

Risikomanagement und Risikocontrolling

von

Prof. Dr. Marc Diederichs

5., vollständig überarbeitete und ergänzte Auflage

Verlag Franz Vahlen München

Inhaltsübersicht

Gedankenanstöße	V
Geleitwort	VII
Vorwort	IX
Inhaltsverzeichnis	XV
Abkürzungsverzeichnis	XXIII
1. Die ewige Renaissance des Risikomanagements	1
2. Grundlagen und Begriffe	7
3. Prozessschritte des Risikomanagements	183
4. Risikomanagement-Organisation und System-Dokumentation ...	311
5. Risikoberichterstattung und Risikokommunikation	359
6. Risikocontrolling in Wachstums- und Expansionsphasen	399
7. Tipps für den eiligen Praktiker	415
8. Fazit und Ausblick	427
Literaturverzeichnis	429
Stichwortverzeichnis	459

Inhaltsverzeichnis

Gedankenanstöße	V
Geleitwort	VII
Vorwort	IX
Inhaltsübersicht	XIII
Abkürzungsverzeichnis	XXIII
1. Die ewige Renaissance des Risikomanagements	1
1.1 Risikomanagement und Risikocontrolling: Mehr en vogue denn je!	1
1.2 In a nutshell	2
2. Grundlagen und Begriffe	7
2.1 Risikomanagement und Risikocontrolling: Eine betriebswirtschaftliche Notwendigkeit	7
2.1.1 Welcome to the VUCA-World!	7
2.1.2 Risikobegriff	18
2.1.3 Risikomanagement: Ein Muss im Rahmen der Unternehmens- führung	19
2.1.3.1 Ziele und Aufgaben des Risikomanagements	20
2.1.3.2 Begriff des Risikomanagements	23
2.1.3.3 Risikostrategie	24
2.1.3.3.1 Risikotragfähigkeit	25
2.1.3.3.2 Risikoappetit	32
2.1.3.3.3 Risikopolitik (Risikopolitische Grundsätze)	35
2.1.3.3.4 Risikotoleranzen	37
2.1.4 Risikocontrolling: „Unterstützer“ des Risikomanagements	39
2.1.4.1 Controlling im Allgemeinen	39
2.1.4.2 Risikocontrolling als Querschnittsfunktion des Controllings	42
2.1.4.3 Ziele und Aufgaben des Risikocontrollings	43
2.1.4.4 Begriff des Risikocontrollings	44
2.2 Der Umgang mit Risiken als gesetzliche Pflicht	45
2.2.1 Risikofrüherkennungs-, Risikoüberwachungs- und Risikomanagement-System	48

2.2.1.1	Einrichtung als Pflicht des Vorstands	48
2.2.1.2	Ausstrahlungswirkung des §91 Abs. 2 und 3 AktG auf andere Rechtsformen	52
2.2.1.3	Überwachung durch den Aufsichtsrat	54
2.2.1.4	Risikofrüherkennungs- & Risikoüberwachungssystem und Internes Kontrollsystem	58
2.2.2	Internes Kontrollsystem (IKS)	58
2.2.2.1	Anforderungen an ein IKS gemäß COSO I	59
2.2.2.1.1	COSO I-Rahmenwerk	59
2.2.2.1.2	COSO I vs. COSO II	61
2.2.2.1.3	COSO I vs. COSO – „Enterprise Risk Management – In- tegrating with Strategy and Performance“	62
2.2.2.1.4	Komponenten, Prinzipien und Fokuspunkte nach COSO I	62
2.2.2.1.5	Geeignete Systemdokumentation	68
2.2.2.2	Anforderungen an ein IKS gemäß IDW PS 261	75
2.2.2.2.1	Begriff und Aufgaben	75
2.2.2.2.2	Internes Steuerungs- und Überwachungssystem	75
2.2.2.2.3	Komponenten nach IDW PS 260	77
2.2.2.2.4	Verantwortung und Wirksamkeit	78
2.2.2.3	Anforderungen an ein IKS gemäß IDW PS 982	79
2.2.2.3.1	Begriff „IKS des Berichtswesens“ und Verantwortlichkei- ten	79
2.2.2.3.2	Grundelemente (Komponenten) nach IDW PS 982	80
2.2.2.3.3	Prüfung des IKS des Berichtswesens	84
2.2.2.3.4	Beschreibung des IKS des Berichtswesens	86
2.2.3	Risikoorientierte Lageberichterstattung	88
2.3	Anforderungen seitens der Abschlussprüfer	92
2.3.1	Prüfung des Risikofrüherkennungs- und Risikoüberwachungssystems	92
2.3.1.1	Rechtliche Grundlagen der Prüfung	92
2.3.1.2	Anforderungen seitens des IDW nach PS 340	96
2.3.1.2.1	Bestandsgefährdende Risikofelder	98
2.3.1.2.2	Grundelemente der Maßnahmen nach §91 Abs. 2 AktG ..	99
2.3.1.2.3	Dokumentation des Risikofrüherkennungssystems	105
2.3.1.2.4	Ausgestaltung der Maßnahmen nach §91 Abs. 2 AktG bei Konzernen	106
2.3.1.2.5	Einrichtung eines Überwachungssystems	108
2.3.1.2.6	Dokumentation der getroffenen Maßnahmen	108
2.3.1.3	Anforderungen seitens des IDW nach PS 981	108
2.3.1.3.1	Prüfungsgegenstand	108
2.3.1.3.2	Prüfungsziel	110
2.3.1.3.3	Prüfungsumfang	110
2.3.1.3.4	Anforderungen an ein Risikomanagement-System nach IDW PS 981	114
2.3.2	Prüfung der risikoorientierten Lageberichterstattung	125
2.3.2.1	Rechtliche Grundlagen der Prüfung	125

2.3.2.2 Anforderungen nach DRS 20 „Konzernlagebericht“	126
2.3.2.2.1 Risikobericht und Chancenbericht	128
2.3.2.2.2 Internes Kontroll- und Risikomanagementsystem bezogen auf den Konzernrechnungslegungsprozess	132
2.3.2.2.3 Risikoberichterstattung bezüglich der Verwendung von Finanzinstrumenten	134
2.3.2.3 Anforderungen nach DRS 16 „Zwischenberichterstattung“ ..	135
2.3.2.3.1 Halbjahresfinanzberichterstattung	136
2.3.2.3.2 Quartalsfinanzberichterstattung	137
2.3.2.3.3 Zwischenmitteilung der Geschäftsführung	138
2.3.2.4 Grenzen der risikoorientierten Lageberichterstattung	138
2.4 Internationale Normen und Standards als weitere Basis für die Etablierung von Risikomanagement-Systemen	140
2.4.1 COSO-Rahmenwerk: Enterprise Risk Management – Integration with Strategy and Performance	140
2.4.1.1 COSO-Rahmenwerk: Enterprise Risk Management – Integrating with Strategy and Performance	140
2.4.1.2 Governance & Culture	142
2.4.1.2.1 Prinzip 1: Risikoüberwachung durch das geschäftsführende und -überwachende Organ	143
2.4.1.2.2 Prinzip 2: Etablierung organisatorischer Strukturen	145
2.4.1.2.3 Prinzip 3: Definition der angestrebten Kultur	146
2.4.1.2.4 Prinzip 4: Sich gegenüber Grundwerten verpflichten	149
2.4.1.2.5 Prinzip 5: Kompetente Mitarbeiter gewinnen, entwickeln und binden	151
2.4.1.3 Strategy & Objective-Setting	152
2.4.1.3.1 Prinzip 6: Analyse der unternehmerischen Rahmenbedingungen	153
2.4.1.3.2 Prinzip 7: Risikoappetit festlegen	153
2.4.1.3.3 Prinzip 8: Evaluierung alternativer Strategien	156
2.4.1.3.4 Prinzip 9: Unternehmensziele formulieren	157
2.4.1.4 Performance	159
2.4.1.4.1 Prinzip 10: Risikoidentifikation	160
2.4.1.4.2 Prinzip 11: Risikobeurteilung	161
2.4.1.4.3 Prinzip 12: Priorisierung von Risiken	164
2.4.1.4.4 Prinzip 13: Maßnahmen zur Risikobewältigung implementieren	165
2.4.1.4.5 Prinzip 14: Portfoliosicht entwickeln	166
2.4.1.5 Review and Revision	168
2.4.1.5.1 Prinzip 15: Wesentliche Änderungen bewerten	168
2.4.1.5.2 Prinzip 16: Review der Risiken und Performance	169
2.4.1.5.3 Prinzip 17: Verbesserung des Risikomanagements	170
2.4.1.6 Information, Communication and Reporting	170
2.4.1.6.1 Prinzip 18: Nutzung von Informationen und Technologie ..	171
2.4.1.6.2 Prinzip 19: Kommunikation risikorelevanter Informationen	173
2.4.1.6.3 Prinzip 20: Berichte zu Risiko, Kultur und Performance ..	175

2.4.2 ISO 31000	177
2.5 Anforderungen an ein „State-of-the-Art“-Risikomanagement.....	180
3. Prozessschritte des Risikomanagements	183
3.1 Risikoidentifikation	184
3.1.1 Ziele und Aufgaben der Risikoidentifikation	184
3.1.2 Postulate der Risikoidentifikation	185
3.1.3 Methoden der Risikoidentifikation	187
3.1.3.1 Progressive Methode	187
3.1.3.2 Retrograde Methode	188
3.1.4 Risikokategorien.....	189
3.1.4.1 Interne Risiken	191
3.1.4.2 Externe Risiken	192
3.1.4.3 Risikointerdependenzen	194
3.1.5 Instrumente der Risikoidentifikation	195
3.1.5.1 Kollektionsmethoden.....	196
3.1.5.1.1 Begehung (Besichtigung)	196
3.1.5.1.2 Risikocheckliste(n)	197
3.1.5.1.3 SWOT-Analyse	199
3.1.5.2 Analysemethoden	200
3.1.5.2.1 Wertkettenanalyse.....	200
3.1.5.2.2 Prozesskettenanalyse	201
3.1.5.2.3 Exkurs: Internes Kontroll- und Risikomanagement-Sys- tem bezogen auf den Rechnungslegungsprozess.....	207
3.1.5.2.4 Netzwerktechnik	210
3.1.5.2.5 Frühaufklärungssysteme	214
3.1.5.2.5.1 Kennzahlen- und hochrechnungsorientierte Früh- warnsysteme	215
3.1.5.2.5.2 Indikatororientierte Früherkennungssysteme	216
3.1.5.2.5.3 Strategische Frühaufklärungssysteme	221
3.1.5.2.6 Daten- und Dokumentenanalysen	224
3.1.5.2.7 Fehlermöglichkeits- und Einflussanalyse (FMEA)	225
3.1.5.2.8 Fault-Tree Analysis (FTA)	234
3.1.5.2.9 Benchmarking	240
3.1.5.3 Kreativitätsmethoden	243
3.1.5.3.1 Brainstorming und Brainwriting	243
3.1.5.3.2 Experten- und Mitarbeiterbefragung	245
3.1.5.4 Praxistipp Integrierte Anwendung der Instrumente zur Risikoidentifikation	246
3.1.5.5 Unternehmensspezifisches Risikoprofil (Risikoinventar)....	254
3.1.6 Grenzen der Risikoidentifikation	255
3.2 Risikobeurteilung	257
3.2.1 Ziele und Aufgaben der Risikobeurteilung	257
3.2.2 Instrumente der Risikobeurteilung.....	257
3.2.2.1 Beurteilung von Risiken mithilfe von Eintrittswahrschein- lichkeit, Schadensausmaß und Erwartungswert	259
3.2.2.1.1 Risikoeintrittswahrscheinlichkeit und Schadensausmaß..	259

3.2.2.1.2	Brutto- und Nettobewertung	261
3.2.2.1.3	Risikoklassifizierung mithilfe eines Risikoportfolios	262
3.2.2.1.4	Schadenerwartungswert	265
3.2.2.1.5	Annualisierter Erwartungswert	265
3.2.2.2	Beurteilung von Risiken mithilfe von Scoring-Modellen	267
3.2.2.2.1	Ziele und Aufgaben von Scoring-Modellen	267
3.2.2.2.2	Business Environmental Risk Index (BERI-Index)	268
3.2.2.2.3	Anwendungspotenzial und Grenzen von Scoring-Modellen	272
3.2.2.3	Beurteilung von Risiken mithilfe der Jahresabschlussanalyse	273
3.2.2.3.1	Ziel und Aufgaben der Jahresabschlussanalyse	273
3.2.2.3.2	Diskriminanzanalyse und Künstliche Neuronale Netze	273
3.2.2.3.3	KNN Backpropagation 14.	275
3.2.2.3.4	Anwendungspotenzial und Grenzen der Jahresabschlussanalyse	277
3.2.2.4	Beurteilung von Risiken mithilfe von Value- und Cash-Flow-at-Risk	278
3.2.2.4.1	Value-at-Risk	278
3.2.2.4.2	Cash-Flow-at-Risk	287
3.2.2.4.3	Kritische Würdigung des VaR und CFaR als Risikomaß	291
3.2.3	Grenzen der Risikobeurteilung	292
3.3	Risikosteuerung und Risikobewältigung	293
3.3.1	Ziele und Aufgaben der Risikosteuerung und Risikobewältigung	293
3.3.2	Risikosteuerungsstrategien	294
3.3.2.1	Risiken vermeiden	295
3.3.2.2	Risiken vermindern	296
3.3.2.3	Risiken begrenzen	297
3.3.2.4	Risiken überwälzen	299
3.3.2.5	Risiken akzeptieren	301
3.3.3	Risikostrategiematrix	302
3.3.4	Risikosteuerungsinstrumente	304
3.3.4.1	Ziele und Aufgaben	304
3.3.4.2	Arten von Risikosteuerungsinstrumenten	309
4.	Risikomanagement-Organisation und System-Dokumentation	311
4.1	Ziele und Aufgaben der Risikomanagement-Organisation	311
4.2	Allgemeine Gestaltungsansätze	312
4.2.1	Zentralisation versus Dezentralisation	312
4.2.2	Stabsfunktion versus Linienfunktion	314
4.2.3	Hierarchische Einbindung	315
4.2.4	Zusammenfassende Würdigung	316
4.3	Organisatorische Gestaltungsempfehlungen für die Unternehmenspraxis	317
4.3.1	Risikomanager	317
4.3.1.1	Aufgaben des Risikomanagers	317
4.3.1.2	Stellenanforderung	319

4.3.2 Risikoausschuss	319
4.3.2.1 Charakteristika und Eignung	319
4.3.2.2 Aufgaben und Kompetenzen	320
4.3.2.3 Besetzung	322
4.3.2.4 Geschäftsordnung	323
4.3.2.5 Risikoausschuss-System	323
4.4 Interne Revision	327
4.4.1 Historische Entwicklung und Begriff	328
4.4.2 Regulatorischer Rahmen, Verhaltensgrundsätze und organisatorische Aspekte	331
4.4.2.1 Wesentliche regulatorische Grundlagen	331
4.4.2.2 Verhaltensgrundsätze	333
4.4.2.3 Organisatorische Aspekte	333
4.4.3 Ziele und Aufgaben, Revisionsprinzipien sowie Revisionsfelder	335
4.4.3.1 Ziele und Aufgaben	335
4.4.3.2 Revisionsprinzipien	336
4.4.3.3 Revisionsfelder	337
4.4.4 Prüfung des Risikomanagements durch die Interne Revision	339
4.4.4.1 Organisation und Risikokultur	341
4.4.4.2 Risikostrategie	342
4.4.4.3 Risikoidentifikation und Risikoerfassung	343
4.4.4.4 Risikoanalyse und Risikobewertung	344
4.4.4.5 Risikosteuerung und Risikoüberwachung	345
4.4.4.6 Risikoberichterstattung und Risikokommunikation	346
4.4.5 Abgrenzung von Risikomanagement-Funktion und Interner Revision	347
4.5 Risikomanagement-Richtlinie (System-Dokumentation)	348
4.5.1 Ziele und Aufgaben	349
4.5.2 Aufbau und Inhalte	349
4.5.3 Prozesstemplates zur vereinfachten Visualisierung der Abläufe	350
5. Risikoberichterstattung und Risikokommunikation	359
5.1 Ziele und Aufgaben der Risikoberichterstattung	359
5.2 Gestaltung und Organisation der Risikoberichterstattung	360
5.2.1 Berichtszweck	361
5.2.2 Berichtssender und Berichtsempfänger	361
5.2.3 Berichtsarten und Berichtsfrequenz	366
5.2.4 Berichtsinhalte und -gestaltung	368
5.3 Berichtshierarchie mit Fallbeispielen	372
5.3.1 Risikoerfassungsbögen als Grundlage der Risikoberichterstattung	373
5.3.2 Risikodatenbank	376
5.3.3 Risk-Card	380
5.3.4 Balanced Chance- & Risk-Card	383
5.3.4.1 Konzeption und Perspektiven der BCR-Card	384
5.3.4.2 Entwicklung und Aufbau der BCR-Card	387

5.3.4.2.1 Strategische Ziele, Perspektivenzuordnung und Strategieleitlinie	387
5.3.4.2.2 Kennzahlen, Indikatoren sowie Zielvorgaben	388
5.3.4.2.3 Risiken und risikorelevante Sachverhalte	390
5.3.4.2.4 Projekte, Maßnahmen und Aktionspläne	392
5.3.4.3 BCR-Card als Kommunikationsinstrument	392
5.4 Störungen der Risikoberichterstattung	395
6. Risikocontrolling in Wachstums- und Expansionsphasen	399
6.1 Kontrollarten in Wachstums- und Expansionsphasen	402
6.1.1 Kontrolle der Prämissen	402
6.1.2 Durchführungskontrolle	403
6.1.3 Strategische Überwachung	403
6.2 Instrumente zur Kontrolle und Analyse von Planungsprämissen ..	404
6.2.1 Globale Umwelt	404
6.2.2 Branchenstruktur	406
6.2.3 Darstellung von strategischen Gruppen	406
6.2.4 SWOT-Analyse	409
6.2.5 Szenario-Darstellungen	410
6.3 Instrumente für das Strategie- und Maßnahmen-Monitoring	411
6.3.1 Balanced Chance- & Risk-Card als Strategie-Monitor	411
6.3.2 Maßnahmen- und Projekt-Monitoring	412
7. Tipps für den eiligen Praktiker	415
7.1 Positionieren Sie das Thema!	416
7.2 Realisieren Sie die Vorteile einer zentralen Koordination!	417
7.3 Klären Sie Verantwortlichkeiten und schaffen Sie einen Plan B! ...	417
7.4 Schaffen Sie Transparenz durch integrierte Risikomanagement-Prozesse!	419
7.5 Machen Sie Werbung für das Risikomanagement!	421
7.6 Machen Sie Ihr Risikomanagement für alle sichtbar!	422
7.7 Was immer Sie tun, halten Sie es einfach!	423
7.8 Und Sie – lieber Risikomanager?	424
7.9 ... zum Guten Schluss!	425
8. Fazit und Ausblick	427
Literaturverzeichnis	429
Stichwortverzeichnis	459