

# Inhaltsverzeichnis

<b>1</b>	<b>Einführung und Basiswissen .....</b>	<b>1</b>
1.1	Worum geht es in ISO/IEC 27001? .....	1
1.2	Begriffsbildung .....	2
1.2.1	Informationen .....	2
1.2.2	Informationssicherheit .....	2
1.2.3	Schutzziele: Aspekte der Informationssicherheit .....	3
1.2.3.1	Vertraulichkeit (Confidentiality) .....	3
1.2.3.2	Integrität (Integrity) .....	3
1.2.3.3	Verfügbarkeit (Availability) .....	4
1.2.3.4	Authentizität (Authenticity) und Authentisierung (Authenticat- tion) .....	4
1.2.3.5	Zurechenbarkeit (Accountability) .....	5
1.2.3.6	Nicht-Abstreitbarkeit/Verbindlichkeit (Non-repudiation) .....	5
1.2.3.7	Verlässlichkeit (Reliability).....	5
1.2.3.8	Zugriffskontrolle (Access Control) .....	5
1.3	Überblick über die folgenden Kapitel .....	5
<b>2</b>	<b>Die Normenreihe ISO/IEC 27000 im Überblick .....</b>	<b>7</b>
2.1	Warum Standardisierung? .....	7
2.2	Grundlagen der ISO/IEC 27000 .....	8
2.3	Normative vs. informative Standards .....	8
2.4	Die Standards der ISMS-Familie und ihre Zusammenhänge .....	9
2.4.1	Allgemeine und normative Anforderungen .....	9
2.4.1.1	ISO/IEC 27001: Anforderungen an ein ISMS .....	9
2.4.1.2	ISO/IEC 27006: Anforderungen an Zertifizierer .....	10
2.4.2	Allgemeine und informative Leitfäden .....	10
2.4.2.1	ISO/IEC 27002: Leitfaden für das Informationssicherheits- Management .....	11
2.4.2.2	ISO/IEC 27003: Umsetzungsempfehlungen.....	11
2.4.2.3	ISO/IEC 27004: Messungen.....	11

2.4.2.4	ISO/IEC 27005: Risikomanagement .....	11
2.4.2.5	ISO/IEC 27007 und ISO/IEC 27008: Audit-Leitfäden .....	11
2.4.3	Branchenspezifische Leitfäden .....	12
2.4.3.1	ISO/IEC 27011: Leitfaden für die Telekommunikationsbranche ..	12
2.4.3.2	ISO 27799: Leitfaden für Organisationen im Gesundheitswesen.	12
2.5	Zusammenfassung .....	13
2.6	Beispiele für Prüfungsfragen zu diesem Kapitel .....	13

### **3 Grundlagen von Informationssicherheits-Managementsystemen**

<b>(ISMS)</b> .....	<b>15</b>
3.1 Das ISMS und seine Bestandteile .....	15
3.1.1 (Informations-)Werte .....	16
3.1.2 Leitlinien, Prozesse und Verfahren .....	16
3.1.3 Dokumente und Aufzeichnungen .....	17
3.1.4 Zuweisung von Verantwortlichkeiten .....	18
3.1.5 Maßnahmenziele und Maßnahmen .....	19
3.2 Was bedeutet Prozessorientierung? .....	20
3.3 Die PDCA-Methodik: Plan-Do-Check-Act .....	21
3.3.1 Planung (Plan) .....	22
3.3.2 Umsetzung (Do) .....	22
3.3.3 Überprüfung (Check) .....	23
3.3.3.1 Konformität .....	23
3.3.3.2 Effektivität .....	23
3.3.3.3 Effizienz .....	23
3.3.4 Verbesserung (Act) .....	24
3.4 Zusammenfassung .....	24
3.5 Beispiele für Prüfungsfragen zu diesem Kapitel .....	25

### **4 ISO/IEC 27001 – Spezifikationen und Mindestanforderungen .... 27**

4.1 Anwendungsbereich .....	29
4.2 Normative Verweisungen .....	30
4.3 Begriffe .....	31
4.4 Informationssicherheits-Managementsystem .....	34
4.4.1 Allgemeine Anforderungen .....	34
4.4.2 Festlegung und Verwaltung des ISMS .....	35
4.4.2.1 Festlegen des ISMS .....	35
4.4.2.2 Umsetzen und Durchführen des ISMS .....	43
4.4.2.3 Überwachen und Überprüfen des ISMS .....	44
4.4.2.4 Instandhalten und Verbessern des ISMS .....	46
4.4.3 Dokumentationsanforderungen .....	46
4.4.3.1 Allgemeines .....	47
4.4.3.2 Lenkung von Dokumenten .....	48

4.4.3.3	Lenkung von Aufzeichnungen .....	49
4.5	Verantwortung des Managements .....	49
4.6	Interne ISMS-Audits .....	51
4.7	Managementbewertung des ISMS .....	53
4.8	Verbesserung des ISMS .....	55
4.9	Zusammenfassung .....	57
4.10	Beispiele für Prüfungsfragen zu diesem Kapitel .....	58
<b>5</b>	<b>Maßnahmenziele und Maßnahmen im Rahmen des ISMS .....</b>	<b>63</b>
5.A.5	Sicherheitsleitlinie (A.5) .....	64
5.A.6	Organisation der Informationssicherheit (A.6) .....	66
5.A.6.1	Interne Organisation (A.6.1) .....	66
5.A.6.2	Externe Beziehungen (A.6.2) .....	69
5.A.7	Management von organisationseigenen Werten (A.7) .....	70
5.A.7.1	Verantwortung für organisationseigene Werte (Assets) (A.7.1) .....	71
5.A.7.2	Klassifizierung von Informationen (A.7.2) .....	72
5.A.8	Personelle Sicherheit (A.8) .....	74
5.A.8.1	Vor der Anstellung (A.8.1) .....	74
5.A.8.2	Während der Anstellung (A.8.2) .....	75
5.A.8.3	Beendigung oder Änderung der Anstellung (A.8.3) .....	76
5.A.9	Physische und umgebungsbezogene Sicherheit (A.9) .....	78
5.A.9.1	Sicherheitsbereiche (A.9.1) .....	78
5.A.9.2	Sicherheit von Betriebsmitteln (A.9.2) .....	80
5.A.10	Betriebs- und Kommunikationsmanagement (A.10) .....	83
5.A.10.1	Verfahren und Verantwortlichkeiten (A.10.1) .....	84
5.A.10.2	Management der Dienstleistungserbringung von Dritten (A.10.2) .....	85
5.A.10.3	Systemplanung und Abnahme (A.10.3) .....	86
5.A.10.4	Schutz vor Schadsoftware und mobilem Programmcode (A.10.4) .....	87
5.A.10.5	Backup (A.10.5) .....	88
5.A.10.6	Management der Netzsicherheit (A.10.6) .....	89
5.A.10.7	Handhabung von Speicher- und Aufzeichnungsmedien (A.10.7) .....	90
5.A.10.8	Austausch von Informationen (A.10.8) .....	92
5.A.10.9	E-Commerce-Anwendungen (A.10.9) .....	94
5.A.10.10	Überwachung (A.10.10) .....	95
5.A.11	Zugangskontrolle (A.11) .....	98
5.A.11.1	Geschäftsanforderungen für Zugangskontrolle (A.11.1) .....	98
5.A.11.2	Benutzerverwaltung (A.11.2) .....	99
5.A.11.3	Benutzerverantwortung (A.11.3) .....	100
5.A.11.4	Zugangskontrolle für Netze (A.11.4) .....	102
5.A.11.5	Zugriffskontrolle auf Betriebssysteme (A.11.5) .....	104
5.A.11.6	Zugangskontrolle zu Anwendungen und Information (A.11.6) .....	106
5.A.11.7	Mobile Computing und Telearbeit (A.11.7) .....	107

5.A.12 Beschaffung, Entwicklung und Wartung von Informationssystemen (A.12) .....	109
5.A.12.1 Sicherheitsanforderungen von Informationssystemen (A.12.1) .....	109
5.A.12.2 Korrekte Verarbeitung in Anwendungen (A.12.2) .....	110
5.A.12.3 Kryptographische Maßnahmen (A.12.3) .....	112
5.A.12.4 Sicherheit von Systemdateien (A.12.4) .....	113
5.A.12.5 Sicherheit bei Entwicklungs- und Unterstützungsprozessen (A.12.5) ....	114
5.A.12.6 Schwachstellenmanagement (A.12.6) .....	116
5.A.13 Umgang mit Informationssicherheitsvorfällen (A.13) .....	117
5.A.13.1 Melden von Informationssicherheitsereignissen und Schwachstellen (A.13.1) .....	117
5.A.13.2 Umgang mit Informationssicherheitsvorfällen und Verbesserungen (A.13.2) .....	118
5.A.14 Sicherstellung des Geschäftsbetriebs (Business Continuity Management) (A.14) ..	120
5.A.15 Einhaltung von Vorgaben (A.15) .....	123
5.A.15.1 Einhaltung gesetzlicher Vorgaben (A.15.1) .....	123
5.A.15.2 Einhaltung von Sicherheitsregelungen und -standards und technischer Vorgaben (A.15.2) .....	125
5.A.15.3 Überlegungen zu Revisionsprüfungen von Informationssystemen (A.15.3) .....	126
5.16 Zusammenfassung .....	128
5.17 Beispiele für Prüfungsfragen zu diesem Kapitel .....	128
 <b>6 Verwandte Standards und Rahmenwerke .....</b>	<b>133</b>
6.1 ISO 9000 (Qualitätsmanagement) .....	133
6.1.1 Zielsetzung und Anwendungsbereich .....	133
6.1.2 Aufbau und Inhalt .....	134
6.1.3 Bezug zu ISO/IEC 27000 .....	135
6.2 ISO/IEC 20000 (IT Service Management) .....	135
6.2.1 Zielsetzung und Anwendungsbereich .....	135
6.2.2 Aufbau und Inhalt .....	136
6.2.3 Bezug zu ISO/IEC 27000 .....	136
6.3 ISO/IEC 15408 (Bewertung der Informationssicherheit) .....	137
6.3.1 Zielsetzung und Anwendungsbereich .....	137
6.3.2 Aufbau und Inhalt .....	138
6.3.3 Bezug zu ISO/IEC 27000 .....	139
6.4 Das COBIT-Framework (IT-Governance) .....	139
6.4.1 Zielsetzung und Anwendungsbereich .....	139
6.4.2 Aufbau und Inhalt .....	140
6.4.3 Bezug zu ISO/IEC 27000 .....	141
6.5 Das COSO ERM-Framework (Risikomanagement) .....	141
6.5.1 Zielsetzung und Anwendungsbereich .....	141
6.5.2 Aufbau und Inhalt .....	142

6.5.3	Bezug zu ISO/IEC 27000 .....	144
6.6	Die BSI-Grundschatzkataloge (IT-Grundschatz).....	144
6.6.1	Zielsetzung und Anwendungsbereich .....	144
6.6.2	Aufbau und Inhalt .....	144
6.6.3	Bezug zu ISO/IEC 27000 .....	145
6.7	Zusammenfassung .....	146
6.8	Beispiele für Prüfungsfragen zu diesem Kapitel .....	146
<b>7</b>	<b>Zertifizierungsmöglichkeiten nach ISO/IEC 27000 .....</b>	<b>149</b>
7.1	ISMS-Zertifizierung nach ISO/IEC 27001 .....	149
7.1.1	Grundlagen der Zertifizierung von Managementsystemen .....	149
7.1.1.1	Zertifizierung .....	149
7.1.1.2	Akkreditierung.....	150
7.1.2	Typischer Ablauf einer Zertifizierung.....	151
7.1.3	Auditumfang .....	153
7.1.4	Akzeptanz und Gültigkeit des Zertifikats.....	153
7.2	Personenqualifizierung auf Basis von ISO/IEC 27000 .....	153
7.2.1	Das Programm des TÜV Süd .....	154
7.2.2	Das Foundation-Zertifikat.....	154
7.2.2.1	Prüfungsspezifikation .....	154
7.2.2.2	Vorbereitung auf die Zertifizierungsprüfung.....	155
7.3	Zusammenfassung .....	156
7.4	Beispiele für Prüfungsfragen zu diesem Kapitel .....	157
<b>A</b>	<b>Prüfungsfragen mit Antworten zur ISO/IEC 27001 Foundation ..</b>	<b>159</b>
A.1	Antworten auf die Prüfungsfragen zu den einzelnen Buchkapiteln .....	159
A.2	Ein beispielhafter Prüfungsfragebogen zur ISO/IEC 27001-Foundation-Prüfung..	166
	<b>Literaturverzeichnis.....</b>	<b>185</b>
	<b>Index.....</b>	<b>189</b>