Inhaltsverzeichnis

Vorwort ..... **XI**

1 Einführung und Basiswissen **1**
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 Sicherheitsanforderungen und Schutzziele 3
1.3 IT-Sicherheitsgesetz & KRITIS 6
1.3.1 Was ist „KRITIS“? 7
1.3.2 Wer ist in Deutschland von KRITIS betroffen? 7
1.3.3 KRITIS-Anforderungen – Informationssicherheit nach dem „Stand der Technik“ 8
1.4 Datenschutz-Grundverordnung 9
1.5 Überblick über die folgenden Kapitel 10
1.6 Beispiele für Prüfungsfragen zu diesem Kapitel 10

2 Die Standardfamilie ISO/IEC 27000 im Überblick **13**
2.1 Warum Standardisierung? 13
2.2 Grundlagen der ISO/IEC 27000 14
2.3 Normative vs. informative Standards 14
2.4 Die Standards der ISMS-Familie und ihre Zusammenhänge 15
2.4.1 ISO/IEC 27000: Grundlagen und Überblick über die Standardfamilie 16
2.4.2 Normative Anforderungen 16
2.4.3 Allgemeine Leitfäden 17
2.4.4 Sektor- und maßnahmenspezifische Leitfäden 19
2.5 Zusammenfassung 21
2.6 Beispiele für Prüfungsfragen zu diesem Kapitel 21

3 Grundlagen von Informationssicherheitsmanagementsystemen **23**
3.1 Das ISMS und seine Bestandteile 23

Bibliografische Informationen
https://d-nb.info/1257251317

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

3.1.1 (Informations-)Werte ... 24
3.1.2 Richtlinien, Prozesse und Verfahren ... 24
3.1.3 Dokumente und Aufzeichnungen ... 25
3.1.4 Zuweisung von Verantwortlichkeiten ... 26
3.1.5 Maßnahmen ... 27
3.2 Was bedeutet Prozessorientierung? ... 28
3.3 Die PDCA-Methodik: Plan-Do-Check-Act ... 29
3.3.1 Planung (Plan) ... 30
3.3.2 Umsetzung (Do) ... 31
3.3.3 Überprüfung (Check) ... 31
3.3.4 Verbesserung (Act) ... 32
3.4 Zusammenfassung ... 32
3.5 Beispiele für Prüfungsfragen zu diesem Kapitel ... 33

4 ISO/IEC 27001 – Spezifikationen und Mindestanforderungen ... 35
4.0 Einleitung ... 37
4.0.1 Allgemeines ... 37
4.0.2 Kompatibilität mit anderen Normen für Managementsysteme ... 38
4.1 Anwendungsbereich ... 38
4.2 Normative Verweisungen ... 39
4.3 Begriffe ... 39
4.4 Kontext der Organisation ... 40
4.4.1 Verstehen der Organisation und ihres Kontextes ... 40
4.4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien ... 41
4.4.3 Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems ... 42
4.4.4 Informationssicherheitsmanagementsystem ... 43
4.5 Führung ... 43
4.5.1 Führung und Verpflichtung ... 43
4.5.2 Politik ... 44
4.5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation ... 45
4.6 Planung ... 46
4.6.1 Maßnahmen zum Umgang mit Risiken und Chancen ... 47
4.6.2 Informationssicherheitsziele und Planung zu deren Erreichung ... 53
4.7 Unterstützung ... 54
4.7.1 Ressourcen ... 54
4.7.2 Kompetenz ... 54
4.7.3 Bewusstsein ... 55
4.7.4 Kommunikation ... 55
4.7.5 Dokumentierte Information ... 56
4.8 Betrieb ... 58
4.8.1 Betriebliche Planung und Steuerung ... 58
4.8.2 Informationssicherheitsrisikobeurteilung ... 59

4.8.3 Informationssicherheitsrisikobehandlung ... 60
4.9 Bewertung der Leistung ... 60
4.9.1 Überwachung, Messung, Analyse und Bewertung ... 60
4.9.2 Internes Audit ... 63
4.9.3 Managementbewertung ... 65
4.10 Verbesserung ... 66
4.10.1 Nichtkonformität und Korrekturmaßnahmen ... 66
4.10.2 Fortlaufende Verbesserung ... 67
4.11 Zusammenfassung ... 67
4.12 Beispiele für Prüfungsfragen zu diesem Kapitel ... 69

5 Maßnahmen im Rahmen des ISMS ... 73
5.1 A.5 Organizational Controls – Organisatorisches Maßnahmen ... 74
5.1.1 A.5.1 Informationssicherheitsrichtlinien ... 74
5.1.2 A.5.2 Rollen und Verantwortlichkeiten für die Informationssicherheit ... 76
5.1.3 A.5.3 Aufgabentrennung ... 77
5.1.4 A.5.4 Verantwortung des Topmanagements ... 77
5.1.5 A.5.5 Kontakt zu Behörden ... 78
5.1.6 A.5.6 Kontakt zu speziellen Interessengruppen ... 78
5.1.7 A.5.7 Erkenntnisse zur Bedrohungslage ... 79
5.1.8 A.5.8 Informationssicherheit im Projektmanagement ... 79
5.1.9 A.5.9 Inventar der Informationswerte und anderer damit verbundener Assets ... 80
5.1.10 A.5.10 Zulässige Nutzung von Informationen und anderen damit verbundenen Assets ... 80
5.1.11 A.5.11 Rückgabe von Assets ... 81
5.1.12 A.5.12 Klassifizierung von Informationen ... 81
5.1.13 A.5.13 Kennzeichnung von Informationen ... 82
5.1.14 A.5.14 Übertragung oder Transport von Informationen ... 83
5.1.15 A.5.15 Zugangssteuerung ... 83
5.1.16 A.5.16 Identitätsmanagement ... 84
5.1.17 A.5.17 Authentisierungsinformationen ... 85
5.1.18 A.5.18 Zugangsberechtigungen ... 86
5.1.19 A.5.19 Informationssicherheit in Lieferantenbeziehungen ... 86
5.1.20 A.5.20 Berücksichtigung der Informationssicherheit in Vereinbarungen mit Lieferanten ... 87
5.1.21 A.5.21 Management der Informationssicherheit in der IKT-Lieferkette ... 87
5.1.22 A.5.22 Überwachung, Überprüfung und Management von Änderungen der Dienstleistungen von Lieferanten ... 88
5.1.23 A.5.23 Informationssicherheit bei der Verwendung von Clouddiensten ... 89
5.1.24 A.5.24 Planung und Vorbereitung des Managements von Informationssicherheitsvorfällen ... 89

5.1.25 A.5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse ... 92
5.1.26 A.5.26 Reaktion auf Informationssicherheitsvorfälle ... 92
5.1.27 A.5.27 Lernen aus Informationssicherheitsvorfällen ... 93
5.1.28 A.5.28 Sammeln von Beweisen ... 93
5.1.29 A.5.29 Informationssicherheit bei Betriebsunterbrechungen ... 94
5.1.30 A.5.30 IKT-bezogene Vorkehrungen zum Erhalt der Geschäftskontinuität 94
5.1.31 A.5.31 Gesetzliche, behördliche und vertragliche Anforderungen ... 95
5.1.32 A.5.32 Rechte an geistigem Eigentum ... 96
5.1.33 A.5.33 Schutz von Aufzeichnungen ... 96
5.1.34 A.5.34 Privatsphäre und Schutz personenbezogener Daten ... 97
5.1.35 A.5.35 Unabhängige Überprüfung der Informationssicherheit ... 97
5.1.36 A.5.36 Konformität mit Richtlinien, Regeln und Standards für die Informationssicherheit ... 98
5.1.37 A.5.37 Dokumentierte Betriebsverfahren ... 98
5.2 A.6 People Controls – Maßnahmen in Verbindung mit Menschen ... 99
5.2.1 A.6.1 Screening ... 99
5.2.2 A.6.2 Vertragsbedingungen für die Beschäftigung ... 100
5.2.3 A.6.3 Sensibilisierung, Ausbildung und Schulung für Informationssicherheit ... 101
5.2.4 A.6.4 Disziplinarverfahren ... 102
5.2.5 A.6.5 Verantwortlichkeiten nach Beendigung oder Wechsel des Beschäftigungsverhältnisses ... 102
5.2.6 A.6.6 Vertraulichkeits- oder Geheimhaltungsvereinbarungen ... 103
5.2.7 A.6.7 Remote-Arbeiten ... 104
5.2.8 A.6.8 Meldung von Informationssicherheitsereignissen ... 105
5.3 A.7 Physical Controls – Physische Maßnahmen ... 106
5.3.1 A.7.1 Physische Sicherheitsperimeter ... 106
5.3.2 A.7.2 Physischer Zutritt ... 108
5.3.3 A.7.3 Sicherung von Büros, Räumlichkeiten und Einrichtungen ... 109
5.3.4 A.7.4 Überwachung der physischen Sicherheit ... 110
5.3.5 A.7.5 Schutz vor physischen und umgebungsbedingten Gefährdungen ... 110
5.3.6 A.7.6 Arbeiten in Sicherheitszonen ... 111
5.3.7 A.7.7 Aufgeräumter Schreibtisch und Gerätesperre ... 112
5.3.8 A.7.8 Platzierung und Schutz von Betriebsmitteln ... 112
5.3.9 A.7.9 Sicherheit von Assets außerhalb der Standorte der Organisation ... 113
5.3.10 A.7.10 Speichermedien ... 114
5.3.11 A.7.11 Unterstützende Versorgungseinrichtungen ... 115
5.3.12 A.7.12 Sicherheit der Verkabelung ... 116
5.3.13 A.7.13 Wartung von Betriebsmitteln ... 116
5.3.14 A.7.14 Sichere Entsorgung oder Wiederverwendung von Betriebsmitteln 117
5.4 A.8 Technological Controls – Technische Maßnahmen ... 118
5.4.1 A.8.1 Anwender-Endgeräte ... 118

5.4.2 A.8.2 Privilegierte Zugangsberechtigungen ... 118
5.4.3 A.8.3 Einschränkung des Zugangs zu Informationen ... 119
5.4.4 A.8.4 Zugang zu Source Code ... 120
5.4.5 A.8.5 Sichere Authentisierung ... 120
5.4.6 A.8.6 Kapazitätsmanagement ... 121
5.4.7 A.8.7 Schutz vor Schadsoftware ... 121
5.4.8 A.8.8 Management technischer Schwachstellen ... 122
5.4.9 A.8.9 Konfigurationsmanagement ... 123
5.4.10 A.8.10 Löschung von Informationen ... 123
5.4.11 A.8.11 Datenmaskierung ... 124
5.4.12 A.8.12 Vermeidung von Datenabfluss ... 124
5.4.13 A.8.13 Datensicherung ... 125
5.4.14 A.8.14 Redundanz informationsverarbeitender Systeme ... 126
5.4.15 A.8.15 Protokollierung ... 126
5.4.16 A.8.16 Überwachungsaktivitäten ... 127
5.4.17 A.8.17 Uhrensynchronisation ... 128
5.4.18 A.8.18 Verwendung von privilegierten Dienstprogrammen ... 128
5.4.19 A.8.19 Installation von Software auf operativen Systemen ... 129
5.4.20 A.8.20 Netzsicherheit ... 130
5.4.21 A.8.21 Sicherheit von Netzdiensten ... 130
5.4.22 A.8.22 Trennung von Netzen ... 131
5.4.23 A.8.23 Webfilterung ... 131
5.4.24 A.8.24 Einsatz von Kryptographie ... 132
5.4.25 A.8.25 Lebenszyklus der sicheren Entwicklung ... 133
5.4.26 A.8.26 Anforderungen an die Sicherheit von Anwendungen ... 133
5.4.27 A.8.27 Sichere Systemarchitektur und Entwicklungsgrundsätze ... 134
5.4.28 A.8.28 Sichere Programmierung ... 135
5.4.29 A.8.29 Sicherheitstests in Entwicklung und Abnahme ... 135
5.4.30 A.8.30 Ausgelagerte Entwicklung ... 136
5.4.31 A.8.31 Trennung von Entwicklungs-, Test- und Produktivumgebungen ... 136
5.4.32 A.8.32 Change Management ... 137
5.4.33 A.8.33 Testdaten ... 138
5.4.34 A.8.34 Schutz von Informationssystemen während Audits ... 138
5.5 Beispiele für Prüfungsfragen zu diesem Kapitel ... 139

6 Verwandte Standards und Rahmenwerke ... 143
6.1 Standards und Rahmenwerke für IT- und Informationssicherheit ... 143
6.1.1 IT-Grundschutz-Kompendium ... 143
6.1.2 BSI-Standards ... 144
6.1.3 CISIS12 ... 145
6.1.4 Cybersecurity Framework ... 146
6.1.5 ISO/IEC 15408 ... 146

6.1.6 VDA ISA (TISAX) 147
6.2 Standards und Rahmenwerke für Qualitätsmanagement, Auditierung und Zertifizierung 149
6.2.1 ISO 9000 149
6.2.2 ISO 19011 150
6.2.3 ISO/IEC 17020 150
6.3 Standards und Rahmenwerke für Governance und Management in der IT 151
6.3.1 ITIL 151
6.3.2 ISO/IEC 20000 152
6.3.3 FitSM 153
6.4 Beispiele für Prüfungsfragen zu diesem Kapitel 154

7 Zertifizierungsmöglichkeiten nach ISO/IEC 27000 157
7.1 ISMS-Zertifizierung nach ISO/IEC 27001 157
7.1.1 Grundlagen der Zertifizierung von Managementsystemen 157
7.1.2 Typischer Ablauf einer Zertifizierung 159
7.1.3 Auditumfang 161
7.1.4 Akzeptanz und Gültigkeit des Zertifikats 161
7.1.5 Aufwände und Kosten für Zertifizierungen 161
7.2 Personenqualifizierung auf Basis von ISO/IEC 27000 162
7.2.1 Programme zur Ausbildung und Zertifizierung von Personal 162
7.2.2 Erlangen eines Foundation-Zertifikats 165
7.3 Zusammenfassung 167
7.4 Beispiele für Prüfungsfragen zu diesem Kapitel 167

A Begriffsbildung nach ISO/IEC 27000 169

B Abdruck der DIN ISO/IEC 27001 187
B.1 ISO/IEC 27001:2017 189
B.2 ISO/IEC 27001:2017, Anhang A 209
B.3 ISO/IEC 27001:2022, Anhang A 224
B.4 Vergleich: Anhang A :2022 vs. :2017 233

C Prüfungsfragen mit Antworten zur ISO/IEC 27001 Foundation 237
C.1 Antworten auf die Prüfungsfragen zu den einzelnen Buchkapiteln 237
C.2 Ein beispielhafter Prüfungsfragebogen zur ISO/IEC 27001-Foundation-Prüfung 244
C.3 Antworten auf den Prüfungsfragebogen zur ISO/IEC 27001-Foundation-Prüfung 255

Literaturverzeichnis 261

Index 265