

Inhaltsübersicht

1	Einführung	1
2	Der Begriff Risiko	11
3	Grundlagen des Risikomanagements	75
4	Aufbauorganisation	109
5	Risiken beherrschen	135
6	Methoden, Werkzeuge und Dokumente	183
7	Strategische Risiken	235
8	IT-Betriebsrisiken	251
9	IT-Projektrisiken	317
10	Risikomanagement im Unternehmen einführen	339
11	Das Interne Kontrollsystem	353
12	Das Risikomanagementsystem prüfen	367
13	Wie könnte es weitergehen?	385
	Anhang	389
A	Übersicht über Normen, Standards und weitere Vorgaben für das IT-Risikomanagement	391
B	Glossar	401
C	Abkürzungsverzeichnis	411
D	Referenzen	419
	Stichwortverzeichnis	431

Inhaltsverzeichnis

1	Einführung	1
2	Der Begriff Risiko	11
2.1	Der Risikobegriff	11
2.1.1	Bedrohungen in der IT	17
2.1.2	Schwachstellen in der IT	19
2.1.3	Schutzziele	24
2.1.4	Risikopotenzial	26
2.1.5	Der Wahrscheinlichkeitsbegriff und das Risiko	28
2.1.6	Risikoarten	32
2.1.7	Systematisierung von Risiken	37
2.1.8	Klassifikation von Risiken	40
2.1.9	Die Darstellung von Risiken in der Praxis	44
2.1.10	Ursache-Wirkungs-Beziehungen in der IT	47
2.1.11	IT und der Faktor Zeit	52
2.2	Risikopolitik	55
2.2.1	Das Risikobewusstsein	56
2.2.2	Die Risikokultur	59
2.2.3	Risikoappetit und Risikoneigung	62
2.2.4	Risikoakzeptanz, Risikotoleranz und Risikotragfähigkeit	66
2.2.5	Risikorichtlinie	70
3	Grundlagen des Risikomanagements	75
3.1	Begriff und Ausprägungen des Risikomanagements	75
3.1.1	Risikomanagement	75
3.1.2	Enterprise Risk Management	78

3.2	Das IT-Risikomanagement	80
3.2.1	Anforderungen an das IT-Risikomanagement	81
3.2.2	Risikostrategien	86
3.3	Normen, Standards und weitere Vorgaben	92
4	Aufbauorganisation	109
4.1	Wahl der Organisationsstruktur	109
4.2	Rollen	117
4.3	Gremien	126
4.4	Externe Gruppen	130
4.5	Qualifikationsaspekte	131
5	Risiken beherrschen	135
5.1	Grundstruktur und organisatorische Verankerung	135
5.2	Zuordnung von Verantwortung	143
5.3	Schritt 1: Definition des Kontexts	146
5.4	Schritt 2: Identifikation	150
5.5	Schritt 3: Analyse	157
5.6	Schritt 4: Bewertung	164
5.7	Schritt 5: Behandlung	167
5.8	Reporting, Kommunikation und Beratung	170
5.9	Risikocontrolling	178
6	Methoden, Werkzeuge und Dokumente	183
6.1	Methoden und Werkzeuge	184
6.2	Dokumente	215
6.3	Hilfestellungen für die Auswahl	224
6.4	Softwareunterstützung	226
7	Strategische Risiken	235
7.1	IT-Strategie	235
7.2	IT-GRC-Management	238
7.3	IT-Architektur	242
7.4	Digitale Geschäftsmodelle und smarte Produkte	247

8	IT-Betriebsrisiken	251
8.1	Organisation des IT-Betriebs	253
8.1.1	Zentraler und dezentraler Betrieb	255
8.1.2	Outsourcing und Outtasking	259
8.1.3	Cloud Computing	268
8.1.4	Virtualisierung	274
8.1.5	Schatten-IT	277
8.2	Unzulänglichkeiten, Fehler und Ausfälle	283
8.2.1	Ursache »Personen und Organisationseinheiten«	284
8.2.2	Ursache »Daten«	286
8.2.3	Ursache »Anwendungen und IT-Infrastruktur«	287
8.2.4	Ursache »IT-Prozesse und IT-Organisation«	290
8.2.5	Ursache »IT-Umfeld«	292
8.3	Angriffe	293
8.4	Notfälle und Katastrophen	297
8.5	Internet der Dinge und Industrie 4.0	300
8.6	Nutzung von Mobilgeräten	307
8.7	IT-Betrieb in kleinen Unternehmen	311
9	IT-Projektrisiken	317
9.1	Risiken in IT-Projekten	324
9.2	DevOps und DevSec	333
9.3	Open-Source-Projekte	335
10	Risikomanagement im Unternehmen einführen	339
10.1	Schritte zur Entwicklung und Einführung	339
10.2	Wirtschaftlichkeitsbetrachtungen	347
11	Das Interne Kontrollsystem	353
11.1	Begriff	353
11.2	Aufbau	354
11.3	Der Begriff »Kontrolle«	358
11.4	Das Three-Lines-of-Defense-Modell	361
11.5	Konzeption des Internen Kontrollsystems	363

12	Das Risikomanagementsystem prüfen	367
12.1	Formen und Varianten der Prüfung	367
12.2	Prüfungsablauf	374
13	Wie könnte es weitergehen?	385
Anhang		389
A	Übersicht über Normen, Standards und weitere Vorgaben für das IT-Risikomanagement	391
B	Glossar	401
C	Abkürzungsverzeichnis	411
D	Referenzen	419
	Stichwortverzeichnis	431