

<b>Vorwort .....</b>	<b>XIII</b>
<b>1 Einführung und Basiswissen .....</b>	<b>1</b>
1.1 Worum geht es in ISO/IEC 27000 und ISO/IEC 27001? .....	2
1.2 Begriffsbildung .....	3
1.2.1 Informationen .....	3
1.2.2 Informationssicherheit .....	3
1.2.3 Sicherheitsanforderungen und Schutzziele .....	3
1.3 IT-Sicherheitsgesetz & KRITIS .....	7
1.3.1 Was ist „KRITIS“? .....	8
1.3.2 Wer ist in Deutschland von KRITIS betroffen? .....	8
1.3.3 KRITIS-Anforderungen – Informationssicherheit nach dem „Stand der Technik“ .....	9
1.4 Datenschutz-Grundverordnung .....	10
1.5 Weitere Richtlinien und Verordnungen der Europäischen Union .....	11
1.5.1 NIS-2-Richtlinie .....	11
1.5.2 Richtlinie über die Resilienz kritischer Einrichtungen (EU RCE Directive/CER-Richtlinie) .....	12
1.5.3 Cyber Resilience Act (CRA) .....	12
1.5.4 DORA-Verordnung .....	13
1.6 Überblick über die folgenden Kapitel.....	13
1.7 Beispiele für Prüfungsfragen zu diesem Kapitel .....	13
<b>2 Die Standardfamilie ISO/IEC 27000 im Überblick .....</b>	<b>15</b>
2.1 Warum Standardisierung? .....	15
2.2 Grundlagen der ISO/IEC 27000 .....	16
2.3 Normative vs. informative Standards .....	16
2.4 Die Standards der ISMS-Familie und ihre Zusammenhänge .....	17
2.4.1 ISO/IEC 27000: Grundlagen und Überblick über die Standardfamilie ..	18
2.4.2 Normative Anforderungen .....	18

2.4.3	Allgemeine Leitfäden .....	20
2.4.4	Sektor- und maßnahmenspezifische Leitfäden .....	22
2.5	Zusammenfassung .....	24
2.6	Beispiele für Prüfungsfragen zu diesem Kapitel .....	24
<b>3</b>	<b>Grundlagen von Informationssicherheitsmanagementsystemen ..</b>	<b>27</b>
3.1	Das ISMS und seine Bestandteile .....	27
3.1.1	(Informations-)Werte .....	28
3.1.2	Richtlinien, Prozesse und Verfahren .....	28
3.1.3	Dokumente und Aufzeichnungen .....	29
3.1.4	Zuweisung von Verantwortlichkeiten .....	30
3.1.5	Maßnahmen .....	31
3.2	Was bedeutet Prozessorientierung? .....	33
3.3	Die PDCA-Methodik: Plan-Do-Check-Act .....	34
3.3.1	Planung (Plan) .....	35
3.3.2	Umsetzung (Do) .....	35
3.3.3	Überprüfung (Check) .....	36
3.3.4	Verbesserung (Act) .....	37
3.4	Zusammenfassung .....	37
3.5	Beispiele für Prüfungsfragen zu diesem Kapitel .....	37
<b>4</b>	<b>DIN EN ISO/IEC 27001 – Spezifikationen und Mindestanforderungen ..</b>	<b>39</b>
4.0	Einleitung .....	41
4.0.1	Allgemeines .....	41
4.0.2	Kompatibilität mit anderen Normen für Managementsysteme .....	42
4.1	Anwendungsbereich .....	43
4.2	Normative Verweisungen .....	43
4.3	Begriffe .....	44
4.4	Kontext der Organisation .....	44
4.4.1	Verstehen der Organisation und ihres Kontextes .....	45
4.4.2	Verstehen der Erfordernisse und Erwartungen interessierter Parteien ..	45
4.4.3	Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems .....	46
4.4.4	Informationssicherheitsmanagementsystem .....	48
4.5	Führung .....	48
4.5.1	Führung und Verpflichtung .....	48
4.5.2	Politik .....	50
4.5.3	Rollen, Verantwortlichkeiten und Befugnisse in der Organisation ..	51
4.6	Planung .....	52
4.6.1	Maßnahmen zum Umgang mit Risiken und Chancen .....	52
4.6.2	Informationssicherheitsziele und Planung zu deren Erreichung .....	58
4.6.3	Planung von Änderungen .....	59

<b>4.7</b>	<b>Unterstützung .....</b>	<b>60</b>
4.7.1	Ressourcen .....	60
4.7.2	Kompetenz .....	61
4.7.3	Bewusstsein .....	61
4.7.4	Kommunikation .....	62
4.7.5	Dokumentierte Information .....	63
<b>4.8</b>	<b>Betrieb .....</b>	<b>65</b>
4.8.1	Betriebliche Planung und Steuerung .....	65
4.8.2	Informationssicherheitsrisikobeurteilung .....	66
4.8.3	Informationssicherheitsrisikobehandlung .....	67
<b>4.9</b>	<b>Bewertung der Leistung .....</b>	<b>67</b>
4.9.1	Überwachung, Messung, Analyse und Bewertung .....	67
4.9.2	Internes Audit .....	70
4.9.3	Managementbewertung .....	73
<b>4.10</b>	<b>Verbesserung .....</b>	<b>74</b>
4.10.1	Fortlaufende Verbesserung .....	75
4.10.2	Nichtkonformität und Korrekturmaßnahmen .....	75
<b>4.11</b>	<b>Zusammenfassung .....</b>	<b>76</b>
<b>4.12</b>	<b>Beispiele für Prüfungsfragen zu diesem Kapitel .....</b>	<b>77</b>
<b>5</b>	<b>Maßnahmen im Rahmen des ISMS .....</b>	<b>81</b>
<b>5.1</b>	<b>A.5 Organisatorisches Maßnahmen .....</b>	<b>82</b>
5.1.1	[A.5.1] Informationssicherheitspolitik und -richtlinien .....	82
5.1.2	[A.5.2] Informationssicherheitsrollen und -verantwortlichkeiten .....	84
5.1.3	[A.5.3] Aufgabentrennung .....	85
5.1.4	[A.5.4] Verantwortlichkeiten der Leitung .....	85
5.1.5	[A.5.5] Kontakt mit Behörden .....	86
5.1.6	[A.5.6] Kontakt mit speziellen Interessensgruppen .....	86
5.1.7	[A.5.7] Informationen über die Bedrohungslage .....	87
5.1.8	[A.5.8] Informationssicherheit im Projektmanagement .....	87
5.1.9	[A.5.9] Inventar der Informationen und anderen damit verbundenen Werten .....	88
5.1.10	[A.5.10] Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten .....	88
5.1.11	[A.5.11] Rückgabe von Werten .....	89
5.1.12	[A.5.12] Klassifizierung von Informationen .....	89
5.1.13	[A.5.13] Kennzeichnung von Informationen .....	90
5.1.14	[A.5.14] Informationsübermittlung .....	91
5.1.15	[A.5.15] Zugangssteuerung .....	92
5.1.16	[A.5.16] Identitätsmanagement .....	92
5.1.17	[A.5.17] Authentisierungsinformationen .....	93

5.1.18	[A.5.18] Zugangsrechte .....	94
5.1.19	[A.5.19] Informationssicherheit in Lieferantenbeziehungen .....	95
5.1.20	[A.5.20] Behandlung von Informationssicherheit in Lieferantenvereinbarungen.....	95
5.1.21	[A.5.21] Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie (IKT) .....	96
5.1.22	[A.5.22] Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen .....	97
5.1.23	[A.5.23] Informationssicherheit für die Nutzung von Cloud-Diensten ..	97
5.1.24	[A.5.24] Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen .....	98
5.1.25	[A.5.25] Beurteilung und Entscheidung über Informationssicherheitereignisse .....	99
5.1.26	[A.5.26] Reaktion auf Informationssicherheitsvorfälle .....	101
5.1.27	[A.5.27] Erkenntnisse aus Informationssicherheitsvorfällen .....	102
5.1.28	[A.5.28] Sammeln von Beweismaterial .....	102
5.1.29	[A.5.29] Informationssicherheit bei Störungen.....	103
5.1.30	[A.5.30] IKT-Bereitschaft für Business-Continuity .....	103
5.1.31	[A.5.31] Juristische, gesetzliche, regulatorische und vertragliche Anforderungen.....	104
5.1.32	[A.5.32] Geistige Eigentumsrechte.....	105
5.1.33	[A.5.33] Schutz von Aufzeichnungen .....	105
5.1.34	[A.5.34] Datenschutz und Schutz von personenbezogenen Daten (PbD) .....	106
5.1.35	[A.5.35] Unabhängige Überprüfung der Informationssicherheit.....	106
5.1.36	[A.5.36] Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit .....	107
5.1.37	[A.5.37] Dokumentierte Betriebsabläufe .....	107
5.2	A.6 Personenbezogene Maßnahmen .....	108
5.2.1	[A.6.1] Sicherheitsüberprüfung .....	108
5.2.2	[A.6.2] Beschäftigungs- und Vertragsbedingungen .....	109
5.2.3	[A.6.3] Informationssicherheitsbewusstsein, -ausbildung und -schulung .....	110
5.2.4	[A.6.4] Maßregelungsprozess .....	111
5.2.5	[A.6.5] Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung .....	111
5.2.6	[A.6.6] Vertraulichkeits- oder Geheimhaltungsvereinbarungen .....	112
5.2.7	[A.6.7] Remote-Arbeit .....	113
5.2.8	[A.6.8] Meldung von Informationssicherheitereignissen .....	114
5.3	A.7 Physische Maßnahmen .....	115
5.3.1	[A.7.1] Physische Sicherheitsperimeter .....	115
5.3.2	[A.7.2] Physischer Zutritt .....	117
5.3.3	[A.7.3] Sichern von Büros, Räumen und Einrichtungen .....	118

5.3.4	[A.7.4] Physische Sicherheitsüberwachung .....	118
5.3.5	[A.7.5] Schutz vor physischen und umweltbedingten Bedrohungen ....	119
5.3.6	[A.7.6] Arbeiten in Sicherheitsbereichen.....	120
5.3.7	[A.7.7] Aufgeräumte Arbeitsumgebung und Bildschirmsperren .....	121
5.3.8	[A.7.8] Platzierung und Schutz von Geräten und Betriebsmitteln .....	121
5.3.9	[A.7.9] Sicherheit von Assets außerhalb der Standorte der Organisation	122
5.3.10	[A.7.10] Speichermedien.....	123
5.3.11	[A.7.11] Versorgungseinrichtungen .....	124
5.3.12	[A.7.12] Sicherheit der Verkabelung.....	124
5.3.13	[A.7.13] Instandhaltung von Geräten und Betriebsmitteln .....	125
5.3.14	[A.7.14] Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln .....	126
5.4	A.8 Technologische Maßnahmen .....	126
5.4.1	[A.8.1] Endpunktgeräte des Benutzers .....	126
5.4.2	[A.8.2] Privilegierte Zugangsrechte .....	127
5.4.3	[A.8.3] Informationszugangsbeschränkung.....	128
5.4.4	[A.8.4] Zugriff auf den Quellcode .....	128
5.4.5	[A.8.5] Sichere Authentisierung .....	129
5.4.6	[A.8.6] Kapazitätssteuerung.....	130
5.4.7	[A.8.7] Schutz gegen Schadsoftware .....	130
5.4.8	[A.8.8] Handhabung von technischen Schwachstellen .....	131
5.4.9	[A.8.9] Konfigurationsmanagement.....	132
5.4.10	[A.8.10] Löschung von Informationen .....	132
5.4.11	[A.8.11] Datenmaskierung.....	133
5.4.12	[A.8.12] Verhinderung von Datenlecks .....	133
5.4.13	[A.8.13] Sicherung von Informationen .....	134
5.4.14	[A.8.14] Redundanz von informationsverarbeitenden Einrichtungen ..	135
5.4.15	[A.8.15] Protokollierung .....	135
5.4.16	[A.8.16] Überwachung von Aktivitäten .....	137
5.4.17	[A.8.17] Uhrensynchronisation .....	138
5.4.18	[A.8.18] Gebrauch von Hilfsprogrammen mit privilegierten Rechten....	138
5.4.19	[A.8.19] Installation von Software auf Systemen im Betrieb .....	139
5.4.20	[A.8.20] Netzwerksicherheit.....	140
5.4.21	[A.8.21] Sicherheit von Netzwerkdiensten .....	140
5.4.22	[A.8.22] Trennung von Netzwerken .....	141
5.4.23	[A.8.23] Webfilterung .....	142
5.4.24	[A.8.24] Verwendung von Kryptographie .....	142
5.4.25	[A.8.25] Lebenszyklus einer sicheren Entwicklung .....	144
5.4.26	[A.8.26] Anforderungen an die Anwendungssicherheit.....	144
5.4.27	[A.8.27] Sichere Systemarchitektur und Entwicklungsgrundsätze .....	145

5.4.28	[A.8.28] Sichere Codierung .....	146
5.4.29	[A.8.29] Sicherheitsprüfung bei Entwicklung und Abnahme .....	146
5.4.30	[A.8.30] Ausgegliederte Entwicklung .....	147
5.4.31	[A.8.31] Trennung von Entwicklungs-, Test- und Produktivumgebungen	147
5.4.32	[A.8.32] Änderungssteuerung.....	148
5.4.33	[A.8.33] Testdaten .....	148
5.4.34	[A.8.34] Schutz der Informationssysteme während Tests im Rahmen von Audits.....	149
5.5	Beispiele für Prüfungsfragen zu diesem Kapitel .....	150
<b>6</b>	<b>Verwandte Standards und Rahmenwerke .....</b>	<b>153</b>
6.1	Standards und Rahmenwerke für IT- und Informationssicherheit.....	153
6.1.1	IT-Grundschutz-Kompendium .....	153
6.1.2	BSI-Standards .....	154
6.1.3	CISIS12 .....	155
6.1.4	Cybersecurity Framework .....	156
6.1.5	ISO/IEC 15408 .....	157
6.1.6	VDA ISA (TISAX) .....	157
6.2	Standards und Rahmenwerke für Qualitätsmanagement, Auditierung und Zertifizierung .....	159
6.2.1	ISO 9000 .....	159
6.2.2	ISO 19011 .....	159
6.2.3	ISO/IEC 17020 .....	161
6.3	Standards und Rahmenwerke für Governance und Management in der IT .....	162
6.3.1	ITIL .....	162
6.3.2	ISO/IEC 20000 .....	162
6.3.3	FitSM .....	164
6.4	Beispiele für Prüfungsfragen zu diesem Kapitel .....	165
<b>7</b>	<b>Zertifizierungsmöglichkeiten nach ISO/IEC 27000 .....</b>	<b>167</b>
7.1	ISMS-Zertifizierung nach ISO/IEC 27001 .....	167
7.1.1	Grundlagen der Zertifizierung von Managementsystemen .....	167
7.1.2	Typischer Ablauf einer Zertifizierung.....	169
7.1.3	Auditumfang .....	171
7.1.4	Akzeptanz und Gültigkeit des Zertifikats .....	171
7.1.5	Aufwände und Kosten für Zertifizierungen .....	171
7.2	Personenqualifizierung auf Basis von ISO/IEC 27000.....	172
7.2.1	Programme zur Ausbildung und Zertifizierung von Personal.....	172
7.2.2	Erlangen eines Foundation-Zertifikats .....	175
7.3	Zusammenfassung .....	177
7.4	Beispiele für Prüfungsfragen zu diesem Kapitel .....	177

<b>A</b>	<b>Begriffsbildung nach ISO/IEC 27000 .....</b>	<b>179</b>
<b>B</b>	<b>Abdruck der DIN EN ISO/IEC 27001:2024 .....</b>	<b>197</b>
B.1	DIN EN ISO/IEC 27001:2024 .....	199
B.2	DIN EN ISO/IEC 27001:2024, Anhang A .....	220
B.3	Vergleich: DIN EN ISO/IEC 27001 Anhang A :2024 vs. :2017 .....	231
<b>C</b>	<b>Prüfungsfragen mit Antworten zur ISO/IEC 27001 Foundation .....</b>	<b>235</b>
C.1	Antworten auf die Prüfungsfragen zu den einzelnen Buchkapiteln .....	235
C.2	Ein beispielhafter Prüfungsfragebogen zur ISO/IEC 27001-Foundation-Prüfung	242
C.3	Antworten auf den Prüfungsfragebogen zur ISO/IEC 27001-Foundation-Prüfung .....	252
	<b>Literaturverzeichnis .....</b>	<b>259</b>
	<b>Index .....</b>	<b>266</b>