozess	707
19. Datenschutz ( <i>Helfer</i> )	716
a) Prozesses Steckbrief	716
b) Regulatorische Anforderungen	719
c) Inhärente Risiken	719
d) Teilprozesse und Kontrollen	720
e) Spezifische Risiken im Prozess	722
20. Interne Revision ( <i>Helfer</i> )	723
a) Prozesses Steckbrief	723
b) Regulatorische Anforderungen	725
c) Inhärente Risiken	726
d) Teilprozesse und Kontrollen	726
e) Spezifische Risiken im Prozess	729

<b>E. IKS als Kontrollrahmen für die Compliance-Funktion</b>	
<b>(Stränger)</b>	<b>731</b>
I. Durchführung geeigneter Fachbereichskontrollen durch die Compliance-Funktion (CoF)	733
II. Wirksamkeit von Stichprobenkontrollen	735

III.	Festlegung von Mindest-Stichprobengrößen	736
IV.	Würdigung der Wirksamkeit von Kontrollen	737
V.	Die Gefährdungsanalyse als Ergebnispool	738
VI.	Kontrollplan, Defizitmanagement und Periodizität	740
VII.	Dokumentationserfordernisse: Schaffung von einheitlichen Standards	741
VIII.	Kontrolltätigkeit: Risikoorientierte Bestimmung von Vor-Ort-Kontrollen und analytischen Kontrollhandlungen	743
IX.	Compliance und Interne Revision: Koordination der Überwachungs- und Kontrollhandlungen	748
<b>F.</b>	<b>IKS als zentrales Prüffeld für die Interne Revision (<i>Helfer</i>)</b>	<b>751</b>
I.	Strategische Positionierung der Internen Revision	753
1.	Externe Vorgaben und Hilfestellungen im Kontext IKS	753
a)	Bankenaufsicht	753
b)	IIA-Standards (Internationale Grundlagen für die berufliche Praxis der Internen Revision)	759
2.	Aktuelle Handlungsfelder für die Interne Revision	761
3.	Risikoorientierung als maßgebliche Anforderung	765
4.	Erfolgsstorys für die Interne Revision	767
a)	Erfolgsstory 1: Einbindung von Vorstand und Key Playern in den Prozess der Jahresplanung und der Risikoanalyse	767
b)	Erfolgsstory 2: Verstärkung der ex ante-Maßnahmen	768
c)	Erfolgsstory 3: Aktives Anbieten von Beratung	769
d)	Erfolgsstory 4: Bekanntgabe der Jahresplanung	770
e)	Erfolgsstory 5: Beziehungsmanagement	771
f)	Erfolgsstory 6: Rollenbasiertes Verhalten der Internen Revision	771
g)	Erfolgsstory 7: Standardisierte Berichte (kurz und knapp!)	772
h)	Erfolgsstory 8: Personalauswahl	773

i)	Erfolgsstory 9: Berichterstattung im Aufsichtsgremium	773
j)	Erfolgsstory 10: Kontinuierliche Verbesserung der Revisionsprozesse	774
5.	Beratung durch die Interne Revision	778
6.	Personelle Anforderungen	782
7.	Entwicklung einer Revisionsstrategie	785
8.	Blick in die Zukunft	788
II.	Ganzheitlicher Revisionsprozess mit Fokussierung auf das IKS	789
1.	Prozessbezogenes Prüfungsuniversum als zentrale Grundlage	789
2.	Überblick über den Revisionsprozess	793
3.	Prozessorientierte Aufbauorganisation	794
4.	IKS-relevante Informationsgewinnung	795
a)	Einleitung	795
b)	Informationspflichten an die Interne Revision	795
c)	Zusätzliche Informationsbeschaffung durch die Interne Revision	797
d)	Risk Control Self Assessment (RCSA) als revisionsunterstützendes Verfahren	800
e)	Dokumentation	802
III.	Planungsprozess	802
1.	Ablauf des Planungsprozesses	802
2.	Jahresplanung – Einschätzung des IKS auf Institutsebene	803
a)	Allgemeine Anforderungen	803
b)	Inhärente Risiken	805
c)	Kontrollrisiken	807
d)	Entdeckungsrisiko	808
e)	Informationsquellen	809
f)	Beurteilung des Fehlerrisikos anhand des COSO II-Modells	809

3.	Jahresplanung – Einschätzung des IKS auf Prüffeld- Ebene	812
a)	Grundlagen für die Einschätzung durch die Interne Revision	812
b)	Festlegung von Risikofaktoren	813
c)	Planungsgespräche mit den verantwortlichen Führungskräften	815
d)	Real Time-Revision: Kontinuierliche Anpassung der Risikoeinschätzung	816
e)	Entwicklung einer IKS-Prüfungsstrategie	817
IV.	Prüfungsprozess	818
1.	Prüfungsplan	818
2.	Prüfung der Schlüsselkontrollen und Öffnungsklauseln	820
3.	IKS-Prüfungs-Checkliste	824
4.	Prüfungsarten	824
5.	Prozess-/Systemprüfung	826
a)	Vorgehensweise bei einer Prozessprüfung	826
b)	Prozessorientierte Wirtschaftlichkeitsprüfungen	832
6.	Aussagebezogene Prüfungshandlungen	838
a)	Analytische Prüfungshandlungen	839
b)	Einzelfallprüfungen	840
7.	Stichproben als Grundlage für eine IKS- Angemessenheitsaussage	840
8.	Einzelengagementprüfungen zum Adressenausfallrisiko	844
9.	Prüfung der Führungswirkung als wesentlicher Teil einer IKS-Prüfung	845
10.	Ex ante-Tätigkeiten/-Prüfungen	846
a)	Vorbemerkung	846
b)	Begleitung wesentlicher Projekte	847
c)	Begleitung von Produkteinführungen	855
d)	Begleitung von Auslagerungen	857
e)	Begleitung von Änderungen betrieblicher Prozesse oder Strukturen	861
V.	Mängelklassifizierung	862

VI.	Berichterstattung	868
1.	Einführung	868
2.	Allgemeine Berichtsanforderungen	870
3.	Umgang mit wesentlichen und schwerwiegenden Mängeln während der Prüfung	871
4.	Hervorheben des IKS im Prüfungsbericht	871
a)	Darstellung im Berichtsteil	871
b)	Darstellung des IKS im Management Summary	873
5.	IKS-Darstellung im Quartals- und Jahresbericht	874
6.	Zusammenarbeit mit dem Aufsichtsorgan	876
VII.	Follow-up-Prozess: Maßnahmenverfolger oder Veränderungsbegleiter?	879
VIII.	Dokumentation	881
 <b>G. IKS aus Sicht des Dienstleisters in Auslagerungsunternehmen (Walla)</b>		 <b>887</b>
I.	Besondere Anforderungen an Dienstleister	889
II.	Nachweis eines angemessenen IKS	891
III.	Auswirkungen auf die Dienstleister-Revision	892
 <b>H. Das Interne Kontrollsystem aus Sicht der Wirtschaftsprüfung (Bolte)</b>		 <b>895</b>
I.	Die Prüfung des Internen Kontrollsystems bei Jahresabschlussprüfungen	897
1.	Prüfungstechnik im Zusammenhang mit dem Internen Kontrollsystem	897
a)	Ausrichtung der Abschlussprüfung	897
b)	Das Prüfungsrisikomodell	901
c)	Das Interne Kontrollsystem als Grundlage der risikoorientierten Abschlussprüfung	905
d)	Feststellung und Beurteilung von Fehlerrisiken	918
e)	Reaktionen auf beurteilte Fehlerrisiken	933

2.	Erläuterungen zu den für Kreditinstitute geltenden ergänzenden Vorschriften zur Rechnungslegung und Prüfung als gesetzlicher Rahmen für die Beurteilung des Internen Kontrollsystems	944
II.	Einzelne Prüfungsstandards und Internes Kontrollsystem	948
1.	Überblick zu Prüfungsstandards und Internem Kontrollsystem im Unternehmen	948
2.	Die Beurteilung des Risikomanagements von Kreditinstituten im Rahmen der Abschlussprüfung (IDW PS 525)	951
3.	Die Prüfung des Risikofrüherkennungssystems als Teilbereich des Internen Kontrollsystems (IDW PS 340)	957
4.	Feststellung und Beurteilung von Fehlerrisiken einschließlich Verständnis des Internen Kontrollsystems sowie Reaktionen des Abschlussprüfers (IDW PS 261)	959
5.	Internes Kontrollsystem und Fraud: Aufdeckung von Unregelmäßigkeiten im Rahmen der Abschlussprüfung (IDW PS 210)	961
6.	Interne Revision als wesentlicher Bestandteil des Internen Kontrollsystems und der Abschlussprüfung (IDW PS 321)	969
7.	Prüfungsnachweise zum Internen Kontrollsystem im Rahmen der Abschlussprüfung (IDW E-PS 300 n. F.)	971
8.	Repräsentative Auswahlverfahren (Stichproben) in der Abschlussprüfung (Überblick zu IDW PS 310)	975
9.	Internes Kontrollsystem bei der Prüfung der Adressenausfallrisiken und des Kreditgeschäfts von Kreditinstituten (IDW PS 522)	983
10.	Prüfung von Compliance-Management-Systemen (IDW PS 980)	987
11.	Die Prüfung des Internen Kontrollsystems bei Dienstleistungsunternehmen (IDW PS 951 n. F.)	996



12. Prüfungsgrundsätze mit der Beurteilung des Internen Kontrollsystems unter Einsatz von Informationstechnologie	1005
a) Abschlussprüfung und Internes Kontrollsystem unter Einsatz von Informationstechnologie (IDW PS 330)	1005
b) Abschlussprüfung und Beurteilung des Internen Kontrollsystems bei teilweiser Auslagerung der Rechnungslegung auf Dienstleistungsunternehmen (IDW PS 331)	1009
III. Die Prüfungsberichtsverordnung (PrüfbV) in Verbindung mit Abschlussprüfung und Internem Kontrollsystem	1012
<b>I. Autorenverzeichnis</b>	<b>1021</b>
<b>J. Literaturverzeichnis</b>	<b>1027</b>
<b>K. Abbildungsverzeichnis</b>	<b>1049</b>
<b>L. Stichwortverzeichnis</b>	<b>1057</b>



## Vorwort der Herausgeber

Die Entwicklung des Internen Kontrollsystems (IKS) im Bankensektor wurde in den letzten 25 Jahren laufend weiterentwickelt. Insbesondere durch die aufgetretenen Schieflagen und Unregelmäßigkeiten in Kreditinstituten resultierend in oder aus der Finanzmarktkrise 2007, steht das IKS ständig im Mittelpunkt der Gesetzgebung und der aufsichtsrechtlichen Vorschriften. Dies führte im Laufe der Entwicklung zu immer weitergehenden Verschärfungen in den gesetzlichen und bankaufsichtlichen Vorgaben, so dass nunmehr (überfällig) die 3. Auflage dieses Werkes erfolgt.

Während die 1. und 2. Auflage noch durch das Herausgeber-Duo Helfer/Ullrich begleitet wurden, erfolgte nun eine Veränderung im Herausgeber-Team sowie die Erweiterung des Autorenteam um erfahrene Bankexperten. An dieser Stelle gebührt unser Dank Herrn *Walter Ullrich*, der als Mit-Herausgeber die 1. und 2. Auflage mit viel Engagement und Leidenschaft begleitet hat. Er befindet sich mittlerweile im verdienten Ruhestand und stand somit für eine neue Auflage leider nicht mehr zur Verfügung.

Mit der nun vorliegenden 3. Auflage wird die Grundidee dieses Buches weiter vorangetrieben. Im Kern soll eine Zusammenführung der in den unterschiedlichen Bereichen enthaltenen IKS-Anforderungen und Risikoanalysen zu einem Gesamtsystem im Rahmen eines ganzheitlichen Risikomanagementsystems dargestellt werden. Dabei spannt sich der Bogen von den international beeinflussenden Modellen (insbesondere COSO) über die gesetzlichen und bankaufsichtlichen Vorgaben (zunehmend verschärft durch die europäischen Anforderungen) bis hin zu praxisorientierten Lösungsansätzen. Abgerundet wird das Thema durch interne und externe (Prüfungs-)Tipps. Hilfreich waren dabei die zahlreich vorhandenen literarischen Quellen als Grundlagen für unsere Ausführungen, den jeweiligen Autoren danken wir für ihre fundierten Aussagen und Anregungen.

Im Kern kann man sagen, dass in den letzten Jahren Umfang und auch Qualität der regulatorischen Anforderungen weiter zugenommen haben. Zudem werden die kommenden Jahre das »Zeitalter der Aufsicht« sicher noch ausdehnen. Besonders hervorzuheben sind die SREP-Neuerungen sowie die vergangenen und bereits angekündigten Anpassungen der MaRisk. Hier ist anzumerken, dass die MaRisk wie auch in der Vergangenheit den einschlägigen europäischen und internationalen Vorgaben folgen. Insbesondere der Prozess der Übernahme von Leitlinien der europäischen Aufsichtsgremien

EBA, ESMA und EIOPA ist weiter strukturiert worden. So hat z. B. die BaFin im Mai 2019 das Protokoll der Sitzung des Fachgremiums MaRisk vom 05.11.2018 auf die Homepage der BaFin gestellt. Darin wird u. a. ausgeführt, dass »im Regelfall davon ausgegangen werden kann, dass die BaFin die Leitlinien der EBA, der ESMA und der EIOPA in ihre Verwaltungspraxis übernimmt. Soll eine Leitlinie der EU-Behörden ausnahmsweise nicht oder – was in der Praxis eher vorkommt – nicht vollständig (etwa aufgrund von Konflikten mit deutschen gesellschaftsrechtlichen Regelungen) übernommen werden, benennt die BaFin diese Leitlinien auf ihrer Homepage. Im Einzelfall kann für die Übernahme in das deutsche Aufsichtsrecht ein Rechtsakt erforderlich sein (z. B. der Erlass oder die Änderung einer Verordnung). Für den Fall der Umsetzung durch ein Rundschreiben oder die Novellierung eines Rundschreibens müssten die LSIs die hieraus resultierenden Anforderungen aus der Guideline dann in der Tat erst mit der Veröffentlichung des nationalen Rundschreibens anwenden. Auch dann seien die LSIs aber gehalten, sich bereits vorher mit dem Inhalt der betreffenden (und regelmäßig auch in der deutschen Amtssprache vorliegenden) Leitlinien zu befassen und organisatorische Vorkehrungen zu treffen, um die hierin adressierten Anforderungen umzusetzen«. Daher sollten sich die Institute frühzeitig mit neuen europäischen Entwicklungen, primär denen bei der EBA, auseinandersetzen. Dies wird insbesondere die kleineren bis mittleren Institute vor große Herausforderungen stellen. Umso mehr wird es darauf ankommen, die bestehenden Systeme mit den aktuellen und den künftigen Anforderungen in einer sinnvollen, sprich ganzheitlichen, Art und Weise zu verbinden.

Letztlich sollte ein wirksames und hinreichend dokumentiertes IKS nicht nur im Interesse der Bank sein, es steht auch im Fokus der Bankenaufsicht und der Abschluss-/Sonderprüfer. Die nach § 25a KWG geforderte IKS-Wirkungsüberwachung (Regel-Einhaltung) kann bei Organisationsmängeln zudem harte Konsequenzen nach sich ziehen, wie z. B. in der Form von Kapitalzuschlägen. Was also tun? Best Practice ist die Erstellung und Dokumentation einer Prozesslandkarte mit den entsprechenden Teilprozessen. Auf dieser Basis können alle Prozessbeteiligten eine konkrete am Prozessablauf orientierte Risiko- und Kontroll-Zuordnung vornehmen. Das Dilemma der Praxis besteht in vielen Instituten aber immer noch in nicht prozessorientierten Arbeitsanweisungen, die zudem nicht die Abläufe der eigenen IT-Anwendungen mit einbeziehen. Die darin enthaltenen Kontrollen sind oftmals »verstreut« und darüber hinaus nicht MaRisk-konform dargestellt (vgl. MaRisk: »... klare Abgrenzung der Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen

und Kommunikationswege«). Dies führt mitarbeiterseitig dazu, dass Arbeitsanweisungen nicht mehr angemessen gewürdigt und Kontrollen nicht immer verstanden und beachtet werden. Zur Unterstützung der eingangs erwähnten, weiteren Anforderungen der Bankenaufsicht, ist daher eine Identifikation und Dokumentation des gesamten IKS zielführend (inkl. der aufbauorganisatorischen Schlüsselkontrollen, welche zumeist unpräzise in Richtlinien dargelegt sind). Neben der verbesserten Transparenz für die Mitarbeiter (und damit einer höheren Akzeptanz der Regelwerke) gewinnen Vorstand und Aufsichtsrat bzw. Verwaltungsrat ein pragmatisch-effizientes und zuverlässiges Organisationsniveau, welches die Regulatorik eher als Leitplanken für das Geschäftsmodell versteht (und somit die bankaufsichtlichen Anforderungen nicht als Zentrum des Handelns). Auf dieser Basis kann das individuelle IKS-Design, die Dokumentation, ein fortlaufendes Monitoring (inkl. Kontroll-Tests) sowie die Prüfung der Internen Revision aller wesentlichen IKS-Bestandteile erfolgen. Einmal derartig implementiert, können sich Vorstand und Aufsichts-/bzw. Verwaltungsrat regelmäßig durch entsprechende IKS-Reports vom Zustand des IKS überzeugen und gegebenenfalls weitere Maßnahmen veranlassen. Für die Institute gilt daher künftig noch mehr als bisher, die bisherigen Regelwerke und alle diesbezüglichen Verfahren zu überprüfen und zukunftsorientiert auszurichten!

Die Autoren haben in ihren praxisnahen Ausführungen diesbezüglich die verschiedenen Eckpunkte herausgearbeitet. Hilfestellung bieten dabei die Darstellung der maßgeblichen wesentlichen IKS-Bestandteile sowie Praxistipps.

Neben den selbstredend erfolgten Anpassungen auf der Basis der letzten MaRisk-Novelle wurde die inhaltliche Strukturierung des Werkes insbesondere im Abschnitt »IKS-Anforderungen für die Bankprozesse« stark prozessorientiert dargestellt. In diesem Kontext findet auch das sogenannte Three-Lines-of-Defense-Modell (3 LoD) zunehmend Beachtung in der Praxis und wurde daher ebenfalls neu in das Werk mit integriert. Da im Autorenteam u. a. auch vier Vertreter der Bankenaufsicht mitgewirkt haben, ist es nicht verwunderlich, dass die Sichtweise der Aufsicht in dieser Auflage nochmals erweitert wurde.

Das vorliegende Handbuch wendet sich an alle, die für ein zeitgemäßes Risikomanagementsystem inkl. eines Internen Kontrollsystems in einer Bank oder Sparkasse verantwortlich zeichnen. Das beginnt mit der Geschäftsleitung, den jeweiligen Verantwortlichkeiten in den Stabs-/Steuerungs-, Fach- und Com-

pliancebereichen und endet mit der Internen Revision. Unser Bestreben war und ist es, zu verdeutlichen, dass die institutsinternen IKS-Lösungen eine wichtige Grundlage für das Risikomanagement darstellen und zudem regelmäßig von externer Seite (Abschlussprüfer und Bankenaufsicht) auf den Prüfstand gestellt werden. Ein angemessenes IKS sowie dessen Dokumentation tragen einerseits zur Risikominimierung und zu positiven externen Prüfungsergebnissen und andererseits zu einer optimierten Umsetzung des Geschäftsmodells bei.

Den beteiligten Autoren sagen wir Danke für ihre fundierten Beiträge, in denen sie ihre umfassenden Erfahrungen aus ihrer Berufspraxis sowie ihre theoretischen Fachkenntnisse haben einfließen lassen. Wir hoffen, dass wir Ihnen mit diesem Werk viele praktische Anregungen und Hilfestellungen für die Umsetzung im eigenen Institut geben können. Als Herausgeber-Team würden wir uns zudem auch über Anregungen und Rückfragen sehr freuen.

Oktober 2019

Michael Helfer

Dr. Karsten Geiersbach

Henning Riediger

Ludger Hanenberg

**A.**

**Bedeutung des IKS für die Bankenaufsicht**





## A. Bedeutung des IKS für die Bankenaufsicht

### I. Europäische Bankenaufsicht – Umsetzung des SREP

#### 1. Einführung

Mit der Verabschiedung der SREP (Supervisory Review and Evaluation Process-)Leitlinien durch die EBA im Dezember 2014 war die Erwartung verbunden gewesen, dass die europäischen Bank-Aufsichtsbehörden ihre nationalen SREP-Verfahren stärker angleichen. Die deutsche Aufsicht hat sich verpflichtet, diese europäischen Anforderungen in ihren Aufsichtsprozess zu integrieren. Dabei betrat die Aufsicht aber keineswegs völlig neues Land, denn der Prozess der Beurteilung der einzelnen Institute bildete schon seit geraumer Zeit einen wichtigen Teil der aufsichtlichen Praxis. Allerdings bedeutet die mit der Veröffentlichung der Leitlinien verbundene Erwartungshaltung der EBA, dass nunmehr generell für die Institute Kapitalaufschläge wegen bestimmter zusätzlicher institutsspezifischer Risiken festzulegen sind, eine Herausforderung für die Aufsicht. Das dazu entwickelte Verfahren, das eine Kombination aus quantitativen und qualitativen Aspekten umfasst, wird im Rahmen eines stufenweisen Vorgehens seit Mitte 2016 umgesetzt.

Dabei kommt u. a. den Governance-Anforderungen eine große Bedeutung zu. Das gilt nicht nur für die nationale Sichtweise, sondern auch für die Erwartungshaltung, wie sie in den SREP-Leitlinien der EBA zum Ausdruck kommt. So beschäftigt sich der Titel 5 der EBA-SREP-Leitlinien (Governance und interne Kontrollen) u. a. mit der Bewertung der internen Unternehmensführung und institutsweiter Kontrollen. Dort wird ein Rahmen abgesteckt, der von den Aufsichtsbehörden auszufüllen ist.

So sollen im SREP die interne Unternehmensführung und institutsweiten Kontrollen u. a. in folgenden Aspekten betrachtet werden:

- Regelrahmenwerk für generelle interne Unternehmensführung
- Unternehmenskultur und Risikokultur
- Organisation und Funktionsweise des Leitungsorgans
- Vergütungsvorschriften und -praktiken
- Regelwerk zum Risikomanagement einschließlich ICAAP und ILAAP

- **Regelwerk für interne Kontrollen einschließlich der Internen Revision**
- Informationssysteme und Geschäftskontinuität
- Sanierungsplanungen.

4 Im Folgenden soll daher der Schwerpunkt auf einige Erwartungen im Hinblick auf interne Kontrollen einschließlich der Internen Revision gelegt werden.

### 2. EBA-Leitlinien über interne Unternehmensführung

5 Gemäß den **EBA-Leitlinien über interne Unternehmensführung (Tz. 104)** sollten die verantwortlichen Aufsichtsbehörden einschätzen, ob das Institut über ein angemessenes Regelwerk für interne Kontrollen verfügt. Hierbei sollen **mindestens** die **folgenden Aspekte** abgedeckt sein:

#### a) Internes Kontrollsystem (IKS), Kontrolleinheiten und Verantwortlichkeiten

6 Das interne Kontrollsystem und seine wesentlichen aufsichtsrechtlichen Anforderungen sind nicht neu. Die aktuelle **MaRisk-Novelle aus 2017** erwartet in AT 4.3 wie bisher auch, dass jedes Institut »entsprechend Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten u. a. Regelungen zur Aufbau- und Ablauforganisation zu treffen hat«. Hierzu gehört insbesondere ein **Regelwerk für das interne Kontrollsystem**. In der Praxis ist zu beobachten, dass t ein solches Rahmenwerk regelmäßig u. a. die folgenden Aspekte umfasst:

- Ausführungen zur IKS-Aufbau- und Ablauforganisation
- Definition von **Aufgabenträgern** (u. a. zentrale sowie dezentrale IKS-Beauftragte, Prozess- und Kontrollverantwortliche sowie die Berichtslinie zur Geschäftsleitung)
- Anwendung des »**3-Lines-of-Defense**«-Modells auf die eigene Organisation
- **IKS-Management** (u. a. Identifizierung und Bewertung von Risiken, Dokumentation, Angemessenheits- und Wirksamkeitsbewertung sowie Maßnahmen zur Stabilisierung/Verbesserung der Kontrollhandlungen und Berichtswesen).

7 So gibt es Modelle, bei der die Verantwortlichkeit für die Implementierung eines solchen Regelwerks in der Hand eines zentralen »IKS-Verantwortlichen«

liegt. Dieser koordiniert nicht nur die Umsetzung, sondern überwacht auch die einheitliche Anwendung der festgelegten Kontrollverfahren.

Aspekte, die zu einem IKS-Rahmenwerk gehören, finden sich u. a. im sog. **3-Lines-of-Defense-Modell** bzw. Modell der 3 Verteidigungs- bzw. Abwehrlinien, auf das sich auch der Baseler Ausschuss in seinem Dokument zur Internen Revision bezieht.

In der nachfolgenden Abbildung wird daher die Trennung der unterschiedlichen – jeweils unabhängig voneinander agierenden – Kontrolleinheiten hervorgehoben.

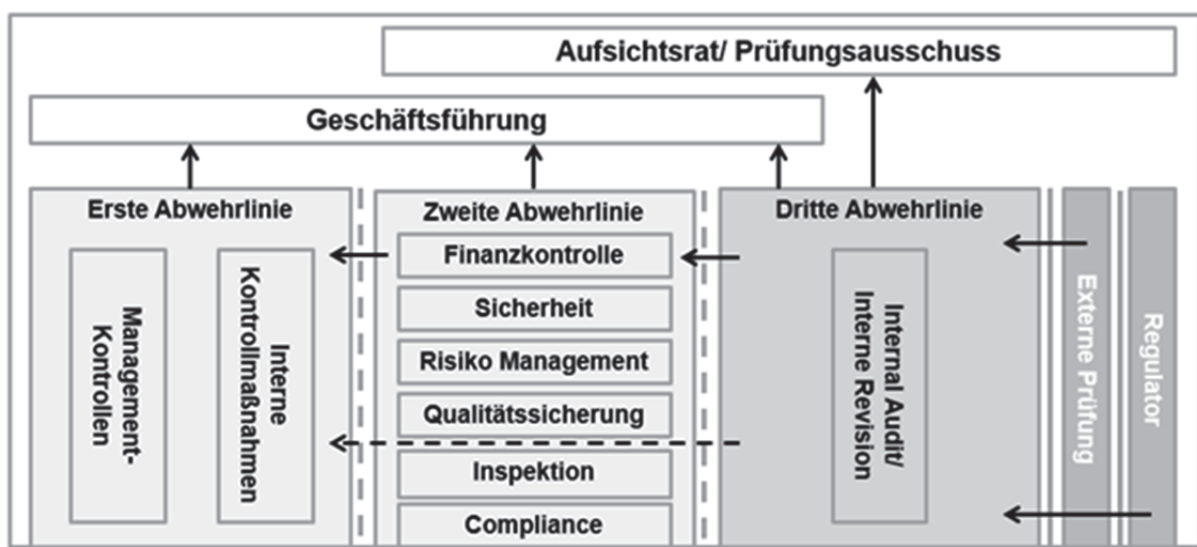


Abbildung A. – 1: 3-Lines-of-Defense-Modell  
(European Confederation of Institutes of Internal Auditing (ECIIA))

Die **erste Verteidigungslinie** umfasst das operative Management sowie prozessintegrierte Kontrollen, die verantwortlich sind für die **Bewertung, Kontrolle und Reduzierung von Risiken**. Diese Kontrollhandlungen sind Bestandteil der Aufgaben **im Rahmen des Tagesgeschäfts** der Geschäftsfelder bzw. Fachbereiche. Hierunter fällt auch die **Überwachung der Aktivitäten und Funktionen der zugelassenen Geschäftsleitung**, für die sie direkt verantwortlich ist. In die Verantwortung der Geschäfts- und Unterstützungseinheiten gehören u. a. folgende Aufgaben:

- **Kennen der »eigenen« Normen** (schriftlich fixierte Ordnung in Form von Arbeitsanweisungen bzw. Prozessdokumentationen)
- Identifizierung und Kennen der Risiken (**Risikoinventur**)
- Definition von **angemessenen** Kontrollen sowie **Transparenz** der eigenen Schlüsselkontrollen

- Herstellen von **Referenzen zwischen Kontrollen und Risiken** (Einttrittswahrscheinlichkeit und Schadenshöhe)
  - Sicherstellen der **Wirksamkeit von Kontrollhandlungen** (Einhaltung der Prozesse und definierten Kontrollen, **Kontroll-Testings**, Kontrollergebnisse, Kontrollreports).
- 11 Die **zweite Verteidigungslinie** überwacht die Umsetzung wirksamer risikomindernder Maßnahmen, die durch das operative Management durchgeführt werden. Darüber hinaus liegt es in der Verantwortung dieser nachgelagerten Verteidigungslinie die Einhaltung externer Anforderungen zu überwachen. Während die erste Verteidigungslinie die **unmittelbare Verantwortung** für die Identifikation und Steuerung der Risiken hat (Kontrollen, u. a. in Form von 4-Augen-Prinzip, Funktionstrennung und Vorgesetztenkontrolle) nimmt die zweite Verteidigungslinie eine **prozessbegleitende Überwachung** wahr.
- 12 Im Unterschied zur ersten und zweiten Verteidigungslinie liefert die **dritte Verteidigungslinie** einen wichtigen Beitrag zur Unterstützung der Geschäftsleitung. Das erfolgt vor allem durch einen **risikoorientierten Prüfungsansatz**. Hierbei geht es i. e. L. um die Beurteilung der Effektivität (Funktionsfähigkeit) der Bewertung und Steuerung der Risiken durch die vorgelagerten Verteidigungslinien. Während die zweite Verteidigungslinie prozessbegleitend tätig ist, nimmt die dritte Verteidigungslinie ihre Aufgaben **prozessunabhängig** wahr.
- 13 In diesem Zusammenhang kann die in den neuen MaRisk AT 4.3.1 geregelte sog. »Cooling-Off-Period« eine besondere Bedeutung erlangen. Gemäß dieser Regelung soll *»beim Wechsel von Mitarbeitern der Vertriebsbereiche in Kontrollbereiche (Risikocontrolling-Funktion, Compliance-Funktion, Marktfolge sowie Abwicklung und Kontrolle) angemessene Übergangsfristen vorzusehen sind, innerhalb derer diese Mitarbeiter keine Tätigkeiten ausüben oder verantworten, die gegen das Verbot der Selbstprüfung und -überprüfung verstoßen«*. Eine ähnliche Vorgabe kennen auch die internationalen Standards für die berufliche Praxis der Internen Revision. Dort beschreibt der Attribut-Standard 1130.A1, dass
- »Interne Revisoren von der Beurteilung von Geschäftsprozessen absehen müssen, für die sie zuvor verantwortlich waren. Die Objektivität kann als beeinträchtigt angenommen werden, wenn ein Interner Revisor eine Aktivität prüft, für die er im Verlauf des vorangegangenen Jahres verantwortlich war.«*
- 14 Hiernach kann auch i. S. d. Vorgaben der MaRisk im Allgemeinen Teil 4.3.1 zumindest in vielen Fällen von einer angemessenen »Abkühlungsphase« von 12 Monaten ausgegangen werden.