Beispielbericht mit Musterdaten (fiktive Firma) - erzeugt mit MGMSYS.de, keine echten Personen- oder Kundendaten

Erklärung zur Anwendbarkeit (SoA) – Annex-A-Controls

Erstellt am 09.11.2026 14:54

Kennzahlen

Controls gesamt	Anwendbar	Nicht anwendbar	Umgesetzt	Umsetzungsquote
93	60	33	36	60,0 %

BEISPIELBERICHT MIT MUSTERDATEN

A.5 Organisatorische Maßnahmen (37)

Control-Nr.	Titel	Anwendbar	Begründung	Umsetzungsstatus	Verantwortlich
A.5.1	Informationssicherheitspolitik und -richtlinien	Ja	Erforderlich gemäß NIS2-Richtlinie und BSI-Grundschutz.	Nicht anwendbar	Demo-Nutzer
A.5.10	Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten	Ja	Anforderung ergibt sich aus der Risikoanalyse und regulatorischen Vorgaben.	In Umsetzung	Demo-Nutzer
A.5.11	Rückgabe von Werten	Ja	Erforderlich gemäß NIS2-Richtlinie und BSI-Grundschutz.	Umgesetzt	Max Mustermann
A.5.12	Klassifizierung von Informationen	Nein	Nicht relevant – Unternehmen betreibt keine eigene Softwareentwicklung.	Nicht anwendbar	–
A.5.13	Kennzeichnung von Informationen	Ja	Relevant für den Schutz der Informationsverarbeitung und -speicherung.	In Umsetzung	Demo-Nutzer
A.5.14	Informationsübermittlung	Ja	Anforderung ergibt sich aus der Risikoanalyse und regulatorischen Vorgaben.	In Umsetzung	Demo-Nutzer
A.5.15	Zugangssteuerung	Ja	Best Practice nach ISO 27001:2022.	In Umsetzung	Max Mustermann
A.5.16	Identitätsmanagement	Ja	Erforderlich gemäß NIS2-Richtlinie und BSI-Grundschutz.	Nicht anwendbar	Max Mustermann
A.5.17	Authentisierungsinformationen	Ja	Best Practice nach ISO 27001:2022.	Umgesetzt	Demo-Nutzer
A.5.18	Zugangsrechte	Ja	Best Practice nach ISO 27001:2022.	Umgesetzt	Demo-Nutzer
A.5.19	Informationssicherheit in Lieferantenbeziehungen	Ja	Relevant für den Schutz der Informationsverarbeitung und -speicherung.	Nicht anwendbar	Demo-Nutzer
A.5.2	Informationssicherheitsrollen und -verantwortlichkeiten	Ja	Anforderung ergibt sich aus der Risikoanalyse und regulatorischen Vorgaben.	Umgesetzt	Demo-Nutzer
A.5.20	Behandlung von Informationssicherheit in Lieferantenvereinbarungen	Ja	Kundenanforderung und vertragliche Verpflichtung.	Umgesetzt	Demo-Nutzer

BEISPIEL - Dokument generiert durch MGMSYS.de - Modul: ISMS - Cockpit-Management-Tool by Dr. Stefan Spoerrer

Beispielbericht mit Musterdaten (fiktive Firma) - erzeugt mit MGMSYS.de, keine echten Personen- oder Kundendaten

Control-Nr.	Titel	Anwendbar	Begründung	Umsetzungsstatus	Verantwortlich
A.5.21	Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie (IKT)	Nein	Nicht relevant – Unternehmen hat keine Produktionsumgebung (OT).	Nicht anwendbar	–
A.5.22	Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen	Ja	Kundenanforderung und vertragliche Verpflichtung.	Umgesetzt	Max Mustermann
A.5.23	Informationssicherheit für die Nutzung von Cloud-Diensten	Ja	Erforderlich gemäß NIS2-Richtlinie und BSI-Grundschutz.	In Umsetzung	Max Mustermann
A.5.24	Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen	Ja	Kontrolle adressiert identifizierte Risiken im Risikoregister.	Umgesetzt	Demo-Nutzer
A.5.25	Beurteilung und Entscheidung über Informationssicherheitsereignisse	Ja	Kontrolle adressiert identifizierte Risiken im Risikoregister.	Umgesetzt	Demo-Nutzer
A.5.26	Reaktion auf Informationssicherheitsvorfälle	Nein	Entfällt – keine Telekommunikationsinfrastruktur im Scope.	Nicht anwendbar	–
A.5.27	Erkenntnisse aus Informationssicherheitsvorfällen	Ja	Anforderung ergibt sich aus der Risikoanalyse und regulatorischen Vorgaben.	Nicht anwendbar	Demo-Nutzer
A.5.28	Sammeln von Beweismaterial	Ja	Relevant für den Schutz der Informationsverarbeitung und -speicherung.	Umgesetzt	Demo-Nutzer
A.5.29	Informationssicherheit bei Störungen	Ja	Notwendig zur Einhaltung der DSGVO und branchenspezifischer Standards.	Nicht anwendbar	Demo-Nutzer
A.5.3	Aufgabentrennung	Ja	Relevant für den Schutz der Informationsverarbeitung und -speicherung.	Umgesetzt	Demo-Nutzer
A.5.30	IKT-Bereitschaft für Business-Continuity	Ja	Best Practice nach ISO 27001:2022.	Nicht anwendbar	Max Mustermann
A.5.31	Juristische, gesetzliche, regulatorische und vertragliche Anforderungen	Ja	Kontrolle adressiert identifizierte Risiken im Risikoregister.	Nicht anwendbar	Max Mustermann
A.5.32	Geistige Eigentumsrechte	Ja	Erforderlich gemäß NIS2-Richtlinie und BSI-Grundschutz.	In Umsetzung	Max Mustermann
A.5.33	Schutz von Aufzeichnungen	Ja	Notwendig zur Einhaltung der DSGVO und branchenspezifischer Standards.	Umgesetzt	Max Mustermann
A.5.34	Datenschutz und Schutz von personenbezogenen Daten (PbD)	Ja	Anforderung ergibt sich aus der Risikoanalyse und regulatorischen Vorgaben.	Nicht anwendbar	Demo-Nutzer
A.5.35	Unabhängige Überprüfung der Informationssicherheit	Nein	Entfällt – keine Telekommunikationsinfrastruktur im Scope.	Nicht anwendbar	–
A.5.36	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit	Ja	Best Practice nach ISO 27001:2022.	Umgesetzt	Max Mustermann
A.5.37	Dokumentierte Betriebsabläufe	Ja	Erforderlich gemäß NIS2-Richtlinie und BSI-Grundschutz.	Umgesetzt	Demo-Nutzer
A.5.4	Verantwortlichkeiten der Leitung	Nein	Nicht zutreffend – kein physischer Serverraum vorhanden (Cloud-only).	Nicht anwendbar	–
A.5.5	Kontakt mit Behörden	Ja	Kundenanforderung und vertragliche Verpflichtung.	Nicht begonnen	Max Mustermann
A.5.6	Kontakt mit speziellen Interessensgruppen	Ja	Kontrolle adressiert identifizierte Risiken im Risikoregister.	Umgesetzt	Max Mustermann

BEISPIELBERICHT MIT MUSTERDATEN

Beispielbericht mit Musterdaten (fiktive Firma) - erzeugt mit MGMSYS.de, keine echten Personen- oder Kundendaten

Control-Nr.	Titel	Anwendbar	Begründung	Umsetzungsstatus	Verantwortlich
A.5.7	Informationen über die Bedrohungslage	Ja	Anforderung ergibt sich aus der Risikoanalyse und regulatorischen Vorgaben.	Umgesetzt	Max Mustermann
A.5.8	Informationssicherheit im Projektmanagement	Ja	Kundenanforderung und vertragliche Verpflichtung.	Umgesetzt	Demo-Nutzer
A.5.9	Inventar der Informationen und anderen damit verbundenen Werte	Ja	Relevant für den Schutz der Informationsverarbeitung und -speicherung.	In Umsetzung	Max Mustermann

A.6 Personenbezogene Maßnahmen (8)

Control-Nr.	Titel	Anwendbar	Begründung	Umsetzungsstatus	Verantwortlich
A.6.1	Sicherheitsüberprüfung	Ja	Best Practice nach ISO 27001:2022.	In Umsetzung	Demo-Nutzer
A.6.2	Beschäftigungs- und Vertragsbedingungen	Ja	Best Practice nach ISO 27001:2022.	Nicht anwendbar	Max Mustermann
A.6.3	Informationssicherheitsbewusstsein, -ausbildung und -schulung	Ja	Notwendig zur Einhaltung der DSGVO und branchenspezifischer Standards.	Umgesetzt	Max Mustermann
A.6.4	Maßregelungsprozess	Ja	Best Practice nach ISO 27001:2022.	Umgesetzt	Max Mustermann
A.6.5	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung	Nein	Nicht relevant – Unternehmen betreibt keine eigene Softwareentwicklung.	Nicht anwendbar	–
A.6.6	BEISPIEL - eits- oder ngsvereinbarungen	Nein	Ausgeschlossen aus dem ISMS-Scope per Managemententscheidung.	Nicht anwendbar	–
A.6.7	Remote-Arbeit	Ja	Notwendig zur Einhaltung der DSGVO und branchenspezifischer Standards.	Umgesetzt	Max Mustermann
A.6.8	Meldung von Informationssicherheitsereignissen	Ja	Kontrolle adressiert identifizierte Risiken im Risikoregister.	Umgesetzt	Demo-Nutzer

A.7 Physische Maßnahmen (14)

Control-Nr.	Titel	Anwendbar	Begründung	Umsetzungsstatus	Verantwortlich
A.7.1	Physische Sicherheitsperimeter	Ja	Relevant für den Schutz der Informationsverarbeitung und -speicherung.	Nicht begonnen	Max Mustermann
A.7.10	Speichermedien	Ja	Kundenanforderung und vertragliche Verpflichtung.	Nicht anwendbar	Demo-Nutzer
A.7.11	Versorgungseinrichtungen	Ja	Kontrolle adressiert identifizierte Risiken im Risikoregister.	Nicht begonnen	Max Mustermann
A.7.12	Sicherheit der Verkabelung	Ja	Anforderung ergibt sich aus der Risikoanalyse und regulatorischen Vorgaben.	Nicht begonnen	Demo-Nutzer
A.7.13	Instandhaltung von Geräten und Betriebsmitteln	Ja	Notwendig zur Einhaltung der DSGVO und branchenspezifischer Standards.	In Umsetzung	Demo-Nutzer

BEISPIELBERICHT MIT MUSTERDATEN

BEISPIEL - Dokument generiert durch MGMSYS.de - Modul: ISMS - Cockpit-Management-Tool by Dr. Stefan Spoerrer

Control-Nr.	Titel	Anwendbar	Begründung	Umsetzungsstatus	Verantwortlich
A.7.14	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	Nein	Entfällt – keine Telekommunikationsinfrastruktur im Scope.	Nicht anwendbar	–
A.7.2	Physischer Zutritt	Ja	Best Practice nach ISO 27001:2022.	Umgesetzt	Max Mustermann
A.7.3	Sichern von Büros, Räumen und Einrichtungen	Nein	Nicht relevant – Unternehmen hat keine Produktionsumgebung (OT).	Nicht anwendbar	–
A.7.4	Physische Sicherheitsüberwachung	Ja	Kontrolle adressiert identifizierte Risiken im Risikoregister.	Umgesetzt	Demo-Nutzer
A.7.5	Schutz vor physischen und umweltbedingten Bedrohungen	Ja	Anforderung ergibt sich aus der Risikoanalyse und regulatorischen Vorgaben.	In Umsetzung	Max Mustermann
A.7.6	Arbeiten in Sicherheitsbereichen	Nein	Nicht relevant – Unternehmen hat keine Produktionsumgebung (OT).	Nicht anwendbar	–
A.7.7	Aufgeräumte Arbeitsumgebung und Bildschirmsperren	Ja	Notwendig zur Einhaltung der DSGVO und branchenspezifischer Standards.	Nicht begonnen	Max Mustermann
A.7.8	Platzierung und Schutz von Geräten und Betriebsmitteln	Ja	Relevant für den Schutz der Informationsverarbeitung und -speicherung.	In Umsetzung	Max Mustermann
A.7.9	Sicherheit von Werten außerhalb der Räumlichkeiten	Ja	Kundenanforderung und vertragliche Verpflichtung.	Umgesetzt	Max Mustermann

BEISPIELBERICHT MIT MUSTERDATEN

A.8 Technologische Maßnahmen (34)

Control-Nr.	Titel	Anwendbar	Begründung	Umsetzungsstatus	Verantwortlich
A.8.1	Endpunktgeräte des Benutzers	Nein	Nicht zutreffend – kein physischer Serverraum vorhanden (Cloud-only).	Nicht anwendbar	–
A.8.10	Löschung von Informationen	Ja	Anforderung ergibt sich aus der Risikoanalyse und regulatorischen Vorgaben.	In Umsetzung	Demo-Nutzer
A.8.11	Datenmaskierung	Ja	Relevant für den Schutz der Informationsverarbeitung und -speicherung.	Umgesetzt	Max Mustermann
A.8.12	Verhinderung von Datenlecks	Ja	Best Practice nach ISO 27001:2022.	Umgesetzt	Max Mustermann
A.8.13	Sicherung von Informationen	Ja	Anforderung ergibt sich aus der Risikoanalyse und regulatorischen Vorgaben.	Umgesetzt	Max Mustermann
A.8.14	Redundanz von informationsverarbeitenden Einrichtungen	Ja	Notwendig zur Einhaltung der DSGVO und branchenspezifischer Standards.	Umgesetzt	Max Mustermann
A.8.15	Protokollierung	Ja	Best Practice nach ISO 27001:2022.	Umgesetzt	Max Mustermann
A.8.16	Überwachung von Aktivitäten	Ja	Kontrolle adressiert identifizierte Risiken im Risikoregister.	Nicht anwendbar	Max Mustermann
A.8.17	Uhrensynchronisation	Ja	Kontrolle adressiert identifizierte Risiken im Risikoregister.	Nicht anwendbar	Max Mustermann
A.8.18	Gebrauch von Hilfsprogrammen mit privilegierten Rechten	Nein	Nicht relevant – Unternehmen hat keine Produktionsumgebung (OT).	Nicht anwendbar	–
A.8.19	Installation von Software auf Systemen im Betrieb	Nein	Ausgeschlossen aus dem ISMS-Scope per Managemententscheidung.	Nicht anwendbar	–

BEISPIEL - Dokument generiert durch MGMSYS.de - Modul: ISMS - Cockpit-Management-Tool by Dr. Stefan Spoerrer

Beispielbericht mit Musterdaten (fiktive Firma) - erzeugt mit MGMSYS.de, keine echten Personen- oder Kundendaten

Control-Nr.	Titel	Anwendbar	Begründung	Umsetzungsstatus	Verantwortlich
A.8.2	Privilegierte Zugangsrechte	Ja	Erforderlich gemäß NIS2-Richtlinie und BSI-Grundschutz.	Umgesetzt	Demo-Nutzer
A.8.20	Netzwerksicherheit	Ja	Relevant für den Schutz der Informationsverarbeitung und -speicherung.	Nicht anwendbar	Demo-Nutzer
A.8.21	Sicherheit von Netzwerkdiensten	Ja	Kundenanforderung und vertragliche Verpflichtung.	In Umsetzung	Max Mustermann
A.8.22	Trennung von Netzwerken	Nein	Ausgeschlossen aus dem ISMS-Scope per Managemententscheidung.	Nicht anwendbar	–
A.8.23	Webfilterung	Ja	Relevant für den Schutz der Informationsverarbeitung und -speicherung.	In Umsetzung	Max Mustermann
A.8.24	Verwendung von Kryptographie	Ja	Best Practice nach ISO 27001:2022.	Umgesetzt	Demo-Nutzer
A.8.25	Lebenszyklus einer sicheren Entwicklung	Nein	Nicht relevant – Unternehmen hat keine Produktionsumgebung (OT).	Nicht anwendbar	–
A.8.26	Anforderungen an die Anwendungssicherheit	Ja	Erforderlich gemäß NIS2-Richtlinie und BSI-Grundschutz.	In Umsetzung	Demo-Nutzer
A.8.27	Sichere Systemarchitektur und Entwicklungsgrundsätze	Ja	Best Practice nach ISO 27001:2022.	Nicht anwendbar	Demo-Nutzer
A.8.28	Sichere Codierung	Ja	Kundenanforderung und vertragliche Verpflichtung.	Nicht anwendbar	Max Mustermann
A.8.29	Sicherheitsprüfung bei Entwicklung und Abnahme	Ja	Relevant für den Schutz der Informationsverarbeitung und -speicherung.	Umgesetzt	Demo-Nutzer
A.8.3	Informationszugangsbeschränkung	Ja	Relevant für den Schutz der Informationsverarbeitung und -speicherung.	Nicht anwendbar	Max Mustermann
A.8.30	Ausgegliederte Entwicklung	Ja	Anforderung ergibt sich aus der Risikoanalyse und regulatorischen Vorgaben.	Umgesetzt	Max Mustermann
A.8.31	Trennung von Entwicklungs-, Test- und Produktionsumgebungen	Ja	Notwendig zur Einhaltung der DSGVO und branchenspezifischer Standards.	Nicht begonnen	Max Mustermann
A.8.32	Änderungssteuerung	Ja	Anforderung ergibt sich aus der Risikoanalyse und regulatorischen Vorgaben.	In Umsetzung	Max Mustermann
A.8.33	Testdaten	Ja	Best Practice nach ISO 27001:2022.	Nicht begonnen	Demo-Nutzer
A.8.34	Schutz der Informationssysteme während Tests im Rahmen von Audits	Ja	Kontrolle adressiert identifizierte Risiken im Risikoregister.	Umgesetzt	Demo-Nutzer
A.8.4	Zugriff auf den Quellcode	Ja	Best Practice nach ISO 27001:2022.	Umgesetzt	Demo-Nutzer
A.8.5	Sichere Authentisierung	Ja	Anforderung ergibt sich aus der Risikoanalyse und regulatorischen Vorgaben.	Nicht begonnen	Max Mustermann
A.8.6	Kapazitätssteuerung	Nein	Nicht zutreffend – kein physischer Serverraum vorhanden (Cloud-only).	Nicht anwendbar	–
A.8.7	Schutz gegen Schadsoftware	Ja	Notwendig zur Einhaltung der DSGVO und branchenspezifischer Standards.	Nicht anwendbar	Max Mustermann
A.8.8	Handhabung von technischen Schwachstellen	Ja	Kontrolle adressiert identifizierte Risiken im Risikoregister.	Umgesetzt	Max Mustermann
A.8.9	Konfigurationsmanagement	Ja	Notwendig zur Einhaltung der DSGVO und branchenspezifischer Standards.	Umgesetzt	Demo-Nutzer

BEISPIELBERICHT MIT MUSTERDATEN