

Inhaltsverzeichnis

Vorwort	7
Geleitworte	9
Abbildungsverzeichnis	25
Tabellenverzeichnis	28
1 Einleitung	29
2 Unternehmensziele bis zur Einbettung des Risikomanagements	39
2.1 Unternehmensziele	40
2.2 Unternehmensstrategie	43
2.3 Unternehmenspolitik	44
2.4 Bestimmung der Steuerungselemente	45
2.5 Ableiten der Risikostrategie	46
2.6 Unternehmenskultur	47
2.6.1 Risikomanagementkultur	49
2.6.2 Tone-at-the-Top	50
2.6.3 Ziele vereinbaren – aber richtig	52
2.6.3.1 Allgemeine Fehlsteuerungen	52
2.6.3.2 Konkrete Beispiele	53
2.6.4 Routinisierung, Standardisierung und Modularisierung	54
2.6.5 Auswirkungen einer starken Unternehmenskultur	57
2.6.5.1 Positive Wirkungen	57
2.6.5.2 Negative Wirkungen	57
2.6.6 Changemanagement	58
2.6.6.1 Wirkfaktoren	59
2.6.6.2 Veränderungsprozess	62
2.6.7 Die Rolle der Risk-und-Compliance-Officer	69
2.7 Wesentliche Vorüberlegungen	71
2.7.1 Proportionalitätsprinzip	72
2.7.2 Ein zweiter Blick auf die Risiken	74
2.7.3 Risiken der zweiten und dritten Ordnung	75
2.7.4 Risikodaten und Medienberichte	76
2.7.5 Psychische Effekte und Einstellungen	79
2.7.5.1 Selektive Wahrnehmung	80
2.7.5.2 Die moderne Informationssituation	81
2.7.5.3 Geringster Widerstand und Verdrängung	82
2.7.5.4 Kognitive Tiefenursachen: Bias	83
2.7.5.5 Priming und Framing	84

2.7.6	Schwarze Schwäne, ihr Nachwuchs und selbst gelegte Eier	85
2.7.6.1	Es beginnt meist ganz oben	85
2.7.6.2	Sich daraus entwickelnde schwarze Schwäne	86
2.7.6.3	... deren Nachwuchs	87
2.7.6.4	... und weitere selbst gelegte Eier	88
2.7.7	Top-down und bottom-up	89
2.7.7.1	Top-down	89
2.7.7.2	Bottom-up	90
2.8	Umgang mit Ressourcen	91
2.8.1	Die wichtigste Ressource »Mensch«	92
2.8.1.1	Das Team	94
2.8.1.2	Agilität	94
2.8.2	Risikocontrolling und Compliance als Wettbewerbsfaktor	99
2.8.2.1	Unternehmensschutz und Regulierung	100
2.8.2.2	Haftungsschutz	101
2.8.2.3	Erschließung von Märkten und Lizenzerweiterungen	101
2.8.2.4	Pitch-Perfect und Ausschreibungen	101
2.8.2.5	Rating	103
2.8.2.6	Lenkung von und Umgang mit Ressourcen	103
2.8.2.7	Prävention sonstiger strafbarer Handlungen	105
2.8.2.8	Third-Party Risk Management	106
2.8.2.9	Prozessdesign, -effizienz und Digitalisierung	106
2.8.2.10	Werbewirksamkeit	107
2.8.2.11	Versicherungen	108
2.8.2.12	Risikoportfolio als Einstieg für neue Mitarbeitende	109
2.8.3	Organisationen als Human-Sammler	110
2.8.4	Desinvestition – aber mit Augenmaß und -kontakt	111
2.8.5	Daten als wertvolle Basis	111
2.8.5.1	Daten externer Parteien	113
2.8.5.2	Intern entstehende Daten	114
2.8.5.3	Analytische Anforderungen und Einschränkungen	115
2.8.5.4	Big Data	116
2.8.6	Glaubwürdigkeitspunkte als Indikator	119
2.8.6.1	Organisatorische Verortung eines Bereichs	120
2.8.6.2	Zuhören und Aussagen prüfen	120
2.8.6.3	Verhaltensweisen analysieren	121
2.8.6.4	Entwicklungsstand einer Abteilung	122
2.8.6.5	Motivationen feststellen	122
2.8.7	Drill Down	123

3	Risiko, Regulierung und effiziente Verankerung im Unternehmen	125
3.1	Begriffseingrenzung »operationelle Risiken«	126
3.1.1	Aufbau- und Ablauforganisation sowie Prozesse	128
3.1.2	Menschliches Versagen	131
3.1.2.1	Allgemeine Risiken	132
3.1.2.2	Spezielle Risiken	134
3.1.3	Systemrisiken (IT)	135
3.1.3.1	Allgemeine Risiken	135
3.1.3.2	Regulatorische Anforderungen und Risiken	136
3.1.4	Rechtsrisiken	142
3.1.5	Externe Risiken	144
3.2	Übergeordnete Risikosteuerung	145
3.2.1	Risikosteuerung	146
3.2.1.1	Präventiv	147
3.2.1.2	Detektiv	147
3.2.1.3	Korrektiv	147
3.2.2	Risk Committee	147
3.2.3	Risk Appetite	148
3.3	Effiziente und effektive Regulierungsarchitektur	150
3.3.1	Zusammenfassung von Anforderungen	152
3.3.2	Nutzenstiftende Erweiterungen	154
3.3.3	Digitalisierte Umsetzung	154
3.4	Überwachung und Verankerung	155
3.4.1	Prüf- und Überwachungsfunktionen	155
3.4.1.1	Unternehmenszugehörige Überwachungsfunktionen	156
3.4.1.2	Unternehmensexterne Prüf- und Aufsichtsinstanzen	161
3.4.2	Kodifizierung und Verankerung	164
3.4.2.1	Weisungswesen	165
3.4.2.2	Handbücher und Prozessbeschreibungen	168
3.4.2.3	Checklisten	168
3.4.2.4	Evidenz	168
3.4.2.5	Schulungen und Trainings	168
3.4.2.6	Fokus auf Ausbildungstechnik und Themenstellungen	169
4	Der Risikomanagementprozess bzw. das Risk Assessment	173
4.1	Identifikation	176
4.1.1	Erfassung aller Risiken	176
4.1.2	Wirkfaktoren und Informationen	177
4.1.2.1	Extern	177
4.1.2.2	Intern	179

4.2	Beurteilung und Bewertung	181
4.2.1	Kritische Würdigung einiger Bewertungs- und Beurteilungsansätze	182
4.2.1.1	Peer-Vergleiche	183
4.2.1.2	Statistische Methoden	184
4.2.1.3	CAPM-Ansatz	184
4.2.1.4	Scoring-Verfahren	184
4.2.1.5	Earnings Volatility	184
4.2.1.6	Organisations- und Unterlagenanalyse	185
4.2.1.7	Prozessorientierter Ansatz	185
4.2.1.8	Subjektivität von Beurteilungen	187
4.2.2	Beurteilung durch Experten	187
4.2.3	Die Beurteilung und Bewertung des Brutto- (Inherent) und Nettorisikos (Residual)	191
4.3	Priorisierung	191
4.3.1	Kontinuierliche Bewertung von Risiken	191
4.3.2	Verzerrungen und Abhängigkeiten	192
4.3.2.1	Persönliche subjektive Sichtweisen	192
4.3.2.2	Eintritt von Risiken	194
4.3.2.3	Korrelationen	195
4.3.2.4	Reihung von Risiken	202
4.4	Risikomanagement	203
4.4.1	Akzeptanz	204
4.4.2	Übertragen und Transferieren	205
4.4.3	Vermeidung	206
4.4.4	Verminderung	207
4.4.5	Kompensation	207
4.4.6	Wirtschaftlichkeit der Maßnahmen	209
4.4.6.1	Soll-Abweichungskosten	209
4.4.6.2	Maßnahmenkosten	209
4.4.6.3	Entscheidungsfindung	210
4.5	Datenzuweisung	212
4.6	Rückmeldung	213
4.7	Auswertung und Datennutzung	213
4.7.1	Qualität der Daten	213
4.7.2	Auswertung, Entwickeln, Monitoring und Berichtswesen	214
4.7.2.1	Maßnahmenentwicklung	214
4.7.2.2	Monitoring	216
4.7.2.3	Zielgruppenorientierte Information	216
4.7.2.4	Datennutzung und Entscheidungen	218

5	Wertvolle Soll-Abweichungen	223
5.1	Voraussetzungen	224
5.1.1	Soll-Abweichungsdatenbanken	224
5.1.2	Datenqualität	226
5.2	Soll-Abweichungen (Gain, Neutral und Loss)	226
5.2.1	Ursachenanalyse (Root Cause)	227
5.2.2	Weitere Zuordnungen der Soll-Abweichungen	228
5.2.3	Wesentliche Daten und deren Interpretation	229
5.2.3.1	Tag der Soll-Abweichung	229
5.2.3.2	Tag der Identifikation	230
5.2.3.3	Tag der taktischen Behebung	230
5.2.3.4	Tag der nachhaltigen Lösungsentwicklung	230
5.2.4	Soll-Abweichungen ohne finanzielle Auswirkungen	231
5.2.4.1	Beinaheverluste (Near Misses)	232
5.2.4.2	Null-Ereignisse (Zero-Events)	232
5.3	Maßnahmenentwicklung	233
5.3.1	Taktische Maßnahmen	233
5.3.2	Nachhaltige Maßnahmen	233
5.4	Analyse und Quantifizierung	235
5.4.1	Periodisierung	236
5.4.1.1	Schätzung von Erwartungswerten	236
5.4.1.2	Nutzung von Erfahrungswerten	237
5.4.2	Faltung	237
5.5	Risikoaggregation	241
5.5.1	Risikoportfolio	241
5.5.2	Berechnungsansätze	243
5.5.2.1	Risk-Adjusted Return on Capital (RAROC), Return on Risk-Adjusted Capital (RORAC)	243
5.5.2.2	Monte-Carlo-Simulation	243
6	Werkzeuge des Risikomanagements	245
6.1	(Key) Procedure Controls (KPC)	245
6.1.1	Aufbau eines Kontrollframeworks	248
6.1.2	Kontrolldokumentation	250
6.1.2.1	Kontrollziel	250
6.1.2.2	Kontrollbeschreibung	250
6.1.3	Kontrolltest	252
6.1.3.1	Design-Effektivität	252
6.1.3.2	Operating-Effektivität	253
6.1.3.3	Klassifikation eines Testergebnisses	253

6.2	(Key) Risk Indicators (KRI)	255
6.2.1	Entwicklungskriterien	255
6.2.2	Review und Überprüfung	256
6.2.3	Eskalationslevel (RAG-Status)	256
6.3	(Key) Performance Indicators (KPI)	257
6.3.1	Entwicklungskriterien	258
6.3.2	Eskalationslevel (RAG-Status)	258
7	Self-Identified-Issue-Konzept (SII)	261
7.1	Vorteile des Konzepts	261
7.2	Ein klarer Rahmen determiniert den Erfolg	262
7.2.1	Definition der Eingangsvoraussetzungen	262
7.2.2	Ablauf des Prozesses	263
8	»Neu-Produkt und wesentliche Änderungen«-Prozess (NPP)	265
8.1	Neue und bestehende Produkte	267
8.1.1	Produktentwicklung für Kunden	267
8.1.2	Bestehende Produkte	268
8.2	Regulierungsanforderungen	269
8.3	Neue Märkte	269
8.4	Wesentliche Prozessänderungen	269
9	Projektmanagement	271
9.1	Interdisziplinarität	273
9.1.1	Weisung	273
9.1.2	Team	274
9.2	Steuerung	274
9.2.1	Planung	274
9.2.2	Bericht	275
9.3	Rahmenbedingungen mit Risiken	276
9.3.1	Zeit	276
9.3.2	Qualität	276
9.3.3	Auftrag	276
9.3.4	Ressourcen	277
10	Sonstige strafbare Handlungen	279
10.1	Motivationsfaktoren und Denkweisen	280
10.1.1	Schwachstellen in der Aufbau- und Ablauforganisation	281
10.1.2	Personenebene	282
10.1.3	Sicht- und Denkweise eines Straftäters	283
10.1.4	White-Collar-Crime-Profil	284

10.2	Umgang mit Vorfällen	285
10.3	Wirkrichtungen auf das Unternehmen	287
10.3.1	Externe strafbare Handlungen	288
10.3.2	Interne strafbare Handlungen	289
10.4	Gefährdungsanalyse	291
10.4.1	Typologien und Beispiele	294
10.4.1.1	Externe Angreifer	295
10.4.1.2	Kombinationen von internen und externen Angreifern	297
10.4.1.3	Interne Angreifer	302
10.4.2	Bestandsaufnahme der Gefährdungen	303
10.4.3	Management der Gefährdungen	305
10.4.3.1	Sprengung Geldausgabeautomat (GAA)	305
10.4.3.2	Preismanipulation von Wertpapieren	306
10.4.3.3	Provisionsbetrug durch Involvierung eines Maklers	306
10.4.4	Nettorisiko-Betrachtung und Risikoappetit	308
10.4.5	Jährliche Analyse und Ad-hoc-Aktualisierung	309
10.5	Reverse Testing	309
11	Risikomodelle, Kalkulationsschemen und Ratingsysteme	313
11.1	Governance	314
11.2	Quellen der Soll-Abweichungen	315
11.2.1	Inputdaten	315
11.2.2	Implementierung	316
11.2.3	Nutzung	317
11.2.3.1	Funktionalität	317
11.2.3.2	Bedienung	318
11.2.4	Ergebnisse	318
11.2.5	Berichtswesen	318
12	Third-Party Risk Management	321
12.1	Auslagerung/Outsourcing	321
12.1.1	Vorüberlegungen, Analyse und Abgrenzung	323
12.1.1.1	Lokale und grenzüberschreitende Auslagerungen	325
12.1.1.2	Bestimmung der Wesentlichkeit	327
12.1.1.3	Abhängigkeit vom Servicedienstleister	329
12.1.1.4	Besondere Anforderungen an IT und Cloud	331
12.1.2	Auswahl eines geeigneten Partners	337
12.1.2.1	Rahmenbedingungen	337
12.1.2.2	Servicedienstleister als langfristiger Partner	338
12.1.2.3	Fachliche Anforderungen	340
12.1.2.4	Finanzielle Anforderungen	341

12.1.2.5	Technische Anforderungen	342
12.1.2.6	Entwicklung eines Alternativplans	342
12.1.3	Vertragerstellung	343
12.1.4	Fortlaufendes Monitoring	345
12.1.5	Auflösung der Geschäftsbeziehung	346
12.2	Übernahme von wesentlichen Aufgaben	347
12.3	Zertifizierungen durch unabhängige Dritte	347
12.3.1	ISAE-3402-Bericht	348
12.3.2	Zertifizierungsmöglichkeiten nach ISO	350
12.3.2.1	ISO 37000 – Good Governance	351
12.3.2.2	ISO 31000 – Risikomanagement	352
12.3.2.3	ISO 37301 – Compliance-Management-System (CMS)	353
12.3.2.4	ISO 27001/2 – Informationssicherheit	354
12.3.2.5	ISO 14001 – Umweltmanagement	354
13	Finanztechnologie und Services (FinTech)	357
13.1	Allgemeine Vorüberlegungen	357
13.1.1	Digitalisierungspotenziale	358
13.1.1.1	Einheitlichkeit von Sprache und Daten	359
13.1.1.2	Interne Potenziale	359
13.1.2	Transformative Strategien	360
13.1.2.1	Globale Kurzdiskussion	360
13.1.2.2	Unternehmen	361
13.1.3	Menschen, Interessen, Ethik und Nachhaltigkeit	362
13.1.3.1	Neudenken auf Führungsebene	363
13.1.3.2	Neudenken auf Ebene der MitarbeiterInnen	364
13.2	Robotic Process Automation (RPA)	364
13.2.1	Einsatzgebiete	365
13.2.2	Erfahrung, Risiken und Regulierung	367
13.2.3	Aus- und Belastungsgrenzen	368
13.2.4	Kosten-Nutzen-Assessment	368
13.3	First Level Automatic Response Systems	370
13.3.1	Vorüberlegungen	370
13.3.2	Einsatzgebiete für Response Systeme	370
13.4	Maintenance Systems	372
13.5	Artificial Intelligence (AI)	373
13.5.1	Machine Learning (ML)	375
13.5.2	Anwendungsbeispiel Cross-Border Compliance	377
13.5.3	Regulierungstechnologie (RegTech)	378

13.6	Risikodatenmanagement und -verwendung	379
13.6.1	Speisung des Data Lakes	380
13.6.2	Erkenntnisgewinnung und Berichtswesen	381
13.6.3	Heat-Maps und Dashboards als Übersichtsinstanz	382
13.6.4	Metaverse/Web 3	382
14	Business Continuity und Resumption Management (BCM)	385
14.1	Business Continuity Planning (BCP)	388
14.1.1	Analyse des Unternehmensumfelds	388
14.1.2	Analyse des Unternehmens	389
14.1.2.1	Festlegung von Zeiten und Datensicherung	390
14.1.2.2	Beurteilung der Wiederherstellungszeit	391
14.1.3	Risk Assessment	393
14.1.4	Systematisierung der Risiken und deren Beeinflussbarkeit	394
14.1.4.1	Interne Ursachen	394
14.1.4.2	Externe Ursachen	394
14.1.5	Entwicklung des Business Continuity Plans (BCP)	398
14.1.6	Test und Wartung	399
14.1.7	Geeigneter Evakuierungsplan und -standort	399
14.1.8	Planung und Routinisierung von Krisenszenarien	400
14.1.8.1	Evakuierung	400
14.1.8.2	Überfall	401
14.1.8.3	Notfallpläne für Reparaturbedarf	402
14.1.9	Faktor Mensch	402
14.1.10	Faktor IT	402
14.2	Incident Response (IR)	403
14.3	Disaster Recovery	405
15	Neue Risiko- und Chancenprofile sowie Wirkfaktoren	407
15.1	Geopolitische Risiken	407
15.1.1	Allgemeine Beispiele	408
15.1.1.1	Ukrainekrieg	408
15.1.1.2	COVID-19-Pandemie	408
15.1.1.3	Volksrepublik China	409
15.1.2	Territoriale Beispiele mit Ausstrahlungswirkungen	409
15.1.2.1	Handelsstreit USA und China	410
15.1.2.2	Brexit	410
15.2	Cyberisiken	410
15.2.1	Physische Angriffe und Vorbereitung	412
15.2.2	Virtuelle Angriffe	413
15.2.2.1	Erpressung und Data Leaks	415
15.2.2.2	Viren und Ransomware	415
15.2.2.3	Initial Access Brokers (IAB)	416

- 15.2.3 Cyberrisiken-Prävention und TIBER 416
 - 15.2.3.1 TIBER-EU 417
 - 15.2.3.2 Risiken im Zusammenhang mit TIBER-Tests 418
- 15.2.4 Berichtswesen 419
- 15.3 Environmental, Social, Governance (ESG) 420
 - 15.3.1 EU Sustainable Finance Taxonomy 425
 - 15.3.2 Theorie of Change 431
 - 15.3.3 Betroffene Bereiche des Finanzdienstleisters 432
 - 15.3.3.1 Governance unter Nachhaltigkeitsaspekten 432
 - 15.3.3.2 Betroffene Finanzdienstleistungsprozesse 440
- 15.4 Datenschutz und DSGVO 449
 - 15.4.1 Datenschutz im internationalen Kontext 450
 - 15.4.2 Daten in der digitalen Ökonomie 451
 - 15.4.2.1 Umgang mit Daten 451
 - 15.4.2.2 Digitale Marktplätze 454
- 16 Epilog und Fazit 457
- Anhänge 463
- Anhang 1 – Risikomanagement für StudentInnen 465
 - Bachelor- und Masterarbeiten 465
 - Plagiatsprüfung 466
 - Bewerbungen 467
- Anhang 2 – Beispiel: Reduktion des Klimawandels 469
- Stichwortverzeichnis 471
- Danksagungen 479
- Der Autor 481