

Klaus-Rainer Müller

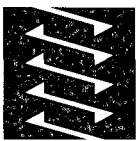
# Handbuch Unternehmens- sicherheit

Umfassendes Sicherheits-, Kontinuitäts-  
und Risikomanagement mit System

2., neu bearbeitete Auflage

Mit 35 Abbildungen

PRAXIS



**VIEWEG+**  
**TEUBNER**

# Inhaltsverzeichnis

<b>1 Ausgangssituation und Zielsetzung</b> .....	<b>1</b>
1.1 Ausgangssituation.....	2
1.1.1 Bedrohungen.....	2
1.1.2 Schwachstellen.....	10
1.1.3 Schutzbedarf und Haftung.....	13
1.2 Zielsetzung des Sicherheits-, Kontinuitäts- und Risikomanagements.....	16
1.3 Lösung.....	16
1.4 Zusammenfassung.....	18
<b>2 Kurzfassung und Überblick für Eilige</b> .....	<b>20</b>
<b>3 Zehn Schritte zum Sicherheitsmanagement</b> .....	<b>25</b>
<b>4 Definitionen zum Sicherheits-, Kontinuitäts- und Risikomanagement</b> .....	<b>27</b>
4.1 Unternehmenssicherheitsmanagementsystem.....	27
4.2 Informationssicherheitsmanagementsystem.....	28
4.3 Sicherheitsmanagement.....	29
4.4 Ingenieurmäßige Sicherheit – (Occupational) Health, Safety, Security and Continuity Engineering.....	32
4.5 Sicherheitspyramide.....	33
4.6 Sicherheitspolitik.....	35
4.7 Sicherheit im Lebenszyklus.....	36
4.8 Ressourcen, Schutzobjekte und -subjekte sowie -klassen.....	37
4.9 Sicherheitskriterien.....	39
4.10 Geschäftseinflussanalyse (Business Impact Analysis).....	39
4.11 Geschäftskontinuität (Business Continuity).....	39
4.12 Sicherheit und Sicherheitsdreiklang.....	39
4.13 Risiko und Risikodreiklang.....	41
4.14 Risikomanagement.....	43
4.15 Sicherheits-, Kontinuitäts- und Risikomanagement.....	43
4.16 Zusammenfassung.....	44
<b>5 Die Sicherheitspyramide – Strategie und Vorgehensmodell</b> .....	<b>47</b>
5.1 Überblick.....	48
5.2 Sicherheitshierarchie.....	52
5.2.1 Sicherheits-, Kontinuitäts- und Risikopolitik.....	52
5.2.2 Sicherheitsziele / Sicherheitsanforderungen.....	53
5.2.3 Sicherheitstransformation und Sicherheitsmerkmale.....	53
5.2.4 Sicherheitsarchitektur.....	54
5.2.5 Sicherheitsrichtlinien – Generische Sicherheitskonzepte.....	54

7.2.17 Weitere Anforderungen .....	125
7.2.18 Normen, Standards, Practices .....	125
7.2.19 Externe Anforderungen an das Unternehmen – Fazit .....	133
7.2.20 Geschäftseinflussanalyse (Business Impact Analysis) .....	134
7.2.21 Betriebseinflussanalyse (Operational Impact Analysis) .....	137
7.3 Tabelle Schadensszenarien .....	138
7.4 Praxisbeispiele .....	139
7.4.1 Schutzbedarf der Prozesse .....	139
7.4.2 Betriebseinflussanalyse .....	139
7.4.3 Schutzbedarfsklassen .....	143
7.5 Zusammenfassung .....	145
<b>8 Sicherheitsmerkmale .....</b>	<b>146</b>
8.1 Haus zur Sicherheit .....	147
8.2 „Occ. Health, Safety, Security and Continuity Function Deployment“ .....	148
8.2.1 Transformation der Anforderungen auf Sicherheitsmerkmale .....	148
8.2.2 Detaillierung der Sicherheitsmerkmale .....	150
8.2.3 Abbildung der Merkmale auf den Lebenszyklus .....	150
8.3 Schutzbedarfsklassen .....	152
8.4 Praxisbeispiele .....	152
8.5 Zusammenfassung .....	154
<b>9 Sicherheitsarchitektur .....</b>	<b>156</b>
9.1 Überblick .....	157
9.2 Prinzipielle Sicherheitsanforderungen .....	158
9.3 Prinzipielle Bedrohungen .....	159
9.4 Strategien und Prinzipien .....	163
9.4.1 Risikostrategie (Risk Strategy) .....	164
9.4.2 Sicherheits- und Kontinuitätsstrategie (Occ. Health, Safety, Security and Continuity Strategy) .....	165
9.4.3 Prinzip der Wirtschaftlichkeit .....	166
9.4.4 Prinzip der Abstraktion .....	166
9.4.5 Prinzip der Klassenbildung .....	167
9.4.6 Poka-Yoke-Prinzip .....	168
9.4.7 Prinzip der Namenskonventionen .....	169
9.4.8 Prinzip der Redundanz (Principle of Redundancy) .....	170
9.4.9 Prinzip des „aufgeräumten“ Arbeitsplatzes (Clear Desk Policy) .....	172
9.4.10 Prinzip des „gesperrten“ Bildschirms (Clear Screen Policy) .....	173
9.4.11 Prinzip der Eigenverantwortlichkeit .....	173
9.4.12 Vier-Augen-Prinzip (Confirmed Double Check Principle) .....	173
9.4.13 Prinzip der Funktionstrennung (Segregation of Duties Principle) ...	173
9.4.14 Prinzip der Sicherheitsschalen (Security Shell Principle) .....	173
9.4.15 Prinzip der Pfadanalyse (Path Analysis Principle) .....	174

9.4.16	Prinzip der Ge- und Verbotsdifferenzierung .....	175
9.4.17	Prinzip des generellen Verbots (Deny All Principle) .....	175
9.4.18	Prinzip der Ausschließlichkeit .....	176
9.4.19	Prinzip der minimalen Rechte (Need to Know/Use Principle).....	176
9.4.20	Prinzip der minimalen Dienste (Minimum Services Principle).....	176
9.4.21	Prinzip der minimalen Nutzung (Minimum Usage Principle).....	176
9.4.22	Prinzip der Nachvollziehbarkeit und Nachweisbarkeit .....	177
9.4.23	Prinzip des „sachverständigen Dritten“ .....	177
9.4.24	Prinzip der Sicherheitszonen und des Closed-Shop-Betriebs .....	177
9.4.25	Prinzip der Immanenz (Principle of Immanence) .....	178
9.4.26	Prinzip der Konsolidierung (Principle of Consolidation) .....	179
9.4.27	Prinzip der Standardisierung (Principle of Standardization) .....	181
9.4.28	Prinzip der Plausibilisierung (Principle of Plausibleness).....	181
9.4.29	Prinzip der Konsistenz (Principle of Consistency) .....	182
9.4.30	Prinzip der Untergliederung (Principle of Compartmentalization) ..	182
9.4.31	Prinzip der Vielfältigkeit (Principle of Diversity).....	182
9.4.32	Distanzprinzip .....	182
9.4.33	Prinzip der Vererbung.....	183
9.4.34	Prinzip der Subjekt-Objekt- bzw. Aktiv-Passiv-Differenzierung .....	184
9.5	Sicherheitselemente .....	184
9.5.1	Prozesse im Überblick .....	186
9.5.2	Konformitätsmanagement (Compliance Management) .....	195
9.5.3	Arbeitsschutzmanagement (Occ. Health and Safety Management) ...	197
9.5.4	Datenschutzmanagement (Privacy Management) .....	199
9.5.5	Risikomanagement (Risk Management) .....	201
9.5.6	Leistungsmanagement (Service Level Management).....	212
9.5.7	Finanzmanagement (Financial Management).....	220
9.5.8	Projektmanagement (Project Management) .....	220
9.5.9	Qualitätsmanagement (Quality Management) .....	220
9.5.10	Ereignismanagement (Incident Management).....	221
9.5.11	Problemmanagement (Problem Management).....	226
9.5.12	Änderungsmanagement (Change Management) .....	227
9.5.13	Releasemanagement (Release Management) .....	229
9.5.14	Konfigurationsmanagement (Configuration Management) .....	229
9.5.15	Lizenzmanagement (Licence Management).....	231
9.5.16	Kapazitätsmanagement (Capacity Management).....	232
9.5.17	Wartungsmanagement (Maintenance Management).....	244
9.5.18	Kontinuitätsmanagement (Continuity Management).....	245
9.5.19	Securitymanagement (Security Management).....	272
9.5.20	Architekturmanagement (Architecture Management) .....	314

9.5.21 Innovationsmanagement (Innovation Management) .....	314
9.5.22 Personalmanagement (Human Resources Management) .....	317
9.5.23 Ressourcen im Überblick .....	322
9.5.24 Organisation im Überblick .....	332
9.5.25 Lebenszyklus im Überblick .....	332
9.6 Hilfsmittel Sicherheits- und Risikoarchitekturmatrix .....	332
9.7 Zusammenfassung .....	333
<b>10 Sicherheitsrichtlinien/-standards.....</b>	<b>335</b>
10.1 Übergreifende Richtlinien .....	336
10.1.1 Sicherheitsregeln .....	336
10.1.2 Kommunikation .....	337
10.1.3 Prozessvorlage.....	338
10.1.4 Sourcing.....	340
10.1.5 Fax .....	343
10.1.6 IKT-Benutzerordnung .....	343
10.1.7 E-Mail-Nutzung .....	345
10.1.8 Internet-Nutzung .....	347
10.2 Kern-, Support-, Begleitprozesse (Managementdisziplinen).....	348
10.2.1 Datenschutzmanagement .....	348
10.2.2 Sicherheits-, Kontinuitäts- und Risikomanagement.....	349
10.2.3 Kapazitätsmanagement.....	350
10.2.4 Kontinuitätsmanagement .....	352
10.2.5 Securitymanagement .....	370
10.3 Ressourcen.....	381
10.4 Organisation .....	381
10.5 Zusammenfassung .....	383
<b>11 Spezifische Sicherheitskonzepte .....</b>	<b>384</b>
11.1 Prozesse.....	385
11.1.1 Kontinuitätsmanagement .....	385
11.2 Ressourcen.....	386
11.2.1 Betriebssystem.....	386
11.3 Zusammenfassung .....	386
<b>12 Sicherheitsmaßnahmen .....</b>	<b>387</b>
12.1 Ressourcen.....	387
12.1.1 Betriebssystem: Protokoll Passworteinstellungen.....	387
12.2 Zusammenfassung .....	388
<b>13 Prozess-, Produkt- und Dienstleistungslebenszyklen .....</b>	<b>389</b>
13.1 Prozesslebenszyklus.....	390
13.2 Produkt- und Dienstleistungslebenszyklus .....	394
13.3 Entscheidungsprozesslebenszyklus.....	396
13.4 Zusammenfassung .....	397

<b>14 Sicherheitsregelkreis</b> .....	<b>398</b>
14.1 Sicherheitsprüfungen .....	399
14.1.1 Sicherheitsstudie/-analyse .....	399
14.1.2 Penetrationstests .....	402
14.1.3 IT-Security-Scans .....	404
14.2 Sicherheitscontrolling .....	404
14.3 Berichtswesen (Occ. Health, Safety, Security and Continuity Reporting) .....	406
14.3.1 Anforderungen .....	406
14.3.2 Inhalte .....	408
14.4 Safety-Security-Continuity-Benchmarks .....	417
14.5 Hilfsmittel IT-Sicherheitsfragen .....	417
14.6 Zusammenfassung .....	418
<b>15 Reifegradmodell des Sicherheits-, Kontinuitäts- und Risiko-managements</b> .....	<b>419</b>
15.1 Systems Security Engineering – Capability Maturity Model® .....	420
15.2 Information Technology Security Assessment Framework .....	421
15.3 Maturity Model nach COBIT® .....	421
15.4 Reifegradmodell Unternehmenssicherheit .....	423
15.4.1 Stufe 0: unbekannt .....	423
15.4.2 Stufe 1: begonnen .....	424
15.4.3 Stufe 2: konzipiert .....	424
15.4.4 Stufe 3: standardisiert .....	424
15.4.5 Stufe 4: integriert .....	424
15.4.6 Stufe 5: gesteuert .....	424
15.4.7 Stufe 6: selbst lernend .....	425
15.5 Checkliste Reifegrad .....	425
15.6 Praxisbeispiel .....	426
15.7 Zusammenfassung .....	427
<b>16 Sicherheitsmanagementprozess</b> .....	<b>428</b>
16.1 Deming- bzw. PDCA-Zyklus .....	428
16.2 Planung .....	429
16.3 Durchführung .....	430
16.4 Prüfung .....	431
16.5 Verbesserung .....	431
16.6 Zusammenfassung .....	432
<b>17 Abbildungsverzeichnis</b> .....	<b>434</b>
<b>18 Markenverzeichnis</b> .....	<b>435</b>

---

<b>19 Verzeichnis über Gesetze, Vorschriften, Standards, Normen.....</b>	<b>436</b>
19.1 Gesetze, Verordnungen und Richtlinien.....	436
19.1.1 Deutschland: Gesetze und Verordnungen.....	436
19.1.2 Österreich: Gesetze und Verordnungen.....	437
19.1.3 Schweiz: Gesetze, Verordnungen und Rundschreiben.....	437
19.1.4 Großbritannien: Gesetze, Vorschriften.....	438
19.1.5 Europa: Entscheidungen und Richtlinien.....	438
19.1.6 USA: Gesetze, Practices und Prüfvorschriften.....	439
19.2 Ausführungsbestimmungen, Grundsätze, Vorschriften.....	440
19.3 Standards, Normen, Leitlinien und Rundschreiben.....	442
<b>20 Literatur- und Quellenverzeichnis.....</b>	<b>451</b>
<b>21 Glossar und Abkürzungsverzeichnis.....</b>	<b>455</b>
<b>22 Sachwortverzeichnis.....</b>	<b>473</b>
<b>23 Über den Autor.....</b>	<b>502</b>