Inhaltsverzeichnis

1 Ausgangssituation und Zielsetzung 1
1.1 Ausgangssituation 3
1.1.1 Bedrohungen 3
1.1.2 Schwachstellen 25
1.1.3 Schutzbedarf und Haftung 29
1.2 Zielsetzung des Sicherheits-, Kontinuitäts- und Risikomanagements 34
1.3 Lösung 34
1.4 Zusammenfassung 36

2 Kurzfassung und Überblick für Eilige 38

3 Zehn Schritte zum Sicherheitsmanagement 44

4 Gesetze, Verordnungen, Vorschriften, Anforderungen 47
4.1 Persönliche Haftungsrisiken und Strafbarkeit 48
4.1.1 Deutschland 48
4.1.2 Schweiz 52
4.2 Haftungsrisiken von Unternehmen 53
4.3 Risikomanagement 53
4.4 Buchführung 54
4.4.1 Deutschland 54
4.4.2 Schweiz 59
4.5 IT-Sicherheit kritischer Infrastrukturen / digitaler Dienste / UBI 59
4.5.1 Deutschland 59
4.5.2 Europäische Union 66
4.6 Datenschutz 66
4.6.1 Deutschland 66
4.6.2 Österreich 68
4.6.3 Schweiz 68
4.6.4 Europäische Union 69
4.6.5 USA 71
4.7 Schutz von Geschäftsgeheimnissen 72
4.8 Arbeitsschutz und Arbeitssicherheit 73
4.8.1 Deutschland 73
4.8.2 Österreich 82
4.8.3 Schweiz 82
4.8.4 Großbritannien 83
4.8.5 Europäische Union 83
4.8.6 USA 84
4.9 Verträge 84
4.10 Mitbestimmung 84
4.11 Gleichbehandlung 85
4.12 Weitere gesetzliche Anforderungen in Deutschland 86
4.13 Unternehmensführung, Corporate Governance 87
4.13.1 Deutschland 87

4.13.2 Schweiz 87
4.13.3 OECD 88
4.14 Energieversorgungsunternehmen 88
4.14.1 Deutschland 88
4.14.2 Schweiz 90
4.15 Telekommunikationsdiensteanbieter 90
4.15.1 Deutschland 90
4.15.2 Österreich 93
4.16 Finanzinstitute und Versicherungsunternehmen 93
4.16.1 Deutschland 93
4.16.2 Schweiz 117
4.16.3 Großbritannien 118
4.16.4 Europäische Union 118
4.16.5 Baseler Ausschuss für Bankenaufsicht (Basel Committee on Banking Supervision, BCBS) 120
4.16.6 USA 124
4.17 Chemische und pharmazeutische Industrie 124
4.17.1 Deutschland 124
4.17.2 Europäische Union 125
4.17.3 USA 126
4.18 Behörden 126
4.18.1 Deutschland 126
4.18.2 Österreich 127
4.19 In USA börsennotierte Unternehmen 128
4.20 Externe Anforderungen – Fazit 129

5 Normen, Standards, Practices 130
5.1 Compliance Management 132
5.1.1 Compliance-Managementsystem: ISO 37301:2021 132
5.1.2 Antikorruptionsmanagementsystem: ISO 37001:2016 132
5.1.3 Whistleblowing-Managementsystem: ISO 37002:2021 132
5.2 Governance 133
5.2.1 Organisation: ISO 37000:2021 133
5.2.2 IT und Daten: ISO/IEC-38500-Familie und COBIT® 2019 133
5.2.3 Informationssicherheit: ISO/IEC 27014:2020 137
5.3 Arbeitsschutz und Arbeitssicherheit 137
5.3.1 ISO 45001:2018, AMS (OHSMS) 137
5.3.2 ANSI Z10.0-2019, AMS (OHSMS) 137
5.3.3 ILO-OSH 138
5.4 Sozialschutz (Social Compliance): SA8000® 138
5.5 Risikomanagement 138
5.5.1 Die ISO-31000-Familie 138
5.5.2 Die ÖNORM-D-4900-Familie 140
5.5.3 OCTAVE® approach, OCTAVE® Allegro, OCTAVE® FORTE 140
5.6 Informationssicherheitsmanagement (ISM) 142
5.6.1 Die ISO/IEC-27000-Familie zum ISM im Überblick 142

5.6.2 ISO/IEC 27001:2022, ISMS – Anforderungen 144
5.6.3 ISO 27001:2022 versus Sicherheitspyramide 147
5.6.4 ISO TS 12812-2: Sicherheit und Datenschutz bei mobilen Finanzdiensten 147
5.6.5 BSI: IT-Grundschutz im Überblick 147
5.6.6 BSI: BSI-Standards im Überblick 148
5.6.7 BSI: IT-Grundschutz-Kompendium im Überblick 148
5.6.8 BSI: BSI-Standards und IT-Grundschutz-Kompendium versus Sicherheitspyramide 150
5.6.9 Federated Identity Management (FIM) 151
5.7 Sicherheit und Resilienz 153
5.7.1 Sicherheitsmanagement der Lieferkette: Die ISO-28000-Familie 153
5.7.2 Sicherheit und Resilienz: Die ISO-22300-Familie 153
5.8 Business Continuity Management: Teil der ISO-22300-Familie 156
5.8.1 ISO 22301:2019, BCMS – Anforderungen 156
5.8.2 ISO 22313:2020, BCMS – Anleitung 157
5.9 Krisenmanagement 159
5.10 Organisatorische Belastbarkeit 160
5.10.1 ISO 22316:2017 160
5.10.2 BS 65000:2022 160
5.11 Schutz vor Insider-Bedrohungen 161
5.12 Gute Praktiken (GxP) 162
5.12.1 Europäische Kommission: Gute klinische Praxis (GCP) 162
5.12.2 OECD: Gute Laborpraxis (GLP) 162
5.12.3 PIC: Gute Herstellungspraxis (GMP) 163
5.12.4 ISPE: Good Automated Manufacturing Practice, GAMP® 5, 2022 164
5.13 Reifegradmodelle 165
5.14 Prüfungsstandards für Dienstleistungsunternehmen 166
5.15 Externe Anforderungen – Fazit 167

6 Begrifflichkeiten im Sicherheits-, Kontinuitäts- und Risikomanagement .. 169
6.1 Grundlagen 169
6.1.1 Werte (Assets) 169
6.1.2 Prozesse 170
6.1.3 Ressourcen 170
6.1.4 Organisation 170
6.1.5 Produkte und Leistungen 170
6.1.6 Funktionale und nichtfunktionale Anforderungen 170
6.1.7 Schutzobjekte und -subjekte sowie -klassen 171
6.1.8 Sicherheit und Sicherheitskriterien (Grundwerte der Sicherheit) 172
6.1.9 Sicherheit und Sicherheitsdreiklang 173
6.1.10 Sicherheitskategorien 174
6.1.11 Risiko und Risikodreiklang 174
6.1.12 Risikokategorien 176
6.1.13 Risikobehandlungsoptionen 177

6.1.14 Geschäftskontinuität (Business Continuity) 177
6.1.15 Zusammenhang Risiko, Sicherheit und Kontinuität 177
6.1.16 Politik/Leitlinie 177
6.1.17 Anforderungsanalyse 177
6.1.18 Prozess-, Ressourcen-, Organisations-, Produkt-, Leistungsimmanenz 178
6.1.19 Lebenszyklusimmanenz 178
6.1.20 Sicherheits-, Kontinuitäts- und Risikomanagement 179
6.2 Managementsysteme 181
6.2.1 Managementsystem, allgemein 181
6.2.2 Unternehmenssicherheitsmanagementsystem 183
6.2.3 Informationssicherheitsmanagementsystem 185
6.2.4 Geschäftskontinuitätsmanagementsystem 187
6.2.5 Risikomanagementsystem 190
6.3 Managementsystemprozesse 192
6.3.1 Unternehmenssicherheitsmanagement 192
6.3.2 Informationssicherheitsmanagement 193
6.3.3 Geschäftskontinuitätsmanagement 193
6.3.4 Risikomanagement 194
6.4 Ergänzende Managementsystemprozesse 194
6.4.1 IKT-Sicherheitsmanagement 194
6.4.2 Facility-Sicherheitsmanagement 195
6.4.3 IKT-Service-Kontinuitätsmanagement 195
6.4.4 Operationelles Risikomanagement 195
6.5 Ingenieurmäßige Sicherheit – OHSSCR Engineering 196
6.6 Sicherheitspyramide 197
6.6.1 Sicherheitspolitik 200
6.7 Zusammenfassung 201

7 Die Sicherheitspyramide – Strategie und Vorgehensmodell 205
7.1 Überblick 206
7.2 Sicherheitshierarchie 209
7.2.1 Sicherheits-, Kontinuitäts- und Risikopolitik 209
7.2.2 Sicherheitsziele / Sicherheitsanforderungen 210
7.2.3 Sicherheitstransformation und Sicherheitsmerkmale 211
7.2.4 Sicherheitsarchitektur 211
7.2.5 Sicherheitsrichtlinien – Generische Sicherheitskonzepte 212
7.2.6 Spezifische Sicherheitskonzepte 213
7.2.7 Sicherheitsmaßnahmen 213
7.3 PROSim 214
7.4 Lebenszyklus 215
7.4.1 Prozess-Lebenszyklus 215
7.4.2 Ressourcen- / Systemlebenszyklen 216
7.4.3 Organisationslebenszyklus 216
7.4.4 Produkt- und (Dienst-)leistungslebenszyklen 217
7.5 Sicherheitsregelkreis 217

7.6 Sicherheitsmanagementprozess 218
7.7 Zusammenfassung 218

8 Sicherheits-, Kontinuitäts- und Risikopolitik 220
8.1 Zielsetzung 221
8.2 Umsetzung 221
8.3 Inhalte 223
8.4 Praxisbeispiel Sicherheits-, Kontinuitäts- und Risikopolitik 226
8.5 Zusammenfassung 238

9 Sicherheitsziele / Sicherheitsanforderungen 239
9.1 Sicherheits- und Kontinuitätskriterien 240
9.2 Interne und externe Schutzanforderungen/Schutzbedarfe 241
9.3 Schutzbedarfsklassen/Schutzniveaus 242
9.4 Schadensklassen 243
9.5 MTA- bzw. Kontinuitätsklassen, MTD-Klassen 243
9.6 Planungshorizont und darin enthaltene Zeitbereiche 243
9.7 Kritikalitätsklassen 244
9.8 Klassifizierung der Informations- und Datenkategorien 245
9.9 Schutzbedarfsanalyse (SBA) 247
9.9.1 Geschäftseinflussanalyse (Business Impact Analysis) 248
9.9.2 Betriebseinflussanalyse (Operational Impact Analysis) 250
9.10 Zusammenfassung 251

10 Sicherheitsmerkmale 252
10.1 Haus zur Sicherheit 253
10.2 „Occ. Health, Safety, Security and Continuity Function Deployment" 254
10.2.1 Transformation der Anforderungen auf Sicherheitsmerkmale 254
10.2.2 Detaillierung der Sicherheitsmerkmale 256
10.2.3 Abbildung der Merkmale auf den Lebenszyklus 256
10.3 Schutzbedarfsklassen 257
10.4 Praxisbeispiele 258
10.5 Zusammenfassung 261

11 Sicherheitsarchitektur 262
11.1 Überblick 263
11.2 Prinzipielle/generische Sicherheitsanforderungen 264
11.3 Prinzipielle/generische Bedrohungen 265
11.4 Strategien und Prinzipien 270
11.4.1 Risikostrategie (Risk strategy), Risikolandkarte, Risikoklassen 271
11.4.2 Sicherheits- und Kontinuitätsstrategie (Occ. Health, Safety, Security and Continuity Strategy) 273
11.4.3 Prinzip der Wirtschaftlichkeit 275
11.4.4 Prinzip der Abstraktion 275
11.4.5 Prinzip der Klassenbildung (Principle of Classification) 276
11.4.6 Poka-Yoke-Prinzip 277
11.4.7 Prinzip der Namenskonventionen (Principle of Naming Conventions) 279
11.4.8 Prinzip der Redundanz (Principle of Redundancy) 279

11.4.9 Prinzip des „aufgeräumten" Arbeitsplatzes (Clear Desk / Workplace Policy) 282
11.4.10 Prinzip der Abwesenheitssperre 282
11.4.11 Prinzip der Eigenverantwortlichkeit 283
11.4.12 Vier-Augen-Prinzip (Confirmed Double Check / Dual Control Principle) 283
11.4.13 Prinzip der Funktionstrennung (Segregation of Duties Principle) 283
11.4.14 Prinzip der Sicherheitsschalen (Safety and Security Shell Principle) 284
11.4.15 Prinzip der Pfadanalyse (Path Analysis Principle) 285
11.4.16 Prinzip des Nicht-Vertrauens (Zero Trust Principle) 286
11.4.17 Prinzip der gesicherten Identität 287
11.4.18 Prinzip der gesicherten Kommunikation 287
11.4.19 Prinzip der Ge- und Verbotsdifferenzierung 288
11.4.20 Prinzip des generellen Verbots (Deny All/Default Deny Principle) 288
11.4.21 Prinzip der Ausschließlichkeit 289
11.4.22 Prinzip des minimalen Bedarfs (Need to Know / Use Principle) 289
11.4.23 Prinzip der minimalen Rechte (Least / Minimum Privileges Principle) 290
11.4.24 Prinzip der minimalen Dienste (Minimum Services Principle) .291
11.4.25 Prinzip der minimalen Nutzung (Minimum Usage Principle) ..291
11.4.26 Prinzip der Nachvollziehbarkeit und Nachweisbarkeit 291
11.4.27 Prinzip des „sachkundigen Dritten" (Principle of Third Party Expert) 292
11.4.28 Prinzip der Sicherheitszonen und des Closed-Shop-Betriebs 292
11.4.29 Prinzip der Sicherheitszonenanalyse 296
11.4.30 Prinzip des abgesicherten Ausfalls (Principle of Fail Safe and Fail Secure) 296
11.4.31 Prinzip der Immanenz (Principle of Immanence) 297
11.4.32 Prinzip der Konsolidierung (Principle of Consolidation) 298
11.4.33 Prinzip der Standardisierung (Principle of Standardization) 300
11.4.34 Prinzip der Plausibilisierung (Principle of Plausibleness) 301
11.4.35 Prinzip der Konsistenz (Principle of Consistency) 303
11.4.36 Prinzip der Untergliederung (Principle of Compartmentalization) 303
11.4.37 Prinzip der Aufteilung 303
11.4.38 Prinzip der Pseudonymisierung bzw. Maskierung 304
11.4.39 Prinzip der Vielfältigkeit (Principle of Diversity) 304
11.4.40 Distanzprinzip (Distance Principle) 304
11.4.41 Prinzip der Vererbung 306
11.4.42 Prinzip der Subjekt-Objekt- / Aktiv-Passiv-Differenzierung 307
11.4.43 Prinzip der Wachsamkeit 307

11.4.44 Prinzip der Regelschleife ... 308
11.4.45 Prinzipien versus Sicherheitskriterien (Sicherheitsgrundwerte) ... 308
11.5 Sicherheitselemente ... 309
11.5.1 Prozesse im Überblick ... 311
11.5.2 Konformitätsmanagement (Compliance Management) ... 321
11.5.3 Arbeitsschutzmanagement (Occ. Health, Safety Management) 326
11.5.4 Datenschutzmanagement (Data Protection Management) ... 328
11.5.5 Risikomanagement (Risk Management) ... 333
11.5.6 Leistungsmanagement (Service Level Management) ... 348
11.5.7 Finanzmanagement (Financial Management) ... 357
11.5.8 Projektmanagement (Project Management) ... 358
11.5.9 Qualitätsmanagement (Quality Management) ... 359
11.5.10 Ereignismanagement (Incident Management) ... 360
11.5.11 Problemmanagement (Problem Management) ... 367
11.5.12 Änderungsmanagement (Change Management) ... 368
11.5.13 Releasemanagement (Release Management) ... 371
11.5.14 Konfigurationsmanagement (Configuration Management) ... 371
11.5.15 Lizenzmanagement (Licence Management) ... 373
11.5.16 Kapazitätsmanagement (Capacity Management) ... 377
11.5.17 Wartungsmanagement (Maintenance Management) ... 380
11.5.18 Kontinuitätsmanagement (Continuity Management) ... 381
11.5.19 Securitymanagement (Security Management) ... 412
11.5.20 Architekturmanagement (Architecture Management) ... 465
11.5.21 Innovationsmanagement (Innovation Management) ... 476
11.5.22 Vertragsmanagement (Contract Management) ... 481
11.5.23 Dokumentationsmanagement (Documentation Management) . 483
11.5.24 Personalmanagement (Human Resources Management) ... 485
11.5.25 Ressourcen (R) im Überblick ... 492
11.5.26 R: Prozesse ... 493
11.5.27 R: Informationen und Daten ... 493
11.5.28 R: Dokumentationen ... 493
11.5.29 R: IKT-Hardware und Software ... 494
11.5.30 R: Infrastruktur ... 524
11.5.31 R: Material ... 525
11.5.32 R: Methoden und Verfahren ... 525
11.5.33 R: Personal ... 525
11.5.34 Organisation (O) im Überblick ... 526
11.5.35 Lebenszyklus im Überblick ... 527
11.6 Interdependenznetz ... 527
11.7 Hilfsmittel RiSiKo-Architekturmatrix ... 530
11.8 Zusammenfassung ... 531

12 Sicherheitsrichtlinien / -standards – Generische Sicherheitskonzepte ... 533
12.1 Übergreifende Richtlinien ... 534
12.1.1 Sicherheitsregeln ... 534
12.1.2 Kommunikation ... 535
12.1.3 Vorlage Prozessbeschreibung ... 536

12.1.4 Sourcing 540
12.1.5 Faxgeräte und Fax-Nutzung 544
12.1.6 Drucker und Ausdrucke 545
12.1.7 IKT-Benutzerordnung 545
12.1.8 E-Mail-Nutzung 555
12.1.9 Internet-Nutzung 557
12.1.10 Cloud-Computing 558
12.2 Management-, Kerngeschäfts-, Support-, Begleitprozesse 561
12.2.1 Konformitätsmanagement 561
12.2.2 Datenschutzmanagement 562
12.2.3 Sicherheits-, Kontinuitäts- und Risikomanagement 570
12.2.4 Risikomanagement 571
12.2.5 Kapazitätsmanagement 576
12.2.6 Kontinuitätsmanagement 578
12.2.7 Securitymanagement 603
12.2.8 Architekturmanagement (Unternehmen) 624
12.3 Ressourcen 628
12.3.1 Zutrittskontrollsystem / Zutrittskontrollanlage 628
12.3.2 Passwortbezogene Systemanforderungen 628
12.4 Organisation 629
12.5 Zusammenfassung 630

13 Spezifische Sicherheitskonzepte 632
13.1 Prozesse 633
13.1.1 Kontinuitätsmanagement 633
13.2 Ressourcen 634
13.2.1 Betriebssystem 634
13.3 Zusammenfassung 635

14 Sicherheitsmaßnahmen 636
14.1 Ressourcen 636
14.1.1 Betriebssystem: Protokoll Passworteinstellungen 636
14.2 Zusammenfassung 636

15 Prozess-, Produkt- und Dienstleistungslebenszyklen 638
15.1 Prozesslebenszyklus 641
15.2 Produkt- und Dienstleistungslebenszyklus 649
15.3 Entscheidungsprozesslebenszyklus 652
15.4 Zusammenfassung 653

16 Sicherheitsregelkreis 655
16.1 Sicherheitsprüfungen 656
16.1.1 Sicherheitsstudie / -analyse 656
16.1.2 IKT-Security-Scans 662
16.1.3 Penetrationstests 663
16.1.4 Verteidigungstest / Cyber-Defence-Übung 663
16.2 Sicherheitscontrolling 665

16.3 Berichtswesen (Reporting) 667
16.3.1 Anforderungen 667
16.3.2 Inhalte 669
16.4 Benchmarks 683
16.5 Hilfsmittel IKT-Sicherheitsfragen 683
16.6 Zusammenfassung 684

17 Reifegradmodell des RiSiKo-Managements 686
17.1 Reifegradmodell Unternehmenssicherheitsmanagement 686
17.1.1 Stufe 0: unbekannt 687
17.1.2 Stufe 1: begonnen 687
17.1.3 Stufe 2: konzipiert 687
17.1.4 Stufe 3: standardisiert 688
17.1.5 Stufe 4: integriert 688
17.1.6 Stufe 5: gesteuert 688
17.1.7 Stufe 6: selbst lernend 688
17.2 Checkliste Reifegrad 692
17.3 Praxisbeispiel 693
17.4 Zusammenfassung 694

18 Sicherheitsmanagementprozess 695
18.1 Deming- bzw. PDCA-Zyklus 695
18.2 Planung 696
18.3 Durchführung 698
18.4 Prüfung 698
18.5 Verbesserung 698
18.6 Zusammenfassung 699

19 Minimalistische Sicherheit 702

20 Verzeichnis der Abbildungen 704

21 Verzeichnis der Tabellen 706

22 Verzeichnis der Checklisten 706

23 Verzeichnis der Beispiele 707

24 Verzeichnis der Tipps 708

25 Verzeichnis der Informationen 709

26 Verzeichnis der Marken 711

27 Verzeichnis über Gesetze, Vorschriften, Normen, Standards, Practices 713
27.1 Gesetze, Verordnungen, Regularien, Richtlinien 713
27.1.1 Deutschland: Gesetze, Verordnungen, Regularien 713
27.1.2 Österreich: Gesetze, Verordnungen 718
27.1.3 Schweiz: Gesetze, Verordnungen, Regularien 719
27.1.4 Großbritannien: Gesetze, Regularien 720
27.1.5 Europa: Richtlinien, Verordnungen, Beschlüsse, Regularien, Practices 720

27.1.6 USA: Gesetze, Vorschriften, Regularien, Practices 724
27.1.7 International: Regularien 726
27.2 Weitere Regelungen, Vorgehensweisen 727
27.3 Standards, Normen, Leitlinien 728

28 Literatur- und Quellenverzeichnis 762

29 Glossar und Abkürzungsverzeichnis 766

30 Sachwortverzeichnis 786

31 Über den Autor 847