Inhaltsverzeichnis

	Vorwort	**5**
	Über dieses Lehrmittel	**7**
Teil A	**Grundlagen**	**9**
1	**Begriffe und Normen**	**11**
1.1	Sicherheitspolitik	11
1.2	Vision und Sicherheitsziele	13
1.3	Schichten der Systemsicherheit	15
1.4	IT-Sicherheit und Informationssicherheit	17
1.5	Rechtliche Aspekte	17
1.6	Verantwortung des Managements	22
	Repetitionsfragen	**24**
2	**Gefahren und Risiken**	**25**
2.1	Angriffsflächen und Sicherheitslücken	25
2.2	Mängel und Fehler bei der Konfiguration	26
2.3	Mängel und Fehler bei der Software	27
	Repetitionsfragen	**29**
3	**Standards und Best Practices**	**30**
3.1	Allgemeine Anforderungen	30
3.2	Überblick über Sicherheitsstandards	31
3.3	Normenreihe ISO 27000	32
3.4	Vorgehen nach BSI 100-2	33
3.5	Kontrollen und Audits	36
	Repetitionsfragen	**38**
4	**Tools und Hilfsmittel**	**39**
4.1	Vulnerability- und Analysetools	39
4.2	Spezialisierte Webseiten und Newsletter	46
4.3	Checklisten	48
4.4	Systemdokumentation und Softwareinventar	49
4.5	Lizenzmanagement	50
	Repetitionsfragen	**53**
Teil B	**Systemsicherheit analysieren und entwerfen**	**55**
5	**Sicherheitssituation und -risiken analysieren**	**57**
5.1	Risikoanalyse	57
5.2	Informationen und Prozesse klassifizieren	59
5.3	Sicherheitseinstellungen überprüfen	61
5.4	Sicherheitslücken und -risiken analysieren	62
	Repetitionsfragen	**63**
6	**Sicherheitsvorgaben und -anforderungen analysieren**	**64**
6.1	Externe Sicherheitsvorgaben berücksichtigen	64
6.2	Interne Sicherheitsanforderungen berücksichtigen	64
6.3	System-Anomalien erkennen und berücksichtigen	70
	Repetitionsfragen	**72**
7	**Geeignete Massnahmen ableiten**	**73**
7.1	Was ist ein Sicherheitsvorfall und wie wird er behandelt?	73
7.2	Notfälle behandeln	74
7.3	Sofortmassnahmen definieren	77
	Repetitionsfragen	**79**

8	**Kosten und Nutzen von Sicherheitsmassnahmen ermitteln**	**80**
8.1	Einzelschäden abschätzen	80
8.2	Einzelrisiken abschätzen	81
8.3	Möglichen Gesamtschaden berechnen	81
8.4	Investitionen in Sicherheitsmassnahmen	81
	Repetitionsfragen	**82**
Teil C	**Systemsicherheit planen und umsetzen**	**83**
9	**Grundschutz, Datenschutz und Systembetrieb sicherstellen**	**85**
9.1	Grundschutz gewährleisten	85
9.2	Datenschutz gewährleisten	89
9.3	Systembetrieb gewährleisten	91
	Repetitionsfragen	**91**
10	**Organisatorische Massnahmen vorbereiten und implementieren**	**92**
10.1	Awareness	92
10.2	Systemüberwachung	92
10.3	Regelmässiger Prozess zur Aktualisierung	97
10.4	Forensische Analysen	97
	Repetitionsfragen	**98**
11	**Technische Massnahmen vorbereiten und implementieren**	**99**
11.1	System aktualisieren	99
11.2	System härten	103
11.3	Minimale Rechte	104
11.4	Intrusion Detection	106
	Repetitionsfragen	**111**
12	**Sicherheitsprüfungen vorbereiten und implementieren**	**112**
12.1	Testbestandteile	112
12.2	Physikalische Kontrollen planen und umsetzen	113
12.3	Technische Kontrollen planen und umsetzen	113
12.4	Administrative Kontrollen planen und umsetzen	114
	Repetitionsfragen	**115**
Teil D	**Anhang**	**117**
	Standards zur Systemsicherheit	**118**
	Gesamtzusammenfassung	**123**
	Antworten zu den Repetitionsfragen	**127**
	Glossar	**133**
	Stichwortverzeichnis	**139**