Inhaltsverzeichnis

1 Einführung 1
1.1 Warum beschäftigen sich Unternehmen mit Risiken? 1
1.2 Risiken und Chancen bei unternehmerischen Tätigkeiten 3
1.3 Inhalt und Aufbau dieses Buchs 4
Literatur 6

Teil I Grundlagen erarbeiten 7

2 Beschäftigung mit Risiken und Risikomanagement 9
2.1 Vernetzte Aktivitäten und Stellenwert Risikomanagement 9
2.2 Betroffene, Kontext und Abgrenzung Risikomanagement 11
2.3 Definition des Begriffs „Risiko“ 11
2.4 Risikomodell und Risikofaktoren 14
2.5 Messbarkeit von Risiken 15
2.5.1 Risiko kombiniert aus Wahrscheinlichkeit und Schadenshöhe 15
2.5.2 Probleme bei Risikobestimmung mittels einfacher Multiplikation 19
2.6 Subjektivität bei Einschätzung und Bewertung der Risiken 20
2.7 Hilfsmittel zur Analyse, Aufbereitung und Darstellung der Risiken 21
2.7.1 Risiko-Bewertungs-Matrix 21
2.7.2 Kriterien zur Schadenseinstufung 23
2.7.3 Kriterien zur Häufigkeitseinstufung 25
2.7.4 Risiko-Kategorien und Risiko-Arten 27
2.7.5 Beispiele von Risiko-Arten 28
2.7.6 Risiko-Landkarte, Risiko-Portfolio und Akzeptanz-Kriterien 29
2.7.7 Risiko-Register 31
2.8 Risiko-Aggregation und Abhängigkeiten 33
2.9 Messung der Risiken mit Risikomasszahlen 35
2.9.1 Stochastische Methoden zur Bestimmung des Risikos 36
2.9.2 Risiko-Analyse und -Überwachung mit Indikatoren 40
2.10 Risiko-Organisation 41

Bibliografische Informationen
http://d-nb.info/1127879820

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

2.11 Kontrollfragen und Aufgaben 42
Literatur 43

3 Risikomanagement als Prozess 45
3.1 Generelle Eigenschaften des Risikomanagement-Prozesses 45
3.1.1 RM-Prozess in einem übergeordneten RM-Framework 46
3.1.2 Modellcharakter des RM-Prozesses 47
3.2 Kommunikation und Konsultation 48
3.3 Festlegung Risikomanagement-Kontext 49
3.4 Risiko-Assessment 52
3.4.1 Risiko-Identifikation (Risk Identification) 53
3.4.2 Risiko-Analyse (Risk Analysis) 56
3.4.3 Teil-Analysen 58
3.4.4 Risiko-Bewertung (Risk Evaluation) 62
3.5 Systematische Risiko-Assessment-Methoden 64
3.5.1 Methoden der Risiko-Identifikation 64
3.5.2 Kollektionsmethoden 65
3.5.3 Suchmethoden 65
3.5.4 Auswahl passender Assessment-Methoden 69
3.6 Risiko-Behandlung 69
3.7 Akzeptanz- und Iterationsentscheide 74
3.8 Überwachung und Überprüfung 75
3.9 Universeller Risikomanagement-Prozess 76
3.10 Kontrollfragen und Aufgaben 77
Literatur 78

Teil II Anforderungen aus Unternehmenssichtberücksichtigen 79

4 Risikomanagement, ein Pflichtfach der Unternehmensführung 81
4.1 Risikomanagement integriert in das Führungssystem 82
4.2 Anforderungen an die Unternehmensführung 84
4.2.1 Corporate Governance 85
4.3 GRC-Anforderungen der Gesetzgeber und Regulierer 86
4.3.1 Gesetz KonTraG in Deutschland 87
4.3.2 Obligationenrecht in der Schweiz 88
4.3.3 Swiss Code of best Practice for Corporate Governance 90
4.3.4 Rahmenwerke Basel II und Basel III 91
4.3.5 Sarbanes-Oxley Act (SOX) und COSO-Rahmenwerke 98
4.3.6 EuroSOX, 8. EU Richtlinie 102
4.3.7 IT-Sicherheitsgesetz in Deutschland 104
4.3.8 Anstrengungen hinsichtlich Informationssicherheit in der Schweiz 105
4.3.9 Datenschutz: Eine wichtige Unternehmensanforderung 108

4.4 Anforderungen an das Risikomanagement als Anliegen der Kunden und der Öffentlichkeit ... 111
4.5 Hauptakteure im unternehmensweiten Risikomanagement ... 113
4.6 Kontrollfragen und Aufgaben ... 115
Literatur ... 116

5 Risikomanagement integriert in das Management-System ... 119
5.1 Management-Ebenen für ein integriertes Risikomanagement ... 119
5.2 Unternehmensweites Risikomanagement ... 121
5.3 Normatives Management ... 122
5.3.1 Unternehmens-Vision als wichtiges normatives Element ... 122
5.3.2 Unternehmens-Politik ... 123
5.3.3 Unternehmens-Verfassung ... 124
5.3.4 Unternehmens-Kultur ... 125
5.3.5 Mission als wichtige Rahmenbedingung für die Strategischen Ziele ... 125
5.3.6 Vision als Input zum Strategischen Management ... 126
5.4 Strategisches Management ... 127
5.4.1 Strategische Ziele ... 128
5.4.2 Strategien ... 131
5.5 Balanced Scorecard zum Umsetzen der Unternehmens-Anforderungen ... 132
5.5.1 Strategie-Umsetzung mittels Balanced Scorecards (BSC) ... 133
5.5.2 Perspektiven der Balanced Scorecard ... 135
5.5.3 Unternehmensübergreifende BSC ... 139
5.5.4 Balanced Scorecard und COBIT für die IT-Strategie ... 139
5.5.5 IT-Indikatoren in der Balanced Scorecard ... 141
5.5.6 Operatives Management (Gewinn-Management) ... 143
5.5.7 Policies und Pläne ... 144
5.5.8 Risikopolitische Grundsätze ... 146
5.6 Umsetzung von Anforderungen mit Management-Systemen ... 146
5.6.1 Management-Systeme ... 147
5.6.2 Vereinheitlichung der Management-System-Standards (MSS) durch ISO ... 149
5.7 Kontrollfragen und Aufgaben ... 150
Literatur ... 151

Teil III Informations-Risiken erkennen und bewältigen ... 153

6 Informationssicherheits- und IT-Risiken ... 155
6.1 Veranschaulichung der Risikozusammenhänge am Modell ... 155
6.2 Informationen – die risikoträchtigen Güter ... 156
6.3 System-Ziele für Risiken der Informationssicherheit und der IT ... 159
6.4 Informationssicherheit versus IT-Sicherheit ... 161

6.5 Informationssicherheits-Risiken versus IT-Risiken ... 162
6.6 Kontrollfragen und Aufgaben ... 163
Literatur ... 163

7 Governance der Informationssicherheit und der IT ... 165
7.1 IT-Governance versus Informationssicherheits-Governance ... 166
7.1.1 IT-Governance nach ITGI der ISACA ... 168
7.1.2 Informationssicherheits-Governance nach ITGI der ISACA ... 170
7.1.3 Praktische Umsetzung der Anforderungen „Informationssicherheit" ... 172
7.2 Organisatorische Funktionen für Informations-Risiken ... 174
7.2.1 Chief Information Officer (CIO) ... 174
7.2.2 Chief Information Security Officer ... 175
7.2.3 Information Security Manager ... 176
7.2.4 Business-Owner, IT-Owner und IT-Administratoren ... 177
7.2.5 Information Security Steering Committee ... 178
7.2.6 Organisatorische „Checks and Balances" ... 179
7.3 Kontrollfragen und Aufgaben ... 181
Literatur ... 181

8 Verantwortlichkeiten und Inhalte von Führungsinstrumenten gemäss Führungspyramide ... 183
8.1 Informations-Risikomanagement in der Führungs-Pyramide ... 184
8.1.1 Risiko- und Sicherheits-Policy auf der Unternehmens-Ebene ... 185
8.1.2 Informationsrisiko-Policy (Information Risk Policy) ... 186
8.1.3 Informationssicherheits-Policy (Information Security Policy) ... 186
8.1.4 Rahmenkonzept mit Weisungen und Anleitungen ... 189
8.1.5 Informationssicherheits-Architektur und -Standards ... 191
8.2 Einrichtung von Grundschutz ... 194
8.3 IT-Sicherheitskonzepte ... 196
8.4 Kontrollfragen und Aufgaben ... 196
Literatur ... 197

9 Informations-Risikomanagement mit Standard-Regelwerken ... 199
9.1 Bedeutung von Standard-Regelwerken ... 200
9.2 Risikomanagement mit der Standard-Reihe ISO/IEC 2700x ... 200
9.3 Für Informations-Risikomanagement wichtige Standards der ISO/IEC 270xx-Reihe ... 202
9.3.1 Informationssicherheits-Management-System nach ISO/IEC 27001 ... 202
9.3.2 Code of Practice ISO/IEC 27002 ... 207
9.3.3 Informationssicherheits-Risikomanagement mit ISO/IEC 27005 ... 211

9.4 COBIT® 5 Framework ... 213
9.4.1 COBIT® 5 als IT-Governance und IT-Management-Rahmenwerk ... 214
9.4.2 Enabler ... 215
9.4.3 Enabler-Kategorie „Prozesse“ ... 216
9.4.4 Zielsystem in COBIT 5 ... 217
9.4.5 Enabler-Ziele in COBIT 5 und COBIT 4.1 ... 220
9.4.6 IT-Risikomanagement und Informationssicherheit in COBIT 5 ... 222
9.4.7 COBIT 5, COBIT 4.1 und andere Rahmenwerke ... 225
9.5 BSI-Standards und Grundschutzkataloge ... 227
9.5.1 Management-Systeme für Informationssicherheit (ISMS) auf der Basis Grundschutz ... 228
9.5.2 Sicherheitsprozess gemäss IT-Grundschutz ... 228
9.5.3 Leitlinie zur Informationssicherheit und Sicherheitskonzept im Informationssicherheitsprozess ... 230
9.5.4 IT-Grundschutz-Kataloge ... 231
9.6 Regelwerke mit Teilaspekten des Informations-Risikomanagements ... 231
9.6.1 Offenes Framework „Common Vulnerability Scoring System“ ... 231
9.6.2 ISO/IEC 15408 Common Criteria ... 232
9.6.3 Service-Management-Standards ... 234
9.7 Beurteilung von Informations-Risikomanagement-Prozessen mit ISO/IEC 33020 ... 236
9.8 Maturity-Modell bei COBIT 4.1 und Prozessfähigkeits-Modell ISO/IEC 33020 bei COBIT 5 ... 239
9.9 Einführung und Einsatz von Standard-Regelwerken ... 241
9.10 Kontrollfragen und Aufgaben ... 244
Literatur ... 245

10 Methoden und Werkzeuge für das Informations-Risikomanagement ... 247
10.1 IT-Risikomanagement mit Sicherheitskonzepten ... 248
10.1.1 Kapitel „Kontextbeschreibung“ ... 250
10.1.2 Kapitel „Risiko-Identifikation“ ... 255
10.1.3 Kapitel „Risiko-Analyse“ ... 256
10.1.4 Schwachstellen-Analyse anstelle einer Risiko-Analyse im Sicherheitskonzept ... 259
10.1.5 Kapitel „Bewertung und Anforderungen an Massnahmen“ ... 260
10.1.6 Kapitel „Definition und Beschreibung der Massnahmen“ ... 261
10.1.7 Kapitel „Umsetzung Massnahmen“ ... 263
10.1.8 Kommunikation und kooperative Ausarbeitung der Kapitel ... 265
10.1.9 Risiko-Akzeptanz, Konzept-Abnahme und -Anpassung ... 265
10.1.10 Überwachung und Überprüfung ... 266
10.2 Die CRAMM-Methode ... 266

10.3 Fehlermöglichkeits- und Einfluss-Analyse (FMEA) ... 272
10.4 Fehlerbaum-Analyse ... 274
10.5 Ereignisbaum-Analyse ... 279
10.6 Kontrollfragen und Aufgaben ... 280
Literatur ... 281

11 Kosten/Nutzen-Relationen der Risiko-Behandlung ... 283
11.1 Forderung nach quantitativen Aussagen über Informationssicherheit ... 284
11.2 Formel für „Return on Security Investments" (ROSI) ... 285
11.3 Ermittlung der Kosten für die Sicherheitsmassnahmen ... 287
11.4 Kostenermittlung der behandelten Risiken ... 290
11.5 Massnahmen-Nutzen ausgerichtet an Unternehmenszielen ... 291
11.6 Fazit zu Ansätzen der Sicherheit-Nutzen-Bestimmung ... 292
11.7 Kontrollfragen und Aufgaben ... 293
Literatur ... 293

Teil IV Unternehmens-Prozesse meistern ... 295

12 Risikomanagement-Prozesse im Unternehmen ... 297
12.1 Verzahnung der RM-Prozesse im Unternehmen ... 297
12.1.1 Risiko-Konsolidierung ... 300
12.1.2 Subsidiäre RM-Prozesse ... 300
12.1.3 Risiko-Ownership in der IT ... 302
12.2 Risikomanagement im Strategie-Prozess ... 302
12.2.1 Risikomanagement und IT-Strategie im Strategie-Prozess ... 303
12.2.2 Periodisches Risiko-Reporting ... 305
12.3 Kontrollfragen und Aufgaben ... 306
Literatur ... 306

13 Geschäftskontinuitäts-Management und IT-Notfall-Planung ... 307
13.1 Bedeutung des Geschäftskontinuitäts-Managements und der IT-Notfallplanung ... 308
13.2 Pläne zur Unterstützung der Kontinuität und Widerstandsfähigkeit gegen eingetretene Risiken ... 309
13.2.1 Einzelne Pläne für einzelne Planungsgebiete ... 309
13.2.2 Pläne mit Zuordnung zur IT oder Informationssicherheit ... 311
13.2.3 Abstimmung der Pläne untereinander ... 313
13.3 Geschäfts-Kontinuitäts-Management-System(BCMS) im Unternehmens-Risikomanagement ... 313
13.4 Einrichtung Kontinuitäts-Management-System ... 316
13.4.1 Kontext des Unternehmens ... 316
13.4.2 Führung ... 317
13.5 BCMS-Aktivitäten im PDCA-Zyklus ... 319
13.5.1 Planung ... 319

13.5.2 Unterstützung ... 320
13.5.3 Operation ... 322
13.6 Leistungsbewertung ... 339
13.6.1 Überwachung und Überprüfung ... 339
13.6.2 Internes und externes Audit ... 339
13.6.3 Überprüfung durch Management ... 340
13.7 Kontinuierliche Verbesserungen und Wiederholungen ... 342
13.8 IT-Notfallplan und Incident- und Vulnerability-Management ... 343
13.8.1 Organisation eines Incident- und Vulnerability-Managements ... 347
13.8.2 Behandlung von plötzlichen Ereignissen als spezieller RM-Prozess ... 350
13.9 Kontrollfragen und Aufgaben ... 351
Literatur ... 352

14 Risikomanagement im Lifecycle von Informationen, Systemen und Applikationen ... 353
14.1 Schutz der Informationen im Informations-Lifecycle ... 354
14.1.1 Einstufung der Informations-Risiken aufgrund ihrer Anforderungen ... 354
14.1.2 Massnahmen gemäss der Einstufungen in den einzelnen Schutzphasen ... 355
14.2 Lifecycle von IT-Systemen ... 355
14.3 Informations-Risikomanagement im IT-System-Lifecycle ... 357
14.3.1 Vorgehen in den Aufbauphasen des System-Lifecycles ... 357
14.3.2 Vorgehen in den Phasen „Betrieb", „Optimierung" und „Systemabbau" ... 358
14.4 Risikomanagement in standardisierten Vorgehens-Methoden ... 359
14.4.1 Datenschutz, Informationssicherheit und RM mit dem V-Modell XT ... 359
14.4.2 Datenschutz, Informationssicherheit und RM mit der HERMES Methode ... 361
14.4.3 Service-Management (ITIL®) und Applikations-Management (ASL®) ... 364
14.4.4 Applikationssicherheit und Risikomanagement gemäss ISO/IEC 27034-x ... 366
14.5 Kontrollfragen und Aufgaben ... 370
Literatur ... 370

15 Risikomanagement in Outsourcing-Prozessen ... 371
15.1 Licht und Schatten beim Outsourcing ... 371
15.2 IT-Risikomanagement im Outsourcing-Vertrag ... 373
15.2.1 Sicherheitskonzept im Sourcing-Lifecycle ... 374
15.2.2 Sicherheitskonzept beim Dienstleister ... 377

15.3 Kontrollfragen und Aufgaben ... 378
Literatur ... 379

16 Risikomanagement bei Nutzung und Angebot von Cloud-Computing ... 381
16.1 Prinzip und Definitionen Cloud-Computing ... 382
16.1.1 Wesentliche Charakteristiken ... 384
16.1.2 Service-Modelle ... 384
16.1.3 Deployment-Modelle ... 385
16.2 Informationssicherheits-Risiken beim Cloud-Computing ... 386
16.3 Cloud-Sourcing als Service aus der Kundenperspektive ... 386
16.3.1 Phase 1: Cloud-Sourcing-Strategie ... 389
16.3.2 Phase 2: Evaluation und Auswahl ... 390
16.3.3 Phase 3: Vertragsentwicklung ... 391
16.3.4 Phase 4: Cloud-Sourcing-Management ... 392
16.4 Risikomanagement für Cloud-Computing aus Kundensicht ... 393
16.4.1 Kontext im Sicherheitskonzept für Cloud-Computing-Einsatz ... 394
16.4.2 Risiko-Assessment ... 396
16.5 Cloud-Sourcing-Lifecycle auf der Provider-Seite ... 402
16.6 Kontrollfragen und Aufgaben ... 403
Literatur ... 404

17 Cyber-Risikomanagement ... 405
17.1 Gründe für die Bedeutung der Cyber-Risiken ... 406
17.2 Definitionen im Zusammenhang mit Cyber-Risiken ... 407
17.3 Cyber-Risiken im Risikomodell ... 409
17.3.1 Risikofaktoren gemäss Risikomodell ... 412
17.3.2 Risikoobjekte und deren Anforderungen ... 413
17.4 Bedrohungen, Schwachstellen und Schäden bei „absichtlichen“ Ursachen ... 414
17.4.1 Bedrohungsquellen ... 414
17.4.2 Bedrohungsereignisse und Angriffs-Mechanismen ... 414
17.4.3 Schwachstellen (Vulnerabilities) ... 417
17.4.4 Schäden (Impacts) bei Cyber-Risiken ... 419
17.5 Risiko-Assessment von „absichtlichen“ Risiken anhand von Beispielen ... 420
17.5.1 Identifikation des Schadens in beiden Fällen ... 422
17.5.2 Identifikation der Risikofaktoren rückwärts bis hin zu den Bedrohungsquellen ... 423
17.5.3 Aus den Beispielsfällen Anthem Inc. und OPM abgeleitete Assessment-Ergebnisse ... 425
17.6 Assessment von unabsichtlichen Cyber-Risiken ... 425

17.7 Risiko-Behandlung von Cyber-Risiken 429
17.7.1 Vielfalt und Dynamik der Cyber-Risiken und Massnahmen 429
17.7.2 Policies und Anleitungen für Cyber-Sicherheit 431
17.7.3 Management der Cyber-Risiken mittels ISMS oder Sicherheitskonzept(en) 432
17.7.4 Bewusstseinsförderung (Awareness), Tests und Übungen 432
17.7.5 Technische Massnahmen zur Behandlung von Cyber-Risiken 433
17.7.6 Einsatz eines SIEM und anderer Werkzeuge zur Entdeckung von APT-Angriffen 435
17.7.7 Massnahmen gegen „Distributeted-Denial-of-Service-Angriffe" 436
17.8 Kontrollfragen und Aufgaben 438
Literatur 438

Anhang 441
A.1 Beispiele von Risiko-Arten 441
A.2 Beispiele von „Cyber Threats" 443
A.3 Muster Ausführungsbestimmung für Informationsschutz 446
A.4 Formulare zur Einschätzung von IT-Risiken 450
A.5 Beispiele zur Aggregation von operationellen Risiken 454
A.5.1 Beispiel der Bildung eines VAR durch Vollenumeration 454
A.5.2 Beispiele für Verteilung von Verlusthöhen und Verlustanzahl 455
A.5.3 Aggregation mittels Monte-Carlo-Methode 456

Stichwortverzeichnis 459