

Sebastian Klipper

Information Security Risk Management

Risikomanagement mit ISO/IEC 27001, 27005
und 31010

Mit 31 Abbildungen, 10 Tabellen und 14 Fallbeispielen

PRAXIS



Inhaltsverzeichnis

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	Begriffe aus ISO/IEC 27001	16
2.1.2	Begriffe aus ISO/IEC 27002	18
2.1.3	Begriffe aus ISO/IEC 27005	19
2.1.4	Übersicht der explizit definierten Begriffe	21
2.2	Entscheidend ist die Methodik.....	23

2.3	Der Ansatz der ISO	25
2.3.1	Die Entwicklung der ISO-Standards	26
2.3.2	Der PDCA-Zyklus.....	29
2.4	Die ISO 31000 Familie.....	31
2.4.1	Risikomanagement mit ISO 31000.....	31
2.4.2	Von der Theorie zur Praxis: ISO/IEC 31010	35
2.5	Die ISO/IEC 27000 Familie	39
2.5.1	Familienübersicht.....	39
2.5.2	Weitere Security-Standards	43
2.6	Abgrenzung zum BSI IT-Grundschutz	43
2.7	Was ist Risikomanagement?.....	46
2.7.1	Typische Bedrohungen der Informationssicherheit	47
2.7.2	Typische Schwachstellen der Informationssicherheit	50
2.7.3	Ursache und Wirkung	51
2.7.4	SANS Risikoliste	53
2.8	ExAmpLe AG - Die Firma für die Fallbeispiele	55
2.9	Die ISO/IEC 27000 Familie in kleinen Organisationen.....	59
2.10	Zusammenfassung.....	60
3	ISO/IEC 27005	63
3.1	Überblick über den Risikomanagement-Prozess	64
3.2	Festlegung des Kontexts.....	66
3.3	Risiko-Assessment	70
3.3.1	Risikoidentifikation	72
3.3.2	Risikoabschätzung.....	76
3.3.3	Risikobewertung/ Priorisierung.....	78
3.4	Risikobehandlung.....	81
3.5	Risikoakzeptanz	89
3.6	Risikokommunikation.....	90

3.7	Risikoüberwachung/ -überprüfung.....	93
3.8	Zusammenfassung.....	96
4	ISO 27005 und BSI IT-Grundschutz.....	99
4.1	Die Vorgehensweise nach IT-Grundschutz.....	100
4.2	BSI-Standard 100-3.....	102
4.3	Die IT-Grundschutz-Kataloge.....	105
4.4	Zusammenfassung.....	107
5	Risiko-Assessment.....	109
5.1	Methodensteckbriefe.....	110
5.2	Merkmale.....	111
5.3	Gruppierungen.....	112
5.4	Brainstorming.....	114
5.5	Strukturierte und semistrukturierte Interviews.....	116
5.6	Die Delphi-Methode.....	118
5.7	Checklisten.....	120
5.8	Vorläufige Sicherheitsanalyse (Preliminary Hazard Analysis PHA).....	122
5.9	HAZOP-Studie (HAZard and OPerability).....	124
5.10	HACCP-Konzept (Hazard Analysis and Critical Control Points).....	128
5.11	SWIFT-Technik (Structured "What if").....	130
5.12	Szenario-Analysen.....	132
5.13	Business Impact Analysen (BIA).....	134
5.14	Ursachenanalyse (Root Cause Analysis RCA).....	136
5.15	Auswirkungsanalysen (FMEA und FMECA).....	138
5.16	Fehler- und Ereignisbaumanalyse (FTA und ETA).....	140
5.17	Ursache-Wirkungsanalysen.....	142
5.18	Bow Tie Methode.....	144
5.19	Zuverlässigkeitsanalyse (Human Reliability Assessment HRA).....	146

5.20	Risikoindizes.....	148
5.21	Auswirkungs-Wahrscheinlichkeits-Matrix	150
5.22	Entscheidungsmatrizen.....	152
5.23	Zusammenfassung.....	154
6	Risikokommunikation	155
6.1	Theoretische Grundlagen.....	156
6.2	Das besondere an Risiken	161
6.3	Konfliktpotential	163
6.4	Kommunikationsmatrix	165
6.5	Zusammenfassung.....	169
7	Wirtschaftlichkeitsbetrachtung	171
7.1	Pacta sunt servanda	173
7.2	Wirtschaftlichkeitsprinzipien	174
7.3	Kosten-Nutzen-Analysen.....	176
7.4	Pareto-Prinzip.....	177
7.5	Total Cost/ Benefit of Ownership (TCO/ TBO)	179
7.6	Return on Security Investment (ROSI).....	182
7.7	Stochastischer ROSI	183
7.8	Return on Information Security Invest (ROISI)	186
7.9	Zusammenfassung.....	189
8	Die 10 wichtigsten Tipps	191
8.1	Hören Sie aufmerksam zu.....	192
8.2	Achten Sie auf die Usability.....	192
8.3	Reden Sie nicht nur von Risiken	192
8.4	Denken Sie wirtschaftlich	193
8.5	Der Weg ist das Ziel.....	193
8.6	Schauen Sie über den Tellerrand	194
8.7	Übernehmen Sie Verantwortung	194
8.8	Geben Sie Verantwortung ab.....	194

8.9 Der Empfänger macht die Nachricht	195
8.10 Verbeißen Sie sich nicht ;-)	195
Interessante Tools und Frameworks	197
Steckbriefe	198
Übersicht	199
Security Risk Management Guide (SRMG)	200
Security Assessment Tool (MSAT)	202
Common Vulnerability Scoring System (CVSS)	204
Risk Management Framework chaRMe	206
Weitere Tools	208
Secricon Risk Management Software	208
Lumension Risk Manager	209
Proteus	209
Modulo Risk Manager (NG)	210
STEAM	210
risk2value	211
BPSResolver ERM	211
Risk Watch	212
Risk Management Studio	212
RA2 Art of Risk	213
OCTAVE	213
Zusammenfassung	214
Sachwortverzeichnis	215
Abkürzungsverzeichnis	223
Literaturverzeichnis	227
GNU General Public License	231