

Inhaltsverzeichnis

Vorwort.....	5
Arbeitskreis „Risikomanagement“.....	7
Inhalte auf der CD.....	13
Abbildungsverzeichnis.....	15
Abkürzungsverzeichnis.....	17
Gesetze und Verordnungen.....	19
1. Grundlagen.....	21
1.1. Definitionen.....	21
1.2. Normative Vorgaben.....	22
1.2.1. Regelungen in Österreich.....	22
1.2.1.1. Gesetzliche Regelungen.....	22
1.2.1.2. Österreichischer Corporate Governance Kodex ...	23
1.2.2. Regelungen in Deutschland.....	25
1.2.2.1. Gesetzliche Regelungen.....	25
1.2.2.2. Deutscher Corporate Governance Kodex.....	26
1.2.3. Regelungen in der Schweiz.....	26
1.2.3.1. Gesetzliche Regelungen.....	26
1.2.3.2. Swiss Code of Best Practice for Corporate Governance.....	27
1.2.4. Internationale und nationale Normen und Standards.....	28
1.2.4.1. IFRS 7.....	28
1.2.4.2. COSO ERM Framework.....	30
1.2.4.3. Standard ISO 31000 und ISO 31010.....	32
1.2.4.4. Standard ONR 49000.....	32
1.3. Beteiligte am Risikomanagementprozess.....	33
1.3.1. Top Management.....	33
1.3.2. Operatives Management.....	33
1.3.3. Risikomanager.....	33
1.3.4. Interne Revision.....	34
1.3.5. Aufsichtsrat – Prüfungsausschuss.....	34
1.3.6. Abschlussprüfer.....	34
1.3.7. Rechnungshöfe.....	34
1.3.8. Eigentümer und andere Interessengruppen.....	34
1.4. Abgrenzungen und Synergien.....	35
1.4.1. Interne Revision ⇔ Risikomanagement.....	35
1.4.2. Internes Kontrollsystem ⇔ Risikomanagement.....	36
1.4.3. Controlling ⇔ Risikomanagement.....	37
1.4.4. Qualitätsmanagement ⇔ Risikomanagement.....	37

1.4.5. Compliance Management System ⇔ Risikomanagement .	37
1.4.6. Corporate Social Responsibility ⇔ Risikomanagement.....	38
1.4.7. Krisenmanagement ⇔ Risikomanagement.....	38
1.4.8. Zusammenwirken der Steuerungs- und Überwachungs- systeme	40
2. Risikomanagementsystem	42
2.1. Risikokultur, risikopolitische Grundsätze, Risikostrategie und Limitsysteme	42
2.2. Risikomanagement-Organisation.....	43
3. Der Risikomanagementprozess	45
3.1. Risiken identifizieren	45
3.1.1. Risikokatalog.....	46
3.1.2. Nicht identifizierte Risiken	47
3.1.3. Ausgewählte Methoden der Risikoidentifizierung.....	47
3.2. Risiken kategorisieren.....	48
3.3. Risiken bewerten.....	49
3.3.1. Messmethoden – Quantität und Qualität.....	50
3.3.2. Brutto-/Nettobewertung	51
3.3.3. Bewertungsparameter.....	51
3.3.4. Überprüfungszyklen der Bewertung	52
3.3.5. Wesentlichkeitsgrenzen und Limit-Systeme.....	52
3.3.6. Orientierungshilfe zur Bewertung.....	54
3.3.7. Nachvollziehbarkeit der Bewertung.....	55
3.3.8. Darstellung der bewerteten Risiken	55
3.4. Risiken aggregieren	55
3.4.1. Monte-Carlo-Simulation	56
3.5. Risiken bewältigen.....	58
3.5.1. Risikovermeidung	58
3.5.2. Risikominderung.....	59
3.5.3. Risikotransfer, -abwälzung	59
3.5.4. Risiko selbst tragen	59
3.6. Risiken steuern.....	59
3.6.1. Risikosteuerung und Monitoring.....	60
3.6.2. Risiko-Controlling.....	60
3.7. Risiken berichten	60
3.7.1. Risikomatrix.....	63
3.8. Risikomanagement für Projekte.....	65
3.9. Software-Tools und Kosten der Implementierung eines ERM-Systems	65
3.9.1. Werkzeuge für das Risikomanagement.....	65
3.9.2. Kosten der Implementierung eines ERM-Systems	67
3.10. Reifegrad von Risikomanagementsystemen	69

4. Risikomanagement und Interne Revision.....	72
4.1. Risikoorientierte Prüfung.....	72
4.1.1. Risikoorientierte Prüfungsplanung.....	72
4.1.1.1. Grundlagen.....	72
4.1.1.2. Beispiel einer risikoorientierten Prüfungs- planung.....	73
4.1.2. Beitrag der Internen Revision zur Risikoerfassung und -bewertung.....	83
4.2. Prüfung des Risikomanagementsystems	83
4.2.1. Spezielle Standards für die Durchführung der Prüfung des ERM durch die Interne Revision	83
4.2.1.1. Internationale Standards für die berufliche Praxis der Internen Revision	83
4.2.1.2. Praktische Ratschläge.....	84
4.2.1.3. Praxisleitfäden.....	84
4.2.1.4. DIIR-Revisionsstandard Nr. 2 „Prüfung des Risikomanagement durch die Interne Revision“ ...	85
4.2.1.5. IDW-Prüfungsstandard	85
4.2.1.6. Normen (ISO 31000, ONR 49000)	85
4.2.2. Prüfungsprozess	85
4.2.2.1. Grundlagen, Vorgaben	86
4.2.2.2. Ist-Erhebung.....	86
4.2.2.3. Analyse (Soll-Ist-Vergleich).....	87
4.2.3. Prüfansätze für das unternehmensweite Risiko- managementsystem	87
4.2.3.1. Organisation	87
4.2.3.2. Risikoidentifikation und -bewertung	88
4.2.3.3. Risikosteuerung und Monitoring	89
4.2.3.4. Kommunikation und Berichterstattung.....	89
4.2.3.5. Dokumentation.....	89
4.2.3.6. Datenmanagement.....	90
4.3. Interne Revision als Risk Owner	90
4.3.1. Risikomanagement der Internen Revision	90
4.3.2. Risiken der Internen Revision.....	91
5. Risikomanagement bei Informations- und Kommunikations- technologien	105
5.1. Definition und Anwendung von IKT in Unternehmen	105
5.2. Risikomanagement, Sicherheit und IT.....	106
5.2.1. Normen und Frameworks	106
5.2.2. IKT und Risikomanagement	108

5.2.2.1. IKT als Erfolgsfaktor	109
5.2.2.2. Risikomanagement in der IKT-Funktion	109
6. Branchenspezifische Aspekte	111
6.1. Öffentlicher Sektor	111
6.1.1. Rechtliche Vorgaben im Bund	111
6.1.2. Internationale Richtlinien	112
6.2. Kreditinstitute	120
6.2.1. Risikomanagement und Interne Revision	121
6.2.2. Gesetzliche und aufsichtsrechtliche Anforderungen in Österreich	121
6.2.3. Gesetzliche und aufsichtsrechtliche Anforderungen in Deutschland	122
6.2.4. Gesetzliche und aufsichtsrechtliche Anforderungen in der Schweiz	124
6.2.5. Übersicht Regelkreis und Spannungsfeld Interne Revision	125
6.3. Versicherungsunternehmen	126
6.3.1. Risikomanagement und Interne Revision	126
6.3.2. Gesetzliche und aufsichtsrechtliche Anforderungen in Österreich	127
6.3.3. Gesetzliche und aufsichtsrechtliche Anforderungen in Deutschland	128
6.3.4. Gesetzliche und aufsichtsrechtliche Anforderungen in der Schweiz	129
Anhang: Umfrage 2013 zum Risikomanagement in Österreich, Deutschland und der Schweiz	131
Literaturverzeichnis	139