

Inhaltsverzeichnis

| | |
|---|-----------|
| 1 Ausgangssituation und Zielsetzung | 1 |
| 1.1 Ausgangssituation | 3 |
| 1.1.1 Bedrohungen | 3 |
| 1.1.2 Schwachstellen | 17 |
| 1.1.3 Schutzbedarf und Haftung | 20 |
| 1.2 Zielsetzung des Sicherheits-, Kontinuitäts- und Risikomanagements | 24 |
| 1.3 Lösung | 24 |
| 1.4 Zusammenfassung | 26 |
| 2 Kurzfassung und Überblick für Eilige | 28 |
| 3 Zehn Schritte zum Sicherheitsmanagement | 34 |
| 4 Gesetze, Verordnungen, Vorschriften, Anforderungen | 36 |
| 4.1 Persönliche Haftungsrisiken und Strafbarkeit | 36 |
| 4.2 Haftungsrisiken von Unternehmen | 40 |
| 4.3 Risikomanagement | 41 |
| 4.4 Buchführung | 42 |
| 4.4.1 Deutschland | 42 |
| 4.4.2 Schweiz | 45 |
| 4.5 IT-Sicherheit | 45 |
| 4.6 Datenschutz | 47 |
| 4.6.1 Deutschland | 47 |
| 4.6.2 Österreich | 51 |
| 4.6.3 Schweiz | 51 |
| 4.6.4 Europäische Union | 51 |
| 4.6.5 USA | 52 |
| 4.7 Arbeitsschutz und Arbeitssicherheit | 53 |
| 4.7.1 Deutschland | 53 |
| 4.7.2 Österreich | 62 |
| 4.7.3 Schweiz | 62 |
| 4.7.4 Großbritannien | 63 |
| 4.7.5 Europäische Union | 63 |
| 4.7.6 USA | 64 |
| 4.8 Verträge | 64 |
| 4.9 Gleichbehandlung | 64 |
| 4.10 Weitere gesetzliche Anforderungen in Deutschland | 65 |
| 4.11 Unternehmensführung, Corporate Governance | 65 |
| 4.11.1 Deutschland | 65 |
| 4.11.2 Schweiz | 65 |
| 4.11.3 OECD | 66 |
| 4.12 Energieversorgungsunternehmen | 66 |
| 4.12.1 Deutschland | 66 |
| 4.12.2 Schweiz | 66 |

| | |
|--|------------|
| 4.13 Finanzinstitute und Versicherungsunternehmen | 67 |
| 4.13.1 Deutschland | 67 |
| 4.13.2 Schweiz | 86 |
| 4.13.3 Großbritannien | 87 |
| 4.13.4 Europäische Union | 87 |
| 4.13.5 USA | 89 |
| 4.14 Chemische und pharmazeutische Industrie | 89 |
| 4.14.1 Deutschland | 89 |
| 4.14.2 Europäische Union | 90 |
| 4.14.3 USA | 91 |
| 4.15 Behörden | 91 |
| 4.16 In USA börsennotierte Unternehmen | 91 |
| 4.17 Weitere Anforderungen | 92 |
| 4.18 Externe Anforderungen – Fazit | 92 |
| 5 Standards, Normen, Practices | 93 |
| 5.1 Informationssicherheitsmanagement | 94 |
| 5.1.1 Die ISO-27000-Familie im Überblick | 94 |
| 5.1.2 ISO/IEC 27001:2013, ISMS – Anforderungen | 95 |
| 5.1.3 BSI: Standards im Überblick | 98 |
| 5.1.4 BSI: IT-Grundschutzkataloge im Überblick | 98 |
| 5.1.5 BSI-IT-Grundschutzkataloge versus Sicherheitspyramide | 99 |
| 5.2 Business Continuity Management: Teil der ISO-22300-Familie | 102 |
| 5.2.1 ISO 22301:2012, BCMS – Anforderungen | 102 |
| 5.2.2 ISO 22313:2012, BCMS – Anleitung | 103 |
| 5.3 Risikomanagement | 104 |
| 5.3.1 Die ISO-31000-Familie | 104 |
| 5.3.2 Die ONR-49000-Familie | 105 |
| 5.3.3 OCTAVE® approach | 106 |
| 5.4 Arbeitsschutz und Arbeitssicherheit | 107 |
| 5.4.1 BS OHSAS | 107 |
| 5.4.2 ANSI Z10 | 107 |
| 5.4.3 ILO-OSH | 107 |
| 5.5 Sozialschutz (Social Compliance) | 108 |
| 5.6 Organisatorische Belastbarkeit | 108 |
| 5.7 Schutz vor Insider-Bedrohungen | 108 |
| 5.8 Gute Praktiken (GxP) | 109 |
| 5.8.1 OECD: Gute Laborpraxis (GLP) | 109 |
| 5.8.2 PIC: Gute Herstellungspraxis (GMP) | 110 |
| 5.8.3 ISPE: Good Automated Manufacturing Practice, GAMP® 5 | 111 |
| 5.9 COBIT®, Version 5.0 | 111 |
| 5.10 Reifegradmodelle | 113 |
| 5.11 Prüfungsstandards für Dienstleistungsunternehmen | 114 |
| 5.12 Externe Anforderungen – Fazit | 115 |
| 6 Definitionen zum Sicherheits-, Kontinuitäts- und Risikomanagement | 117 |
| 6.1 Unternehmenssicherheitsmanagementsystem | 117 |
| 6.2 Informationssicherheitsmanagementsystem | 118 |

| | |
|--|------------|
| 6.3 Sicherheitsmanagement | 119 |
| 6.4 IKT-Sicherheitsmanagement | 120 |
| 6.5 Ingenieurmäßige Sicherheit – Occ. Health, Safety, Security, Continuity, Risk Engineering | 121 |
| 6.6 Sicherheitspyramide | 122 |
| 6.7 Sicherheitspolitik | 124 |
| 6.8 Sicherheit im Lebenszyklus | 126 |
| 6.9 Ressourcen, Schutzobjekte und -subjekte sowie -klassen | 127 |
| 6.10 Sicherheitskriterien (Grundwerte der Sicherheit) | 128 |
| 6.11 Geschäftseinflussanalyse (Business Impact Analysis) | 129 |
| 6.12 Geschäftskontinuität (Business Continuity) | 129 |
| 6.13 Sicherheit und Sicherheitsdreiklang | 129 |
| 6.14 Risiko und Risikodreiklang | 131 |
| 6.15 Risikomanagement | 133 |
| 6.16 Sicherheits-, Kontinuitäts- und Risikomanagement | 133 |
| 6.17 Zusammenfassung | 134 |
| 7 Die Sicherheitspyramide – Strategie und Vorgehensmodell | 137 |
| 7.1 Überblick | 138 |
| 7.2 Sicherheitshierarchie | 141 |
| 7.2.1 Sicherheits-, Kontinuitäts- und Risikopolitik | 141 |
| 7.2.2 Sicherheitsziele / Sicherheitsanforderungen | 142 |
| 7.2.3 Sicherheitstransformation und Sicherheitsmerkmale | 142 |
| 7.2.4 Sicherheitsarchitektur | 143 |
| 7.2.5 Sicherheitsrichtlinien – Generische Sicherheitskonzepte | 143 |
| 7.2.6 Spezifische Sicherheitskonzepte | 144 |
| 7.2.7 Sicherheitsmaßnahmen | 145 |
| 7.3 PROSim | 145 |
| 7.4 Lebenszyklus | 146 |
| 7.4.1 Geschäfts-, Support- und Begleitprozess-Lebenszyklus | 146 |
| 7.4.2 Ressourcen- / Systemlebenszyklen | 147 |
| 7.4.3 Organisationslebenszyklus | 147 |
| 7.4.4 Produkt- und (Dienst-)leistungslebenszyklen | 147 |
| 7.5 Sicherheitsregelkreis | 148 |
| 7.6 Sicherheitsmanagementprozess | 148 |
| 7.7 Zusammenfassung | 149 |
| 8 Sicherheits-, Kontinuitäts- und Risikopolitik | 151 |
| 8.1 Zielsetzung | 152 |
| 8.2 Umsetzung | 152 |
| 8.3 Inhalte | 154 |
| 8.4 Checkliste | 157 |
| 8.5 Praxisbeispiel Sicherheits-, Kontinuitäts- und Risikopolitik | 158 |
| 8.6 Zusammenfassung | 168 |

| | |
|---|------------|
| 9 Sicherheitsziele / Sicherheitsanforderungen | 170 |
| 9.1 Schutzbedarfsklassen | 171 |
| 9.2 Schutzbedarfsanalyse | 172 |
| 9.2.1 Prozessarchitektur und Prozesscharakteristika | 173 |
| 9.2.2 Externe Anforderungen an das Unternehmen (Gesetze, Vorschriften, Normen, Practices) – Einleitung | 174 |
| 9.2.3 Geschäftseinflussanalyse (Business Impact Analysis) | 176 |
| 9.2.4 Betriebseinflussanalyse (Operational Impact Analysis) | 179 |
| 9.3 Akteursanalyse | 180 |
| 9.4 Umgebungs- / Umfeldanalyse | 181 |
| 9.5 Tabelle Schadensszenarien | 181 |
| 9.5 Praxisbeispiele | 183 |
| 9.5.1 Schutzbedarf der Prozesse | 183 |
| 9.5.2 Betriebseinflussanalyse | 183 |
| 9.5.3 Schutzbedarfsklassen | 188 |
| 9.6 Zusammenfassung | 190 |
| 10 Sicherheitsmerkmale | 191 |
| 10.1 Haus zur Sicherheit | 192 |
| 10.2 „Occ. Health, Safety, Security and Continuity Function Deployment“ ... | 193 |
| 10.2.1 Transformation der Anforderungen auf Sicherheitsmerkmale ... | 193 |
| 10.2.2 Detaillierung der Sicherheitsmerkmale | 195 |
| 10.2.3 Abbildung der Merkmale auf den Lebenszyklus | 195 |
| 10.3 Schutzbedarfsklassen | 196 |
| 10.4 Praxisbeispiele | 197 |
| 10.5 Zusammenfassung | 199 |
| 11 Sicherheitsarchitektur | 201 |
| 11.1 Überblick | 202 |
| 11.2 Prinzipielle / generische Sicherheitsanforderungen | 203 |
| 11.3 Prinzipielle / generische Bedrohungen | 204 |
| 11.4 Strategien und Prinzipien | 208 |
| 11.4.1 Risikostrategie (Risk Strategy), Risikolandkarte, Risikoklassen ... | 210 |
| 11.4.2 Sicherheits- und Kontinuitätsstrategie (Occ. Health, Safety, Security and Continuity Strategy) | 211 |
| 11.4.3 Prinzip der Wirtschaftlichkeit | 212 |
| 11.4.4 Prinzip der Abstraktion | 212 |
| 11.4.5 Prinzip der Klassenbildung (Principle of Classification) | 213 |
| 11.4.6 Poka-Yoke-Prinzip | 215 |
| 11.4.7 Prinzip der Namenskonventionen (Principle of Naming Conventions) | 216 |
| 11.4.8 Prinzip der Redundanz (Principle of Redundancy) | 216 |
| 11.4.9 Prinzip des „aufgeräumten“ Arbeitsplatzes (Clear Desk Policy) . | 219 |
| 11.4.10 Prinzip der Abwesenheitssperre | 219 |
| 11.4.11 Prinzip der Eigenverantwortlichkeit | 220 |
| 11.4.12 Vier-Augen-Prinzip (Confirmed Double Check / Dual Control Principle) | 220 |

| | |
|---|-----|
| 11.4.13 Prinzip der Funktionstrennung (Segregation of Duties Principle)..... | 220 |
| 11.4.14 Prinzip der Sicherheitsschalen (Safety and Security Shell Principle) | 221 |
| 11.4.15 Prinzip der Pfadanalyse (Path Analysis Principle) | 221 |
| 11.4.16 Prinzip der Ge- und Verbotsdifferenzierung..... | 223 |
| 11.4.17 Prinzip des generellen Verbots (Deny All Principle)..... | 223 |
| 11.4.18 Prinzip der Ausschließlichkeit..... | 223 |
| 11.4.19 Prinzip des minimalen Bedarfs (Need to Know / Use Principle)..... | 224 |
| 11.4.20 Prinzip der minimalen Rechte (Least / Minimum Privileges Principle)..... | 224 |
| 11.4.21 Prinzip der minimalen Dienste (Minimum Services Principle) | 225 |
| 11.4.22 Prinzip der minimalen Nutzung (Minimum Usage Principle) | 225 |
| 11.4.23 Prinzip der Nachvollziehbarkeit und Nachweisbarkeit..... | 225 |
| 11.4.24 Prinzip des „sachverständigen Dritten“ (Principle of Third Party Expert) | 226 |
| 11.4.25 Prinzip der Sicherheitszonen und des Closed-Shop-Betriebs | 226 |
| 11.4.26 Prinzip der Sicherheitszonenanalyse | 229 |
| 11.4.27 Prinzip der Immanenz (Principle of Immanence)..... | 229 |
| 11.4.28 Prinzip der Konsolidierung (Principle of Consolidation) | 231 |
| 11.4.29 Prinzip der Standardisierung (Principle of Standardization)..... | 233 |
| 11.4.30 Prinzip der Plausibilisierung (Principle of Plausibleness) | 234 |
| 11.4.31 Prinzip der Konsistenz (Principle of Consistency)..... | 235 |
| 11.4.32 Prinzip der Untergliederung (Principle of Compartmentalization) | 235 |
| 11.4.33 Prinzip der Aufteilung | 235 |
| 11.4.34 Prinzip der Pseudonymisierung bzw. Maskierung | 236 |
| 11.4.35 Prinzip der Vielfältigkeit (Principle of Diversity) | 236 |
| 11.4.36 Distanzprinzip (Distance Principle) | 236 |
| 11.4.37 Prinzip der Vererbung | 237 |
| 11.4.38 Prinzip der Subjekt-Objekt- / Aktiv-Passiv-Differenzierung..... | 238 |
| 11.4.39 Prinzipien versus Sicherheitskriterien | 239 |
| 11.5 Sicherheitselemente | 240 |
| 11.5.1 Prozesse im Überblick..... | 242 |
| 11.5.2 Konformitätsmanagement (Compliance Management)..... | 251 |
| 11.5.3 Arbeitsschutzmanagement (Occ. Health, Safety Management).... | 254 |
| 11.5.4 Datenschutzmanagement (Privacy Management) | 256 |
| 11.5.5 Risikomanagement (Risk Management)..... | 261 |
| 11.5.6 Leistungsmanagement (Service Level Management) | 273 |
| 11.5.7 Finanzmanagement (Financial Management) | 280 |
| 11.5.8 Projektmanagement (Project Management)..... | 281 |
| 11.5.9 Qualitätsmanagement (Quality Management) | 281 |
| 11.5.10 Ereignismanagement (Incident Management) | 282 |
| 11.5.11 Problemmanagement (Problem Management)..... | 287 |

| | |
|--|------------|
| 11.5.12 Änderungsmanagement (Change Management)..... | 289 |
| 11.5.13 Releasemanagement (Release Management)..... | 291 |
| 11.5.14 Konfigurationsmanagement (Configuration Management)..... | 291 |
| 11.5.15 Lizenzmanagement (Licence Management) | 293 |
| 11.5.16 Kapazitätsmanagement (Capacity Management) | 295 |
| 11.5.17 Wartungsmanagement (Maintenance Management) | 297 |
| 11.5.18 Kontinuitätsmanagement (Continuity Management) | 298 |
| 11.5.19 Securitymanagement (Security Management) | 328 |
| 11.5.20 Architekturmanagement (Architecture Management)..... | 374 |
| 11.5.21 Innovationsmanagement (Innovation Management)..... | 376 |
| 11.5.22 Vertragsmanagement (Contract Management) | 379 |
| 11.5.23 Dokumentationsmanagement (Documentation Management) .. | 381 |
| 11.5.24 Personalmanagement (Human Resources Management) | 383 |
| 11.5.25 Ressourcen im Überblick..... | 388 |
| 11.5.26 Organisation im Überblick | 416 |
| 11.5.27 Lebenszyklus im Überblick..... | 416 |
| 11.6 Interdependenznetz | 417 |
| 11.7 Hilfsmittel RiSiKo-Architekturmatrix | 418 |
| 11.8 Zusammenfassung | 420 |
| 12 Sicherheitsrichtlinien / -standards – Generische Sicherheitskonzepte | 422 |
| 12.1 Übergreifende Richtlinien | 423 |
| 12.1.1 Sicherheitsregeln..... | 423 |
| 12.1.2 Kommunikation..... | 424 |
| 12.1.3 Prozessvorlage | 425 |
| 12.1.4 Sourcing | 427 |
| 12.1.5 Faxgeräte und Fax-Nutzung | 430 |
| 12.1.6 Drucker und Ausdrucke..... | 431 |
| 12.1.7 IKT-Benutzerordnung..... | 431 |
| 12.1.8 E-Mail-Nutzung | 433 |
| 12.1.9 Internet-Nutzung..... | 435 |
| 12.2 Kern-, Support-, Begleitprozesse (Managementdisziplinen) | 437 |
| 12.2.1 Datenschutzmanagement..... | 437 |
| 12.2.2 Sicherheits-, Kontinuitäts- und Risikomanagement | 438 |
| 12.2.3 Kapazitätsmanagement | 440 |
| 12.2.4 Kontinuitätsmanagement | 442 |
| 12.2.5 Securitymanagement | 463 |
| 12.2.6 Architekturmanagement (Unternehmen) | 475 |
| 12.3 Ressourcen..... | 476 |
| 12.3.1 Zutrittskontrollsyste / Zutrittskontrollanlage | 476 |
| 12.3.2 Passwortbezogene Systemanforderungen | 476 |
| 12.4 Organisation | 477 |
| 12.5 Zusammenfassung | 478 |
| 13 Spezifische Sicherheitskonzepte | 479 |
| 13.1 Prozesse | 480 |
| 13.1.1 Kontinuitätsmanagement | 480 |

| | |
|---|------------|
| 13.2 Ressourcen | 481 |
| 13.2.1 Betriebssystem | 481 |
| 13.3. Zusammenfassung | 481 |
| 14 Sicherheitsmaßnahmen | 482 |
| 14.1 Ressourcen | 482 |
| 14.1.1 Betriebssystem: Protokoll Passworteinstellungen | 482 |
| 14.2 Zusammenfassung | 482 |
| 15 Prozess-, Produkt- und Dienstlebenszyklen | 484 |
| 15.1 Prozesslebenszyklus | 486 |
| 15.2 Produkt- und Dienstlebenszyklus | 492 |
| 15.3 Entscheidungsprozesslebenszyklus | 495 |
| 15.4 Zusammenfassung | 496 |
| 16 Sicherheitsregelkreis | 498 |
| 16.1 Sicherheitsprüfungen | 499 |
| 16.1.1 Sicherheitsstudie / -analyse | 499 |
| 16.1.2 Penetrationstests | 502 |
| 16.1.3 IT-Security-Scans | 503 |
| 16.2 Sicherheitscontrolling | 503 |
| 16.3 Berichtswesen (Occ. Health, Safety, Security and Continuity Reporting) | 505 |
| 16.3.1 Anforderungen | 505 |
| 16.3.2 Inhalte | 507 |
| 16.4 Occ. Health Safety Security Continuity Risk Benchmarks | 518 |
| 16.5 Hilfsmittel IKT-Sicherheitsfragen | 518 |
| 16.6 Zusammenfassung | 519 |
| 17 Reifegradmodell des RiSiKo-Managements | 520 |
| 17.1 Reifegradmodell Unternehmenssicherheitsmanagement | 520 |
| 17.1.1 Stufe 0: unbekannt | 521 |
| 17.1.2 Stufe 1: begonnen | 521 |
| 17.1.3 Stufe 2: konzipiert | 521 |
| 17.1.4 Stufe 3: standardisiert | 521 |
| 17.1.5 Stufe 4: integriert | 522 |
| 17.1.6 Stufe 5: gesteuert | 522 |
| 17.1.7 Stufe 6: selbst lernend | 522 |
| 17.2 Checkliste Reifegrad | 525 |
| 17.3 Praxisbeispiel | 527 |
| 17.4 Zusammenfassung | 527 |
| 18 Sicherheitsmanagementprozess | 529 |
| 18.1 Deming- bzw. PDCA-Zyklus | 529 |
| 18.2 Planung | 530 |
| 18.3 Durchführung | 531 |
| 18.4 Prüfung | 532 |

| | |
|---|------------|
| 18.5 Verbesserung..... | 532 |
| 18.6 Zusammenfassung | 532 |
| 19 Abbildungsverzeichnis | 535 |
| 20 Tabellenverzeichnis..... | 536 |
| 21 Verzeichnis der Checklisten | 536 |
| 22 Verzeichnis der Beispiele | 537 |
| 23 Verzeichnis der Tipps | 538 |
| 24 Verzeichnis der Informationen | 539 |
| 25 Markenverzeichnis | 540 |
| 26 Verzeichnis über Gesetze, Vorschriften, Standards, Normen | 541 |
| 26.1 Gesetze, Verordnungen, Richtlinien | 541 |
| 26.1.1 Deutschland: Gesetze, Verordnungen | 541 |
| 26.1.2 Österreich: Gesetze, Verordnungen..... | 542 |
| 26.1.3 Schweiz: Gesetze, Verordnungen, Rundschreiben | 543 |
| 26.1.4 Großbritannien: Gesetze, Vorschriften | 544 |
| 26.1.5 Europa: Entscheidungen, Richtlinien, Practices..... | 544 |
| 26.1.6 USA: Gesetze, Practices, Prüfvorschriften | 546 |
| 26.2 Ausführungsbestimmungen, Grundsätze, Vorschriften..... | 548 |
| 26.3 Standards, Normen, Leitlinien und Rundschreiben..... | 549 |
| 27 Literatur- und Quellenverzeichnis..... | 569 |
| 28 Glossar und Abkürzungsverzeichnis | 573 |
| 29 Sachwortverzeichnis | 591 |
| 30 Über den Autor | 629 |