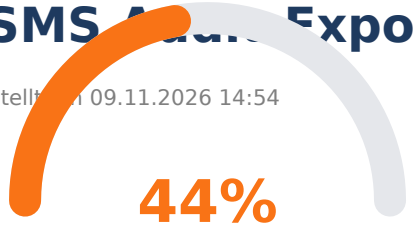
Beispielbericht mit Musterdaten (fiktive Firma) - erzeugt mit MGMSYS.de, keine echten Personen- oder Kundendaten

ISMS Audit-Export (ISO/IEC 27001)

Erstellt am 09.11.2026 14:54



BEISPIELBERICHT MIT MUSTERDATEN

Kontext der Organisation 100%	**Risikobehandlung** 16%	**Statement of Applicability** 60%	**Sicherheitsziele** 0%
Dokumentenlenkung 71%	**Schulung / Awareness** 49%	**Maßnahmen umgesetzt** 30%	**Internes Audit** 39%
Managementbewertung 0%	**Korrekturmaßnahmen** 100%	**Nachweis-Abdeckung** 0%	

Zertifizierungs-Readiness (Übersicht)

Gesamt-Reifegrad: 44.3 % audit-ready.

ISO-27001-Baustein	Gewicht	Erfüllung
Kontext der Organisation (Kap. 4)	5 %	100.0 %
Risikobehandlung (Kap. 6.1)	15 %	15.5 %
Statement of Applicability (6.1.3)	20 %	60.0 %
Sicherheitsziele (Kap. 6.2)	5 %	0.0 %
Dokumentenlenkung (Kap. 7.5)	15 %	71.1 %

ISO-27001-Baustein	Gewicht	Erfüllung
Schulung / Awareness (7.2/7.3)	5 %	48.6 %
Maßnahmen umgesetzt (Kap. 8)	10 %	29.7 %
Internes Audit (Kap. 9.2)	10 %	39.3 %
Managementbewertung (Kap. 9.3)	5 %	0.0 %
Korrekturmaßnahmen (Kap. 10)	5 %	100.0 %
Nachweis-Abdeckung (Control→Nachweis)	5 %	0.0 %

Statement of Applicability (SoA)

BEISPIELBERICHT MIT MUSTERDATEN

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

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

BEISPIELBERICHT MIT MUSTERDATEN

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	Titel	Anwendbar	Umsetzung	Begründung	Nächste Überprüfung
A.5.4	Verantwortlichkeiten der Leitung	Nein	Nicht anwendbar	Nicht zutreffend – kein physischer Serverraum vorhanden (Cloud-only).	-
A.5.5	Kontakt mit Behörden	Ja	Nicht begonnen	Kundenanforderung und vertragliche Verpflichtung.	-
A.5.6	Kontakt mit speziellen Interessensgruppen	Ja	Umgesetzt	Kontrolle adressiert identifizierte Risiken im Risikoregister.	-
A.5.7	Informationen über die Bedrohungslage	Ja	Umgesetzt	Anforderung ergibt sich aus der Risikoanalyse und regulatorischen Vorgaben.	-
A.5.8	Informationssicherheit im Projektmanagement	Ja	Umgesetzt	Kundenanforderung und vertragliche Verpflichtung.	-
A.5.9	Inventar der Informationen und anderen damit verbundenen Werte	Ja	In Umsetzung	Relevant für den Schutz der Informationsverarbeitung und -speicherung.	-
A.6.1	Sicherheitsüberprüfung	Ja	In Umsetzung	Best Practice nach ISO 27001:2022.	-
A.6.2	Beschäftigungs- und Vertragsbedingungen	Ja	Nicht anwendbar	Best Practice nach ISO 27001:2022.	-
A.6.3	Informationssicherheitsbewusstsein, -ausbildung und -schulung	Ja	Umgesetzt	Notwendig zur Einhaltung der DSGVO und branchenspezifischer Standards.	-
A.6.4	Maßregelungsprozess	Ja	Umgesetzt	Best Practice nach ISO 27001:2022.	-
A.6.5	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung	Nein	Nicht anwendbar	Nicht relevant – Unternehmen betreibt keine eigene Softwareentwicklung.	-
A.6.6	BEISPIEL - eits- oder ngsvereinbarungen	Nein	Nicht anwendbar	Ausgeschlossen aus dem ISMS-Scope per Managemententscheidung.	-
A.6.7	Remote-Arbeit	Ja	Umgesetzt	Notwendig zur Einhaltung der DSGVO und branchenspezifischer Standards.	-
A.6.8	Meldung von Informationssicherheitsereignissen	Ja	Umgesetzt	Kontrolle adressiert identifizierte Risiken im Risikoregister.	-
A.7.1	Physische Sicherheitsperimeter	Ja	Nicht begonnen	Relevant für den Schutz der Informationsverarbeitung und -speicherung.	-
A.7.10	Speichermedien	Ja	Nicht anwendbar	Kundenanforderung und vertragliche Verpflichtung.	-
A.7.11	Versorgungseinrichtungen	Ja	Nicht begonnen	Kontrolle adressiert identifizierte Risiken im Risikoregister.	-
A.7.12	Sicherheit der Verkabelung	Ja	Nicht begonnen	Anforderung ergibt sich aus der Risikoanalyse und regulatorischen Vorgaben.	-
A.7.13	Instandhaltung von Geräten und Betriebsmitteln	Ja	In Umsetzung	Notwendig zur Einhaltung der DSGVO und branchenspezifischer Standards.	-
A.7.14	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	Nein	Nicht anwendbar	Entfällt – keine Telekommunikationsinfrastruktur im Scope.	-
A.7.2	Physischer Zutritt	Ja	Umgesetzt	Best Practice nach ISO 27001:2022.	-

BEISPIELBERICHT MIT MUSTERDATEN

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

TESTZUGANG GmbH

Control	Titel	Anwendbar	Umsetzung	Begründung	Nächste Überprüfung
A.7.3	Sichern von Büros, Räumen und Einrichtungen	Nein	Nicht anwendbar	Nicht relevant – Unternehmen hat keine Produktionsumgebung (OT).	-
A.7.4	Physische Sicherheitsüberwachung	Ja	Umgesetzt	Kontrolle adressiert identifizierte Risiken im Risikoregister.	-
A.7.5	Schutz vor physischen und umweltbedingten Bedrohungen	Ja	In Umsetzung	Anforderung ergibt sich aus der Risikoanalyse und regulatorischen Vorgaben.	-
A.7.6	Arbeiten in Sicherheitsbereichen	Nein	Nicht anwendbar	Nicht relevant – Unternehmen hat keine Produktionsumgebung (OT).	-
A.7.7	Aufgeräumte Arbeitsumgebung und Bildschirmsperren	Ja	Nicht begonnen	Notwendig zur Einhaltung der DSGVO und branchenspezifischer Standards.	-
A.7.8	Platzierung und Schutz von Geräten und Betriebsmitteln	Ja	In Umsetzung	Relevant für den Schutz der Informationsverarbeitung und -speicherung.	-
A.7.9	Sicherheit von Werten außerhalb der Räumlichkeiten	Ja	Umgesetzt	Kundenanforderung und vertragliche Verpflichtung.	-
A.8.1	Endpunktgeräte des Benutzers	Nein	Nicht anwendbar	Nicht zutreffend – kein physischer Serverraum vorhanden (Cloud-only).	-
A.8.10	Löschung von Informationen	Ja	In Umsetzung	Anforderung ergibt sich aus der Risikoanalyse und regulatorischen Vorgaben.	-
A.8.11	Datenmaskierung	Ja	Umgesetzt	Relevant für den Schutz der Informationsverarbeitung und -speicherung.	-
A.8.12	Verhinderung von Datenlecks	Ja	Umgesetzt	Best Practice nach ISO 27001:2022.	-
A.8.13	Sicherung von Informationen	Ja	Umgesetzt	Anforderung ergibt sich aus der Risikoanalyse und regulatorischen Vorgaben.	-
A.8.14	Redundanz von informationsverarbeitenden Einrichtungen	Ja	Umgesetzt	Notwendig zur Einhaltung der DSGVO und branchenspezifischer Standards.	-
A.8.15	Protokollierung	Ja	Umgesetzt	Best Practice nach ISO 27001:2022.	-
A.8.16	Überwachung von Aktivitäten	Ja	Nicht anwendbar	Kontrolle adressiert identifizierte Risiken im Risikoregister.	-
A.8.17	Uhrensynchronisation	Ja	Nicht anwendbar	Kontrolle adressiert identifizierte Risiken im Risikoregister.	-
A.8.18	Gebrauch von Hilfsprogrammen mit privilegierten Rechten	Nein	Nicht anwendbar	Nicht relevant – Unternehmen hat keine Produktionsumgebung (OT).	-
A.8.19	Installation von Software auf Systemen im Betrieb	Nein	Nicht anwendbar	Ausgeschlossen aus dem ISMS-Scope per Managemententscheidung.	-
A.8.2	Privilegierte Zugangsrechte	Ja	Umgesetzt	Erforderlich gemäß NIS2-Richtlinie und BSI-Grundschutz.	-
A.8.20	Netzwerksicherheit	Ja	Nicht anwendbar	Relevant für den Schutz der Informationsverarbeitung und -speicherung.	-

BEISPIELBERICHT MIT MUSTERDATEN

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

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

BEISPIELBERICHT MIT MUSTERDATEN

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

Risikoregister

Ref.	Titel	Score	Behandlung	Restrisiko	Status
R-0000-47B4	Veraltete Firewall-Firmware (behoben)	53.28	Reduzieren	6.66	Geschlossen
RISK-NEW-01	Datenverlust durch Ransomware-Angriff	49.95	Reduzieren	3.33	Akzeptiert
R-0000-09A4	Unbefugter Zugriff auf Kundendaten	49.95	Reduzieren	33.30	Bewertet
R-0000-9FC8	Kompromittierung der Cloud-Infrastruktur (AWS)	45.00	Reduzieren	15.00	Behandelt
R-0000-6D2C	Ransomware-Angriff auf zentrale Server	45.00	Reduzieren	15.00	Identifiziert
RISK-NEW-02	Unbefugter Zugriff auf KI-API-Keys	44.04	Reduzieren	3.67	Bewertet
R-0000-38A0	Kompromittierung von Benutzerkonten	42.72	Reduzieren	16.02	Behandelt
R-0000-236C	B007 - Unzureichende Vertragsregelungen	39.96	Reduzieren	19.98	Bewertet
RISK-NEW-04	Ausfall Produktionsdatenbank	36.70	Reduzieren	3.67	Bewertet
R-0000-A0A3	B001 - Verstoß gegen Gesetze / Vorschriften, Daten	36.00	Reduzieren	18.00	Bewertet
R-0000-E57F	B022 - Hard- und Software-Fehler	36.00	Reduzieren	18.00	Bewertet
R-0000-6419	Social Engineering gegen Führungskräfte	36.00	Reduzieren	12.00	Identifiziert
RISK-NEW-08	Insider-Bedrohung durch privilegierten Admin	33.30	Reduzieren	3.33	Bewertet
R-0000-3087	Verlust von HR-Daten durch Personio-Kompromittieru	33.30	Reduzieren	13.32	Behandelt
R-0000-66B1	Ausfall des ERP-Systems	33.30	Reduzieren	13.32	Bewertet
R-0000-1DCA	B022 - Hard- und Software-Fehler	33.03	Reduzieren	14.68	Bewertet
R-0000-19ED	B022 - Hard- und Software-Fehler	33.03	Reduzieren	14.68	Bewertet
R-0000-F102	Datenverlust durch Fehlbedienung im CRM	33.03	Reduzieren	14.68	Behandelt
R-0000-A55E	Abfluss von Finanzdaten	30.00	Reduzieren	12.00	Bewertet
R-0000-BD48	Datenverlust durch fehlende Datensicherung	30.00	Reduzieren	15.00	Identifiziert
R-0000-7F13	B022 - Hard- und Software-Fehler	29.97	Reduzieren	13.32	Bewertet
R-0000-7BAD	B022 - Hard- und Software-Fehler	29.97	Reduzieren	13.32	Bewertet
RISK-NEW-05	Social Engineering gegen Helpdesk	29.97	Reduzieren	3.33	Bewertet
R-0000-C839	Ausfall der Internetanbindung	29.97	Reduzieren	6.66	Behandelt
RISK-NEW-07	Supply-Chain-Angriff über npm-Package	29.36	Reduzieren	3.67	Bewertet
R-0000-3567	Kompromittierung des Netzwerkspeicher (NAS)	27.96	Reduzieren	6.99	Bewertet
R-0000-56F1	Abfluss BEISPIEL - r Dokumente	27.96	Reduzieren	13.98	Behandelt

BEISPIELBERICHT MIT MUSTERDATEN

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

Ref.	Titel	Score	Behandlung	Restrisiko	Status
R-0000-F4CC	B007 - Unzureichende Vertragsregelungen	27.00	Reduzieren	12.00	Bewertet
R-0000-73FF	B023 - Fehlplanung oder fehlende Anpassung	27.00	Reduzieren	12.00	Bewertet
RISK-NEW-09	Denial-of-Service auf öffentliche API	27.00	Reduzieren	3.00	Bewertet
RISK-NEW-06	Compliance-Verstoß durch KI-Halluzinationen	27.00	Akzeptieren	3.00	Bewertet
R-0000-A954	B021 - Manipulation von Hardware, Software oder In	26.64	Reduzieren	9.99	Bewertet
R-0000-C1C9	B026 - Vertragsverletzungen	26.64	Reduzieren	9.99	Bewertet
R-0000-21AA	B018 - Diebstahl / Verlust von Geräten, Datenträge	26.64	Reduzieren	9.99	Bewertet
RISK-NEW-12	Ausfall Cloud-Provider > 4h	26.64	Übertragen	3.33	Bewertet
RISK-NEW-11	DSGVO-Bußgeld durch verspätete Vorfallmeldung	26.64	Reduzieren	3.33	Bewertet
RISK-NEW-03	Datenleck durch fehlkonfigurierte Cloud-Bucket	26.64	Reduzieren	3.33	Bewertet
R-0000-90EB	Ausfall der USV im Serverraum	26.64	Reduzieren	6.66	Identifiziert
R-0000-315E	Verlust der E-Mail-Verfügbarkeit	26.64	Akzeptieren	19.98	Akzeptiert
R-0000-A838	B015 - Ausfall oder Störung von Kommunikationsnetz	24.03	Reduzieren	10.68	Bewertet
R-0000-AD77	B023 - Fehlplanung oder fehlende Anpassung	24.03	Reduzieren	10.68	Bewertet
R-0000-87C4	B019 - Unberechtigte Wiederherstellung von Informa	24.00	Reduzieren	9.00	Bewertet
R-0000-D4A0	B015 - Ausfall oder Störung von Kommunikationsnetz	24.00	Reduzieren	12.00	Bewertet
R-0000-7A87	B018 - Diebstahl / Verlust von Geräten, Datenträge	24.00	Reduzieren	9.00	Bewertet
R-0000-41ED	Physischer Einbruch in Serverraum	24.00	Reduzieren	12.00	Bewertet
R-0000-5508	Zero-Day-Exploit der Perimeter-Firewall	23.30	Reduzieren	9.32	Behandelt
R-0000-9E69	Manipulation von Projektdokumentation	22.02	Reduzieren	7.34	Behandelt
R-0000-B434	B021 - Manipulation von Hardware, Software oder In	19.98	Reduzieren	6.66	Bewertet
R-0000-2C37	B019 - Unberechtigte Wiederherstellung von Informa	19.98	Reduzieren	6.66	Bewertet
R-0000-152E	B026 - Vertragsverletzungen	19.98	Reduzieren	6.66	Bewertet
R-0000-05AC	B001 - Verstoß gegen Gesetze / Vorschriften, Daten	19.98	Reduzieren	6.66	Bewertet
R-0000-9981	B014 - Ausfall Versorgung (Strom, Wasser, etc.)	19.98	Reduzieren	6.66	Bewertet
R-0000-2E7F	B018 - Diebstahl / Verlust von Geräten, Datenträge	19.98	Reduzieren	6.66	Bewertet
R-0000-3037	B022 - Hard- und Software-Fehler	19.98	Reduzieren	6.66	Bewertet
R-0000-BC5A	B015 - Ausfall oder Störung von Kommunikationsnetz	18.64	Reduzieren	6.99	Bewertet
R-0000-722D	B004 - Unzureichendes Notfall-Management	18.64	Reduzieren	6.99	Bewertet
R-0000-32B1	B021 - Manipulation von Hardware, Software oder In	18.00	Reduzieren	6.00	Bewertet

BEISPIELBERICHT MIT MUSTERDATEN

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

Ref.	Titel	Score	Behandlung	Restrisiko	Status
R-0000-B94C	B026 - Vertragsverletzungen	18.00	Reduzieren	6.00	Bewertet
R-0000-1C44	B007 - Unzureichende Vertragsregelungen	18.00	Reduzieren	6.00	Bewertet
R-0000-B130	B007 - Unzureichende Vertragsregelungen	18.00	Reduzieren	6.00	Bewertet
R-0000-D524	B007 - Unzureichende Vertragsregelungen	18.00	Reduzieren	6.00	Bewertet
R-0000-9726	B004 - Unzureichendes Notfall-Management	18.00	Reduzieren	6.00	Bewertet
R-0000-DD2A	Ausfall der Zutrittskontrolle	18.00	Reduzieren	6.00	Behandelt
R-0000-2F8B	B004 - Unzureichendes Notfall-Management	16.02	Reduzieren	5.34	Bewertet
R-0000-AB5B	Phishing-Angriff auf Geschäftsführung (CEO-Fraud)	16.00	Reduzieren	8.00	Behandelt
RISK-NEW-10	Verlust kryptographischer Schlüssel	15.00	Reduzieren	3.00	Bewertet
R-0000-0301	B009 - Konfigurationsfehler	14.68	Reduzieren	3.67	Bewertet
R-0000-2D86	B009 - Konfigurationsfehler	14.68	Reduzieren	11.01	Bewertet
R-0000-02AA	B023 - Fehlplanung oder fehlende Anpassung	13.98	Reduzieren	4.66	Bewertet
R-0000-E69C	Verlust von Notebooks im Außendienst	13.98	Akzeptieren	6.99	Akzeptiert
R-0000-4659	Natürliche Schadensereignisse (Brand, Wasser)	13.35	Übertragen	8.01	Akzeptiert
R-0000-B6A5	B019 - Unberechtigte Wiederherstellung von Informa	13.32	Reduzieren	3.33	Bewertet
R-0000-84F1	B010 - Unzureichende Verfügbarkeit von Personen	13.32	Reduzieren	9.99	Bewertet
R-0000-C935	B010 - Unzureichende Verfügbarkeit von Personen	13.32	Reduzieren	9.99	Bewertet
R-0000-D8FA	B006 - Ausfall oder Störung von Dienstleister	13.32	Reduzieren	3.33	Bewertet
R-0000-944B	B015 - Ausfall oder Störung von Kommunikationsnetz	13.32	Reduzieren	9.99	Bewertet
R-0000-E51C	B009 - Konfigurationsfehler	13.32	Reduzieren	3.33	Bewertet
R-0000-3BF0	B021 - Manipulation von Hardware, Software oder In	12.00	Reduzieren	3.00	Bewertet
R-0000-FE3A	B019 - Unberechtigte Wiederherstellung von Informa	12.00	Reduzieren	3.00	Bewertet
R-0000-7AD7	B010 - Unzureichende Verfügbarkeit von Personen	12.00	Reduzieren	3.00	Bewertet
R-0000-7F27	B010 - Unzureichende Verfügbarkeit von Personen	12.00	Reduzieren	4.00	Bewertet
R-0000-3BC7	B001 - Verstoß gegen Gesetze / Vorschriften, Daten	12.00	Reduzieren	3.00	Bewertet
R-0000-9886	B014 - Ausfall Versorgung (Strom, Wasser, etc.)	12.00	Reduzieren	4.00	Bewertet
R-0000-5CA4	B004 - Unzureichendes Notfall-Management	12.00	Reduzieren	4.00	Bewertet
R-0000-A8C8	Verstoß gegen DSGVO-Löschpflichten	12.00	Reduzieren	6.00	Bewertet
R-0000-FDD8	B014 - Ausfall Versorgung (Strom, Wasser, etc.)	10.68	Reduzieren	2.67	Bewertet
R-0000-B4C8	Supply-Chain-Angriff über Softwarelieferanten	10.00	Reduzieren	5.00	Bewertet

BEISPIELBERICHT MIT MUSTERDATEN

Ref.	Titel	Score	Behandlung	Restrisiko	Status
R-0000-0803	Insider-Bedrohung durch privilegierte Administrato	10.00	Reduzieren	4.00	Bewertet
R-0000-127A	B007 - Unzureichende Vertragsregelungen	9.99	Reduzieren	6.66	Bewertet
R-0000-E011	B009 - Konfigurationsfehler	9.99	Reduzieren	6.66	Bewertet
R-0000-D2FB	B006 - Ausfall oder Störung von Dienstleister	9.32	Reduzieren	6.99	Bewertet
R-0000-5576	B006 - Ausfall oder Störung von Dienstleister	9.00	Reduzieren	6.00	Bewertet
R-0000-DE5B	DDoS-Angriff auf externe Webdienste	9.00	Reduzieren	4.00	Behandelt
R-0000-9E66	B026 - Vertragsverletzungen	8.00	Reduzieren	6.00	Bewertet
R-0000-2016	B022 - Hard- und Software-Fehler	8.00	Reduzieren	2.00	Bewertet
R-0000-A9D7	B007 - Unzureichende Vertragsregelungen	7.98	Reduzieren	2.66	Bewertet
R-0000-37B4	B006 - Ausfall oder Störung von Dienstleister	7.98	Reduzieren	2.66	Bewertet
R-0000-1BC5	B022 - Hard- und Software-Fehler	6.66	Reduzieren	3.33	Bewertet
R-0000-3433	B001 - Verstoß gegen Gesetze / Vorschriften, Daten	6.00	Reduzieren	3.00	Bewertet
R-0000-C60A	B018 - Diebstahl / Verlust von Geräten, Datenträge	6.00	Reduzieren	4.00	Bewertet
R-0000-6C8A	B007 - Unzureichende Vertragsregelungen	4.66	Reduzieren	2.33	Bewertet
R-0000-4A24	B014 - Ausfall Versorgung (Strom, Wasser, etc.)	4.66	Reduzieren	2.33	Bewertet
R-0000-1309	B023 - Fehlplanung oder fehlende Anpassung	4.00	Reduzieren	2.00	Bewertet

Dokumentenverzeichnis

Titel	Typ	Version	Status	Freigabe
Acceptable Use Policy	Richtlinie / Policy	1.3	Freigegeben	-
Asset-Management-Richtlinie	Richtlinie / Policy	2.2	Freigegeben	-
Awareness-Schulungskonzept	Leitfaden	3.0	Entwurf	-
Bericht Schwachstellen-Scan	Bericht	2.1	Freigegeben	-
Business Continuity Plan	Verfahrensanweisung	1.2	Freigegeben	-
Change-Management-Verfahren	Verfahrensanweisung	1.4	Freigegeben	-
Change-Management-Verfahren	Verfahrensanweisung	3.3	Freigegeben	-
Cloud-Nutzungsrichtlinie	Richtlinie / Policy	2.1	Entwurf	-
Datensicherungs- und Wiederherstellungskonzept	Verfahrensanweisung	2.0	Freigegeben	-
E-Mail- und Internetnutzungsrichtlinie	Richtlinie / Policy	3.2	In Prüfung	-

BEISPIEL BERICHT MIT MUSTERDATEN

TESTZUGANG GmbH

Titel	Typ	Version	Status	Freigabe
Formular Sicherheitsvorfall-Meldung	Formular / Vorlage	1.2	Entwurf	-
Formular Zugriffsbeantragung	Formular / Vorlage	2.3	In Prüfung	-
Home-Office-Sicherheitsrichtlinie	Richtlinie / Policy	2.3	Freigegeben	-
Incident-Response-Verfahren	Verfahrensanweisung	2.0	Freigegeben	-
Informationssicherheitsrichtlinie	Richtlinie / Policy	2.1	Freigegeben	-
Internes Auditprogramm 2026	Aufzeichnung / Nachweis	1.0	Entwurf	-
Kryptografie-Richtlinie	Richtlinie / Policy	1.1	Freigegeben	-
Lieferantensicherheitsrichtlinie	Richtlinie / Policy	1.0	In Prüfung	-
Löschkonzept personenbezogener Daten	Verfahrensanweisung	1.2	Freigegeben	-
Management Review Protokoll Q4/2025	Bericht	1.0	Freigegeben	-
Management-Review-Protokoll	Aufzeichnung / Nachweis	2.0	Freigegeben	-
Mobile Device Policy	Richtlinie / Policy	1.0	In Prüfung	-
Nachweis Backup-Restore-Test	Aufzeichnung / Nachweis	1.1	Freigegeben	-
Netzwerksicherheitskonzept	Verfahrensanweisung	1.3	Freigegeben	-
Notfallhandbuch	Verfahrensanweisung	1.1	In Prüfung	-
Physische Sicherheitsrichtlinie	Richtlinie / Policy	1.0	Freigegeben	-
Physische Sicherheitsrichtlinie	Richtlinie / Policy	1.2	Freigegeben	-
Prüfbericht Internes ISMS-Audit	Bericht	1.3	Freigegeben	-
Prüfbericht Penetrationstest	Bericht	3.0	Freigegeben	-
Richtlinie sichere Softwareentwicklung	Richtlinie / Policy	1.0	In Prüfung	-
Risikoanalyse-Bericht	Bericht	3.1	Freigegeben	-
Risikomanagement-Leitfaden	Leitfaden	1.3	Freigegeben	-
Schulungskonzept Informationssicherheit	Leitfaden	1.1	Freigegeben	-
Statement of Applicability (SoA)	Statement of Applicability	3.0	Freigegeben	-
Verfahrensanweisung Datenträgerentsorgung	Verfahrensanweisung	1.2	Freigegeben	-
Verfahrensanweisung Schlüsselmanagement	Verfahrensanweisung	3.3	Entwurf	-
Vorlage Lieferantenbewertung	Formular / Vorlage	2.2	Freigegeben	-
Zugriffskontrollrichtlinie	Richtlinie / Policy	1.5	Freigegeben	-

BEISPIELBERICHT MIT MUSTERDATEN

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

Maßnahmen

Titel	Status	Priorität	Frist	Wirksamkeit
Klassifizierungsschema für Informationen einführen	Abgeschlossen	Mittel	31.12.2025	4
Überarbeitung Onboarding-/Offboarding-Prozess	Abgeschlossen	Mittel	20.01.2026	4
Phishing-Awareness-Kampagne Q1/2026	Abgeschlossen	Mittel	09.02.2026	4
Datenverlustprävention (DLP) evaluieren	Geplant	Mittel	29.07.2026	-
Home-Office-Sicherheitsrichtlinie kommunizieren	In Umsetzung	Mittel	30.07.2026	-
Sicherheitskonfiguration der Cloud-Tenants härten	Abgeschlossen	Mittel	18.08.2026	4
Lieferanten-Sicherheitsbewertung durchführen	In Umsetzung	Mittel	24.10.2026	-
Notfallübung Cyberangriff simulieren	Geplant	Mittel	18.11.2026	-
Datenschutz-Folgenabschätzung mit ISMS verzahnen	Geplant	Mittel	05.12.2026	-
Sichere Softwareentwicklungsrichtlinie erstellen	Geplant	Mittel	13.12.2026	-
Datenträgervernichtung nach DIN 66399 sicherstellen	In Umsetzung	Mittel	11.01.2027	-
Schutzbedarfsfeststellung der Fachverfahren	Geplant	Mittel	06.02.2027	-
Sicherheits-KPIs im Management-Review berichten	In Umsetzung	Mittel	18.04.2027	-
Clean-Desk-Policy umsetzen	Abgeschlossen	Niedrig	01.12.2025	3
Schlüsselmanagement für Zertifikate aufsetzen	Geplant	Niedrig	26.09.2026	-
Awareness-Schulung für neue Mitarbeitende verpflichtend	In Umsetzung	Niedrig	02.12.2026	-
Privilegierte Konten in PAM-Lösung überführen	Geplant	Niedrig	22.02.2027	-
Penetrationstest für Webanwendungen beauftragen	In Umsetzung	Niedrig	16.03.2027	-
Vulnerability-Scanner implementieren	Abgeschlossen	Hoch	31.12.2025	4
E-Mail-Sicherheit (DMARC/SPF/DKIM) konfigurieren	In Umsetzung	Hoch	29.08.2026	-
Sicherheitsvorfälle revisionssicher dokumentieren	In Umsetzung	Hoch	02.09.2026	-
VPN-Zugang auf Zero-Trust-Architektur umstellen	Geplant	Hoch	23.09.2026	-
Wechseldatenträger-Nutzung technisch beschränken	Geplant	Hoch	26.09.2026	-
Notfallrufkette und Erreichbarkeiten aktualisieren	Geplant	Hoch	09.10.2026	-
Zugriffsrechte-Review aller Systeme	In Umsetzung	Hoch	19.10.2026	-
Patch-Management-Prozess optimieren	In Umsetzung	Hoch	22.11.2026	-
Netzwerksegmentierung Produktions-VLAN	In Umsetzung	Hoch	06.12.2026	-
Backup-Wiederherstellungstest durchführen	Geplant	Hoch	18.12.2026	-

BEISPIELBERICHT MIT MUSTERDATEN

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

Titel	Status	Priorität	Frist	Wirksamkeit
Verschlüsselung ruhender Daten auf Fileservern	In Umsetzung	Hoch	24.12.2026	-
Lieferketten-Risiken (Software Supply Chain) bewerten	Abgeschlossen	Hoch	07.01.2027	2
Mobile-Device-Management (MDM) konfigurieren	Abgeschlossen	Hoch	12.04.2027	5
Endpoint Detection & Response (EDR) ausrollen	Abgeschlossen	Kritisch	15.01.2026	5
MFA für alle Benutzerkonten einführen	Abgeschlossen	Kritisch	30.01.2026	5
SIEM-System einführen	Geplant	Kritisch	29.06.2026	-
Offboarding-Prozess (Entzug Rechte) automatisieren	Geplant	Kritisch	26.09.2026	-
Physische Zutrittskontrolle Serverraum prüfen	Abgeschlossen	Kritisch	03.05.2027	5
Asset-Inventar vervollständigen und pflegen	In Umsetzung	Kritisch	22.06.2027	-

BEISPIELBERICHT MIT MUSTERDATEN

Auditfeststellungen

Audit	Feststellung	Schwere	Status	Ursachenanalyse
Internes ISMS-Audit – Incident	Incident-Klassifizierungsschema zu grob	Beobachtung	Offen	
Internes ISMS-Audit – Complian	Rechtskataster nicht aktuell	Beobachtung	Offen	
Externes Überwachungsaudit ISO	Verbesserungspotenzial bei der Wirksamkeitsmessung	Beobachtung	Behoben	
Internes ISMS-Audit – Lieferan	Kein systematisches Monitoring von Lieferanten-Inc	Beobachtung	Offen	
Management Review Q4/2025	Personalressourcen für ISMS unzureichend	Beobachtung	In Bearbeitung	
Internes ISMS-Audit – Physisch	Fehlende Protokollierung der Besucherregistrierung	Beobachtung	Behoben	
Internes ISMS-Audit Q1/2026	Datenlöschung nicht nachweisbar dokumentiert	Nebenabweichung	In Bearbeitung	
Internes ISMS-Audit Q1/2026	KI-Nutzungsrichtlinie nicht allen MA bekannt	Nebenabweichung	In Bearbeitung	
Internes ISMS-Audit – Incident	Keine Nachbereitung (Lessons Learned) für 2 Vorfäl	Nebenabweichung	Offen	
Internes ISMS-Audit – Datensic	Asset-Register unvollständig für Cloud-Dienste	Nebenabweichung	Behoben	
Internes ISMS-Audit – Datensic	Klassifizierungslabels nicht konsistent angewendet	Nebenabweichung	Behoben	
Internes ISMS-Audit – Netzwerk	Log-Retention für Firewall-Logs zu kurz	Nebenabweichung	Offen	
Externes Überwachungsaudit ISO	Risikobewertungsmethodik nicht vollständig dokumen	Nebenabweichung	Behoben	
Internes ISMS-Audit – Lieferan	Fehlende Sicherheitsklauseln in 4 Altverträgen	Nebenabweichung	Offen	
Management Review Q4/2025	Awareness-Schulungsquote unter Zielwert	Nebenabweichung	Behoben	

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

Audit	Feststellung	Schwere	Status	Ursachenanalyse
Internes ISMS-Audit – Backup &	Backup-Monitoring-Alerts werden nicht ausgewertet	Nebenabweichung	Behoben	
Internes ISMS-Audit – Backup &	Restore-Test für E-Mail-Server nicht dokumentiert	Nebenabweichung	In Bearbeitung	
Internes ISMS-Audit – Zugriffs	Dokumentation der Berechtigungsvergabe unvollständ	Nebenabweichung	Behoben	
Internes ISMS-Audit Q1/2026	DR-Test nur für 3 von 8 kritischen Systemen	Hauptabweichung	Offen	
Internes ISMS-Audit Q1/2026	Patch-SLA für kritische CVEs nicht eingehalten	Hauptabweichung	Offen	
Internes ISMS-Audit Q1/2026	PAM nicht implementiert für Cloud-Admin-Konten	Hauptabweichung	In Bearbeitung	
Internes ISMS-Audit – Endpoint	12 Systeme mit kritischem Patch-Rückstand >30 Tage	Hauptabweichung	In Bearbeitung	
Internes ISMS-Audit – Endpoint	3 Endpoints ohne aktuellen EDR-Agent	Hauptabweichung	Behoben	
Internes ISMS-Audit – Lieferan	Lieferantensicherheitsrichtlinie noch nicht freige	Hauptabweichung	In Bearbeitung	
Internes ISMS-Audit – Physisch	Serverraum-Tür ohne automatische Verriegelung	Hauptabweichung	Behoben	
Internes ISMS-Audit – Zugriffs	Fehlende MFA für VPN-Zugang externer Dienstleister	Hauptabweichung	Behoben	
Internes ISMS-Audit – Zugriffs	Veraltete Service-Accounts im Active Directory	Hauptabweichung	In Bearbeitung	
Internes ISMS-Audit Q1/2026	Unzureichende Segmentierung Dev/Prod	Kritische Abweichung	Offen	

Korrekturmaßnahmen (CAPA)

Titel	Ursachenanalyse	Status	Frist	Wirksamkeit geprüft	Wirksamkeitsprüfung
–	–	–	–	–	–

Sicherheitsziele

Ziel	Termin	Zielwert	Ist	Erreicht
–	–	–	–	–

Managementbewertungen

BEISPIELBERICHT MIT MUSTERDATEN

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

Titel	Datum	Status	Version	Freigegeben am
–	–	–	–	–

Nachweis-Index

Nachweis	Typ	Controls	Nachweisdatum	Gültig bis
–	–	–	–	–

BEISPIELBERICHT MIT MUSTERDATEN