ISO 27001:2022 ANNEX A

Statement of Applicability

Vorlage für alle 93 Annex-A-Controls

VERSION	STAND	LIZENZ
1.0	6. Oktober 2026	Creative Commons CC-BY-4.0

OPEN LICENCE · CC-BY-4.0

Diese Vorlage ist unter Creative Commons CC-BY-4.0 lizenziert. Freie Nutzung, Weitergabe und Anpassung erlaubt — mit Nennung: Kopexa GmbH, kopexa.com.

Ausfüllhinweise

Diese Vorlage unterstützt die strukturierte Erstellung deines Statement of Applicability nach ISO 27001:2022 Klausel 6.1.3(d). Fülle jede Zeile für alle 93 Annex-A-Controls aus.

Die 9 Pflichtfelder je Control-Zeile

1. Control-Nr.: Unveränderliche Kennung (z.B. A.5.1)
2. Titel: Normativer Control-Titel
3. Anwendbar: Ja oder Nein
4. Begründung: Schriftliche Begründung der Entscheidung
5. Status: implementiert / teilweise / geplant / n.v.
6. Policy-Ref: Dokumentennummer der zugehörigen Policy
7. Evidence-Ref: Verweis auf Nachweis / Audit-Evidence
8. Rolle: Verantwortliche Rolle (z.B. CISO)
9. Datum: Zuletzt geprüft

Versionierung

Das SoA ist ein lebendes Dokument. Jährliche Überarbeitung ist Pflicht (ISO 27001 Klausel 9.3). Jede Version benötigt Datum, Versionsnummer und Management-Genehmigung.

Diese Vorlage ist CC-BY-4.0 lizenziert. Freie Nutzung mit Nennung: Kopexa GmbH, kopexa.com. Kein Ersatz für Rechtsberatung. ISO 27001:2022 Annex A — Stand 2026-04-17.

A.5 — Organisatorische Controls (37 Controls)

Control-Nr.	Titel	Anwend-bar	Begründung	Status	Policy-Ref	Evidence-Ref	Rolle	Datum
A.5.1	Informationssicherheitsrichtlinien							
A.5.2	Informationssicherheitsrollen und -verant-wortlichkeiten							
A.5.3	Aufgabentrennung							
A.5.4	Managementverantwortlichkeiten							
A.5.5	Kontakt mit Behörden							
A.5.6	Kontakt mit speziellen Interessengruppen							
A.5.7	Bedrohungsintelligenz							
A.5.8	Informationssicherheit im Projektmanagement							
A.5.9	Inventarisierung von Informationen und zuge-hörigen Vermögenswerten							
A.5.10	Zulässige Nutzung von Informationen und zuge-hörigen Vermögenswerten							
A.5.11	Rückgabe von Vermögenswerten							
A.5.12	Klassifizierung von Informationen							
A.5.13	Kennzeichnung von Informationen							
A.5.14	Informationsübertragung							
A.5.15	Zugangssteuerung							
A.5.16	Identitätsmanagement							
A.5.17	Authentifizierungsinformationen							
A.5.18	Zugangsrechte							
A.5.19	Informationssicherheit in Lieferantenbeziehungen							
A.5.20	Berücksichtigung der Informationssicherheit in Lieferantenvereinbarungen							

Control-Nr.	Titel	Anwend-bar	Begründung	Status	Policy-Ref	Evidence-Ref	Rolle	Datum
A.5.21	Management der Informationssicherheit in der IKT-Lieferkette							
A.5.22	Überwachung, Überprüfung und Änderungs-management von Lieferantendienstleistungen							
A.5.23	Informationssicherheit bei Nutzung von Cloud-Diensten							
A.5.24	Planung und Vorbereitung des Information-ssicherheitsvorfallmanagements							
A.5.25	Beurteilung und Entscheidung über Information-ssicherheitsereignisse							
A.5.26	Reaktion auf Informationssicherheitsvorfälle							
A.5.27	Erkenntnisse aus Informationssicherheitsvorfällen							
A.5.28	Sammlung von Beweismaterial							
A.5.29	Informationssicherheit bei Störungen							
A.5.30	IKT-Bereitschaft für Business Continuity							
A.5.31	Rechtliche, gesetzliche, regulatorische und ver-tragliche Anforderungen							
A.5.32	Geistiges Eigentum							
A.5.33	Schutz von Aufzeichnungen							
A.5.34	Datenschutz und Schutz personenbezogener Daten							
A.5.35	Unabhängige Überprüfung der Information-ssicherheit							
A.5.36	Einhaltung von Richtlinien, Regeln und Standards für die Informationssicherheit							
A.5.37	Dokumentierte Betriebsverfahren							

A.6 — Personenbezogene Controls (8 Controls)

Control-Nr.	Titel	Anwend-bar	Begründung	Status	Policy-Ref	Evidence-Ref	Rolle	Datum
A.6.1	Sicherheitsüberprüfung							
A.6.2	Beschäftigungsbedingungen							
A.6.3	Informationssicherheitsbewusstsein, -ausbildung und -schulung							
A.6.4	Disziplinarverfahren							
A.6.5	Verantwortlichkeiten nach Beendigung oder Änderung der Beschäftigung							
A.6.6	Vertraulichkeits- oder Geheimhaltungsvereinbarungen							
A.6.7	Telearbeit							
A.6.8	Meldung von Informationssicherheitsereignissen							

A.7 — Physische Controls (14 Controls)

Control-Nr.	Titel	Anwend-bar	Begründung	Status	Policy-Ref	Evidence-Ref	Rolle	Datum
A.7.1	Physische Sicherheitsperimeter							
A.7.2	Physischer Zutritt							
A.7.3	Sicherung von Büros, Räumen und Einrichtungen							
A.7.4	Physische Sicherheitsüberwachung							
A.7.5	Schutz vor physischen und umweltbedingten Bedrohungen							
A.7.6	Arbeit in Sicherheitszonen							
A.7.7	Aufgeräumte Arbeitsumgebung und Bildschirmsperre							
A.7.8	Platzierung und Schutz von Betriebsmitteln							

Control-Nr.	Titel	Anwend-bar	Begründung	Status	Policy-Ref	Evidence-Ref	Rolle	Datum
A.7.9	Sicherheit von Vermögenswerten außerhalb der Geschäftsräume							
A.7.10	Speichermedien							
A.7.11	Versorgungseinrichtungen							
A.7.12	Sicherheit der Verkabelung							
A.7.13	Instandhaltung von Betriebsmitteln							
A.7.14	Sichere Entsorgung oder Wiederverwendung von Betriebsmitteln							

A.8 — Technologische Controls (34 Controls)

Control-Nr.	Titel	Anwend-bar	Begründung	Status	Policy-Ref	Evidence-Ref	Rolle	Datum
A.8.1	Endbenutzergeräte							
A.8.2	Privilegierte Zugangsrechte							
A.8.3	Einschränkung des Informationszugangs							
A.8.4	Zugang zu Quellcode							
A.8.5	Sichere Authentifizierung							
A.8.6	Kapazitätsmanagement							
A.8.7	Schutz vor Schadsoftware							
A.8.8	Management von technischen Schwachstellen							
A.8.9	Konfigurationsmanagement							
A.8.10	Löschung von Informationen							
A.8.11	Datenmaskierung							
A.8.12	Verhinderung von Datenlecks							
A.8.13	Sicherung von Informationen							
A.8.14	Redundanz von informationsverarbeitenden Einrichtungen							
A.8.15	Protokollierung							
A.8.16	Überwachung von Aktivitäten							
A.8.17	Uhrensynchronisation							
A.8.18	Nutzung privilegierter Hilfsprogramme							
A.8.19	Installation von Software auf Betriebssystemen							
A.8.20	Netzwerksicherheit							

Control-Nr.	Titel	Anwend-bar	Begründung	Status	Policy-Ref	Evidence-Ref	Rolle	Datum
A.8.21	Sicherheit von Netzwerkdiensten							
A.8.22	Trennung von Netzwerken							
A.8.23	Webfilterung							
A.8.24	Einsatz von Kryptographie							
A.8.25	Sicherer Entwicklungslebenszyklus							
A.8.26	Anforderungen an die Anwendungssicherheit							
A.8.27	Sichere Systemarchitektur und technische Grundsätze							
A.8.28	Sicheres Coding							
A.8.29	Sicherheitstests in Entwicklung und Abnahme							
A.8.30	Ausgelagerte Entwicklung							
A.8.31	Trennung von Entwicklungs-, Test- und Produk-tionsumgebungen							
A.8.32	Änderungsmanagement							
A.8.33	Testinformationen							
A.8.34	Schutz von Informationssystemen während der Auditprüfung							