

# HANSER



## Leseprobe

zu

## Praxisbuch ISO/IEC 27001

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

Print-ISBN: 978-3-446-47711-7

E-Book-ISBN: 978-3-446-47845-9

E-Pub-ISBN: 978-3-446-48267-8

Weitere Informationen und Bestellungen unter

<https://www.hanser-kundencenter.de/fachbuch/artikel/9783446477117>

sowie im Buchhandel

© Carl Hanser Verlag, München

# Inhaltsverzeichnis

<b>Vorwort</b> .....	<b>XIII</b>
<b>1 Einführung und Basiswissen</b> .....	<b>1</b>
1.1 Worum geht es in ISO/IEC 27000 und ISO/IEC 27001? .....	2
1.2 Begriffsbildung.....	3
1.2.1 Informationen .....	3
1.2.2 Informationssicherheit .....	3
1.2.3 Sicherheitsanforderungen und Schutzziele .....	3
1.3 IT-Sicherheitsgesetz & KRITIS .....	7
1.3.1 Was ist „KRITIS“? .....	8
1.3.2 Wer ist in Deutschland von KRITIS betroffen? .....	8
1.3.3 KRITIS-Anforderungen – Informationssicherheit nach dem „Stand der Technik“ .....	9
1.4 Datenschutz-Grundverordnung .....	10
1.5 Weitere Richtlinien und Verordnungen der Europäischen Union .....	11
1.5.1 NIS-2-Richtlinie .....	11
1.5.2 Richtlinie über die Resilienz kritischer Einrichtungen (EU RCE Directive/CER-Richtlinie) .....	12
1.5.3 Cyber Resilience Act (CRA) .....	12
1.5.4 DORA-Verordnung .....	13
1.6 Überblick über die folgenden Kapitel.....	13
1.7 Beispiele für Prüfungsfragen zu diesem Kapitel .....	13
<b>2 Die Standardfamilie ISO/IEC 27000 im Überblick</b> .....	<b>15</b>
2.1 Warum Standardisierung? .....	15
2.2 Grundlagen der ISO/IEC 27000 .....	16
2.3 Normative vs. informative Standards .....	16
2.4 Die Standards der ISMS-Familie und ihre Zusammenhänge .....	17
2.4.1 ISO/IEC 27000: Grundlagen und Überblick über die Standardfamilie ..	18
2.4.2 Normative Anforderungen .....	18

2.4.3	Allgemeine Leitfäden .....	20
2.4.4	Sektor- und maßnahmenspezifische Leitfäden .....	22
2.5	Zusammenfassung .....	24
2.6	Beispiele für Prüfungsfragen zu diesem Kapitel .....	24
<b>3</b>	<b>Grundlagen von Informationssicherheitsmanagementsystemen ..</b>	<b>27</b>
3.1	Das ISMS und seine Bestandteile .....	27
3.1.1	(Informations-)Werte.....	28
3.1.2	Richtlinien, Prozesse und Verfahren .....	28
3.1.3	Dokumente und Aufzeichnungen .....	29
3.1.4	Zuweisung von Verantwortlichkeiten .....	30
3.1.5	Maßnahmen .....	31
3.2	Was bedeutet Prozessorientierung? .....	33
3.3	Die PDCA-Methodik: Plan-Do-Check-Act .....	34
3.3.1	Planung (Plan) .....	35
3.3.2	Umsetzung (Do) .....	35
3.3.3	Überprüfung (Check).....	36
3.3.4	Verbesserung (Act) .....	37
3.4	Zusammenfassung .....	37
3.5	Beispiele für Prüfungsfragen zu diesem Kapitel .....	37
<b>4</b>	<b>DIN EN ISO/IEC 27001 – Spezifikationen und Mindestanforderungen .....</b>	<b>39</b>
4.0	Einleitung .....	41
4.0.1	Allgemeines.....	41
4.0.2	Kompatibilität mit anderen Normen für Managementsysteme .....	42
4.1	Anwendungsbereich .....	43
4.2	Normative Verweisungen .....	43
4.3	Begriffe .....	44
4.4	Kontext der Organisation .....	44
4.4.1	Verstehen der Organisation und ihres Kontextes .....	45
4.4.2	Verstehen der Erfordernisse und Erwartungen interessierter Parteien ..	45
4.4.3	Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems .....	46
4.4.4	Informationssicherheitsmanagementsystem .....	48
4.5	Führung .....	48
4.5.1	Führung und Verpflichtung.....	48
4.5.2	Politik .....	50
4.5.3	Rollen, Verantwortlichkeiten und Befugnisse in der Organisation .....	51
4.6	Planung .....	52
4.6.1	Maßnahmen zum Umgang mit Risiken und Chancen .....	52
4.6.2	Informationssicherheitsziele und Planung zu deren Erreichung .....	58
4.6.3	Planung von Änderungen .....	59

4.7	Unterstützung .....	60
4.7.1	Ressourcen .....	60
4.7.2	Kompetenz .....	61
4.7.3	Bewusstsein .....	61
4.7.4	Kommunikation .....	62
4.7.5	Dokumentierte Information .....	63
4.8	Betrieb .....	65
4.8.1	Betriebliche Planung und Steuerung .....	65
4.8.2	Informationssicherheitsrisikobeurteilung .....	66
4.8.3	Informationssicherheitsrisikobehandlung .....	67
4.9	Bewertung der Leistung .....	67
4.9.1	Überwachung, Messung, Analyse und Bewertung .....	67
4.9.2	Internes Audit .....	70
4.9.3	Managementbewertung .....	73
4.10	Verbesserung .....	74
4.10.1	Fortlaufende Verbesserung .....	75
4.10.2	Nichtkonformität und Korrekturmaßnahmen .....	75
4.11	Zusammenfassung .....	76
4.12	Beispiele für Prüfungsfragen zu diesem Kapitel .....	77
<b>5</b>	<b>Maßnahmen im Rahmen des ISMS .....</b>	<b>81</b>
5.1	A.5 Organisatorisches Maßnahmen .....	82
5.1.1	[A.5.1] Informationssicherheitspolitik und -richtlinien .....	82
5.1.2	[A.5.2] Informationssicherheitsrollen und -verantwortlichkeiten .....	84
5.1.3	[A.5.3] Aufgabentrennung .....	85
5.1.4	[A.5.4] Verantwortlichkeiten der Leitung .....	85
5.1.5	[A.5.5] Kontakt mit Behörden .....	86
5.1.6	[A.5.6] Kontakt mit speziellen Interessensgruppen .....	86
5.1.7	[A.5.7] Informationen über die Bedrohungslage .....	87
5.1.8	[A.5.8] Informationssicherheit im Projektmanagement .....	87
5.1.9	[A.5.9] Inventar der Informationen und anderen damit verbundenen Werte .....	88
5.1.10	[A.5.10] Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten .....	88
5.1.11	[A.5.11] Rückgabe von Werten .....	89
5.1.12	[A.5.12] Klassifizierung von Informationen .....	89
5.1.13	[A.5.13] Kennzeichnung von Informationen .....	90
5.1.14	[A.5.14] Informationsübermittlung .....	91
5.1.15	[A.5.15] Zugangssteuerung .....	92
5.1.16	[A.5.16] Identitätsmanagement .....	92
5.1.17	[A.5.17] Authentisierungsinformationen .....	93

5.1.18	[A.5.18] Zugangsrechte .....	94
5.1.19	[A.5.19] Informationssicherheit in Lieferantenbeziehungen .....	95
5.1.20	[A.5.20] Behandlung von Informationssicherheit in Lieferantenvereinbarungen .....	95
5.1.21	[A.5.21] Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie (IKT) .....	96
5.1.22	[A.5.22] Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen .....	97
5.1.23	[A.5.23] Informationssicherheit für die Nutzung von Cloud-Diensten ..	97
5.1.24	[A.5.24] Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen .....	98
5.1.25	[A.5.25] Beurteilung und Entscheidung über Informationssicherheitsereignisse .....	99
5.1.26	[A.5.26] Reaktion auf Informationssicherheitsvorfälle .....	101
5.1.27	[A.5.27] Erkenntnisse aus Informationssicherheitsvorfällen .....	102
5.1.28	[A.5.28] Sammeln von Beweismaterial .....	102
5.1.29	[A.5.29] Informationssicherheit bei Störungen .....	103
5.1.30	[A.5.30] IKT-Bereitschaft für Business-Continuity .....	103
5.1.31	[A.5.31] Juristische, gesetzliche, regulatorische und vertragliche Anforderungen .....	104
5.1.32	[A.5.32] Geistige Eigentumsrechte .....	105
5.1.33	[A.5.33] Schutz von Aufzeichnungen .....	105
5.1.34	[A.5.34] Datenschutz und Schutz von personenbezogenen Daten (PbD)	106
5.1.35	[A.5.35] Unabhängige Überprüfung der Informationssicherheit .....	106
5.1.36	[A.5.36] Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit .....	107
5.1.37	[A.5.37] Dokumentierte Betriebsabläufe .....	107
5.2	A.6 Personenbezogene Maßnahmen .....	108
5.2.1	[A.6.1] Sicherheitsüberprüfung .....	108
5.2.2	[A.6.2] Beschäftigungs- und Vertragsbedingungen .....	109
5.2.3	[A.6.3] Informationssicherheitsbewusstsein, -ausbildung und -schulung .....	110
5.2.4	[A.6.4] Maßregelungsprozess .....	111
5.2.5	[A.6.5] Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung .....	111
5.2.6	[A.6.6] Vertraulichkeits- oder Geheimhaltungsvereinbarungen .....	112
5.2.7	[A.6.7] Remote-Arbeit .....	113
5.2.8	[A.6.8] Meldung von Informationssicherheitsereignissen .....	114
5.3	A.7 Physische Maßnahmen .....	115
5.3.1	[A.7.1] Physische Sicherheitsperimeter .....	115
5.3.2	[A.7.2] Physischer Zutritt .....	117
5.3.3	[A.7.3] Sichern von Büros, Räumen und Einrichtungen .....	118

5.3.4	[A.7.4] Physische Sicherheitsüberwachung .....	118
5.3.5	[A.7.5] Schutz vor physischen und umweltbedingten Bedrohungen ....	119
5.3.6	[A.7.6] Arbeiten in Sicherheitsbereichen .....	120
5.3.7	[A.7.7] Aufgeräumte Arbeitsumgebung und Bildschirmsperren .....	121
5.3.8	[A.7.8] Platzierung und Schutz von Geräten und Betriebsmitteln .....	121
5.3.9	[A.7.9] Sicherheit von Assets außerhalb der Standorte der Organisation	122
5.3.10	[A.7.10] Speichermedien .....	123
5.3.11	[A.7.11] Versorgungseinrichtungen .....	124
5.3.12	[A.7.12] Sicherheit der Verkabelung .....	124
5.3.13	[A.7.13] Instandhaltung von Geräten und Betriebsmitteln .....	125
5.3.14	[A.7.14] Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln .....	126
5.4	A.8 Technologische Maßnahmen .....	126
5.4.1	[A.8.1] Endpunktgeräte des Benutzers .....	126
5.4.2	[A.8.2] Privilegierte Zugangsrechte .....	127
5.4.3	[A.8.3] Informationszugangsbeschränkung .....	128
5.4.4	[A.8.4] Zugriff auf den Quellcode .....	128
5.4.5	[A.8.5] Sichere Authentisierung .....	129
5.4.6	[A.8.6] Kapazitätssteuerung .....	130
5.4.7	[A.8.7] Schutz gegen Schadsoftware .....	130
5.4.8	[A.8.8] Handhabung von technischen Schwachstellen .....	131
5.4.9	[A.8.9] Konfigurationsmanagement .....	132
5.4.10	[A.8.10] Löschung von Informationen .....	132
5.4.11	[A.8.11] Datenmaskierung .....	133
5.4.12	[A.8.12] Verhinderung von Datenlecks .....	133
5.4.13	[A.8.13] Sicherung von Informationen .....	134
5.4.14	[A.8.14] Redundanz von informationsverarbeitenden Einrichtungen ..	135
5.4.15	[A.8.15] Protokollierung .....	135
5.4.16	[A.8.16] Überwachung von Aktivitäten .....	137
5.4.17	[A.8.17] Uhrensynchronisation .....	138
5.4.18	[A.8.18] Gebrauch von Hilfsprogrammen mit privilegierten Rechten....	138
5.4.19	[A.8.19] Installation von Software auf Systemen im Betrieb .....	139
5.4.20	[A.8.20] Netzwerksicherheit .....	140
5.4.21	[A.8.21] Sicherheit von Netzwerkdiensten .....	140
5.4.22	[A.8.22] Trennung von Netzwerken .....	141
5.4.23	[A.8.23] Webfilterung .....	142
5.4.24	[A.8.24] Verwendung von Kryptographie .....	142
5.4.25	[A.8.25] Lebenszyklus einer sicheren Entwicklung .....	144
5.4.26	[A.8.26] Anforderungen an die Anwendungssicherheit .....	144
5.4.27	[A.8.27] Sichere Systemarchitektur und Entwicklungsgrundsätze .....	145

5.4.28	[A.8.28] Sichere Codierung .....	146
5.4.29	[A.8.29] Sicherheitsprüfung bei Entwicklung und Abnahme .....	146
5.4.30	[A.8.30] Ausgegliederte Entwicklung .....	147
5.4.31	[A.8.31] Trennung von Entwicklungs-, Test- und Produktivumgebungen .....	147
5.4.32	[A.8.32] Änderungssteuerung.....	148
5.4.33	[A.8.33] Testdaten .....	148
5.4.34	[A.8.34] Schutz der Informationssysteme während Tests im Rahmen von Audits.....	149
5.5	Beispiele für Prüfungsfragen zu diesem Kapitel .....	150
<b>6</b>	<b>Verwandte Standards und Rahmenwerke .....</b>	<b>153</b>
6.1	Standards und Rahmenwerke für IT- und Informationssicherheit.....	153
6.1.1	IT-Grundschutz-Kompendium .....	153
6.1.2	BSI-Standards .....	154
6.1.3	CISIS12 .....	155
6.1.4	Cybersecurity Framework.....	156
6.1.5	ISO/IEC 15408 .....	157
6.1.6	VDA ISA (TISAX).....	157
6.2	Standards und Rahmenwerke für Qualitätsmanagement, Auditierung und Zertifizierung .....	159
6.2.1	ISO 9000 .....	159
6.2.2	ISO 19011 .....	159
6.2.3	ISO/IEC 17020 .....	161
6.3	Standards und Rahmenwerke für Governance und Management in der IT .....	162
6.3.1	ITIL .....	162
6.3.2	ISO/IEC 20000 .....	162
6.3.3	FitSM.....	164
6.4	Beispiele für Prüfungsfragen zu diesem Kapitel .....	165
<b>7</b>	<b>Zertifizierungsmöglichkeiten nach ISO/IEC 27000 .....</b>	<b>167</b>
7.1	ISMS-Zertifizierung nach ISO/IEC 27001 .....	167
7.1.1	Grundlagen der Zertifizierung von Managementsystemen .....	167
7.1.2	Typischer Ablauf einer Zertifizierung.....	169
7.1.3	Auditumfang .....	171
7.1.4	Akzeptanz und Gültigkeit des Zertifikats .....	171
7.1.5	Aufwände und Kosten für Zertifizierungen .....	171
7.2	Personenqualifizierung auf Basis von ISO/IEC 27000.....	172
7.2.1	Programme zur Ausbildung und Zertifizierung von Personal.....	172
7.2.2	Erlangen eines Foundation-Zertifikats .....	175
7.3	Zusammenfassung .....	177
7.4	Beispiele für Prüfungsfragen zu diesem Kapitel .....	177

<b>A</b>	<b>Begriffsbildung nach ISO/IEC 27000</b> .....	<b>179</b>
<b>B</b>	<b>Abdruck der DIN EN ISO/IEC 27001:2024</b> .....	<b>197</b>
B.1	DIN EN ISO/IEC 27001:2024 .....	199
B.2	DIN EN ISO/IEC 27001:2024, Anhang A .....	220
B.3	Vergleich: DIN EN ISO/IEC 27001 Anhang A :2024 vs. :2017 .....	231
<b>C</b>	<b>Prüfungsfragen mit Antworten zur ISO/IEC 27001 Foundation</b> .....	<b>235</b>
C.1	Antworten auf die Prüfungsfragen zu den einzelnen Buchkapiteln .....	235
C.2	Ein beispielhafter Prüfungsfragebogen zur ISO/IEC 27001-Foundation-Prüfung	242
C.3	Antworten auf den Prüfungsfragebogen zur ISO/IEC 27001-Foundation-Prüfung .....	252
	<b>Literaturverzeichnis</b> .....	<b>259</b>
	<b>Index</b> .....	<b>266</b>



# Vorwort

Liebe Leserinnen und Leser,

dieses nunmehr in seiner fünften überarbeiteten Auflage vorliegende Buch verfolgt das Ziel, Sie auf Basis des Wortlauts der aktuellen deutschen Fassung der internationalen Norm ISO/IEC 27001 durch die Welt der Informationssicherheitsmanagementsysteme (ISMS) zu begleiten. Es wird Ihnen sowohl bei der Vorbereitung auf eine Personen- oder Organisationszertifizierung als auch bei der praktischen Anwendung als Nachschlagewerk nützlich sein.

Für alle, die sich mit Informationssicherheit und ISMS sowie verwandten Themen wie Datenschutz, IT-Governance, Risikomanagement und Compliance auseinandersetzen, führt branchenübergreifend faktisch kein Weg an ISO/IEC 27001 vorbei. Diese Norm ist seit rund zwei Jahrzehnten der international bewährte gemeinsame Nenner, der sich beispielsweise auch im *IT-Grundschutz* des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) und den *Branchenspezifischen Sicherheitsstandards (B3S)* für Kritische Infrastrukturen wiederfindet. Zuletzt wurde die englische ISO/IEC 27001 im Jahr 2022 deutlich überarbeitet; die 2024 erschienene deutsche Fassung, DIN EN ISO/IEC 27001:2024-01, ist in Anhang B dieses Buchs im Originallayout vollständig abgedruckt.

Die ersten drei Buchkapitel führen Sie zunächst kompakt in die spannende, aber auch komplexe Welt der ISMS und der Normenreihe ISO/IEC 27000 ein. In den Kapiteln 4 und 5 werden alle Anforderungen und Maßnahmen aus der DIN EN ISO/IEC 27001 in grau hinterlegten Kästen im Wortlaut wiedergegeben, im Sinne einer verständlichen Einführung im Einzelnen erläutert und mit Umsetzungsbeispielen sowie ergänzenden Hinweisen aus der Praxis angereichert. Anschließend zeigt Kapitel 6 Schnittstellen zu verwandten Standards und Rahmenwerken auf. Kapitel 7 erläutert die Vorgehensweisen bei der Zertifizierung von ISMS sowie bei der Personenqualifizierung. In Anhang A dieses Buchs finden Sie zudem alle in der DIN EN ISO/IEC 27000 definierten Fachbegriffe im Wortlaut.

Die Schwerpunkte unserer Erläuterungen orientieren sich an den Prüfungsinhalten zu den Foundation-Lehrgangskonzepten u. a. von APMG, ICO und der TÜV Süd Akademie. Jeweils am Ende der Kapitel 1 bis 7 finden Sie in Summe 40 exemplarische Prüfungsfragen, deren Schwierigkeitsgrad und Format der ISO/IEC 27001 Foundation-Prüfung der TÜV Süd Akademie entsprechen, aber ein auch von anderen Anbietern häufig verwendetes Prüfungsschema darstellen. In Anhang C sind 40 weitere Prüfungsfragen am Stück abgedruckt; dies entspricht dem Umfang der „richtigen“ Prüfung, sodass Sie ein Gespür für die 60 Minuten Prüfungszeit entwickeln können. Die begründeten Musterlösungen zu allen 80 Prüfungsfragen finden Sie dort ebenfalls.

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

München, im Juli 2024

*Die Autoren*



Aufgrund der besseren Lesbarkeit haben wir auf eine gendergerechte Sprache verzichtet. Selbstverständlich sprechen wir aber alle Personen jeglichen Geschlechts gleichermaßen an.

Verweise auf *Kapitel* beziehen sich ohne weitere Angabe immer auf dieses Buch. Verweise auf *Abschnitte* beziehen sich immer auf den entsprechenden Standard.

# 5

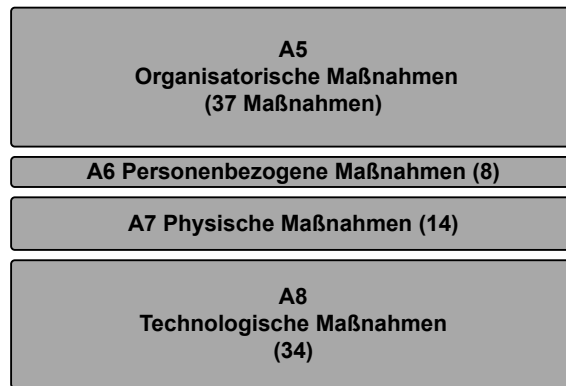
## Maßnahmen im Rahmen des ISMS

Im normativen Anhang A *Verweisungen auf Informationssicherheitsmaßnahmen* (vgl. S. 220) beschreibt DIN EN 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 in jedem Fall als vollständig und abschließend zu betrachten; jede Organisation muss sich 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 DIN EN 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 DIN EN ISO/IEC 27001 waren es elf und dann 14. Die Kapitel von ISO/IEC 27002 verwenden ebenfalls diese Struktur und Reihenfolge. Auch die Anzahl der Maßnahmen wurde von ursprünglich 133 über 114 auf mittlerweile 93 konsolidiert.

In diesem Kapitel gehen wir auf alle in Anhang A von DIN EN 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 DIN EN ISO/IEC 27001 Foundation-Kurses wider. Zu ausgewählten Maßnahmen werden in Anlehnung an ISO/IEC 27002 jeweils auch praktische Beispiele zur Umsetzung gegeben. An einigen Stellen wird auf typische Dokumente und Aufzeichnungen bzw. Ergebnisse der Maßnahmenumsetzung eingegangen, die bei der Durchführung interner oder externer Audits oft als Auditnachweise herangezogen werden.

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 DIN EN ISO/IEC 27001 genannt sind, besprochen:

<b>Anhang</b>	<b>Bezeichnung</b>	<b>ab Seite</b>
A.5	Organisatorische Maßnahmen	82
A.6	Personenbezogene Maßnahmen	108
A.7	Physische Maßnahmen	115
A.8	Technologische Maßnahmen	126



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

## ■ 5.1 A.5 Organisatorische Maßnahmen

### 5.1.1 [A.5.1] Informationssicherheitspolitik und -richtlinien

Maßnahme A.5.1 behandelt die Informationssicherheitspolitik und -richtlinien und ist eine präventive Maßnahme.



Maßnahme **Informationssicherheitspolitik und -richtlinien** nach DIN EN ISO/IEC 27001:

Informationssicherheitspolitik und themenspezifische Richtlinien müssen definiert, von der Geschäftsleitung genehmigt, veröffentlicht, dem zuständigen Personal und den interessierten Parteien mitgeteilt und von diesen zur Kenntnis genommen sowie in geplanten Abständen und bei wesentlichen Änderungen überprüft werden.

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.

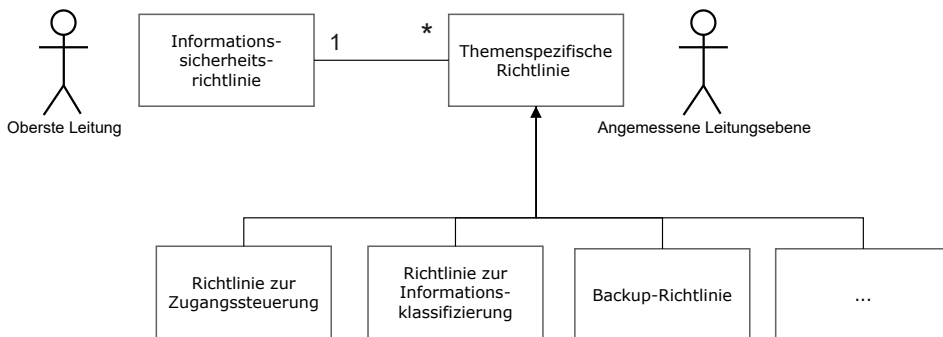
Berücksichtigt werden sollten in der übergeordneten Richtlinie allgemeine ISMS-Ziele und -Prinzipien (z. B. risikobasierter Ansatz, Schutz von Werten, kontinuierliche Verbesserung), aber auch vertragliche und gesetzliche Rahmenbedingungen sowie Strategien und allgemeine Ziele der Organisation. Die Richtlinie 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 Zugangsrechte (siehe Kapitel 5.1.15 und 5.1.18)
- Lieferantenbeziehungen (siehe Kapitel 5.1.19)
- Verwendung von Cloud-Diensten (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-Arbeit (siehe Kapitel 5.2.7)
- Aufgeräumte Schreibtische und Gerätesperren (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] Informationssicherheitsrollen und -verantwortlichkeiten

Maßnahme A.5.2 behandelt die Informationssicherheitsrollen und -verantwortlichkeiten und ist eine präventive Maßnahme.



Maßnahme **Informationssicherheitsrollen und -verantwortlichkeiten** nach DIN EN ISO/IEC 27001:

Die Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit müssen entsprechend den Erfordernissen des Unternehmens definiert und zugewiesen werden.

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 sind 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 Informationssicherheit 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

Maßnahme A.5.3 behandelt die Aufgabentrennung und ist eine präventive Maßnahme.



Maßnahme **Aufgabentrennung** nach DIN EN ISO/IEC 27001:  
Sich widersprechende Aufgaben und Verantwortungsbereiche müssen voneinander getrennt werden.

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] Verantwortlichkeiten der Leitung

Maßnahme A.5.4 behandelt die Verantwortlichkeiten der Leitung und ist eine präventive Maßnahme.

Maßnahme **Verantwortlichkeiten der Leitung** nach DIN EN ISO/IEC 27001:  
Die Leitung muss vom gesamten Personal verlangen, dass es die Informationssicherheit im Einklang mit der eingeführten Informationssicherheitspolitik, und den themenspezifischen Richtlinien und Verfahren der Organisation umsetzt.

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 Organisation 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 sollten dafür auch motiviert und kontinuierlich weitergebildet werden (siehe auch Kapitel 5.2.3).

### 5.1.5 [A.5.5] Kontakt mit Behörden

Maßnahme A.5.5 behandelt den Kontakt mit Behörden und ist eine präventive, korrigierende Maßnahme.



Maßnahme **Kontakt mit Behörden** nach DIN EN ISO/IEC 27001:  
Die Organisation muss mit den zuständigen Behörden Kontakt aufnehmen und halten.

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 mit speziellen Interessensgruppen

Maßnahme A.5.6 behandelt den Kontakt mit speziellen Interessensgruppen und ist eine präventive, korrigierende Maßnahme.

Maßnahme **Kontakt mit speziellen Interessensgruppen** nach DIN EN ISO/IEC 27001:  
Die Organisation muss mit speziellen Interessensgruppen oder sonstigen sicherheitsorientierten Expertenforen und Fachverbänden Kontakt aufnehmen und halten.

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

A.6.1.4 Kontakt mit speziellen Interessengruppen

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 Koordination geschlossen werden. Als Beispiel für spezielle Interessengruppen sind hier CERTs (Computer Emergency Response Teams) oder deren Verbände zu nennen. Diese können mit sachdienlichen Hinweisen die Schutzmaßnahmen unterstützen oder stetig verbessern helfen.



### 5.1.7 [A.5.7] Informationen über die Bedrohungslage

Maßnahme A.5.7 behandelt die Informationen über die Bedrohungslage und ist eine präventive, detektierende, korrigierende Maßnahme.



Maßnahme **Informationen über die Bedrohungslage** nach DIN EN ISO/IEC 27001: Informationen über Bedrohungen der Informationssicherheit müssen erhoben und analysiert werden, um Erkenntnisse über Bedrohungen zu gewinnen.

Korrespondiert mit **DIN EN ISO/IEC 27001:2017**:  
(neu)

Informationen zur allgemeinen Gefährdungs- bzw. Bedrohungslage (z. B. aus BSI-Lageberichten) können dazu genutzt werden, um Bedrohungen zu verhindern, zu erkennen oder besser darauf reagieren zu können. Insbesondere stellen solche Daten einen wichtigen Input für die Beurteilung von Informationssicherheitsereignissen (vgl. Kapitel 5.1.25) sowie für die angemessene Konfiguration von Antiviren-Software, Angriffserkennungssystemen und Webfiltern (vgl. Kapitel 5.4.7, 5.4.16 und 5.4.23) dar.

### 5.1.8 [A.5.8] Informationssicherheit im Projektmanagement

Maßnahme A.5.8 behandelt die Informationssicherheit im Projektmanagement und ist eine präventive Maßnahme.

Maßnahme **Informationssicherheit im Projektmanagement** nach DIN EN ISO/IEC 27001:  
Die Informationssicherheit muss in das Projektmanagement integriert werden.

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

A.6.1.5 Informationssicherheit im Projektmanagement

A.14.1.1 Analyse und Spezifikation von Informationssicherheitsanforderungen

Bei allen Projekten – insbesondere natürlich bei denen, durch die sich potenziell sicherheitsrelevante Änderungen für die Organisation oder ihre Werte ergeben – ist die Informationssicherheit von Anfang an zu berücksichtigen.

Informationssicherheitsziele sind also Teil der Projektziele, Anforderungen an das Projektergebnis beinhalten Sicherheitsanforderungen, Informationssicherheitsrisiken werden neben den anderen Projektrisiken bewertet und gemanagt und so weiter. Das heißt, die Berücksichtigung der Informationssicherheit ist fester Bestandteil der Projektmethodik der Organisation.

### 5.1.9 [A.5.9] Inventar der Informationen und anderen damit verbundenen Werte

Maßnahme A.5.9 behandelt ein Inventar der Informationen und anderen damit verbundenen Werten und ist eine präventive Maßnahme.



Maßnahme **Inventar der Informationen und anderen damit verbundenen Werte** nach DIN EN ISO/IEC 27001:

Ein Inventar der Informationen und anderen damit verbundenen Werte, einschließlich der Eigentümer, muss erstellt und gepflegt werden.

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

A.8.1.1 Inventarisierung der Werte

A.8.1.2 Zuständigkeit für Werte

Ein Inventar der Assets bzw. Werte (vgl. Kapitel 3.1.1) dient dazu, einen vollständigen Überblick über die zu schützenden Werte der Organisation zu haben. Dies ist eine fundamentale Voraussetzung für das Risikomanagement (vgl. Kapitel 4.6.1), in dem die Risiken für diese Werte bestimmt und bewertet werden. Wie bei den Risiken sind auch allen Werten verantwortliche Eigentümer zuzuordnen.

In Anlehnung an die Empfehlungen der ISO/IEC 27005 [ISO22f] zur Risikoidentifikation unterscheidet man oft grundsätzlich zwischen primären Assets, also dem, was primär geschützt werden soll (Informationen oder auch Geschäftsprozesse), und den unterstützenden Assets, welche die primären Assets unterstützen, verarbeiten usw. (also z. B. informationsverarbeitende Systeme). Wichtig ist in diesem Fall eine saubere Dokumentation der Abhängigkeiten zwischen den Assets, da sich der Schutzbedarf an den primären Assets orientiert, Gefährdungen sich in der Regel aber auf unterstützende Assets beziehen.

### 5.1.10 [A.5.10] Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten

Maßnahme A.5.10 behandelt den zulässigen Gebrauch von Informationen und anderen damit verbundenen Werten und ist eine präventive Maßnahme.

Maßnahme **Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten** nach DIN EN ISO/IEC 27001:

Regeln für den zulässigen Gebrauch und Verfahren für den Umgang mit Informationen und anderen damit verbundenen Werten müssen aufgestellt, dokumentiert und angewendet werden.

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

A.8.1.3 Zulässiger Gebrauch von Werten

A.8.2.3 Handhabung von Werten

Für den Umgang mit Informationen und anderen Werten sollte eine themenspezifische Richtlinie definiert werden. Diese sollte grundlegend regeln, was eine zulässige Verwen-

dung, Speicherung, Herausgabe usw. von Information je nach deren Klassifizierung (vgl. Kapitel 5.1.12) darstellt.

Beispielsweise kann in solch einer Richtlinie geregelt sein, unter welchen Voraussetzungen und Auflagen als „intern“ klassifizierte Information an externe Parteien (z. B. Kunden, Partner, Lieferanten) herausgegeben werden kann.

### 5.1.11 [A.5.11] Rückgabe von Werten

Maßnahme A.5.11 behandelt die Rückgabe von Werten und ist eine präventive Maßnahme.



Maßnahme **Rückgabe von Werten** nach DIN EN ISO/IEC 27001:

Das Personal und gegebenenfalls andere interessierte Parteien müssen alle Werte der Organisation, die sich in ihrem Besitz befinden, bei Änderung oder Beendigung ihres Beschäftigungsverhältnisses, Vertrags oder ihrer Vereinbarung zurückgeben.

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

#### A.8.1.4 Rückgabe von Werten

Welche Schritte im Hinblick auf die Rückgabe von Werten bei Beendigung oder Änderung von Beschäftigungsverhältnissen und die damit verbundenen Verträge und Vereinbarungen durchzuführen sind, wird am besten in einem Prozess oder Verfahren definiert und dokumentiert. Ein zentrales Element dabei kann eine Checkliste sein, die idealerweise in digitalisierter Form im Rahmen der Abwicklung des jeweiligen Vorgangs abgearbeitet wird. Es sollte Klarheit darüber geschaffen werden, wie die Rückgabe physischer und elektronischer Werte, darunter Anwender-Endgeräte (Laptop, Smartphone), Datenträger, physische Schlüssel und Authentifizierungsmedien, durchgeführt wird. Das schließt auch die Fragen nach den Zuständigkeiten und Dokumentationsanforderungen zur Sicherstellung der Nachvollziehbarkeit ein. Typische Nachweise für die Umsetzung dieser Maßnahme im Rahmen von Audits sind neben dem festgelegten Verfahren vor allem ausgefüllte Checklisten (auch denkbar als Teil von Tickets in einem Ticketsystem) oder gegengezeichnete Rückgabe- bzw. Rücknahmeprotokolle.

Logische Werte im weiteren Sinne, wie etwa Zugänge zu IT-Diensten und -Systemen oder erworbenes Wissen, können nicht im eigentlichen Wortsinne „zurückgegeben“ werden. Sie fallen entsprechend nicht unter diese Maßnahme. Allerdings werden Themen wie die Sicherstellung, dass Vertraulichkeit auch über eine Beendigung der Beschäftigung hinaus gewahrt wird, oder der Entzug von nicht mehr benötigten Zugangsrechten im Rahmen anderer Maßnahmen adressiert.

### 5.1.12 [A.5.12] Klassifizierung von Informationen

Maßnahme A.5.12 behandelt die Klassifizierung von Informationen und ist eine präventive Maßnahme.



Maßnahme **Klassifizierung von Informationen** nach DIN EN ISO/IEC 27001: Informationen müssen entsprechend den Informationssicherheitsanforderungen der Organisation auf der Grundlage von Vertraulichkeit, Integrität, Verfügbarkeit und relevanten Anforderungen der interessierten Parteien klassifiziert werden.

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

#### A.8.2.1 Klassifizierung von Informationen

Grundlage der Umsetzung dieser Maßnahme ist ein Klassifizierungsschema, das idealerweise als Teil einer themenspezifischen Richtlinie definiert wird. In der Anwendung wird es dann zunächst darum gehen, die Informationswerte im Asset-Inventar entsprechend ihrer Informationssicherheitsanforderungen bzw. ihres Schutzbedarfs zu klassifizieren. Dies erfolgt in der Praxis meistens auf Basis der drei „CIA“-Schutzziele, gegebenenfalls (z. B. wo durch behördliche Anforderungen verlangt) ergänzt um weitere Schutzziele wie die Authentizität.

Bei der Klassifizierung einzelner Dokumente (also z. B. Verträge, Protokolle, Präsentationen, E-Mails usw.) liegt der Fokus meistens auf der Vertraulichkeit. Ziel ist es dabei vor allem, den Umgang mit Kopien und Ausdrucken dieser Dokumente für alle Angehörigen der Organisation und ggf. auch für externe Parteien klar zu regeln. Hier erfolgt die Klassifizierung dann meistens mit nur einer Kategorie bzw. auf einer Achse, die dann beispielsweise von „0 – nicht klassifiziert/öffentlich“ über „1 – nur für den internen Gebrauch“ und „2 – geheim/vertraulich“ bis „3 – streng geheim/streng vertraulich“ reicht. Natürlich können auch nur mit einer Kategorie ab einer bestimmten Stufe Regelungen nicht nur hinsichtlich der Geheimhaltung, sondern auch der Sicherung von Verfügbarkeit und Integrität festgelegt werden.

In der deutschen Behördenlandschaft kommt im Regelfall die Verschlusssachenanweisung (VSA) des Bundesministeriums des Inneren und für Heimat zum Einsatz. Bei gegenüber *offenen* Informationen erhöhtem Schutzbedarf kommen dabei die vier Abstufungen *VS-NfD* (Verschlusssache, nur für Dienstgebrauch), *VS-vertraulich*, *geheim* und *streng geheim* zum Einsatz. In der organisationsübergreifenden, auch internationalen Kommunikation findet hingegen häufig das sogenannte Traffic Light Protocol (TLP) Anwendung. In Anlehnung an Ampelfarben mit ihrer englischen Bezeichnung werden dabei einerseits die Abstufungen *green* (Weitergabe an andere Organisationen, aber keine Veröffentlichung), *amber* (Weitergabe an Partner und Dritte gemäß dem Prinzip „Kenntnis nur, wenn nötig“) und *red* (persönlich, nur für bekannte Empfänger) verwendet. Andererseits wird *clear* (früher *white*) für die unbegrenzte Weitergabe verwendet, und *amber* kann in Form von *amber:strict* eine Weitergabe an Dritte, also einen über die direkt beteiligten Organisationen hinausgehenden Verteilerkreis, einschränken.

### 5.1.13 [A.5.13] Kennzeichnung von Informationen

Maßnahme A.5.13 behandelt die Kennzeichnung von Informationen und ist eine präventive Maßnahme.



Maßnahme **Kennzeichnung von Informationen** nach DIN EN ISO/IEC 27001:  
Ein angemessener Satz von Verfahren zur Kennzeichnung von Informationen muss entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema entwickelt und umgesetzt werden.

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

#### A.8.2.2 Kennzeichnung von Information

Die Informationsklassifizierung entfaltet natürlich nur dann ihre Wirksamkeit, wenn man Informationen ihre zugewiesene Klasse auch ansehen kann. Eine Herausforderung bei der Kennzeichnung der Informationen ist, dass selten eine einzelne Methode ausreicht, um alle Formate und Trägermedien von Informationen abzudecken.

Beispielsweise könnte die Klassifizierung eines Vertragsdokuments als „geheim/vertraulich“ direkt in die Fußzeile oder Kopfzeile auf jeder Seite geschrieben werden – sie könnte aber auch, wenn der Vertrag in einem elektronischen Dokumentenmanagementsystem verwaltet wird, in dort verwalteten Metadaten erfasst werden. Manche Information in anderen Formaten lässt sich eventuell nur indirekt (z. B. über eine Zuordnungsliste) oder implizit (über spezifizierte Ablageorte) einer Klasse zuordnen.

### 5.1.14 [A.5.14] Informationsübermittlung

Maßnahme A.5.14 behandelt die Informationsübermittlung und ist eine präventive Maßnahme.

Maßnahme **Informationsübermittlung** nach DIN EN ISO/IEC 27001:  
Für alle Arten von Übermittlungseinrichtungen innerhalb der Organisation und zwischen der Organisation und anderen Parteien müssen Regeln, Verfahren oder Vereinbarungen zur Informationsübermittlung vorhanden sein.

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

#### A.13.2.1 Richtlinien und Verfahren zur Informationsübertragung

#### A.13.2.2 Vereinbarungen zur Informationsübertragung

#### A.13.2.3 Elektronische Nachrichtenübermittlung

Zur Verarbeitung und Nutzung müssen Informationen und Daten oft zwischen verschiedenen internen und externen Stellen ausgetauscht werden. Auch hier bietet sich die Dokumentation grundlegender Vorgaben in einer themenspezifischen Richtlinie an. Bei der Definition der im Kontext dieses Themas verfolgten Informationssicherheitsziele spielen auch die in der Kommunikation und bei Transaktionen anzuwendenden Schutzziele Authentizität und Nichtabstreitbarkeit häufig eine Rolle.

Informationsübermittlung kann nicht nur zwischen vielen Stellen, sondern auch über unterschiedliche Arten – elektronisch, physisch oder mündlich – erfolgen. Entsprechend können die Regelungen ein breites Spektrum umfassen wie

- Vorgaben für den Abschluss von Vertraulichkeitsvereinbarungen,
- Regeln für Besprechungen an öffentlichen Orten,

- Anweisungen zur Verpackung von Kuriersendungen und Auswahl geeigneter Versandmethoden,
- Verwendung von elektronischen Signaturen und Verschlüsselung im E-Mail-Verkehr etc.,

um nur einige zu nennen.

### 5.1.15 [A.5.15] Zugangssteuerung

Maßnahme A.5.15 behandelt die Zugangssteuerung und ist eine präventive Maßnahme.



Maßnahme **Zugangssteuerung** nach DIN EN ISO/IEC 27001:  
Regeln zur Steuerung des physischen und logischen Zugriffs auf Informationen und andere damit verbundene Werte müssen auf der Grundlage von Geschäfts- und Informationssicherheitsanforderungen aufgestellt und umgesetzt werden.

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

A.9.1.1 Zugangssteuerungsrichtlinie

A.9.1.2 Zugang zu Netzwerken und Netzwerkdiensten

Als Basis für ein Zugangskonzept sollten in einem ersten Schritt die Anforderungen an die Zugangskontrolle von den Eigentümern der betroffenen Assets (vgl. Kapitel 5.1.9) erhoben werden. Auf dieser Basis sind dann Fragen des physischen Zugangs bzw. Zutritts (z. B.: „Wer darf in welchen Raum?“, „Wer hat die Schlüssel zu welchem Aktenschrank?“) und des logischen Zugangs bzw. Zugriffs (z. B.: „Wer darf auf welches Verzeichnis zugreifen?“, „Wer erhält Zugang zu welchem System?“, „Wer erhält welche Lese- und Schreibberechtigungen?“) zu klären.

Für schützenswerte Informationen sollten in diesem Zusammenhang Prinzipien wie „Need to know“ und „Least Privilege“ angewendet werden: Jeder erhält nur das Maß an Zugang, das er oder sie auch wirklich benötigt, und standardmäßig ist jeder Zugang zu Informationen verboten, der nicht explizit erlaubt wurde.

### 5.1.16 [A.5.16] Identitätsmanagement

Maßnahme A.5.16 behandelt das Identitätsmanagement und ist eine präventive Maßnahme.

Maßnahme **Identitätsmanagement** nach DIN EN ISO/IEC 27001:  
Der gesamte Lebenszyklus von Identitäten muss verwaltet werden.

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

A.9.2.1 Registrierung und Deregistrierung von Benutzern

Ziel dieser Maßnahme ist die Ermöglichung der eindeutigen Identifizierung und zuverlässigen Authentisierung von Personen und Systemen, die auf die Informationen der Organisation und andere zugehörige Assets ihren Berechtigungen entsprechend zugreifen.

Wenn möglich, sollte eine Identität immer nur genau einer natürlichen Person zugeordnet sein. Dieser Identität können dann entweder direkt oder, z. B. durch Gruppen- oder Rollenzuordnungen, indirekt Zugangsrechte (vgl. Kapitel 5.1.18) zugewiesen werden. Handlungen, die von dieser Identität mit den ihr zugewiesenen Zugangsrechten ausgeführt werden, lassen sich so wieder eindeutig zuordnen.

Neben natürlichen Personen können auch IT-Systeme, beispielsweise Server und Arbeitsplatz-PCs, oder Geräte wie Sensoren, z. B. in der Gebäudeleittechnik, eindeutige digitale Identitäten und Berechtigungen erhalten. Sofern sich mehrere Personen eine digitale Identität teilen, beispielsweise den *Administrator*-Account eines Systems oder ein funktionsbezogenes E-Mail-Postfach wie *support@domainname*, sollten weiterführende Maßnahmen ergriffen werden, um eine eindeutige Zuordnung durchgeführter Aktionen zu ermöglichen. Als Oberbegriff für die Verwaltung von digitalen Identitäten und Zugangsrechten wird in der Praxis oft auch der Begriff „Identity and Access Management“ (IAM) verwendet.

### 5.1.17 [A.5.17] Authentisierungsinformationen

Maßnahme A.5.17 behandelt Authentisierungsinformationen und ist eine präventive Maßnahme.



Maßnahme **Authentisierungsinformationen** nach DIN EN ISO/IEC 27001:  
Die Zuweisung und Verwaltung von Authentisierungsinformationen muss durch einen Managementprozess gesteuert werden, der auch die Beratung des Personals über den angemessenen Umgang mit Authentisierungsinformationen umfasst.

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

A.9.2.4 Verwaltung geheimer Authentisierungsinformation von Benutzern

A.9.3.1 Gebrauch geheimer Authentisierungsinformation

A.9.4.3 System zur Verwaltung von Kennwörtern

Bei den meisten IT-Systemen kommen nach wie vor Benutzername- und Passwort-Kombinationen für die Authentisierung zum Einsatz. Auch die Verwaltung zusätzlicher Authentisierungsmittel wie z. B. *security tokens* für eine Zwei-Faktor-Authentisierung sollte im Rahmen dieser Maßnahme geregelt werden.

Für die Verwaltung dieser Authentisierungsinformationen ist ein Prozess zu definieren. Dabei sollte klar festgelegt werden, wie Passwörter eingerichtet werden, welche Eigenschaften bzw. Qualitätsmerkmale sie haben müssen (Länge, enthaltene Sonderzeichen etc.), wann sie geändert werden müssen und so weiter.

Ein System zur Verwaltung von Passwörtern sollte insbesondere auch die Stärke des gewählten Passworts überprüfen. Von der früher geforderten regelmäßigen Passwortänderung wird mittlerweile Abstand genommen, da sie von vielen Personen nur minimalistisch umgesetzt wurde und somit als lästig gilt, ohne ihre ursprüngliche Intention zu erfüllen. Nur leicht variierte Passwörter könnten genauso gut durch systematisches Ausprobieren erraten werden wie die „Originale“. Passwörter sind aber mindestens dann zu ändern, wenn aus konkretem Anlass davon auszugehen ist, dass sie kompromittiert wurden.

Für eine starke Authentisierung sollten laut ISO/IEC 27002 neben dem Einsatz von Kennwörtern auch kryptographische Verfahren, Smartcards, Token oder biometrische Verfahren Anwendung finden. Für die weiterhin eingesetzten Passwörter können auch dedizierte Software-Werkzeuge, sogenannte Passwort-Manager, eingesetzt werden, die qualitativ gute Passwörter zufällig generieren und das Ausfüllen von Login-Formularen in Webbrowsern und anderen Anwendungen automatisieren, sodass man sich keine Vielzahl von Passwörtern mehr auswendig merken und sie manuell eintippen muss.

### 5.1.18 [A.5.18] Zugangsrechte

Maßnahme A.5.18 behandelt die Zugangsrechte und ist eine präventive Maßnahme.



Maßnahme **Zugangsrechte** nach DIN EN ISO/IEC 27001:  
Zugangsrechte zu Informationen und anderen damit verbundenen Werten müssen in Übereinstimmung mit der themenspezifischen Richtlinie und den Regeln der Organisation für die Zugangssteuerung bereitgestellt, überprüft, geändert und entfernt werden.

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

A.9.2.2 Zuteilung von Benutzerzugängen

A.9.2.5 Überprüfung von Benutzerzugangsrechten

A.9.2.6 Entzug oder Anpassung von Zugangsrechten

Es soll sichergestellt werden, dass der Zugang zu Informationen und anderen Werten entsprechend den Geschäftsanforderungen definiert und autorisiert wird.

Hierzu bedarf es eines formalen Prozesses, der neben der Erteilung von Zugangsrechten auch deren regelmäßige Überprüfung sowie bedarfsorientierte Änderungen bzw. deren Entzug regelt. In diesen Prozess sollten die Eigentümer der Assets, zu denen Zugang gewährt wird (vgl. Kapitel 5.1.9), zumindest grundlegend autorisierend eingebunden werden.

In der Praxis wird schon in mittelgroßen Organisationen das Geflecht zwischen den Assets und den zu berechtigenden Entitäten (Mitglieder der Organisation, externe Arbeitskräfte, Systeme usw.) schnell sehr komplex. Um das Management der Zugangsrechte inklusive der notwendigen regelmäßigen Überprüfung bestehender Berechtigungen handhabbar zu halten, empfiehlt sich die Verwendung standardisierter Benutzer- bzw. Berechtigungsprofile. Häufig kommt dabei rollenbasierte Zugriffskontrolle (engl. *role-based access control*, RBAC) zum Einsatz, bei der die Berechtigungen an zu definierende Rollen vergeben werden, denen dann wiederum einzelne Accounts oder Gruppen von Personen zugewiesen werden. Ebenso können oftmals Berechtigungen automatisch aus Attributen bzw. Datenfeldern digitaler Identitäten, z. B. der Zugehörigkeit zu Abteilungen oder Projekten, abgeleitet werden und müssen dann nicht mehr zusätzlich manuell vergeben werden (engl. *attribute-based access control*, ABAC).

Typische Nachweise für die Umsetzung dieser Maßnahme im Rahmen von Audits sind die dokumentierten Nutzer- und Berechtigungsprofile, Informationen über konkret zugewiesene Berechtigungen aus den jeweiligen IT-Systemen und Verzeichnisdiensten sowie Auf-



zeichnungen über durchgeführte Überprüfungen von Berechtigungen, etwa in Form von Checklisten oder Tickets.

### 5.1.19 [A.5.19] Informationssicherheit in Lieferantenbeziehungen

Maßnahme A.5.19 behandelt die Informationssicherheit in Lieferantenbeziehungen und ist eine präventive Maßnahme.



Maßnahme **Informationssicherheit in Lieferantenbeziehungen** nach DIN EN ISO/IEC 27001:

Es müssen Prozesse und Verfahren festgelegt und umgesetzt werden, um die mit der Nutzung der Produkte oder Dienstleistungen des Lieferanten verbundenen Informationssicherheitsrisiken zu beherrschen.

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

A.15.1.1 Informationssicherheit in Lieferantenbeziehungen

Die Organisation soll Prozesse und Verfahren identifizieren und umsetzen, um Risiken, die mit der Nutzung von Diensten oder Produkten von Lieferanten verbunden sind, zu adressieren. Dies umfasst u. a. die Dokumentation der Lieferanten, die Festlegung und Überprüfung angemessener Informationssicherheitsmaßnahmen bei den Lieferanten, ggf. notwendige Zertifizierungen, aber auch die Festlegung von Zugriffs- und Zugangsregelungen der Lieferanten auf Informationen und Werte des Unternehmens.

Unter Lieferanten sind in diesem Zusammenhang jegliche externe Organisationen zu verstehen, von denen Produkte oder Dienstleistungen bezogen werden. Aus Sicht der Aufrechterhaltung der Informationssicherheit haben nicht alle Lieferanten die gleiche Bedeutung. Besonders kritisch sind beispielsweise Lieferanten, die etwa Zugriff auf besonders schützenswerte Informationen der Organisation erhalten oder im Rahmen ihrer Leistungserbringung Zutritt zu Räumlichkeiten erhalten, in denen solche Informationswerte aufbewahrt oder verarbeitet werden. Typische Nachweise für die Umsetzung dieser Maßnahme im Rahmen von Audits sind eine Liste der Lieferanten, zusammen mit einer Bewertung ihrer Kritikalität für die Informationssicherheit. In der Praxis werden diese Informationen idealerweise als Teil des Lieferantenmanagements (Supplier Management) oder beim (zentralen) Einkauf gepflegt.

### 5.1.20 [A.5.20] Behandlung von Informationssicherheit in Lieferantenvereinbarungen

Maßnahme A.5.20 behandelt die Informationssicherheit in Lieferantenvereinbarungen und ist eine präventive Maßnahme.

Maßnahme **Behandlung von Informationssicherheit in Lieferantenvereinbarungen** nach DIN EN ISO/IEC 27001:

Je nach Art der Lieferantenbeziehung müssen die entsprechenden Anforderungen an die Informationssicherheit festgelegt und mit jedem Lieferanten vereinbart werden.

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

#### A.15.1.2 Behandlung von Sicherheit in Lieferantenvereinbarungen

Verträge mit jedem Lieferanten dienen dem klaren Verständnis zwischen dem Lieferanten und der Organisation. Darin werden die Rechte und Pflichten zur Erfüllung der Anforderungen sowie der Maßnahmen der Informationssicherheit, die für beide Parteien gelten, festgelegt. Eine solche Vereinbarung umfasst z. B. neben rechtlichen, regulatorischen, datenschutzrechtlichen, urheberrechtlichen u. ä. Regelungen auch die Mindestanforderungen der Informationssicherheit, die zu erfüllen sind. Der Lieferant muss regelmäßig die Effektivität seiner Maßnahmen gegenüber der Organisation belegen.

Typische Nachweise für die Umsetzung dieser Maßnahme im Rahmen von Audits sind informationssicherheitsrelevante Klauseln in Verträgen mit Lieferanten, gegebenenfalls entsprechende Vertragsanlagen oder auch Informationssicherheitsrichtlinien, die speziell für (unterschiedliche Kategorien von) Lieferanten erstellt wurden und die organisatorischen, personellen, physischen und technischen Anforderungen beschreiben, die durch Lieferanten umzusetzen sind – zusammen mit Aufzeichnungen darüber, dass, wann und durch wen die Lieferanten die Anforderungen zur Kenntnis genommen bzw. ihre Einhaltung bestätigt haben.

### 5.1.21 [A.5.21] Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie (IKT)

Maßnahme A.5.21 behandelt den Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie (IKT) und ist eine präventive Maßnahme.



Maßnahme **Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie (IKT)** nach DIN EN ISO/IEC 27001:

Es müssen Prozesse und Verfahren festgelegt und umgesetzt werden, um die mit der IKT-Produkt- und Dienstleistungslieferkette verbundenen Informationssicherheitsrisiken zu beherrschen.

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

#### A.15.1.3 Lieferkette für Informations- und Kommunikationstechnologie

Die mit den Lieferanten geschlossenen Vereinbarungen sollen die zugrunde liegenden IKT-Dienste sowie die gesamte Lieferkette berücksichtigen. Nutzt ein Lieferant zur Erbringung seiner Dienste Unterauftragnehmer, dann müssen die mit dem Lieferanten vereinbarten Sicherheitsmaßnahmen und Regelungen auch für die Zulieferer gelten. Die Organisation muss auch wissen, welche Zulieferer an der IKT-Lieferkette beteiligt sind und wie die nachgelagerte *supply chain* auf die mit der Organisation vereinbarten Regelungen verpflichtet wurde. Nur durch die Einbeziehung der gesamten Lieferkette lässt sich ein angemessenes Sicherheitsniveau erreichen.

### 5.1.22 [A.5.22] Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen

Maßnahme A.5.22 behandelt die Überwachung, Überprüfung und das Änderungsmanagement von Lieferantendienstleistungen und ist eine präventive Maßnahme.



Maßnahme **Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen** nach DIN EN ISO/IEC 27001:

Die Organisation muss regelmäßig die Informationssicherheitspraktiken der Lieferanten und die Erbringung von Dienstleistungen überwachen, überprüfen, bewerten und Änderungen steuern.

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

A.15.2.1 Überwachung und Überprüfung von Lieferantendienstleistungen

A.15.2.2 Handhabung der Änderungen von Lieferantendienstleistungen

DIN EN ISO/IEC 27001 spricht hier drei Aufgaben der Organisation bei ihren Lieferanten an:

- „Überwachen“ (*monitor*): Erfassung und ggf. Zusammenstellung von Kennzahlen, die in der Regel automatisiert und in Echtzeit gemessen werden.
- „Überprüfen“ (*review*): Allgemeine Überprüfung, beispielsweise durch Auswertung von Service-Reports, bzw. die Evaluierung von Lieferanten mittels (Lieferanten-)Audits.
- „Änderungsmanagement“ (*change management*): Auch die Dienste der Lieferanten unterliegen einem Änderungsmanagement, das von der Organisation überwacht werden muss. Hierbei zu berücksichtigende Änderungen liegen also nicht nur vor, wenn sich an der Dienstleistung selbst etwas ändert, sondern auch, wenn sich z. B. sicherheitsrelevante Verfahren oder Maßnahmen in der eigenen Organisation oder beim Dritten verändern.

Die Leistungen der Lieferanten werden also mit den gleichen Ansätzen überprüft, die in einem Managementsystem im „Check“ des PDCA-Zyklus zum Einsatz kommen. Der Standard empfiehlt, für das Management der Lieferantenbeziehungen einen Verantwortlichen bzw. ein verantwortliches Team zu benennen und mit den notwendigen Ressourcen auszustatten.

Typische Nachweise für die Umsetzung dieser Maßnahme im Rahmen von Audits sind Aufzeichnungen darüber, mithilfe welcher konkreter Mechanismen die Einhaltung der Informationssicherheitsanforderungen, die durch Lieferanten erfüllt werden müssen, überprüft wurden.

### 5.1.23 [A.5.23] Informationssicherheit für die Nutzung von Cloud-Diensten

Maßnahme A.5.23 behandelt die Informationssicherheit für die Nutzung von Cloud-Diensten und ist eine präventive Maßnahme.



Maßnahme **Informationssicherheit für die Nutzung von Cloud-Diensten** nach DIN EN ISO/IEC 27001:

Die Verfahren für den Erwerb, die Nutzung, die Verwaltung und den Ausstieg aus Cloud-Diensten müssen in Übereinstimmung mit den Informationssicherheitsanforderungen der Organisation festgelegt werden.

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

(neu)

In der Regel sind Cloud-Serviceverträge vordefiniert und bieten wenig Spielraum für individuelle Verhandlungen oder Vereinbarungen. Die Organisation sollte eine Cloud-Strategie entwickeln und an alle relevanten Parteien kommunizieren. Die Serviceverträge sollten einer Risikoanalyse im Hinblick auf Informationssicherheit unterzogen werden. Etwaige verbleibende Risiken, die mit der Nutzung von Cloud-Diensten verbunden sind, müssen klar identifiziert und von der Leitung akzeptiert werden.

Die Nutzung von Clouds kann mit geteilten Verantwortlichkeiten und kooperativen Leistungen zwischen Cloud-Provider und Cloud-Kunde einhergehen. Entscheidend hierbei ist wieder, dass die Verantwortlichkeiten klar definiert und angemessen umgesetzt werden.

Typische Nachweise für die Umsetzung dieser Maßnahme im Rahmen von Audits sind etwa ausgefüllte Checklisten über die Evaluation (Bewertung) eingesetzter Cloud-Dienste im Hinblick auf die relevanten Aspekte der Informationssicherheit, Aufzeichnungen über die getroffenen Entscheidungen für oder gegen den Einsatz von Cloud-Diensten auf Basis dieser Evaluationen sowie Dokumentationen über bewertete Risiken im Zusammenhang mit Cloud-Diensten, wenn diese bestimmte Anforderungen nicht erfüllen oder Schwachstellen aufweisen.

### 5.1.24 [A.5.24] Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen

Maßnahme A.5.24 behandelt die Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen und ist eine reagierende Maßnahme.

Maßnahme **Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen** nach DIN EN ISO/IEC 27001:

Die Organisation muss die Handhabung von Informationssicherheitsvorfällen planen und vorbereiten, indem sie Prozesse, Rollen und Verantwortlichkeiten für die Handhabung von Informationssicherheitsvorfällen definiert, einführt und kommuniziert.

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

A.16.1.1 Verantwortlichkeiten und Verfahren

Im Einklang mit dem Prinzip des prozessorientierten Ansatzes, der durch ein Managementsystem verfolgt wird, müssen vor allem diese zwei Fragen klar beantwortet werden: Wer ist in welcher Rolle involviert, wenn es um Informationssicherheitsvorfälle geht? Was ist in Abhängigkeit von der jeweiligen Situation konkret zu tun?

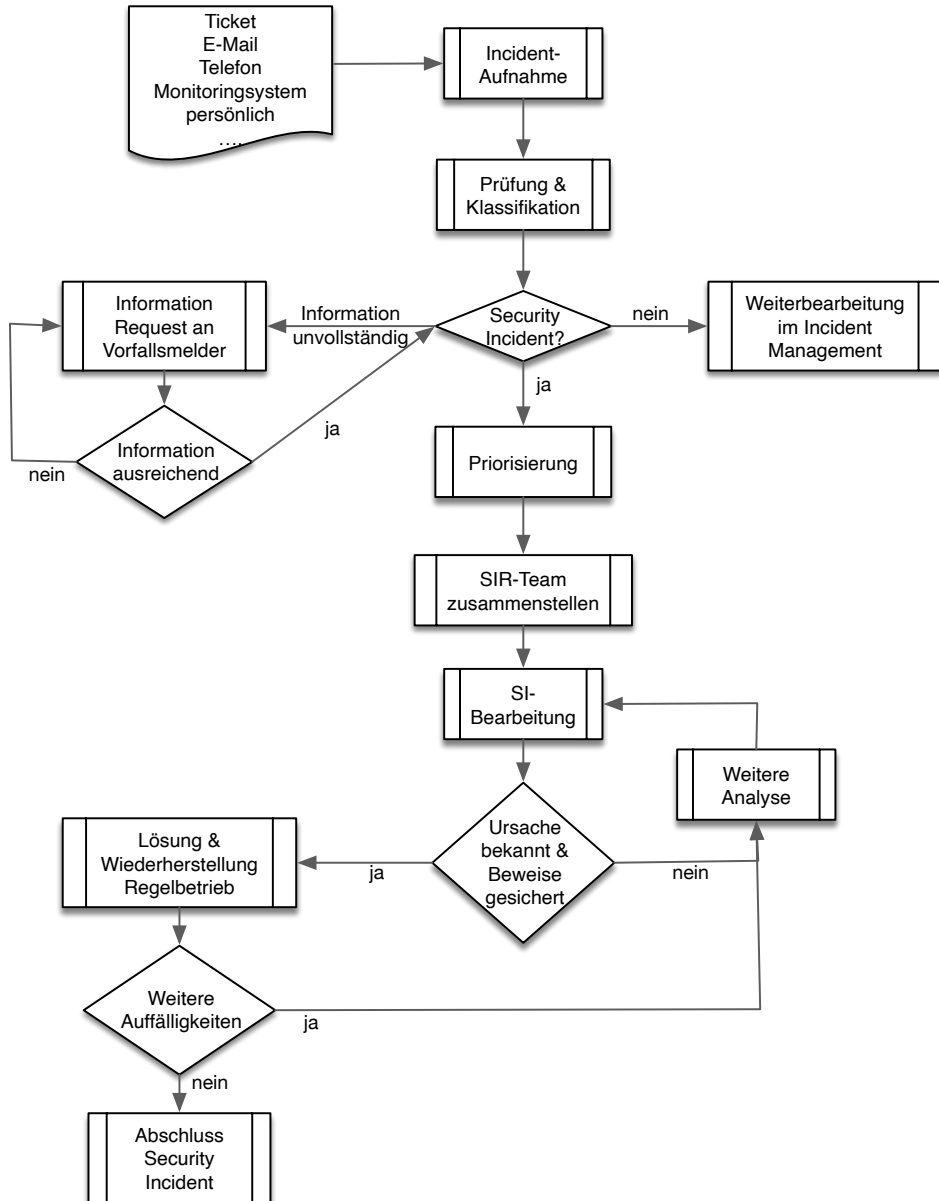
Der entsprechende Prozess zur Behandlung eines Informationssicherheitsvorfalls wird vorab festgelegt. Abbildung 5.3 stellt ein Beispiel eines möglichen Ablaufdiagramms dar. Eindeutige und wirksam an die betroffenen Personenkreise kommunizierte Festlegungen sind hier wichtig, um den Aspekt der Konsistenz zu adressieren. Verantwortlichkeiten werden typischerweise festgelegt, indem Rollen definiert und (dauerhaft oder temporär/situationsabhängig) Personen oder Gruppen zugewiesen werden. Denkbare Rollen sind ein Prozessverantwortlicher für den *Security Incident Response-(SIR-)*Prozess sowie ein Manager, auch als *Security Incident Coordinator (SIC)* bezeichnet, der für jeden identifizierten Informationssicherheitsvorfall bestimmt wird. Der SIC stellt ein aus festen und variablen Mitgliedern bestehendes Expertenteam zusammen, das schnell und konzentriert jeden Informationssicherheitsvorfall behandelt (siehe Kapitel 5.1.26). Zusammen bilden diese Personen, ggf. zusammen mit dem Vorfallsmelder, das SIR-Team, das den konkreten Informationssicherheitsvorfall (SI) bearbeitet. In der Literatur findet man hierfür häufig auch den Begriff *Computer Security Incident Response Team (CSIRT)*. Aus dem Team wird ein *CSIRT-Hotliner* bestimmt, der in Abstimmung mit dem SIC die externe ebenso wie die interne Kommunikation übernimmt und damit den Experten den Rücken frei hält. Bei schwerwiegenden Sicherheitsvorfällen wird die Leitung beteiligt und mit ihr die Vorfallobearbeitung ebenso wie die Kommunikationsstrategie abgestimmt. Sowohl die Aufgaben als auch die Befugnisse, wie etwa (temporäre) Weisungsbefugnisse gegenüber anderen Personen im Falle eines Informationssicherheitsvorfalls, sollten als Teil von Rollenbeschreibungen klar definiert werden.

Bevor man auf Informationssicherheitsvorfälle reagieren kann, stellt sich die Frage, auf Basis welcher Informationen diese eigentlich erkannt werden können. Die wichtigste Quelle zur Identifikation von Informationssicherheitsvorfällen sind Informationssicherheitsereignisse. Informationssicherheitsereignisse müssen einzeln betrachtet nicht notwendigerweise besorgniserregend sein. Häufig entsteht erst in einer bestimmten Korrelation, etwa einer Häufung in einem bestimmten Zeitintervall, ein Verdacht auf eine Verletzung von Informationssicherheitsregeln oder -maßnahmen. Ein fehlgeschlagener Authentisierungsversuch aufgrund eines falschen Passworts ist ein Beispiel dafür. Während in vielen Fällen ein großer Teil der Informationssicherheitsereignisse durch ein technisches Monitoring der IT- und Kommunikationsinfrastruktur identifiziert und aufgezeichnet werden kann, darf nicht außer Acht gelassen werden, dass sich manche Anhaltspunkte für mögliche Verletzungen der Informationssicherheit frühzeitiger oder sogar ausschließlich aus dem Wissen und der Erfahrung von Personen in Verbindung mit der entsprechenden Aufmerksamkeit im täglichen Betrieb ergeben. Hierfür müssen entsprechende Meldewege und Dokumentationsmöglichkeiten geschaffen werden.

### **5.1.25 [A.5.25] Beurteilung und Entscheidung über Informationssicherheitsereignisse**

Maßnahme A.5.25 behandelt die Beurteilung und Entscheidung über Informationssicherheitsereignisse und ist eine detektierende Maßnahme.

### Informationssicherheitsereignis



**Abbildung 5.3** Prozess zur Behandlung von Informationssicherheitsvorfällen

# Index

#Detektiv 32  
#Korrektiv 32  
#Präventiv 32

## A

ABAC *siehe* Attribute based access control  
Abhören 124  
Abnahme 146  
Abnahmetest 146  
Abschreckung 111, 118  
Abweichung  
– Hauptabweichung 168  
– Nebenabweichung 168  
Access Control 7  
Accountability 7  
Accredited Training Organizations 172  
Act-Phase 37, 39, 74  
Änderungen 59, 97  
Änderungssteuerung **148**  
Akkreditierung 19, **168**  
Aktivität 29  
Akzeptanzkriterien 146  
Alarmanlage 119  
Allowlisting 142  
Analyse 67  
Anforderung 190  
– behördlich 104  
– gesetzlich 104  
– KRITIS 9  
– vertraglich 104  
Anforderungsmanagement 144  
Angriff 179  
Anlieferungen 117  
Anonymisierung 133  
Anwendungen 153  
Anwendungsbereich 16, **43**, 46, 58, 168, 171  
Anwendungssicherheit 144  
APMG 173

App *siehe* Anwendungen  
Arbeitsverträge 109  
Asset *siehe* Wert  
Asset Management 118  
ATO *siehe* Accredited Training Organizations  
Attributbasierte Zugangskontrolle 94  
Attribute based access control 94  
Audit 21, **70**, 75, 106, 149, 167, 170, 179  
– Begriffe 70  
– Bericht 72, 168  
– Drittparteien- 179  
– Erstparteien- 179  
– externes 71, 179  
– internes 70, 179  
– Nachweise 71  
– Programm 159  
– Protokoll 72  
– Schutz 149  
– Umfang 171, 180  
Auditierung 159  
Auditor 72, 161  
Aufgabe des Managements 30  
Aufgabentrennung 85  
Aufgeräumte Arbeitsumgebung 121  
Aufzeichnung **29**, 105  
Ausbildung 110  
Ausgelagerte Entwicklung 147  
Ausgliedern 189  
Ausweise 117  
Authentication *siehe* Authentisierung  
Authenticity *siehe* Authentizität  
Authentisierung **6**, 93, 129, 180  
– Mehrfaktor 117, 129  
Authentizität **6**, 90, 91, 180  
Availability *siehe* Verfügbarkeit  
AXELOS 162

**B**

B3S *siehe* Branchenspezifische Sicherheitsstandards  
 Büros *siehe* Räume  
 Backup 134  
 BBK *siehe* Bundesamt für Bevölkerungsschutz und Katastrophenhilfe  
 BCP *siehe* Business Continuity Plan  
 Bedrohung 194  
 Bedrohungslage 87  
 Befugnisse 51  
 Benutzer 126  
 Beschädigung 121, 124  
 Beschäftigungsverhältnis 111  
 – Beendigung 111  
 – Wechsel 111  
 Betrieb 65, 139, 153  
 Betriebsabläufe 107  
 Betriebsablauf-Verantwortung 107  
 Betriebsmittel 121  
 – Wartung 125  
 Beweismaterial 102  
 Beweissicherung 23  
 Bewertung 67  
 Bewusstsein 61  
 BIA *siehe* Business-Impact-Analyse  
 Bildschirmsperre 121  
 Blacklisting 142  
 Blickschutzfolie 123  
 Branche 8  
 Branchenspezifische Sicherheitsstandards 10  
 Bring your own Device 127  
 BSI *siehe* Bundesamt für Sicherheit in der Informationstechnik  
 BSI-Gesetz 7  
 BSI-KritisV *siehe* BSI-Kritisverordnung  
 BSI-Kritisverordnung 8  
 BSI-Standards 154  
 BSIG *siehe* BSI-Gesetz  
 BS 7799 20  
 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 12  
 Bundesamt für Sicherheit in der Informationstechnik 8, 153  
 – Gesetz 7  
 – IT-Grundschutz-Kompendium 153  
 – IT-Grundschutz-Standards 154  
 – Kritisverordnung 8  
 Business Continuity Plan 103, 148  
 Business-Impact-Analyse 104  
 BYOD *siehe* Bring your own Device

**C**

CER *siehe* Critical Entities Resilience Directive  
 CERT *siehe* Computer Emergency Response Team  
 CFA *siehe* Component Failure Impact Analysis  
 Chancen 52  
 Change Management 97, 140, 148  
 Check-Phase 36, 39, 67  
 Chief Information Security Officer 31, 84  
 CISA *siehe* Cybersecurity and Infrastructure Security Agency  
 CISIS12 155  
 CISO *siehe* Chief Information Security Officer  
 Clouddienste 23, 97  
 Coding 146  
 Compliance 104, 105  
 Component Failure Impact Analysis 135  
 Computer Emergency Response Team 86  
 Computer Security Incident Response Team 99  
 CON *siehe* Konzepte und Vorgehensweisen  
 Confidentiality *siehe* Vertraulichkeit  
 Controls 39  
 CRA *siehe* Cyber Resilience Act  
 Critical Entities Resilience Directive 12  
 – CER-Richtlinie 12  
 CSA *siehe* Cybersecurity Act  
 CSIRT *siehe* Computer Security Incident Response Team  
 Cyber Resilience Act 12  
 Cybersecurity Act 12  
 Cybersecurity and Infrastructure Security Agency 110  
 Cybersecurity Framework 156

**D**

DAkKS *siehe* Deutsche Akkreditierungsstelle  
 Data Leakage 133  
 Daten  
 – Abfluss 133  
 – Leck 133  
 – Maskierung 133  
 – Minimierung 10  
 – personenbezogene 10  
 – Richtigkeit 11  
 – Sicherung 134  
 – Speicherbegrenzung 11  
 Datenschutz 106  
 – Beauftragter 30  
 – Folgenabschätzung 11  
 – Grundverordnung 10  
 Datenschutzvorfälle melden 114  
 Datenträger *siehe* Speichermedien



- DDoS *siehe* Distributed Denial of Service  
 Definitionsebene 29  
 Demilitarised Zone 141  
 Deming-Kreislauf 34, 39  
 Denial of Service 5  
 DER *siehe* Detektion und Reaktion  
 Detektierend 32, 136  
 Detektion und Reaktion 153  
 Deutsche Akkreditierungsstelle 22, 156, 168  
 Diebstahl 121  
 Dienstleistungen 97  
 Dienstprogramme  
 – privilegierte 138  
 Digital Operational Resilience Act 13  
 – DORA-Verordnung 13  
 DIN EN ISO/IEC 27001 197–230  
 Distributed Denial of Service 5  
 Disziplinarverfahren *siehe*  
 – Maßregelungsprozess  
 DMZ *siehe* Demilitarised Zone  
 DNS-Firewall 142  
 Do-Phase 35, 39, 60, 65  
 Dokument 29  
 Dokumentation 29, 63  
 Dokumentenaudit 170  
 Dokumentenlenkung 30, 64, 64  
 Dokumentenvorlage 65  
 DORA *siehe* Digital Operational Resilience Act  
 DoS *siehe* Denial of Service  
 DSGVO *siehe* Datenschutz-Grundverordnung  
 Durchführungsebene 29
- E**
- Effektivität 36, 73  
 Effizienz 36, 73  
 Eigentum 105  
 Einbruchmeldeanlage 119  
 Einbrüche 115, 119  
 Einrichtungen 118, 124  
 Elementarmessgröße 180  
 Elementarschaden 119  
 Endpunktgeräte 126  
 Energieversorger 23  
 ENISA *siehe* European Union Agency for  
 Cybersecurity  
 Entscheidung 99  
 Entsorgung  
 – von Betriebsmitteln 126  
 – von Speichermedien 121, 123, 126  
 Entwicklung 144, 146  
 – sichere 144  
 Entwicklungsgrundsätze 145
- Entwicklungsumgebung 147  
 ENX *siehe* European Network Exchange  
 Association  
 Ereignis 183  
 Erkenntnisse 102  
 European Network Exchange Association 158  
 European Union Agency for Cybersecurity 110  
 Examination Institute 172  
 Externes Audit 71, 167  
 Externe Mitarbeitende 30
- F**
- Festplatten *siehe* Speichermedien  
 FitSM 163, 164  
 Folge 181  
 Forensik 23  
 Fortbildung 110  
 Fortbildungsprogramme 30  
 Foundation-Zertifikat 173, 175  
 – Prüfungsspezifikation 175  
 – Prüfungsvorbereitung 175  
 Führung 48
- G**
- Gäste 117  
 Gebäude 115, 118  
 Geheimhaltungsvereinbarung 112  
 Geistiges Eigentum 105  
 Geräte 121, 125  
 Gerätesperre 121  
 Gesamtverantwortung 30  
 Good Practices 20
- H**
- Handhabung technischer Schwachstellen 131  
 Hauptabweichung 168  
 Homeoffice *siehe* Remote-Arbeit
- I**
- IAM *siehe* Identity and Access Management  
 ICO *siehe* International Certification  
 Organization  
 Identitätsmanagement 92  
 Identity and Access Management 93  
 IDS *siehe* Intrusion-Detection-System  
 IEC *siehe* International Electrotechnical  
 Commission  
 IKT *siehe* Informations- und  
 Kommunikationstechnik  
 IND *siehe* Industrielle IT  
 Indikator 29, 184  
 Industrielle IT 153

- INF *siehe* Infrastruktur
- Information 3, 182
  - Kennzeichnung 90
  - Klassifizierung 89
  - Transport 91
  - Übermittlung 91
  - Zulässiger Gebrauch 88
- Information Security
  - Assessment 157
  - Auditor 173
  - Foundation 173
  - Metrics 68
  - Officer 31, 84, 173
- Informations- und Kommunikationstechnik 96, 103
- informationsaustauschende Gemeinschaft 185
- Informationsbedarf 184
- Informationssicherheit 3, 184
  - Aufrechterhaltung 184
  - bei Störungen 103
  - Clouddienste 97
  - IKT-Lieferkette 96
  - im Projektmanagement 87
  - Konformität 107
  - Lieferantenbeziehungen 95
  - Lieferantenvereinbarungen 95
  - Richtlinien 107
  - Standards 107
  - Steuerung 183
  - unabhängige Überprüfung 106
- Informationssicherheitsrichtlinien 82
- Informationssicherheitsbeauftragter 31, 52
- Informationssicherheitsereignis 185
  - melden 114
- Informationssicherheitsmanagementsystem 27, 48
  - Audit 21
  - Dokumentation 29
  - Kernbestandteile 27
- Informationssicherheitsrisikobehandlung 56
- Informationssicherheitsrisikobeurteilung 54
- Informationssicherheitsvorfall 98, 185
  - Beurteilung 99
  - Entscheidung 99
  - Erkenntnisse 102
  - Handhabung 185
  - Reaktion 101
- Informationssysteme 185
- Informationsveranstaltungen 30
- Informationsverarbeitende Einrichtungen 184
- Informationszugang 128
- Informationszugangsbeschränkung 128
- Informativer Standard 16
- Infrastruktur 153
- Installation 139
- Instandhaltung *siehe* Wartung
- Instandsetzung *siehe* Wartung
- Integrität 4, 11, 186
- Integrity *siehe* Integrität
- Interessengruppen 86
- Interessierte Partei 186
- interessierte Partei 45
- International Certification Organization 174
- International Electrotechnical Commission 2, 157
- International Organization for Standardization 2, 157, 159
- Internes Audit 70
- Internet of Things 24
- Intrusion-Detection-System 137
- Inventar 88
- ISA *siehe* Information Security Assessment
- ISB *siehe* Informationssicherheitsbeauftragter, 60
- ISMS *siehe* Informationssicherheitsmanagementsystem
- ISO *siehe* International Organization for Standardization, *siehe* Information Security Officer
- ISO/IEC 15408 157
- ISO/IEC 17020 161
- ISO/IEC 17021 19, 161, 168, 171
- ISO/IEC 17024 161
- ISO/IEC 17025 161
- ISO/IEC 17799 20, 81, 167
- ISO/IEC 20000 33, 162
- ISO/IEC 27000 16
- ISO/IEC 27001 18, 197–230
- ISO/IEC 27002 20
- ISO/IEC 27003 20
- ISO/IEC 27004 20
- ISO/IEC 27005 20
- ISO/IEC 27006 19, 161, 171, 172
- ISO/IEC 27007 21
- ISO/IEC 27008 21
- ISO/IEC 27009 18, 19
- ISO/IEC 27010 22
- ISO/IEC 27011 23
- ISO/IEC 27013 21, 163
- ISO/IEC 27014 21
- ISO/IEC 27016 21
- ISO/IEC 27017 23
- ISO/IEC 27018 21, 23
- ISO/IEC 27019 23

ISO/IEC 27032 23  
 ISO/IEC 27034 23  
 ISO/IEC 27701 18  
 ISO 19011 159, 171  
 ISO 31000 21  
 ISO 9000 16, 33, 159  
 ISO 9001 159  
 ISO 9004 159  
 IT Infrastructure Library 162  
 IT Service Management 108, 148, 162  
 IT-Grundschutz-Kompendium 153  
 IT-Sicherheitscluster e.V. 155  
 IT-Sicherheitsgesetz 7  
 IT-SiG *siehe* IT-Sicherheitsgesetz  
 IT-Systeme 153  
 ITEMO e.V. 163  
 ITIL *siehe* IT Infrastructure Library, 162  
 ITSM *siehe* IT Service Management

## K

Kapazitätssteuerung 130  
 Kategorien von Werten 28  
 Kennzahlensteckbrief 68  
 Kennzeichnung 90  
 Kernbestandteile eines ISMS 27  
 Key Performance Indicator 68  
 Klassifizierung 89  
 Klimatisierung 124  
 Kommunikation 62  
 Kommunikationsstrategie 99  
 Kompetenz 61, 180  
 Konfigurationsmanagement 132  
 Konformität 18, 36, 73, 75, 107, 181  
 Kontakt  
 – Behörden 86  
 – Interessengruppen 86  
 Kontext 183  
 – der Organisation 44  
 – interessierte Parteien 45  
 – interner 186  
 Kontinuierliche Verbesserung 34  
 Kontinuität 103  
 Kontinuitätsplan 104  
 Konzepte und Vorgehensweisen 153  
 Korrektiv 32  
 Korrektur 182  
 Korrekturmaßnahme 182  
 KPI *siehe* Key Performance Indicator  
 KRITIS *siehe* Kritische Infrastrukturen  
 Kritische Infrastrukturen 8  
 Kryptographie 142  
 Kündigung 111

Künstliche Intelligenz 24

## L

Label 158  
 Least Privilege 92  
 Lebenszyklus  
 – sichere Entwicklung 144  
 Leistung 67, 189  
 Leitfaden 20  
 – maßnahmenspezifisch 22, 23  
 – sektorspezifisch 22  
 Leitung 48, 195  
 Lieferanten 97  
 – Beziehungen 23, 95  
 – Vereinbarungen 95  
 Lizenzen 126  
 Lizenzmanagement 105  
 Löschung 123, 132  
 Logging 136

## M

Maßnahmenspezifische Leitfäden 23  
 Maßregelungsprozess 111  
 Malware 130  
 Man-in-the-Middle-Angriff 6  
 Management Review 73  
 Managementbewertung 73  
 Managementsystem 27, 187  
 Manipulation 124  
 Maßnahme 31, 81–181  
 – organisatorische 82  
 – personenbezogen 108  
 – physische 115  
 – technische und organisatorische 32  
 – technologische 126  
 Maßnahmenziele 182  
 Measurement 20  
 Mehrfaktor Authentisierung 117, 129  
 Menschen 108  
 Messfunktion 187  
 Messgröße 182, 187  
 Messmethode 188  
 Messung 20, 67, 187  
 Mitarbeitende *siehe* Menschen  
 Mitarbeiterausweise *siehe* Ausweise  
 Mobiles Arbeiten *siehe* Remote-Arbeit  
 Mobilgeräte 113, 122

## N

NAC *siehe* Network-Access-Control  
 Nachvollziehbarkeit 29

- National Institute of Standards and Technology 156
- Cybersecurity Framework 156
- Naturkatastrophen 119
- Nebenabweichung 168
- Need to know 92
- NET *siehe* Netze und Kommunikation
- Network-Access-Control 140
- Netzdienste 140
- Netze und Kommunikation 153
- Netzicherheit 23, 140
- Netztrennung 141
- Netzwerk für Informationssicherheit im Mittelstand 155
- Nichtabstreitbarkeit 6, 91, 188
- Nichtkonformität 188
- Nichtkonformität 182
- NIM *siehe* Netzwerk für Informationssicherheit im Mittelstand
- NIS-2-Richtlinie 11
- NIST *siehe* National Institute of Standards and Technology
- Non-Conformities 169
- Non-disclosure agreement 112
- Non-repudiation 6
- Norm 16
- Normative Verweisungen 43
- Normativer Standard 16
- Notfallmanagement 23
- O**
- OLA *siehe* Operational Level Agreement
- Operational Level Agreement 141
- OPS *siehe* Betrieb
- Organisation 189
- Organisation und Personal 153
- Organisationszertifizierung 167
- Organisatorische Maßnahmen 82
- ORP *siehe* Organisation und Personal
- P**
- PDCA 34, 34, 39
- PDCA-Methodik 27, 34
- Penetration Test 131
- Personal *siehe* Menschen
- Personally Identifiable Information 23
- Personenbezogene Daten 10, 106
- Personenbezogene Maßnahmen 108
- Personenzertifizierung 167, 172
- Physische Bedrohungen 119
- Physische Maßnahmen 115
- Physische Sicherheit 115
- Physischer Zutritt 117
- PII *siehe* Personally Identifiable Information
- PIMS *siehe* Privacy Information Management Systems
- PKI *siehe* Public Key Infrastructure
- Plan 52
- Plan-Do-Check-Act 34
- Plan-Phase 35, 39, 52
- Planung 35, 52, 65, 98
- Policy 28, 82
- Politik 50, 189
- Post-Quantum-Cryptography 143
- PQC *siehe* Post-Quantum-Cryptography
- Präventiv 32
- Privacy Information Management Systems 19
- Privatsphäre 106
- Privilegierte Rechte 138
- Privilegierte Zugangsrechte 127
- Procedure 28
- Process *siehe* Prozess
- Produktivumgebung 147
- Programmierung 146
- Projektmanagement 87
- Protokollierung 135
- Provider 23
- Prozess 28, 33, 190
- Prozess-Bausteine 153
- Prozessmanagement 34
- Prozessorientierung 33
- Prüfungstaktik 176
- Prüfungsvorbereitung 176
- Pseudonymisierung 133
- Public Key Infrastructure 143
- Q**
- Qualifizierungsprogramm 172
- Qualitätsmanagement 34, 159
- Quellcode 128
- R**
- Räume 118
- Rahmenwerk 153
- RBAC *siehe* Role Based Access Control
- RCE Directive 12
- Rechtmäßigkeit 10
- Rechtsprechung 30
- Recovery Time Objective 104
- Redundanz 135
- Release and Deployment Management 146, 163
- Release Management 140
- Reliability 6

- Remote-Arbeit 113
- Reparatur *siehe* Wartung
- Requirements Engineering 144
- Resilience of Critical Entities 12
- Response Policy Zone 142
- Ressourcen 35, 60
- Restrisiko 190
- Review 102
- Rezertifizierung 171
- Richtigkeit 11
- Richtlinie 28, 82, 107
  - themenspezifisch 83
- Risiko 191
  - Absprache 192
  - Akzeptanz 55, 191
  - Analyse 56, 192
  - Behandlung 56, 67, 194
  - Beurteilung 55, 66, 192
  - Bewertung 56, 193
  - Eigentümer 58, 84, 194
  - Identifizierung 56, 193
  - Kommunikation 192
  - Kriterien 192
  - Management 20
  - Matrix 57
  - Niveau 186
- Risikomanagement 21, 52, 88, 193
  - Prozess 193
- Role Based Access Control 94
- Rollen 30, 31, 51, 84
- Rollenbasierte Zugangskontrolle 94
- Rollenzuweisung 84
- RPZ *siehe* Response Policy Zone
- RTO *siehe* Recovery Time Objective
- Rückverfolgbarkeit 29
  
- S**
- Schadsoftware 130
- Schlüsselverwaltung 143
- Schulung 110
- Schutz
  - Aufzeichnungen 105
  - Bedarf 116
  - gegen Schadsoftware 130
  - Klasse 116
  - Niveau 31
  - personenbezogene Daten 106
  - Privatsphäre 106
  - Ziel 3
- Schwachstelle 131, 195
- Schwachstellenscan 131
- Scope *siehe* Anwendungsbereich
- Scoping 16, 168
- Scoping Statement 168
- Security Incident Coordinator 99
- Security Incident Response 99
- Security Information & Event Management 137
- Sektor 8
- Sektorspezifische Leitfäden 22
- Sensibilisierung 110
- Service Level Agreement 141
- SIC *siehe* Security Incident Coordinator
- Sichere Authentisierung 129
- Sicherheit
  - Netzsicherheit 140
  - von Anwendungen 144
- Sicherheitsanforderung 3
- Sicherheitsbereiche 115, 120
- Sicherheitsgesetz 7
- Sicherheitslücke melden 114
- Sicherheitsperimeter 115
- Sicherheitstests 146
- Sicherheitsüberprüfung 108
- Sicherheitsüberprüfungsgesetz 109
- Sicherheitsvorfälle 23
  - melden 114
- Sicherheitsziele 58
- Sicherheitszonen 115
- Sicherung 134
- SIEM *siehe* Security Information & Event Management
- Single Points Of Failure 135
- SIR *siehe* Security Incident Response
- SLA *siehe* Service Level Agreement
- Smart City 24
- SOA *siehe* Statement Of Applicability
- Softwareinstallation 139
- Softwarelizenzen *siehe* Lizenzen
- Speicherbegrenzung 11
- Speichermedien 123, 126
- SPOF *siehe* Single Points Of Failure
- Störungen 103
- Stand der Technik 9, 11
- Stand-by 135
  - heiß 135
  - kalt 135
- Standard 16, 107
  - informativer 16
  - normativer 16
- Standardfamilie 15
- Standardisierung 15
- Standort 115, 122
- Statement of Applicability 58, 168
- Steuerung 65, 183

- Steuerungsebene 29
  - Steuerungsgremium 184
  - Stromversorgung 124
  - SÜG *siehe* Sicherheitsüberprüfungsgesetz
  - Support 60
  - SYS *siehe* IT-Systeme
  - System zur Angriffserkennung 137
  - System-Bausteine 153
  - Systemabnahmetest 146
  - Systemarchitektur 145
  - Systems zur Angriffserkennung 9
  - SZA *siehe* System zur Angriffserkennung
- T**
- TÜV Süd 173
  - Technische Schwachstellen 131
  - Technische und organisatorische Maßnahmen 32
  - Technologische Maßnahmen 126
  - Telearbeit *siehe* Remote-Arbeit
  - Terminologie 16
  - Testdaten 148
  - Testumgebung 147
  - TISAX *siehe* Trusted Information Security Assessment Exchange
  - TOM *siehe* Technische und organisatorische Maßnahmen
  - Topmanagement 85
  - Training 110
  - Transparenz 10
  - Trennung 147
  - Trusted Information Security Assessment Exchange 158
- U**
- Überblicksdokument 16
  - Überprüfung 36, 67, 97, 106, 190
    - Ziel 191
  - Überwachung 67, 97, 118, 188
  - Überwachungsaktivitäten 137
  - Überwachungsaudit 171
  - Uhrensynchronisation 138
  - Umgebungstrennung 147
  - Umsetzung 35, 60, 65
  - Umweltbedingte Bedrohungen 119
  - Unterstützung 60
  - User Endpoint Devices 126
- V**
- VDA *siehe* Verband der Automobilindustrie
  - VDA ISA (TISAX) 157
  - Verantwortlichkeit 30, 51, 82, 84
  - Verantwortung 85
  - Verband der Automobilindustrie 157
  - Verbesserung 37, 74, 181
  - Verbesserungsmaßnahmen 37
  - Verbindlichkeit 6
  - Verfahren 28
  - Verfahrensanweisung 29
  - Verfügbarkeit 5, 180
  - Verhinderung von Datenlecks 133
  - Verkabelung 124
  - Verlässlichkeit 6
  - Verlust 121
  - Vernichtung *siehe* Entsorgung
  - Verschwiegenheitspflicht 112
  - Versorgungseinheiten 124
  - Versorgungseinrichtungen 118
  - Verstöße 111
  - Vertragsbedingungen für die Beschäftigung 109
  - Vertrauenswürdige Einheit 195
  - Vertraulichkeit 4, 11, 181
  - Vertraulichkeitsvereinbarung 109, 112, 112
  - Verwandte Standards 153
    - Auditierung 159
    - Governance 162
    - IT- und Informationssicherheit 153
    - Management der IT 162
    - Qualitätsmanagement 159
    - Zertifizierung 159
  - Videüberwachung *siehe* Überwachung
  - Vorfall 183
  - Vorstand 30
  - Vulnerability Management 131
- W**
- Wahrscheinlichkeit 187
  - Wartung 125
  - Webfilterung 142
  - Wechseldatenträger *siehe* Speichermedien
  - Wert 28, 88
    - Rückgabe 89
  - Wiederherstellungsmaßnahmen 104
  - Wiederherstellungszeit 104
  - Wiederholungsaudit 171
  - Wiederverwendung
    - von Betriebsmitteln 126
    - von Speichermedien 123, 126
  - Wirksamkeit 67, 183
  - Wirkungsgrad 36
- Z**
- Zeitpunkte 35

- Zerstörung *siehe* Entsorgung
- Zertifikat 171
- Zertifizierung 167
  - Ablauf 169
  - Akkreditierung 168
  - Gültigkeit 171
  - Kosten 171
  - Organisationszertifizierung 167
  - Personenzertifizierung 167, 172
  - Rezertifizierung 171
- Zertifizierungsaudit 18, **169**
- Zertifizierungsprüfung 235
- Zertifizierungsstelle **19**, 169
- Ziel 188
- Zonenmodell 115
- Zugang 7
  - Quellcode 128
- Zugangsberechtigung
  - attributbasiert 94
  - rollenbasiert 94
- Zugangsrechte 94
- Zugangssteuerung 92, **179**
- Zugriffskontrolle 7
- Zugriffssteuerung 7
- Zurechenbarkeit 7
- Zutritt 7, 115, 117
- Zutrittspunkte 117
- Zutrittssteuerung 117
- Zuverlässigkeit 190
- Zuweisung
  - Rollen 30
- Zweckbindung 10
- Zwischenfall 183