

Inhaltsübersicht

1	Ausgangssituation und Zielsetzung	1
2	Kurzfassung und Überblick für Eilige.....	29
3	Zehn Schritte zum Sicherheitsmanagement	36
4	Gesetze, Verordnungen, Vorschriften, Anforderungen.....	39
5	Normen, Standards, Practices.....	90
6	Definitionen zum Sicherheits-, Kontinuitäts- und Risikomanagement	197
7	Die Sicherheitspyramide – Strategie und Vorgehensmodell.....	220
8	Sicherheits-, Kontinuitäts- und Risikopolitik	236
9	Sicherheitsziele/Sicherheitsanforderungen.....	255
10	Sicherheitsmerkmale	268
11	Sicherheitsarchitektur	279
12	Sicherheitsrichtlinien/-standards – Generische Sicherheitskonzepte	556
13	Spezifische Sicherheitskonzepte	647
14	Sicherheitsmaßnahmen.....	650
15	Lebenszyklus – mit integrierter Sicherheit.....	652
16	Sicherheitsregelkreis	686
17	Reifegradmodell des Sicherheits-, Kontinuitäts- und Risikomanagements	713
18	Sicherheitsmanagementprozess	723
19	Minimalistische Sicherheit	730
20	Verzeichnis der Abbildungen	732
21	Verzeichnis der Tabellen	734
22	Verzeichnis der Checklisten.....	734
23	Verzeichnis der Beispiele.....	735
24	Verzeichnis der Tipps	737
25	Verzeichnis der Informationen	738
26	Verzeichnis der Marken.....	740
27	Verzeichnis über Gesetze, Vorschriften, Standards, Normen, Practices.....	742
	Literatur- und Quellenverzeichnis	780
	Glossar und Abkürzungsverzeichnis	785
	Sachwortverzeichnis.....	816
	Über den Autor	864

Inhaltsverzeichnis

1	Ausgangssituation und Zielsetzung	1
1.1	Ausgangssituation.....	3
1.1.1	Bedrohungen.....	3
1.1.2	Schwachstellen.....	17
1.1.3	Schadenshöhen, Schutzbedarfe	20
1.2	Zielsetzung des Sicherheits-, Kontinuitäts- und Risikomanagements	25
1.3	Lösung	25
1.4	Zusammenfassung.....	27
2	Kurzfassung und Überblick für Eilige	29
3	Zehn Schritte zum Sicherheitsmanagement.....	36
4	Gesetze, Verordnungen, Vorschriften, Anforderungen.....	39
4.1	Persönliche Haftungsrisiken.....	39
4.2	Haftungsrisiken von Unternehmen.....	42
4.3	Risikomanagement.....	42
4.4	Buchführung	43
4.5	IT-Sicherheit kritischer Infrastrukturen/wesentlicher Dienste	48
4.5.1	Deutschland.....	48
4.5.2	Europäische Union	53
4.6	Datenschutz.....	54
4.6.1	Deutschland.....	54
4.6.2	Österreich.....	59
4.6.3	Schweiz	59
4.6.4	Europäische Union	59
4.6.5	USA.....	62
4.7	Arbeitsschutz und Arbeitssicherheit	63
4.8	Verträge	63
4.9	Mitbestimmung	64
4.10	Gleichbehandlung.....	65
4.11	Weitere gesetzliche Anforderungen in Deutschland	65
4.12	Energieversorgungsunternehmen	66
4.13	Finanzinstitute und Versicherungsunternehmen.....	68
4.13.1	Deutschland.....	68
4.13.2	Europäische Union	84
4.13.3	Basler Ausschuss für Bankenaufsicht	85

4.14	Chemische Industrie	87
4.14.1	Deutschland	87
4.14.2	USA	88
4.15	Behörden	88
5	Normen, Standards, Practices	90
5.1	Informationssicherheitsmanagement (ISM)	90
5.1.1	BSI IT-Grundschutz im Überblick	90
5.1.2	BSI-Standard 200-1, ISMS	91
5.1.3	BSI-Standard 200-2, IT-Grundschutz-Methodik	91
5.1.4	BSI-Standard 200-3, Risikoanalyse	93
5.1.5	BSI-Standard 100-4, Notfallmanagement	94
5.1.6	Vergleich der BSI-Standards mit der Sicherheitspyramide	97
5.1.7	BSI IT-Grundschutz-Kompendium	101
5.1.8	BSI-IT-Grundschutz-Kompendium versus Sicherheitspyramide	103
5.1.9	ISO/IEC-27000-Familie zum ISM im Überblick	104
5.1.10	ISO/IEC 27000:2016, Überblick und Vokabular	108
5.1.11	ISO/IEC 27001:2013, ISMS – Requirements	109
5.1.12	ISO/IEC 27002:2013, ISM – Code of practice for IS controls	112
5.1.13	ISO/IEC 27003:2017, ISMS – Anleitung	115
5.1.14	ISO/IEC 27004:2016, ISM – Measurement	117
5.1.15	ISO/IEC 27005:2011, Information security risk management	118
5.1.16	ISO/IEC 27010:2015, ISM for inter-sector and inter- organizational communications	120
5.1.17	ISO/IEC 27013:2015, Guidance on the integrated imple- mentation of ISO/IEC 27001 and ISO/IEC 20000-1	121
5.1.18	ISO/IEC 27014:2013, Governance of information security	122
5.1.19	ISO/IEC TR 27016:2014, Wirtschaftlichkeit des ISM	123
5.1.20	ISO/IEC 27017:2015, Leitfaden für Informationssicherheitsmaßnahmen bei Cloud-Services	123
5.1.21	ISO/IEC 27018:2014, Leitfaden zum Schutz personenbe- zogener Daten in öffentlichen Clouds	124
5.1.22	ISO/IEC 27019:2017, Informationssicherheit für Energieversorger	124
5.1.23	ISO/IEC 27031:2011, Guidelines for ICT readiness for BC (IRBC)	126
5.1.24	ISO/IEC 27032:2012, Guidelines for cybersecurity	128
5.1.25	ISO/IEC 27033, Network security	130
5.1.26	ISO/IEC 27034, Application security	131
5.1.27	ISO/IEC 27035, Information security incident management	133

5.1.28	ISO/IEC 27036, Information security for supplier relationships..	134
5.1.29	ISO/IEC 27037:2012, Guidelines for identification, collection, acquisition and preservation of digital evidence	135
5.1.30	ISO/IEC 27039:2015, IDPS.....	135
5.1.31	ISO/IEC 27040:2015, Storage Security	137
5.1.32	IEC 62443, Netzwerk- und Systemsicherheit.....	138
5.1.33	OECD Digital Security Risk Management	139
5.1.34	PCI Data Security Standard (DSS).....	140
5.2	Business Continuity Management (BCM): Teil der ISO-22300-Familie..	140
5.2.1	ISO 22301:2012, BCM-System – Anforderungen	140
5.2.2	ISO 22313:2012, BCMS – Anleitung.....	142
5.3	Risikomanagement.....	143
5.3.1	OCTAVE® Approach	143
5.4	IT Service Management	145
5.4.1	ISO/IEC 20000, IT Service Management	145
5.4.2	ISO/IEC 19770, IT und Software asset management (ITAM, SAM).....	149
5.4.3	ITIL® im Überblick.....	151
5.4.4	ITIL® Information Security Management	153
5.4.5	ITIL® IT Service Continuity Management.....	154
5.4.6	COBIT®, Version 5.0	155
5.5	Zusammenfassender Vergleich mit der Sicherheitspyramide.....	158
5.6	Reifegradmodelle	165
5.6.1	Systems Security Engineering – Capability Maturity Model® ..	166
5.6.2	Software Assurance Maturity Model.....	167
5.6.3	Information Technology Security Assessment Framework.....	168
5.6.4	Maturity Model nach COBIT® 5	169
5.6.5	Zusammenfassung	170
5.7	Federated Identity Management.....	170
5.8	Architekturen.....	172
5.8.1	Serviceorientierte Architektur (SOA).....	172
5.8.2	Open Grid Services Architecture® (OGSA®).....	184
5.8.3	OSGi™ Architecture.....	185
5.9	Projektmanagement	185
5.10	Entwicklungsmethoden	186
5.11	Programmier-/Entwicklungsrichtlinien	187
5.11.1	C, C++ und Java.....	187
5.11.2	Webanwendungen	188
5.11.3	Android™	189

5.12	Schwachstellen (Vulnerabilities)	189
5.12.1	Identifikation	189
5.12.2	Bewertung (Scoring)	190
5.13	Schutz vor Insider-Bedrohungen	191
5.14	Gute Praktiken (GxP)	192
5.14.1	OECD: Gute Laborpraxis (GLP)	192
5.14.2	PIC: Gute Herstellungspraxis (GMP)	193
5.14.3	ISPE: Good Automated Manufacturing Practice, GAMP® 5	194
5.15	Prüfungsstandards für Dienstleistungsunternehmen	195
6	Definitionen zum Sicherheits-, Kontinuitäts- und Risikomanagement	197
6.1	Unternehmenssicherheitsmanagementsystem	197
6.2	Informationssicherheitsmanagementsystem	198
6.3	Sicherheitsmanagement	200
6.4	IKT-Sicherheitsmanagement	200
6.5	Ingenieurmäßige Sicherheit – Safety, Security, Continuity, Risk Engineering	202
6.6	Sicherheitspyramide	203
6.7	Sicherheitspolitik	206
6.8	Sicherheit im Lebenszyklus	208
6.9	Ressourcen, Schutzobjekte und -subjekte sowie -klassen	209
6.10	Sicherheitskriterien (Grundwerte der Sicherheit)	211
6.11	Geschäftseinflussanalyse (Business Impact Analysis)	211
6.12	Geschäftskontinuität (Business Continuity)	212
6.13	Sicherheit und Sicherheitsdreiklang	212
6.14	Risiko und Risikodreiklang	214
6.15	Risikomanagement	216
6.16	Sicherheits-, Kontinuitäts- und Risikomanagement der IKT	216
6.17	Zusammenfassung	217
7	Die Sicherheitspyramide – Strategie und Vorgehensmodell	220
7.1	Überblick	221
7.2	Sicherheitshierarchie	225
7.2.1	Sicherheits-, Kontinuitäts- und Risikopolitik	225
7.2.2	Sicherheitsziele/Sicherheitsanforderungen	225
7.2.3	Sicherheitstransformation und Sicherheitsmerkmale	226
7.2.4	Sicherheitsarchitektur	227
7.2.5	Sicherheitsrichtlinien	227
7.2.6	Spezifische Sicherheitskonzepte	228
7.2.7	Sicherheitsmaßnahmen	229
7.3	PROSim	229

- 7.4 Lebenszyklus230
 - 7.4.1 Prozesslebenszyklus.....231
 - 7.4.2 Ressourcen-/Systemlebenszyklus.....231
 - 7.4.3 Organisationslebenszyklus232
 - 7.4.4 Produkt- und Dienstleistungslebenszyklus232
- 7.5 Sicherheitsregelkreis232
- 7.6 Sicherheitsmanagementprozess233
- 7.7 Zusammenfassung233
- 8 **Sicherheits-, Kontinuitäts- und Risikopolitik**236
 - 8.1 Zielsetzung237
 - 8.2 Umsetzung238
 - 8.3 Inhalte239
 - 8.4 Praxisbeispiele242
 - 8.4.1 Sicherheits-, kontinuieräts- und risikopolitische Leitsätze
Versicherung242
 - 8.4.2 Sicherheits-, Kontinuitäts- und Risikopolitik.....244
 - 8.5 Zusammenfassung253
- 9 **Sicherheitsziele/Sicherheitsanforderungen**255
 - 9.1 Sicherheits- und Kontinuitätskriterien257
 - 9.2 Interne und externe Schutzanforderungen/Schutzbedarfe258
 - 9.3 Schutzbedarfsklassen/Schutzniveaus.....258
 - 9.4 Planungshorizont und zeitliche Staffelung259
 - 9.5 Klassifizierung der Informations- und Datenkategorien.....260
 - 9.6 Schutzbedarfsanalyse (SBA)263
 - 9.6.1 Geschäftseinflussanalyse (Business Impact Analysis).....264
 - 9.6.2 Betriebseinflussanalyse (Operational Impact Analysis).....266
 - 9.7 Zusammenfassung267
- 10 **Sicherheitsmerkmale**268
 - 10.1 Haus zur Sicherheit – House of Safety, Security, Continuity (HoSSC)....269
 - 10.2 Safety, Security and Continuity Function Deployment (SSCFD)270
 - 10.2.1 Transformation der Anforderungen auf Sicherheitsmerkmale ..271
 - 10.2.2 Detaillierung der Sicherheitsmerkmale272
 - 10.2.3 Abbildung der Merkmale auf den Lebenszyklus.....273
 - 10.3 Schutzbedarfsklassen.....274
 - 10.4 Praxisbeispiele275
 - 10.5 Zusammenfassung277

11 Sicherheitsarchitektur	279
11.1 Überblick.....	280
11.2 Prinzipielle/generische Sicherheitsanforderungen	282
11.3 Prinzipielle/generische Bedrohungen.....	282
11.4 Strategien und Prinzipien.....	287
11.4.1 Risikostrategie (Risk Strategy), Risikolandkarte, Risikoklassen	288
11.4.2 Sicherheits- und Kontinuitätsstrategie (Safety, Security and Continuity Strategy)	290
11.4.3 Prinzip der Wirtschaftlichkeit	291
11.4.4 Prinzip der Abstraktion	291
11.4.5 Prinzip der Klassenbildung (Principle of Classification)	292
11.4.6 Poka-Yoke-Prinzip	293
11.4.7 Prinzip der Namenskonventionen (Principle of Naming Conventions)	295
11.4.8 Prinzip der Redundanz (Principle of Redundancy).....	295
11.4.9 Prinzip des „aufgeräumten“ Arbeitsplatzes (Clear Desk/ Workplace Policy).....	299
11.4.10 Prinzip der Abwesenheitssperre.....	299
11.4.11 Prinzip der Eigenverantwortlichkeit.....	300
11.4.12 Vier-Augen-Prinzip (Confirmed Double Check/ Dual Control Principle).....	300
11.4.13 Prinzip der Funktionstrennung (Segregation of Duties Principle).....	300
11.4.14 Prinzip der Sicherheitsschalen (Safety and Security Shell Principle).....	301
11.4.15 Prinzip der Pfadanalyse (Path Analysis Principle)	302
11.4.16 Prinzip der gesicherten Identität	303
11.4.17 Prinzip der gesicherten Kommunikation	303
11.4.18 Prinzip der Ge- und Verbotsdifferenzierung.....	304
11.4.19 Prinzip des generellen Verbots (Deny All Principle).....	304
11.4.20 Prinzip der Ausschließlichkeit.....	304
11.4.21 Prinzip des minimalen Bedarfs (Need to Know/Use Principle).....	305
11.4.22 Prinzip der minimalen Rechte (Least/Minimum Privileges Principle).....	306
11.4.23 Prinzip der minimalen Dienste (Minimum Services Principle).....	306
11.4.24 Prinzip der minimalen Nutzung (Minimum Usage Principle)	307
11.4.25 Prinzip der Nachvollziehbarkeit und Nachweisbarkeit.....	307

11.4.26	Prinzip des „sachverständigen Dritten“ (Principle of Third Party Expert)	307
11.4.27	Prinzip der Sicherheitszonen und des Closed-Shop-Betriebs ...	308
11.4.28	Prinzip der Sicherheitszonenanalyse	312
11.4.29	Prinzip des abgesicherten Ausfalls (Principle of Fail Safe and Fail Secure).....	312
11.4.30	Prinzip der Immanenz (Principle of Immanence).....	313
11.4.31	Prinzip der Konsolidierung (Principle of Consolidation).....	314
11.4.32	Prinzip der Standardisierung (Principle of Standardization)....	317
11.4.33	Prinzip der Plausibilisierung (Principle of Plausibleness)	318
11.4.34	Prinzip der Konsistenz (Principle of Consistency).....	319
11.4.35	Prinzip der Untergliederung (Principle of Compartmentalization).....	320
11.4.36	Prinzip der Aufteilung.....	320
11.4.37	Prinzip der Pseudonymisierung bzw. Maskierung	321
11.4.38	Prinzip der Vielfältigkeit (Principle of Diversity)	321
11.4.39	Distanzprinzip (Distance Principle).....	321
11.4.40	Prinzip der Vererbung	323
11.4.41	Prinzip der Subjekt-Objekt-/Aktiv-Passiv-Differenzierung	323
11.4.42	Prinzip der Wachsamkeit	324
11.4.43	Prinzip der Regelschleife	325
11.4.44	Prinzipien versus Sicherheitskriterien (Sicherheitsgrundwerte).....	325
11.5	Sicherheitselemente.....	327
11.5.1	Prozesse im Überblick.....	329
11.5.2	Konformitätsmanagement (Compliance Management).....	339
11.5.3	Datenschutzmanagement (Data Protection Management).....	343
11.5.4	Risikomanagement (Risk Management).....	348
11.5.5	Leistungsmanagement (Service/Service Level Management) ...	362
11.5.6	Finanzmanagement (Financial Management)	367
11.5.7	Projektmanagement (Project Management).....	368
11.5.8	Qualitätsmanagement (Quality Management).....	369
11.5.9	Ereignismanagement (Incident Management)	370
11.5.10	Problemmanagement (Problem Management)	377
11.5.11	Änderungsmanagement (Change Management).....	379
11.5.12	Releasemanagement (Release Management).....	383
11.5.13	Konfigurationsmanagement (Configuration Management).....	383
11.5.14	Lizenzmanagement (Licence Management)	386
11.5.15	Kapazitätsmanagement (Capacity Management)	388
11.5.16	Wartungsmanagement (Maintenance Management)	391

11.5.17	Kontinuitätsmanagement (Continuity Management)	392
11.5.18	Securitymanagement (Security Management).....	426
11.5.19	Architekturmanagement (Architecture Management)	467
11.5.20	Innovationsmanagement (Innovation Management)	482
11.5.21	Vertragsmanagement (Contract Management)	486
11.5.22	Dokumentationsmanagement (Documentation Management).....	488
11.5.23	Personalmanagement (Human Resources Management)	491
11.5.24	Ressourcen im Überblick	498
11.5.25	Prozesse.....	499
11.5.26	Informationen und Daten	499
11.5.27	Dokumentationen	499
11.5.28	IKT-Hardware und Software	500
11.5.29	Infrastruktur	547
11.5.30	Material	548
11.5.31	Methoden und Verfahren	548
11.5.32	Personal.....	548
11.5.33	Organisation im Überblick	549
11.5.34	Lebenszyklus im Überblick	550
11.6	Interdependenznetz	551
11.7	Hilfsmittel RiSiKo-Architekturmatrix	553
11.8	Zusammenfassung	554
12	Sicherheitsrichtlinien/-standards – Generische Sicherheitskonzepte	556
12.1	Übergreifende Richtlinien	557
12.1.1	Sicherheitsregeln.....	557
12.1.2	Vorlage Prozessbeschreibung	559
12.1.3	Vorlage Ressourcenbeschreibung.....	562
12.1.4	Faxgeräte und Fax-Nutzung	564
12.1.5	Drucker.....	564
12.1.6	IKT-Benutzerordnung.....	564
12.1.7	E-Mail-Nutzung	576
12.1.8	Internet-Nutzung	577
12.1.9	Cloud Computing.....	578
12.2	Betriebs- und Begleitprozesse (Managementdisziplinen).....	581
12.2.1	Konformitätsmanagement	581
12.2.2	Datenschutzmanagement	582
12.2.3	Risikomanagement	586
12.2.4	Kapazitätsmanagement.....	591
12.2.5	Kontinuitätsmanagement	593
12.2.6	Securitymanagement.....	613
12.2.7	Architekturmanagement.....	635

12.3	Ressourcen	640
12.3.1	Zutrittskontrollsystem	640
12.3.2	Passwortbezogene Systemanforderungen	640
12.3.3	Firewall	642
12.3.4	Wireless LAN (WLAN).....	643
12.4	Organisation.....	644
12.5	Zusammenfassung	645
13	Spezifische Sicherheitskonzepte.....	647
13.1	Prozesse	648
13.1.1	Kontinuitätsmanagement	648
13.2	Ressourcen	649
13.2.1	Betriebssystem	649
13.3	Zusammenfassung	649
14	Sicherheitsmaßnahmen.....	650
14.1	Ressourcen	650
14.1.1	Betriebssystem: Protokoll Passworteinstellungen	650
14.2	Zusammenfassung	651
15	Lebenszyklus – mit integrierter Sicherheit.....	652
15.1	Übergreifendes	655
15.2	Sichere Beantragung (Secure Proposal Application).....	656
15.3	Sichere Planung (Secure Planning)	658
15.4	Sichere Fachkonzeption, sichere Anforderungsspezifikation.....	658
15.5	Sichere technische Grobkonzeption (Secure Technical Basic Design)	662
15.6	Sichere technische Feinkonzeption (Secure Technical Design).....	668
15.7	Sichere Entwicklung (Secure Development/Coding).....	670
15.8	Sichere Integrations- und Systemtest (Secure Integration/ System Tests).....	675
15.9	Sichere Freigabe (Secure Approval)	676
15.10	Sichere Software-Evaluation (Secure Software Evaluation).....	676
15.11	Sichere Auslieferung (Secure Delivery)	677
15.12	Sicherer Abnahmetest und sichere Abnahme (Secure Acceptance).....	678
15.13	Sichere Software-Verteilung (Secure Software Deployment)	679
15.14	Sichere Inbetriebnahme (Secure Startup Procedure).....	679
15.15	Sicherer Betrieb (Secure Operation).....	680
15.16	Sichere Außerbetriebnahme (Secure Decommissioning)	681
15.17	Hilfsmittel erweiterte Phasen-Ergebnistypen-Tabelle (ePET).....	682
15.18	Zusammenfassung	684

16 Sicherheitsregelkreis	686
16.1 Sicherheitsprüfungen	687
16.1.1 Sicherheitsstudie/Risikoanalyse	687
16.1.2 Penetrationstests	692
16.1.3 IKT-Security-Scans	693
16.2 Sicherheitscontrolling	694
16.3 Berichtswesen (SSCRPC-Reporting)	696
16.3.1 Anforderungen	696
16.3.2 Inhalte	698
16.4 Safety-Security-Continuity-Risk-Privacy-Compliance-Benchmarks	711
16.5 Hilfsmittel IKT-Sicherheitsfragen	711
16.6 Zusammenfassung	712
17 Reifegradmodell des Sicherheits-, Kontinuitäts- und Risikomanagements	713
17.1 Reifegradmodell RiSiKo-Management	713
17.1.1 Stufe 0: unbekannt	714
17.1.2 Stufe 1: begonnen	714
17.1.3 Stufe 2: konzipiert	715
17.1.4 Stufe 3: standardisiert	715
17.1.5 Stufe 4: integriert	715
17.1.6 Stufe 5: gesteuert	715
17.1.7 Stufe 6: selbst lernend	716
17.2 Checkliste Reifegrad	719
17.3 Praxisbeispiel	721
17.4 Zusammenfassung	722
18 Sicherheitsmanagementprozess	723
18.1 Deming- bzw. PDCA-Zyklus	723
18.2 Planung	724
18.3 Durchführung	726
18.4 Prüfung	726
18.5 Verbesserung	727
18.6 Zusammenfassung	727
19 Minimalistische Sicherheit	730
20 Verzeichnis der Abbildungen	732
21 Verzeichnis der Tabellen	734
22 Verzeichnis der Checklisten	734
23 Verzeichnis der Beispiele	735

24 Verzeichnis der Tipps.....737

25 Verzeichnis der Informationen.....738

26 Verzeichnis der Marken.....740

27 Verzeichnis über Gesetze, Vorschriften, Standards, Normen, Practices742

 27.1 Gesetze, Verordnungen, Richtlinien.....742

 27.1.1 Deutschland: Gesetze, Verordnungen.....742

 27.1.2 Österreich: Gesetze, Verordnungen744

 27.1.3 Schweiz: Gesetze, Verordnungen, Rundschreiben744

 27.1.4 Großbritannien: Gesetze745

 27.1.5 Europa: Entscheidungen, Richtlinien, Verordnungen,
 Practices745

 27.1.6 USA: Gesetze, Practices, Prüfvorschriften.....747

 27.2 Bestimmungen, Grundsätze, Vorschriften748

 27.3 Standards, Normen, Leitlinien751

Literatur- und Quellenverzeichnis780

Glossar und Abkürzungsverzeichnis785

Sachwortverzeichnis.....816

Über den Autor864