

1 Die Normenreihe ISO/IEC 27000 und ihre Grundbegriffe	1
1.1 Übersicht und Verfügbarkeit	1
1.2 Die Basisnormen	2
1.3 Weitere Normen der Reihe im Überblick	5
1.4 Grundbegriffe und Zusammenhänge	7
Literatur	30
2 Anforderungen an das ISMS	31
2.1 Kontext der Organisation (ISMS-4)	32
ISMS-4.1 – Verstehen der Organisation und ihres Kontextes	33
ISMS-4.2 – Verstehen der Erfordernisse und Erwartungen interessierter Parteien	36
ISMS-4.3 – Festlegen des Anwendungsbereichs des ISMS	37
ISMS-4.4 – Das Informationssicherheits-Managementsystem (ISMS) ...	39
2.2 Führung (ISMS-5)	40
ISMS-5.1 – Führung und Verpflichtung	41
ISMS-5.2 – Politik	45
ISMS-5.3 – Rollen, Verantwortlichkeiten und Befugnisse in der Organisation	47
2.3 Planung (ISMS-6)	50
ISMS-6.1 – Maßnahmen zum Umgang mit Risiken und Chancen	50
ISMS-6.2 – Informationssicherheitsziele und Planung zu deren Erreichung	58
ISMS-6.3 – Planung von Änderungen	62
2.4 Unterstützung (ISMS-7)	63
ISMS-7.1 – Ressourcen	63
ISMS-7.2 – Kompetenz	65
ISMS-7.3 – Bewusstsein	65
ISMS-7.4 – Kommunikation	66
ISMS 7.5 – Dokumentierte Information	68

2.5	Betrieb (ISMS-8)	71
	ISMS-8.1 – Betriebliche Planung und Steuerung	71
	ISMS-8.2 – Informationssicherheitsrisikobeurteilung	72
	ISMS-8.3 – Informationssicherheitsrisikobehandlung	73
2.6	Bewertung der Leistung (ISMS-9)	74
	ISMS-9.1 – Überwachung, Messung, Analyse und Bewertung	75
	ISMS-9.2 – Internes Audit	82
	ISMS-9.3 – Managementbewertung	85
2.7	Verbesserung (ISMS-10)	87
	ISMS-10.1 Fortlaufende Verbesserung	87
	ISMS-10.2 Nichtkonformität und Korrekturmaßnahmen	88
	Literatur	90
3	Controls: Anforderungen und Maßnahmen	91
3.1	Einführung in die Anwendung	91
3.2	Ordnungsmerkmale der Controls	93
3.3	Organisatorische Controls (Gruppe 5)	95
	A-5.1 Informationssicherheitsrichtlinien	95
	A-5.2 Informationssicherheitsrollen und -verantwortlichkeiten	97
	A-5.3 Aufgabentrennung	97
	A-5.4 Verantwortlichkeiten der Leitung	99
	A-5.5 Kontakt mit Behörden	99
	A-5.6 Kontakte mit speziellen Interessengruppen	100
	A-5.7 Bedrohungssintelligenz	101
	A-5.8 Informationssicherheit im Projektmanagement	103
	A-5.9 Inventar der Informationen und anderen damit verbundenen Werten	104
	A-5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten	108
	A-5.11 Rückgabe von Werten	111
	A-5.12 Klassifizierung von Information	112
	A-5.13 Kennzeichnung von Information	115
	A-5.14 Informationsübertragung	116
	A-5.15 Zugangssteuerung	119
	A-5.16 Identitätsmanagement	123
	A-5.17 Informationen zur Authentifizierung	124
	A-5.18 Zugangsrechte	126
	A-5.19 Informationssicherheit in Lieferantenbeziehungen	127
	A-5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen	129
	A-5.21 Umgang mit der Informationssicherheit in der IKT-Lieferkette	132

A-5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen	132
A-5.23 Informationssicherheit für die Nutzung von Cloud-Diensten	133
A-5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen	135
A-5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse	135
A-5.26 Reaktion auf Informationssicherheitsvorfälle	135
A-5.27 Erkenntnisse aus Informationssicherheitsvorfällen	135
A-5.28 Sammeln von Beweismaterial	135
A-5.29 Informationssicherheit bei Störungen	137
A-5.30 IKT-Bereitschaft für Business Continuity	139
A-5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen	140
A-5.32 Geistige Eigentumsrechte	142
A-5.33 Schutz von Aufzeichnungen	143
A-5.34 Datenschutz und Schutz personenbezogener Daten	145
A-5.35 Unabhängige Überprüfung der Informationssicherheit	147
A-5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit	148
A-5.37 Dokumentierte Betriebsabläufe	149
3.4 Controls betreffend Personal (Gruppe 6)	151
A-6.1 Sicherheitsüberprüfung	151
A-6.2 Beschäftigungs- und Vertragsbedingungen	152
A-6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung	153
A-6.4 Maßregelungsprozess	155
A-6.5 Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung	156
A-6.6 Vertraulichkeits- oder Geheimhaltungsvereinbarungen	157
A-6.7 Telearbeit	158
A-6.8 Melden von Informationssicherheitereignissen	162
3.5 Controls betreffend Infrastruktur (Gruppe 7)	163
A-7.1 Physische Sicherheitsperimeter	163
A-7.2 Physischer Zutritt	164
A-7.3 Sichern von Büros, Räumen und Einrichtungen	166
A-7.4 Physische Sicherheitsüberwachung	167
A-7.5 Schutz vor physischen und umweltbedingten Bedrohungen	168
A-7.6 Arbeiten in Sicherheitsbereichen	168
A-7.7 Aufgeräumte Arbeitsumgebung und Bildschirmsperren	169
A-7.8 Platzierung und Schutz von Geräten und Betriebsmitteln	171

A-7.9 Sicherheit von Werten außerhalb der Räumlichkeiten	172
A-7.10 Speichermedien	173
A-7.11 Versorgungseinrichtungen	176
A-7.12 Sicherheit der Verkabelung	178
A-7.13 Instandhaltung von Geräten und Betriebsmitteln	179
A-7.14 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	180
3.6 Technologische Controls (Gruppe 8)	181
A-8.1 Endpunktgeräte des Benutzers	182
A-8.2 Privilegierte Zugangsrechte	185
A-8.3 Informationszugangsbeschränkung	185
A-8.4 Zugriff auf Quellcode	188
A-8.5 Sichere Authentifizierung	190
A-8.6 Kapazitätssteuerung	192
A-8.7 Schutz gegen Schadsoftware	193
A-8.8 Handhabung von technischen Schwachstellen	195
A-8.9 Konfigurationsmanagement	197
A-8.10 Löschung von Informationen	198
A-8.11 Datenmaskierung	200
A-8.12 Verhinderung von Datenlecks	201
A-8.13 Sicherung von Information	202
A-8.14 Redundanz von informationsverarbeitenden Einrichtungen	204
A-8.15 Protokollierung	206
A-8.16 Überwachung von Aktivitäten	209
A-8.17 Uhrensynchronisation	211
A-8.18 Gebrauch von Hilfsprogrammen mit privilegierten Rechten	212
A-8.19 Installation von Software auf Systemen im Betrieb	213
A-8.20 Netzwerksicherheit	216
A-8.21 Sicherheit von Netzwerkdiensten	220
A-8.22 Trennung von Netzwerken	221
A-8.23 Webfilterung	223
A-8.24 Verwendung von Kryptografie	224
A-8.25 Lebenszyklus einer sicheren Entwicklung	226
A-8.26 Anforderungen an die Anwendungssicherheit	228
A-8.27 Sichere Systemarchitektur und technische Grundsätze	229
A-8.28 Sichereres Coding	231
A-8.29 Sicherheitsprüfung in Entwicklung und Abnahme	232
A-8.30 Ausgegliederte Entwicklung	233
A-8.31 Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen	234
A-8.32 Änderungssteuerung	235

A-8.33 Prüfinformationen	237
A-8.34 Schutz der Informationssysteme während der Überwachungsprüfung	238
Literatur	239
4 Fahrplan zur Umstellung auf die neue Norm	241
4.1 Fahrplan für den Hauptteil der ISO 27001	241
4.2 Fahrplan für den Anhang A und seine Controls	245
5 Anwendungsfall: Kritische Infrastrukturen	253
5.1 Die IT-Sicherheitsgesetze und ihre Umsetzung	253
5.2 Anmerkungen zum Stand der Technik	260
Literatur	263
Stichwortverzeichnis	265