

Informationssicherheitsmanagement nach ISO 27001

Norm, Umsetzung, Best Practices

DAS INHALTS- VERZEICHNIS

» Hier geht's
direkt
zum Buch

Inhalt

Geleitwort des Fachgutachters	13
1 Einleitung	15
1.1 Für wen ist dieses Buch?	15
1.2 Was erwartet Sie?	16
2 Was ist ein ISMS?	21
2.1 Ziele und Vorteile eines ISMS	22
2.2 Abgrenzung zu anderen Managementsystemen	26
2.2.1 ISO 9001 (Qualitätsmanagementsystem)	27
2.2.2 ISO 22301 (Business Continuity Management System)	27
2.2.3 ISO 27701 (Datenschutz-Managementsystem)	27
3 Warum auch Sie ein ISMS verwenden sollten?	29
3.1 Bedeutung der Informationssicherheit	30
3.2 Risiken und Bedrohungen für Unternehmen	33
3.3 Wirtschaftliche und rechtliche Notwendigkeit	35
4 Begriffe zur Informationssicherheit	37
4.1 Was sind Informationen?	37
4.2 Die CIA-Triade	40
4.3 Authentizität und Verbindlichkeit	41
4.4 Grundbegriffe	43
5 Einführung in die Normenreihe ISO 27000	47
5.1 Inhalt und Aufbau	48
5.1.1 ISO/IEC 27000	48
5.1.2 ISO/IEC 27001	50
5.1.3 Der PDCA-Kreislauf	50
5.1.4 Der Security-Kreislauf	52
5.1.5 ISO/IEC 27002	53

6	Die ISO 27001 verstehen	55
6.1	NK 4 – Kontext der Organisation	55
6.1.1	NA 4.1 – Verstehen der Organisation und ihres Kontextes	56
6.1.2	NA 4.2 – Verstehen der Erfordernisse und Erwartungen interessierter Parteien	58
6.1.3	NA 4.3 – Festlegen des Anwendungsbereichs des ISMS	60
6.1.4	NA 4.4 – Informationssicherheitsmanagementsystem	62
6.2	NK 5 – Führung	63
6.2.1	NA 5.1 – Führung und Verpflichtung	63
6.2.2	NA 5.2 – Politik	66
6.2.3	NA 5.3 – Rollen, Verantwortlichkeiten und Befugnisse in der Organisation	67
6.3	NK 6 – Planung	70
6.3.1	NA 6.1 – Maßnahmen zum Umgang mit Risiken und Chancen	70
6.3.2	NA 6.2 – Informationssicherheitsziele und Planung zu deren Erreichung	75
6.3.3	NA 6.3 – Planung von Änderungen	76
6.4	Einschub: Praxisbeispiel Risikomanagement	77
6.4.1	Bedrohungen	77
6.4.2	Risikobewertung	79
6.4.3	Risikobehandlung	84
6.5	NK 7 – Unterstützung	84
6.5.1	NA 7.1 – Ressourcen	85
6.5.2	NA 7.2 – Kompetenz	86
6.5.3	NA 7.3 – Bewusstsein	87
6.5.4	NA 7.4 – Kommunikation	89
6.5.5	NA 7.5 – Dokumentierte Information	90
6.6	NK 8 – Betrieb	93
6.6.1	NA 8.1 – Betriebliche Planung und Steuerung	93
6.6.2	NA 8.2 – Informationssicherheitsrisikobeurteilung	94
6.6.3	NA 8.3 – Informationssicherheitsrisikobehandlung	95
6.7	NK 9 – Bewertung der Leistung	96
6.7.1	NA 9.1 – Überwachung, Messung, Analyse und Bewertung	96
6.7.2	NA 9.2 – Internes Audit	97
6.7.3	NA 9.3 – Managementbewertung	100
6.8	NK 10 – Verbesserung	102
6.8.1	NA 10.1 – Fortlaufende Verbesserung	103
6.8.2	NA 10.2 – Nichtkonformität und Korrekturmaßnahmen	104

7	Die Anhänge der ISO 27001: die Controls A.5 bis A.8	107
7.1	Die Attribut-Tabelle	108
7.1.1	Praxisbeispiel	110
7.2	NK A.5 – Organisatorische Maßnahmen	112
7.2.1	NA A.5.1 – Informationssicherheitspolitik und -richtlinien	113
7.2.2	NA A.5.2 – Informationssicherheitsrollen und -verantwortlichkeiten	114
7.2.3	NA A.5.3 – Aufgabentrennung	115
7.2.4	NA A.5.4 – Verantwortlichkeiten der Leitung	116
7.2.5	NA A.5.5 – Kontakt mit Behörden	117
7.2.6	NA A.5.6 – Kontakt mit speziellen Interessensgruppen	119
7.2.7	NA A.5.7 – Informationen über die Bedrohungslage	121
7.2.8	NA A.5.8 – Informationssicherheit im Projektmanagement	123
7.2.9	NA A.5.9 – Inventar der Informationen und anderen damit verbundenen Werte	124
7.2.10	NA A.5.10 – Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten	126
7.2.11	NA A.5.11 – Rückgabe von Werten	127
7.2.12	NA A.5.12 – Klassifizierung von Informationen	128
7.2.13	NA A.5.13 – Kennzeichnung von Informationen	129
7.2.14	NA A.5.14 – Informationsübermittlung	130
7.2.15	NA A.5.15 – Zugangssteuerung	132
7.2.16	NA A.5.16 – Identitätsmanagement	133
7.2.17	NA A.5.17 – Authentisierungsinformationen	135
7.2.18	NA A.5.18 – Zugangsrechte	136
7.2.19	NA A.5.19 – Informationssicherheit in Lieferantenbeziehungen	137
7.2.20	NA A.5.20 – Behandlung von Informationssicherheit in Lieferantenvereinbarungen	138
7.2.21	NA A.5.21 – Umgang mit der Informationssicherheit in der IKT-Lieferkette	139
7.2.22	NA A.5.22 – Überwachung, Überprüfung und Änderungs- management von Lieferantendienstleistungen	140
7.2.23	NA A.5.23 – Informationssicherheit für die Nutzung von Cloud-Diensten	141
7.2.24	NA A.5.24 – Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen	142
7.2.25	NA A.5.25 – Beurteilung und Entscheidung über Informationssicherheitsereignisse	143
7.2.26	NA A.5.26 – Reaktion auf Informationssicherheitsvorfälle	147

7.2.27	NA A.5.27 – Erkenntnisse aus Informationssicherheits- vorfällen	148
7.2.28	NA A.5.28 – Sammeln von Beweismaterial	149
7.2.29	NA A.5.29 – Informationssicherheit bei Störungen	149
7.2.30	NA A.5.30 – IKT-Bereitschaft für Business-Continuity	150
7.2.31	NA A.5.31 – Juristische, gesetzliche, regulatorische und vertragliche Anforderungen	151
7.2.32	NA A.5.32 – Geistige Eigentumsrechte	153
7.2.33	NA A.5.33 – Schutz von Aufzeichnungen	154
7.2.34	NA A.5.34 – Datenschutz und Schutz von personenbezogenen Daten (PbD)	154
7.2.35	NA A.5.35 – Unabhängige Überprüfung der Informations- sicherheit	155
7.2.36	NA A.5.36 – Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit	156
7.2.37	NA A.5.37 – Dokumentierte Betriebsabläufe	157
7.3	NK A.6 – Personenbezogene Maßnahmen	158
7.3.1	NA A.6.1 – Sicherheitsüberprüfung	158
7.3.2	NA A.6.2 – Beschäftigungs- und Vertragsbedingungen	159
7.3.3	NA A.6.3 – Informationssicherheitsbewusstsein, -ausbildung und -schulung	159
7.3.4	NA A.6.4 – Maßregelungsprozess	160
7.3.5	NA A.6.5 – Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung	161
7.3.6	NA A.6.6 – Vertraulichkeits- oder Geheimhaltungs- vereinbarungen	162
7.3.7	NA A.6.7 – Remote-Arbeit	163
7.3.8	NA A.6.8 – Meldung von Informationssicherheitsereignissen	164
7.4	NK A.7 – Physische Maßnahmen	165
7.4.1	NA A.7.1 – Physische Sicherheitsperimeter	166
7.4.2	NA A.7.2 – Physischer Zutritt	167
7.4.3	NA A.7.3 – Sichern von Büros, Räumen und Einrichtungen	168
7.4.4	NA A.7.4 – Physische Sicherheitsüberwachung	169
7.4.5	NA A.7.5 – Schutz vor physischen und umweltbedingten Bedrohungen	170
7.4.6	NA A.7.6 – Arbeiten in Sicherheitsbereichen	171
7.4.7	NA A.7.7 – Aufgeräumte Arbeitsumgebung und Bildschirm Sperren	172
7.4.8	NA A.7.8 – Platzierung und Schutz von Geräten und Betriebsmitteln	173

7.4.9	NA A.7.9 – Sicherheit von Werten außerhalb der Räumlichkeiten	173
7.4.10	NA A.7.10 – Speichermedien	174
7.4.11	NA A.7.11 – Versorgungseinrichtungen	175
7.4.12	NA A.7.12 – Sicherheit der Verkabelung	176
7.4.13	NA A.7.13 – Instandhaltung von Geräten und Betriebsmitteln	177
7.4.14	NA A.7.14 – Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	178
7.5	NK A.8 – Technologische Maßnahmen	180
7.5.1	NA A.8.1 – Endpunktgeräte des Benutzers	180
7.5.2	NA A.8.2 – Privilegierte Zugangsrechte	181
7.5.3	NA A.8.3 – Informationszugangsbeschränkung	182
7.5.4	NA A.8.4 – Zugriff auf den Quellcode	182
7.5.5	NA A.8.5 – Sichere Authentisierung	183
7.5.6	NA A.8.6 – Kapazitätssteuerung	184
7.5.7	NA A.8.7 – Schutz gegen Schadsoftware	185
7.5.8	NA A.8.8 – Handhabung von technischen Schwachstellen	186
7.5.9	NA A.8.9 – Konfigurationsmanagement	187
7.5.10	NA A.8.10 – Löschung von Informationen	188
7.5.11	NA A.8.11 – Datenmaskierung	189
7.5.12	NA A.8.12 – Verhinderung von Datenlecks	190
7.5.13	NA A.8.13 – Sicherung von Informationen	191
7.5.14	NA A.8.14 – Redundanz von informationsverarbeitenden Einrichtungen	192
7.5.15	NA A.8.15 – Protokollierung	193
7.5.16	NA A.8.16 – Überwachung von Aktivitäten	194
7.5.17	NA A.8.17 – Uhrensynchronisation	196
7.5.18	NA A.8.18 – Gebrauch von Hilfsprogrammen mit privilegierten Rechten	198
7.5.19	NA A.8.19 – Installation von Software auf Systemen im Betrieb	198
7.5.20	NA A.8.20 – Netzwerksicherheit	199
7.5.21	NA A.8.21 – Sicherheit von Netzwerkdiensten	200
7.5.22	NA A.8.22 – Trennung von Netzwerken	201
7.5.23	NA A.8.23 – Webfilterung	202
7.5.24	NA A.8.24 – Verwendung von Kryptographie	203
7.5.25	NA A.8.25 – Lebenszyklus einer sicheren Entwicklung	204
7.5.26	NA A.8.26 – Anforderungen an die Anwendungssicherheit	204
7.5.27	NA A.8.27 – Sichere Systemarchitektur und Entwicklungsgrundsätze	206
7.5.28	NA A.8.28 – Sichere Codierung	207
7.5.29	NA A.8.29 – Sicherheitsprüfung bei Entwicklung und Abnahme	208

7.5.30	NA A.8.30 – Ausgegliederte Entwicklung	209
7.5.31	NA A.8.31 – Trennung von Entwicklungs-, Test- und Produktionsumgebungen	211
7.5.32	NA A.8.32 – Änderungssteuerung	211
7.5.33	NA A.8.33 – Testdaten	212
7.5.34	NA A.8.34 – Schutz der Informationssysteme während Tests im Rahmen von Audits	213
8	Wie wird ein ISMS umgesetzt?	215
8.1	Leitfaden für KMUs: Best Practices für die Umsetzung	215
8.2	Stolpersteine	218
8.3	Mindestens notwendige Dokumente	219
8.4	Tools und Ressourcen	221
8.4.1	Blogs und Wikis	222
9	Informationssicherheit messen	225
9.1	ISO 27004 – Überwachung, Messung, Analyse und Bewertung	225
9.2	Kennzahlen und Metriken für ein ISMS	228
9.3	Das Reifegrad-Modell	231
9.3.1	Reifegrad 1 – initial / ad hoc	232
9.3.2	Reifegrad 2 – wiederholbar / Basisimplementierung	232
9.3.3	Reifegrad 3 – definiert / etabliert	232
9.3.4	Reifegrad 4 – gesteuert / überwacht	233
9.3.5	Reifegrad 5 – optimiert / kontinuierlich verbessert	233
9.3.6	Interpretation und Anwendung	233
9.3.7	Beispiel für eine Reifegradbewertung	234
10	Audits	235
10.1	Interne vs. externe Audits	238
10.2	ISO 19011 – Auditierung von Managementsystemen	238
10.3	Das Audit-Programm	244
10.3.1	3-Jahresplanung	244
10.3.2	Jahresplanung	245
10.4	Audit-Plan	246
10.4.1	Beispiel für das interne Audit	246

10.5	Audit-Bericht	248
10.5.1	Bewertungen	249
10.6	Audit-Fragen	250
10.7	Typische Audit-Feststellungen	282
11	Zertifizierung	285
11.1	Ablauf	285
11.2	Akkreditierung	287
12	Weitere Normen bzw. Standards	291
12.1	ISO 27003 – Umsetzung eines ISMS	291
12.2	ISO 27799 – Informationssicherheit im Gesundheitswesen	293
12.3	ISO 27006 – Anforderungen an die Zertifizierer	296
12.4	ISO 27007 – Leitfaden für das Auditieren eines ISMS	299
12.5	ISO 27008 – Leitlinien für die Bewertung von Informationssicherheitskontrollen	302
12.6	ISO 27018 – Sicherheit in Cloud-Diensten	305
12.7	ISO 27701 – Datenschutz-Managementsystem	307
12.8	CISIS12	311
12.9	VdS 10000	317
12.10	Vergleich von ISO 27001, VdS 10000 und CISIS12	319
12.11	DIN SPEC 27076 – IT-Sicherheitsberatung für Klein- und Kleinstunternehmen	320
12.12	Umsetzung eines ISMS mit BSI-Standards	325
12.12.1	Standard 200-1	325
12.12.2	Standard 200-2	328
12.13	NIST Cybersecurity Framework	331
12.14	COBIT	334
13	Gesetzliche Anforderungen	337
13.1	Datenschutz	337
13.2	Cyber Resilience Act (CRA)	342
13.3	NIS-2	344
13.4	TISAX 6	353

Anhang	357
A Beispieldokumente	357
A.1 Projektplan	357
A.2 Informationssicherheitspolitik	365
A.3 Rollenbeschreibungen	376
A.4 Klassifizierungsrichtlinie	386
A.5 Interne und externe Kommunikation	395
A.6 IT-Nutzungsrichtlinie	400
A.7 Zugriffskontrollkonzept	415
A.8 Change-Management	426
A.9 Entwicklungssicherheitsrichtlinie	434
A.10 BCM-Konzept	442
A.11 Business-Impact-Analyse (BIA)	445
A.12 BCM-Plan	449
B Die DIN EN ISO/IEC 27001:2024-01 mit Anhang und Änderung im Wortlaut	455
 Index	 493