
Inhaltsverzeichnis

1	Einführung	1
2	IT-Risiko	7
2.1	Der Risikobegriff	7
2.1.1	Der Wahrscheinlichkeitsbegriff und das Risiko	11
2.1.2	Risikoarten	13
2.2	Das IT-Risiko	17
2.2.1	Systematisierung von IT-Risiken	20
2.2.2	Die Darstellung von IT-Risiken in der Praxis	27
2.2.3	Ursache-Wirkungs-Beziehungen in der IT	29
2.2.4	IT und der Faktor Zeit	32
2.2.5	Bedrohungen in der IT	35
2.2.6	Verwundbarkeiten in der IT	36
2.3	IT-Riskobewusstsein, IT-Risikokultur, IT-Riskoneigung und IT-Risikopolitik	39
2.3.1	Das IT-Riskobewusstsein	39
2.3.2	Die IT-Risikokultur	42
2.3.3	Die IT-Riskoneigung und IT-Risikoakzeptanz	44
2.3.4	Die IT-Risikopolitik	50
2.3.5	IT-Risikorichtlinie	50
3	IT-Risikomanagement	55
3.1	Begriff und Ausprägungen des Risikomanagements	55
3.1.1	Risikomanagement	55
3.1.2	Enterprise Risk Management	56

3.2	Das IT-Risikomanagement	57
3.2.1	Anforderungen an das IT-Risikomanagement	59
3.2.2	IT-Risikostrategien	63
3.3	Vorgaben für das IT-Risikomanagement	68
4	Aufbauorganisation des IT-Risikomanagements	87
4.1	Organisationsstrukturen im IT-Risikomanagement	87
4.2	Rollen im IT-Risikomanagement	94
4.3	Gremien für das IT-Risikomanagement	102
4.4	Externe Gruppen mit Bezug zum IT-Risikomanagement	106
4.5	Qualifikationsaspekte	107
5	Der IT-Risikomanagement-Prozess	111
5.1	Grundstruktur und organisatorische Verankerung	111
5.2	Zuordnung von Verantwortung im IT-Risikomanagement-Prozess	117
5.3	Schritt 1: Definition des Kontexts	120
5.4	Schritt 2: Identifikation	124
5.5	Schritt 3: Analyse	131
5.6	Schritt 4: Bewertung	137
5.7	Schritt 5: Behandlung der IT-Risiken	140
5.8	Reporting, Kommunikation und Beratung	143
5.9	IT-Risiko-Controlling	150
6	Methoden und Werkzeuge für das IT-Risikomanagement	155
6.1	Methoden und Werkzeuge	156
6.2	Dokumente	184
6.3	Hilfestellungen für die Methoden- und Werkzeugwahl	192
6.4	Software für das IT-Risikomanagement	193
6.4.1	Anforderungen	195
6.4.2	Übersicht über Lösungen	199

7	Risikomanagement im IT-Betrieb	203
7.1	Organisation des IT-Betriebs	205
7.1.1	Zentraler und dezentraler Betrieb	205
7.1.2	Outsourcing und Outtasking	214
7.1.3	Cloud Computing	222
7.2	Unzulänglichkeiten, Fehler und Ausfälle	226
7.2.1	Ursache »Mitarbeiter, Kunde, Partner«	226
7.2.2	Ursache »Daten«	228
7.2.3	Ursache »Anwendungen und IT-Infrastruktur«	229
7.2.4	Ursache »IT-Prozesse und IT-Organisation«	231
7.2.5	Ursache »IT-Umfeld«	233
7.3	Angriffe	234
7.4	Notfälle und Katastrophen	238
7.5	Nutzung von Mobilgeräten	240
7.6	IT-Betrieb in kleinen Unternehmen	244
8	Risikomanagement in IT-Projekten	249
8.1	Risiken in IT-Projekten	255
8.2	Open-Source-Projekte	263
9	Einführung des IT-Risikomanagements	267
9.1	Schritte zur Entwicklung und Einführung	267
9.2	Wirtschaftlichkeitsbetrachtungen	274
10	Das Interne Kontrollsystem in der IT	279
10.1	Begriff und Aufbau	279
10.2	Konzeption	285
11	Prüfung des IT-Risikomanagements	287
11.1	Formen und Varianten der Prüfung	287
11.2	Prüfungsablauf	293
12	Wie könnte es weitergehen?	303

Anhang	307
A Übersicht über Vorgaben für das IT-Risikomanagement	309
B Glossar	319
C Abkürzungsverzeichnis	327
D Literaturverzeichnis	335
Stichwortverzeichnis	347