ISO 27001 Erklärung zur Anwendbarkeit (SoA)

Die Erklärung zur Anwendbarkeit nach Abschnitt 6.1.3(d), bereit zum Ausfüllen: alle 93 Kontrollen aus Anhang A der ISO/IEC 27001:2022, vorbefüllt über die vier Themen hinweg (Organisatorisch 37, Personenbezogen 8, Physisch 14, Technologisch 34), mit gekennzeichneten Neuerungen der Revision 2022, automatischer Auswertung und einem Mapping auf NIS2 Artikel 21(2).

Dieses PDF ist der Begleiter zum Ausdrucken und Prüfen. Die Arbeitsdatei ist das XLSX (Dropdowns für Anwendbarkeit und Umsetzungsstatus, automatisch berechnete Zusammenfassung); für KI-Agenten wird eine maschinenlesbare Markdown-Variante bereitgestellt. Alle drei Dateien sind kostenlos unter orbiqhq.com/templates/iso-27001-statement-of-applicability-template verfügbar — ohne E-Mail-Adresse.

Norm: ISO/IEC 27001:2022 (einschließlich Amd 1:2024), Abschnitt 6.1.3(d) und Anhang A. Diese Datei führt ausschließlich die Kennungen und Titel der Kontrollen auf; Kontrolltext und Umsetzungsleitlinien stehen in ISO/IEC 27001:2022 und ISO/IEC 27002:2022 und sind über die ISO oder Ihr nationales Normungsinstitut (in Deutschland: DIN) zu beziehen. Diese Vorlage ist eine Hilfestellung, keine Rechtsberatung.

Was Abschnitt 6.1.3(d) verlangt

Die SoA muss mindestens enthalten: **(1)** die notwendigen Kontrollen, die im Rahmen der Risikobehandlung bestimmt wurden (Anhang A zuzüglich etwaiger weiterer Kontrollsätze); **(2)** die Begründung für die Einbeziehung jeder notwendigen Kontrolle; **(3)** ob jede notwendige Kontrolle umgesetzt ist oder nicht; **(4)** die Begründung für den Ausschluss jeder Kontrolle aus Anhang A.

So füllen Sie sie aus

1. Arbeiten Sie von der Risikobewertung aus, nicht von der Kontrollliste. Kontrollen werden ausgewählt, weil sie identifizierte Risiken behandeln; die SoA dokumentiert das Ergebnis dieser Entscheidung, sie ersetzt sie nicht.

2. Entscheiden Sie jede der 93 Zeilen. Setzen Sie „Anwendbar?“ auf Ja oder Nein. Leere Zeilen werden im Zertifizierungsaudit als unvollständige SoA gewertet; das Blatt „Zusammenfassung“ zählt sie.

3. Begründen Sie die Einbeziehung. Benennen Sie bei anwendbaren Kontrollen das Risiko bzw. die rechtliche, vertragliche oder geschäftliche Anforderung, die die Kontrolle behandelt, setzen Sie den Umsetzungsstatus und verweisen Sie auf den Nachweis.

4. Begründen Sie den Ausschluss inhaltlich. „Nicht relevant, da wir keine physischen Büros unterhalten“ trägt; „zu teuer“ nicht.

5. Halten Sie sie unter Versionskontrolle. Weisen Sie je Zeile eine verantwortliche Person und ein Datum der letzten Überprüfung zu; aktualisieren Sie die SoA, sobald sich Risikobewertung, Risikobehandlungsplan oder Kontrollsatz ändern, und überprüfen Sie sie mindestens einmal je ISMS-Zyklus.

Hinweis: „Anwendbar? = Nein“ und „Umsetzungsstatus = Nicht anwendbar“ sind zwei verschiedene Aussagen: Die erste besagt, dass die Kontrolle nicht benötigt wird; die zweite sollte bei einer als anwendbar gekennzeichneten Kontrolle nicht auftauchen.

Dokumentenlenkung

Feld	Wert
Organisation	_____
Referenz des ISMS-Geltungsbereichs	_____
SoA-Version	_____
Genehmigt von	_____
Genehmigungsdatum	_____
Nächste Überprüfung fällig	_____
Referenz der Risikobewertung	_____
Referenz des Risikobehandlungsplans	_____

Verzeichnis der Erklärung zur Anwendbarkeit (93 Kontrollen)

Spalte „Anwendbar?“: Ja / Nein. Umsetzungsstatus: Umgesetzt / Teilweise umgesetzt / Geplant / Nicht umgesetzt / Nicht anwendbar. Die 11 mit der Revision 2022 eingeführten Kontrollen sind in der Spalte „Neu“ mit Ja gekennzeichnet.

Organisatorisch (37 Kontrollen)

ID	Name der Kontrolle	Neu	Anwendbar?	Begründung	Status
A.5.1	Informationssicherheitsrichtlinien	Nein			
A.5.2	Informationssicherheitsrollen und -verantwortlichkeiten	Nein			
A.5.3	Aufgabentrennung	Nein			
A.5.4	Verantwortlichkeiten der Leitung	Nein			
A.5.5	Kontakt mit Behörden	Nein			
A.5.6	Kontakt mit speziellen Interessengruppen	Nein			
A.5.7	Bedrohungsintelligenz	Ja			
A.5.8	Informationssicherheit im Projektmanagement	Nein			
A.5.9	Inventar der Informationen und anderer zugehöriger Werte	Nein			
A.5.10	Zulässiger Gebrauch von Informationen und anderen zugehörigen Werten	Nein			
A.5.11	Rückgabe von Werten	Nein			
A.5.12	Klassifizierung von Informationen	Nein			
A.5.13	Kennzeichnung von Informationen	Nein			
A.5.14	Informationsübertragung	Nein			
A.5.15	Zugangssteuerung	Nein			
A.5.16	Identitätsmanagement	Nein			
A.5.17	Authentisierungsinformation	Nein			
A.5.18	Zugangsrechte	Nein			
A.5.19	Informationssicherheit in Lieferantenbeziehungen	Nein			
A.5.20	Behandlung von Informationssicherheit in Lieferantenvereinbarungen	Nein			
A.5.21	Umgang mit Informationssicherheit in der IKT-Lieferkette	Nein			
A.5.22	Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen	Nein			
A.5.23	Informationssicherheit bei der Nutzung von Cloud-Diensten	Ja			
A.5.24	Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen	Nein			

ID	Name der Kontrolle	Neu	Anwendbar ?	Begründung	Status
A.5.25	Beurteilung und Entscheidung über Informationssicherheitsereignisse	Nein			
A.5.26	Reaktion auf Informationssicherheitsvorfälle	Nein			
A.5.27	Erkenntnisse aus Informationssicherheitsvorfällen	Nein			
A.5.28	Sammeln von Beweismaterial	Nein			
A.5.29	Informationssicherheit während einer Störung	Nein			
A.5.30	IKT-Bereitschaft für Business Continuity	Ja			
A.5.31	Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen	Nein			
A.5.32	Geistige Eigentumsrechte	Nein			
A.5.33	Schutz von Aufzeichnungen	Nein			
A.5.34	Privatsphäre und Schutz von personenbezogenen Daten (PII)	Nein			
A.5.35	Unabhängige Überprüfung der Informationssicherheit	Nein			
A.5.36	Einhaltung von Richtlinien, Regeln und Normen für Informationssicherheit	Nein			
A.5.37	Dokumentierte Betriebsabläufe	Nein			

Personenbezogen (8 Kontrollen)

ID	Name der Kontrolle	Neu	Anwendbar ?	Begründung	Status
A.6.1	Sicherheitsüberprüfung	Nein			
A.6.2	Beschäftigungs- und Vertragsbedingungen	Nein			
A.6.3	Informationssicherheitsbewusstsein, -ausbildung und -schulung	Nein			
A.6.4	Maßregelungsprozess	Nein			
A.6.5	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung	Nein			
A.6.6	Vertraulichkeits- oder Geheimhaltungsvereinbarungen	Nein			
A.6.7	Remote-Arbeit	Nein			
A.6.8	Meldung von Informationssicherheitsereignissen	Nein			

Physisch (14 Kontrollen)

ID	Name der Kontrolle	Neu	Anwendbar ?	Begründung	Status
A.7.1	Physische Sicherheitsperimeter	Nein			
A.7.2	Physischer Zutritt	Nein			
A.7.3	Sichern von Büros, Räumen und Einrichtungen	Nein			

ID	Name der Kontrolle	Neu	Anwendbar ?	Begründung	Status
A.7.4	Physische Sicherheitsüberwachung	Ja			
A.7.5	Schutz vor physischen und umweltbedingten Bedrohungen	Nein			
A.7.6	Arbeiten in Sicherheitsbereichen	Nein			
A.7.7	Aufgeräumte Arbeitsumgebung und Bildschirmsperren	Nein			
A.7.8	Platzierung und Schutz von Geräten und Betriebsmitteln	Nein			
A.7.9	Sicherheit von Werten außerhalb der Räumlichkeiten	Nein			
A.7.10	Speichermedien	Nein			
A.7.11	Versorgungseinrichtungen	Nein			
A.7.12	Sicherheit der Verkabelung	Nein			
A.7.13	Instandhaltung von Geräten und Betriebsmitteln	Nein			
A.7.14	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	Nein			

Technologisch (34 Kontrollen)

ID	Name der Kontrolle	Neu	Anwendbar ?	Begründung	Status
A.8.1	Endpunktgeräte von Benutzern	Nein			
A.8.2	Privilegierte Zugangsrechte	Nein			
A.8.3	Informationszugangsbeschränkung	Nein			
A.8.4	Zugang zum Quellcode	Nein			
A.8.5	Sichere Authentisierung	Nein			
A.8.6	Kapazitätssteuerung	Nein			
A.8.7	Schutz gegen Schadsoftware	Nein			
A.8.8	Handhabung von technischen Schwachstellen	Nein			
A.8.9	Konfigurationsmanagement	Ja			
A.8.10	Löschung von Informationen	Ja			
A.8.11	Datenmaskierung	Ja			
A.8.12	Verhinderung von Datenlecks	Ja			
A.8.13	Sicherung von Informationen	Nein			
A.8.14	Redundanz von informationsverarbeitenden Einrichtungen	Nein			
A.8.15	Protokollierung	Nein			
A.8.16	Überwachungstätigkeiten	Ja			
A.8.17	Uhrensynchronisation	Nein			

ID	Name der Kontrolle	Neu	Anwendbar ?	Begründung	Status
A.8.18	Gebrauch von Hilfsprogrammen mit privilegierten Rechten	Nein			
A.8.19	Installation von Software auf Systemen im Betrieb	Nein			
A.8.20	Netzwerksicherheit	Nein			
A.8.21	Sicherheit von Netzwerkdiensten	Nein			
A.8.22	Trennung von Netzwerken	Nein			
A.8.23	Webfilterung	Ja			
A.8.24	Gebrauch von Kryptografie	Nein			
A.8.25	Sicherer Entwicklungslebenszyklus	Nein			
A.8.26	Anforderungen an die Anwendungssicherheit	Nein			
A.8.27	Sichere Systemarchitektur und Prinzipien für die Systemtechnik	Nein			
A.8.28	Sicheres Codieren	Ja			
A.8.29	Sicherheitsprüfung in Entwicklung und Abnahme	Nein			
A.8.30	Ausgegliederte Entwicklung	Nein			
A.8.31	Trennung von Entwicklungs-, Test- und Produktivumgebungen	Nein			
A.8.32	Änderungssteuerung	Nein			
A.8.33	Testinformationen	Nein			
A.8.34	Schutz von Informationssystemen während Auditprüfungen	Nein			

Mapping auf NIS2 Artikel 21(2)

Maßnahme nach NIS2 Artikel 21(2)	Repräsentative Kontrollen aus Anhang A
(a) Konzepte für die Risikoanalyse und Sicherheit von Informationssystemen	A.5.1, A.5.2, A.5.4, A.5.35
(b) Bewältigung von Sicherheitsvorfällen	A.5.24, A.5.25, A.5.26, A.5.27, A.5.28, A.6.8
(c) Aufrechterhaltung des Betriebs, Backup-Management, Wiederherstellung nach einem Notfall, Krisenmanagement	A.5.29, A.5.30, A.8.13, A.8.14
(d) Sicherheit der Lieferkette, einschließlich der Beziehungen zu Lieferanten	A.5.19, A.5.20, A.5.21, A.5.22, A.5.23
(e) Sicherheit bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen	A.8.8, A.8.9, A.8.25, A.8.26, A.8.28, A.8.29, A.8.30, A.8.32
(f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen	A.5.35, A.5.36, A.8.34
(g) Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen zur Cybersicherheit	A.6.3, A.8.7, A.8.1
(h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung	A.8.24
(i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen	A.6.1, A.6.2, A.6.5, A.5.9, A.5.15, A.5.16, A.5.18, A.8.2, A.8.5
(j) Multi-Faktor-Authentifizierung, gesicherte Kommunikation und gesicherte Notfallkommunikationssysteme	A.8.5, A.5.14, A.8.20, A.8.21

Nur zur Orientierung: NIS2 Artikel 21 stellt eigene Erwartungen an Governance, Meldewesen und Durchsetzung — eine Ausrichtung an ISO 27001 unterstützt den Nachweis der NIS2-Konformität, erbringt ihn aber nicht für sich allein. Ordnen Sie jede Maßnahme Ihrer nationalen Umsetzung zu.

Auslöser für eine Überprüfung

Aktualisieren Sie diese SoA, sobald einer der folgenden Fälle eintritt, sowie mindestens einmal je ISMS-Zyklus (Managementbewertung, vor Überwachungs- und Rezertifizierungsaudits): Die Risikobewertung oder der Risikobehandlungsplan ändert sich wesentlich · Eine Kontrolle wird ergänzt, außer Kraft gesetzt oder erheblich geändert · Der Kontext der Organisation ändert sich (Abschnitt 4.1 — seit Amd 1:2024 umfasst dies ausdrücklich die Feststellung, ob der Klimawandel ein relevantes Thema ist) · Die Anforderungen interessierter Parteien ändern sich (Abschnitt 4.2) · Die Norm selbst ändert sich (der Übergang von 2013 auf 2022 endete am 31. Oktober 2025; alle gültigen Zertifikate beziehen sich nun auf ISO/IEC 27001:2022).