

Inhaltsübersicht

Vorwort	1
A. Das Beauftragtenwesen – Gesamtzusammenhänge & Aufbau	3
B. Prüfung Wertpapiercompliance	9
C. Prüfung Geldwäsche und Betrugsprävention	31
D. Prüfung Compliance-Funktion gemäß MaRisk	121
E. Prüfung Datenschutz	139
F. Prüfung IT-Sicherheit	181
G. Prüfung Auslagerungsbeauftragter	221
H. »Nach der Prüfung ist vor der Prüfung« Prüfungserleichterungen für das kommende Jahr	253

Inhaltsverzeichnis

Vorwort (<i>Daumann</i>)	1
A. Das Beauftragtenwesen – Gesamtzusammenhänge & Aufbau (<i>Daumann</i>)	3
A. Das Beauftragtenwesen – Gesamtzusammenhänge & Aufbau	5
B. Prüfung Wertpapiercompliance	9
Einleitung (<i>Daumann</i>)	11
I. Überblick über die Funktion (<i>Kaiser</i>)	13
II. Rechtliche Rahmenbedingungen (<i>Kaiser</i>)	15
III. Prüffelder und Turnus (<i>Kaiser</i>)	18
1. Definition Prüffelder	19
2. Turnusprüfungsplan	20
IV. Mustercheckliste (<i>Kaiser</i>)	20
1. Prüfung der Wertpapiercompliance-Funktion	20
2. Kundenbeschwerden	22
3. Prüfung der Protokolle nach WpHG und der Ordererfassung	24
V. Musterbericht (<i>Kaiser</i>)	26
VI. Praxistipps (<i>Kaiser</i>)	27
1. Protokolle nach WpHG	27
2. Wertpapierorders	28
3. Mitarbeitergeschäfte	28

C. Prüfung Geldwäsche und Betrugsprävention	31
Einleitung (<i>Daumann</i>)	33
I. Überblick über die Funktion (<i>Baumann/Meyer im Hagen</i>)	37
II. Rechtliche Rahmenbedingungen und anstehende rechtliche Änderungen (<i>Baumann/Meyer im Hagen</i>)	40
1. Überblick über die geldwäscherelevanten Vorschriften	40
2. Novellierung des GwG 2017	42
III. Prüffeldgliederung und Turnus definieren (<i>Baumann/Meyer im Hagen</i>)	48
1. Gliederung des Prüffelds	48
2. Risikoorientierte Prüfungsplanung	49
IV. Prüfungs-Checklisten (<i>Baumann/Meyer im Hagen</i>)	53
1. Hinweise zur Struktur der Checklisten	53
2. Kundenbezogene Sorgfaltspflichten	54
a) Allgemeine kundenbezogene Sorgfaltspflichten	54
b) Risikoorientierte kundenbezogene Sorgfaltspflichten	64
3. Geldwäsche-Compliance bzw. Tätigkeit des GwB – Wesentliche Tätigkeiten	72
4. Geldwäsche-Compliance bzw. Tätigkeit des GwB – Sonstige Tätigkeiten	82
5. Betrugsprävention	107
V. Musterbericht (<i>Baumann/Meyer im Hagen</i>)	118
VI. Literaturverzeichnis (<i>Baumann/Meyer im Hagen</i>)	120
D. Prüfung Compliance-Funktion gemäß MaRisk	121
Einleitung (<i>Daumann</i>)	123
I. Überblick über die Funktion (<i>Dox</i>)	125
II. rechtliche Rahmenbedingungen (<i>Dox</i>)	126
1. Regelungen in den MaRisk vom 14.12.2012	126
2. Änderungen mit der MaRisk Novelle 2017	126

III.	Abgrenzung der CoF zur Internen Revision (<i>Dox</i>)	127
IV.	Prüfung der CoF durch die IR (<i>Dox</i>)	128
V.	Übersicht der benötigten Unterlagen (<i>Dox</i>)	128
VI.	Prüfungschecklisten (<i>Dox</i>)	129
E.	Prüfung Datenschutz	139
	Einleitung (<i>Daumann</i>)	141
I.	Überblick über die Funktion (<i>Müller</i>)	144
1.	Bestellung des betrieblichen Datenschutzbeauftragten	144
2.	Anforderungen an den betrieblichen Datenschutzbeauftragten	145
a)	Zuverlässigkeit	145
b)	Fachkunde	146
3.	Aufgaben des betrieblichen Datenschutzbeauftragten	147
4.	Fazit	149
II.	Rechtliche Rahmenbedingungen/anstehende rechtliche Änderungen (<i>Müller</i>)	150
1.	Rechtliche Rahmenbedingungen	150
a)	Kreditwesengesetz	150
b)	BDSG	151
c)	MaRisk	153
d)	Mindestanforderungen an die Sicherheit von Internetzahlungen	153
e)	weitere Gesetze und Vorschriften mit Datenschutzrelevanz	154
2.	Anstehende rechtliche Änderungen	155
III.	Prüffelder und Turnus definieren (<i>Müller</i>)	159
1.	Bedeutung des Prüffeldes für die Bank	159
2.	Risikoorientierte Prüfungsplanung und -durchführung	160
3.	Prozessorientierte Prüfungsplanung und -durchführung	161
IV.	Mustercheckliste (<i>Müller</i>)	162

V.	Musterbericht (<i>Müller</i>)	168
1.	Risikoorientierung	169
a)	Vorabestufung durch die BaFin	169
b)	Bewertung des inhärenten Risikos	169
c)	Bewertung des Kontroll- und Ableitung des Fehlerrisikos	169
2.	Management Summary	170
a)	Zusammengefasstes Prüfungsergebnis	170
b)	Bewertung des Risikos der Einzelfeststellungen	172
3.	Herleitung des Prüfungsergebnisses	172
a)	Rahmenbedingungen und Aufgaben des Datenschutzbeauftragten	172
b)	Aufgaben der Mitarbeiter	173
c)	Beratungs- und Unterstützungsleistungen	174
d)	Kommunikation und Berichterstattung	175
4.	Hinweise und Bemerkungen	176
VI.	Praxistipps und Hinweise/Risikobewertung/ ggf. weitere Muster oder Vorlagen (<i>Müller</i>)	176
F.	Prüfung IT-Sicherheit	181
	Einleitung (<i>Daumann</i>)	183
I.	Überblick über die Funktion (<i>Kolb</i>)	186
1.	Einführung	186
2.	Security Governance	188
3.	Security Awareness	191
4.	Information Risk Management	192
5.	Technische IT-Sicherheit	194
6.	Risikomanagement bei Dienstleistungen	195
II.	Rechtliche Rahmenbedingungen (<i>Kolb</i>)	196
1.	Rahmenbedingungen der Aufsicht – SREP	196
2.	KWG/MaRisk	197
3.	BAIT (Entwurf)	198

4.	Bundesdatenschutzgesetz/Datenschutzgrundverordnung	199
5.	IT-Sicherheitsgesetz	200
6.	Mindestanforderungen an die Sicherheit von Internetzahlungen	201
III.	Prüffelder (<i>Kolb</i>)	201
IV.	Mustercheckliste (<i>Kolb</i>)	203
V.	Musterbericht (<i>Kolb</i>)	210
1.	Titelblatt	210
2.	Inhaltsverzeichnis	211
3.	Zusammenfassung	212
4.	Hintergrundinformationen	213
5.	Feststellungen	215
VI.	Praxistipps (<i>Kolb</i>)	216
VII.	Literaturverzeichnis (<i>Kolb</i>)	218
G.	Prüfung Auslagerungsbeauftragter	221
	Einleitung (<i>Daumann</i>)	223
I.	Überblick über die Funktion (<i>Weiss</i>)	225
1.	Entwicklung Auslagerung im Zeitverlauf	225
2.	Management Auslagerung	226
II.	Rechtliche Rahmenbedingungen und deren Veränderung (<i>Weiss</i>)	227
1.	Anforderungen aus AT 9	227
a)	Definition des Auslagerungstatbestandes gemäß Tz. 1 des Abschnitts	227
b)	Bestimmung der Wesentlichkeit einer Auslagerung und Einbeziehung in das Risikomanagement einer Bank gemäß Tz. 2 des Abschnitts	228
c)	Risikoanalyse	229
d)	Umgang mit nicht wesentlichen Auslagerungen und deren Einbeziehung in das Risikomanagement gemäß Tz. 3 des Abschnitts	231

e)	Zulässigkeit und Grenzen von Auslagerung gemäß Tz. 4 des Abschnitts	232
f)	Vorkehrungen im Fall der Beendigung der Auslagerungsvereinbarung bei wesentlichen Auslagerungen gemäß Tz. 5 des Abschnitts	233
g)	Anforderungen an den Auslagerungsvertrag gemäß Tz. 6 des Abschnitts	234
f)	Anforderung an die laufende Steuerung und Überwachung von Auslagerungen gemäß Tz. 7 des Abschnitts	237
g)	Spezielle Anforderungen an die Vollausslagerung der Internen Revision	238
h)	Anforderungen an die Auslagerung von Aktivitäten und Prozesse bei Weiterverlagerungen	238
2.	Organisation des Auslagerungsmangement	239
III.	Prüffelder und Turnus definieren (<i>Weiss</i>)	241
1.	Gesetzliche und aufsichtsrechtliche Aufforderungen	241
2.	Festlegung Prüffelder und Prüfungsturnus	242
a)	Teilprüffeld Aufbau- und Ablauforganisation Auslagerungsmanagement	242
b)	Teilprüffeld wesentliche Auslagerungen gem. AT 9 Tz. 2, ggf. in Verbindung mit den Anforderungen aus BT 2.1 Tz. 3	243
c)	Teilprüffeld nicht wesentliche Auslagerungen und Vereinbarungen über den »sonstigen Fremdbezug von Leistungen«	243
IV.	Mustercheckliste (<i>Weiss</i>)	243
V.	Musterbericht (<i>Weiss</i>)	250

H. »Nach der Prüfung ist vor der Prüfung«	
Prüfungserleichterungen für das kommende Jahr (<i>Horn</i>)	253
I. Darstellung Kooperatives Modell	255
1. Problemstellung	255
2. Lösung nach dem Kooperativen Modell	257
II. Integrierte Gefährdungsanalyse	262
III. Aktivitätenpläne und Aufteilung der Prüfungsobjekte auf Basis funktionsweiser Nettorisikobewertungen	266
IV. Korrespondierende Berichterstattung	268
V. Vorbereitung zur Einführung des Kooperativen Modells	269
VI. Auszug Mustergefährdungsanalyse	270