

**Monika Roth**

Prof. Dr. iur., Advokatin

***Good Corporate Governance:*  
Compliance als Bestandteil  
des internen Kontrollsystems**

**Ein Handbuch für die Praxis**

2., aktualisierte und überarbeitete Auflage



# Inhaltsverzeichnis

ZITIERTE UND WEITERFÜHRENDE LITERATUR	13
ABKÜRZUNGSVERZEICHNIS	19
ABBILDUNGSVERZEICHNIS	22
PROLOG: SIEMENS	23
1. EINLEITUNG	31
1.1 Corporate Governance	31
1.2 Erfordernis des systemischen Ansatzes	37
1.3 Corporate Governance und Internes Kontrollsystem	41
1.4 FINMA-Rundschreiben 2008/24 «Überwachung und interne Kontrolle Banken»	43
1.5 Internes Kontrollsystem in der Finanzmarktregulierung	45
1.6 Internationale Standards	49
1.7 Internationale Standards, nationale Bankenaufsicht und Reputation	52
1.8 Compliance: Generelle Grundlagen und Begriffe laut FINMA-Rundschreiben 2008/24 «Überwachung und interne Kontrolle Banken»	55
2. ORGANISATIONSVERANTWORTUNG	65
2.1 Ausgangslage: Unübertragbare Aufgaben des Verwaltungsrates	65
2.2 IKS und Haftung für Verwaltung, Geschäftsführung und Liquidation (Art. 754 OR)	67
2.3 IKS und strafrechtliche Verantwortlichkeit des Unternehmens (Art. 102 StGB)	68
2.3.1 Grundsätzliches	68
2.3.2 Betriebstypische Gefahren der Industrie	71
2.4 Strafrecht, IKS und Gewähr der einwandfreien Geschäftstätigkeit (Art. 3 Abs. 2 Bst. c BankG)	73
2.5 Geschäftsherrenhaftung (Art. 55 OR)	75

3.	RISIKOBEURTEILUNG	77
3.1	Zuständigkeit und Verantwortung	77
3.2	Risks and Rules	78
3.3	Rückschaufehler (Hindsight bias)	81
4.	INTERNES KONTROLLSYSTEM (IKS)	83
4.1	Internes Kontrollsystem – ein Instrument der Unternehmensführung	83
4.1.1	Verwaltungsrat	83
4.1.2	Geschäftsleitung	83
4.2	Begriff IKS	84
4.2.1	Was ist Kontrolle	84
4.2.2	Was ist das interne Kontrollsystem	85
4.3	IKS und Risikomanagement	88
4.4	IKS, Compliance und operationelle Risiken	90
4.5	Compliance und Risikomanagement	94
4.6	IKS und betrieblicher Alltag	94
4.7	IKS und Qualitätsmanagement	95
5.	KONTROLLUMFELD	99
5.1	Begriff des Kontrollumfelds	99
5.2	Rolle der Verantwortlichen	99
5.3	Organisationelles Umfeld	102
5.4	Anreize und Sanktionen	103
5.5	Fallbeispiel Citigroup und Fazit	106
5.6	Verdiente Reputation	110
6.	FUNKTIONEN UND PROZESSE IN UND MIT BEZUG AUF DAS IKS	113
6.1	IKS-Vorgänge als solche	113
6.2	IKS und externe Revision	114
6.2.1	Im Allgemeinen	115
6.2.2	Spezielles in der Bankenregulierung	117
6.3	IKS und Interne Revision (Control of Controls)	119
6.3.1	Basler Ausschuss	119
6.3.2	Im Allgemeinen	119
6.3.3	IKS, Interne Revision und Risk Management	121

6.3.4	Spezielles in der Bankenregulierung	121
6.4	Whistleblowing	122
6.5	IKS und Controlling	125
6.6	IKS und Compliance	126
6.6.1	Compliance als Unterstützung für die Geschäftsleitung	126
6.6.2	Compliance-Risiken	128
6.6.2.1	Rechtsrisiken	129
6.6.2.2	Reputationsrisiken	129
6.6.2.3.	Strategische Risiken	132
7.	LEGAL AND COMPLIANCE ODER COMPLIANCE AND LEGAL?	135
7.1	Berufsbilder und Funktionen im Wandel	135
7.2	Organisationsformen	137
8.	COMPLIANCE-FUNKTION UND FRONT	141
9.	COMPLIANCE ALS VERHALTENSKONZEPT	145
10.	COMPLIANCE IM ALLGEMEINEN	149
11.	COMPLIANCE IM BANKBEREICH	153
11.1	Die Gewähr der einwandfreien Geschäftstätigkeit	153
11.1.1	Im nationalen Kontext	153
11.1.2	Finanzgruppen (Finanzkonglomerate)	155
11.1.3	Kein <i>moral free riding</i>	156
11.1.4	Bei grenzüberschreitender Dienstleistungserbringung	160
11.1.4.1	Ein Schreiben der EBK	160
11.1.4.2	Heutige Haltung der Aufsicht	162
11.2	Kernaufgaben von Compliance gemäss EBK	165
11.3	Bericht der Expertenkommission Revisionswesen (Dezember 2000)	165
12.	COMPLIANCE: BEGRIFF UND VORGABEN GEMÄSS FINMA-RS 2008/24 IM EINZELNEN	167
12.1	Rundschreiben der FINMA	167
12.2	Compliance als Teil des Managements operationeller Risiken: Die Umsetzung des FINMA-Rundschreibens	168
12.2.1	Erfordernis einer GAP-Analyse	168

12.2.2	Risk Assessment	169
13.	THEMEN DER GAP-ANALYSE: RZ 97–112 DES FINMA-RS 2008/24 «ÜBERWACHUNG UND INTERNE KONTROLLE BANKEN»	171
13.1	Fragestellungen aufgrund des FINMA-RS 2008/24	171
13.2	Normeinhaltung	171
13.3	Einrichtung und Unterstellung	175
13.4	Aufgaben und Verantwortlichkeiten	179
13.5	Outsourcing der Compliance-Funktion	184
13.5.1	Begriff Outsourcing	186
13.5.2	Rechtliches zum Outsourcing	187
13.5.3	Internationale Standards zum Outsourcing	191
14.	SCHLUSSFOLGERUNGEN	193
Anhang 1	Die zehn Regeln der Good Compliance	195
Anhang 2	FINMA-Rundschreiben 2008/24 Überwachung und interne Kontrolle bei Banken	196
Anhang 3	FINMA-Rundschreiben 2008/32 Corporate Governance Versicherer	213
Anhang 4	FINMA-Rundschreiben 2008/7 Outsourcing Banken	222
Anhang 5	Basel Committee on Banking Supervision, Principles for enhancing corporate governance	233
Anhang 6	Basel Committee on Banking Supervision, Consultative document	271
Anhang 7	Basel Committee on Banking Supervision, Compliance and the compliance function in banks	310
Anhang 8	FINMA-Rundschreiben 2008/21 Operationelle Risiken Banken	324
Anhang 9	Compliance darf weder Papiertiger noch lahme Ente sein	362
Anhang 10	Es gibt beim Thema Compliance viele Gretchenfragen	368
Anhang 11	Zur Haftung des Compliance-Officer	369

# Abbildungsverzeichnis

Abb. 1:	Verteidigungslinien	56
Abb. 2:	Anforderungen an das IKS	67
Abb. 3:	Wechselwirkungen in einem IKS	78
Abb. 4:	Die drei Säulen des Risikomanagements	90
Abb. 5:	Compliance Management und Management operationeller Risiken im Überblick	93/94
Abb. 6:	IKS-Stern	114
Abb. 7:	Compliance als Verhaltenskonzept	145