Inhaltsverzeichnis

	Vorwort	6
Teil A	Grundlagen für das IT-Sicherheitsmanagement	9
1	Schutzziele und Schutzbedarf	10
1.1	IT-Sicherheit	10
1.2	Schutzziel Datensicherheit	11
1.3	Schutzziel Datenschutz	12
1.4	Datensicherung und Notfallvorsorge	13
1.5	Sicherheitsgefahren und -bedürfnisse	13
1.6	Sicherheit der Geschäftsprozesse	18
1.7	Rolle der Informatik	19
1.8	Sicherheitskriterien	20
2	Gesetze, Standards und Regelwerke	23
2.1	Gesetze und Verordnungen	23
2.2	Best Practices und Standards	31
2.3	Verwendung mehrerer Standards	38
2.4	Weitere Regelwerke	39
3	Sicherheitsanforderungen und -aufgaben	42
3.1	Anforderungen an die IT-Sicherheit	42
3.2	Rolle des IT-Sicherheitsbeauftragten	45
3.3	Organisation der IT-Sicherheit	46
4	Methoden und Techniken	54
4.1	PDCA-Zyklus	54
4.2	Risikomanagement und Risikoanalyse	55
4.3	Business-Impact-Analyse	64
4.4	Strukturanalyse und Schutzbedarfsfeststellung	66
Teil B	IT-Sicherheit planen	71
5	Sicherheitsstrategie und Sicherheitskonzept erstellen	72
5.1	Strategien	72
5.2	IT-Sicherheitskonzept	75
5.3	Kontrollmodell	78
6	Risiken analysieren, Schutzbedarf feststellen, Schwachstellen aufdecken	80
6.1	Sicherheitsrisiken analysieren	80
6.2	Sicherheitsrisiken prozessorientiert analysieren	83
6.3	Schutzbedarf feststellen	84
6.4	Sicherheitslücken aufdecken	88
7	Managementsystem für IT-Sicherheit entwickeln	91
7.1	Informationssicherheits-Managementsystem	91
7.2	Sicherheitsvorfälle behandeln	95
8	Sicherheits- und Notfallmassnahmen entwickeln	100
8.1	Sicherheitsmassnahmen entwickeln	100
8.2	Notfallvorsorge	105
Teil C	IT-Sicherheit auf- und ausbauen	111
9	Sicherheitsmassnahmen aufeinander abstimmen	112
9.1	Sicherheitsmassnahmen gliedern	112
9.2	Zur Wirtschaftlichkeit von Sicherheitsmassnahmen	114
9.3	Über Restrisiko entscheiden	118
9.4	Sicherheitsprogramm und Realisierungspläne	119
9.5	Sicherheitsbewusstsein stärken	120

10	Personelle Massnahmen planen und umsetzen	124
10.1	Zum Nutzen personeller Massnahmen	124
10.2	Sicherheitsmassnahmen nach ISO/IEC 17799	124
10.3	Sicherheitsmassnahmen nach BSI-Grundschutzmethode	126
11	Organisatorische Massnahmen planen und umsetzen	133
11.1	ISMS etablieren	133
11.2	Sicherheitskonzepte erstellen	134
11.3	Weisungen erstellen	136
11.4	Dokumentationssystem etablieren	139
11.5	Life-Cycle-Management etablieren	139
12	Technische Massnahmen planen und umsetzen	144
12.1	Massnahmenkatalog Hardware und Software	144
12.2	Massnahmenkatalog Kommunikation	149
12.3	Massnahmenkatalog Infrastruktur in Gebäuden	151
12.4	Massnahmenkatalog Infrastruktur für Gebäude	152
13	Bereichsübergreifende Massnahmen	155
13.1	Massnahmen für den Datenschutz	155
13.2	Massnahmen für sichere Internetdienste	159
13.3	Einsatz von Remote-Access-Systemen	162
13.4	Einsatz von Firewalls	165
13.5	Einsatz mobiler Speichergeräte	168
Teil D	IT-Sicherheit überprüfen	171
14	Sicherheitsmassnahmen und -aktivitäten überwachen	172
14.1	Störungen analysieren	172
14.2	Störungen nach ITIL behandeln	174
14.3	Störungen protokollieren	176
14.4	ICT-Systeme überwachen	179
14.5	Wirksamkeit von Massnahmen überprüfen	181
15	Audits und Tests organisieren und durchführen	184
15.1	IT-Sicherheitsaudit	184
15.2	Technische Überprüfung	187
15.3	Ethical Hacking	192
15.4	IT-Sicherheitsaudit durchführen	194
15.5	Zweitmeinung einholen	195
15.6	Benchmarking durchführen	195
15.7	Kryptoanalyse	195
15.8	Risk Acceptance Process	197
15.9	Security Sign-off	199
16	Wirksamkeit und Wirtschaftlichkeit der Massnahmen kontrollieren	201
16.1	Reifegrad der ISMS-Prozesse überprüfen	201
16.2	Maturitätsmodelle	202
16.3	Effektivität und Effizienz	203
16.4	Konsistenz und Vollständigkeit	204
16.5	Kennzahlen	205
17	Prüf- und Messergebnisse auswerten und dokumentieren	207
17.1	Dokumentenkontrolle	207
17.2	Logfile-Zusammenführung	208
17.3	Ergebnisse konsolidieren	209
17.4	Interpretation und Meinungsbildung	210
17.5	Security Cockpit und Security MIS	210
17.6	Arbeitsplatz überwachen	213

Teil E	IT-Sicherheit verbessern	217
18	Optimierungsmöglichkeiten ermitteln	218
18.1	Beiträge zum Unternehmenserfolg	218
18.2	Managemententscheidung zur Optimierung	220
19	Verbesserungsmassnahmen planen und umsetzen, Sicherheitskultur fördern	222
19.1	Risikokommunikation	222
19.2	Sicherheit in der Softwareentwicklung	223
20	Strategie, Konzepte, Notfallpläne, ISMS und Massnahmen anpassen	227
20.1	Sicherheitsstrategie anpassen	227
20.2	Sicherheitskonzepte anpassen	228
20.3	Notfallpläne anpassen	229
20.4	Weitere Schwachstellen	231
21	Kontinuierliche Qualitätsverbesserung	233
21.1	Kontinuierlicher Verbesserungsprozess	233
21.2	Total Quality Management	238
Teil F	Anhang	241
	Lösungen zu den Aufgaben	242
	Weiterführende Literatur zum Thema	255
	Nützliche Links zum Thema	256
	Stichwortverzeichnis	259