

DIN EN ISO/IEC 27017:2026-11 (D)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre -
Informationssicherheitsmaßnahmen auf der Grundlage von ISO/IEC 27002 für Cloud-
Dienste (ISO/IEC 27017:2026); Deutsche Fassung EN ISO/IEC 27017:2026

Inhalt	Seite
Europäisches Vorwort.....	9
Vorwort	10
Einleitung	12
1 Anwendungsbereich.....	13
2 Normative Verweisungen	13
3 Begriffe und Abkürzungen	13
3.1 Begriffe	13
3.2 Abkürzungen	14
4 Anleitung zur Verwendung dieses Dokuments	14
4.1 Beziehung zwischen diesem Dokument und ISO/IEC 27002:2022	14
4.2 Aufbau dieses Dokuments	15
4.3 Spezifische Konzepte des Cloud Computing	16
4.3.1 Lieferantenbeziehungen bei Cloud-Diensten.....	16
4.3.2 Beziehungen zwischen CSCs und CSPs.....	16
4.3.3 Umgang mit Informationssicherheitsrisiken bei Cloud-Diensten.....	17
5 Spezifische Anleitungen für Cloud-Dienste in Zusammenhang mit organisatorischen Maßnahmen	18
5.1 Informationssicherheitsrichtlinien.....	18
5.2 Informationssicherheitsrollen und -verantwortlichkeiten.....	19
5.3 Aufgabentrennung	20
5.4 Verantwortlichkeiten der Leitung.....	20
5.5 Kontakt mit Behörden	20
5.6 Kontakt mit speziellen Interessengruppen	20
5.7 Informationen über die Bedrohungslage	20
5.8 Informationssicherheit im Projektmanagement.....	21
5.9 Inventar der Informationen und anderer damit verbundener Werte.....	21
5.10 Zulässige Verwendung von Informationen und anderen damit verbundenen Werten	22
5.11 Rückgabe von Werten	22
5.12 Klassifizierung von Information.....	22
5.13 Kennzeichnung von Information.....	22
5.14 Informationsübermittlung.....	23
5.15 Zugangssteuerung.....	23
5.16 Identitätsmanagement	23
5.17 Authentifizierungsinformationen.....	23
5.18 Zugangsrechte	24
5.19 Informationssicherheit in Lieferantenbeziehungen.....	24
5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen	24
5.21 Umgang mit der Informationssicherheit in der IKT-Lieferkette	25
5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen	26
5.23 Informationssicherheit für die Nutzung von Cloud-Diensten.....	26
5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen.....	26
5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse.....	27

5.26	Reaktion auf Informationssicherheitsvorfälle	27
5.27	Erkenntnisse aus Informationssicherheitsvorfällen.....	27
5.28	Sammeln von Beweismaterial.....	27
5.29	Informationssicherheit bei Störungen	28
5.30	IKT-Bereitschaft für Business Continuity.....	28
5.31	Juristische, gesetzliche, regulatorische und vertragliche Anforderungen	28
5.32	Geistige Eigentumsrechte	30
5.33	Schutz von Aufzeichnungen	30
5.34	Datenschutz und Schutz personenbezogener Daten (pbd).....	30
5.35	Unabhängige Überprüfung der Informationssicherheit.....	31
5.36	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit.....	31
5.37	Dokumentierte Betriebsabläufe.....	31
5.38	CLD — Verteilte Rollen und Verantwortlichkeiten in einer Cloud-Computing-Umgebung	32
5.39	CLD — Vereinbarung über die Rollen und Verantwortlichkeiten des Cloud-Dienstleistungspartners	33
6	Spezifische Anleitungen für Cloud-Dienste in Zusammenhang mit personenbezogenen Maßnahmen	35
6.1	Sicherheitsüberprüfung.....	35
6.2	Beschäftigungs- und Vertragsbedingungen.....	35
6.3	Informationssicherheitsbewusstsein, -ausbildung und -schulung.....	35
6.4	Maßregelungsprozess.....	36
6.5	Verantwortlichkeiten bei Beendigung oder Änderung des Beschäftigungsverhältnisses	36
6.6	Vertraulichkeits- oder Geheimhaltungsvereinbarungen.....	36
6.7	Remote-Arbeit.....	36
6.8	Meldung von Informationssicherheitsereignissen	36
7	Spezifische Anleitungen für Cloud-Dienste in Zusammenhang mit personenbezogenen Maßnahmen	37
7.1	Physische Sicherheitsperimeter	37
7.2	Physischer Zutritt.....	37
7.3	Sicherung von Büros, Räumen und Einrichtungen.....	37
7.4	Physische Sicherheitsüberwachung.....	37
7.5	Schutz vor physischen und umweltbedingten Bedrohungen	37
7.6	Arbeiten in Sicherheitsbereichen	37
7.7	Aufgeräumte Arbeitsumgebung und Bildschirmsperren.....	37
7.8	Platzierung und Schutz von Geräten und Betriebsmitteln	37
7.9	Sicherheit von Werten außerhalb der Räumlichkeiten.....	38
7.10	Speichermedien.....	38
7.11	Versorgungseinrichtungen	38
7.12	Sicherheit der Verkabelung.....	38
7.13	Instandhaltung von Geräten und Betriebsmitteln	38
7.14	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	38
8	Spezifische Anleitungen für Cloud-Dienste in Zusammenhang mit technologischen Maßnahmen	39
8.1	Endpunktgeräte des Benutzers	39
8.2	Privilegierte Zugangsrechte	39
8.3	Informationszugangsbeschränkung	39
8.4	Zugriff auf den Quellcode.....	40
8.5	Sichere Authentifizierung.....	40
8.6	Kapazitätssteuerung	40
8.7	Schutz gegen Schadsoftware.....	41
8.8	Handhabung von technischen Schwachstellen.....	41
8.9	Konfigurationsmanagement.....	42
8.10	Löschung von Informationen	43
8.11	Datenmaskierung.....	43
8.12	Verhinderung von Datenlecks	44
8.13	Sicherung von Information	44

8.14	Redundanz von informationsverarbeitenden Einrichtungen	45
8.15	Protokollierung.....	45
8.16	Überwachung von Aktivitäten.....	45
8.17	Uhrensynchronisation	46
8.18	Gebrauch von Hilfsprogrammen mit privilegierten Rechten	47
8.19	Installation von Software auf Systemen in Betrieb	47
8.20	Netzwerksicherheit	47
8.21	Sicherheit von Netzwerkdiensten.....	48
8.22	Trennung von Netzwerken.....	48
8.23	Webfilterung.....	48
8.24	Verwendung von Kryptographie.....	48
8.25	Lebenszyklus einer sicheren Entwicklung.....	49
8.26	Anforderungen an die Anwendungssicherheit.....	50
8.27	Sichere Systemarchitektur und Entwicklungsgrundsätze.....	50
8.28	Sichere Codierung	50
8.29	Sicherheitsprüfung bei Entwicklung und Abnahme	50
8.30	Ausgegliederte Entwicklung.....	50
8.31	Trennung von Entwicklungs-, Test- und Produktionsumgebungen	50
8.32	Änderungssteuerung.....	51
8.33	Testdaten	51
8.34	Schutz von Informationssystemen bei Audits und Tests.....	51
8.35	CLD — Trennung in virtuelle Computing-Umgebungen	52
8.36	CLD — Erkennung und Verhinderung einer unbefugten Nutzung von Cloud-Diensten.....	53
Anhang A (informativ) Zusammenhang zwischen diesem Dokument und der ersten Ausgabe (ISO/IEC 27017:2015)		55
Anhang B (informativ) Überwachung von Cloud-Diensten.....		62
Literaturhinweise		64

Tabellen

Tabelle 1 — Typ 1	15
Tabelle 2 — Typ 2	15
Tabelle 3 — Anleitung für Informationssicherheitsrichtlinien.....	18
Tabelle 4 — Anleitung für Informationssicherheitsrollen und -verantwortlichkeiten.....	20
Tabelle 5 — Anleitung für Informationen über die Bedrohungslage	20
Tabelle 6 — Anleitung für Informationssicherheit im Projektmanagement	21
Tabelle 7 — Anleitung für ein Inventar der Informationen und anderer damit verbundener Werte	21
Tabelle 8 — Anleitung für die Rückgabe von Werten	22
Tabelle 9 — Anleitung für die Kennzeichnung von Information.....	22
Tabelle 10 — Anleitung für die Identitätsmanagement.....	23
Tabelle 11 — Anleitung für Authentifizierungsinformationen	24
Tabelle 12 — Anleitung für Zugangsrechte	24

Tabelle 13 — Anleitung zur Behandlung von Informationssicherheit in Lieferantenvereinbarungen.....	25
Tabelle 14 — Anleitung für den Umgang mit der Informationssicherheit in der IKT-Lieferkette.....	26
Tabelle 15 — Anleitung für die Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen.....	27
Tabelle 16 — Anleitung für das Sammeln von Beweismaterial.....	28
Tabelle 17 — Anleitung für die IKT-Bereitschaft für Business Continuity	28
Tabelle 18 — Anleitung für juristische, gesetzliche, regulatorische und vertragliche Anforderungen	29
Tabelle 19 — Anleitung für geistige Eigentumsrechte	30
Tabelle 20 — Anleitung für den Schutz von Aufzeichnungen.....	30
Tabelle 21 — Anleitung für die unabhängige Überprüfung der Informationssicherheit.....	31
Tabelle 22 — Anleitung für dokumentierte Betriebsabläufe.....	32
Tabelle 23 — CLD — Verteilte Rollen und Verantwortlichkeiten in einer Cloud-Computing-Umgebung	32
Tabelle 24 — Anleitung für CLD — Verteilte Rollen und Verantwortlichkeiten in einer Cloud-Computing-Umgebung	33
Tabelle 25 — Attribute für CLD — Vereinbarung über die Rollen und Verantwortlichkeiten des Cloud-Dienstleistungspartners.....	34
Tabelle 26 — Anleitung für CLD — Vereinbarung über die Rollen und Verantwortlichkeiten des Cloud-Dienstleistungspartners.....	34
Tabelle 27 — Anleitung für Informationssicherheitsbewusstsein, -ausbildung und -schulung.....	35
Tabelle 28 — Anleitung für die Meldung von Informationssicherheitsereignissen	36
Tabelle 29 — Anleitung für die sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	38
Tabelle 30 — Anleitung für privilegierte Zugangsrechte	39
Tabelle 31 — Anleitung für die Informationszugangsbeschränkung.....	39
Tabelle 32 — Anleitung für die Kapazitätssteuerung.....	40
Tabelle 33 — Anleitung für die Handhabung von technischen Schwachstellen	41
Tabelle 34 — Anleitung für das Konfigurationsmanagement.....	42
Tabelle 35 — Anleitung für die Löschung von Informationen	43
Tabelle 36 — Anleitung für die Datenmaskierung	43
Tabelle 37 — Anleitung für die Sicherung von Information	44

Tabelle 38 — Anleitung für die Protokollierung	45
Tabelle 39 — Anleitung für die Überwachung von Aktivitäten	46
Tabelle 40 — Anleitung für die Uhrensynchronisation.....	46
Tabelle 41 — Anleitung für den Gebrauch von Hilfsprogrammen mit privilegierten Rechten.....	47
Tabelle 42 — Anleitung für die Netzwerksicherheit	47
Tabelle 43 — Anleitung für die Verwendung von Kryptographie.....	49
Tabelle 44 — Anleitung für einen Lebenszyklus einer sicheren Entwicklung.....	50
Tabelle 45 — Anleitung für die Änderungssteuerung	51
Tabelle 46 — Attribute für CLD — Trennung in virtuelle Computing-Umgebungen	52
Tabelle 47 — Anleitung für CLD — Trennung in virtuelle Computing-Umgebungen	52
Tabelle 48 — Attribute für CLD — Erkennung und Verhinderung einer unbefugten Nutzung von Cloud-Diensten	53
Tabelle 49 — Anleitung für CLD — Erkennung und Verhinderung einer unbefugten Nutzung von Cloud-Diensten	54
Tabelle A.1 — Übereinstimmung zwischen Maßnahmen in diesem Dokument und ISO/IEC 27017:2015	56
Tabelle A.2 — Übereinstimmung zwischen Maßnahmen in ISO/IEC 27017:2015 und diesem Dokument.....	59