

Inhaltsverzeichnis

	Vorwort	6
	Über dieses Lehrmittel	8
Teil A	Grundlagen der Informationssicherheit	11
	Einleitung, Lernziele und Schlüsselbegriffe	12
1	Gefährdungsbereiche	14
1.1	Höhere Gewalt	14
1.2	Organisatorische Mängel	16
1.3	Menschliche Fehlhandlungen	19
1.4	Technisches Versagen	22
1.5	Vorsätzliche Handlungen	26
	Repetitionsfragen	30
2	Informationssicherheitsmanagement	31
2.1	Leitbild und Sicherheitsziele	31
2.2	Sicherheitsziele und Risikoüberlegungen	31
2.3	Merkmale des IT-Sicherheitsmanagements	32
2.4	IT-Sicherheitsprozess	33
2.5	Strukturanalyse	35
2.6	Schutzbedarfsfeststellung	36
	Repetitionsfragen	37
3	Business Continuity Management	38
3.1	Gesetzliche Grundlagen und Standards	38
3.2	Krisenmanagement, Risikomanagement und BCM	38
3.3	Wichtige Begriffe	39
3.4	Vorgehen	40
3.5	Rechtliche Anforderungen	44
3.6	Standards und Frameworks	51
	Repetitionsfragen	63
Teil B	Sicherheitsrisiken aufdecken und beurteilen	65
	Einleitung, Lernziele und Schlüsselbegriffe	66
4	Sicherheitsrisiken identifizieren	68
4.1	IT-Sicherheit und Informationssicherheit	68
4.2	Risikoverständnis nach BSI-Grundschutz	69
4.3	Kleines Audit	74
4.4	KMU-Test nach InfoSurance	74
4.5	Automatisiertes Vulnerability Assessment	75
4.6	Prozessanalyse	76
	Repetitionsfragen	78
5	Folgen für die Informationssicherheit beurteilen	79
5.1	Folgen für die Vertraulichkeit, die Verfügbarkeit und die Integrität	79
5.2	Folgen für die Nicht-Abstreitbarkeit und die Verbindlichkeit	81
5.3	Folgen für die Geschäftsprozesse	81
5.4	Folgen für die Mitarbeitenden	92
	Repetitionsfragen	94
6	Folgen für den operativen ICT-Betrieb beurteilen	95
6.1	Service Level Agreements	95
6.2	Disaster Recovery Planning	96
6.3	Business Continuity Management	103
	Repetitionsfragen	108

Teil C	Sicherheitsanforderungen ermitteln	109
	Einleitung, Lernziele und Schlüsselbegriffe	110
7	Interne und externe Vorgaben	112
7.1	Betriebliche Richtlinien und Anweisungen	112
7.2	Arbeitsrechtliche Vorgaben	117
7.3	Datenschutzgesetz (DSG)	118
7.4	Regulatorische Vorgaben	119
	Repetitionsfragen	123
8	Sicherheitskritische Geschäftsprozesse identifizieren	124
8.1	Ziele und Voraussetzungen	124
8.2	Hauptprozesse identifizieren	125
8.3	Supportprozesse identifizieren	125
8.4	Führungsprozesse identifizieren	126
8.5	Praxisbeispiel	127
	Repetitionsfragen	129
9	Unterstützende Systeme und Komponenten identifizieren	130
9.1	Kritische Applikationen und IT-Infrastruktur	130
9.2	Kritische IT-Systeme	137
9.3	Abhängigkeiten und Zusammenhänge	139
9.4	Nationale Strategie zum Schutz vor Cyber-Risiken	143
	Repetitionsfragen	146
10	Daten- und Informationsflüsse analysieren	147
10.1	Grundbegriffe und Darstellungstechniken	147
10.2	Zugangs- und Zugriffsregelungen	148
10.3	Geschäftsprozessanalyse	151
10.4	Datenanalyse und -klassifikation	152
	Repetitionsfragen	154
Teil D	Technische und organisatorische Massnahmen definieren und überprüfen	155
	Einleitung, Lernziele und Schlüsselbegriffe	156
11	Massnahmen ermitteln und analysieren	158
11.1	Ebenen des Informationssicherheitsmanagements	158
11.2	Organisatorische Massnahmen	159
11.3	Physische und bauliche Massnahmen	164
11.4	Personenbezogene Massnahmen	168
11.5	Authentifizierung	169
11.6	Biometrie	174
	Repetitionsfragen	180
12	Technische und organisatorische Massnahmen	181
12.1	Standards und Frameworks	181
12.2	Kryptologie	184
12.3	Firewall	191
12.4	Kommunikationssicherheit	194
	Repetitionsfragen	198
13	Personenbezogene Massnahmen und Sicherheitskonzept	199
13.1	Awareness und Sensibilisierung	199
13.2	Sicherheitskonzept	201
	Repetitionsfragen	204
14	Massnahmen zur Sicherstellung des operativen ICT-Betriebs	205
14.1	ITIL	205
14.2	Informationssicherheit als zyklischer Prozess	209
14.3	Computer Emergency Response Team	210
	Repetitionsfragen	215

15	Wirksamkeit der Massnahmen prüfen und dokumentieren	216
15.1	Auditarten	216
15.2	Penetration Tests	216
15.3	Zertifizierungen	219
15.4	Penetration Tests durchführen	219
15.5	Prozesse auditieren	220
15.6	Auditbericht erstellen	222
	Repetitionsfragen	223
Teil E	Anhang	225
	Antworten zu den Repetitionsfragen	226
	Stichwortverzeichnis	242