

Inhaltsverzeichnis

1	Einleitung	1
	Literatur.....	4
2	Wichtige Begriffe rund um Informationssicherheit	5
2.1	Wie sicher ist sicher?.....	5
2.2	Informationssicherheit aus historischer Sicht	6
2.3	Grundlagen der Informationssicherheit.....	8
2.3.1	Grundbegriffe der Informationssicherheit.....	8
2.3.2	Grundwerte der Informationssicherheit	9
2.3.3	Weitere relevante Definitionen der Informationssicherheit.....	9
2.3.4	Sonstige Begriffe (Auswahl)	10
2.4	Grundlagen des Managements der Informationssicherheit.....	12
2.4.1	Einführung in das Informationssicherheitsmanagement.....	12
2.4.2	Definition des Informationssicherheitsmanagements	13
	Literatur.....	15
3	Management der Informationssicherheit als Prozess	17
3.1	Plan-Do-Check-Act-Zyklus der Informationssicherheit.....	18
3.1.1	Besondere Anforderungen bezüglich Detektion und Reaktion.....	19
3.2	Organisation des Informationssicherheitsmanagements	20
3.2.1	Sicherheitsbeauftragte und Sicherheitsorganisation.....	21
3.2.2	Zentrales Sicherheitsmanagement.....	27
3.3	Rechtliche Grundlagen der IT-Sicherheit.....	27
3.3.1	Grundsätze ordnungsmäßiger Buchführung	29
3.3.2	Standards und Grundsätze des IDW.....	30
3.3.3	Neu: IT-Sicherheitsgesetz	32
	Literatur.....	33
4	Schichten des Informationssicherheitsmanagements	35
	Literatur.....	37

5 Risiko-Schicht: Plan-Phase des Managements der Informationssicherheit	39
5.1 Definition Risikomanagement	40
5.2 Abgrenzung und Begriffe	41
5.3 Sicherheit aus Risikosicht.....	42
5.4 Risikomanagement als Prozess.....	43
5.5 Risikoarten.....	44
5.6 Risiken bestimmen – aber wie?.....	46
5.7 Risikoanalyse.....	46
5.8 Klassische Risikobewertung	48
5.9 Kritik der klassischen Risikobewertung	48
5.10 Dynamische Risikobewertung	49
5.11 Alternative zur Risikoanalyse: Sicherheitsanalyse.....	51
Literatur.....	52
6 Governance-Schicht: Do-Phase des Management der Informationssicherheit.....	55
6.1 Gängige Standards	55
6.2 Sicherheitskontrollen (Security Controls).....	57
6.3 Datenschutzkontrollen – technisch-organisatorische Maßnahmen gemäß BDSG	60
6.4 Das absolute Minimum an Sicherheitskontrollen – Information Security Starting Point	64
Literatur.....	65
7 Compliance-Schicht: Die Check-Phase des Managements der Informationssicherheit.....	67
7.1 Incident Management – Management von Informationssicherheitsvorfällen.....	68
7.1.1 Angriffstrends und Angreifer	69
7.1.2 Relevante Angreifergruppen	69
7.1.3 Hacking-Trends.....	71
7.1.4 Ziele des Information Security Incident Management.....	73
7.1.5 Incident Management als Prozess	75
7.1.6 Notfallmanagement.....	76
7.1.7 Disaster Recovery	84
7.2 Security Audit, Monitoring und Reporting.....	84
7.2.1 Monitoring als Überwachungsfunktion.....	85
7.2.2 Audit bzw. Prüfung der Informationssicherheit als Aufgabe interner Revision	86
7.2.3 Kontinuierliches (ongoing) Monitoring	88
7.2.4 Continuous Auditing.....	90

7.3	Ziel des Security Monitorings.....	90
7.3.1	Was ist eine Metrik?.....	90
7.3.2	Anwendungsgebiet der Metriken	91
7.3.3	Metriken vs. Key Performance Indicators (KPIs).....	91
7.3.4	Metriken vs. Messungen	92
7.3.5	Goal-Question-Paradigma (GQM).....	92
7.3.6	Beispiele für Metriken zur Bewertung von Verwundbarkeit der Systeme (operative Ebene).....	93
7.3.7	Einsatz des Goal-Question-Paradigmas zur Ableitung von Metriken zur Bewertung der Effektivität von Security Policy	95
7.4	Reporting und Berichterstattung	97
7.4.1	Reporting-Arten	97
7.4.2	Internes Reporting.....	98
7.4.3	Externes Reporting.....	99
	Literatur.....	100
8	Cyber- und Computerkriminalität: Prüfung doloser Handlungen.....	103
8.1	„Neue“ Kriminalität	104
8.2	Relevante Prüfungsarten.....	105
8.3	Jahresabschlussprüfung und die neue Wirtschaftskriminalität	106
8.4	Unterschlagungsprüfungen	107
8.5	Instrumente einer forensischen Prüfung.....	108
8.6	IT-forensische Untersuchungen.....	108
8.6.1	Ziel einer forensischen Untersuchung.....	109
8.6.2	Cybercrime im Transaktionsumfeld.....	110
8.6.3	Schritte einer forensischen Untersuchung (best practices)	111
8.7	Ausgewählte forensische Techniken	112
8.8	Kennzahlenanalyse nach dem Benford'schen Gesetz.....	113
8.8.1	Anwendungsbeispiele	115
8.9	Social Engineering	117
8.9.1	Zulässigkeit der Datenauswertungen	118
	Literatur.....	121
9	Act-Phase: Bewerten – verbessern – optimieren.....	123
9.1	Bewertung des ISMS: Anforderungen aus dem ISO 27001	124
9.2	Anforderungen an Kennzahlensysteme.....	125
9.3	Sicherheit bewerten, verbessern, optimieren.....	126
9.3.1	Ziele des Exposure Index	126
9.3.2	Relevante Indikatoren.....	127
9.3.3	Ermittlung der Indizes für Verwundbarkeit und Bedrohung.....	127
9.3.4	Berechnung des Verwundbarkeitsindex	128

9.3.5	Berechnung des Index der Bedrohungslage	130
9.3.6	Vor- und Nachteile des Modells	132
9.4	Ziel der Verfahren	133
	Literatur.....	134
10	Schlussbetrachtung	135
	Literatur.....	136
	Literatur	137
	Stichwortverzeichnis	139