

# Inhaltsübersicht

1	Ausgangssituation und Zielsetzung .....	1
2	Kurzfassung und Überblick für Eilige .....	18
3	Zehn Schritte zum Sicherheitsmanagement .....	24
4	Gesetze, Verordnungen, Vorschriften, Anforderungen .....	27
5	Standards, Normen, Practices .....	39
6	Definitionen .....	95
7	Die Sicherheitspyramide – Strategie und Vorgehensmodell .....	120
8	Sicherheits-, Kontinuitäts- und Risikopolitik .....	135
9	Sicherheitsziele / Sicherheitsanforderungen .....	151
10	Sicherheitsmerkmale .....	168
11	Sicherheitsarchitektur .....	178
12	Sicherheitsrichtlinien/-standards – Generische Sicherheitskonzepte .....	379
13	Spezifische Sicherheitskonzepte .....	425
14	Sicherheitsmaßnahmen .....	428
15	Lebenszyklus .....	430
16	Sicherheitsregelkreis .....	451
17	Reifegradmodell des Sicherheits-, Kontinuitäts- und Risikomanagements ...	472
18	Sicherheitsmanagementprozess .....	481
19	Minimalistische Sicherheit .....	487
20	Abbildungsverzeichnis .....	488
21	Markenverzeichnis .....	489
22	Verzeichnis über Gesetze, Vorschriften, Standards, Normen, Practices .....	490
23	Literatur- und Quellenverzeichnis .....	508
24	Glossar und Abkürzungsverzeichnis .....	513
25	Sachwortverzeichnis .....	543
26	Über den Autor .....	576

# Inhaltsverzeichnis

1	Ausgangssituation und Zielsetzung.....	1
1.1	Ausgangssituation.....	2
1.1.1	Bedrohungen.....	2
1.1.2	Schwachstellen.....	9
1.1.3	Schadenshöhen, Schutzbedarfe .....	12
1.2	Zielsetzung des Sicherheits-, Kontinuitäts- und Risikomanagements .....	14
1.3	Lösung .....	15
1.4	Zusammenfassung.....	16
2	Kurzfassung und Überblick für Eilige.....	18
3	Zehn Schritte zum Sicherheitsmanagement .....	24
4	Gesetze, Verordnungen, Vorschriften, Anforderungen.....	27
5	Standards, Normen, Practices.....	39
5.1	Standards des BSI.....	39
5.1.1	Überblick.....	39
5.1.2	BSI-Standard 100-1, ISMS .....	39
5.1.3	BSI-Standard 100-2, IT-Grundschatz-Vorgehensweise.....	40
5.1.4	BSI-Standard 100-3, Risikoanalyse .....	41
5.1.5	BSI-Standard 100-4, Notfallmanagement .....	42
5.1.6	Vergleich mit der Sicherheitspyramide .....	44
5.2	IT-Grundschatzkataloge des BSI.....	46
5.3	ISO/IEC 27000er-Familie .....	49
5.3.1	Überblick.....	49
5.3.2	ISO/IEC 27001:2005, ISMS – Requirements .....	51
5.3.3	ISO/IEC 27002:2005, ISM – Code of Practice .....	53
5.3.4	ISO/IEC 27003:2010, ISM – Implementation Guidance .....	54
5.3.5	ISO/IEC 27004:2009, ISM – Measurement .....	56
5.3.6	ISO/IEC 27005:2008, IS – Risk Management .....	57
5.3.7	ISO/IEC 27033, Network Security .....	57
5.4	ISO/IEC 24762:2008, ICT Disaster Recovery Services.....	58
5.5	ISO/IEC 20000, IT Service Management.....	59
5.6	ITIL® .....	61
5.6.1	Überblick.....	61
5.6.2	ITIL® Security Management .....	63
5.6.3	ITIL® IT Service Continuity Management.....	64
5.7	COBIT®, Version 4.0.....	65

5.8	Zusammenfassender Vergleich mit der Sicherheitspyramide .....	67
5.9	Risikoanalyse mittels OCTAVE® Approach .....	75
5.10	Reifegradmodelle .....	76
5.10.1	Systems Security Engineering – Capability Maturity Model® .....	77
5.10.2	Information Technology Security Assessment Framework .....	78
5.10.3	Maturity Model nach COBIT® .....	79
5.10.4	Zusammenfassung .....	80
5.11	Federated Identity Management .....	81
5.12	Architekturen .....	82
5.12.1	Serviceorientierte Architektur (SOA) .....	82
5.12.2	Open Grid Services Architecture® (OGSA®) .....	94
6	Definitionen .....	95
6.1	Unternehmenssicherheitsmanagementsystem .....	95
6.2	Informationssicherheitsmanagementsystem .....	96
6.3	Sicherheitsmanagement .....	97
6.4	IKT-Sicherheitsmanagement .....	98
6.5	Ingenieurmäßige Sicherheit – Safety, Security, Continuity Engineering .....	100
6.6	Sicherheitspyramide .....	101
6.7	Sicherheitspolitik .....	102
6.7.1	... nach IT-Grundschutzkatalogen .....	103
6.7.2	... nach ISO/IEC 13335-1:2004 .....	104
6.7.3	... nach ISO/IEC 27001:2005 .....	105
6.7.4	... nach ISO/IEC 27002:2005 .....	105
6.7.5	... nach ISO/IEC 27003:2010 .....	105
6.7.6	... nach ITSEC .....	106
6.7.7	... nach Common Criteria (ISO/IEC 15408) .....	106
6.7.8	... nach Dr.-Ing. Müller .....	107
6.7.9	Vergleich .....	108
6.8	Sicherheit im Lebenszyklus .....	108
6.9	Ressourcen, Schutzobjekte und -subjekte sowie -klassen .....	110
6.10	Sicherheitskriterien .....	111
6.11	Geschäftseinflussanalyse (Business Impact Analysis) .....	112
6.12	Geschäftskontinuität (Business Continuity) .....	112
6.13	Sicherheit und Sicherheitsdreiklang .....	112
6.14	Risiko und Risikodreiklang .....	114
6.15	Risikomanagement .....	116
6.16	IT-Sicherheits-, IT-Kontinuitäts- und IT-Risikomanagement .....	116
6.17	Zusammenfassung .....	117

7	Die Sicherheitspyramide – Strategie und Vorgehensmodell .....	120
7.1	Überblick .....	121
7.2	Sicherheitshierarchie.....	125
7.2.1	Sicherheits-, Kontinuitäts- und Risikopolitik.....	125
7.2.2	Sicherheitsziele / Sicherheitsanforderungen.....	125
7.2.3	Sicherheitstransformation und Sicherheitsmerkmale.....	126
7.2.4	Sicherheitsarchitektur .....	126
7.2.5	Sicherheitsrichtlinien.....	127
7.2.6	Spezifische Sicherheitskonzepte .....	128
7.2.7	Sicherheitsmaßnahmen.....	128
7.3	PROSim.....	129
7.4	Lebenszyklus .....	130
7.4.1	Geschäfts-, Support- und Begleitprozess-Lebenszyklus .....	130
7.4.2	Ressourcen-/Systemlebenszyklus.....	131
7.4.3	Organisationslebenszyklus .....	131
7.4.4	Produkt- und Dienstleistungslebenszyklus .....	131
7.5	Sicherheitsregelkreis .....	132
7.6	Sicherheitsmanagementprozess .....	132
7.7	Zusammenfassung .....	132
8	Sicherheits-, Kontinuitäts- und Risikopolitik .....	135
8.1	Zielsetzung.....	136
8.2	Umsetzung .....	136
8.3	Inhalte .....	138
8.4	Checkliste .....	139
8.5	Praxisbeispiele .....	141
8.5.1	Sicherheits-, kontinuieräts- und risikopolitische Leitsätze Versicherung .....	141
8.5.2	Sicherheits-, Kontinuitäts- und Risikopolitik.....	143
8.6	Zusammenfassung.....	150
9	Sicherheitsziele / Sicherheitsanforderungen.....	151
9.1	Schutzbedarfsklassen.....	152
9.2	Schutzbedarfsanalyse .....	153
9.2.1	Prozessarchitektur und Prozesscharakteristika.....	154
9.2.2	Externe Sicherheitsanforderungen – Überblick.....	155
9.2.3	Geschäftseinflussanalyse (Business Impact Analysis).....	156
9.2.4	Betriebseinflussanalyse (Operational Impact Analysis).....	159
9.3	Tabelle Schadensszenarien.....	160

9.4	Praxisbeispiele .....	161
9.4.1	Schutzbedarf der Geschäftsprozesse.....	162
9.4.2	IKT-Schutzbedarfsanalyse .....	162
9.4.3	Schutzbedarfsklassen .....	166
9.5	Zusammenfassung .....	167
10	Sicherheitsmerkmale .....	168
10.1	Haus zur Sicherheit – House of Safety, Security, Continuity (HoSSC) ..	169
10.2	Safety, Security and Continuity Function Deployment (SSCFD) .....	170
10.2.1	Transformation der Anforderungen auf Sicherheitsmerkmale.....	171
10.2.2	Detaillierung der Sicherheitsmerkmale .....	172
10.2.3	Abbildung der Merkmale auf den Lebenszyklus.....	173
10.3	Schutzbedarfsklassen.....	174
10.4	Praxisbeispiele .....	174
10.5	Zusammenfassung .....	176
11	Sicherheitsarchitektur .....	178
11.1	Überblick.....	179
11.2	Prinzipielle Sicherheitsanforderungen.....	181
11.3	Prinzipielle Bedrohungen.....	181
11.4	Strategien und Prinzipien.....	186
11.4.1	Risikostrategie (Risk Strategy) .....	187
11.4.2	Sicherheits- und Kontinuitätsstrategie (Safety, Security and Continuity Strategy) .....	188
11.4.3	Prinzip der Wirtschaftlichkeit.....	189
11.4.4	Prinzip der Abstraktion .....	189
11.4.5	Prinzip der Klassenbildung.....	190
11.4.6	Poka-Yoke-Prinzip.....	191
11.4.7	Prinzip der Namenskonventionen .....	192
11.4.8	Prinzip der Redundanz (Principle of Redundancy).....	193
11.4.9	Prinzip des „aufgeräumten“ Arbeitsplatzes (Clear Desk Policy).....	196
11.4.10	Prinzip des „gesperrten“ Bildschirms (Clear Screen Policy) .....	196
11.4.11	Prinzip der Eigenverantwortlichkeit.....	196
11.4.12	Vier-Augen-Prinzip (Confirmed Double Check Principle).....	196
11.4.13	Prinzip der Funktionstrennung (Segregation of Duties Principle).....	197
11.4.14	Prinzip der Sicherheitsschalen (Safety and Security Shell Principle).....	197
11.4.15	Prinzip der Pfadanalyse (Path Analysis Principle) .....	197
11.4.16	Prinzip der Ge- und Verbotsdifferenzierung.....	198
11.4.17	Prinzip des generellen Verbots (Deny All Principle).....	198
11.4.18	Prinzip der Ausschließlichkeit.....	198

11.4.19	Prinzip des minimalen Bedarfs (Need to Know/Use Principle)	199
11.4.20	Prinzip der minimalen Rechte (Least/Minimum Privileges Principle).....	199
11.4.21	Prinzip der minimalen Dienste (Minimum Services Principle)	199
11.4.22	Prinzip der minimalen Nutzung (Minimum Usage Principle)	199
11.4.23	Prinzip der Nachvollziehbarkeit und Nachweisbarkeit .....	200
11.4.24	Prinzip des „sachverständigen Dritten“ .....	200
11.4.25	Prinzip der Sicherheitszonen und des Closed-Shop-Betriebs ...	200
11.4.26	Prinzip der Immanenz (Principle of Immanence).....	201
11.4.27	Prinzip der Konsolidierung.....	202
11.4.28	Prinzip der Standardisierung (Principle of Standardization)....	204
11.4.29	Prinzip der Plausibilisierung (Principle of Plausibleness).....	205
11.4.30	Prinzip der Konsistenz (Principle of Consistency).....	205
11.4.31	Prinzip der Untergliederung (Principle of Compartmentalization).....	206
11.4.32	Prinzip der Vielfältigkeit (Principle of Diversity) .....	206
11.4.33	Distanzprinzip .....	206
11.4.34	Prinzip der Vererbung.....	207
11.4.35	Prinzip der Subjekt-Objekt- / Aktiv-Passiv-Differenzierung.....	207
11.5	Sicherheitselemente.....	208
11.5.1	Prozesse im Überblick.....	210
11.5.2	Konformitätsmanagement (Compliance Management).....	220
11.5.3	Datenschutzmanagement (Privacy Management) .....	222
11.5.4	Risikomanagement (Risk Management).....	225
11.5.5	Leistungsmanagement (Service / Service Level Management)	236
11.5.6	Finanzmanagement (Financial Management) .....	240
11.5.7	Projektmanagement (Project Management).....	241
11.5.8	Qualitätsmanagement (Quality Management).....	241
11.5.9	Ereignismanagement (Incident Management) .....	242
11.5.10	Problemmanagement (Problem Management) .....	248
11.5.11	Änderungsmanagement (Change Management).....	249
11.5.12	Releasemanagement (Release Management).....	252
11.5.13	Konfigurationsmanagement (Configuration Management).....	253
11.5.14	Lizenzmanagement (Licence Management) .....	254
11.5.15	Kapazitätsmanagement (Capacity Management) .....	256
11.5.16	Wartungsmanagement (Maintenance Management) .....	258
11.5.17	Kontinuitätsmanagement (Continuity Management) .....	259
11.5.18	Securitymanagement (Security Management) .....	288
11.5.19	Architekturmanagement (Architecture Management).....	323
11.5.20	Innovationsmanagement (Innovation Management) .....	328

11.5.21	Vertragsmanagement (Contract Management) .....	330
11.5.22	Dokumentenmanagement (Document Management) .....	332
11.5.23	Personalmanagement (Human Resources Management) .....	332
11.5.24	Ressourcen im Überblick .....	337
11.5.25	Daten.....	338
11.5.26	Dokumente .....	338
11.5.27	IKT-Hardware und Software .....	339
11.5.28	Infrastruktur .....	371
11.5.29	Material .....	373
11.5.30	Methoden und Verfahren .....	373
11.5.31	Personal.....	373
11.5.32	Organisation im Überblick .....	373
11.5.33	Lebenszyklus im Überblick .....	374
11.6	Interdependenznetz .....	374
11.7	Hilfsmittel RiSiKo-Architekturmatrix .....	376
11.8	Zusammenfassung .....	378
12	Sicherheitsrichtlinien/-standards – Generische Sicherheitskonzepte .....	379
12.1	Übergreifende Richtlinien .....	380
12.1.1	Sicherheitsregeln.....	380
12.1.2	Prozessvorlage.....	381
12.1.3	IKT-Benutzerordnung.....	383
12.1.4	E-Mail-Nutzung .....	385
12.1.5	Internet-Nutzung.....	388
12.2	Betriebs- und Begleitprozesse (Managementdisziplinen).....	390
12.2.1	Kapazitätsmanagement.....	390
12.2.2	Kontinuitätsmanagement .....	392
12.2.3	Securitymanagement.....	410
12.3	Ressourcen.....	420
12.3.1	Zutrittskontrollsystem.....	420
12.3.2	Passwortspezifische Systemanforderungen.....	421
12.3.3	Wireless LAN .....	421
12.4	Organisation.....	423
12.5	Zusammenfassung .....	424
13	Spezifische Sicherheitskonzepte .....	425
13.1	Prozesse .....	426
13.1.1	Kontinuitätsmanagement .....	426
13.2	Ressourcen.....	427
13.2.1	Betriebssystem.....	427
13.3	Zusammenfassung .....	427

14 Sicherheitsmaßnahmen.....	428
14.1 Ressourcen .....	428
14.1.1 Betriebssystem: Protokoll Passworteinstellungen .....	428
14.2 Zusammenfassung.....	429
15 Lebenszyklus.....	430
15.1 Beantragung.....	431
15.2 Planung.....	432
15.3 Fachkonzept, Anforderungsspezifikation .....	432
15.4 Technisches Grobkonzept .....	434
15.5 Technisches Feinkonzept .....	437
15.6 Entwicklung.....	439
15.7 Integrations- und Systemtest .....	442
15.8 Freigabe .....	443
15.9 Software-Evaluation .....	443
15.10 Auslieferung .....	444
15.11 Abnahmetest und Abnahme.....	444
15.12 Software-Verteilung.....	446
15.13 Inbetriebnahme.....	446
15.14 Betrieb .....	446
15.15 Außerbetriebnahme .....	447
15.16 Hilfsmittel Phasen-Ergebnistypen-Tabelle .....	448
15.17 Zusammenfassung.....	449
16 Sicherheitsregelkreis .....	451
16.1 Sicherheitsprüfungen.....	452
16.1.1 Sicherheitsstudie/Risikoanalyse .....	452
16.1.2 Penetrationstests .....	455
16.1.3 IT Security Scans .....	456
16.2 Sicherheitscontrolling.....	457
16.3 Berichtswesen (Safety-Security-Continuity-Reporting).....	459
16.3.1 Anforderungen .....	459
16.3.2 Inhalte.....	461
16.4 Safety-Security-Continuity-Risk-Benchmarks.....	470
16.5 Hilfsmittel IKT-Sicherheitsfragen .....	470
16.6 Zusammenfassung.....	471
17 Reifegradmodell des Sicherheits-, Kontinuitäts- und Risikomanagements.....	472
17.1 Reifegradmodell RiSiKo-Management.....	472
17.1.1 Stufe 0: unbekannt .....	473
17.1.2 Stufe 1: begonnen.....	473
17.1.3 Stufe 2: konzipiert.....	473



17.1.4	Stufe 3: standardisiert.....	474
17.1.5	Stufe 4: integriert.....	474
17.1.6	Stufe 5: gesteuert.....	474
17.1.7	Stufe 6: selbst lernend.....	474
17.2	Checkliste Reifegrad .....	478
17.3	Praxisbeispiel .....	479
17.4	Zusammenfassung .....	480
18	Sicherheitsmanagementprozess.....	481
18.1	Deming- bzw. PDCA-Zyklus.....	481
18.2	Planung.....	482
18.3	Durchführung .....	483
18.4	Prüfung.....	484
18.5	Verbesserung.....	484
18.6	Zusammenfassung .....	485
19	Minimalistische Sicherheit.....	487
20	Abbildungsverzeichnis .....	488
21	Markenverzeichnis .....	489
22	Verzeichnis über Gesetze, Vorschriften, Standards, Normen, Practices.....	490
22.1	Gesetze, Verordnungen und Richtlinien.....	490
22.1.1	Deutschland: Gesetze und Verordnungen .....	490
22.1.2	Österreich: Gesetze und Verordnungen .....	491
22.1.3	Schweiz: Gesetze, Verordnungen und Rundschreiben .....	491
22.1.4	Großbritannien: Gesetze .....	492
22.1.5	Europa: Entscheidungen und Richtlinien.....	492
22.1.6	USA: Gesetze, Practices und Prüfvorschriften.....	493
22.2	Ausführungsbestimmungen, Grundsätze, Vorschriften.....	494
22.3	Standards, Normen, Leitlinien und Rundschreiben.....	495
23	Literatur- und Quellenverzeichnis .....	508
24	Glossar und Abkürzungsverzeichnis.....	513
25	Sachwortverzeichnis.....	543
26	Über den Autor .....	576