

Inhaltsverzeichnis

Vorwort	IX
Einleitung	1
1 Definition von IT-Risikomanagement	5
1.1 Grundlegende Definitionen.....	7
1.1.1 Risiko.....	7
1.1.2 Operationelle Risiken	9
1.1.3 IT-Risiko.....	11
1.1.4 Risikomanagement.....	11
1.1.5 Risikoszenario.....	12
1.1.6 Risikopotenzial	13
1.1.7 Gefahr	13
1.1.8 Schaden.....	13
1.1.9 IT-Notfall/Krisenfall.....	14
1.2 Kategorisierung von Risiken.....	15
1.2.1 Ursachen-/Wirkungsprinzip.....	15
1.2.2 Zeiträume	19
1.2.3 Risikoeigenschaften.....	21
1.2.4 Spezielle Kategorisierung von IT-Risiken	26
1.3 Generische Risikostrategien.....	30
1.3.1 Risikovermeidung	30
1.3.2 Risikoreduzierung.....	31
1.3.3 Risikodiversifikation/-konzentration	31
1.3.4 Risikoübertragung.....	32
1.3.5 Risikotransformation	32
1.3.6 Risikoakzeptanz	33
1.4 Themenabgrenzung.....	33
1.4.1 IT-Security	33
1.4.2 Service Level Management.....	34
1.4.3 Qualitätsmanagement.....	35
1.4.4 IT-/Projektcontrolling	36
1.4.5 Management operationeller Risiken im Unternehmen.....	37

1.4.6	Interne Revision.....	38
1.4.7	Geschäftsrisiko und Ineffizienz	39
1.5	Exemplarische Schadensfälle	40
1.5.1	IT-Katastrophe bei der Danske Bank.....	40
1.5.2	Gepäcktransportsystem-Desaster am Denver International Airport	42
1.5.3	Unterschlagungen bei Charter plc.....	43
1.5.4	Keylogger-Attacke auf die Sumitomo Mitsui Bank	44
2	IT-Risikotransparenz	47
2.1	Kulturelle Voraussetzungen.....	47
2.1.1	Risikokultur	48
2.1.2	Fehlerkultur	51
2.1.3	Wissensmanagement	51
2.2	Identifizierung von IT-Risiken	56
2.2.1	Self-Assessment	56
2.2.2	Prozessanalysen	59
2.2.3	IT-Systemanalyse	63
2.2.4	Schadensfälle analysieren.....	63
2.2.5	Erfahrungsaustausch	67
2.2.6	Prüfungen	70
2.2.7	Allgemeine Bedrohungs-/Risikokataloge	71
2.2.8	Kreativitäts- und Bewertungstechniken.....	71
2.3	Risikoszenarien erarbeiten.....	72
2.3.1	Risikoszenarien definieren.....	73
2.3.2	Risikoszenarien klassifizieren	76
2.3.3	Risikoszenarien operationalisieren	79
2.3.4	Risikoszenarien qualitätssichern.....	85
2.3.5	Risikoportfolio erstellen (Riskmap).....	86
2.4	Bewerten von Risiken.....	87
2.4.1	Grundlegende Bewertungstechniken	88
2.4.2	Kausal-Analysen.....	95
2.4.3	Quantitative Ansätze.....	99
2.4.4	Detaillierte Systemrisikoanalyse	102
2.4.5	Einzelssystem-Restrisikoanalyse (ESRRA).....	106
2.4.6	Projektrisikoanalyse.....	115
2.5	Risikoindikatoren identifizieren	120
2.5.1	Eigenschaften von Risikoindikatoren	123
2.5.2	Risikoindikatorarten	126
2.5.3	Grenzwertdefinitionen	128
2.5.4	IT-Risikoindikatoren operationalisieren/aggregieren	129
2.6	Exkurs: Exemplarische Definition eines Risikoindikators	130

3	IT-Risikosteuerung	155
3.1	IT-Risk-Policy	135
3.1.1	Definition und Ziele des IT-Risikomanagements	135
3.1.2	Organisatorische Eingliederung des IT-Risikomanagements	136
3.1.3	Risikoeinteilungen/-strukturen.....	138
3.1.4	IT-Risikostrategie	139
3.1.5	Methoden des IT-Risikomanagements.....	146
3.2	Managementtechniken.....	147
3.2.1	IT-Risikoportfoliosteuerung	148
3.2.2	Balanced Scorecard.....	153
3.3	Risikoreduzierungsmaßnahmen	162
3.3.1	IT-Architektur.....	163
3.3.2	IT-Security.....	166
3.3.3	IT-Controlling.....	167
3.3.4	IT-Projektmanagement	169
3.3.5	HR-Management.....	174
3.3.6	Qualitätsmanagement.....	177
3.3.7	Anwendungsentwicklung.....	179
3.3.8	RZ-Betrieb	182
3.3.9	Standards und Best Practices	184
3.3.10	Schadensmanagement.....	199
3.3.11	Outsourcing.....	201
3.4	Risikoprognosen	206
3.4.1	Elemente von Zeitreihen	206
3.4.2	Wirtschaftlichkeitsberechnungen für Risikoreduzierungsmaßnahmen	207
3.4.3	Risikoportfolioänderungen	213
3.5	Reporting der IT-Risiken	214
3.5.1	Reportinginhalte.....	215
3.5.2	Reportingarten	218
3.5.3	Risikomanagement-Informationssysteme (RMIS).....	220
3.6	Exkurs: Anwender-IT-Risiken.....	222
4	Grundlagen des IT-Krisenmanagements	227
4.1	Anforderungen an das IT-Krisenmanagement	229
4.1.1	Krisenprävention.....	229
4.1.2	Business Continuity	230
4.1.3	Disaster Recovery	230
4.2	Inhalte des IT-Krisenmanagements	231
4.2.1	Kritikalitätsanalyse	231
4.2.2	Krisenpräventionsmaßnahmen.....	238
4.2.3	Notfallkonzepte.....	242

4.3	Struktur des IT-Krisenmanagements	249
4.3.1	Implementierung in das Unternehmenskrisenmanagement	249
4.3.2	IT-Krisenstab	250
4.3.3	IT-Krisenprozesse.....	251
4.3.4	Dokumentation des IT-Krisenmanagements.....	255
4.4	Nachhaltigkeit.....	257
4.4.1	Aktualisierung	258
4.4.2	Qualitätssicherung	258
4.4.3	Schulung der Mitarbeiter	259
4.4.4	Notfallübungen	261
4.4.5	Kommunikation	262
Abbildungsverzeichnis		265
Tabellenverzeichnis		267
Literaturverzeichnis		269
Stichwortverzeichnis		277