

Auf einen Blick

Über die Autoren	7
Einleitung	23
Teil I: Informationssicherheit mit System.....	29
Kapitel 1: Verständnis von Informationssicherheit – Basiswissen	31
Teil II: Informationssicherheit und Management nach Norm	65
Kapitel 2: Die Geschichte der ISO 27001	67
Kapitel 3: Struktur der ISO 27001	71
Kapitel 4: Die Normfamilie ISO 27000.....	73
Kapitel 5: Vorteile der ISO 27001-Zertifizierung	79
Teil III: Implementierung der ISO 27001 im Unternehmen ...	81
Kapitel 6: Die Einführung eines ISMS	83
Teil IV: Normanforderungen in der Praxis	89
Kapitel 7: Anwendungsbereich, normative Verweisungen und Begriffe	91
Kapitel 8: Kontext und Stakeholder.....	93
Kapitel 9: Führung und Verpflichtung der obersten Leitung.....	103
Kapitel 10: Die Leitlinie	109
Kapitel 11: Rollen und Verantwortlichkeiten	115
Kapitel 12: Risikomanagement.....	121
Kapitel 13: Ziele und Zielerreichung	145
Kapitel 14: Planung von Änderungen	149
Kapitel 15: Unterstützung und Ressourcen	151
Kapitel 16: Kompetenz und Bewusstsein.....	155
Kapitel 17: Kommunikation	161
Kapitel 18: Dokumentation.....	165
Kapitel 19: Umsetzung und Betrieb des ISMS	171
Kapitel 20: Kennzahlen und KPIs.....	175
Kapitel 21: Interne Audits	181
Kapitel 22: Die Management Review.....	191
Kapitel 23: Der kontinuierliche Verbesserungsprozess	197
Teil V: Maßgeschneiderte Maßnahmen, der Anhang A der Norm.....	203
Kapitel 24: Maßnahmen zur Informationssicherheit	205
Kapitel 25: Organisatorische Maßnahmen.....	215
Kapitel 26: Personenbezogene Maßnahmen.....	255

10 Auf einen Blick

Kapitel 27: Physische Maßnahmen	271
Kapitel 28: Technologische Maßnahmen	293
Teil VI: Die Zertifizierung.....	341
Kapitel 29: Die Zertifizierung nach ISO 27001	343
Kapitel 30: Best Practices für Audits	349
Kapitel 31: Wichtige Standards im Kontext von Audits und Zertifizierung	353
Teil VII: ISO 27001, und jetzt?.....	357
Kapitel 32: Weitere Standards und Normen für Informationssicherheit.....	359
Kapitel 33: Integrierte Managementsysteme.....	367
Kapitel 34: Andere Standards in der IT	375
Teil VIII: Der Top-Ten-Teil.....	377
Kapitel 35: Zehn Schritte zur ISO 27001-Zertifizierung.....	379
Kapitel 36: Zehn Dinge, die Sie tun sollten, bevor Sie ein ISMS einführen	383
Kapitel 37: Zehn Maßnahmen zur Organisation der Informationssicherheit.....	387
Kapitel 38: Zehn Basismaßnahmen für Informationssicherheit.....	391
Kapitel 39: Zehn Rollen, die Sie in Ihrem ISMS brauchen können	395
Anhang	399
Anhang A: Eine exemplarische ISMS-Leitlinie.....	401
Anhang B: Übersicht über die Mindest-Dokumente	405
Anhang C: Typische interne Stakeholder	409
Anhang D: Typische externe Stakeholder	415
Anhang E: Abdruck der DIN EN ISO/IEC 27001:2024-01	419
Abbildungsverzeichnis	453
Stichwortverzeichnis	457

Inhaltsverzeichnis

Über die Autoren	7
Einleitung	23
Über dieses Buch	23
Törichte Annahmen über die Leser	24
Was Sie nicht lesen müssen	24
Wie dieses Buch aufgebaut ist	25
Teil I: Informationssicherheit mit System	25
Teil II: Informationssicherheit und Management nach Norm	25
Teil III: Implementierung der ISO 27001 im Unternehmen	26
Teil IV: Normanforderungen in der Praxis	26
Teil V: Maßgeschneiderte Maßnahmen, der Anhang A der Norm	26
Teil VI: Die Zertifizierung	26
Teil VII: ISO 27001, und jetzt?	26
Teil VIII: Der Top-Ten-Teil	27
Anhang	27
Konventionen in diesem Buch	27
Symbole, die in diesem Buch verwendet werden	27
Wie es weitergeht	28
TEIL I INFORMATIONSSICHERHEIT MIT SYSTEM	29
Kapitel 1 Verständnis von Informationssicherheit – Basiswissen	31
Motivation	31
Informationen	33
Informationswerte (Assets)	35
Informationssicherheit	36
IT-Sicherheit	36
Datensicherheit	37
Cybersecurity	38
Datenschutz	39
Hauptaspekte der Informationssicherheit	41
Vertraulichkeit (Confidentiality)	42
Integrität (Integrity)	44
Verfügbarkeit (Availability)	45
Authentizität (authenticity)	46
Zurechenbarkeit (accountability) und Nichtabstreitbarkeit (non-repudiation)	48
Zuverlässigkeit (reliability)	49
Weitere Aspekte	49

12 Inhaltsverzeichnis

Organisationen und Managementsysteme	50
Die Bedeutung der Organisationsstruktur.....	50
Unterschiedliche Organisationsmodelle.....	51
Verantwortlichkeiten für Informationssicherheit	51
Die Rolle der Führungsebene.....	52
Die Bedeutung der Kommunikation	52
Die Integration der Informationssicherheit in die Organisationsstruktur	52
Management	52
Was ist Management?.....	53
Deming-Kreislauf (PDCA)	53
Planung (Plan).....	54
Durchführung (Do).....	55
Überprüfung (Check).....	55
Verbesserung (Act).....	55
Richtlinien, Prozesse und Verfahren.....	55
Systeme und Systemtheorie	60
TEIL II INFORMATIONSSICHERHEIT UND MANAGEMENT NACH NORM.....	65
Kapitel 2 Die Geschichte der ISO 27001	67
Von BS 7799 zu ISO/IEC 27001: Die Anfänge.....	69
Die Evolution der ISO 27001	69
Die Rolle der ISO 27001 in der heutigen Zeit.....	70
Kapitel 3 Struktur der ISO 27001	71
Kapitel 4 Die Normfamilie ISO 27000.....	73
ISO/IEC 27000: Überblick und Terminologie	75
ISO/IEC 27001: Anforderungen an ein ISMS	75
ISO/IEC 27002: Informationssicherheitsmaßnahmen	75
ISO/IEC 27003: Anleitung und Umsetzungsempfehlungen.....	76
ISO/IEC 27004: Überwachung und Messung.....	76
ISO/IEC 27005: Risikomanagement.....	76
Weitere Normen der ISO 27000-Familie	77
Anforderungen, und wie man sie erfüllt	78
Kapitel 5 Vorteile der ISO 27001-Zertifizierung.....	79

TEIL III	
IMPLEMENTIERUNG DER ISO 27001 IM UNTERNEHMEN	81
Kapitel 6	
Die Einführung eines ISMS.....	83
Projektinitiierung	84
Kontextanalyse.....	84
Risikobewertung	85
ISMS-Entwurf	85
Implementierung.....	85
Überwachung und Überprüfung.....	86
Kontinuierliche Verbesserung	86
Mögliche Hindernisse	87
TEIL IV	
NORMANFORDERUNGEN IN DER PRAXIS	89
Kapitel 7	
Anwendungsbereich, normative Verweisungen und Begriffe	91
Einleitung	91
Anwendungsbereich der Norm.....	92
Normative Verweisungen und Begriffe	92
Kapitel 8	
Kontext und Stakeholder.....	93
Was verlangt die ISO 27001?	94
Die Praxis: Wie setzt man den Kontext der Organisation um?.....	95
Interne Faktoren.....	95
Externe Faktoren	96
Relevante Parteien.....	96
Der Anwendungsbereich	101
Was möchte der Auditor sehen?.....	102
Kapitel 9	
Führung und Verpflichtung der obersten Leitung	103
Die Bedeutung des Top-Managements	103
Was verlangt die ISO 27001?	104
Die Praxis: Wie setzt man Führung und Verpflichtung der obersten Leitung um?	106
Was möchte der Auditor sehen?.....	106
Kapitel 10	
Die Leitlinie	109
Warum ist die Leitlinie wichtig?.....	109
Was verlangt die ISO 27001?	110

14 Inhaltsverzeichnis

Die Praxis: Wie setzt man eine Leitlinie um?	111
Was möchte die Auditorin sehen?.....	112
Kapitel 11	
Rollen und Verantwortlichkeiten	115
Was verlangt die ISO 27001?	115
Die Praxis: Wie setzt man Rollen um?.....	116
Die RACI-Matrix	118
Was möchte der Auditor sehen?.....	119
Kapitel 12	
Risikomanagement	121
Was verlangt die ISO 27001?	122
Die Praxis: Wie setzt man Risikomanagement um?.....	125
Risikokriterien.....	126
Asset-Inventar und Risikoidentifikation	127
Risikoanalyse und Bewertung	135
Risikoakzeptanz	139
Risikobehandlung.....	140
Anhang A und SoA	141
Was möchte die Auditorin sehen?.....	143
Kapitel 13	
Ziele und Zielerreichung	145
Was verlangt die ISO 27001?	145
Die Praxis: Wie setzt man Ziele um?.....	147
Was möchte der Auditor sehen?.....	148
Kapitel 14	
Planung von Änderungen.....	149
Was verlangt die ISO 27001?	149
Die Praxis: Wie setzt man Change Management um?	149
Was möchte der Auditor sehen?.....	150
Kapitel 15	
Unterstützung und Ressourcen	151
Ressourcen.....	152
Was verlangt die ISO 27001?	152
Die Praxis: Wie setzt man die Ressourcenplanung um?	152
Was möchte die Auditorin sehen?.....	153
Kapitel 16	
Kompetenz und Bewusstsein	155
Was verlangt die ISO 27001?	155
Die Praxis: Wie setzt man Kompetenzen und Bewusstsein um?	156
Awareness-Schulungen und Programme.....	158
Sicherheitsvorfälle und Konsequenzen	158
Was möchte der Auditor sehen?.....	159

Kapitel 17 Kommunikation	161
Was verlangt die ISO 27001?	162
Die Praxis: Wie setzt man einen Kommunikationsplan um?.....	162
Was möchte die Auditorin sehen?.....	162
Kapitel 18 Dokumentation	165
Was verlangt die ISO 27001?	166
Die Praxis: Wie setzt man die Dokumentation um?.....	167
Vertraulichkeitsstufen.....	168
Was möchte der Auditor sehen?.....	169
Kapitel 19 Umsetzung und Betrieb des ISMS.....	171
Was verlangt die ISO 27001?	171
Die Praxis: Was setzt man im Betrieb um?	172
Was möchte die Auditorin sehen?.....	174
Kapitel 20 Kennzahlen und KPIs.....	175
Was verlangt die ISO 27001?	176
Die Praxis: Wie setzt man Kennzahlen und deren Messungen um?	177
Was möchte der Auditor sehen?.....	179
Kapitel 21 Interne Audits	181
Konformität, Effektivität und Effizienz	183
Verschiedene Arten von Audits.....	184
Was verlangt die ISO 27001?	186
Die Praxis: Wie setzt man ein Audit-Programm und Audits um?	187
Was möchte die Auditorin sehen?.....	189
Kapitel 22 Die Management Review	191
Was verlangt die ISO 27001?	192
Die Praxis: Wie setzt man die Management Reviews um?	193
Was möchte der Auditor sehen?.....	194
Kapitel 23 Der kontinuierliche Verbesserungsprozess	197
Was verlangt die ISO 27001?	198
Die Praxis: Wie setzt man kontinuierliche Verbesserung um?	198
Was möchte die Auditorin sehen?.....	200

16 Inhaltsverzeichnis

TEIL V MAßGESCHNEIDERTE MAßNAHMEN, DER ANHANG A DER NORM 203

Kapitel 24		
Maßnahmen zur Informationssicherheit.....		205
ISO 27002 und der Anhang A.....		206
Attribute von Maßnahmen.....		207
Die Maßnahmenart		207
Informationssicherheitseigenschaften		208
Cybersicherheitskonzepte		209
Betriebsfähigkeit		210
Sicherheitsdomänen		211
Anwendung der Maßnahmen		212
Kapitel 25		
Organisatorische Maßnahmen.....		215
Informationssicherheitsrichtlinien (5.1).....		215
Informationssicherheitsrollen und -verantwortlichkeiten (5.2)		217
Aufgabentrennung (5.3)		218
Verantwortlichkeiten der Leitung (5.4).....		219
Kontakt mit Behörden (5.5)		220
Kontakt mit speziellen Interessengruppen (5.6).....		221
Erkenntnisse über Bedrohungen (5.7)		222
Informationssicherheit im Projektmanagement (5.8)		223
Inventar der Informationen und anderer damit verbundenen Werte		224
Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten (5.10).....		225
Rückgabe von Werten (5.11)		226
Klassifizierung von Information (5.12)		227
Kennzeichnung von Information (5.13)		229
Informationsübertragung (5.14)		230
Zugangssteuerung (5.15)		231
Identitätsmanagement (5.16).....		232
Informationen zur Authentifizierung (5.17).....		233
Zugangsrechte (5.18).....		234
Supplier Management (5.19–5.22)		235
Informationssicherheit für die Nutzung von Cloud-Diensten (5.23)		238
Information Security Incident Management (5.24–5.28)		239
Informationssicherheit bei Störungen (5.29).....		243
IKT-Bereitschaft für Business Continuity (5.30).....		245
Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen (5.31)		246
Geistige Eigentumsrechte (5.32)		247
Schutz von Aufzeichnungen (5.33)		248
Privatsphäre und Schutz von personenbezogenen Daten (5.34).....		249
Unabhängige Überprüfung der Informationssicherheit (5.35).....		250

Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit (5.36)	251
Dokumentierte Bedienabläufe (5.37)	253

Kapitel 26 Personenbezogene Maßnahmen 255

Sicherheitsüberprüfung (6.1)	256
Beschäftigungs- und Vertragsbedingungen (6.2)	258
Informationssicherheitsbewusstsein, -ausbildung und -schulung (6.3)	259
Maßregelungsprozess (6.4)	261
Verantwortlichkeiten nach Beendigung oder Änderung der Beschäftigung (6.5)	263
Vertraulichkeits- oder Geheimhaltungsvereinbarungen (6.6)	264
Telearbeit (6.7)	266
Meldung von Informationssicherheitereignissen (6.8)	268

Kapitel 27 Physische Maßnahmen 271

Physische Sicherheitsperimeter (7.1)	272
Physischer Zutritt (7.2)	274
Sichern von Büros, Räumen und Einrichtungen (7.3)	275
Physische Sicherheitsüberwachung (7.4)	276
Schutz vor physischen und umweltbedingten Bedrohungen (7.5)	277
Klimawandel und ISO 27001	278
Arbeiten in Sicherheitsbereichen (7.6)	279
Aufgeräumte Arbeitsumgebung und Bildschirmsperren (7.7)	280
Platzierung und Schutz von Geräten und Betriebsmitteln (7.8)	281
Sicherheit von Werten außerhalb der Räumlichkeiten (7.9)	283
Speichermedien (7.10)	284
Versorgungseinrichtungen (7.11)	285
Sicherheit der Verkabelung (7.12)	287
Instandhalten von Geräten und Betriebsmitteln (7.13)	288
Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln (7.14)	290

Kapitel 28 Technologische Maßnahmen 293

Endpunktgeräte des Benutzers (8.1)	293
Sichere Konfiguration von Benutzerendgeräten	294
Bring Your Own Device (BYOD)	295
Verfügbare Bandbreiten	295
Privilegierte Zugangsrechte (8.2)	296
Informationszugangsbeschränkung (8.3)	298
Zugriff auf den Quellcode (8.4)	299
Sichere Authentifizierung (8.5)	300
Kapazitätssteuerung (8.6)	302
Schutz gegen Schadsoftware (8.7)	304
Handhabung von technischen Schwachstellen (8.8)	305

18 Inhaltsverzeichnis

Konfigurationsmanagement (8.9)	307
Löschen von Informationen (8.10)	308
Datenmaskierung (8.11)	309
Verhinderung von Datenlecks (8.12)	311
Sicherung von Information (8.13)	312
Redundanz von informationsverarbeitenden Einrichtungen (8.14)	313
Protokollierung (8.15)	314
Überwachung von Aktivitäten (8.16)	316
Uhrensynchronisation (8.17)	317
Gebrauch von Hilfsprogrammen mit privilegierten Rechten (8.18)	318
Installation von Software auf Systemen im Betrieb (8.19)	320
Netzwerksicherheit (8.20)	321
Sicherheit von Netzwerkdiensten (8.21)	322
Trennung von Netzwerken (8.22)	323
Webfilterung (8.23)	325
Verwendung von Kryptografie (8.24)	327
Sichere Entwicklung	329
Lebenszyklus einer sicheren Entwicklung (8.25)	330
Anforderungen an die Anwendungssicherheit (8.26)	331
Sichere Systemarchitektur und technische Grundsätze (8.27)	332
Sichere Codierung (8.28)	333
Sicherheitsprüfung in Entwicklung und Abnahme (8.29)	334
Ausgegliederte Entwicklung (8.30)	335
Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen (8.31)	336
Änderungssteuerung (8.32)	337
Informationen zur Prüfung (8.33)	339
Schutz der Informationssysteme während der Überwachungsprüfung (8.34)	340
TEIL VI DIE ZERTIFIZIERUNG	341
Kapitel 29 Die Zertifizierung nach ISO 27001	343
Vorbereitung und Planung	344
Auswahl der Zertifizierungsstelle	344
Optionales Voraudit	345
Stufe-1-Audit: Dokumentenprüfung	345
Stufe-2-Audit: Vor-Ort-Audit	346
Zertifizierung und Ausstellung des Zertifikats	346
Überwachungsaudits	347
Kapitel 30 Best Practices für Audits	349
Vorbereitung auf das Audit	349
Durchführung des Audits	350
Nach dem Audit	350

Kapitel 31	
Wichtige Standards im Kontext von Audits und Zertifizierung	353
ISO 19011: Ein Leitfaden für Audits	354
ISO 27006, ISO 27007 und ISO 27008.....	354
ISO 17021	355
TEIL VII	
ISO 27001, UND JETZT?.....	357
Kapitel 32	
Weitere Standards und Normen für Informationssicherheit	359
IT-Grundschutz.....	359
CISIS12®.....	361
BSI-Standards.....	362
BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)	362
BSI-Standard 200-2: IT-Grundschutz-Methodik.....	362
BSI-Standard 200-3: Risikomanagement	362
BSI-Standard 200-4: Business Continuity Management (BCM).....	363
BSI-Standard 100-4: Notfallmanagement.....	363
VDA ISA und TISAX®.....	363
Weitere Rahmenwerke und Standards	365
Managementsystemansatz	365
Kapitel 33	
Integrierte Managementsysteme.....	367
ISO 9001	368
ISO 20000-1	369
Weitere Managementsysteme.....	371
ISO 14001	372
ISO 45001	372
ISO 50001	373
Kapitel 34	
Andere Standards in der IT.....	375
ITIL®	375
FitSM	376
TEIL VIII	
DER TOP-TEN-TEIL.....	377
Kapitel 35	
Zehn Schritte zur ISO 27001-Zertifizierung	379
Warum wollen Sie zertifiziert werden?.....	379
Dokumentation des Geltungsbereichs.....	379

20 Inhaltsverzeichnis

Gap-Analyse: Abgleich der Anforderungen mit dem Ist-Zustand.....	380
Dokumentation der Prozesse	380
Umsetzung der Prozesse	380
Internes Audit.....	380
Management Review.....	380
Zertifizierungsstelle auswählen.....	381
Zertifizierungsaudit.....	381
Zertifizierung aufrecht erhalten	381

Kapitel 36

Zehn Dinge, die Sie tun sollten, bevor Sie ein

ISMS einführen

383	
Unterstützung des Managements sichern.....	383
Ziele festlegen	383
Mitarbeiter sensibilisieren	384
Ressourcen bereitstellen	384
Risiken identifizieren.....	384
Bestandsaufnahme der Assets	384
Rechtliche und regulatorische Anforderungen klären.....	385
Externe Berater einbeziehen	385
Kommunikation vorbereiten	385
Langfristige Planung	385

Kapitel 37

Zehn Maßnahmen zur Organisation der

Informationssicherheit

387	
Erstellen einer Informationssicherheitsrichtlinie	387
Festlegung von ISMS-Zielen	387
Pflege eines Asset-Registers.....	388
Durchführung regelmäßiger Risikoanalysen.....	388
Sensibilisierung und Schulung der Mitarbeiter.....	388
Implementierung eines Berechtigungsmanagements.....	388
Erstellen eines Incident-Response-Plans	388
Regelmäßige interne Audits.....	389
Erstellen eines Notfallwiederherstellungsplans	389
Implementierung technischer Schutzmaßnahmen	389

Kapitel 38

Zehn Basismaßnahmen für Informationssicherheit

391	
Starke Passwortrichtlinien einführen.....	391
Sicherheitsupdates und Patches regelmäßig installieren	391
Sicherheitsbewusstsein schulen	392
Regelmäßige Backups durchführen	392
Zugriffsrechte einschränken	392
Firewalls und Antivirensoftware verwenden.....	392
Mitarbeiterzugänge überwachen und protokollieren	392
Sichere Remote-Arbeitslösungen anbieten	393

Mobile Geräte absichern	393
Notfallplan für Sicherheitsvorfälle entwickeln	393
Kapitel 39	
Zehn Rollen, die Sie in Ihrem ISMS brauchen können	395
Top-Management	395
Chief Information Officer (CIO)	395
Informationssicherheitsbeauftragter (ISB/CISO)	396
ISMS-Team	396
IT-Leitung	396
IT-Sicherheitsbeauftragter	396
Security-Incident-Response-Team	396
Auditoren	397
Risikomanager	397
Compliance-Beauftragter/Datenschutzbeauftragter (DSB)	397
ANHANG	399
Anhang A: Eine exemplarische ISMS-Leitlinie	401
Leitlinie zur Informationssicherheit	401
1. Zweck	401
2. Geltungsbereich	401
3. Grundsätze der Informationssicherheit	402
4. Verantwortlichkeiten	402
5. Risikomanagement	402
6. Schulungen	403
7. Überwachung und Verbesserung	403
Anhang B: Übersicht über die Mindest-Dokumente	405
Mindestdokumente aus Kapitel 4-10	406
Mindestdokumente aus Anhang A	406
Anhang C: Typische interne Stakeholder	409
Geschäftsführung	409
IT-Abteilung	409
Rechtsabteilung (Legal)	409
Personalabteilung (HR)	409
Einkauf	410
Facility Management	410
Finanzabteilung und Buchhaltung	410
Marketingabteilung	410
Entwicklungsabteilung	410
Qualitätsmanagement und Qualitätsmanagementbeauftragte	410
Interne Revision	411
Geschäftsbereichsleiter	411
Compliance-Beauftragter	411
IT-Sicherheitsbeauftragter	412

22 Inhaltsverzeichnis

Risikomanagement	412
Schulungsabteilung.....	412
Innovationsabteilung	412
Datenanalysten	412
Kundenbetreuung	412
IT-Support.....	413
Arbeitssicherheit	413
Datenschutzbeauftragter.....	413
Betriebsrat	413
Anhang D: Typische externe Stakeholder	415
Kunden	415
Lieferanten und Dienstleister	415
Gesetzgeber und Behörden.....	415
Regulierungsbehörden und Wettbewerbsbehörden.....	415
Aktionäre, Anleger und Investoren.....	416
Finanzinstitute	416
Versicherer	416
Wirtschaftsprüfer.....	416
Verbände und Interessengruppen	416
Konkurrenten.....	417
Medien	417
Anwaltskanzleien.....	417
Beratungsunternehmen.....	417
Technologiepartner.....	417
Ethikkommissionen.....	418
Wissenschaftliche Institutionen.....	418
Nachbarn	418
Öffentlichkeit	418
Anhang E: Abdruck der DIN EN ISO/IEC 27001:2024-01	419
Abbildungsverzeichnis	453
Stichwortverzeichnis	457