

---

# Inhaltsverzeichnis

<b>1</b>	<b>Zur Motivation und Einführung</b>	<b>1</b>
1.1	Management-Prozess	1
1.2	Verantwortlichkeit	2
1.3	Umfang	2
1.4	Betrachtungsebene	3
1.5	Vorgehensmodell	4
1.6	ISO 27000	4
1.7	IT-Grundschutz	5
1.8	Mentalitäten	5
1.9	Ganzheitliches Vorgehen?	5
1.10	Erfahrungen	6
<b>2</b>	<b>Inventarisierung</b>	<b>9</b>
2.1	„Inventar“ der Begriffe	9
2.2	Organisation und Rollen	10
2.3	Geschäfts- und Verwaltungsprozesse	18
2.4	IT-Anwendungen	23
2.5	Information und Daten	27
2.6	IT-Systeme	32
2.7	Netzwerk	35
2.8	Infrastruktur	37
2.9	Zusammenfassung	39
	Literatur	40
<b>3</b>	<b>Wesentliche Elemente des Sicherheitsprozesses</b>	<b>41</b>
3.1	Die kontinuierliche Verbesserung	41
3.2	Unverzichtbar: Sensibilisierung, Schulung, Training	49
3.3	Lenkung der Dokumentation	52
3.4	Steuerung der Aufzeichnungen	56
3.5	Interne Audits	57

---

3.6	Die Management-Bewertung .....	58
3.7	Grundsätzliches zum Compliance Management .....	59
	Literatur .....	61
<b>4</b>	<b>Sicherheitsziele auf allen Ebenen .....</b>	<b>63</b>
4.1	Informationen und Daten .....	63
4.2	IT-Systeme .....	72
4.3	Geschäftsprozesse .....	76
<b>5</b>	<b>Analysen .....</b>	<b>79</b>
5.1	Analyse nach IT-Grundschutz .....	80
5.2	Die Schwachstellenanalyse .....	86
5.3	Ein Ansatz auf der Basis der ISO 15408 .....	88
5.4	Risikoanalyse nach ISO/IEC 13335-3 .....	98
5.5	Betrachtungsmodell der ISO 27005 .....	108
5.6	Restrisiken und ihre Behandlung .....	116
	Literatur .....	117
<b>6</b>	<b>Die Sicherheitsleitlinie .....</b>	<b>119</b>
6.1	Inhalte der Sicherheitsleitlinie .....	120
6.2	Management der Sicherheitsleitlinie .....	124
	Literatur .....	126
<b>7</b>	<b>Grundsätzliches zu Sicherheitsmaßnahmen .....</b>	<b>127</b>
7.1	Maßnahmenklassen .....	127
7.2	Validierung von Maßnahmen .....	129
	Literatur .....	132
<b>8</b>	<b>Das Sicherheitskonzept .....</b>	<b>133</b>
8.1	Grundsätzliches .....	133
8.2	Sicherheitskonzept nach IT-Grundschutz .....	135
8.3	Klassisches IT-Sicherheitskonzept .....	136
8.4	Sicherheitskonzept nach ISO 27001 .....	149
	Literatur .....	154
<b>9</b>	<b>Rechtliche Sicherheit .....</b>	<b>155</b>
9.1	Befolgen von Gesetzen .....	156
9.2	Vermeidung von Strafprozessen .....	160
9.3	Outsourcing .....	160
9.4	Verschiedenes .....	163

---

<b>10 Organisatorische Maßnahmen</b>	167
10.1 Vorgaben für die Abwicklung von Geschäftsprozessen	167
10.2 Festlegen von Rollen und Organisationplänen	168
10.3 Organisatorische Anweisungen	169
<b>11 Personelle Sicherheit</b>	173
11.1 Arbeitsverträge	174
11.2 Vertrauliche Personaldaten	176
11.3 Verantwortung der Mitarbeiter für die Informationssicherheit	178
11.4 Personalmanagement	181
11.5 Ausscheiden von Mitarbeitern	181
11.6 Verschiedenes	182
<b>12 Verhinderung unerwünschten Datenabflusses</b>	183
12.1 Definitionen	184
12.2 Sensible Daten	184
12.3 Arten von Data Leakage	185
12.4 Rechtliche Maßnahmen	188
12.5 Organisatorische Maßnahmen	191
12.6 Data Leakage Protection in der Praxis	193
12.7 Zusammenfassung	197
<b>13 Technische Sicherheitsmaßnahmen</b>	199
13.1 Wahrung der Vertraulichkeit	199
13.2 Identifizierung und Authentisierung	200
13.3 Zugriffskontrolle	204
13.4 Wiederaufbereitung	209
13.5 Verschlüsselung	211
13.6 Wahrung der Integrität	219
13.7 Elektronische Signatur	222
13.8 Verfügbarkeit von Daten	230
13.9 System-Verfügbarkeit	233
13.10 Übertragungssicherung	239
13.11 Beweissicherung und Auswertung	240
Literatur	242
<b>14 Sicherheit im Internet</b>	243
14.1 Gefährdungen	244
14.2 Schutzmaßnahmen: Regelwerke für Internet und Email	246
14.3 Technische Schutzmaßnahmen: Internet-Firewalls	247
14.4 Zusammenfassung	252

---

<b>15 Infrastruktursicherheit</b> .....	253
15.1 Geltungsbereiche und Schutzziele .....	253
15.2 Gebäude, Fenster, Türen .....	254
15.3 Verkabelung .....	255
15.4 Drahtlose Netzwerke .....	256
15.5 802.11x WLAN (Wireless LAN) .....	257
15.6 Wi-Fi Protected Access (WPA/WPA2) .....	258
15.7 Weitere Infrastrukturprobleme und -maßnahmen .....	259
15.8 Richtlinien zur Zutrittskontrolle .....	262
15.9 Verfahren der Zutrittskontrolle .....	263
Literatur .....	265
<b>16 Sicherheitsmanagement – die tägliche Praxis</b> .....	267
16.1 Aufrechterhaltung der Sicherheit .....	267
16.2 Messen der Sicherheit .....	269
16.3 Management von Sicherheitsvorfällen .....	271
16.4 Berichtswesen .....	274
Literatur .....	275
<b>17 IT Compliance</b> .....	277
17.1 Unternehmensstrategie .....	277
17.2 Compliance als essentieller Bestandteil der IT-Strategie .....	278
17.3 Compliance und Risikomanagement .....	280
Literatur .....	281
<b>18 Zum Schluss...</b> .....	283
Literatur .....	286
<b>Fachbegriffe englisch./ . deutsch</b> .....	287
<b>Sachwortverzeichnis</b> .....	289

**Der IT Security Manager**

Aktuelles Praxiswissen für IT Security Manager und  
IT-Sicherheitsbeauftragte in Unternehmen und  
Behörden

Kersten, H.; Klett, G.

2015, XX, 297 S. 24 Abb., Softcover

ISBN: 978-3-658-09973-2