

---

Heinrich Kersten • Gerhard Klett  
Jürgen Reuter • Klaus-Werner Schröder

# IT-Sicherheitsmanagement nach der neuen ISO 27001

ISMS, Risiken, Kennziffern, Controls

---

# Inhaltsverzeichnis

<b>1 Einführung</b> .....	1
1.1 Historie und Informationen.....	1
1.2 Die Normenreihe.....	2
1.3 Das ISMS.....	4
1.4 Der Anhang A.....	11
1.5 ISMS und Auslagerung.....	13
1.6 Checkliste.....	14
Literatur.....	15
<b>2 Die Anforderungen an ein ISMS</b> .....	17
2.1 Kontext der Organisation (NK 4).....	17
2.2 Führung (NK 5).....	20
2.3 Planung (NK 6).....	22
2.4 Unterstützung (NK 7).....	27
2.5 Betrieb (NK 8).....	31
2.6 Bewertung der Leistung (NK 9).....	32
2.7 Verbesserung (NK 10).....	35
2.8 Checkliste.....	36
Literatur.....	37
<b>3 Risikomanagement</b> .....	39
3.1 Risikomanagement als Aufgabe.....	39
3.2 Verfahren der Risikobeurteilung.....	47
3.2.1 IT-Grundschutz und Erweiterung.....	48
3.2.2 Ein Beispiel aus ISO 27005.....	50
3.2.3 Die Scorecard-Methode.....	52
3.2.4 Angriffspotenzial nach ISO 15408.....	59
Literatur.....	61

<b>4</b>	<b>Sicherheit messen</b> .....	63
4.1	Ziele .....	63
4.2	Überwachen und Messen .....	64
4.3	Messungen bewerten .....	72
	Literatur .....	74
<b>5</b>	<b>Interne und externe Audits</b> .....	75
5.1	Ziele und Nutzen .....	76
5.2	Die Rahmenbedingungen .....	79
5.3	Vorbereiten eines Audits .....	88
5.4	Durchführung eines Audits .....	91
5.5	Typische Defizite .....	93
5.6	Auditbericht und Auswertung .....	97
	Literatur .....	98
<b>6</b>	<b>Die Controls im Anhang A</b> .....	99
6.1	Überblick .....	99
6.2	Die einzelnen Controls .....	101
6.2.1	Informationssicherheitsrichtlinien (A.5) .....	101
6.2.2	Organisation der Informationssicherheit (A.6) .....	104
6.2.3	Personalsicherheit (A.7) .....	110
6.2.4	Verwaltung der Werte (A.8) .....	115
6.2.5	Zugangsteuerung (A.9) .....	123
6.2.6	Kryptographie (A.10) .....	136
6.2.7	Physische und umgebungsbezogene Sicherheit (A.11) .....	138
6.2.8	Betriebssicherheit (A.12) .....	150
6.2.9	Kommunikationssicherheit (A.13) .....	163
6.2.10	Anschaffung, Entwicklung und Instandhalten von Systemen (A.14) .....	171
6.2.11	Lieferantenbeziehungen (A.15) .....	183
6.2.12	Handhabung von Informationssicherheitsvorfällen (A.16) .....	189
6.2.13	Informationssicherheitsaspekte beim Business Continuity Management (A.17) .....	195
6.2.14	Compliance (A.18) .....	201
	Literatur .....	208
<b>7</b>	<b>ISMS und mobile Infrastrukturen</b> .....	209
7.1	Übersicht .....	209
7.2	Mobile Infrastrukturen in Unternehmen .....	210
7.3	ISMS und Mobile Device Management .....	211
7.4	Sicherheitsleitlinie .....	213
7.5	Sicherheitsrichtlinie .....	214
7.6	BCM und Notfallmanagement .....	219
	Literatur .....	221

---

<b>8 Umsteigen von „alt“ nach „neu“</b> .....	223
8.1 Vorüberlegungen .....	223
8.2 Hauptteil der ISO 27001 .....	226
8.3 Anhang A der Norm.....	228
8.4 Weitere Dokumente und Pläne.....	230
8.5 Checkliste.....	231
Literatur.....	232
<b>9 Interne Kontrollsysteme</b> .....	233
9.1 Problemstellung .....	233
9.2 Klassische Beispiele.....	237
9.3 Handlungsempfehlung .....	239
Literatur.....	240
<b>10 ISMS und IT-Sicherheitsgesetz</b> .....	243
10.1 Überblick.....	243
10.2 ISMS-Anpassungen .....	244
Literatur.....	246
<b>Fachbegriffe englisch/deutsch</b> .....	247
<b>Stichwortverzeichnis</b> .....	249