

# Inhaltsübersicht

1	Ausgangssituation und Zielsetzung .....	1
2	Kurzfassung und Überblick für Eilige.....	22
3	Zehn Schritte zum Sicherheitsmanagement .....	28
4	Gesetze, Verordnungen, Vorschriften, Anforderungen.....	31
5	Standards, Normen, Practices.....	45
6	Definitionen.....	120
7	Die Sicherheitspyramide – Strategie und Vorgehensmodell.....	146
8	Sicherheits-, Kontinuitäts- und Risikopolitik .....	161
9	Sicherheitsziele / Sicherheitsanforderungen.....	180
10	Sicherheitsmerkmale .....	200
11	Sicherheitsarchitektur .....	210
12	Sicherheitsrichtlinien/-standards – Generische Sicherheitskonzepte.....	437
13	Spezifische Sicherheitskonzepte.....	487
14	Sicherheitsmaßnahmen.....	490
15	Lebenszyklus.....	492
16	Sicherheitsregelkreis .....	522
17	Reifegradmodell des Sicherheits-, Kontinuitäts- und Risikomanagements.....	544
18	Sicherheitsmanagementprozess .....	553
19	Minimalistische Sicherheit .....	560
20	Abbildungsverzeichnis .....	562
21	Tabellenverzeichnis.....	564
22	Verzeichnis der Checklisten.....	565
23	Verzeichnis der Beispiele.....	565
24	Markenverzeichnis .....	567
25	Verzeichnis über Gesetze, Vorschriften, Standards, Normen, Practices.....	569
26	Literatur- und Quellenverzeichnis.....	594

---

27 Glossar und Abkürzungsverzeichnis.....	599
28 Sachwortverzeichnis.....	630
29 Über den Autor .....	668

# Inhaltsverzeichnis

1	Ausgangssituation und Zielsetzung .....	1
1.1	Ausgangssituation.....	2
1.1.1	Bedrohungen .....	2
1.1.2	Schwachstellen.....	12
1.1.3	Schadenshöhen, Schutzbedarfe .....	15
1.2	Zielsetzung des Sicherheits-, Kontinuitäts- und Risikomanagements .....	18
1.3	Lösung .....	19
1.4	Zusammenfassung.....	20
2	Kurzfassung und Überblick für Eilige.....	22
3	Zehn Schritte zum Sicherheitsmanagement .....	28
4	Gesetze, Verordnungen, Vorschriften, Anforderungen.....	31
5	Standards, Normen, Practices.....	45
5.1	BSI: Standards.....	45
5.1.1	Überblick.....	45
5.1.2	BSI-Standard 100-1, ISMS.....	46
5.1.3	BSI-Standard 100-2, IT-Grundschutz-Vorgehensweise .....	46
5.1.4	BSI-Standard 100-3, Risikoanalyse .....	48
5.1.5	BSI-Standard 100-4, Notfallmanagement .....	48
5.1.6	Vergleich mit der Sicherheitspyramide .....	50
5.2	BSI-IT-Grundschutzkataloge versus Sicherheitspyramide.....	52
5.3	ISO/IEC 19770, Software asset management (SAM).....	55
5.4	ISO 22301:2012, Business Continuity Management Systems .....	56
5.5	ISO/IEC 24762:2008, ICT disaster recovery services.....	57
5.6	ISO/IEC-27000-Familie zum ISM .....	58
5.6.1	Überblick.....	58
5.6.2	ISO/IEC 27001:2013, ISMS – Requirements .....	61
5.6.3	ISO/IEC 27002:2013, ISM – Code of practice for IS controls .....	63
5.6.4	ISO/IEC 27003:2010, ISM – Implementation Guidance .....	66
5.6.5	ISO/IEC 27004:2009, ISM – Measurement .....	67
5.6.6	ISO/IEC 27005:2011, IS – Risk Management .....	68
5.6.7	ISO/IEC 27010:2012, ISM for inter-sector and inter-organizational communications.....	70
5.6.8	ISO/IEC 27013:2012, Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1.....	71

5.6.9	ISO/IEC TR 27015:2012, Information security management guidelines for financial services.....	72
5.6.10	ISO/IEC 27032:2012, Guidelines for cybersecurity .....	73
5.6.11	ISO/IEC 27033, Network security .....	74
5.6.12	ISO/IEC 27034, Application security .....	75
5.6.13	ISO/IEC 27035:2011, Information security incident management .....	77
5.6.14	ISO/IEC 27037:2012, Guidelines for identification, collection, acquisition and preservation of digital evidence.....	78
5.7	ISO/IEC 20000, IT Service Management .....	78
5.8	ITIL® .....	82
5.8.1	Überblick.....	82
5.8.2	ITIL® Information Security Management .....	84
5.8.3	ITIL® IT Service Continuity Management .....	85
5.9	COBIT®, Version 5.0 .....	86
5.10	PCI Data Security Standard (DSS).....	88
5.11	Zusammenfassender Vergleich mit der Sicherheitspyramide .....	89
5.12	Risikoanalyse mittels OCTAVE® Approach .....	96
5.13	Reifegradmodelle .....	97
5.13.1	Systems Security Engineering – Capability Maturity Model® .....	98
5.13.2	Software Assurance Maturity Model .....	99
5.13.3	Information Technology Security Assessment Framework .....	100
5.13.4	Maturity Model nach COBIT® 5.....	100
5.13.5	Zusammenfassung.....	101
5.14	Federated Identity Management .....	102
5.15	Architekturen.....	103
5.15.1	Serviceorientierte Architektur (SOA).....	103
5.15.2	Open Grid Services Architecture® (OGSA®).....	115
5.15.3	OSGi™ Architecture.....	116
5.16	Programmier-/Entwicklungsrichtlinien .....	116
5.16.1	C, C++ und Java .....	116
5.16.2	Webanwendungen.....	117
5.17	Schutz vor Insider-Bedrohungen .....	118
6	Definitionen.....	120
6.1	Unternehmenssicherheitsmanagementsystem.....	120
6.2	Informationssicherheitsmanagementsystem .....	121
6.3	Sicherheitsmanagement.....	123
6.4	IKT-Sicherheitsmanagement.....	123
6.5	Ingenieurmäßige Sicherheit – Safety, Security, Continuity Engineering .....	125

6.6	Sicherheitspyramide .....	126
6.7	Sicherheitspolitik.....	128
6.7.1	... nach IT-Grundschutzkatalogen .....	128
6.7.2	... nach ISO/IEC 13335-1:2004 .....	129
6.7.3	... nach ISO/IEC 27001:2013 .....	130
6.7.4	... nach ISO/IEC 27002:2013 .....	130
6.7.5	... nach ISO/IEC 27003:2010 .....	131
6.7.6	... nach ITSEC .....	131
6.7.7	... nach Common Criteria (ISO/IEC 15408).....	131
6.7.8	... nach der Sicherheitspyramide <sup>Dr.-Ing. Müller</sup> .....	132
6.7.9	Vergleich.....	133
6.8	Sicherheit im Lebenszyklus .....	134
6.9	Ressourcen, Schutzobjekte und -subjekte sowie -klassen.....	135
6.10	Sicherheitskriterien (Grundwerte der IS).....	136
6.11	Geschäftseinflussanalyse (Business Impact Analysis) .....	137
6.12	Geschäftskontinuität (Business Continuity) .....	137
6.13	Sicherheit und Sicherheitsdreiklang .....	137
6.14	Risiko und Risikodreiklang .....	139
6.15	Risikomanagement.....	141
6.16	IT-Sicherheits-, IT-Kontinuitäts- und IT-Risikomanagement.....	142
6.17	Zusammenfassung .....	143
7	Die Sicherheitspyramide – Strategie und Vorgehensmodell.....	146
7.1	Überblick .....	147
7.2	Sicherheitshierarchie.....	151
7.2.1	Sicherheits-, Kontinuitäts- und Risikopolitik.....	151
7.2.2	Sicherheitsziele / Sicherheitsanforderungen.....	151
7.2.3	Sicherheitstransformation und Sicherheitsmerkmale.....	152
7.2.4	Sicherheitsarchitektur .....	153
7.2.5	Sicherheitsrichtlinien.....	153
7.2.6	Spezifische Sicherheitskonzepte .....	154
7.2.7	Sicherheitsmaßnahmen.....	155
7.3	PROSim.....	155
7.4	Lebenszyklus .....	156
7.4.1	Geschäfts-, Support- und Begleitprozess-Lebenszyklus .....	156
7.4.2	Ressourcen-/Systemlebenszyklus.....	157
7.4.3	Organisationslebenszyklus .....	157
7.4.4	Produkt- und Dienstleistungslebenszyklus .....	158
7.5	Sicherheitsregelkreis .....	158
7.6	Sicherheitsmanagementprozess .....	159
7.7	Zusammenfassung .....	159

8	Sicherheits-, Kontinuitäts- und Risikopolitik.....	161
8.1	Zielsetzung .....	162
8.2	Umsetzung .....	162
8.3	Inhalte .....	164
8.4	Checkliste.....	166
8.5	Praxisbeispiele .....	168
8.5.1	Sicherheits-, kontinuieräts- und risikopolitische Leitsätze Versicherung.....	168
8.5.2	Sicherheits-, Kontinuitäts- und Risikopolitik.....	170
8.6	Zusammenfassung .....	178
9	Sicherheitsziele / Sicherheitsanforderungen .....	180
9.1	Schutzbedarfsklassen.....	181
9.2	Schutzbedarfsanalyse.....	182
9.2.1	Prozessarchitektur und Prozesscharakteristika.....	183
9.2.2	Externe Sicherheitsanforderungen – Überblick .....	184
9.2.3	Geschäftseinflussanalyse (Business Impact Analysis).....	186
9.2.4	Betriebseinflussanalyse (Operational Impact Analysis) .....	189
9.3	Akteursanalyse .....	190
9.4	Umgebungs-/Umfeldanalyse .....	191
9.5	Tabelle Schadensszenarien.....	191
9.6	Praxisbeispiele .....	193
9.6.1	Schutzbedarf der Geschäftsprozesse.....	193
9.6.2	IKT-Schutzbedarfsanalyse.....	193
9.6.3	Schutzbedarfsklassen .....	198
9.7	Zusammenfassung .....	199
10	Sicherheitsmerkmale .....	200
10.1	Haus zur Sicherheit – House of Safety, Security, Continuity (HoSSC)..	201
10.2	Safety, Security and Continuity Function Deployment (SSCFD) .....	202
10.2.1	Transformation der Anforderungen auf Sicherheitsmerkmale.	203
10.2.2	Detaillierung der Sicherheitsmerkmale .....	204
10.2.3	Abbildung der Merkmale auf den Lebenszyklus.....	205
10.3	Schutzbedarfsklassen.....	206
10.4	Praxisbeispiele .....	206
10.5	Zusammenfassung .....	208
11	Sicherheitsarchitektur .....	210
11.1	Überblick.....	211
11.2	Prinzipielle/generische Sicherheitsanforderungen .....	213
11.3	Prinzipielle/generische Bedrohungen.....	213
11.4	Strategien und Prinzipien.....	218

11.4.1	Risikostrategie (Risk Strategy), Risikolandkarte, Risikoklassen.....	219
11.4.2	Sicherheits- und Kontinuitätsstrategie (Safety, Security and Continuity Strategy).....	221
11.4.3	Prinzip der Wirtschaftlichkeit.....	222
11.4.4	Prinzip der Abstraktion.....	222
11.4.5	Prinzip der Klassenbildung (Principle of Classification).....	223
11.4.6	Poka-Yoke-Prinzip.....	224
11.4.7	Prinzip der Namenskonventionen (Principle of Naming Conventions).....	226
11.4.8	Prinzip der Redundanz (Principle of Redundancy).....	226
11.4.9	Prinzip des „aufgeräumten“ Arbeitsplatzes (Clear Desk Policy).....	230
11.4.10	Prinzip der Abwesenheitssperre.....	230
11.4.11	Prinzip der Eigenverantwortlichkeit.....	230
11.4.12	Vier-Augen-Prinzip (Confirmed Double Check/Dual Control Principle).....	231
11.4.13	Prinzip der Funktionstrennung (Segregation of Duties Principle).....	231
11.4.14	Prinzip der Sicherheitsschalen (Safety and Security Shell Principle).....	231
11.4.15	Prinzip der Pfadanalyse (Path Analysis Principle).....	232
11.4.16	Prinzip der Ge- und Verbotsdifferenzierung.....	233
11.4.17	Prinzip des generellen Verbots (Deny All Principle).....	233
11.4.18	Prinzip der Ausschließlichkeit.....	234
11.4.19	Prinzip des minimalen Bedarfs (Need to Know/Use Principle).....	234
11.4.20	Prinzip der minimalen Rechte (Least/Minimum Privileges Principle).....	234
11.4.21	Prinzip der minimalen Dienste (Minimum Services Principle).....	235
11.4.22	Prinzip der minimalen Nutzung (Minimum Usage Principle).....	235
11.4.23	Prinzip der Nachvollziehbarkeit und Nachweisbarkeit.....	236
11.4.24	Prinzip des „sachverständigen Dritten“ (Principle of Third Party Expert).....	236
11.4.25	Prinzip der Sicherheitszonen und des Closed-Shop-Betriebs.....	236
11.4.26	Prinzip der Sicherheitszonenanalyse.....	239
11.4.27	Prinzip der Immanenz (Principle of Immanence).....	240
11.4.28	Prinzip der Konsolidierung (Principle of Consolidation).....	241
11.4.29	Prinzip der Standardisierung (Principle of Standardization).....	243
11.4.30	Prinzip der Plausibilisierung (Principle of Plausibleness).....	244
11.4.31	Prinzip der Konsistenz (Principle of Consistency).....	245

11.4.32	Prinzip der Untergliederung (Principle of Compartmentalization).....	245
11.4.33	Prinzip der Aufteilung.....	246
11.4.34	Prinzip der Pseudonymisierung bzw. Maskierung.....	246
11.4.35	Prinzip der Vielfältigkeit (Principle of Diversity).....	246
11.4.36	Distanzprinzip (Distance Principle).....	247
11.4.37	Prinzip der Vererbung.....	248
11.4.38	Prinzip der Subjekt-Objekt- / Aktiv-Passiv-Differenzierung.....	248
11.4.39	Prinzipien versus Sicherheitskriterien.....	249
11.5	Sicherheitselemente.....	251
11.5.1	Prozesse im Überblick.....	252
11.5.2	Konformitätsmanagement (Compliance Management).....	262
11.5.3	Datenschutzmanagement (Privacy Management).....	265
11.5.4	Risikomanagement (Risk Management).....	268
11.5.5	Leistungsmanagement (Service / Service Level Management).....	280
11.5.6	Finanzmanagement (Financial Management).....	286
11.5.7	Projektmanagement (Project Management).....	286
11.5.8	Qualitätsmanagement (Quality Management).....	287
11.5.9	Ereignismanagement (Incident Management).....	288
11.5.10	Problemmanagement (Problem Management).....	294
11.5.11	Änderungsmanagement (Change Management).....	295
11.5.12	Releasemanagement (Release Management).....	298
11.5.13	Konfigurationsmanagement (Configuration Management).....	299
11.5.14	Lizenzmanagement (Licence Management).....	300
11.5.15	Kapazitätsmanagement (Capacity Management).....	302
11.5.16	Wartungsmanagement (Maintenance Management).....	304
11.5.17	Kontinuitätsmanagement (Continuity Management).....	305
11.5.18	Securitymanagement (Security Management).....	337
11.5.19	Architekturmanagement (Architecture Management).....	373
11.5.20	Innovationsmanagement (Innovation Management).....	379
11.5.21	Vertragsmanagement (Contract Management).....	382
11.5.22	Dokumentenmanagement (Document Management).....	384
11.5.23	Personalmanagement (Human Resources Management).....	384
11.5.24	Ressourcen im Überblick.....	389
11.5.25	Daten.....	390
11.5.26	Dokumente.....	390
11.5.27	IKT-Hardware und Software.....	391
11.5.28	Infrastruktur.....	429
11.5.29	Material.....	430
11.5.30	Methoden und Verfahren.....	430



---

11.5.31	Personal.....	430
11.5.32	Organisation im Überblick.....	431
11.5.33	Lebenszyklus im Überblick.....	431
11.6	Interdependenznetz.....	432
11.7	Hilfsmittel RiSiKo-Architekturmatrix.....	434
11.8	Zusammenfassung.....	435
12	Sicherheitsrichtlinien/-standards – Generische Sicherheitskonzepte.....	437
12.1	Übergreifende Richtlinien.....	438
12.1.1	Sicherheitsregeln.....	438
12.1.2	Prozessvorlage.....	440
12.1.3	IKT-Benutzerordnung.....	442
12.1.4	E-Mail-Nutzung.....	444
12.1.5	Internet-Nutzung.....	446
12.2	Betriebs- und Begleitprozesse (Managementdisziplinen).....	448
12.2.1	Kapazitätsmanagement.....	449
12.2.2	Kontinuitätsmanagement.....	451
12.2.3	Securitymanagement.....	469
12.2.4	Architekturmanagement.....	480
12.3	Ressourcen.....	482
12.3.1	Zutrittskontrollsystem.....	482
12.3.2	Passwortbezogene Systemanforderungen.....	482
12.3.3	Wireless LAN.....	483
12.4	Organisation.....	484
12.5	Zusammenfassung.....	485
13	Spezifische Sicherheitskonzepte.....	487
13.1	Prozesse.....	488
13.1.1	Kontinuitätsmanagement.....	488
13.2	Ressourcen.....	489
13.2.1	Betriebssystem.....	489
13.3	Zusammenfassung.....	489
14	Sicherheitsmaßnahmen.....	490
14.1	Ressourcen.....	490
14.1.1	Betriebssystem: Protokoll Passwordeinstellungen.....	490
14.2	Zusammenfassung.....	491
15	Lebenszyklus.....	492
15.1	Sichere Beantragung (Secure Proposal Application).....	495
15.2	Sichere Planung (Secure Planning).....	496

15.3	Sicheres Fachkonzept, sichere Anforderungsspezifikation (Secure Requirements Specification).....	496
15.4	Sicheres technisches Grobkonzept (Secure Technical Basic Design).....	500
15.5	Sicheres technisches Feinkonzept (Secure Technical Design) .....	505
15.6	Sichere Entwicklung (Secure Development / Coding) .....	508
15.7	Sichere Integrations- und Systemtest (Secure Integration / System Tests) .....	512
15.8	Sichere Freigabe (Secure Approval).....	513
15.9	Sichere Software-Evaluation (Secure Software Evaluation) .....	513
15.10	Sichere Auslieferung (Secure Delivery).....	514
15.11	Sicherer Abnahmetest und sichere Abnahme (Secure Acceptance Test and Secure Acceptance).....	514
15.12	Sichere Software-Verteilung (Secure Software Deployment).....	515
15.13	Sichere Inbetriebnahme (Secure Startup Procedure).....	516
15.14	Sicherer Betrieb (Secure Operation) .....	516
15.15	Sichere Außerbetriebnahme (Secure Decommissioning).....	517
15.16	Hilfsmittel erweiterte Phasen-Ergebnistypen-Tabelle (ePET).....	518
15.17	Zusammenfassung .....	519
16	Sicherheitsregelkreis.....	522
16.1	Sicherheitsprüfungen.....	523
16.1.1	Sicherheitsstudie/Risikoanalyse.....	523
16.1.2	Penetrationstests .....	526
16.1.3	IT Security Scans .....	527
16.2	Sicherheitscontrolling .....	528
16.3	Berichtswesen (Safety-Security-Continuity-Reporting) .....	530
16.3.1	Anforderungen.....	530
16.3.2	Inhalte.....	532
16.4	Safety-Security-Continuity-Risk-Benchmarks.....	541
16.5	Hilfsmittel IKT-Sicherheitsfragen .....	542
16.6	Zusammenfassung .....	542
17	Reifegradmodell des Sicherheits-, Kontinuitäts- und Risikomanagements .....	544
17.1	Reifegradmodell RiSiKo-Management.....	544
17.1.1	Stufe 0: unbekannt .....	545
17.1.2	Stufe 1: begonnen.....	545
17.1.3	Stufe 2: konzipiert .....	545
17.1.4	Stufe 3: standardisiert.....	546
17.1.5	Stufe 4: integriert.....	546
17.1.6	Stufe 5: gesteuert .....	546
17.1.7	Stufe 6: selbst lernend.....	546

17.2	Checkliste Reifegrad .....	550
17.3	Praxisbeispiel .....	552
17.4	Zusammenfassung .....	552
18	Sicherheitsmanagementprozess .....	553
18.1	Deming- bzw. PDCA-Zyklus.....	553
18.2	Planung.....	554
18.3	Durchführung.....	556
18.4	Prüfung.....	556
18.5	Verbesserung .....	556
18.6	Zusammenfassung.....	557
19	Minimalistische Sicherheit .....	560
20	Abbildungsverzeichnis.....	562
21	Tabellenverzeichnis.....	564
22	Verzeichnis der Checklisten.....	565
23	Verzeichnis der Beispiele.....	565
24	Markenverzeichnis .....	567
25	Verzeichnis über Gesetze, Vorschriften, Standards, Normen, Practices.....	569
25.1	Gesetze, Verordnungen und Richtlinien.....	569
25.1.1	Deutschland: Gesetze und Verordnungen.....	569
25.1.2	Österreich: Gesetze und Verordnungen.....	570
25.1.3	Schweiz: Gesetze, Verordnungen und Rundschreiben .....	570
25.1.4	Großbritannien: Gesetze .....	571
25.1.5	Europa: Entscheidungen, Richtlinien, Practices .....	571
25.1.6	USA: Gesetze, Practices und Prüfvorschriften .....	572
25.2	Ausführungsbestimmungen, Grundsätze, Vorschriften .....	573
25.3	Standards, Normen, Leitlinien und Rundschreiben.....	574
26	Literatur- und Quellenverzeichnis.....	594
27	Glossar und Abkürzungsverzeichnis .....	599
28	Sachwortverzeichnis .....	630
29	Über den Autor .....	668