

Compliance-Funktion nach MaRisk

Relevante Rechtsnormen ■ Prozessuale Herausforderungen ■
Anwendungs- und Prüfungserfahrungen

in der Reihe:

Bearbeitungs- und Prüfungsleitfaden

Prozesse prüfen * Risiken vermeiden * Fehler aufdecken
→ Handlungsempfehlungen ableiten

Bearbeitungs- und Prüfungsleitfaden

Compliance-Funktion nach MaRisk

**Relevante Rechtsnormen ■ Prozessuale Herausforderungen ■
Anwendungs- und Prüfungserfahrungen**

Frank Borrmann
Bundesbankdirektor
Bankgeschäftliche Prüfungen
Deutsche Bundesbank
Hannover

Jan Hendrik Meyer im Hagen
Direktor
Interne Revision
Sparkasse Paderborn-Detmold
Paderborn

Dr. Kevin Niwek
Rechtsanwalt
Regulatory and Financial Crime Compliance
HSBC Trinkaus & Burkhardt AG
Düsseldorf

Volker Schmidt (Hrsg.)
Senior Manager
Fachbereich Banken & Finanzdienstleister
BDO AG Wirtschaftsprüfungsgesellschaft
Frankfurt am Main

Axel Schmitt
Abteilungsleiter Compliance
Kreissparkasse München Starnberg Ebersberg
München

Inhaltsverzeichnis

A. Die Compliance-Funktion als Bestandteil des Internen Kontrollsystems	1
I. Einleitung	3
II. Das Interne Kontrollsystem von Instituten	5
1. Gesetzliche und aufsichtsrechtlich Anforderungen	5
2. Bestandteile und Aufgaben des Internen Kontrollsystems	7
a) Bestandteile des Internen Kontrollsystems	7
b) Aufgaben des Internen Kontrollsystems	9
c) Compliance-Funktion gemäß AT 4.4.2 MaRisk	13
III. Die Rolle der Compliance-Funktion im Internen Kontrollsystem	15
1. Abgrenzung von Verantwortlichkeiten	15
2. Aufgaben und Tätigkeiten der Compliance-Funktion	16
a) Risikobasierte Überwachungshandlungen	16
b) Beratungsfunktion und Berichterstattung	17
B. Errichtung/Umsetzung einer institutsweiten MaRisk-Compliance-Funktion im Fokus der Aufsicht	23
I. Einfluss aktueller gesetzlicher und bankaufsichtlicher (Mindest-)Anforderungen	25
II. Mögliche Prüfungsansätze/-felder zur Beurteilung der Wirksamkeit der Compliance-Funktion nach MaRisk	26
1. Aufgaben und Befugnisse	27
2. Aufbauorganisatorische Einbettung	29
3. Berichtswesen	30
4. Sonstige mögliche relevante Prüfungsansätze/-felder	31
III. Zusammenfassung und Ausblick	33
IV. Checkliste inklusive Erläuterungen	34

C. Abgrenzung der Tätigkeiten, Rechte und Pflichten zwischen (MaRisk-)Compliance-Funktion, anderen IKS-Funktionen und der Internen Revision	39
I. Der »Drei-Verteidigungslinien-Ansatz« als Ausgangspunkt einer Systematisierung	41
1. Einleitung	41
2. Modell der drei Verteidigungslinien	43
a) Erste Verteidigungslinie	46
b) Zweite Verteidigungslinie	47
c) Dritte Verteidigungslinie	48
II. Integration der verschiedenen Überwachungsfunktionen in das Interne Kontrollsystem	49
1. Organisatorische Einbindung der Funktionen	49
2. Auslagerung von Funktionen/Arbeitsteilung im Verbund	51
3. Anforderungen an die Qualifikation der Funktionsträger	54
III. Abstimmung der Kontrolleinheiten zur Vermeidung von Konflikten und zur Erreichung von Synergieeffekten	55
1. Aufgaben und Ziele der Kontrolleinheiten	55
2. Informationsrechte	59
3. Risikoidentifikation und -bewertung	60
4. Kontroll- und Prüfungstätigkeiten	62
5. Beratung der Geschäftsleitung	63
6. Berichterstattung	65
IV. Checkliste zur Vermeidung von Abstimmungsproblemen und Doppelarbeiten	66
1. Allgemeine Anforderungen an die Zusammenarbeit der Kontrollfunktionen und die Kontrollen der ersten Verteidigungslinie	67
2. Hinweise für die Risikocontrolling-Funktion	69
3. Hinweise für die Compliance-Funktion	69
4. Hinweise für die Interne Revision	71

D. Relevante rechtliche Risiken für die MaRisk-Compliance-Funktion	73
I. Übersicht	75
II. Europäische Herleitung der MaRisk-Compliance-Funktion	76
III. Identifizierung der wesentlichen Risiken des Instituts	79
1. Zwingender Katalog von wesentlichen Risiken	80
2. Sonstige wesentliche Risiken	81
IV. Nicht abschließende Darstellung der in die MaRisk- Compliance-Funktion einzubeziehenden wesentlichen rechtlichen Risiken	83
1. Compliance-Risiken aus Wertpapierrechtsprechung und Wertpapieraufsichtsrecht/Kapitalmarktrecht	84
2. Risiken im Zusammenhang mit Geldwäschebekämpfung, Terrorismusfinanzierung und sonstigen strafbaren Handlungen	86
3. Vorgaben zur Verhinderung doloser Handlungen zu Lasten des Instituts	89
4. Allgemeine Verbraucherschutzvorgaben (z. B. auch mit Bezug auf das Kreditgeschäft oder andere Aktivitäten)	89
5. Datenschutzvorgaben	89
6. Allgemeines Aufsichtsrecht	90
7. Bilanzierungsregeln	90
8. Wettbewerbsrecht und gewerblicher Rechtsschutz	90
9. Bankvertrags- und Zivilrecht	91
10. Verfahrens- und Vollstreckungsrecht	91
11. Insolvenzrecht	91
12. Corporate Governance und Gesellschaftsrecht	92
13. Steuerrecht	92
14. Arbeits- und Sozialrecht	93
15. Ausländische Rechtsvorgaben	93

V.	Aufbau einer Risikoinventur	96
1.	Aufbau nach Gesetzen und anderen Vorgaben	97
2.	Aufbau nach Themen	98
3.	Aufbau nach Bereichen	99
4.	Zusammenfassung	100
VI.	Prozess zur Identifizierung von neuen rechtlichen Risiken	100
VII.	Fazit	102
E.	Organisatorische Ausgestaltung der Compliance-Funktion zur unabhängigen Aufgabenwahrnehmung	105
I.	Einbindung der institutsweiten Compliance-Funktion in das Interne Kontrollsystem	107
1.	Internes Kontrollsystem	110
a)	Funktionstrennung	110
b)	Angemessene organisatorische Regelungen	110
c)	Kontrollen	111
2.	Compliance als zweite Kontrollebene	113
a)	Risikoanalyse	114
b)	Beurteilung der Risikosteuerungsinstrumente	115
c)	Überwachungsplan	117
d)	Eigene Kontrollen	117
II.	Hierarchische Stellung der Compliance-Funktion und des Compliance-Beauftragten	119
1.	Grundlagen	119
2.	Hierarchische Stellung und Ausgestaltung der Compliance-Funktion	122
3.	Anbindung an bestehende Organisationseinheiten	123
a)	Anbindung an Rechtsabteilung	123
b)	Anbindung an die Funktion des Datenschutzbeauftragten	125
c)	Keine Beschneidung von anderweitigen Hierarchien und Zuständigkeiten	126

4.	Compliance als Koordinierungsstelle (Komitee-Organisation)	128
III.	Befugnisse und Rechte für die Sicherstellung unabhängiger Aufgabenwahrnehmung	130
1.	Zugang zu compliance-relevanten Informationen	132
2.	Einbindung in Neue-Produkte-/Neue-Märkte Prozess	134
3.	Exkurs: Strafrechtliche Verantwortlichkeit	135
a)	Unterlassungstaten	136
b)	Garantenpflicht des MaRisk-Compliance- Beauftragten	139
IV.	Checkliste zur Einhaltung organisatorischer Anforderungen, Rechte und Pflichten	141
1.	Einbindung der institutsweiten Compliance-Funktion in das Interne Kontrollsystem	141
2.	Hierarchische Stellung der Compliance-Funktion und des Compliance-Beauftragten	142
3.	Befugnisse und Rechte für die Sicherstellung unabhängiger Aufgabenwahrnehmung	144
F.	Erweiterung der bisherigen Risiko-/Gefährdungsanalysen (GFA) um wesentliche Rechtsnormen	147
I.	Einleitung	149
II.	Einfluss gesetzlicher, aufsichtsrechtlicher sowie interner Regelungen auf die GFA-Erstellung	150
1.	Geldwäsche/Terrorismusfinanzierung/sonstige strafbare Handlungen	150
2.	WpHG-Compliance	152
3.	Datenschutz und Informationssicherheit	153
4.	Weitere Grundlage: MaRisk AT 4.4.2	155
III.	Prozesse der Risikoidentifizierung und (monetären/qualitativen) Risikobewertung	156
1.	Risikoidentifizierung	156

2.	Operationelle Risiken	158
IV.	Aufbau einer Compliance-Risiko-Landkarte	159
1.	Risikobewertung	161
a)	Bewertungsschema Geldwäsche-Prävention	161
b)	Bewertungsschema sonstigen strafbaren Handlungen.	161
2.	Ad-hoc-Berichterstattung	162
3.	Dokumentation der Risikobewertung	162
V.	Einheitliches Vorgehen der IKS-Bereiche bei Durchführung einer GFA-Compliance	164
VI.	Verwendung aktualisierter GFA-Ergebnisse für ein Backtesting des laufenden Monitorings	165
VII.	Checkliste für die sukzessive Abarbeitung/Durchführung einer institutsweiten GFA	166
G.	Aufgaben und Prozesse zur Sicherstellung der Compliance-Funktion	173
I.	Durchführung geeigneter Überwachungshandlungen der Compliance-Funktion auf Basis der Risiko-/Gefährdungsanalyse	175
1.	Einführung – Die Compliance-Funktion als Teil des internen Kontrollsystems	175
2.	Tätigkeit der Compliance-Funktion als »zweite Verteidigungslinie«	176
3.	Die Risiko-/Gefährdungsanalyse als Ausgangsbasis von Überwachungs- und Kontrollhandlungen der Compliance-Funktion	178
4.	Überwachungshandlungen der Compliance-Funktion	178
5.	Dokumentation der Überwachungshandlungen	181
6.	Mögliche Maßnahmen bei festgestellten Defiziten	182
7.	Checkliste für die Überwachungshandlungen der Compliance-Funktion	183

II.	Beratung zu compliance-relevanten Fragestellungen sowie Schulung der Mitarbeiter	185
1.	Grundlagen und Praxisrelevanz der Beratung	185
2.	Checkliste Beratungsfunktion durch Compliance	187
3.	Grundlagen und Praxisrelevanz von Schulungen	188
4.	Checkliste Durchführungen von Schulungen	190
III.	Einbindung in wesentliche compliance-relevante Prozesse des Instituts	191
1.	Formen und Erforderlichkeit der Einbindung	191
2.	Checkliste Prozesseinbindung der Compliance-Funktion	197
3.	Checkliste für Interne Revision und externe Prüfer	200
4.	Checkliste für die Beurteilung der Compliance-Funktion	201
IV.	Berichterstattung an die Geschäftsleitung und das Aufsichtsorgan	205
1.	Gesetzliche und aufsichtsrechtliche Grundlagen	205
2.	Allgemeine Anforderungen an die Berichterstattung	206
3.	Inhalt und konkrete Ausgestaltung der Compliance-Berichterstattung	207
4.	Zusammenfassung	210
5.	Checkliste Berichterstattung der Compliance-Funktion	210
6.	Hinweise und Checkliste für Interne Revision und externe Prüfer	211
7.	Checkliste	212
H.	Abkürzungsverzeichnis	215