

ISMS - SoA (Stellungnahme zur Anwendbarkeit)

Controls Annex A ISO 27001		Status		Gründe für die Auswahl		
A.1 (27001:2022)	ISMS-Control	Umgesetzt	Anwendbar	rechtliche Vorgaben	vertr. Verpflichtun- gen	Untern.-Anf. best practice
5	Organisatorische Maßnahmen					
5.1	Informationssicherheitsrichtlinien	Ja	Ja			x
5.2	Informationssicherheitsrollen und -verantwortlichkeiten	Ja	Ja			x
5.3	Aufgabentrennung	Ja	Ja			x
5.4	Verantwortlichkeiten der Leitung	Ja	Ja			x
5.5	Kontakt mit Behörden	Ja	Ja	x		
5.6	Kontakt mit speziellen Interessensgruppen	Ja	Ja	x		
5.7	Bedrohungsintelligenz	Ja	Ja			x
5.8	Informationssicherheit im Projektmanagement	Ja	Ja			x
5.9	Inventar der Informationen und anderen Daten	Ja	Ja			x
5.10	Zulässiger Gebrauch von Informationen und Daten	Ja	Ja			x
5.11	Rückgabe von Werten	Ja	Ja			x
5.12	Klassifizierung von Information	Ja	Ja			x
5.13	Kennzeichnung von Information	Ja	Ja			x
5.14	Informationsübertragung	Ja	Ja			x
5.15	Zugangsteuerung	Ja	Ja			x
5.16	Identitätsmanagement	Ja	Ja			x
5.17	Informationen zur Authentifizierung	Ja	Ja			x
5.18	Zugangsrechte	Ja	Ja			x
5.19	Informationssicherheit in Lieferantenbeziehungen	Ja	Ja			x
5.20	Behandlung von Informationssicherheit in Lieferantensystemen	Ja	Ja			x
5.21	Umgang mit der Informationssicherheit in Lieferantensystemen	Ja	Ja			x
5.22	Überwachung, Überprüfung und Änderung	Ja	Ja			x
5.23	Informationssicherheit für die Nutzung von Diensten	Ja	Ja			x
5.24	Planung und Vorbereitung der Handhabung von Risiken	Ja	Ja			x
5.25	Beurteilung und Entscheidung über Informationsrisiken	Ja	Ja			x
5.26	Reaktion auf Informationssicherheitsvorfälle	Ja	Ja			x
5.27	Erkenntnisse aus Informationssicherheitsvorfällen	Ja	Ja			x
5.28	Sammeln von Beweismaterial	Ja	Ja			x
5.29	Informationssicherheit bei Störungen	Ja	Ja			x
5.30	IKT-Bereitschaft für Business Continuity	Ja	Ja			x
5.31	Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen	Ja	Ja			x
5.32	Geistige Eigentumsrechte	Ja	Ja			x
5.33	Schutz von Aufzeichnungen	Ja	Ja			x
5.34	Datenschutz und Schutz personenbezogener Daten	Ja	Ja			x

Controls Annex A ISO 27001		Status		Gründe für die Auswahl		
A.1 (27001:2022)	ISMS-Control	Umgesetzt	Anwendbar	rechtliche Vorgaben	vertr. Verpflichtun- gen	Untern.-Anf. best practice
5.35	Unabhängige Überprüfung der Information	Ja	Ja			x
5.36	Einhaltung von Richtlinien, Vorschriften und	Ja	Ja			x
5.37	Dokumentierte Betriebsabläufe	Ja	Ja			x
6	Personenbezogene Maßnahmen					
6.1	Sicherheitsüberprüfung	Ja	Ja	x		x
6.2	Beschäftigungs- und Vertragsbedingungen	Ja	Ja	x	x	x
6.3	Informationssicherheitsbewusstsein, -ausst	Ja	Ja	x		x
6.4	Maßregelungsprozess	Ja	Ja			x
6.5	Verantwortlichkeiten bei Beendigung oder	Ja	Ja			x
6.6	Vertraulichkeits- oder Geheimhaltungsver	Ja	Ja	x		x
6.7	Telearbeit	Ja	Ja	x		
6.8	Meldung von Informationssicherheitsereig	Ja	Ja	x		x
7	Physische Maßnahmen					
7.1	Physische Sicherheitsperimeter	Ja	Ja	x		x
7.2	Physischer Zutritt	Ja	Ja	x		x
7.3	Sichern von Büros, Räumen und Einrichtu	Ja	Ja	x		x
7.4	Physische Sicherheitsüberwachung	Ja	Ja	x		x
7.5	Schutz vor physischen und umweltbeding	Ja	Ja	x		x
7.6	Arbeiten in Sicherheitsbereichen	Ja	Ja	x		x
7.7	Aufgeräumte Arbeitsumgebung und Bildsc	Ja	Ja	x		x
7.8	Platzierung und Schutz von Geräten und	Ja	Ja	x		x
7.9	Sicherheit von Werten außerhalb der Räu	Ja	Ja	x		x
7.10	Speichermedien	Ja	Ja	x		x
7.11	Versorgungseinrichtungen	Ja	Ja	x		x
7.12	Sicherheit der Verkabelung	Ja	Ja	x		x
7.13	Instandhaltung von Geräten und Betriebs	Ja	Ja	x		x
7.14	Sichere Entsorgung oder Wiederverwend	Ja	Ja	x		x
8	Technologische Maßnahmen					
8.1	Endpunktgeräte des Benutzers	Ja	Ja	x		x
8.2	Privilegierte Zugangsrechte	Ja	Ja	x		x
8.3	Informationszugangsbeschränkung	Ja	Ja	x		x
8.4	Zugriff auf den Quellcode	Ja	Ja	x		x
8.5	Sichere Authentifizierung	Ja	Ja	x		x
8.6	Kapazitätssteuerung	Ja	Ja	x		x
8.7	Schutz gegen Schadsoftware	Ja	Ja	x		x
8.8	Handhabung von technischen Schwachst	Ja	Ja	x		x
8.9	Konfigurationsmanagement	Ja	Ja	x		x
8.10	Löschung von Informationen	Ja	Ja	x		x
8.11	Datenmaskierung	Ja	Ja	x		x
8.12	Verhinderung von Datenlecks	Ja	Ja	x		x
8.13	Sicherung von Information	Ja	Ja	x		x

Controls Annex A ISO 27001		Status		Gründe für die Auswahl		
A.1 (27001:2022)	ISMS-Control	Umgesetzt	Anwendbar	rechtliche Vorgaben	vertr. Verpflichtun- gen	Untern.-Anf. best practice
8.14	Redundanz von informationsverarbeitend	Ja	Ja	x		x
8.15	Protokollierung	Ja	Ja	x		x
8.16	Überwachungstätigkeiten	Ja	Ja	x		x
8.17	Uhrensynchronisation	Ja	Ja	x		x
8.18	Gebrauch von Hilfsprogrammen mit privile	Ja	Ja	x		x
8.19	Installation von Software auf Systemen im	Ja	Ja	x		x
8.20	Netzwerksicherheit	Ja	Ja	x		x
8.21	Sicherheit von Netzwerkdiensten	Ja	Ja	x		x
8.22	Trennung von Netzwerken	Ja	Ja	x		x
8.23	Webfilterung	Ja	Ja	x		x
8.24	Verwendung von Kryptographie	Ja	Ja	x		x
8.25	Lebenszyklus einer sicheren Entwicklung	Ja	Ja			x
8.26	Anforderungen an die Anwendungssicherh	Ja	Ja			x
8.27	Sichere Systemarchitektur und technische	Ja	Ja			x
8.28	Sicheres Coding	Ja	Ja			x
8.29	Sicherheitsprüfung bei Entwicklung und A	Ja	Ja			x
8.30	Ausgliederte Entwicklung	Ja	Ja			x
8.31	Trennung von Entwicklungs-, Prüf- und Pr	Ja	Ja	x		x
8.32	Änderungssteuerung	Ja	Ja	x		x
8.33	Prüfinformationen	Ja	Ja			x
8.34	Schutz der Informationssysteme während	Ja	Ja	x		x