

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
1.2.3.1 Vertraulichkeit (Confidentiality)	3
1.2.3.2 Integrität (Integrity)	4
1.2.3.3 Verfügbarkeit (Availability)	4
1.2.3.4 Authentizität (Authenticity) und Authentisierung (Authentication).....	5
1.2.3.5 Nichtabstreitbarkeit/Verbindlichkeit (Non-repudiation)	5
1.2.3.6 Verlässlichkeit (Reliability)	5
1.2.3.7 Zugriffssteuerung (Access Control)	5
1.2.3.8 Zurechenbarkeit (Accountability)	6
1.3 IT-Sicherheitsgesetz & KRITIS	6
1.3.1 Was ist „KRITIS“?.....	6
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.....	8
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
2.4.2.1	ISO/IEC 27001: Anforderungen an ein ISMS.....	16
2.4.2.2	ISO/IEC 27006: Anforderungen an Zertifizierer	16
2.4.2.3	ISO/IEC 27009: Anforderungen an die branchenspezifische Anwendung von ISO/IEC 27001	17
2.4.3	Allgemeine Leitfäden	17
2.4.3.1	ISO/IEC 27002: Leitfaden für das Informationssicherheits- management	17
2.4.3.2	ISO/IEC 27003: Umsetzungsempfehlungen	17
2.4.3.3	ISO/IEC 27004: Messungen	18
2.4.3.4	ISO/IEC 27005: Risikomanagement.....	18
2.4.3.5	ISO/IEC 27007 und ISO/IEC TR 27008: Audit-Leitfäden	18
2.4.3.6	ISO/IEC 27013: Kombination mit dem IT Service Management	18
2.4.3.7	ISO/IEC 27014 und ISO/IEC 27016: Governance und Entschei- dungen auf Vorstandsebene	18
2.4.3.8	ISO/IEC 27018: Leitfaden zum Schutz personenbezogener Daten in öffentlichen Cloud-Diensten als Auftragsdatenver- arbeitung.....	19
2.4.3.9	ISO/IEC TR 27023: Gegenüberstellung mit früheren Fassungen	19
2.4.4	Sektor- und maßnahmenspezifische Leitfäden.....	19
2.4.4.1	Ausgewählte sektorspezifische Leitfäden	20
2.4.4.2	Ausgewählte maßnahmenspezifische Leitfäden	21
2.5	Zusammenfassung	21
2.6	Beispiele für Prüfungsfragen zu diesem Kapitel.....	22
3	Grundlagen von Informationssicherheitsmanagementsystemen	23
3.1	Das ISMS und seine Bestandteile.....	23
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	Maßnahmenziele und 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
3.3.3.1	Konformität.....	31
3.3.3.2	Effektivität	32
3.3.3.3	Effizienz	32
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	46
4.6.1.1	Bestimmung allgemeiner Risiken und Chancen	47
4.6.1.2	Informationssicherheitsrisikobeurteilung	48
4.6.1.3	Informationssicherheitsrisikobehandlung	51
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	Maßnahmenziele und Maßnahmen im Rahmen des ISMS.....	73
5.1	A.5 Informationssicherheitsrichtlinien	75
5.1.1	A.5.1 Vorgaben der Leitung für Informationssicherheit	75
5.2	A.6 Organisation der Informationssicherheit.....	77
5.2.1	A.6.1 Interne Organisation	77
5.2.2	A.6.2 Mobilgeräte und Telearbeit	79
5.3	A.7 Personalsicherheit	80
5.3.1	A.7.1 Vor der Beschäftigung.....	81
5.3.2	A.7.2 Während der Beschäftigung	82
5.3.3	A.7.3 Beendigung und Änderung der Beschäftigung.....	83
5.4	A.8 Verwaltung der Werte.....	84
5.4.1	A.8.1 Verantwortlichkeit für Werte	84
5.4.2	A.8.2 Informationsklassifizierung.....	86
5.4.3	A.8.3 Handhabung von Datenträgern	87
5.5	A.9 Zugangssteuerung	90
5.5.1	A.9.1 Geschäftsanforderungen an die Zugangssteuerung.....	90
5.5.2	A.9.2 Benutzerzugangsverwaltung	91
5.5.3	A.9.3 Benutzerverantwortlichkeiten.....	93
5.5.4	A.9.4 Zugangssteuerung für Systeme und Anwendungen	93
5.6	A.10 Kryptographie	96
5.6.1	A.10.1 Kryptographische Maßnahmen.....	96
5.7	A.11 Physische und umgebungsbezogene Sicherheit	98
5.7.1	A.11.1 Sicherheitsbereiche	98
5.7.2	A.11.2 Geräte und Betriebsmittel	101
5.8	A.12 Betriebssicherheit	105
5.8.1	A.12.1 Betriebsabläufe und -verantwortlichkeiten	105
5.8.2	A.12.2 Schutz vor Schadsoftware.....	107
5.8.3	A.12.3 Datensicherung	108
5.8.4	A.12.4 Protokollierung und Überwachung	109
5.8.5	A.12.5 Steuerung von Software im Betrieb.....	111
5.8.6	A.12.6 Handhabung technischer Schwachstellen	111
5.8.7	A.12.7 Audit von Informationssystemen	113
5.9	A.13 Kommunikationssicherheit	115
5.9.1	A.13.1 Netzwerksicherheitsmanagement	115
5.9.2	A.13.2 Informationsübertragung.....	116
5.10	A.14 Anschaffung, Entwicklung und Instandhalten von Systemen	119
5.10.1	A.14.1 Sicherheitsanforderungen an Informationssysteme.....	119
5.10.2	A.14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen	120
5.10.3	A.14.3 Testdaten	123
5.11	A.15 Lieferantenbeziehungen.....	125
5.11.1	A.15.1 Informationssicherheit in Lieferantenbeziehungen	125
5.11.2	A.15.2 Steuerung der Dienstleistungserbringung von Lieferanten.....	126

5.12	A.16 Handhabung von Informationssicherheitsvorfällen.....	128
5.12.1	A.16.1 Handhabung von Informationssicherheitsvorfällen und Verbesserungen	128
5.13	A.17 Informationssicherheitsaspekte beim Business Continuity Management ...	133
5.13.1	A.17.1 Aufrechterhalten der Informationssicherheit	133
5.13.2	A.17.2 Redundanzen	135
5.14	A.18 Compliance.....	136
5.14.1	A.18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen	136
5.14.2	A.18.2 Überprüfungen der Informationssicherheit	138
5.15	Zusammenfassung	139
5.16	Beispiele für Prüfungsfragen zu diesem Kapitel.....	140
6	Verwandte Standards und Rahmenwerke	145
6.1	Standards und Rahmenwerke für IT- und Informationssicherheit	145
6.1.1	IT-Grundschrift-Kompendium	145
6.1.2	BSI-Standards	146
6.1.3	ISIS12	147
6.1.4	Cybersecurity Framework	147
6.1.5	ISO/IEC 15408	148
6.1.6	PCI-DSS	149
6.1.7	VDA ISA (TISAX)	150
6.2	Standards und Rahmenwerke für Qualitätsmanagement, Auditierung und Zertifizierung.....	151
6.2.1	ISO 9000	151
6.2.2	ISO 19011.....	152
6.2.3	ISO/IEC 17020	153
6.3	Standards und Rahmenwerke für Risikomanagement	154
6.3.1	ISO 31000.....	154
6.3.2	COSO ERM	154
6.4	Standards und Rahmenwerke für Governance und Management in der IT	155
6.4.1	ITIL.....	155
6.4.2	ISO/IEC 20000	156
6.4.3	FitSM.....	157
6.4.4	COBIT.....	158
6.4.5	EN 50600	159
6.5	Beispiele für Prüfungsfragen zu diesem Kapitel.....	159
7	Zertifizierungsmöglichkeiten nach ISO/IEC 27000	163
7.1	ISMS-Zertifizierung nach ISO/IEC 27001	163
7.1.1	Grundlagen der Zertifizierung von Managementsystemen	163
7.1.1.1	Zertifizierung.....	163
7.1.1.2	Akkreditierung	164
7.1.2	Typischer Ablauf einer Zertifizierung	165

7.1.3	Auditumfang.....	167
7.1.4	Akzeptanz und Gültigkeit des Zertifikats	167
7.1.5	Aufwände und Kosten für Zertifizierungen.....	167
7.2	Personenqualifizierung auf Basis von ISO/IEC 27000	168
7.2.1	Programme zur Ausbildung und Zertifizierung von Personal	168
7.2.1.1	TÜV Süd: Qualifizierungsprogramm nach ISO/IEC 27000.....	169
7.2.1.2	APMG: ISO/IEC 27001 Certification.....	170
7.2.1.3	ICO: Ausbildungsschema ISMS nach ISO/IEC 27000	170
7.2.2	Das Foundation-Zertifikat des TÜV Süd	171
7.2.2.1	Prüfungsspezifikation	171
7.2.2.2	Vorbereitung auf die Foundation-Prüfung	172
7.3	Zusammenfassung	173
7.4	Beispiele für Prüfungsfragen zu diesem Kapitel.....	174
A	Begriffsbildung nach ISO/IEC 27000	175
B	Abdruck der DIN ISO/IEC 27001	193
C	Prüfungsfragen mit Antworten zur ISO/IEC 27001 Foundation	231
C.1	Antworten auf die Prüfungsfragen zu den einzelnen Buchkapiteln	231
C.2	Ein beispielhafter Prüfungsfragebogen zur ISO/IEC 27001-Foundation-Prüfung	238
C.3	Antworten auf den Prüfungsfragebogen zur ISO/IEC 27001-Foundation-Prüfung	250
	Literaturverzeichnis	257
	Index.....	263