

Inhaltsverzeichnis

Dank	V
Vorwort	VII
Inhaltsverzeichnis	XI
1 Einführung	1
1.1 Wie wir uns entscheiden	1
1.2 ISMS – Managementsysteme für Informationssicherheit	3
1.3 Schritt für Schritt.....	6
1.4 Hinweise zum Buch	8
2 Grundlagen	13
2.1 Sprachgebrauch, Begriffe und Besonderheiten der Übersetzung	14
2.1.1 Mindmap und Definition wichtiger Begriffe.....	16

2.2	Entscheidend ist die Methodik.....	21
2.3	Der Ansatz der ISO	23
2.3.1	Die Entwicklung der ISO-Standards	24
2.3.2	Der PDCA-Zyklus	27
2.4	Die ISO 31000 Familie.....	28
2.4.1	Risikomanagement mit ISO 31000	29
2.4.2	Von der Theorie zur Praxis: ISO/IEC 31010	32
2.5	Die ISO/IEC 27000 Familie	37
2.5.1	Familienübersicht	37
2.5.2	Weitere Security-Standards.....	43
2.6	Was ist Risikomanagement?	44
2.6.1	Typische Bedrohungen der Informationssicherheit.....	45
2.6.2	Typische Schwachstellen der Informationssicherheit.....	47
2.6.3	Ursache und Wirkung.....	48
2.6.4	SANS Institut.....	50
2.7	ExAmple AG - Die Firma für die Fallbeispiele	53
2.8	Die ISO/IEC 27000 Familie in kleinen Organisationen .	55
2.9	Zusammenfassung	56
3	ISO/IEC 27005	59
3.1	Überblick über den Risikomanagement-Prozess.....	60
3.2	Festlegung des Kontexts.....	62
3.3	Risiko-Assessment.....	66
3.3.1	Risikoidentifikation	67
3.3.2	Risikoanalyse.....	72
3.3.3	Risikobewertung/ Priorisierung	75
3.4	Risikobehandlung	78
3.5	Risikoakzeptanz.....	87
3.6	Risikokommunikation und Beratung.....	89

3.7	Risikoüberwachung/ -überprüfung	92
3.8	Zusammenfassung	94
4	ISO 27005 und BSI IT-Grundschutz	97
4.1	Die Vorgehensweise nach IT-Grundschutz.....	98
4.2	BSI-Standard 100-3	100
4.3	Die IT-Grundschutz-Kataloge	103
4.4	Zusammenfassung	105
5	Risiko-Assessment	107
5.1	Methodensteckbriefe.....	108
5.2	Merkmale.....	109
5.3	Gruppierungen	110
5.4	Brainstorming	112
5.5	Strukturierte und semistrukturierte Interviews	114
5.6	Die Delphi-Methode.....	116
5.7	Checklisten	118
5.8	Szenario-Analysen.....	120
5.9	Business Impact Analysen (BIA).....	122
5.10	Ursachenanalyse (Root Cause Analysis RCA).....	124
5.11	Fehler- und Ereignisbaumanalyse (FTA und ETA) ...	126
5.12	Ursache-Wirkungsanalysen.....	128
5.13	Bow Tie Methode	130
5.14	Risikoidizes.....	132
5.15	Auswirkungs-Wahrscheinlichkeits-Matrix.....	134
5.16	Entscheidungsmatrizen.....	136
5.17	Zusammenfassung.....	138
6	Risikokommunikation	139
6.1	Theoretische Grundlagen	140
6.2	Das besondere an Risiken	145
6.3	Konfliktpotential.....	148

6.4	Kommunikationsmatrix	149
6.5	Zusammenfassung	153
7	Wirtschaftlichkeitsbetrachtung	155
7.1	Pacta sunt servanda	157
7.2	Wirtschaftlichkeitsprinzipien	158
7.3	Kosten-Nutzen-Analysen.....	160
7.4	Pareto-Prinzip	161
7.5	Total Cost/ Benefit of Ownership (TCO/ TBO)	163
7.6	Return on Security Investment (ROSI).....	166
7.7	Stochastischer ROSI	168
7.8	Return on Information Security Invest (ROISI)	170
7.9	Zusammenfassung	173
8	Die 10 wichtigsten Tipps	175
8.1	Hören Sie aufmerksam zu.....	176
8.2	Achten Sie auf die Usability.....	176
8.3	Reden Sie nicht nur von Risiken	176
8.4	Denken Sie wirtschaftlich.....	177
8.5	Der Weg ist das Ziel.....	177
8.6	Schauen Sie über den Tellerrand	178
8.7	Übernehmen Sie Verantwortung	178
8.8	Geben Sie Verantwortung ab.....	178
8.9	Der Empfänger macht die Nachricht	179
8.10	Verbeißen Sie sich nicht ;-).....	179
	Sachwortverzeichnis	181
	Abkürzungsverzeichnis	187
	Literaturverzeichnis	191
	GNU General Public License	195