

PRODUKT - WALKTHROUGH · FASSUNG ÖSTERREICH

NIS2-Manager

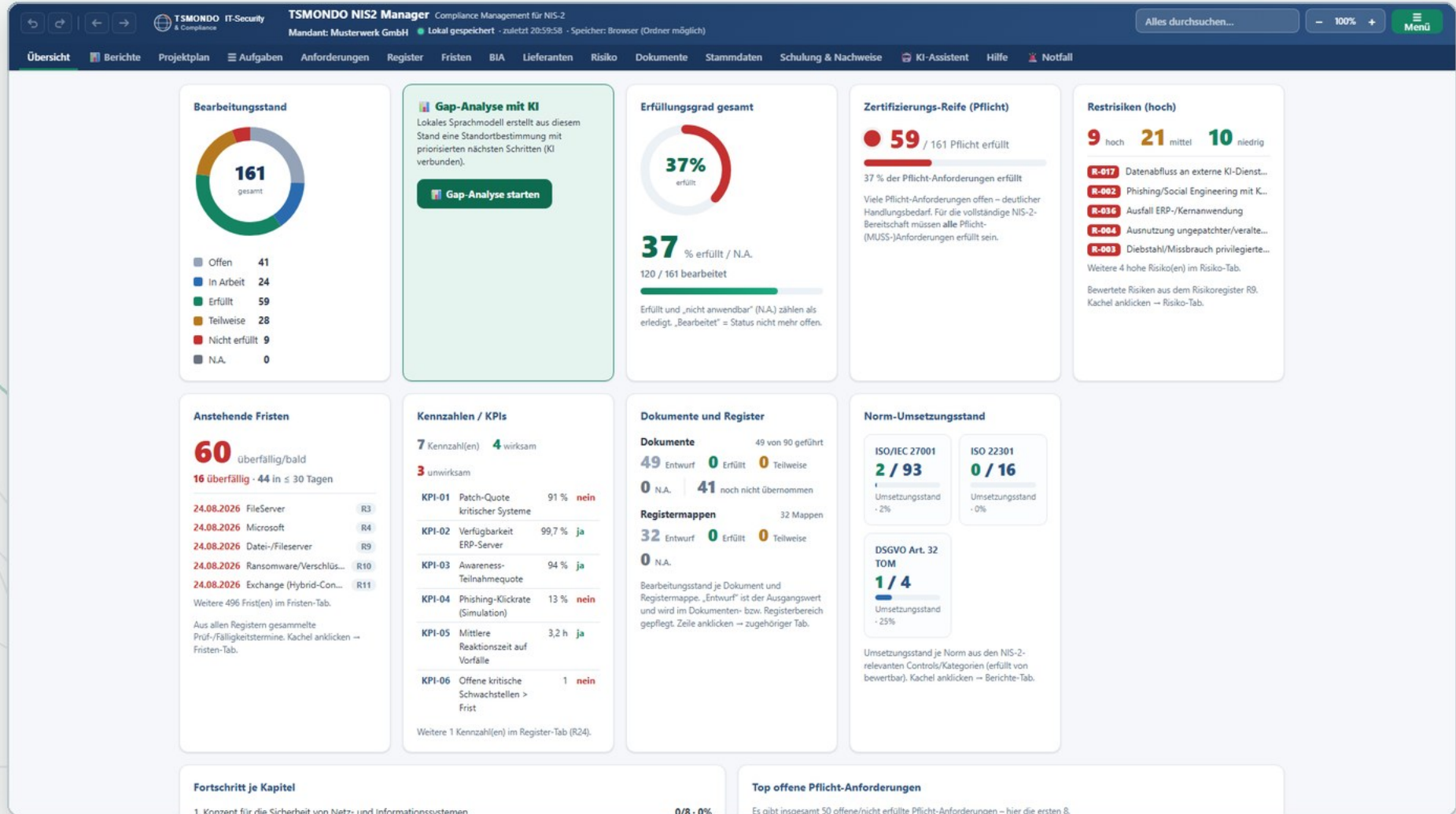
NIS-2 und NISG umsetzen, dokumentieren und nachweisen — in einer Anwendung

TSMONDO · Fassung Österreich

EINSTIEG

Was die Anwendung leistet

- Lokal auf Ihrem Rechner
- 161 Anforderungen, 32 Register
- Über 80 Dokumentvorlagen



STAMMDATEN

Einmal erfassen, überall verwendet

- Organisation und Geltungsbereich

- Füllt Berichte und Vorlagen

- Eigenes Logo möglich

Stammdaten / Kundendaten

Diese Angaben werden im Kopf der App (Mandant) sowie in allen Reports (Compliance-Report & Anwendbarkeitserklärung) verwendet. Speicherung ausschließlich lokal in diesem Browser.

ORGANISATION

ORGANISATION / FIRMA

Musterwerk GmbH

STRASSE & HAUSNUMMER

Industriestraße 12

PLZ

4600

ORT

Wels

LAND

Österreich

BRANCHE (OPTIONAL)

Maschinenbau

MITARBEITERZAHL (OPTIONAL)

240

ANSPRECHPARTNER

ANSPRECHPARTNER

Erika Mustermann

ROLLE / FUNKTION

Geschäftsführung

E-MAIL

info@musterwerk.example

TELEFON

+43 7242 12345-0

INFORMATIONSSICHERHEITSBEAUFTRAGTER
(ISB)

Max Mustermann (ISB)

GELTUNGSBEREICH

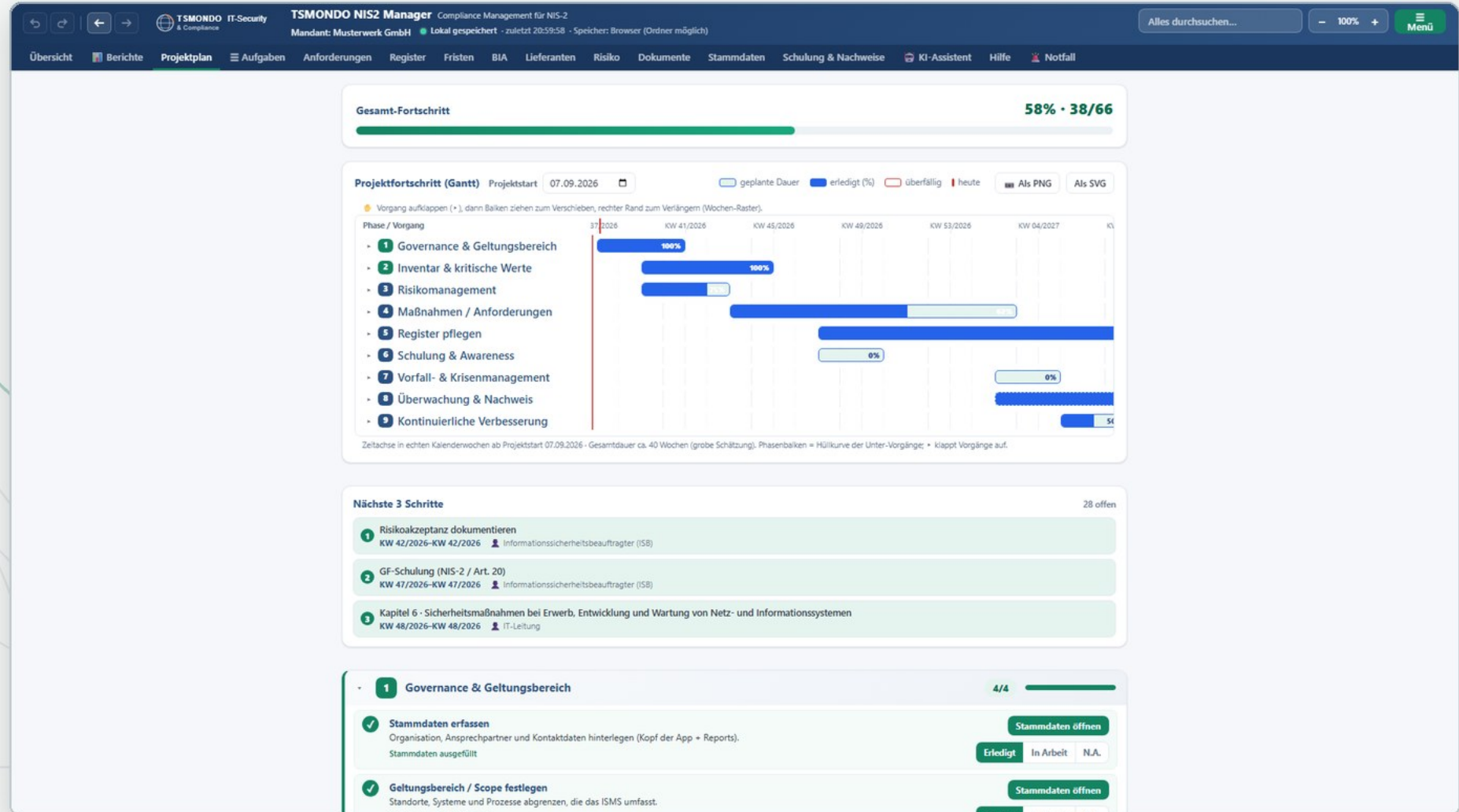
GELTUNGSBEREICH (SCOPE DES ISMS)

Alle Standorte, IT-Betrieb, Produktion und Logistik

PROJEKTPLAN

Der geführte Weg

- 9 Phasen von Anfang bis Nachweis
- Jeder Schritt springt an seinen Ort
- Status wird zurückgemeldet



ÜBERSICHT

Der Stand auf
einen Blick

- Erfüllungsgrad und Reife-Ampel
- Restrisiken und Fristen
- Umsetzungsstand je Norm

Bearbeitungsstand



■ Offen	41
■ In Arbeit	24
■ Erfüllt	59
■ Teilweise	28
■ Nicht erfüllt	9
■ N.A.	0

Gap-Analyse mit KI

Lokales Sprachmodell erstellt aus diesem Stand eine Standortbestimmung mit priorisierten nächsten Schritten (KI verbunden).

Gap-Analyse starten

Erfüllungsgrad gesamt



37 % erfüllt / N.A.

120 / 161 bearbeitet

Erfüllt und „nicht anwendbar“ (N.A.) zählen als erledigt. „Bearbeitet“ = Status nicht mehr offen.

Zertifizierungs-Reife (Pflicht)

59 / 161 Pflicht erfüllt

37 % der Pflicht-Anforderungen erfüllt

Viele Pflicht-Anforderungen offen – deutlicher Handlungsbedarf. Für die vollständige NIS-2-Bereitschaft müssen alle Pflicht-(MUS-)Anforderungen erfüllt sein.

Restrisiken (hoch)

9 hoch 21 mittel 10 niedrig

- R-017 Datenabfluss an externe KI-Dienst...
- R-002 Phishing/Social Engineering mit K...
- R-036 Ausfall ERP-/Kernanwendung
- R-004 Ausnutzung ungepatchter/veralte...
- R-003 Diebstahl/Missbrauch privilegierte...

Weitere 4 hohe Risiko(en) im Risiko-Tab.

Bewertete Risiken aus dem Risikoregister R9. Kachel anklicken → Risiko-Tab.

Anstehende Fristen

60 überfällig/bald
16 überfällig · 44 in ≤ 30 Tagen

24.08.2026	FileServer	R3
24.08.2026	Microsoft	R4
24.08.2026	Datei-/Fileserver	R9
24.08.2026	Ransomware/Verschlüs...	R10
24.08.2026	Exchange (Hybrid-Con...	R11

Weitere 496 Frist(en) im Fristen-Tab.

Aus allen Registern gesammelte Prüf-/Fälligkeitstermine. Kachel anklicken → Fristen-Tab.

Kennzahlen / KPIs

7 Kennzahl(en) 4 wirksam
3 unwirksam

KPI-01	Patch-Quote kritischer Systeme	91 %	nein
KPI-02	Verfügbarkeit ERP-Server	99,7 %	ja
KPI-03	Awareness-Teilnahmequote	94 %	ja
KPI-04	Phishing-Klickrate (Simulation)	13 %	nein
KPI-05	Mittlere Reaktionszeit auf Vorfälle	3,2 h	ja
KPI-06	Offene kritische Schwachstellen > Frist	1	nein

Weitere 1 Kennzahl(en) im Register-Tab (R24).

Dokumente und Register

Dokumente 49 von 90 geführt
49 Entwurf 0 Erfüllt 0 Teilweise
0 N.A. 41 noch nicht übernommen

Registermappen 32 Mappen
32 Entwurf 0 Erfüllt 0 Teilweise
0 N.A.

Bearbeitungsstand je Dokument und Registermappe. „Entwurf“ ist der Ausgangswert und wird im Dokumenten- bzw. Registerbereich gepflegt. Zeile anklicken → zugehöriger Tab.

Norm-Umsetzungsstand

ISO/IEC 27001
2 / 93
Umsetzungsstand · 2%

ISO 22301
0 / 16
Umsetzungsstand · 0%

DSGVO Art. 32 TOM
1 / 4
Umsetzungsstand · 25%

Umsetzungsstand je Norm aus den NIS-2-relevanten Controls/Kategorien (erfüllt von bewertbar). Kachel anklicken → Berichte-Tab.

ANFORDERUNGEN

Bewerten und belegen

- 161 Einzelanforderungen
- Status, Kommentar, Nachweis
- Bezug zu NIS-2 Artikel 21

Anforderungen NIS-2

KAPITEL/GRUPPEN: Alle einklappen Alle ausklappen Status-Vorschlag

▼ 2. Konzept für das Risikomanagement 5 100%

2.1 – Risikomanagementrahmen

IR2024-2690-2.1.1

Für die Zwecke von Artikel 21 Absatz 2 Buchstabe a der Richtlinie (EU) 2022/2555 führen die betreffenden Einrichtungen einen geeigneten Risikomanagementrahmen ein, um die Risiken für die Sicherheit von Netz- und Informationssystemen zu ermitteln und anzugehen, und erhalten diesen Rahmen aufrecht. Die betreffenden Einrichtungen führen Risikobewertungen durch und dokumentieren diese; auf der Grundlage der Ergebnisse erstellen sie einen Risikobehandlungsplan, setzen diesen um und überwachen ihn. Die Ergebnisse der Risikobewertung und die Restrisiken werden von den Leitungsorganen oder – soweit anwendbar – von Personen akzeptiert, die für das Risikomanagement rechenschaftspflichtig und befugt sind, sofern die betreffenden Einrichtungen für eine angemessene Berichterstattung an die Leitungsorgane sorgen.

Pflicht **MÜSSEN** **Art. 21 Abs. 2 Bst. a** **IR (EU) 2024/2690, Punkt 2.1.1**

● Erfüllt Erfüllt ▼ Detail anzeigen

2.1 – Risikomanagementrahmen

IR2024-2690-2.1.3

Bei der Ermittlung und Priorisierung geeigneter Risikomanagementoptionen und -maßnahmen berücksichtigen die betreffenden Einrichtungen die Ergebnisse der Risikobewertung, die Ergebnisse des Verfahrens zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit, die Umsetzungskosten im Verhältnis zum erwarteten Nutzen, die in Nummer 12.1 genannte Klassifizierung von Anlagen und Werten und die in Nummer 4.1.3 genannte Analyse der betrieblichen Auswirkungen.

Pflicht **MÜSSEN** **Art. 21 Abs. 2 Bst. a** **IR (EU) 2024/2690, Punkt 2.1.3**

● Erfüllt Erfüllt ▼ Detail anzeigen

DOKUMENTE

Vorlagen mit Beispiel

- Über 80 Vorlagen, sortiert

- Jede Vorlage nennt ihren Normbezug

- Ausgefülltes Beispiel dabei

Richtlinien 35						
	Richtlinie zur akzeptablen Nutzung von Unternehmenssystemen NIS 2 Art. 21 Abs. 2 lit. g (Cyberhygiene) · EU-Anforderungskatalog · ISO/IEC 27001:2022 A.5.10/A.8.1	erstellt · 08.09.2026 20:59	Vorlage	Beispiel	Bearbeiten	Word PDF
	Richtlinie zur akzeptablen Nutzung von KI-Systemen NIS 2 Art. 21 Abs. 2 lit. g (Cyberhygiene) · EU-KI-Verordnung · EU-Anforderungskatalog · ISO/IEC 27001:2022 A.5.10/A.8.3	erstellt · 08.09.2026 20:59	Vorlage	Beispiel	Bearbeiten	Word PDF
	Richtlinie für Change Management NIS 2 Art. 21 Abs. 2 lit. e (Systementwicklung und -wartung) · EU-Anforderungskatalog · ISO/IEC 27001:2022 A.8.32	erstellt · 08.09.2026 20:59	Vorlage	Beispiel	Bearbeiten	Word PDF
	Richtlinie für Clear Desk Policy NIS 2 Art. 21 Abs. 2 lit. i (Anlagenverwaltung) · EU-Anforderungskatalog · ISO/IEC 27001:2022 A.7.7/A.5.12	erstellt · 08.09.2026 20:59	Vorlage	Beispiel	Bearbeiten	Word PDF
	Richtlinie zur Nutzung von Cloud-Diensten NIS 2 Art. 21 Abs. 2 lit. d/e (Lieferkette/Erwerb von IKT-Diensten) · EU-Anforderungskatalog · ISO/IEC 27001:2022 A.5.23	erstellt · 08.09.2026 20:59	Vorlage	Beispiel	Bearbeiten	Word PDF
	Richtlinie zur Datensicherung NIS 2 Art. 21 Abs. 2 lit. c (Backup- und Krisenmanagement) · EU-Anforderungskatalog · ISO/IEC 27001:2022 A.8.13	erstellt · 08.09.2026 20:59	Vorlage	Beispiel	Bearbeiten	Word PDF
	Richtlinie zur Informationsklassifizierung und -schutz NIS 2 Art. 21 Abs. 2 lit. i (Anlagenverwaltung) · EU-Anforderungskatalog · ISO/IEC 27001:2022 A.5.12/A.5.13	erstellt · 08.09.2026 20:59	Vorlage	Beispiel	Bearbeiten	Word PDF
	Richtlinie zur Protokollierung und Überwachung NIS 2 Art. 21 Abs. 2 lit. b/g (Vorfallserkennung/Cyberhygiene) · EU-Anforderungskatalog · ISO/IEC 27001:2022 A.8.15/A.8.16	erstellt · 08.09.2026 20:59	Vorlage	Beispiel	Bearbeiten	Word PDF
	Richtlinie zur Netzwerksicherheit NIS 2 Art. 21 Abs. 2 lit. a (Sicherheitskonzepte für Netze) · EU-Anforderungskatalog · ISO/IEC 27001:2022 A.8.20/A.8.21/A.8.22	erstellt · 08.09.2026 20:59	Vorlage	Beispiel	Bearbeiten	Word PDF
	Richtlinie zur Personalsicherheit					

EDITOR

Aus der Vorlage wird Ihr Dokument

- In System übernehmen

- Platzhalter aus den Stammdaten

- Export als Word oder PDF

Informationssicherheitsleitlinie · Bearbeiten Mit Stammdaten ausfüllen Mit KI vervollständigen Word (.doc) PDF ×

H2 H3 1 F K U • Liste 1. Liste Link Tabelle ↶ ↷ Speichern

Informationssicherheitsleitlinie der Musterwerk GmbH

TSMONDO IT-Security & Compliance · Dokumentvorlage zum EU-Anforderungskatalog · Leervorlage zum Ausfüllen

Feld	Angabe
Titel	Informationssicherheitsleitlinie der Musterwerk GmbH
Version	1.0
Freigabe durch	Geschäftsleitung der Musterwerk GmbH
Datum	08.09.2026
Klassifizierung	Intern – nur für den internen Gebrauch

Änderungshistorie

Version	Datum	Änderung	Bearbeiter
1.0	08.09.2026	Erstfassung, in Kraft gesetzt durch die Geschäftsleitung	Erika Mustermann, Informationssicherheitsbeauftragte/r (ISB)

Diese Leitlinie ist für alle Beschäftigten verbindlich. Bitte lesen Sie sie aufmerksam. Wenn Sie etwas nicht verstehen oder unsicher sind, fragen Sie Ihre Führungskraft oder die/den Informationssicherheitsbeauftragte/n (ISB).

1. Worum es geht

Die Musterwerk GmbH [kurze Beschreibung des Kerngeschäfts]. Fast alle unsere Abläufe hängen heute von funktionierender IT ab. Unsere Daten, unser technisches Know-how und die Daten unserer Kundinnen und Kunden sind wertvoll und müssen geschützt werden.

Diese Leitlinie beschreibt, wie wir gemeinsam für Informationssicherheit sorgen – verständlich und verbindlich für alle. Informationssicherheit bedeutet, dass unsere Informationen vertraulich bleiben, richtig und vollständig sind und dann verfügbar sind, wenn wir sie brauchen.

2. Für wen gilt diese Leitlinie?

Diese Leitlinie gilt für alle, die mit IT-Systemen oder Daten der Musterwerk GmbH arbeiten. Dazu gehören:

- Mitarbeiterinnen und Mitarbeiter,
- Auftragnehmer und Berater,
- Zeitarbeitskräfte,
- Praktikantinnen und Praktikanten.

Jede dieser Personen ist mitverantwortlich dafür, dass unsere Informationen sicher bleiben.

REGISTER

Die Nachweisführung

2 Verzeichnis der Verantwortlichkeiten / Rollenmatrix	3 IT-System-Inventar	4 Software-/Lizenzverzeichnis	5 Prozessverzeichnis (zentrale Prozesse & Prozesse mit hohem Schadenpotenzial)	6 Verzeichnis wichtiger und kritischer IT-Ressourcen	7 Verzeichnis kritischer Informationen
11 Schwachstellenregister	12 Maßnahmenregister (Maßnahmen-/Aktionsplan)	13 Berechtigungs-/Identitätsverzeichnis (Zugänge, Zugriffs- & Zutrittsrechte)	14 Verzeichnis administrativer Zugänge	15 Wechseldatenträger-Verzeichnis	16 Verzeichnis mobiler IT-Systeme
17 Schulungs- und Awareness-Nachweise	18 Nachweis Geschäftsleitungsschulung (NIS-2 / Art. 20 NIS-2-Richtlinie, § 31 NISG 2026)	19 Vorfallsregister / Logbuch der Sicherheitsvorfälle	20 Behördenmeldungen-Register (erhebliche Sicherheitsvorfälle)	21 Krypto-/Schlüsselverzeichnis	22 Protokollierungsquellen-Verzeichnis
23 Kontakt-/Erreichbarkeits- und Adresslisten (intern/extern, Notfall)	24 Kennzahlen-/KPI-Register	25 Test- und Übungsnachweise (Krisen-/Verfahrenstests)	26 Datensicherungs- und Restore-Test-Nachweise	28 Verzeichnis administrativer Tätigkeiten (wichtige IT-Systeme)	29 Abhängigkeitsverzeichnis & Wiederherstellungsreihenfolge
30 Ausnahmeregister (genehmigte Abweichungen)	31 Verzeichnis der Erkennungsmaßnahmen (Detection-Nachweis)	32 Netzübergangs-/Konfigurationsverzeichnis (jährliche Prüfung)			

- 32 Register, direkt bearbeitbar
- Inventar, Prozesse, Vorfälle
- Import und Export als CSV

RISIKO

Bewerten und behandeln

- Risikoregister und Matrix
- Wahrscheinlichkeit mal Auswirkung
- Maßnahmen mit Verantwortlichen

Risiken – Initialrisiko (R9)

9 HOCH	21 MITTEL	10 NIEDRIG
------------------	---------------------	----------------------

Auswirkung ↓ / Eintritt →		Eintrittswahrscheinlichkeit		
		niedrig	mittel	hoch
Auswirkung / Schadenshöhe	hoch	9 HOCH	7 HOCH	2 HOCH
	mittel	10 MITTEL	12 MITTEL	0 HOCH
	niedrig	0 NIEDRIG	0 MITTEL	0 HOCH

Methodik: 3×3-Matrix, Risikowert = Eintrittswahrscheinlichkeit × Auswirkung. Bänder: 1–2 niedrig, 3–4 mittel, 6–9 hoch. Quelle: Register R9 (live). Details siehe Vorlage „Verfahren zum Risikomanagement“.

Restrisiken (nach Maßnahmen, R9)

1 HOCH	15 MITTEL	24 NIEDRIG
------------------	---------------------	----------------------

Restrisiko ↓ / Eintritt →		Eintrittswahrscheinlichkeit		
		niedrig	mittel	hoch
Restrisiko-Stufe	hoch	0 HOCH	0 HOCH	0 HOCH
	mittel	14 MITTEL	14 MITTEL	1 HOCH
	niedrig	5 NIEDRIG	5 MITTEL	1 HOCH

Restrisiko-Matrix: Eintrittswahrscheinlichkeit (unverändert) × erfasste Restrisiko-Stufe (nach Maßnahmen) als Auswirkungs-Achse. Quelle: Register R9, Spalte „Restrisiko“ (live).

Was zuerst wieder laufen muss

- Prozesse aus dem Verzeichnis
- Ausfallzeit und Datenverlust
- Wiederanlauf-Reihenfolge

▼ Abgeleitete Wiederanlauf-Reihenfolge (zentral zuerst, dann nach RTO bzw. MTA aufsteigend)

1	zentral	PRZ-01	Auftragsabwicklung	RTO/MTA: 4 h
2	zentral	PRZ-02	Produktion/Fertigungssteuerung	RTO/MTA: 8 h
3	zentral	PRZ-05	E-Mail-Kommunikation	RTO/MTA: 8 h
4	zentral	PRZ-07	Versand/Logistik	RTO/MTA: 8 h
5		PRZ-03	Rechnungsstellung/Faktura	RTO/MTA: 24 h
6		PRZ-06	Einkauf/Beschaffung	RTO/MTA: 48 h
7		PRZ-04	Lohn- und Gehaltsabrechnung	RTO/MTA: 72 h

PROZESS	EINSTUFUNG	MTA	RTO	RPO	SCHADEN (F / R / REP / B)	BENÖTIGTE RESSOURCEN / SYSTEME	RANG	VERANTWORTLICH	NÄCHSTE PRÜFUNG
PRZ-01 Auftragsabwicklung	zentral	4 h	4 h	1 h	F hoch Rep hoch	R mittel B hoch SRV-001 – FileServer SRV-002 – ERP-Server (Muster-E... + Ressource verknüpfen ... aus R5 (Prozesse) übernehmen	1	Vertriebsleitung	30.06.2027
PRZ-02 Produktion/Fertigungssteuerung	zentral	8 h	8 h	1 h	F hoch Rep hoch	R mittel B hoch SRV-002 – ERP-Server (Muster-E... SRV-003 – Domaincontroller (AD) + Ressource verknüpfen ... aus R5 (Prozesse) übernehmen	2	Produktionsleitung	30.06.2027

NOTFALL

Vorbereitet für den Ernstfall

B · NIS2 / NISG – MELDUNG AN DIE ZUSTÄNDIGE BEHÖRDE (CYBERSICHERHEITSBEHÖRDE) **erheblicher Sicherheitsvorfall**

FRÜHWARNUNG

24 Stunden

Erste Kurzmeldung ab Kenntnis

MELDUNG (FOLGEMELDUNG)

72 Stunden

Bewertung: Schwere, Auswirkungen, ggf. IoCs

ABSCHLUSSMELDUNG

1 Monat

Nach der 72-h-Meldung (oder früher bei Abschluss)

- **Frühwarnung: binnen 24 Stunden** ab Kenntnis – erste Kurzmeldung.
- **Meldung (Folgemeldung): binnen 72 Stunden** – mit Bewertung von Schwere und Auswirkungen sowie ggf. Kompromittierungsindikatoren (IoCs).
- **Zwischenmeldung:** auf Anforderung der zuständigen Behörde (Cybersicherheitsbehörde).
- **Abschlussmeldung: binnen 1 Monat** nach der 72-h-Meldung (oder früher, wenn der Vorfall abgeschlossen ist). Bei länger andauerndem Vorfall: Fortschrittsmeldung.

Meldeweg: Meldewege der Cybersicherheitsbehörde ([nis.gv.at](https://www.nis.gv.at)) — sektoral getrennt: nis.cert.at (allgemein), nis.govcert.gv.at (öffentliche Verwaltung), nis.energy-cert.at (Energiesektor) – „Sicherheitsvorfall melden“

NIS-Meldeportale (sektoral, Einstieg über [nis.gv.at](https://www.nis.gv.at)) öffnen <https://www.nis.gv.at> [kopieren](#)

Informationen zur NIS-2-Meldepflicht:

Cybersicherheitsbehörde – Informationen zur Meldepflicht <https://www.nis.gv.at> [kopieren](#)

Gilt ab dem 01.10.2026 nach dem NISG 2026 für betroffene Einrichtungen (besonders wichtige / wichtige Einrichtungen).

- Sofortmaßnahmen und Kontakte

- 24 Stunden, 72 Stunden, ein Monat

- Meldeassistent für die Meldestelle

FRISTEN

Termine im Blick

16

überfällig

44

fällig in ≤ 30 Tagen

501

Fristen gesamt

REGISTER	EINTRAG	BEZEICHNUNG	FRIST-ART	DATUM	STATUS	AKTION
filtern...	filtern...	filtern...	filtern...	filtern...	filtern...	Filter zurücksetzen
R3 IT-System-Inventar	SRV-001	FileServer	Letzte Prüfung	24.08.2026	überfällig	✓ Geprüft In Kalender
R4 Software-/Lizenzverzeichnis	Windows Server 2022	Microsoft	Letzte Prüfung	24.08.2026	überfällig	✓ Geprüft In Kalender
R9 Risikoregister (Risikoidentifikation & -analyse)	R-001	Datei-/Fileserver	Letzte Prüfung	24.08.2026	überfällig	✓ Geprüft In Kalender
R10 Risikobehandlungsplan	R-001	Ransomware/Verschlüsselungstrojaner – Datei-/Fileserver	Letzte Prüfung	24.08.2026	überfällig	✓ Geprüft In Kalender
R11 Schwachstellenregister	SW-001	Exchange (Hybrid-Connector)	Letzte Prüfung	24.08.2026	überfällig	✓ Geprüft In Kalender
R12 Maßnahmenregister (Maßnahmen-/Aktionsplan)	M-001	Risiko (R-002)	Letzte Prüfung	24.08.2026	überfällig	✓ Geprüft In Kalender
R15 Wechseldatenträger-Verzeichnis	WDT-001	USB-Stick 64 GB (BitLocker)	Letzte Prüfung	24.08.2026	überfällig	✓ Geprüft In Kalender
R16 Verzeichnis mobiler IT-Systeme	MOB-001	Notebook (Lenovo T14)	Letzte Prüfung	24.08.2026	überfällig	✓ Geprüft In Kalender
R24 Kennzahlen-/KPI-Register	KPI-01	Patch-Quote kritischer Systeme	Letzte Prüfung	24.08.2026	überfällig	✓ Geprüft In Kalender

- Termine aus allen Registern
- Überfällig und fällig in 30 Tagen
- Export in den Kalender

LIEFERANTEN

Die Lieferkette prüfen

NAME / KATEGORIE	KRITIKALITÄT	LETZTES ASSESSMENT	SCORE	AMPEL	AKTIONEN
Muster Cloud Services GmbH Account-Team (Partner) kein Datenzugriff	hoch	15.06.2026	98	● Grün	NIS-2-Selbstbewertung Fragebogen-Versand Audit-PDF
MusterIT GmbH Systeme GmbH E. Beispiel kein Datenzugriff	hoch	15.06.2026	71	● Gelb	NIS-2-Selbstbewertung Fragebogen-Versand Audit-PDF
Muster Telekom Austria GmbH Geschäftskundenservice kein Datenzugriff	hoch	15.06.2026	88	● Grün	NIS-2-Selbstbewertung Fragebogen-Versand Audit-PDF
Muster Hosting AG Solutions Architect kein Datenzugriff	mittel	15.06.2026	62	● Gelb	NIS-2-Selbstbewertung Fragebogen-Versand Audit-PDF
Muster-ERP GmbH Support-Team kein Datenzugriff	hoch	15.06.2026	87	● Grün	NIS-2-Selbstbewertung Fragebogen-Versand Audit-PDF
Muster Security Reseller GmbH Vertriebspartner kein Datenzugriff	hoch	15.06.2026	49	● Rot	NIS-2-Selbstbewertung Fragebogen-Versand Audit-PDF
Lokaler IT-Dienstleister Musterstadt F. Muster kein Datenzugriff	niedrig	15.06.2026	52	● Rot	NIS-2-Selbstbewertung Fragebogen-Versand Audit-PDF

- Eigene Pflicht aus NIS-2
- Fragebogen mit Gewichtung
- Punktwert je Lieferant

LIEFERANTEN

Der Fragebogen für den Lieferanten

- Ausfüllbares PDF

- Auftraggeber und Lieferant im Kopf

- 37 Fragen, zehn Bereiche

NIS-2 Lieferanten-Selbstauskunft

Informationssicherheit in der Lieferkette (Art. 21 Abs. 2 a–j NIS-2)

Auftraggeber: Musterwerk GmbH
Industriestraße 12
4600 Wels
Österreich

Kontakt: Erika Mustermann (Geschäftsführung)
info@musterwerk.example
Tel.: +43 7242 12345-0

Lieferant: Muster Hosting AG

Ansprechpartner: Solutions Architect

Datum: 08.09.2026

Dieser Fragebogen erfasst die Informationssicherheit Ihres Unternehmens als Lieferant/Dienstleister entlang der zehn Maßnahmenbereiche der NIS-2-Richtlinie (Art. 21 Abs. 2 a–j).

So gehen Sie vor:

1. Füllen Sie die Formularfelder direkt in diesem PDF aus (Ja/Nein-Auswahl, Auswahllisten, Freitext).
2. SPEICHERN Sie die Datei anschließend (Datei > Speichern) — bitte nicht nur drucken.
3. Senden Sie das gespeicherte PDF an Ihren Auftraggeber zurück.

Hinweis: Felder, die auf Ihr Unternehmen nicht zutreffen, wählen Sie bitte als „nicht zutreffend“ — sie werden dann aus der Bewertung herausgenommen.

Risikomanagement & ISMS

Verfügt Ihr Unternehmen über ein dokumentiertes Informationssicherheits-Managementsystem (ISMS), z. B. nach ISO/IEC 27001 oder einem gleichwertigen anerkannten Rahmenwerk?

Gemeint ist ein gelebtes, dokumentiertes Managementsystem (Leitlinie, Rollen, Steuerung) — eine Zertifizierung ist nicht zwingend, aber von Vorteil.
NIS-2 Art.21(2)(a)

☒ Ja ☐ Nein ☐ Nicht zutreffend

Anmerkung (optional):

Führen Sie regelmäßig (mindestens jährlich) eine strukturierte Risikoanalyse für Ihre Informationswerte durch?

Risiken werden identifiziert, bewertet (Eintritt/Schaden) und behandelt; Ergebnisse sind nachvollziehbar dokumentiert.
NIS-2 Art.21(2)(a)

☐ Ja ☒ Nein ☐ Nicht zutreffend

Anmerkung (optional):

Existiert eine von der Leitung verabschiedete Informationssicherheits-Leitlinie?

Eine durch die Geschäftsführung freigegebene, kommunizierte Sicherheitsleitlinie als Rahmen aller Maßnahmen.
NIS-2 Art.21(2)(a)

☐ Ja ☒ Nein ☐ Nicht zutreffend

Anmerkung (optional):

LIEFERANTEN

Die Antwort kommt zurück

- Antwort-PDF importieren
- Punktwert und Ampel
- Erfüllung je Maßnahmenbereich

75
von 100 Punkten

● Ampel: Gelb
Stand: 08.09.2026

Audit-PDF exportieren

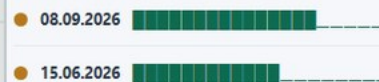
Bewertung je Maßnahmenbereich

MASSNAHMENBEREICH (NIS-2)	ERFÜLLUNG	FORTSCHRITT
Risikomanagement & ISMS	42%	
Vorfallsbehandlung & Meldung	79%	
Business Continuity & Backup	94%	
Lieferketten-Sicherheit	94%	
Beschaffung, Entwicklung & Schwachstellen	77%	
Wirksamkeitsbewertung	93%	
Cyber-Hygiene & Schulung	60%	
Kryptografie & Verschlüsselung	100%	
Personal, Zugriff & Assets	54%	
MFA & gesicherte Kommunikation	67%	

Kritische Befunde (3)

FRAGE	ANTWORT	NIS-2 / NISG
Verfügt Ihr Unternehmen über ein dokumentiertes Informationssicherheits-Managementsystem (ISMS), z. B. nach ISO/IEC 27001 oder einem gleichwertigen anerkannten Rahmenwerk?	Nein	Art.21(2)(a)
Führen Sie regelmäßige Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit für alle Mitarbeitenden durch?	Nein	Art.21(2)(g)
Setzen Sie Multi-Faktor-Authentifizierung (MFA) für administrative und privilegierte Zugänge ein?	Nein	Art.21(2)(j)

Verlauf (2 Assessments)



75 / 100 · Gelb PDF

62 / 100 · Gelb PDF

AUFGABEN

Wer macht was bis wann

- Vorgänge aus dem Projektplan
- Kanban-Tafel und Balkenplan
- Ausgabe je Verantwortlichem

Aufgaben nach Zuständigen 66 Aufgaben · 38 erledigt · 28 offen

Ansicht: **Nach Person** Kanban Auslastung Bearbeiter: Alle Bearbeiter

• Geschäftsführung / Topmanagement 6 Aufgaben · 5 erledigt · nächster Termin KW 06/2027 [CSV](#) [ICS](#) [Mail](#) [PDF](#)

Phase 1

Stammdaten erfassen

1 KW 37/2026–KW 37/2026

Phase 1

Geltungsbereich / Scope festlegen

1 KW 38/2026–KW 38/2026

Phase 1

Rollen & Verantwortlichkeiten (ISB benennen)

1 KW 39/2026–KW 39/2026

Phase 1

Geltung NIS-2 prüfen

1 KW 40/2026–KW 40/2026

Phase 9

Management-Review

1 KW 05/2027–KW 06/2027

Phase 9

Regelmäßige Wiederholung

1 KW 07/2027–KW 07/2027

• Informationssicherheitsbeauftragter (ISB) 11 Aufgaben · 4 erledigt · nächster Termin KW 42/2026 [CSV](#) [ICS](#) [Mail](#) [PDF](#)

Phase 3

Risiken erfassen (R9)

1 KW 39/2026–KW 39/2026

SCHULUNG

Die Leitung in der Pflicht

- Schulungsreihe mit 12 Modulen
- Checkpunkte für die Leitung
- Nachweise in den Registern

01 Geltungsbereich Betroffenheit feststellen: Registrierung nach Art. 27 NIS-2-Richtlinie (§ 29 NISG 2026), Anwendbarkeits-Begründung und Verankerung der Art.-21-Maßnahmen.

4/4 erledigt

- ✓ Nachweis der Registrierung nach Art. 27 NIS-2-Richtlinie (§ 29 NISG 2026) als betroffene Einrichtung inkl. hinterlegter Kontaktstellen und Sektor-/NACE-Zuordnung
Von wem: IT-Leitung gemeinsam mit ISB · Wie oft: einmalig (Registrierung), danach jährliche Aktualisierung
- ✓ Schriftliche Begründung der Anwendbarkeit (Schwellenwerte: Mitarbeiterzahl, Umsatz, Bilanzsumme, NACE-Zuordnung) als audit-fester Aktenvermerk
Von wem: ISB · Wie oft: jährlich und anlassbezogen bei Strukturänderungen
→ Anwendbarkeitserklärung (SoA)
- ✓ Bestätigung, dass alle zehn Maßnahmen aus Art. 21 Abs. 2 und die Meldepflichten nach Art. 23 verbindlich im Maßnahmenplan verankert sind
Von wem: ISB · Wie oft: einmalig (Initial-Setup), danach jährliches Review
→ Anforderungen
- ✓ Formale Billigung der NIS-2-Maßnahmen durch die Geschäftsführung (schriftlicher Genehmigungs-Beschluss; nicht delegierbar)
Von wem: Geschäftsführung selbst · Wie oft: einmalig bei Inkrafttreten, danach jährlich bestätigen
→ GF-Billigungs-Beschluss

02 Haftung & Reporting Nicht-delegierbare GF-Pflichten, regelmäßiges Reporting, Ansprechpartner für die Cybersicherheitsbehörde und 24h-Meldevorlage.

6/6 erledigt

03 Zehn Pflichten (Art. 21) Status-Ampel je Pflicht a-j, SCRM-Owner benennen, rote Pflichten priorisieren.

5/5 erledigt

BERICHTE

Der Nachweis auf Papier

- 10 Berichte, ein Klick

- Compliance-Report und
Anwendbarkeitserklärung

- Bericht für die Geschäftsführung

Berichte

Zentrale Sammelstelle aller Berichte. „Anzeigen“ öffnet den Bericht im Fenster (referenzierte Nachweise sind anklickbar und springen ins Tool); dort lässt er sich per „Als PDF drucken“ im TSMONDO-Layout ausgeben. Die Stammdaten erscheinen automatisch im Kopf.

- Projekt-Fortschrittsbericht (ISMS-Aufbau)**
Gesamt-Projektfortschritt und Phasen-Status (erledigt/laufend/offen) des ISMS-Aufbaus als Gantt-Graphik plus Phasen-Tabelle (Dauer, Start/Ende, Fortschritt %, offene Schritte) und Handlungsempfehlungen.
Anzeigen
- Compliance-Report (NIS 2)**
Umsetzungsstand aller Anforderungen mit Kennzahlen, Status-Verteilung je Verbindlichkeit, Tier und Kapitel — inkl. NIS-2-Bezug.
Anzeigen
- Geschäftsführungs-/Management-Report**
Verdichtete Steuerungssicht für die Leitung: Erfüllungsgrad, Restrisiken, Fristen, Lieferanten-Ampel, offene Maßnahmen, Vorfälle, Handlungsempfehlungen.
Anzeigen
- Anwendbarkeitserklärung (SoA)**
Statement of Applicability: Anwendbarkeit, Umsetzungsstatus und Begründung je Anforderung, gruppiert nach Kapitel.
Anzeigen
- Notfallplan / Erste-Hilfe-Bericht**
Sofortmaßnahmen, gesetzliche Meldefristen (NIS2/NISG 2026 & DSGVO), Behörden- und eigene Notfallkontakte, Wiederanlauf-Reihenfolge.
Anzeigen
- Dokumentations-Nachweis je Pflicht (NIS-2-sortiert)**
Alle Anforderungen aufsteigend nach NIS-2-/NISG-Bezug: Status und ob ein Nachweis vorliegt. Leitprinzip „nicht dokumentiert“ = nicht vorhanden; fehlende Nachweise rot markiert.
Anzeigen
- ISO/IEC-27001-Konformitätsreport**
Kuratierte Zuordnung NIS-2 Art. 21 (a-j) → ISO/IEC 27001:2022 (Annex A): abgeleiteter Erfüllungsstatus je Bereich, Abdeckungs-Kennzahl und Lückenliste. Fachlich zu prüfende Zuordnung.
Anzeigen
- ISO-22301-Konformitätsreport (BCM)**
Kuratierte Zuordnung NIS-2 Art. 21 (a-j) → ISO 22301:2019 (Business Continuity, Schwerpunkt Klausel 8) mit abgeleitetem Status und Lückenliste. Fachlich zu prüfende Zuordnung.
Anzeigen
- DSGVO Art. 32 - TOM-Konformitätsreport**
TOM-Kategorien nach Art. 32 Abs. 1 DSGVO (Pseudonymisierung/Verschlüsselung, Vertraulichkeit/Integrität/Verfügbarkeit/Belastbarkeit, Wiederherstellbarkeit, regelmäßige Überprüfung) → Art. 21, Status und verknüpfte Nachweise.
Anzeigen
- Managementbewertung (kombinierte Jahresbewertung)**

KI - ASSISTENT

Entwurfshilfe, kein Ersatz

- Lokales Modell oder EU-Anbieter
- Standortbestimmung aus Ihrem Stand
- Jeder Text bleibt ein Entwurf

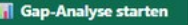
 **KI-Assistent** (lokal, Entwurfshilfe)

Entwirft Texte (Richtlinien, Maßnahmen, Risiken, Anschreiben, Reports) mit einem **lokalen** Sprachmodell (Ollama) und nutzt dabei den aktuellen Stand dieser Anwendung als Kontext (RAG-lite). Alle Verarbeitung erfolgt auf diesem Gerät.

 KI-Entwurf — fachlich/juristisch prüfen. Keine Rechtsberatung.

 **Gap-Analyse — Wo stehe ich?**

Erzeugt aus dem aktuellen Stand (Erfüllungsgrad, Restrisiken, offene Maßnahmen, Fristen, Lieferanten, BIA, Vorfälle, fehlende Pflichtdokumente) eine geschäftsführungstaugliche Standortbestimmung mit priorisierten nächsten Schritten.

 Gap-Analyse starten

 **Einstellungen** (lokales Modell)

● Verbunden · 6 Modell(e)

VERARBEITUNG

☒ Lokal (Ollama)

☐ Mistral (EU-Cloud, DSGVO)

BASIS-URL (OLLAMA)

http://localhost:11434

MODELL

tsmondo-nis2

EMBEDDING-MODELL

bge-m3

Modelle laden

Verbindung testen

Chat

DOKUMENTE & RICHTLINIEN

Richtlinie entwerfen

Verfahrensweisung

Maßnahme beschreiben

RISIKO & BIA

Risiko beschreiben & bewerten

Nächste Schritte aus offenen Risiken (R10)

BIA-Auswertung kommentieren

KOMMUNIKATION & BERICHTE

Lieferanten-Anschreiben

GF-Report-Text

Schulungs-/Awareness-Text

Notfall-/Incident-Kommunikation

ANFORDERUNGEN VERSTEHEN

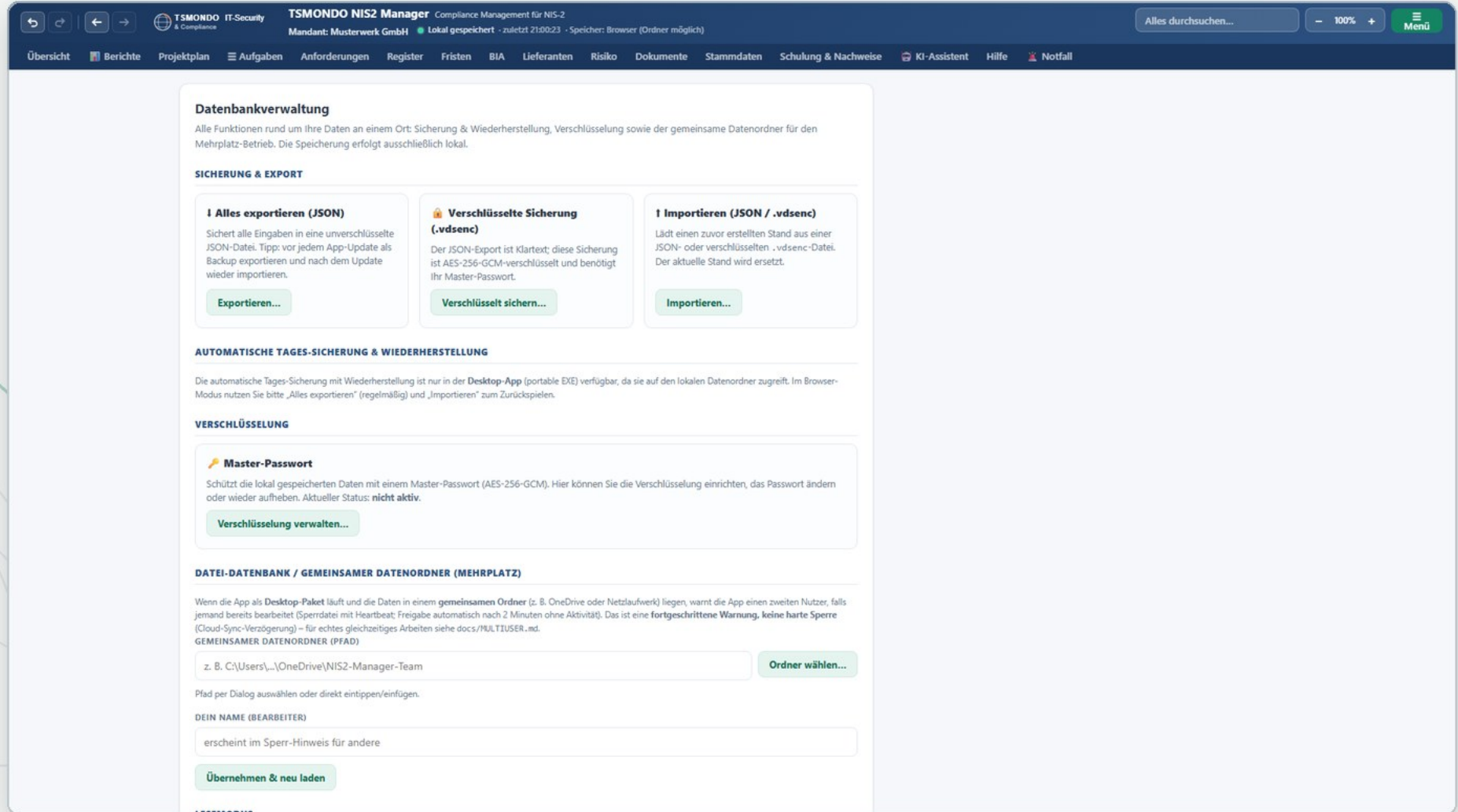
Anforderung erklären & umsetzen

Stellen Sie eine Frage oder nutzen Sie eine Schnellaktion. Die Antwort ist ein Entwurf und muss fachlich geprüft werden.

ABSCHLUSS

Ihre Daten, Ihr Nachweis

- Ihre Daten bleiben lokal
- Verschlüsselte Sicherung
- Änderungsprotokoll inbegriffen



TSMONDO NIS2 Manager Compliance Management für NIS-2
Mandant: Musterwerk GmbH • Lokal gespeichert • zuletzt 21.09.23 • Speicher: Browser (Ordner möglich)

Übersicht Berichte Projektplan Aufgaben Anforderungen Register Fristen BIA Lieferanten Risiko Dokumente Stammdaten Schulung & Nachweise KI-Assistent Hilfe Notfall

Datenbankverwaltung

Alle Funktionen rund um Ihre Daten an einem Ort: Sicherung & Wiederherstellung, Verschlüsselung sowie der gemeinsame Datenordner für den Mehrplatz-Betrieb. Die Speicherung erfolgt ausschließlich lokal.

SICHERUNG & EXPORT

1 Alles exportieren (JSON)
Sichert alle Eingaben in eine unverschlüsselte JSON-Datei. Tipp: vor jedem App-Update als Backup exportieren und nach dem Update wieder importieren.
[Exportieren...](#)

Verschlüsselte Sicherung (.vdsenc)
Der JSON-Export ist Klartext; diese Sicherung ist AES-256-GCM-verschlüsselt und benötigt Ihr Master-Passwort.
[Verschlüsselt sichern...](#)

1 Importieren (JSON / .vdsenc)
Lädt einen zuvor erstellten Stand aus einer JSON- oder verschlüsselten .vdsenc-Datei. Der aktuelle Stand wird ersetzt.
[Importieren...](#)

AUTOMATISCHE TAGES-SICHERUNG & WIEDERHERSTELLUNG

Die automatische Tages-Sicherung mit Wiederherstellung ist nur in der Desktop-App (portable EXE) verfügbar, da sie auf den lokalen Datenordner zugreift. Im Browser-Modus nutzen Sie bitte „Alles exportieren“ (regelmäßig) und „Importieren“ zum Zurückspielen.

VERSCHLÜSSELUNG

Master-Passwort
Schützt die lokal gespeicherten Daten mit einem Master-Passwort (AES-256-GCM). Hier können Sie die Verschlüsselung einrichten, das Passwort ändern oder wieder aufheben. Aktueller Status: **nicht aktiv**.
[Verschlüsselung verwalten...](#)

DATEI-DATENBANK / GEMEINSAMER DATENORDNER (MEHRPLATZ)

Wenn die App als Desktop-Paket läuft und die Daten in einem **gemeinsamen Ordner** (z. B. OneDrive oder Netzlaufwerk) liegen, warnt die App einen zweiten Nutzer, falls jemand bereits bearbeitet (Sperrdatei mit Heartbeat; Freigabe automatisch nach 2 Minuten ohne Aktivität). Das ist eine **fortgeschrittene Warnung, keine harte Sperre** (Cloud-Sync-Verzögerung) – für echtes gleichzeitiges Arbeiten siehe docs/MULTIUSER.md.

GEMEINSAMER DATENORDNER (PFAD)

z. B. C:\Users\...\OneDrive\NIS2-Manager-Team [Ordner wählen...](#)

Platz per Dialog auswählen oder direkt eintippen/einfügen.

DEIN NAME (BEARBEITER)

erscheint im Sperr-Hinweis für andere

[Übernehmen & neu laden](#)

LESEMODUS



Vielen Dank.

`tsmondo.eu` • Münster

Nachweisbare Compliance, Schritt für Schritt.