

Dr. iur. Mirjam Durrer

**Die Pflicht
des Verwaltungsrates
zum integralen
Risikomanagement in KMU**

Inhaltsübersicht

Inhaltsverzeichnis	IX
Abkürzungsverzeichnis	XVII
Literaturverzeichnis.....	XXIV
Materialienverzeichnis	XLVI
1. Kapitel: Einleitung	1
2. Kapitel: Die Konzeption des Schweizerischen Obligationenrechts.....	5
3. Kapitel: Die Konzeption des COSO-ERM-Framework und ISO 31000 ..	59
4. Kapitel: Die Konzeption des „Knowledge Framework“ der HSLU	155
5. Kapitel: Die Neukonzeption des integralen Risikomanagements als System für KMU	197
6. Kapitel: Haftung und Haftungsprävention	279
7. Kapitel: Empfehlungen zuhanden des Verwaltungsrates von KMU	310
Sachregister	319

Inhaltsverzeichnis

Abkürzungsverzeichnis	XVII
Literaturverzeichnis.....	XXIV
Materialienverzeichnis	XLVI
1. Kapitel: Einleitung	1
2. Kapitel: Die Konzeption des Schweizerischen Obligationenrechts	5
I. Einführung.....	5
1. Was ist ein schweizerisches KMU?.....	5
2. Die volkswirtschaftliche Bedeutung schweizerischer KMU	7
II. Die Entstehungsgeschichte des OR 2008.....	8
III. Die Risikobeurteilung gemäss OR 2008	9
1. Formelles	9
2. Materielles	10
A) Konzeptioneller Fokus auf Risiken mit wesentlichem Einfluss auf die Jahresrechnung	10
B) Angaben über die Durchführung der Risikobeurteilung	12
C) Prüfung durch die Revisionsstelle.....	14
IV. Das IKS gemäss OR 2008.....	16
1. Formelles	16
A) Art. 728a Abs. 1 Ziff. 3 OR 2008: IKS im engeren Sinn (i.e.S.) ..	16
B) Art. 728a Abs. 2 OR 2008: IKS im weiteren Sinn (i.w.S.).....	21
C) Art. 728b Abs. 1 OR 2008: Revisionsbericht.....	22
2. Materielles	23
V. Die Risikobeurteilung gemäss OR 2013	24
1. Formelles	24
2. Materielles	25
A) Konzeptioneller Fokus auf unternehmensweite Risiken	25
B) Aufschluss über die Durchführung der Risikobeurteilung	27
C) Prüfung durch die Revisionsstelle.....	28
VI. Die Risikobeurteilung und das IKS als Ausfluss der Oberleitungspflicht gemäss Art. 716a Abs. 1 OR i.V.m. Art. 717 Abs. 1 OR.....	29
1. Formelles	31
A) Die Oberleitung der Gesellschaft (Art. 716a Abs. 1 Ziff. 1 OR).....	31
a) Prüfungspflicht: Die Pflicht des Verwaltungsrates zur Durchführung einer Risikobeurteilung	33

b)	Handlungspflicht: Die Pflicht des Verwaltungsrates zum Risikomanagement	34
c)	Die Pflicht des Verwaltungsrates zur Risikobeurteilung und zum Risikomanagement in KMU	37
B)	Die Ausgestaltung der Finanzkontrolle (Art. 716a Abs. 1 Ziff. 3 OR)	39
a)	Prüfungs- und Handlungspflicht: Die Pflicht des Verwaltungsrates zum IKS	39
b)	Die Pflicht des Verwaltungsrates zum IKS in KMU	41
C)	Die weiteren Pflichten gemäss Art. 716a Abs. 1 OR	42
a)	Die Festlegung der Organisation (Art. 716a Abs. 1 Ziff. 2 OR)	43
b)	Die Oberaufsicht über die Geschäftsführung (Art. 716a Abs. 1 Ziff. 5 OR)	44
D)	Der Sorgfaltsmassstab (Art. 717 Abs. 1 OR)	45
E)	Die Delegationsmöglichkeiten	47
2.	Materielles	49
VII.	Der hilfswise Bezug von „technischen Normen“	51
1.	Die Rechtsnatur technischer Normen	51
2.	Die Rechtsverbindlichkeit technischer Normen	53
VIII.	Würdigung	55

3. Kapitel: Die Konzeption des COSO-ERM-Framework und ISO 31000	59	
I.	Die Konzeption des COSO-ERM-Framework	59
1.	Einführung	59
2.	Die Entstehungsgeschichte	61
A)	Das COSO-IC-Framework	61
B)	Das COSO-ERM-Framework	62
3.	Die interne Kontrolle gemäss COSO-IC-Framework	63
A)	Formelles	63
B)	Materielles	64
4.	Das Risikomanagement gemäss COSO-ERM-Framework	66
A)	Formelles	66
B)	Materielles	67
a)	Das „Enterprise Risk Management“ gemäss COSO	67
b)	Der COSO-ERM-Würfel als Modell	70
c)	Die vier Zielkategorien	71
d)	Die acht Komponenten	71
aa)	1. Komponente: Das Interne Umfeld des ERM	72
bb)	2. Komponente: Die Zielfestlegung des ERM	74
cc)	3. Komponente: Die Ereignisidentifikation des ERM	76

	dd) 4. Komponente: Die Risikobeurteilung des ERM.....	77
	ee) 5. Komponente: Die Risikosteuerung des ERM	82
	ff) 6. Komponente: Die Kontrollaktivitäten des ERM.....	83
	gg) 7. Komponente: Die Information und Kommunikation des ERM.....	84
	hh) 8. Komponente: Die Überwachung des ERM.....	86
	5. Die Umsetzung des COSO-ERM-Framework in der Praxis	87
	A) Application Techniques.....	87
	B) Embracing Enterprise Risk Management: Practical Approaches for Getting Started.....	88
	6. Kritische Würdigung.....	90
II.	Die Konzeption von ISO 31000	99
	1. Einführung	99
	2. Die Entstehungsgeschichte	103
	3. Das Risikomanagement gemäss ISO 31000	105
	A) Formelles	105
	B) Materielles.....	109
	a) 1. Kapitel: Anwendungsbereich.....	109
	b) 2. Kapitel: Begriffe	110
	c) 3. Kapitel: Grundsätze	112
	d) 4. Kapitel: Risikomanagementrahmen.....	114
	aa) 1. Element: Mandat und Verpflichtung.....	115
	bb) 2. Element: Gestaltung des Rahmens für die Behandlung von Risiken	116
	cc) 3. Element: Umsetzung des Risikomanagements	118
	dd) 4. Element: Überwachung und Überprüfung des Rahmens.....	118
	ee) 5. Element: Kontinuierliche Verbesserung des Rahmens.....	119
	e) 5. Kapitel: Risikomanagementprozess.....	119
	aa) 1. Tätigkeit: Kommunikation und Konsultation	120
	bb) 2. Tätigkeit: Erstellen des Zusammenhangs.....	120
	cc) 3. Tätigkeit: Risikobeurteilung.....	122
	dd) 4. Tätigkeit: Risikobewältigung	124
	ee) 5. Tätigkeit: Überwachung und Überprüfung	125
	4. Keine ISO-Norm zum IKS	125
	5. Zertifizierung	126
	6. Die Umsetzung von ISO 31000 in der Praxis.....	126
	7. Kritische Würdigung.....	128
III.	COSO-ERM-Framework und ISO 31000: Zwischenfazit	133
	1. Zwei Risikomanagement-Frameworks	133

2. Die Pflicht des Verwaltungsrates eines schweizerischen KMU zur Ausgestaltung, Implementierung und Überwachung des Risikomanagement-Systems	138
A) Das Risikomanagement als System	139
a) Definition „Risiko“	139
b) Definition „Managementsystem“	141
c) Definition „Risikomanagement-System“	143
B) Fazit	146
3. Die Tauglichkeit des COSO-ERM-Framework und ISO 31000 für die Pflichterfüllung des Verwaltungsrates eines schweizerischen KMU	149

4. Kapitel: Die Konzeption des „Knowledge Framework“ der HSLU	155
I. Einführung	155
II. Die Entstehungsgeschichte	155
1. Die Projektidee zum „Knowledge Framework“ der HSLU	155
2. Die Projektziele des „Knowledge Framework“ der HSLU.....	159
III. Die Rechtsnatur des „Knowledge Framework“ der HSLU	162
IV. Das „integrale Risikomanagement“ im „Knowledge Framework“ der HSLU.....	163
V. Das „Knowledge Framework“ der HSLU	165
1. Das Risikomanagement (RM) gemäss „Knowledge Framework“ der HSLU	166
A) Formelles	166
B) Materielles	166
2. Das interne Kontrollsystem (IKS) gemäss „Knowledge Framework“ der HSLU	169
A) Formelles	169
B) Materielles	169
3. Das Business Continuity Management (BCM) gemäss „Knowledge Framework“ der HSLU	171
A) Formelles	171
B) Materielles	171
4. Das Crisis Management (CM) gemäss „Knowledge Framework“ der HSLU	174
A) Formelles	174
B) Materielles	174
VI. Die Umsetzung des „Knowledge Framework“ der HSLU in der Praxis	175
1. Das online Benchmark-Tool im „Knowledge Framework“ der	

HSLU	176
2. Die Hilfsmittel des „Knowledge Framework“ der HSLU	177
A) Die Checklisten	178
B) Die Übersichtsdokumente	178
VII. Kritische Würdigung der Gesamtkonzeption des „Knowledge Framework“ der HSLU	179

5. Kapitel: Die Neukonzeption des integralen Risikomanagements als System für KMU197

I. Die Bedeutung von „integral“	197
1. Bedeutung und Wortherkunft	197
2. „Integral“ - Ein juristischer Begriff?	198
3. Der hilfswise Beizug der Wirtschaftswissenschaften	199
4. „Integriert“ - Ein juristischer Begriff?	200
5. Integriertes Risikomanagement	201
6. Fazit	202
II. Die Rechtsgrundlage für das BCM und das CM	203
1. Die formelle Rechtsgrundlage	204
A) Die juristische Auslegung	205
a) Die grammatikalische Auslegung	205
b) Die systematische Auslegung	208
c) Die historische Auslegung	209
d) Die teleologische Auslegung	210
B) Die wirtschaftliche Auslegung anhand des St. Galler Management-Modells	214
a) Ein Überblick über das St. Galler Management-Modell	214
b) Das Risikomanagement gemäss St. Galler Management-Modell	216
c) Das BCM und das CM im St. Galler Management-Modell	217
2. Zwischenergebnis	219
3. Die materiellen Gehalte des BCM und des CM	220
A) Der Kerngehalt des Business Continuity Management (BCM)	220
B) Der Kerngehalt des Crisis Management (CM)	222
III. Die Pflicht des Verwaltungsrates zur Ausgestaltung, Implementierung und Überwachung des integralen Risikomanagements als System	225
1. Der Kerngehalt des Risikomanagement-Prozesses	225
A) 1. Prozess-Schritt: Die Gefahrenidentifikation	226
B) 2. Prozess-Schritt: Die Risikobeurteilung	230
C) 3. Prozess-Schritt: Die Risikobewältigung	235
D) 4. Prozess-Schritt: Die Kontrollaktivitäten	236
2. Zwischenergebnis: Die materiellen Gehalte des BCM und des	

	CM als integrale Bestandteile des Risikomanagement-Systems	238
3.	Der Kerngehalt der internen Kontrolle als Prozess	240
	A) 1. Prozess-Schritt: Die Gefahrenidentifikation	241
	B) 2. Prozess-Schritt: Die Risikobeurteilung	242
	C) 3. Prozess-Schritt: Die Risikobewältigung	243
	D) 4. Prozess-Schritt: Die Kontrollaktivitäten	244
4.	Zwischenergebnis: Das IKS als integraler Bestandteil des Risikomanagement-Systems	244
5.	Ergebnis: Die Neukonzeption des integralen Risikomanagement- Systems	249
IV.	Die Ausgestaltung, Implementierung und Überwachung der Neukonzeption des integralen Risikomanagements als System für KMU	250
1.	1. System-Schritt: Die Pflicht des Verwaltungsrates zur Ausgestaltung des integralen Risikomanagement-Systems	251
	A) Die Festlegung des normativen Rahmens	252
	a) Die Risikopolitik	253
	b) Die Risikokultur	253
	B) Die Definition von vier kritischen Kategorien	254
2.	2. System-Schritt: Die Pflicht des Verwaltungsrates zur Implementierung des integralen Risikomanagement-Systems	257
	A) 1. Prozess-Schritt: Die Gefahrenidentifikation	257
	a) Ursachen mit unternehmensinterner Wirkung	258
	b) Ursachen mit unternehmensexterner Wirkung	259
	B) 2. Prozess-Schritt: Die Risikobeurteilung	261
	a) Die Risikoanalyse	262
	b) Die Risikobewertung	263
	C) 3. Prozess-Schritt: Die Risikobewältigung	266
	a) Die Priorisierung	266
	b) Die Definition des Soll-Zustands	267
	c) Die Ausarbeitung der Risikobewältigungsmassnahmen	267
	D) 4. Prozessschritt: Die Kontrollaktivitäten	269
3.	3. System-Schritt: Das Pflicht des Verwaltungsrates zur Überwachung des integralen Risikomanagement-Systems	270
	A) Überwachung und Übung	271
	B) Interne Kommunikation und externe Berichterstattung	272
4.	4. System-Schritt: Die Resilienz stärken	273
5.	Fazit	276
6. Kapitel:	Haftung und Haftungsprävention	279
I.	Einführung	279

B)	Die Definition von vier kritischen Kategorien	312
2.	2. System-Schritt: Die Pflicht des Verwaltungsrates zur Implementierung des integralen Risikomanagement-Systems	313
A)	1. Prozess-Schritt: Die Gefahrenidentifikation	313
B)	2. Prozess-Schritt: Die Risikobeurteilung	314
C)	3. Prozess-Schritt: Die Risikobewältigung	315
D)	4. Prozess-Schritt: Die Kontrollaktivitäten	316
3.	3. System-Schritt: Die Pflicht des Verwaltungsrates zur Überwachung des integralen Risikomanagement-Systems	316
A)	Überwachung und Übung	316
B)	Interne Kommunikation und externe Berichterstattung	317
4.	4. System-Schritt: Die Resilienz stärken	317
II.	Ausblick	318
	Sachregister	319