

Inhaltsübersicht

1 Ausgangssituation und Zielsetzung.....	1
2 Kurzfassung und Überblick für Eilige	13
3 Zehn Schritte zum Sicherheitsmanagement	15
4 Definitionen zum Sicherheits-, Kontinuitäts- und Risikomanagement ...	19
5 Die Sicherheitspyramide – Strategie und Vorgehensmodell	67
6 Sicherheits-, Kontinuitäts- und Risikopolitik.....	81
7 Sicherheitsziele / Sicherheitsanforderungen.....	97
8 Sicherheitstransformation	119
9 Sicherheitsarchitektur	129
10 Sicherheitsrichtlinien/-standards – Generische Sicherheitskonzepte...	301
11 Spezifische Sicherheitskonzepte	341
12 Sicherheitsmaßnahmen	345
13 Lebenszyklus	347
14 Sicherheitsregelkreis	365
15 Reifegradmodell des Sicherheitsmanagements – Safety/Security/Continuity Management Maturity Model	383
16 Sicherheitsmanagementprozess.....	393
17 Minimalistische Sicherheit	401
Abbildungsverzeichnis.....	403
Markenverzeichnis	404
Verzeichnis über Gesetze, Vorschriften, Standards, Normen, Practices.....	405
Literatur- und Quellenverzeichnis	419
Glossar und Abkürzungsverzeichnis.....	425
Sachwortverzeichnis.....	475
Über den Autor	505

Inhaltsverzeichnis

1 Ausgangssituation und Zielsetzung	1
1.1 Ausgangssituation	2
1.1.1 Bedrohungen	2
1.1.2 Schwachstellen	6
1.1.3 Schutzbedarf	9
1.2 Zielsetzung des Sicherheits-, Kontinuitäts- und Risikomanagements	10
1.3 Lösung	10
1.4 Zusammenfassung	12
2 Kurzfassung und Überblick für Eilige	13
3 Zehn Schritte zum Sicherheitsmanagement	15
4 Definitionen zum Sicherheits-, Kontinuitäts- und Risikomanagement	19
4.1 Unternehmenssicherheitsmanagementsystem	20
4.2 Informationssicherheitsmanagementsystem	21
4.3 Sicherheitsmanagement	22
4.4 ITK-Sicherheitsmanagement	23
4.4.1 ISO/IEC 13335-1:2004	24
4.4.2 ISO/IEC 17799:2005, ISO/IEC 27002:2005	26
4.4.3 ISO/IEC 27001:2005	28
4.4.4 ISO/IEC 27000-Reihe	30
4.4.5 ITIL® Security Management	31
4.4.6 IT-Grundschutzhandbuch, IT-Grundschutzkataloge des BSI	32
4.4.7 COBIT®, Version 4.0	37
4.4.8 BS 25999-1:2006	39
4.4.9 BS 25999-2	42
4.4.10 Fazit: Normen und Practices versus Sicherheitspyramide	43
4.5 Ingenieurmäßige Sicherheit – Safety, Security, Continuity Engineering	47
4.6 Sicherheitspyramide	47
4.7 Sicherheitspolitik	49
4.7.1 ... nach IT-Grundschutzhandbuch/-katalogen (IT-GSHB 2006)	49
4.7.2 ... nach ITSEC	50
4.7.3 ... nach ISO/IEC 13335-1:2004	51
4.7.4 ... nach ISO 15408 (Common Criteria)	52
4.7.5 ... nach ISO/IEC 17799:2005 bzw. ISO/IEC 27002:2005	52
4.7.6 ... nach ISO/IEC 27001:2005	53
4.7.7 ... nach Dr.-Ing. Müller	53
4.7.8 Vergleich	54
4.8 Sicherheit im Lebenszyklus	55

4.9 Ressourcen, Schutzobjekte und -subjekte sowie -klassen	56
4.10 Sicherheitskriterien	57
4.11 Geschäftseinflussanalyse (Business Impact Analysis)	58
4.12 Geschäftskontinuität (Business Continuity)	58
4.13 Sicherheit und Sicherheitsdreiklang	61
4.14 Risiko und Risikodreiklang	63
4.15 Risikomanagement	65
4.16 Zusammenfassung	65
5 Die Sicherheitspyramide – Strategie und Vorgehensmodell	67
5.1 Überblick	68
5.2 Sicherheitshierarchie	72
5.2.1 Sicherheits-, Kontinuitäts- und Risikopolitik	73
5.2.2 Sicherheitsziele / Sicherheitsanforderungen	73
5.2.3 Sicherheitstransformation	73
5.2.4 Sicherheitsarchitektur	74
5.2.5 Sicherheitsrichtlinien	74
5.2.6 Spezifische Sicherheitskonzepte	74
5.2.7 Sicherheitsmaßnahmen	75
5.3 PROSim	75
5.4 Lebenszyklus von Prozessen, Ressourcen, Produkten und Leistungen (Services)	76
5.4.1 Geschäfts-, Support- und Begleitprozess-Lebenszyklus	76
5.4.2 Ressourcen-/Systemlebenszyklus	77
5.4.3 Dienstleistungs- und Produktlebenszyklus	77
5.5 Sicherheitsregelkreis	77
5.6 Sicherheitsmanagementprozess	78
5.7 Zusammenfassung	78
6 Sicherheits-, Kontinuitäts- und Risikopolitik	81
6.1 Zielsetzung	82
6.2 Umsetzung	82
6.3 Inhalte	83
6.4 Checkliste	85
6.5 Praxisbeispiele	87
6.5.1 Sicherheits-, kontinuieräts- und risikopolitische Leitsätze Versicherung	87
6.5.2 Sicherheits-, Kontinuitäts- und Risikopolitik	89
6.6 Zusammenfassung	96
7 Sicherheitsziele / Sicherheitsanforderungen	97
7.1 Schutzbedarfsklassen	98
7.2 Schutzbedarfsanalyse	98
7.2.1 Prozessarchitektur und Prozesscharakteristika	99

7.2.2 Externe Sicherheitsanforderungen	100
7.2.3 Geschäftseinflussanalyse (Business Impact Analysis)	108
7.2.4 Betriebseinflussanalyse (Operational Impact Analysis)	110
7.3 Tabelle Schadensszenarien	111
7.4 Praxisbeispiele	113
7.4.1 Schutzbedarf der Geschäftsprozesse	113
7.4.2 ITK-Schutzbedarfsanalyse	113
7.4.3 Schutzbedarfsklassen	117
7.5 Zusammenfassung	118
8 Sicherheitstransformation	119
8.1 Haus zur Sicherheit – House of Safety, Security and Continuity (HoSSC)	120
8.2 Safety, Security and Continuity Function Deployment (SSCFD)	121
8.2.1 Transformation der Anforderungen auf Sicherheitscharakteristika	121
8.2.2 Detaillierung der Sicherheitscharakteristika	123
8.2.3 Abbildung der Charakteristika auf den Lebenszyklus	123
8.3 Schutzbedarfsklassen	124
8.4 Praxisbeispiele	125
8.5 Zusammenfassung	127
9 Sicherheitsarchitektur	129
9.1 Überblick	130
9.2 Prinzipielle Sicherheitsanforderungen	132
9.3 Prinzipielle Bedrohungen	132
9.4 Strategien und Prinzipien	135
9.4.1 Risikostrategie (Risk Strategy)	137
9.4.2 Sicherheitsstrategie (Safety, Security and Continuity Strategy)	138
9.4.3 Prinzip der Wirtschaftlichkeit	139
9.4.4 Prinzip der Abstraktion	139
9.4.5 Prinzip der Klassenbildung	140
9.4.6 Poka-Yoke-Prinzip	140
9.4.7 Prinzip der Namenskonventionen	142
9.4.8 Prinzip der Redundanz (Principle of Redundancy)	142
9.4.9 Prinzip des „aufgeräumten“ Arbeitsplatzes (Clear Desk Policy)	145
9.4.10 Prinzip des „gesperrten“ Bildschirms (Clear Screen Policy)	145
9.4.11 Prinzip der Eigenverantwortlichkeit	145
9.4.12 Vier-Augen-Prinzip (Confirmed Double Check Principle)	146
9.4.13 Prinzip der Funktionstrennung (Segregation of Duties)	146
9.4.14 Prinzip der Sicherheitsschalen (Security Shells)	146
9.4.15 Prinzip der Pfadanalyse	147
9.4.16 Prinzip des generellen Verbots (Deny All Principle)	147
9.4.17 Prinzip der minimalen Rechte (Need to Use Principle)	147
9.4.18 Prinzip der minimalen Dienste	147

9.4.19 Prinzip der minimalen Nutzung	148
9.4.20 Prinzip der Nachvollziehbarkeit und Nachweisbarkeit	148
9.4.21 Prinzip des „sachverständigen Dritten“	148
9.4.22 Prinzip des Closed-Shop-Betriebs und der Sicherheitszonen	148
9.4.23 Prinzip der Prozess-, Ressourcen- und Lebenszyklusimmanenz	149
9.4.24 Prinzip der Konsolidierung	150
9.4.25 Prinzip der Standardisierung (Principle of Standardization)	151
9.4.26 Prinzip der Plausibilisierung (Principle of Plausibleness)	151
9.4.27 Prinzip der Konsistenz (Principle of Consistency)	152
9.4.28 Prinzip der Untergliederung (Principle of Compartmentalization)	152
9.4.29 Prinzip der Vielfältigkeit (Principle of Diversity)	153
9.5 Sicherheitselemente	153
9.5.1 Prozesse im Überblick	154
9.5.2 Konformitätsmanagement (Compliance Management)	165
9.5.3 Datenschutzmanagement (Privacy Management)	166
9.5.4 Risikomanagement (Risk Management)	168
9.5.5 Leistungsmanagement (Service Level Management)	172
9.5.6 Finanzmanagement (Financial Management)	176
9.5.7 Projektmanagement (Project Management)	177
9.5.8 Qualitätsmanagement (Quality Management)	177
9.5.9 Ereignismanagement (Incident Management)	178
9.5.10 Problemmanagement (Problem Management)	184
9.5.11 Änderungsmanagement (Change Management)	185
9.5.12 Releasemanagement (Release Management)	188
9.5.13 Konfigurationsmanagement (Configuration Management)	188
9.5.14 Lizenzmanagement (Licence Management)	189
9.5.15 Kapazitätsmanagement (Capacity Management)	190
9.5.16 Wartungsmanagement (Maintenance Management)	192
9.5.17 Kontinuitätsmanagement (Continuity Management)	193
9.5.18 Securitymanagement (Security Management)	211
9.5.19 Architekturmanagement (Architecture Management)	246
9.5.20 Innovationsmanagement (Innovation Management)	259
9.5.21 Personalmanagement (Human Resources Management)	261
9.5.22 Ressourcen im Überblick	265
9.5.23 ITK-Hard- und Software	265
9.5.24 Infrastruktur	295
9.5.25 Dokumente	297
9.5.26 Personal	297
9.5.27 Organisation im Überblick	297
9.5.28 Lebenszyklus im Überblick	298
9.6 Hilfsmittel Sicherheits- und Risikoarchitekturmatrix	298
9.7 Zusammenfassung	300

10 Sicherheitsrichtlinien/-standards – Generische Sicherheitskonzepte	301
10.1 Übergreifende Richtlinien	302
10.1.1 Sicherheitsregeln	302
10.1.2 Prozessvorlage	303
10.1.3 IT-Benutzerordnung	305
10.1.4 E-Mail-Nutzung	307
10.1.5 Internet-Nutzung	310
10.2 Betriebs- und Begleitprozesse (Managementdisziplinen)	311
10.2.1 Kapazitätsmanagement	311
10.2.2 Kontinuitätsmanagement	313
10.2.3 Securitymanagement	325
10.3 Ressourcen	337
10.3.1 Zutrittskontrollsystem	337
10.3.2 Passwortspezifische Systemanforderungen	337
10.3.3 Wireless LAN	338
10.4 Organisation	339
10.5 Zusammenfassung	340
11 Spezifische Sicherheitskonzepte	341
11.1 Prozesse	342
11.1.1 Kontinuitätsmanagement	342
11.2 Ressourcen	343
11.2.1 Betriebssystem	343
11.3 Zusammenfassung	343
12 Sicherheitsmaßnahmen	345
12.1 Ressourcen	345
12.1.1 Betriebssystem: Protokoll Passworteinstellungen	345
12.2 Zusammenfassung	346
13 Lebenszyklus	347
13.1 Beantragung	348
13.2 Planung	349
13.3 Fachkonzept, Anforderungsspezifikation	349
13.4 Technisches Grobkonzept	350
13.5 Technisches Feinkonzept	351
13.6 Entwicklung	354
13.7 Integrations- und Systemtest	356
13.8 Freigabe	357
13.9 Software-Evaluation	357
13.10 Auslieferung	358
13.11 Abnahmetest und Abnahme	358

13.12 Software-Verteilung	359
13.13 Inbetriebnahme	360
13.14 Betrieb	360
13.15 Außerbetriebnahme	361
13.16 Hilfsmittel Phasen-Ergebnistypen-Tabelle	362
13.17 Zusammenfassung	363
14 Sicherheitsregelkreis	365
14.1 Sicherheitsprüfungen	366
14.1.1 Sicherheitsstudie/Risikoanalyse	366
14.1.2 Penetrationstests	370
14.1.3 IT-Security-Scans	371
14.2 Sicherheitscontrolling	372
14.3 Berichtswesen (Safety-Security-Reporting)	374
14.3.1 Anforderungen	374
14.3.2 Inhalte	377
14.4 Safety-Security-Benchmarks	380
14.5 Hilfsmittel IT-Sicherheitsfragen	380
14.6 Zusammenfassung	381
15 Reifegradmodell des Sicherheitsmanagements – Safety/Security/Continuity Management Maturity Model	383
15.1 Systems Security Engineering – Capability Maturity Model®	384
15.2 Information Technology Security Assessment Framework	385
15.3 Security-Maturity-Modell	386
15.4 Reifegradmodell nach Dr.-Ing. Müller	386
15.4.1 Stufe 0: unbekannt	386
15.4.2 Stufe 1: begonnen	387
15.4.3 Stufe 2: konzipiert	387
15.4.4 Stufe 3: standardisiert	387
15.4.5 Stufe 4: integriert	388
15.4.6 Stufe 5: gesteuert	388
15.4.7 Stufe 6: selbst lernend	388
15.5 Checkliste Reifegrad	388
15.6 Praxisbeispiel	390
15.7 Zusammenfassung	391
16 Sicherheitsmanagementprozess	393
16.1 Deming- bzw. PDCA-Zyklus	393
16.2 Planung	394
16.3 Durchführung	396
16.4 Prüfung	396
16.5 Verbesserung	397

16.6 Zusammenfassung.....	397
17 Minimalistische Sicherheit	401
Abbildungsverzeichnis.....	403
Markenverzeichnis	404
Verzeichnis über Gesetze, Vorschriften, Standards, Normen, Practices.....	405
Deutsche Gesetze und Verordnungen.....	405
Österreichische Gesetze und Verordnungen	406
Schweizer Gesetze, Verordnungen und Richtlinien	406
Britische Gesetze, Verordnungen und Richtlinien.....	407
Europäische Richtlinien	407
US-amerikanische Gesetze, Verordnungen und Richtlinien	408
Ausführungsbestimmungen, Grundsätze, Vorschriften.....	409
Standards, Normen, Leitlinien und Rundschreiben	410
Literatur- und Quellenverzeichnis	419
Glossar und Abkürzungsverzeichnis.....	425
Sachwortverzeichnis.....	475
Über den Autor.....	505