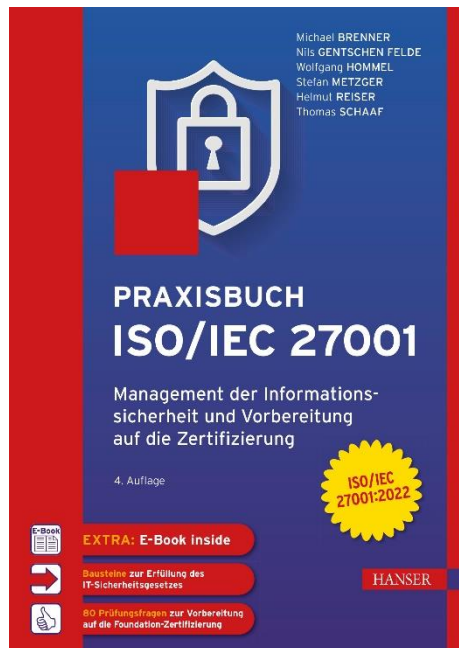


HANSER



Leseprobe

zu

Praxisbuch ISO/IEC 27001

von Michael Brenner, Nils gentschen Felde, Wolfgang Hommel, Stefan Metzger, Helmut Reiser und Thomas Schaaf

Print-ISBN: 978-3-446-47395-9

E-Book-ISBN: 978-3-446-47458-1

E-Pub-ISBN: 978-3-446-47615-8

Weitere Informationen und Bestellungen unter

<https://www.hanser-kundencenter.de/fachbuch/artikel/9783446473959>

sowie im Buchhandel

© Carl Hanser Verlag, München

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

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 ver- bundenen 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 Informations- sicherheitsvorfällen	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

Vorwort

Liebe Leserinnen und Leser,

dieses Buch ist dafür konzipiert, Sie auf Basis des Wortlauts der internationalen Norm ISO/IEC 27001 in das Thema Informationssicherheitsmanagementsysteme einzuführen, auf eine Personenzertifizierung vorzubereiten und als Nachschlagewerk zu dienen.

Im Jahr 2022 haben sich im wichtigen Anhang A der internationalen ISO/IEC 27001 größere Veränderungen ergeben, deren Überführung in die deutsche DIN ISO/IEC 27001 zum Zeitpunkt der Drucklegung der vorliegenden vierten Auflage dieses Buchs noch in Arbeit sind. Kapitel 4 des Buchs enthält den deutschen Wortlaut der DIN ISO/IEC 27001:2017, da die entsprechenden Teile in der englischen Norm bis auf kleine textuelle Ergänzungen, die wir berücksichtigt haben, nicht verändert wurden. Anhang B.1 enthält die deutsche Fassung der Norm ISO/IEC 27001 vollständig und im Original-Wortlaut und -Layout. Für die noch nicht offiziell übersetzten veränderten Teile der Norm, also den Anhang A, liefern wir in Kapitel 5 des Buchs zusätzlich eigene deutsche Fachübersetzungen, sowie in Anhang B.3 einen tabellarischen Überblick über alle aktuellen Maßnahmen (Controls), damit Sie sowohl mit dem englischen Original als auch einem deutschen Text arbeiten können.

Das erste Kapitel führt Sie kompakt in die spannende, aber auch komplexe Welt der Informationssicherheit, Managementsysteme und Standards ein. Nach einem Überblick über die Reihe der ISO/IEC 27000-Standards und die Grundlagen von Informationssicherheitsmanagementsystemen finden Sie in den Kapiteln 4 und 5 alle Anforderungen und Maßnahmen aus ISO/IEC 27001. Sie werden in grau hinterlegten Boxen wörtlich wiedergegeben und zusätzlich erläutert. Die Schwerpunkte der Erklärungen orientieren sich an den Inhalten der Prüfungen zu den Foundation-Lehrgangskonzepten u. a. von APMG, ICO und TÜV Süd Akademie; das Buch ist aber auch für die Vorbereitung auf die Prüfung in einem der anderen Qualifizierungsprogramme nach ISO/IEC 27001 verwendbar. Ferner finden Sie in diesem Buch insgesamt 80 Beispiel-Prüfungsfragen. Ihr Format und Schwierigkeitsgrad entspricht dem der ISO/IEC 27001 Foundation-Prüfung der TÜV Süd Akademie mit genau einer richtigen Antwort pro Frage. Die Hälfte der Fragen finden Sie über die Kapitel 2–7 verteilt jeweils am Ende, wo auch die wichtigsten Inhalte nochmals kompakt zusammengefasst werden. Im Anhang finden Sie dann nochmals 40 Fragen am Stück. Dies entspricht dem Umfang der „richtigen“ Prüfung. Dadurch können Sie ein Gespür für die 60 Minuten Prüfungszeit entwickeln.

Wir wünschen Ihnen viel Erfolg bei der Prüfung und bei der praktischen Anwendung!

München, im September 2022

Die Autoren

1

Einführung und Basiswissen

Nachdem das Thema Informationssicherheit einige Jahrzehnte lang ein gewisses Nischendasein gefristet hat, gewinnt es in den letzten Jahren massiv an Bedeutung. Das hängt nicht zuletzt mit einem steigenden öffentlichen Bewusstsein für die Sicherheit und den Schutz von Daten und Informationen zusammen. Auch die mediale Aufmerksamkeit ist einem Unternehmen sicher, wenn sich beispielsweise herausstellt, dass es nachlässig mit seinen Kundendaten umgeht, oder wenn sicherheitsrelevante Vorfälle zu Ausfällen mit großer geschäftlicher Auswirkung führen.

Der Gesetzgeber hat mit dem IT-Sicherheitsgesetz und entsprechenden Verordnungen kritische Infrastrukturen definiert. Für diese wurden höhere rechtliche Anforderungen im Hinblick auf die IT-Sicherheit erlassen und die Betreiber verpflichtet, angemessene organisatorische und technische Vorkehrungen für die IT-Sicherheit zu treffen und dabei den Stand der Technik einzuhalten.

Wenn sich eine Organisation heute vornimmt, einen strukturierten Ansatz zum wirksamen Management der Informationssicherheit einzuführen, kommt sie an der Standardreihe ISO/IEC 27000 praktisch nicht vorbei. Bei ISO/IEC 27000 handelt es sich um eine Reihe von Dokumenten, in denen verschiedene Aspekte des Informationssicherheitsmanagements betrachtet werden. Dass es sich um von der ISO (International Organization for Standardization) und der IEC (International Electrotechnical Commission) standardisierte Dokumente handelt, erhöht dabei die Verbreitung, Bedeutung und Akzeptanz dieser Standards ganz maßgeblich. Das zentrale und wichtigste Dokument der Reihe ist dabei ISO/IEC 27001.

■ 1.1 Worum geht es in ISO/IEC 27001?

Die Standardfamilie ISO/IEC 27000 befasst sich hauptsächlich mit drei Kernbereichen:

1. **Begriffe:** Es werden die wichtigsten Fachbegriffe aus der Welt der Informationssicherheit definiert.
2. **Grundlegendes Managementsystem:** Es wird beschrieben, was eine Organisation umzusetzen hat und sicherstellen muss, um die eigenen Aktivitäten und Maßnahmen im Bereich Informationssicherheit wirksam steuern zu können.

3. **Maßnahmen:** Es werden Maßnahmen beschrieben, die eine Organisation grundsätzlich umzusetzen hat, um ein hohes Maß an Informationssicherheit gewährleisten zu können.

Dieses Buch bietet einen Überblick über alle drei Bereiche. Während die beiden letzteren in späteren Kapiteln behandelt werden, beschäftigt sich dieses Kapitel zunächst mit der Begriffsbildung.

■ 1.2 Begriffsbildung

Die Standardfamilie ISO/IEC 27000 dient ganz wesentlich dazu, die Verwendung von Fachbegriffen zu vereinheitlichen. Nur so kann erreicht werden, dass diejenigen, die sich mit Informationssicherheitsmanagement beschäftigen, nicht aneinander vorbeireden, obwohl sie eigentlich inhaltlich dasselbe meinen.

Im Folgenden werden die wichtigsten Begriffe und Grundlagen rund um das Thema Informationssicherheit vorgestellt, die zum Verständnis der ISO/IEC 27000 Standards erforderlich sind.

1.2.1 Informationen

In unserer inzwischen hochgradig vernetzten Welt sind Informationen Werte, die von entscheidender Wichtigkeit für den Geschäftsbetrieb einer Organisation sind. Dabei sind diese Informationen einer stark zunehmenden Zahl von Bedrohungen ausgesetzt. Informationssysteme, Netze und Organisationen sind dabei beispielsweise durch Cyber-Angriffe (Ransomware, Denial-of-Service-Angriffe, Hacking, Spam etc.), Sabotage, Spionage und Vandalismus, aber auch Elementarschäden durch Wasser, Feuer sowie Katastrophen und andere Gefahren gefährdet. Gesetzliche Regelungen (wie z. B. das IT-Sicherheitsgesetz oder die Datenschutz-Grundverordnung) fordern entsprechend Schutzmaßnahmen für sensible Informationen.

Der Begriff „Informationen“ wird hierbei sehr weit gefasst. Sie können in Form verschiedener Medien vorliegen: geschrieben, gedruckt, elektronisch, als Film etc., und auf unterschiedlichen Wegen übermittelt werden, z. B. per Post, per Funk, über das Internet usw. Unabhängig vom Medium und vom Übertragungsweg ist die Aufgabe der Informationssicherheit, diese Informationen angemessen vor der zunehmenden Zahl von Bedrohungen zu schützen. Nur so können die Risiken minimiert, der Geschäftsbetrieb gesichert und die Wettbewerbsfähigkeit, Rentabilität sowie die Chancen einer Organisation maximiert werden.

1.2.2 Informationssicherheit

Für die Informationssicherheit existiert, anders als beispielsweise für Gewichte, Längen oder Temperaturen, keine physikalische Maßeinheit, um sie einfach in Zahlen – also *quantitativ* – auszudrücken. Deshalb wählen die Standards der Reihe ISO/IEC 27000 – und damit auch das Hauptdokument ISO/IEC 27001 – einen praxisbewährten *qualitativen* Ansatz

über Schutzziele. Diese werden nachfolgend im Einzelnen vorgestellt und genauer erläutert.

1.2.3 Sicherheitsanforderungen und Schutzziele

Die Gefährdung wichtiger Informationen lässt sich alleine mit Beispielen natürlich nur ungenau und unvollständig fassen. In der ISO/IEC 27000 und im Security Engineering werden deshalb abstrakte Schutzziele bzw. Sicherheitsanforderungen für Informationswerte (zum Begriff der „(Informations-)Werte“ vgl. Kapitel 3.1.1) definiert. Die zentralen Schutzziele sind Vertraulichkeit, Integrität und Verfügbarkeit (engl. *Confidentiality, Integrity and Availability*, als Eselsbrücke gerne mit „CIA“ abgekürzt) von Informationen. Andere wünschenswerte Eigenschaften, deren Aufrechterhaltung nach ISO/IEC 27000 ebenfalls Gegenstand der Informationssicherheit sein können, sind Authentizität, Zurechenbarkeit, Nichtabstreitbarkeit und Verlässlichkeit (engl. *Authenticity, Accountability, Non-repudiation and Reliability*). Diese Schutzziele, auf denen der Informationssicherheitsbegriff der Standardfamilie ISO/IEC 27000 basiert, werden im Folgenden erläutert.

Zur Beschreibung von Angriffsszenarien und Sicherheitsmaßnahmen werden oft fiktive Personen verwendet. Diese Personen haben definierte Rollen und Namen. Die „Guten“ heißen immer Alice und Bob und versuchen in der Regel, miteinander zu kommunizieren. Der „Böse“ (engl. *malicious*) heißt Mallet; er versucht, Alice, Bob oder deren Interaktionen oder Kommunikation anzugreifen, abzuhören oder zu stören. Im Folgenden werden Alice, Bob und Mallet in diesem Sinn verwendet, um die Verletzung von Schutzziele zu verdeutlichen.

1.2.3.1 Vertraulichkeit (Confidentiality)

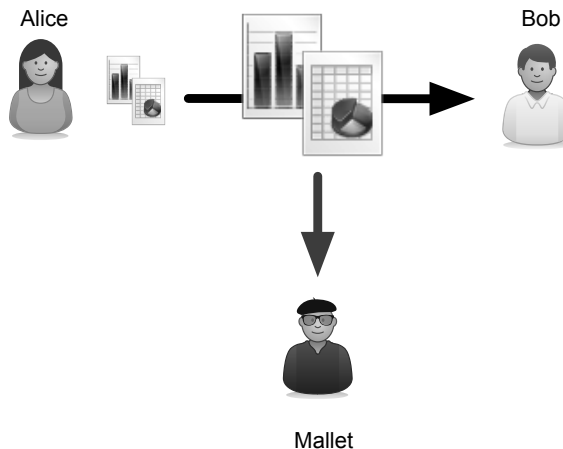


Abbildung 1.1 Verletzung der Vertraulichkeit durch Abhören

Die Vertraulichkeit bezeichnet die Eigenschaft, dass eine Information für unautorisierte Personen, Entitäten oder Prozesse nicht zugänglich ist und von diesen auch nicht offen-

5

Maßnahmen im Rahmen des ISMS

Im normativen Anhang A *Referenzmaßnahmen* (vgl. S. 209) beschreibt ISO/IEC 27001 eine sehr umfangreiche Reihe von Maßnahmen, deren Umsetzung zur Reduzierung der Risiken für die Informationssicherheit beiträgt. Trotz des Umfangs ist diese Maßnahmenliste nicht vollständig; jede Organisation muss sich deshalb auch überlegen, welche weiteren Maßnahmen in ihrem konkreten Fall benötigt werden. Die Maßnahmen wurden ursprünglich aus den Abschnitten 5 bis 15 der Norm ISO/IEC 17799 abgeleitet, woraus sich auch die Nummerierung des Anhangs A von ISO/IEC 27001 beginnend mit A.5 ergibt. In der aktuellen Version der Norm wurde die Anzahl der Abschnitte drastisch auf nur noch vier reduziert. In der ersten Version von ISO/IEC 27001 waren es elf und dann 14. Die Kapitel von ISO/IEC 27002 orientieren sich auch an dieser Struktur und Reihenfolge. Auch die Anzahl der Maßnahmen wurde von 114 auf 93 konsolidiert.

In diesem Kapitel gehen wir auf alle in Anhang A von ISO/IEC 27001 aufgeführten Maßnahmen ein. Einige Maßnahmen sind dabei ausführlicher beschrieben als andere. Das bedeutet **nicht**, dass sie theoretisch oder in der Praxis wichtiger sind als die anderen, sondern spiegelt vielmehr die Schwerpunkte des ISO/IEC 27001 Foundation-Kurses wider. Zu ausgewählten Maßnahmen werden in Anlehnung an ISO/IEC 27002 jeweils auch praktische Beispiele zur Umsetzung gegeben.

Die ISO/IEC 27000-Normenreihe fasst die Maßnahmen in vier Kategorien zusammen (vgl. Abbildung 5.1). Nachfolgend werden die einzelnen Kategorien in der Reihenfolge, wie sie auch in ISO/IEC 27001 genannt sind, besprochen:

Anhang	Bezeichnung	ab Seite
A.5	Organisatorische Maßnahmen	74
A.6	Menschen	99
A.7	Physische Maßnahmen	106
A.8	Technische Maßnahmen	118

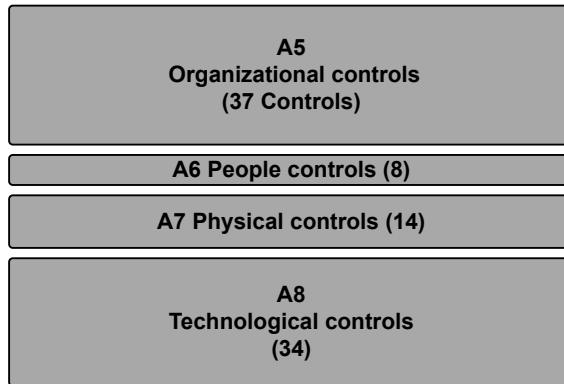


Abbildung 5.1 Struktur der Maßnahmen aus Anhang A von ISO/IEC 27001

■ 5.1 A.5 Organizational Controls – Organisatorisches Maßnahmen

5.1.1 A.5.1 Informationssicherheitsrichtlinien

Anforderungen: Eine Informationssicherheitsrichtlinie und themenspezifische Richtlinien müssen definiert, vom Topmanagement genehmigt, veröffentlicht, an relevante Mitarbeitende und andere interessierte Parteien kommuniziert und von diesen zur Kenntnis genommen sowie in geplanten Abständen und bei wesentlichen Änderungen überprüft werden.



Control Policies for information security according to ISO/IEC 27001:2022: Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

Korrespondiert mit **DIN EN ISO/IEC 27001:2017:**

A.5.1.1 Informationssicherheitsrichtlinien

A.5.1.2 Überprüfung der Informationssicherheitsrichtlinien

Wie bereits in Kapitel 3.1.2 und Kapitel 4.5.2 erläutert, sind die mit dem ISMS verbundenen Zielsetzungen – die Informationssicherheitspolitik der Organisation – von der höchsten Ebene des Managements der Organisation zu definieren. Dokumentiert wird dies in einer übergeordneten Informationssicherheitsrichtlinie, die eine organisationsweit kommunizierte Absichtserklärung des Topmanagements darstellt.

Berücksichtigt werden sollten in der übergeordneten Richtlinie allgemeine ISMS-Ziele und -Prinzipien (z. B. risikobasierter Ansatz, Schutz von Werten, kontinuierliche Verbesserung), aber auch vertragliche und gesetzliche Rahmenbedingungen sowie Strategien und allge-

meine Ziele der Organisation. Die Richtlinie ist auch eine gute Stelle, um übergreifende Verantwortlichkeiten für die Informationssicherheit und deren Management zu definieren.

Die übergeordnete Informationssicherheitsrichtlinie (oder auch: ISMS-Richtlinie) wird durch themenspezifische Richtlinien ergänzt.

Themen für spezifische Richtlinien können beispielsweise sein:

- Umgang mit Informationen und Werten bzw. Assets (siehe Kapitel 5.1.10)
- Informationsklassifizierung (siehe Kapitel 5.1.12)
- Übertragung von Informationen (siehe Kapitel 5.1.14)
- Zugangssteuerung und Zugangsberechtigungen (siehe Kapitel 5.1.15 und 5.1.18)
- Lieferantenbeziehungen (siehe Kapitel 5.1.19)
- Verwendung von Clouddiensten (siehe Kapitel 5.1.23)
- Schutz der Rechte an geistigem Eigentum (siehe Kapitel 5.1.32)
- Umgang mit Aufzeichnungen (siehe Kapitel 5.1.33)
- Privatsphäre und Schutz personenbezogener Daten (siehe Kapitel 5.1.34)
- Home Office und Remote-Arbeiten (siehe Kapitel 5.2.7)
- Aufgeräumte Schreibtische und Gerätesperren (clear desk and clear screen) (siehe Kapitel 5.3.7)
- Mobile Speichermedien (siehe Kapitel 5.3.10)
- Anwender-Endgeräte (siehe Kapitel 5.4.1)
- Management technischer Schwachstellen und Kommunikation dieser (siehe Kapitel 5.4.8)
- Aufbewahrung und Löschung von Informationen (siehe Kapitel 5.4.10)
- Datensicherung und Backups (siehe Kapitel 5.4.13)
- Protokollierung und Umgang mit Log-Files (siehe Kapitel 5.4.15)
- Einsatz von Kryptographie (siehe Kapitel 5.4.24)

Die themenspezifischen Richtlinien müssen nicht notwendigerweise von der obersten Leitung erlassen und freigegeben werden; dies kann auf einer niedrigeren, der Regelung des jeweiligen Themas angemessenen Ebene geschehen.

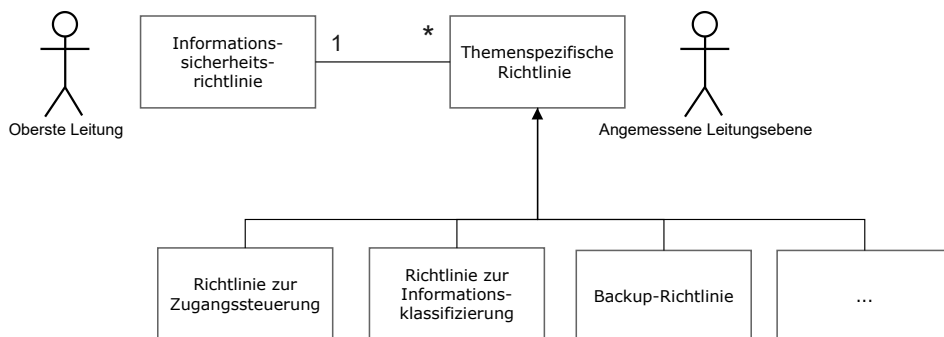


Abbildung 5.2 Informationssicherheitsrichtlinie und themenspezifische Richtlinien

Richtlinien adressieren meist nicht nur einen kleinen Kreis von Spezialisten, sondern ein relativ breites Publikum innerhalb (und teilweise auch außerhalb) der Organisation. Sie

sollten immer relativ kurz gehalten werden sowie prägnant und verständlich formuliert sein. Regelungen zu Details finden gegebenenfalls ihren Platz besser in anderen Vorgabedokumenten wie Prozess- und Verfahrensdefinitionen, Arbeitsanweisungen und Ähnlichem.

Richtlinien sind allen maßgeblichen Parteien zu kommunizieren. Dabei ist natürlich darauf zu achten, dass es hierbei nicht zu einer unnötigen Verbreitung vertraulicher Informationen außerhalb der Organisation kommt.

Richtlinien als übergeordnete Zielvorgaben ändern sich in der Regel seltener als Prozess- und Verfahrensdefinitionen und andere konkretere Vorgabedokumente. Dennoch müssen auch sie einer regelmäßigen Überprüfung unterzogen und kontinuierlich weiter entwickelt werden. Für die Überprüfung, Weiterentwicklung und Freigabe der verschiedenen Richtlinien sollten jeweils geeignete Verantwortlichkeiten definiert und zugewiesen werden. Eine Überprüfung einer Richtlinie sollte spätestens in einem festgelegten Abstand (z. B. jährlich) erfolgen. Auch wenn sich neue Erkenntnisse oder Erfordernisse – z. B. aus Managementbewertungen, Audits, Änderungen im Geschäftsumfeld, neuen Gefahrenlagen oder der Analyse von Informationssicherheitsvorfällen – ergeben, kann eine Überprüfung angezeigt sein.

5.1.2 A.5.2 Rollen und Verantwortlichkeiten für die Informationssicherheit

Anforderungen: Die Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit müssen entsprechend den Erfordernissen der Organisation definiert und zugewiesen werden.



Control **Information security roles and responsibilities** according to ISO/IEC 27001:2022:

Information security roles and responsibilities shall be defined and allocated according to the organization needs. ■

Korrespondiert mit **DIN EN ISO/IEC 27001:2017:**

A.6.1.1 Informationssicherheitsrollen und -verantwortlichkeiten

Die wirksame Wahrnehmung von Verantwortlichkeiten im Kontext der Informationssicherheit ist die Basis für deren Erhalt und Management. Wichtig ist also, dass eine angemessene Struktur von Rollen und Funktionen mit zugewiesenen Verantwortlichkeiten (man sagt manchmal auch: eine Informationssicherheitsorganisation) definiert und innerhalb der Gesamtorganisation bekannt ist.

Die Rollen sollten so definiert sein, dass die Verantwortlichkeiten beim Schutz von Werten, bei der Ausführung der Informationssicherheitsprozesse sowie im Risikomanagement eindeutig festgelegt sind – bei Letzterem speziell auch die Rolle des Risikoeigentümers (vgl. Kapitel 4.6.1.2 und 4.6.1.3).

Für alle Rollen ist ihre jeweilige Verantwortung sowie ihre Zuweisung an eine konkrete Person, Funktion oder Stelle in der Organisation zu dokumentieren. Es empfiehlt sich, die Verantwortung für die übergreifende Koordination des Managements der Informations-

sicherheit einer Person bzw. Stelle zuzuweisen, welche diese Rolle als ihre Hauptfunktion erfüllt. Diese Rolle bzw. Funktion wird in der Praxis unterschiedlich benannt – gängige Bezeichnungen sind z. B. Chief Information Security Officer (CISO), Informationssicherheitsbeauftragte(r), Information Security Officer oder ISMS-Beauftragte(r).

5.1.3 A.5.3 Aufgabentrennung

Anforderungen: Die Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit müssen entsprechend den Erfordernissen der Organisation definiert und zugewiesen werden.



Control **Segregation of duties** according to ISO/IEC 27001:2022:
Information security roles and responsibilities shall be defined and allocated according to the organization needs.

Korrespondiert mit **DIN EN ISO/IEC 27001:2017:**

A.6.1.2 Aufgabentrennung

Bei der Zuweisung von Verantwortlichkeiten und Pflichten – im ISMS selbst, aber auch in anderen relevanten Bereichen wie z. B. der IT-Administration – sollte auf eine angemessene Trennung von Aufgaben geachtet werden.

Mit der Aufgabentrennung wird das Risiko eines Missbrauchs, sei er irrtümlich oder vorsätzlich, minimiert. Ein Ziel kann hierbei beispielsweise sein, dass Werte mit hohem Schutzbedarf nur unter Einhaltung eines Vieraugenprinzips verwendet und modifiziert werden dürfen.

Für kleine Organisationen, in denen eine Aufgabentrennung in allen Bereichen nur schwer umsetzbar ist, können andere Maßnahmen wie Überwachung der Tätigkeiten, Prüfpfade und Leitungsaufsicht etabliert werden.

5.1.4 A.5.4 Verantwortung des Topmanagements

Anforderungen: Das Topmanagement muss alle Mitarbeitenden verpflichten, die Informationssicherheit in Übereinstimmung mit der Informationssicherheitsrichtlinie, themenspezifischen Richtlinien und Verfahren der Organisation aufrechtzuerhalten.

Control **Management responsibilities** according to ISO/IEC 27001:2022:
Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.

Korrespondiert mit **DIN EN ISO/IEC 27001:2017:**

A.7.2.1 Verantwortlichkeiten der Leitung

Das Engagement der obersten Leitung ist ein kritischer Erfolgsfaktor für ein wirksames ISMS. Insbesondere sollte die Leitung bei der Informationssicherheit innerhalb der Or-

ganisation eine Vorbildfunktion erfüllen. Sie muss die Informationssicherheit aktiv fördern sowie unterstützen und dafür sorgen, dass die Beschäftigten über ihre Rollen, Verantwortlichkeiten und über die Richtlinien, Regeln, Maßnahmen und Verfahren Bescheid wissen. Das Bewusstsein für Informationssicherheit sollte gestärkt und die Beschäftigten dafür auch motiviert und kontinuierlich weitergebildet werden (siehe auch Kapitel 5.2.3).

5.1.5 A.5.5 Kontakt zu Behörden

Anforderungen: Die Organisation muss den Kontakt zu den zuständigen Behörden herstellen und aufrechterhalten.



Control **Contact with authorities** according to ISO/IEC 27001:2022:
The organization shall establish and maintain contact with relevant authorities.

Korrespondiert mit **DIN EN ISO/IEC 27001:2017:**

A.6.1.3 Kontakt mit Behörden

Oft auch auf regelmäßiger Basis, insbesondere aber in besonderen Situationen wie beim Umgang mit schweren Informationssicherheitsvorfällen (vgl. Kapitel 5.1.24), ist eine angemessene Kommunikation mit Behörden notwendig.

Bereits vor einem solchen Kontakt werden Verfahren und Verantwortlichkeiten bestimmt und dokumentiert, die festlegen, wer wann mit welchen Behörden kommuniziert. Dies betrifft z. B. Strafverfolgungsbehörden oder auch Aufsichtsbehörden. Dabei ist auch festzulegen, wer berechtigt ist, Informationen über Sicherheitsvorfälle an Externe weiterzugeben und in welcher Art die Weitergabe solcher Informationen erfolgt. Gegebenenfalls besteht durch gesetzliche und behördliche Auflagen (vgl. Kapitel 1.3) sogar eine gesetzliche Verpflichtung zur Meldung.

5.1.6 A.5.6 Kontakt zu speziellen Interessengruppen

Anforderungen: Die Organisation muss Kontakte zu speziellen Interessengruppen oder sonstigen sicherheitsorientierten Expertenforen und Fachverbänden herstellen und pflegen.

Control **Contact with special interest groups** according to ISO/IEC 27001:2022:
The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations

Korrespondiert mit **DIN EN ISO/IEC 27001:2017:**

A.6.1.4 Kontakt mit speziellen Interessensgruppen

Ein Austausch mit anderen Organisationen zum Thema Informationssicherheit kann vielfältige Vorteile haben. Mitgliedschaften in Interessengruppen können dazu dienen, besser über den aktuellen Stand allgemeiner und sektorspezifischer Gefährdungen sowie Good Practices informiert zu sein. Es können auch Vereinbarungen zur Kooperation und Koor-

eines Lesezugriffs, der mitunter auch auf zuvor erstellte Kopien von Systemdateien erfolgt, die im Anschluss an die Tests wieder gelöscht werden.

■ 5.5 Beispiele für Prüfungsfragen zu diesem Kapitel

Nachfolgend finden Sie Beispiele für Prüfungsfragen, die sich thematisch mit den in diesem Kapitel erlernten Inhalten auseinandersetzen. Die richtigen Antworten inklusive Erläuterungen und Verweisen befinden sich in Anhang C.1 ab Seite 240.



Prüfungsfrage 5.22:

Durch welche Maßnahme gemäß Anhang A aus ISO/IEC 27001 wird am ehesten vermieden, dass beispielsweise Entwickler von Software versehentlich oder absichtlich produktive Systeme kompromittieren?

- A) Sichere Authentifizierung
- B) Redundanz informationsverarbeitender Systeme
- C) Trennung von Netzen
- D) Trennung von Entwicklungs-, Test- und Produktivumgebungen

Prüfungsfrage 5.23:

Welche der folgenden Aspekte und Anforderungen sind im Zusammenhang mit Betriebsmitteln und unterstützenden Versorgungseinrichtungen *nicht* Teil der Maßnahmen zur physischen Sicherheit gemäß Abschnitt A.7 in ISO/IEC 27001?

- A) Betriebsmittel müssen sicher und geschützt platziert werden.
- B) Die Konfigurationen, einschließlich der Sicherheitskonfigurationen, von Hardware, Software, Diensten und Netzwerken müssen festgelegt, dokumentiert, umgesetzt, überwacht und überprüft werden.
- C) Kabel zur Stromversorgung, Datenübertragung oder Anbindung an Informationsdienste müssen vor Abhören, Manipulation oder Beschädigung geschützt werden.
- D) Betriebsmittel müssen sachgerecht gewartet werden, um die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen zu gewährleisten.



Prüfungsfrage 5.24:

Was muss gemäß Maßnahme A.6.5 aus ISO/IEC 27001 im Zusammenhang mit Beendigung oder Wechsel des Beschäftigungsverhältnisses festgelegt werden?

- A) Kennungen der Nutzerendgeräte, die nach Beendigung oder Wechsel des Beschäftigungsverhältnisses zurückgegeben werden müssen
- B) Verantwortlichkeiten und Pflichten im Zusammenhang mit der Informationssicherheit, die nach Beendigung oder Wechsel des Beschäftigungsverhältnisses fortbestehen
- C) Verträge, die nach Beendigung oder Wechsel des Beschäftigungsverhältnisses neu ausgehandelt werden müssen
- D) Gültigkeitsdauer von digitalen Identitäten, Benutzerkennungen und Zertifikaten, die auch nach Beendigung oder Wechsel des Beschäftigungsverhältnisses noch verwendet werden

Prüfungsfrage 5.25:

Wobei handelt es sich um eine technische Maßnahme gemäß ISO/IEC 27001, Anhang A.8?

- A) Aufgabentrennung
- B) Screening
- C) Datensicherung
- D) Remote-Arbeiten

Prüfungsfrage 5.26:

Was ist Gegenstand der Maßnahme *Überwachungsaktivitäten (A.8.16)* gemäß Anhang A in ISO/IEC 27001?

- A) Überwachung des Personals im Hinblick auf vorsätzliche Verletzungen der Informationssicherheit
- B) Überwachung des Umsetzungsstands von Maßnahmen zur Risikobehandlung
- C) Überwachung von Netzen, Systemen und Anwendungen im Hinblick auf Anomalien
- D) Überwachung von Sicherheitsbereichen mithilfe von Videokameras

Prüfungsfrage 5.27:

Wobei handelt es sich um eine organisatorische Maßnahme gemäß ISO/IEC 27001, Anhang A.5?

- A) Aufgeräumter Schreibtisch und Gerätesperre
- B) Schutz vor Schadsoftware
- C) Reaktion auf Informationssicherheitsvorfälle
- D) Einsatz von Kryptographie

7

Zertifizierungsmöglichkeiten nach ISO/IEC 27000

Im Kontext von ISO/IEC 27000 gibt es zwei grundsätzlich verschiedene Arten der Zertifizierung. Zunächst kann natürlich das ISMS einer Organisation nach ISO/IEC 27001 zertifiziert werden – diese Möglichkeit zu schaffen, war ja in der Entstehungsgeschichte der ISO/IEC 27000 der wesentliche Grund für die Ergänzung des Leitfadens für Informationssicherheitsmanagement (ISO/IEC 17799 bzw. ISO/IEC 27002) um die normativen Anforderungen in ISO/IEC 27001.

Daneben gibt es die Personenzertifizierungen, die keine Zertifizierungen nach der Norm ISO/IEC 27001 darstellen, sondern Personen ermöglichen, ihr Wissen und ihre Qualifikationen hinsichtlich der Inhalte und der Anwendung der ISO/IEC 27000-Standardfamilie nachzuweisen.

■ 7.1 ISMS-Zertifizierung nach ISO/IEC 27001

Die Zertifizierung des ISMS ermöglicht es einer Organisation, ihre Fähigkeit, ein effektives Informationssicherheitsmanagement zu betreiben, gegenüber bestehenden und zukünftigen Kunden, Aufsichtsbehörden oder anderen interessierten Parteien nachzuweisen.

7.1.1 Grundlagen der Zertifizierung von Managementsystemen

Nachfolgend werden die Begriffe Zertifizierung und Akkreditierung erläutert, die im Zusammenhang mit Konformitätsbewertungen von Managementsystemen wichtig sind.

7.1.1.1 Zertifizierung

Zum Erreichen einer *Zertifizierung* eines Managementsystems ist ein externes, von einer akkreditierten Zertifizierungsstelle beauftragtes Audit (vgl. Kapitel 4.9.2 ab Seite 63) zwingend notwendig. Im Rahmen dieses sogenannten Zertifizierungsaudits wird die Einhaltung der Anforderungen des Standards, d. h. die Konformität des Managementsystems zum Standard, überprüft und bewertet.

Welche Bereiche der Organisation dabei auditiert werden, ergibt sich auf Basis des erklärten Anwendungsbereichs des Managementsystems (*Scoping Statement*). Welche Maßnahmen auditiert werden, leitet sich aus der Erklärung zur Anwendbarkeit des Standards (*Statement of Applicability*), s. a. Kapitel 4.4.3 und 4.6.1.3, ab. Die Angemessenheit dieser Erklärung und der dort festgelegten Ausschlüsse wird selbstverständlich überprüft. Die Anforderungen aus den Kapiteln 4 bis 10 der Norm sind in einem Zertifizierungsaudit immer Teil der Auditkriterien.

Im Nachgang eines Audits wird ein Auditbericht erstellt. Dieser enthält die im Audit getroffenen Feststellungen, welche in verschiedene Kategorien – z. B. positiver Aspekt, Verbesserungspotenzial, Nebenabweichung, (Haupt-)Abweichung – eingeteilt sind. Sind während des Audits keine (Haupt-)Abweichungen festgestellt worden, d. h. keine Defizite, welche die Wirksamkeit des ISMS infrage stellen, wird als Auditschlussfolgerung vom Audit-Team die Ausstellung des Zertifikats empfohlen werden. In diesem Fall wird die Zertifizierungsstelle das Zertifikat nach einer Überprüfung der vom Audit-Team eingereichten Unterlagen ausstellen.

7.1.1.2 Akkreditierung

Auch an die Organisationen, die Managementsysteme zertifizieren, werden Anforderungen gestellt. Die Erfüllung dieser Anforderungen wird von einer Akkreditierungsstelle überprüft.

Vereinfacht ausgedrückt ist eine Akkreditierung eine Art Zertifizierung der Zertifizierer. Obwohl die Worte Akkreditierung und Zertifizierung häufig synonym verwendet werden, sind es genau genommen unterschiedliche Dinge: Eine Zertifizierung bestätigt die Konformität zu einem Standard, eine Akkreditierung ist die formale Anerkennung einer Kompetenz (hier: die Kompetenz einer Stelle, Konformitätsbewertungen von ISMS durchzuführen).

Die Europäische Union sieht Akkreditierung als eine hoheitliche Aufgabe. Entsprechend lassen sich in Europa Zertifizierungsstellen für Managementsysteme die Kompetenz, bestimmte Konformitätsbewertungsaufgaben durchzuführen, bei einem zentralen, nationalen Akkreditierer bestätigen. Dies ist beispielsweise in Deutschland die DAkkS (Deutsche Akkreditierungsstelle GmbH), in Österreich die vom Bundesministerium für Wissenschaft, Forschung und Wirtschaft betriebene „Akkreditierung Austria“, in der Schweiz die SAS (Schweizerische Akkreditierungsstelle, Teil des Staatssekretariats für Wirtschaft). Die Harmonisierung und wechselseitige Anerkennung von Akkreditierungen wird durch die *European co-operation for Accreditation*¹ geregelt.

Allgemeine Anforderungen an Zertifizierungsstellen, nach denen alle in der *European co-operation for Accreditation* organisierten Akkreditierer prüfen, sind in ISO/IEC 17021 (*Konformitätsbewertung – Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren*) [DIN15] festgelegt. ISO/IEC 27006 (*Requirements for bodies providing audit and certification of information security management systems*) [DIN15] konkretisiert und ergänzt die Anforderungen aus ISO/IEC 17021 für Stellen, die Managementsysteme für Informationssicherheit auditieren und zertifizieren.

Abbildung 7.1 verdeutlicht die Zusammenhänge noch einmal an einem Beispiel. Will die spanische Firma Colmo S. A. beispielsweise die Archivierung ihrer Dokumente an die deut-

¹ <http://www.european-accrreditation.org/>

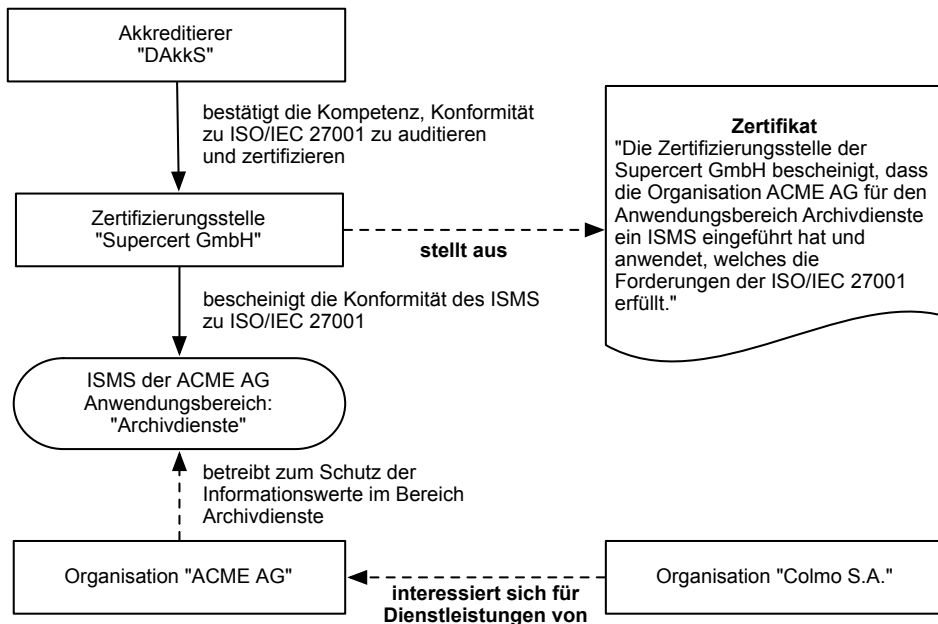


Abbildung 7.1 Zertifizierung und Akkreditierung

sche ACME AG auslagern, so wird es sie sicherlich interessieren, ob die ACME AG in diesem Bereich ein vernünftiges Informationssicherheitsmanagement betreibt. Hier kann die ACME AG darauf verweisen, dass es die Anforderungen der ISO/IEC 27001 erfüllt und dass dies von der Supercert GmbH bestätigt worden ist. Nun hat vielleicht bei der Colmo S.A. noch nie jemand etwas von der Supercert GmbH gehört. Die Kompetenz der Supercert GmbH, solche Bewertungen vorzunehmen, ist aber von einem nationalen Akkreditierer bestätigt worden, der nach denselben Prinzipien vorgeht und prüft wie die nationale Akkreditierungsstelle in Spanien. Daher kann die Colmo S.A. die von der ACME AG vorgelegte Zertifizierung als seriös ansehen.

Natürlich erlaubt auch die Vorlage einer ISO/IEC 27001-Zertifizierung nicht das bedenkenlose Vertrauen in die Informationssicherheit bei einer Organisation. Aber sie zeigt immerhin, dass – zumindest im zertifizierten Geltungsbereich – die notwendigen Grundlagen für ein effektives Management der Informationssicherheit vorhanden sind.

7.1.2 Typischer Ablauf einer Zertifizierung

Eine Zertifizierung erfolgt durch eine entsprechend akkreditierte Zertifizierungsstelle. Die Abbildung 7.2 zeigt exemplarisch einen typischen Ablauf.

Ein Zertifizierungsaudit sollte gründlich vorbereitet werden. Die Ergebnisse interner Audits (siehe Kapitel 4.9.2) bzw. Self-Assessments helfen bei der Erkennung von Lücken bis zur Erfüllung aller in ISO/IEC 27001 enthaltenen Anforderungen. Es lohnt sich aber oft, bereits frühzeitig mit der gewünschten Zertifizierungsstelle Kontakt aufzunehmen, um z. B. in Vorgesprächen zu klären, welche Unterlagen die Auditoren erwarten oder wie die wichtigs-

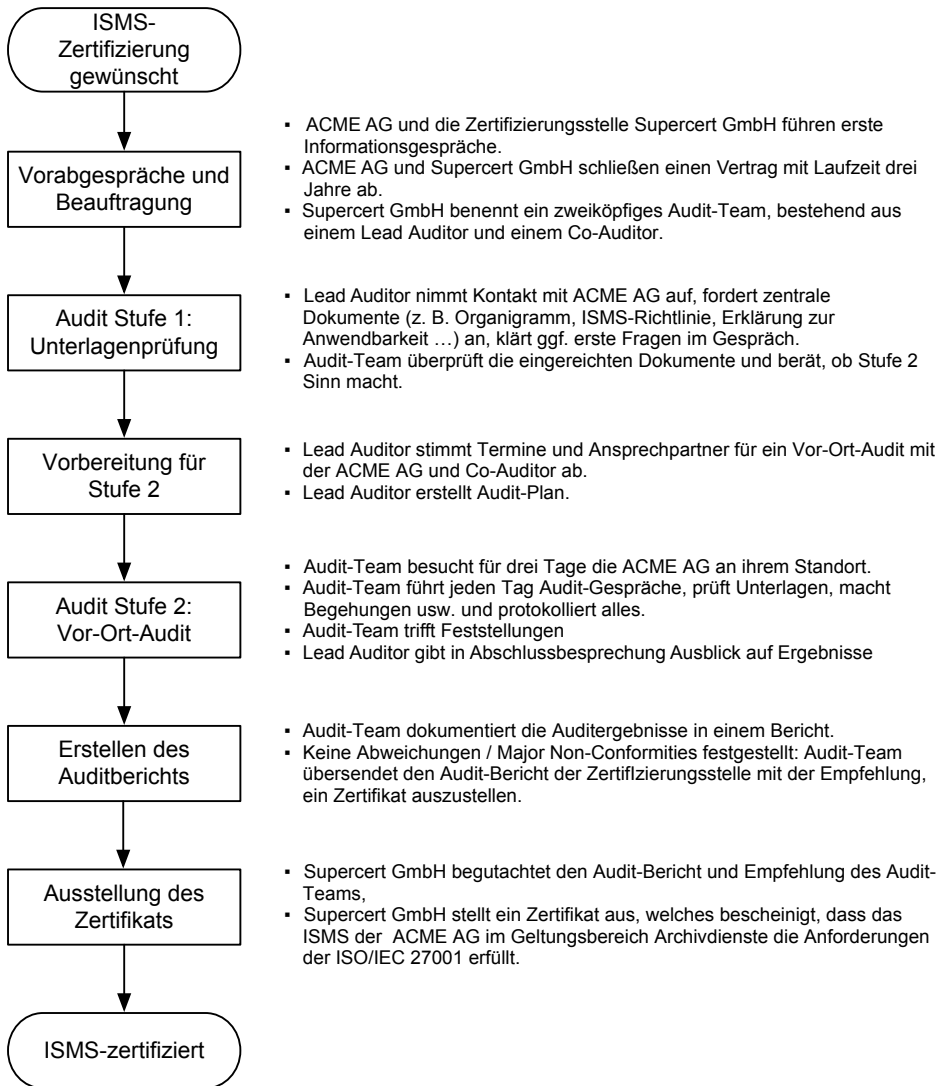


Abbildung 7.2 Beispielhafter Ablauf einer Zertifizierung

ten Verbesserungsmaßnahmen grob zu priorisieren sind. Viele Zertifizierungsstellen bieten auch ein sogenanntes Vor-Audit als Dienstleistung an, welches eine Art vereinfachten Probelauf für das Zertifizierungsaudit bietet und hilft, unangenehme Überraschungen zu vermeiden.

Das eigentliche Zertifizierungsaudit läuft meist in zwei Phasen ab. In der ersten Phase (Stufe 1) werden von den Auditoren primär Dokumente und Aufzeichnungen überprüft. Basierend auf den Ergebnissen dieses Dokumentenaudits geben die Auditoren eine Empfehlung ab, ob es sinnvoll ist, mit dem Audit zu diesem Zeitpunkt weiter zu verfahren. Wenn ja, wird ein Auditplan für die zweite Phase erstellt. In der zweiten Phase (Stufe 2) führt ein Team von

Index

A

ABAC *siehe* Attribute based access control
Abhören 116
Abschreckung 102, 110
Acceptance Criteria 136
Access Control 6
Accountability 6
Act-Phase 32, 35, 66
Änderungen 88
Akkreditierung 16, 158
Akzeptanzkriterien 136
Anforderung 180
– behördlich 95
– gesetzlich 95
– vertraglich 95
Anforderungsmanagement 134
Angriff 169
Anlieferungen 109
Anonymisierung 124
Anwendungsbereich 14, 38, 42, 52, 158, 161
Anwendungssicherheit 133
APMG 163
Arbeitsverträge 100
Asset *siehe* Wert
Asset Management 109
Attributbasierte Zugangskontrolle 86
Attribute based access control 86
Audit 18, 63, 66, 97, 138, 157, 160, 169
– Bericht 65
– externes 63
– internes 63
– Nachweise 64
– Programm 64
– Protokoll 65
– Schutz 138
– Umfang 161, 170
Auditor 64
Aufgabe des Managements 26
Aufgabentrennung 77

Aufgeräumter Schreibtisch 112
Aufzeichnung 25, 96
Ausbildung 101
Ausgelagerte Entwicklung 136
Ausgliedern 179
Ausweise 109
Authentication *siehe* Authentisierung
Authenticity *siehe* Authentizität
Authentisierung 5, 85, 120, 170
– Mehrfaktor 109, 121
Authentizität 5, 82, 83, 170
Availability *siehe* Verfügbarkeit
AXELOS 151

B

B3S *siehe* Branchenspezifische
Sicherheitsstandards
Büros *siehe* Räumlichkeiten
Backup 125
BCP *siehe* Business Continuity Plan
Bedrohung 185
Bedrohungslage 79
Befugnisse 45
Beschädigung 112, 116
Beschäftigungsverhältnis 102
– Beendigung 102
– Wechsel 102
Best Practices 17
Betrieb 58
Betriebsablauf-Verantwortung 98
Betriebsmittel 112
– Wartung 116
Betriebsunterbrechungen 94
Betriebsverfahren 98
Beweise 93
Bewusstsein 55
BIA *siehe* Business-Impact-Analyse
Bildschirmschoner 112
Bildschirm Sperre 112

Blacklisting 132
 Blickschutzfolie 114
 Branchenspezifische Sicherheitsstandards 8
 Bring your own Device 118
 BSI *siehe* Bundesamt für Sicherheit in der Informationstechnik
 BSI-Standards 144
 BS 7799 17
 Bundesamt für Sicherheit in der Informationstechnik 143
 – IT-Grundschutz-Kompendium 143
 – IT-Grundschutz-Standards 144
 Business Continuity Plan 94, 137
 Business-Impact-Analyse 95
 BYOD *siehe* Bring your own Device

C

CERT *siehe* Computer Emergency Response Team
 Chancen 47
 Change Management 88, 129, 137
 Check-Phase 31, 35, 60
 Chief Information Security Officer 27, 77
 CISA *siehe* Cybersecurity and Infrastructure Security Agency
 CISIS12 145
 CISO *siehe* Chief Information Security Officer
 Clouddienste 89
 Code of Practice 21
 Compliance 95, 96
 Computer Emergency Response Team 79
 Computer Security Incident Response Team 90
 Confidentiality *siehe* Vertraulichkeit
 Controls 35
 CSIRT *siehe* Computer Security Incident Response Team
 Cybersecurity and Infrastructure Security Agency 102
 Cybersecurity Framework 146

D

DAKS *siehe* Deutsche Akkreditierungsstelle
 Data Leakage 125
 Daten
 – Abfluss 124
 – Leck 125
 – Maskierung 124
 – Minimierung 9
 – personenbezogene 9
 – Richtigkeit 9
 – Sicherung 125
 – Speicherbegrenzung 9

Datenschutz-Folgenabschätzung 9
 Datenschutz-Grundverordnung 9
 Datenschutzbeauftragter 26
 Datenschutzvorfälle melden 106
 Datenträger *siehe* Speichermedien
 DDoS *siehe* Distributed Denial of Service
 Definitionsebene 25
 Deming-Kreislauf 30, 35
 Denial of Service 5
 Deutsche Akkreditierungsstelle 158
 Diebstahl 112
 Dienstleistungen 88
 Dienstprogramme
 – privilegierte 128
 Distributed Denial of Service 5
 Disziplinarverfahren 102
 Do-Phase 31, 35, 54, 58
 Dokument 25
 Dokumentation 25, 56
 Dokumentenaudit 160
 Dokumentenlenkung 26, 57, 57
 Dokumentenvorlage 58
 DoS *siehe* Denial of Service
 DSGVO *siehe* Datenschutz-Grundverordnung
 Durchführungsebene 25

E

Effektivität 31, 65
 Effizienz 32, 65
 Eigentum 96
 Einbrüche 107, 110
 Einrichtungen 109, 115
 Elementarmessgröße 170
 Elementarschaden 111
 Endgeräte 118
 ENISA *siehe* European Union Agency for Cybersecurity
 Entscheidung 92
 Entsorgung
 – von Betriebsmitteln 117
 – von Speichermedien 112, 114, 117
 Entwicklung 133
 – sichere 133
 Entwicklungsgrundsätze 134
 Entwicklungsumgebung 136
 Ereignis 173
 European Union Agency for Cybersecurity 102
 Examination Institute 162
 Externes Audit 63, 157
 Externe Mitarbeitende 26

F

Festplatten *siehe* Speichermedien
 FitSM 153
 Folge 171
 Fortbildung 101
 Fortbildungsprogramme 26
 Foundation-Zertifikat 163, 165
 – Prüfungsspezifikation 165
 – Prüfungsvorbereitung 165
 Führung 43

G

Gäste 109
 Gebäude 107, 109
 Geheimhaltungsvereinbarung 103
 geistiges Eigentum 96
 Gerätesperre 112
 Gesamtverantwortung 26

H

Hintergrundüberprüfungen *siehe* Screening
 Homeoffice *siehe* Remote-Arbeiten

I

IAM *siehe* Identity and Access Management
 ICO 164
 Identitätsmanagement 84
 Identity and Access Management 85
 IDS *siehe* Intrusion-Detection-System
 IEC *siehe* International Electrotechnical Commission
 IKT *siehe* Informations- und Kommunikationstechnik
 Indikator 25, 174
 Information 2, 172
 – Kennzeichnung 82
 – Klassifizierung 81
 – Transport 83
 – Übertragung 83
 – Zulässige Nutzung 80, 81
 Information Security Assessment 147
 Information Security Officer 27, 77
 Informations- und Kommunikationstechnik 87, 94
 Informationsaustauschende Gemeinschaft 175
 Informationsbedarf 174
 Informationssicherheit 2, 174
 – Aufrechterhaltung 174
 – bei Betriebsunterbrechungen 94
 – Clouddienste 89
 – IKT-Lieferkette 87
 – im Projektmanagement 79

– Konformität 98
 – Lieferantenbeziehungen 86
 – Lieferantenvereinbarungen 87
 – Richtlinien 98
 – Standards 98
 – Steuerung 173
 – unabhängige Überprüfung 97
 Informationssicherheitsrichtlinien 74
 Informationssicherheitsbeauftragter 27
 Informationssicherheitsereignis 175
 – melden 105
 Informationssicherheitsmanagementsystem 23, 43
 – Audit 18
 – Dokumentation 25
 – Kernbestandteile 23
 Informationssicherheitsrisikobehandlung 51
 Informationssicherheitsrisikobeurteilung 48
 Informationssicherheitsvorfall 89, 175
 – Beurteilung 92
 – Entscheidung 92
 – Handhabung 175
 – Lernen 93
 – Reaktion 92
 Informationssysteme 175
 Informationsveranstaltungen 26
 informationsverarbeitende Einrichtungen 174
 Informationszugang 119
 Informativer Standard 14
 Installation 129
 Instandsetzung *siehe* Wartung
 Integrität 4, 9, 82, 176
 Integrity *siehe* Integrität
 Interessengruppen 78
 Interessierte Partei 176
 International Electrotechnical Commission 1, 147
 International Organization for Standardization 1, 147, 149
 Internes Audit 63
 Intrusion-Detection-System 128
 Inventar 80
 ISA *siehe* Information Security Assessment
 ISMS *siehe* Informationssicherheitsmanagementsystem
 ISO *siehe* International Organization for Standardization, *siehe* Information Security Officer
 ISO/IEC 15408 146
 ISO/IEC 17020 150
 ISO/IEC 17021 16, 17, 150, 158, 161
 ISO/IEC 17024 151

- ISO/IEC 17025 151
 - ISO/IEC 17799 17, 73, 157
 - ISO/IEC 20000 28, 152
 - ISO/IEC 27000 14
 - ISO/IEC 27001 16
 - ISO/IEC 27002 17
 - ISO/IEC 27003 17
 - ISO/IEC 27004 18
 - ISO/IEC 27005 18
 - ISO/IEC 27006 16, 151, 161, 162
 - ISO/IEC 27007 18
 - ISO/IEC 27008 18
 - ISO/IEC 27009 16, 17
 - ISO/IEC 27010 20
 - ISO/IEC 27011 20
 - ISO/IEC 27013 18, 153
 - ISO/IEC 27014 18
 - ISO/IEC 27016 18
 - ISO/IEC 27017 20
 - ISO/IEC 27018 19, 20
 - ISO/IEC 27019 20
 - ISO/IEC 27032 20
 - ISO/IEC 27034 20
 - ISO 19011 149, 150, 161
 - ISO 9000 14, 28, 149
 - ISO 9001 149
 - ISO 9004 149
 - IT Infrastructure Library 151
 - IT Service Management 99, 137
 - IT-Grundschutz-Kompendium 143
 - IT-Sicherheitscluster e.V. 145
 - IT-Sicherheitsgesetz 6
 - ITEMO e.V. 153
 - ITIL *siehe* IT Infrastructure Library, 151
 - ITSM *siehe* IT Service Management
- K**
- Kapazitätsmanagement 121
 - Kategorien von Werten 24
 - Kennzeichnung 82
 - Kernbestandteile eines ISMS 23
 - Klassifizierung 81
 - Klimatisierung 115
 - Kommunikation 55
 - Kommunikationsstrategie 90
 - Kompetenz 54, 170
 - Konfigurationsmanagement 123
 - Konformität 16, 31, 65, 66, 98, 171
 - Kontakt
 - Behörden 78
 - Interessengruppen 78
 - Kontext 173
 - der Organisation 40
 - Interessierte Parteien 41
 - interner 176
 - Kontinuierliche Verbesserung 29
 - Kontinuität 94
 - Kontinuitätsplan 95
 - Korrektur 172
 - Korrekturmaßnahme 172
 - KRITIS *siehe* Kritische Infrastrukturen
 - Kritische Infrastrukturen 7
 - Kryptographie 132
 - Kündigung 102
- L**
- Least Privilege 84
 - Lebenszyklus
 - sichere Entwicklung 133
 - Leistung 179
 - Leitfaden 17
 - maßnahmenspezifisch 20
 - sektorspezifisch 20
 - Leitung 43, 185
 - Lernen 93
 - Lieferanten 88
 - Vereinbarungen 87
 - Lieferantenbeziehungen 86, 87
 - Lizenzen 117
 - Lizenzmanagement 96
 - Löschung 114, 123
 - Logging 126
- M**
- Maßnahmenspezifische Leitfäden 20
 - Maßregelungsprozess *siehe*
 - Disziplinarverfahren
 - Man-in-the-Middle-Angriff 5
 - Management Review 65
 - Management technischer Schwachstellen 122
 - Managementbewertung 65
 - Managementsystem 23, 177
 - Manipulation 116
 - Maßnahme 27, 73–171
 - in Verbindung mit Menschen 99
 - organisatorische 74
 - physische 106
 - technische 118
 - Maßnahmenziele 172
 - Measurement 18
 - Mehrfaktor Authentisierung 109, 121
 - Menschen 99
 - Messfunktion 177
 - Messgröße 172, 177

- Messmethode 178
Messung 18, 60, 177
Mitarbeitende *siehe* Menschen
Mitarbeiterausweise *siehe* Ausweise
Mobiles Arbeiten *siehe* Remote-Arbeiten
Mobilgeräte 104, 113
- N**
NAC *siehe* Network-Access-Control
Nachvollziehbarkeit 25
National Institute of Standards and Technology 146
– Cybersecurity Framework 146
Naturkatastrophen 111
Need to know 84
Network-Access-Control 130
Netzdienste 130
Netzdomäne 131
Netzsicherheit 130
Netztrennung 131
Nichtabstreitbarkeit 5, 83, 178
Nichtkonformität 178
NIM *siehe* Netzwerk für
Informationssicherheit im Mittelstand
NIST *siehe* National Institute of Standards and Technology
Non-disclosure agreement 103
Non-repudiation 5
Norm 14
Normative Verweisungen 39
Normativer Standard 14
- O**
Organisation 179
Organisationszertifizierung 157
Organisatorische Maßnahmen 74
- P**
PDCA 29, 29, 35
PDCA-Methodik 23, 29
Penetration Test 122
Personal *siehe* Menschen
Personenbezogene Daten 9, 97
Personenzertifizierung 157, 162
Physische Gefährdungen 110
Physische Maßnahmen 106
Physische Sicherheit 106
Physischer Zutritt 108
PKI *siehe* Public Key Infrastructure
Plan 46
Plan-Do-Check-Act 29
Plan-Phase 30, 35, 46
Planung 30, 46, 89
Policy 24, 74
Politik 44, 180
Principle of Least Privilege 134
Prinzip der geringsten Rechte 134
Privatsphäre 97
Privilegierte Zugangsberechtigungen 118
Procedure 24
Process 24
Produktivumgebung 136
Projektmanagement 79
Protokollierung 126
Prozess 24, 28, 180
Prozessmanagement 29
Prozessorientierung 28
Pseudonymisierung 124
Public Key Infrastructure 133
- Q**
Qualifizierungsprogramm 162
Qualitätsmanagement 29
- R**
Räumlichkeiten 109
Rahmenwerk 143
RBAC *siehe* Role based access control
Rechtmäßigkeit 9
Rechtsprechung 26
Recovery time objective 95
Redundanz 126
Release Management 129, 136
Reliability 5
Remote-Arbeiten 104
Reparatur *siehe* Wartung
Requirements Engineering 134
Ressourcen 30, 54
Restrisiko 180
Review 93
Rezertifizierung 161
Richtigkeit 9
Richtlinie 24, 74, 98
– themenspezifisch 75
Risiko 181
– Absprache 182
– Akzeptanz 49, 182
– Analyse 50, 182
– Behandlung 51, 184
– Beurteilung 49, 50, 59, 182
– Bewertung 51, 183
– Eigentümer 53, 76, 184
– Identifizierung 50, 183
– Kommunikation 182

- Kriterien 183
- Management 18, 80
- Matrix 51
- Niveau 176
- Risikomanagement 47, 183
 - Prozess 184
- Role based access control 86
- Rollen 26, 27, 76
- Rollenbasierte Zugangskontrolle 86
- Rollenzuweisung 76
- RTO *siehe* Recovery time objective
- Rückverfolgbarkeit 25

S

- Schadsoftware 121
- Schlüsselverwaltung 133
- Schulung 101
- Schutz
 - Aufzeichnungen 96
 - Bedarf 107
 - Klasse 107
 - Niveau 27
 - personenbezogene Daten 97
 - Privatsphäre 97
 - vor Schadsoftware 121
 - Ziel 3
- Schwachstelle 122, **185**
- Schwachstellenscan 122
- Scope *siehe* Anwendungsbereich
- Scoping 14, 158
- Scoping Statement 158
- Screening 99
- Security Incident Coordinator 90
- Security Incident Response 90
- Security-Information-&-Event-Management 127
- Sektorspezifische Leitfäden 20
- Sensibilisierung 101
- SIC *siehe* Security Incident Coordinator
- Sichere Authentisierung 120
- Sicherheit
 - Netzsicherheit 130
 - von Anwendungen 133
- Sicherheitsanforderung 3
- Sicherheitsbereiche 106
- Sicherheitslücke melden 105
- Sicherheitsperimeter 106
- Sicherheitstests 135
- Sicherheitsüberprüfungsgesetz 100
- Sicherheitsvorfälle melden 106
- Sicherheitsziele 53
- Sicherheitszonen 106, 107, 111

- SIEM *siehe*
 - Security-Information-&-Event-Management
- SIR *siehe* Security Incident Response
- Softwareinstallation 129
- Softwarelizenzen *siehe* Lizenzen
- Source Code 120
- Speicherbegrenzung 9
- Speichermedien 114, 117
- Stand der Technik 8
- Stand-by 126
 - heiß 126
 - kalt 126
- Standard 14, 98
 - informativer 14
 - normativer 14
- Standardfamilie 13
- Standardisierung 13
- Standort 107, 113
- Statement of Applicability 158
- Steuerung 173
- Steuerungsebene 25
- Steuerungsgremium 174
- Stromversorgung 115, 116
- SÜG *siehe* Sicherheitsüberprüfungsgesetz
- Support 54
- Systemabnahmetest 135
- Systemarchitektur 134

T

- TÜV Süd 163
- Technische Maßnahmen 118
- Technische Schwachstellen 122
- Telearbeit *siehe* Remote-Arbeiten
- Terminologie 14
- Testdaten 138
- Testumgebung 136
- TISAX *siehe* Trusted Information Security
 - Assessment Exchange
- Topmanagement 77
- Training 101
- Transparenz 9
- Trennung 136
- Trusted Information Security Assessment
 - Exchange 147

U

- Überblicksdokument 14
- Überprüfung **31**, 60, 88, 97, 181
 - Ziel 181
- Überwachung 60, 88, 110, 178
- Überwachungsaktivitäten 127
- Überwachungsaudit 161

Uhrensynchronisation 128
Umgebungsbedingte Gefährdungen 110
Umgebungstrennung 136
Umsetzung 31, 54, 58
User Endpoint Devices 118

V

VDA *siehe* Verband der Automobilindustrie
VDA ISA (TISAX) 147
Verantwortlichkeit 26, 45, 75, 76
Verantwortung 77
Verband der Automobilindustrie 147
Verbesserung 32, 66, 171
Verbesserungsmaßnahmen 32
Verbindlichkeit 5
Verfahren 24
Verfahrensweisung 25
Verfügbarkeit 4, 82, 170
Verkabelung 116
Verlässlichkeit 5, 180
Verlust 112
Vernichtung *siehe* Entsorgung
Verschwiegenheitspflicht 103
Versorgungseinrichtungen 109
Verstöße 102
Vertragsbedingungen für die Beschäftigung 100
Vertrauenswürdige Einheit 185
Vertraulichkeit 3, 9, 82, 171
Vertraulichkeitsvereinbarung 101, 103, 103
Verwandte Standards 143
– Auditierung 149
– Governance 151
– IT- und Informationssicherheit 143
– Management der IT 151
– Qualitätsmanagement 149
– Zertifizierung 149
Videoüberwachung *siehe* Überwachung
Vorstand 26

W

Wahrscheinlichkeit 177
Wartung 116
Webfilterung 131

Wechseldatenträger *siehe* Speichermedien
Wert 24, 80
– Rückgabe 81
Whitelisting 132
Wiederherstellungsmaßnahmen 95
Wiederherstellungszeit 95
Wiederholungsaudit 161
Wiederverwendung
– von Betriebsmitteln 117
– von Speichermedien 114, 117
Wirksamkeit 173
Wirkungsgrad 32

Z

Zeitpunkte 30
Zerstörung *siehe* Entsorgung
Zertifikat 161
Zertifizierung 157
– Ablauf 159
– Akkreditierung 158
– Organisationszertifizierung 157
– Personenzertifizierung 157, 162
– Rezertifizierung 161
Zertifizierungsaudit 16, 169
Zertifizierungsprüfung 237
Zertifizierungsstelle 16, 159
Ziel 178
Zonenmodell 106
Zugang 6
– Source Code 120
Zugangsberechtigung 86
– attributbasiert 86
– rollenbasiert 86
Zugangssteuerung 83, 169
Zugriffskontrolle 6
Zugriffssteuerung 6
Zurechenbarkeit 6
Zutritt 6, 107, 108
Zutrittspunkte 108
Zutrittssteuerung 108
Zuweisung
– Rollen 26
Zweckbindung 9