

PRODUCT WALKTHROUGH

NIS2 Manager

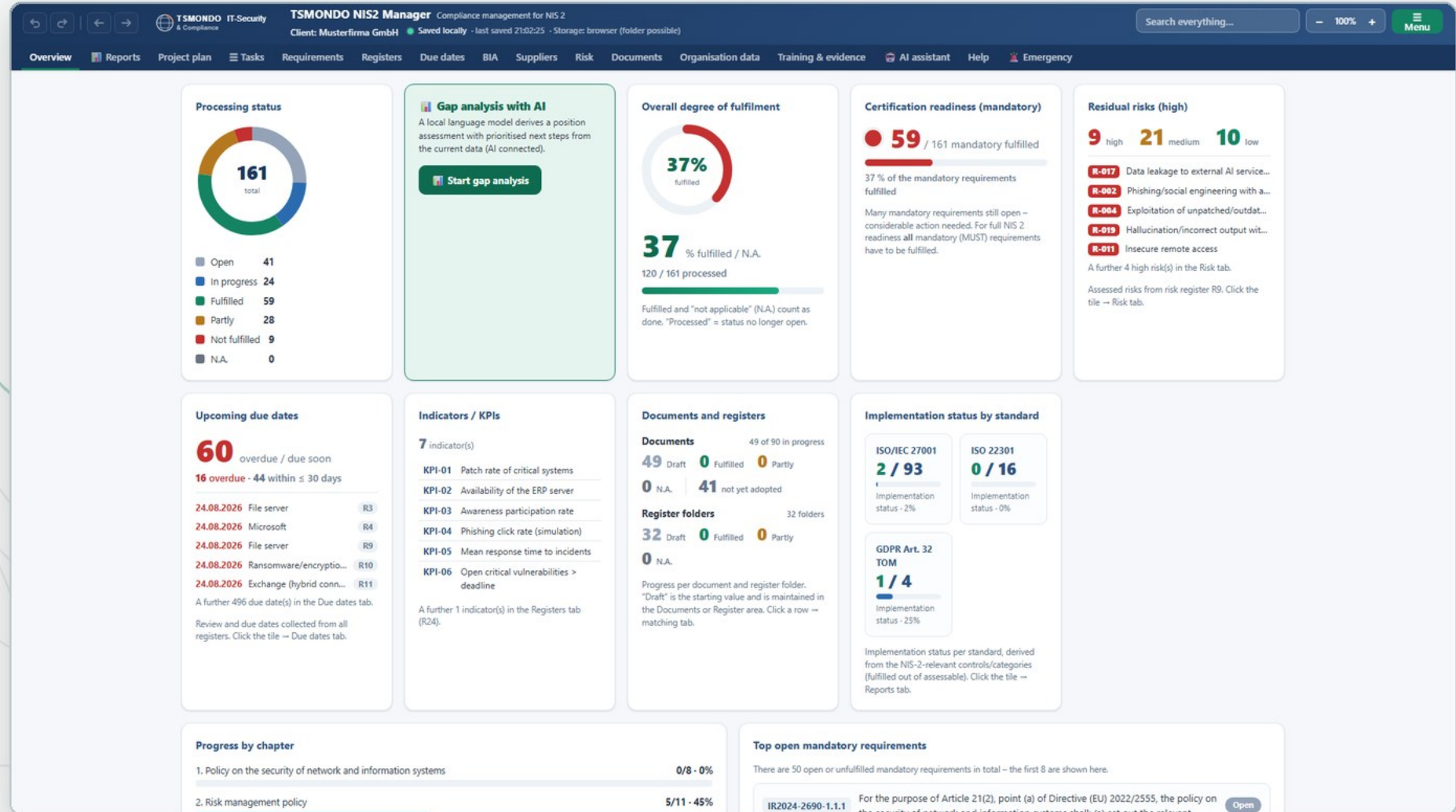
Implement, document and evidence NIS 2 — in a single application

TSMONDO · Münster

INTRODUCTION

What the application does

- Runs locally on your machine
- 161 requirements, 32 registers
- Over 80 document templates



ORGANISATION DATA

Enter once, used everywhere

- Organisation and scope
- Feeds reports and templates
- Your own logo

Master data / customer data

This information is used in the app header (client) and in all reports (compliance report & statement of applicability). Stored exclusively locally in this browser.

ORGANISATION

ORGANISATION / COMPANY

Musterfirma GmbH

STREET & HOUSE NUMBER

Industriestraße 12

POSTCODE

48155

TOWN/CITY

Münster

COUNTRY

Germany

INDUSTRY (OPTIONAL)

Mechanical engineering

EMPLOYEES (OPTIONAL)

240

CONTACT PERSON

CONTACT PERSON

Erika Mustermann

ROLE / FUNCTION

Managing director

E-MAIL

info@musterfirma.example

TELEPHONE

+49 251 1234-0

INFORMATION SECURITY OFFICER (ISB)

Max Mustermann (ISB)

SCOPE

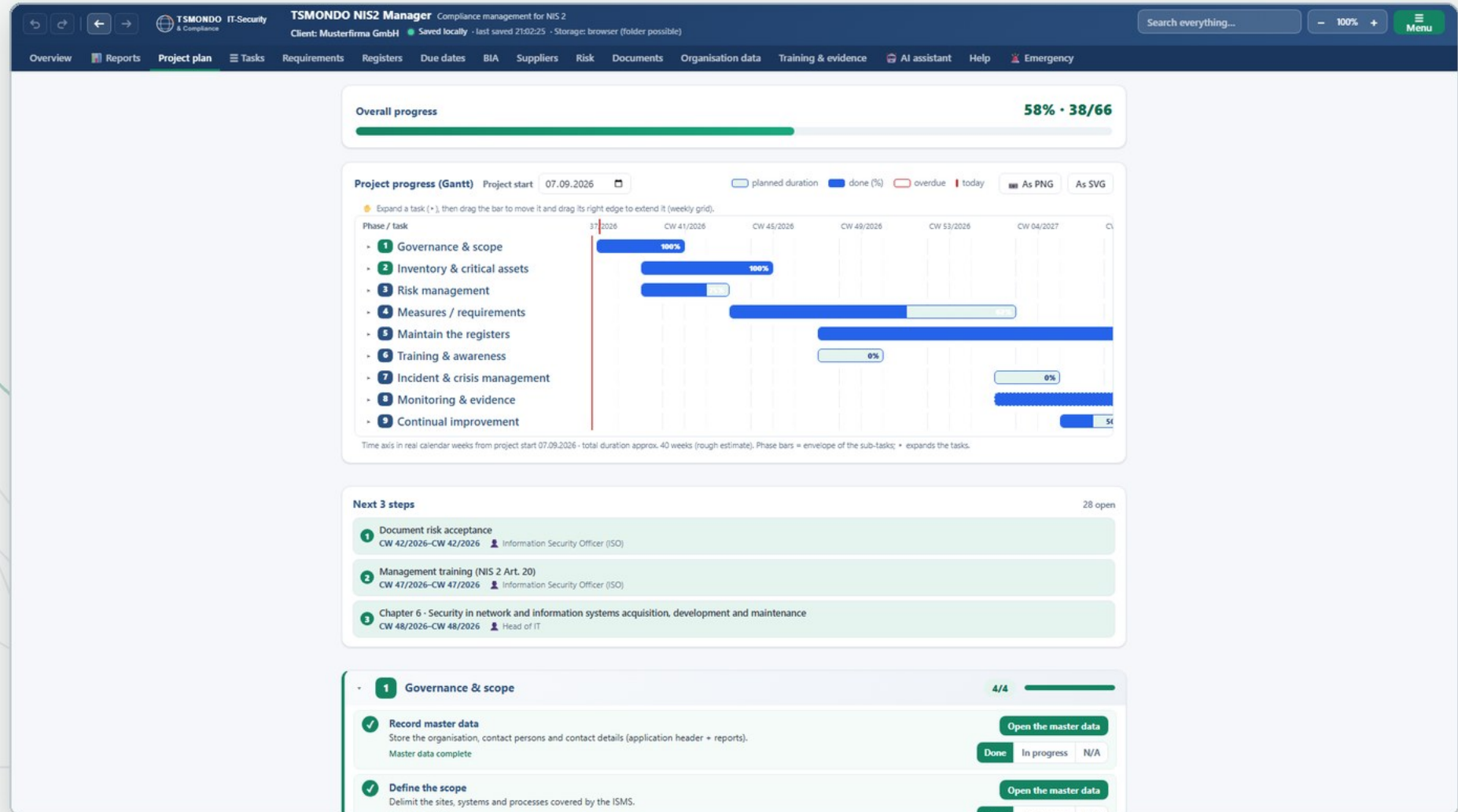
SCOPE (ISMS SCOPE)

All sites, IT operations, production and logistics

PROJECT PLAN

The guided route

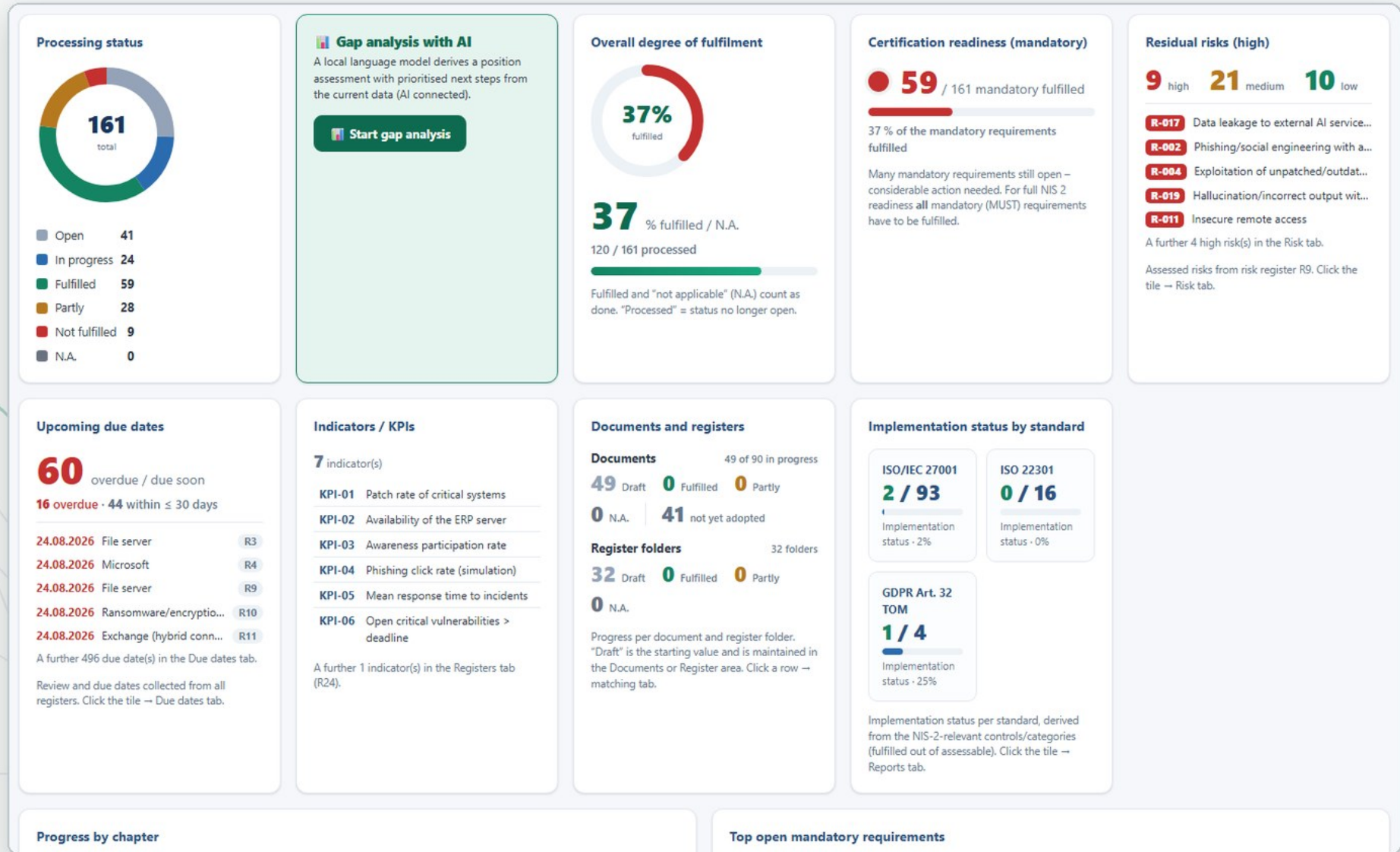
- 9 phases from start to evidence
- Every step jumps to its place
- Status is reported back



OVERVIEW

The current position at a glance

- Level of fulfilment and readiness
- Residual risks and due dates
- Status per standard



REQUIREMENTS

Assess and evidence

- 161 requirements

- Status, comment, evidence

- Reference to Article 21

Requirements NIS-2

CHAPTERS/GROUPS: Collapse all Expand all Status suggestion

▼ 2. Risk management policy 5

100%

2.1 – Risk management policy

IR2024-2690-2.1.1

For the purpose of Article 21(2), point (a) of Directive (EU) 2022/2555, the relevant entities shall establish and maintain an appropriate risk management framework to identify and address the risks posed to the security of network and information systems. The relevant entities shall perform and document risk assessments and, based on the results, establish, implement and monitor a risk treatment plan. Risk assessment results and residual risks shall be accepted by management bodies or, where applicable, by persons who are accountable and have the authority to manage risks, provided that the relevant entities ensure adequate reporting to the management bodies.

Mandatory

SHALL

Art. 21(2), point a

IR (EU) 2024/2690, point 2.1.1

Fulfilled

Fulfilled ▼

Show detail

2.1 – Risk management policy

IR2024-2690-2.1.3

When identifying and prioritising appropriate risk treatment options and measures, the relevant entities shall take into account the risk assessment results, the results of the procedure to assess the effectiveness of cybersecurity risk-management measures, the cost of implementation in relation to the expected benefit, the asset classification referred to in point 12.1, and the business impact analysis referred to in point 4.1.3.

Mandatory

SHALL

Art. 21(2), point a

IR (EU) 2024/2690, point 2.1.3

Fulfilled

Fulfilled ▼

Show detail

DOCUMENTS

Templates with a worked example

- Over 80 templates, sorted
- Each template names its requirement
- A completed example included

Directives 35						
	Acceptable Use Policy for Corporate Systems NIS 2 Article 21(2), point (g) (basic cyber hygiene) · ISO/IEC 27001:2022 A.5.10/A.8.1	created · 08.09.2026 21:02	Template	Example	Edit	Word PDF
	Acceptable Use Policy for AI Systems NIS 2 Article 21(2), point (g) (basic cyber hygiene) · EU AI Act · ISO/IEC 27001:2022 A.5.10/A.8.3	created · 08.09.2026 21:02	Template	Example	Edit	Word PDF
	Change Management Policy NIS 2 Article 21(2), point (e) (security in development and maintenance) · ISO/IEC 27001:2022 A.8.32	created · 08.09.2026 21:02	Template	Example	Edit	Word PDF
	Clear Desk Policy NIS 2 Article 21(2), point (i) (asset management) · ISO/IEC 27001:2022 A.7.7/A.5.12	created · 08.09.2026 21:02	Template	Example	Edit	Word PDF
	Cloud Services Usage Policy NIS 2 Article 21(2), points (d) and (e) (supply chain security, acquisition of ICT services) · ISO/IEC 27001:2022 A.5.23	created · 08.09.2026 21:02	Template	Example	Edit	Word PDF
	Data Backup Policy NIS 2 Article 21(2), point (c) (backup and crisis management) · ISO/IEC 27001:2022 A.8.13	created · 08.09.2026 21:02	Template	Example	Edit	Word PDF
	Information Classification and Protection Policy NIS 2 Article 21(2), point (i) (asset management) · ISO/IEC 27001:2022 A.5.12/A.5.13	created · 08.09.2026 21:02	Template	Example	Edit	Word PDF
	Logging and Monitoring Policy NIS 2 Article 21(2), points (b) and (g) (incident handling, basic cyber hygiene) · ISO/IEC 27001:2022 A.8.15/A.8.16	created · 08.09.2026 21:02	Template	Example	Edit	Word PDF
	Network Security Policy NIS 2 Article 21(2), point (a) (security policies for networks) · ISO/IEC 27001:2022 A.8.20/A.8.21/A.8.22	created · 08.09.2026 21:02	Template	Example	Edit	Word PDF
	Personnel Security Policy					

EDITOR

From template to your document

- Template and worked example
- Editor built into the program
- Export as Word or PDF

Information Security Policy · Completed example Edit in system Fill from master data PDF / Print ×

Information Security Policy of Musterfirma GmbH

TSMONDO IT-Security & Compliance · Document template for NIS 2 · Completed example

Field	Detail
Title	Information Security Policy of Musterfirma GmbH
Version	1.0
Approved by	Management of Musterfirma GmbH
Date	15.01.2026
Classification	Internal – for internal use only

Change history

Version	Date	Change	Editor
1.0	15.01.2026	Initial version, put into effect by Management	Mr Max Mustermann, Information Security Officer (ISB)

This policy is binding for all employees. Please read it carefully. If there is anything you do not understand or you are unsure, ask your manager or the Information Security Officer (ISB).

1. What this is about

Musterfirma GmbH develops, manufactures and sells technical products and related services for customers at home and abroad. Almost all of our processes today depend on IT working properly. Our data, our technical know-how and our customers' data are valuable and must be protected.

This policy describes how we work together to ensure information security – clear and binding for everyone. Information security means that our information remains confidential, is accurate and complete, and is available when we need it.

2. Who does this policy apply to?

This policy applies to everyone who works with IT systems or data belonging to Musterfirma GmbH. This includes:

- Employees,
- contractors and consultants,
- temporary staff,
- Interns.

Each of these individuals shares responsibility for keeping our information secure.

REGISTERS

The evidence base

2 Register of responsibilities / role matrix	3 IT system inventory	4 Software/licence register	5 Process register (central processes & processes with high damage potential)	6 Register of important and critical IT resources	7 Register of critical information
11 Vulnerability register	12 Measures register (measures/action plan)	13 Access rights/identity register (accounts, access and entry rights)	14 Register of administrative accounts	15 Removable media register	16 Register of mobile IT systems
17 Training and awareness evidence	18 Evidence of top management training (NIS-2 / national implementing act)	19 Incident register / log of security incidents	20 Authority notification register (significant security incidents)	21 Cryptography/key register	22 Register of logging sources
23 Contact, availability and address lists (internal/external, emergency)	24 Key figures/KPI register	25 Test and exercise evidence (crisis/procedure tests)	26 Backup and restore test evidence	28 Register of administrative activities (important IT systems)	29 Dependency register & restore order
30 Exception register (approved deviations)	31 Register of detection measures (detection evidence)	32 Network gateway/configuration register (annual review)			

- 32 registers, editable in place
- Inventory, processes, incidents
- Import and export as CSV

RISK

Assess and treat

Risks – initial risk (R9)

9 HIGH	21 MEDIUM	10 LOW
------------------	---------------------	------------------

Impact ↓ / Likelihood →		Likelihood		
		low	medium	high
Impact / severity	high	9 HIGH	7 HIGH	2 HIGH
	medium	10 MEDIUM	12 MEDIUM	0 HIGH
	low	0 LOW	0 MEDIUM	0 HIGH

Method: 3×3 matrix, risk value = likelihood × impact. Bands: 1–2 low, 3–4 medium, 6–9 high. Source: register R9 (live). For details see the template "Risk management procedure".

Residual risks (after measures, R9)

1 HIGH	15 MEDIUM	24 LOW
------------------	---------------------	------------------

Residual risk ↓ / Likelihood →		Likelihood		
		low	medium	high
Residual risk level	high	0 HIGH	0 HIGH	0 HIGH
	medium	14 MEDIUM	14 MEDIUM	1 HIGH
	low	5 LOW	5 MEDIUM	1 HIGH

Residual risk matrix: likelihood (unchanged) × the recorded residual risk level (after measures) as the impact axis. Source: register R9, column "Restrisiko" (live).

- Risk register and matrix
- Likelihood times impact
- Measures with owners

What has to run again first

- Processes from the register
- Outage time and data loss
- Recovery sequence

▼ **Derived restart order** (central first, then ascending by RTO or MTO)

1	central	PRC-01	Order processing	RTO/MTO: 4 h
2	central	PRC-02	Production/manufacturing control	RTO/MTO: 8 h
3	central	PRC-05	E-mail communication	RTO/MTO: 8 h
4	central	PRC-07	Shipping/logistics	RTO/MTO: 8 h
5		PRC-03	Invoicing/billing	RTO/MTO: 24 h
6		PRC-06	Purchasing/procurement	RTO/MTO: 48 h
7		PRC-04	Payroll accounting	RTO/MTO: 72 h

PROCESS	CLASSIFICATION	MTO	RTO	RPO	DAMAGE (F / R / REP / B)	REQUIRED RESOURCES / SYSTEMS	RANK	RESPONSIBLE	NEXT REVIEW
PRC-01 Order processing	central	4 h	4 h	1 h	F: high Rep: high	R: medium B: high R3: SRV-001 – File server R3: SRV-002 – ERP server (Sample E... + Link a resource ... adopt from R5 (processes)	1	Head of sales	30.06.2027
PRC-02 Production/manufacturing control	central	8 h	8 h	1 h	F: high Rep: high	R: medium B: high R3: SRV-002 – ERP server (Sample E... R3: SRV-003 – Domain controller (AD) + Link a resource ... adopt from R5 (processes)	2	Head of production	30.06.2027

EMERGENCY

Prepared for the worst case

- Immediate actions and contacts
- 24 hours, 72 hours, one month
- Reporting assistant for the authority

Competent authorities & notification deadlines — European Union (neutral country pack)

EARLY WARNING

24 hours

First short notification after becoming aware

NOTIFICATION

72 hours

Assessment: severity and impact

FINAL REPORT

1 month (or a progress report if the incident is ongoing)

After the notification, or once the incident is closed

- **NIS 2 authority:** the competent national cybersecurity authority or your national CSIRT – There is no single EU-wide reporting body. Each Member State designates its own competent authorities and CSIRTs under Articles 8 and 10 of Directive (EU) 2022/2555. The current name of the authority, its portal, and the exact reporting channel must be looked up in the relevant Member State before reporting, for example via ENISA's overview of national CSIRTs.
- **CSIRT:** the national CSIRT of the relevant Member State
- **Registration required:** yes – With the competent national CSIRT or authority of the Member State in which the entity is established or provides services
- **Data protection authority:** the competent national data protection supervisory authority – Parallel notification under Art. 33 GDPR within 72 hours if personal data is affected. The competent authority depends on the entity's establishment or main establishment and should be looked up via the European Data Protection Board's list of data protection authorities.
- **Law:** Directive (EU) 2022/2555 (NIS 2 Directive) and Implementing Regulation (EU) 2024/2690 (in force; national transposition at different stages across the Member States)
- **Sanctions:** particularly important entities: up to EUR 10 million or 2 % of total worldwide annual turnover, whichever is higher (EU framework under Art. 34(4) of the Directive); the amounts actually in force are set out in the national transposition law of the respective Member State · important entities: up to EUR 7 million or 1.4 % of total worldwide annual turnover, whichever is higher (EU framework under Art. 34(5) of the Directive); the amounts actually in force are set out in the national transposition law of the respective Member State · Management: Responsibility of the management body for approving and overseeing the risk-management measures (Art. 20 of the Directive); the specific form of liability is governed by national transposition law

CSIRT – open the notification portal <https://www.enisa.europa.eu/tools/csirts-by-country-interactive-map> [copy](#)CSIRT: the national CSIRT of the relevant Member State <https://www.enisa.europa.eu/tools/csirts-by-country-interactive-map> [copy](#)Data protection authority – overview https://www.edpb.europa.eu/about-edpb/about-edpb/members_en [copy](#)

DUE DATES

Dates in view

16 overdue		44 due within 30 days		501 due dates in total		
REGISTER	ENTRY	DESIGNATION	TYPE OF DUE DATE	DATE	STATUS	ACTION
filter...	filter...	filter...	filter...	filter...	filter...	Reset filters
R3 IT system inventory	SRV-001	File server	Last review	24.08.2026	overdue	✓ Reviewed Add to calendar
R4 Software/licence register	Windows Server 2022	Microsoft	Last review	24.08.2026	overdue	✓ Reviewed Add to calendar
R9 Risk register (risk identification & analysis)	R-001	File server	Last review	24.08.2026	overdue	✓ Reviewed Add to calendar
R10 Risk treatment plan	R-001	Ransomware/encryption trojan – File server	Last review	24.08.2026	overdue	✓ Reviewed Add to calendar
R11 Vulnerability register	SW-001	Exchange (hybrid connector)	Last review	24.08.2026	overdue	✓ Reviewed Add to calendar
R12 Measures register (measures/action plan)	M-001	Risk (R-002)	Last review	24.08.2026	overdue	✓ Reviewed Add to calendar
R15 Removable media register	WDT-001	USB stick 64 GB (BitLocker)	Last review	24.08.2026	overdue	✓ Reviewed Add to calendar
R16 Register of mobile IT systems	MOB-001	Notebook (Lenovo T14)	Last review	24.08.2026	overdue	✓ Reviewed Add to calendar
R24 Key figures/KPI register	KPI-01	Patch rate of critical systems	Last review	24.08.2026	overdue	✓ Reviewed Add to calendar

- Dates from every register
- Overdue and due within 30 days
- Export to the calendar

SUPPLIERS

Examining the supply chain

NAME / CATEGORY	CRITICALITY	LAST ASSESSMENT	SCORE	TRAFFIC LIGHT	ACTIONS
Muster Cloud Services GmbH Account team (partner) no data access	hoch	15.06.2026	98	● Green	NIS 2 self-assessment Questionnaire dispatch Audit PDF
MusterIT GmbH Systeme GmbH E. Example no data access	hoch	15.06.2026	71	● Yellow	NIS 2 self-assessment Questionnaire dispatch Audit PDF
Muster Telekommunikation GmbH Business customer service no data access	hoch	15.06.2026	88	● Green	NIS 2 self-assessment Questionnaire dispatch Audit PDF
Muster Hosting AG Solutions Architect no data access	mittel	15.06.2026	62	● Yellow	NIS 2 self-assessment Questionnaire dispatch Audit PDF
Sample ERP GmbH Support team no data access	hoch	15.06.2026	87	● Green	NIS 2 self-assessment Questionnaire dispatch Audit PDF
Muster Security Reseller GmbH Sales partner no data access	hoch	15.06.2026	49	● Red	NIS 2 self-assessment Questionnaire dispatch Audit PDF
Local IT service provider Musterstadt F. Sample no data access	niedrig	15.06.2026	52	● Red	NIS 2 self-assessment Questionnaire dispatch Audit PDF

- An obligation in its own right
- Weighted questionnaire
- A score per supplier

SUPPLIERS

The questionnaire for the supplier

- A fillable PDF

- Client and supplier in the header

- 37 questions, ten areas

NIS 2 supplier self-assessment

Information security in the supply chain (Art. 21(2)(a)-(j) NIS 2)

Client: Musterfirma GmbH
Industriestraße 12
48155 Münster
Germany

Contact: Erika Mustermann (Managing director)
info@musterfirma.example
Tel.: +49 251 1234-0

Supplier: Muster Hosting AG

Contact person: Solutions Architect

Date: 08.09.2026

This questionnaire records the information security of your company as a supplier or service provider along the ten measure areas of the NIS 2 Directive (Art. 21(2)(a)-(j)).

How to proceed:

1. Fill in the form fields directly in this PDF (yes/no choices, drop-down lists, free text).
2. SAVE the file afterwards (File > Save) — please do not just print it.
3. Send the saved PDF back to your client.

Note: for fields that do not apply to your company, please select "not applicable" — they are then excluded from the assessment.

Risk Management & ISMS

Does your organisation have a documented information security management system (ISMS), e.g. based on ISO/IEC 27001 or an equivalent recognised framework?

This means a lived, documented management system (policy, roles, governance) — certification is not mandatory, but advantageous.
NIS-2 Art.21(2)(a)

☒ Yes ☐ No ☐ Not applicable

Comment (optional):

Do you carry out a structured risk analysis of your information assets on a regular basis (at least annually)?

Risks are identified, assessed (likelihood/impact) and treated; results are documented in a traceable manner.
NIS-2 Art.21(2)(a)

☐ Yes ☒ No ☐ Not applicable

Comment (optional):

Does your organisation have an information security policy approved by top management?

A security policy approved by top management and communicated as the framework for all measures.
NIS-2 Art.21(2)(a)

☐ Yes ☒ No ☐ Not applicable

Comment (optional):

SUPPLIERS

The answer comes back

- Import the answer PDF
- Fulfilment per measure area
- Score and history

Assessment by measure area

MEASURE AREA (NIS 2)	FULFILMENT	PROGRESS
Risk Management & ISMS	42%	
Incident Handling & Notification	79%	
Business Continuity & Backup	94%	
Supply Chain Security	94%	
Procurement, Development & Vulnerabilities	77%	
Effectiveness Assessment	93%	
Cyber Hygiene & Training	60%	
Cryptography & Encryption	100%	
Personnel, Access & Assets	54%	
MFA & Secure Communication	67%	

Critical findings (3)

QUESTION	ANSWER	NIS 2 / BSI
Does your organisation have a documented information security management system (ISMS), e.g. based on ISO/IEC 27001 or an equivalent recognised framework?	No	Art.21(2)(a)
Do you carry out regular awareness and training measures on information security for all employees?	No	Art.21(2)(g)
Do you use multi-factor authentication (MFA) for administrative and privileged access?	No	Art.21(2)(j)

History (2 assessments)

08.09.2026		75 / 100 · Yellow	PDF
15.06.2026		62 / 100 · Yellow	PDF

TASKS

Who does what by when

- Tasks from the project plan
- Board and bar chart
- Output per owner

The screenshot displays a task management dashboard. At the top, it shows 'Tasks by assignee' with a total of 66 tasks (38 done, 28 open). The view is set to 'By person'. The dashboard is divided into two main sections for assignees.

Head of IT (49 tasks, 29 done, next due date CW 48/2026):

- Phase 3: Identify risks (R9) (CW 39/2026–CW 39/2026)
- Phase 3: Assess risks on a 3×3 scale (CW 40/2026–CW 40/2026)
- Phase 3: Risk treatment plan (R10) (CW 41/2026–CW 41/2026)
- Phase 3: Document risk acceptance (CW 42/2026–CW 42/2026)
- Phase 6: Management training (NIS 2 Art. 20) (CW 47/2026–CW 47/2026)
- Phase 6: Staff awareness (CW 48/2026–CW 48/2026)
- Phase 6: Evidence (R17/R18) (CW 49/2026–CW 49/2026)

Information Security Officer (ISO) (11 tasks, 4 done, next due date CW 42/2026):

- Phase 3: Identify risks (R9) (CW 39/2026–CW 39/2026)
- Phase 3: Assess risks on a 3×3 scale (CW 40/2026–CW 40/2026)
- Phase 3: Risk treatment plan (R10) (CW 41/2026–CW 41/2026)
- Phase 3: Document risk acceptance (CW 42/2026–CW 42/2026)
- Phase 6: Management training (NIS 2 Art. 20) (CW 47/2026–CW 47/2026)
- Phase 6: Staff awareness (CW 48/2026–CW 48/2026)
- Phase 6: Evidence (R17/R18) (CW 49/2026–CW 49/2026)

TRAINING

Management under obligation

- A series of 12 modules
- Checkpoints for management
- Evidence in the registers

01 Scope Establish applicability: registration with the competent national authority, justification of applicability, and embedding the Article 21 measures.

4/4 completed

✓ Evidence of registration with the competent national authority as an affected entity, including the contact points on file and sector/NACE classification
From whom: Head of IT together with the Information Security Officer · **How often:** Once (registration), then annual update

✓ Written justification of applicability (thresholds: headcount, turnover, balance sheet total, NACE classification) as an audit-proof file note
From whom: Information Security Officer · **How often:** Annually and on an ad hoc basis for structural changes

→ Statement of Applicability (SoA)

✓ Confirmation that all ten measures under Art. 21(2) and the reporting obligations under Art. 23 are firmly anchored in the measures plan
From whom: Information Security Officer · **How often:** Once (initial setup), then annual review

→ Requirements

✓ Formal approval of the NIS-2 measures by the management body (written approval resolution, non-delegable)
From whom: Management itself · **How often:** Once on entry into force, then confirm annually

→ Management approval resolution

02 Liability and reporting Management's non-delegable duties, regular reporting, the contact point for the competent national authority, and the 24-hour notification template.

6/6 completed

03 Ten obligations (Art. 21) Status traffic light for each obligation (a) to (j), naming the SCRM owner, and prioritising red obligations.

5/5 completed

REPORTS

Evidence on paper

- 10 reports, one click

- Compliance report and statement of applicability

- Report for management

Reports

Central collection point for all reports. "Show" opens the report in a window (referenced evidence is clickable and jumps into the tool); there it can be printed via "Print as PDF" in the TSMONDO layout. The organisation data appears automatically in the header.

- Project progress report (ISMS implementation)** new
Overall project progress and phase status (done/in progress/open) of the ISMS implementation as a Gantt chart plus a phase table (duration, start/end, progress %, open steps) and recommended actions.
[Show](#)
- Compliance report (NIS 2)**
Implementation status of all requirements with key figures, status distribution by obligation level, tier and chapter — including NIS-2 reference.
[Show](#)
- Management report**
Condensed governance overview for management: level of fulfilment, residual risks, deadlines, supplier traffic-light status, open measures, incidents, recommended actions.
[Show](#)
- Statement of applicability (SoA)**
Statement of applicability: applicability, implementation status and justification for each requirement, grouped by chapter.
[Show](#)
- Emergency plan / first-aid report**
Immediate measures, statutory notification deadlines (NIS 2 & GDPR), authority and organisation's own emergency contacts, restart order.
[Show](#)
- Documentation evidence per obligation (sorted by NIS-2)** new
All requirements in ascending order by NIS 2 reference: status and whether evidence is available. Guiding principle: "not documented = not in place"; missing evidence marked in red.
[Show](#)
- ISO/IEC 27001 conformity report** new
Curated mapping of NIS-2 Art. 21 (a-j) → ISO/IEC 27001:2022 (Annex A): derived fulfilment status per area, coverage key figure and gap list. Mapping subject to expert review.
[Show](#)
- ISO 22301 conformity report (BCM)** new
Curated mapping of NIS-2 Art. 21 (a-j) → ISO 22301:2019 (business continuity, focus on clause 8) with derived status and gap list. Mapping subject to expert review.
[Show](#)
- GDPR Art. 32 - TOM conformity report** new
TOM categories under Art. 32(1) GDPR (pseudonymisation/encryption, confidentiality/integrity/availability/resilience, ability to restore data, regular review) → Art. 21, status and linked evidence.
[Show](#)
- Management review (combined annual review)** new
Annual management review in a SINGLE document.
[Show](#)

AI ASSISTANT

Drafting aid, not a substitute

- Local model or EU provider
- A baseline assessment from your own data
- Every text stays a draft

 **AI assistant** (local, drafting aid)
Drafts texts (policies, measures, risks, cover letters, reports) with a **local** Language model (Ollama) and uses the current status of this application as context (RAG-lite). All processing takes place on this device.

 AI draft — have it reviewed professionally and legally. Not legal advice.

 **Gap analysis — Where do I stand?**
Generates a management-ready assessment of the current position from the current status (degree of fulfilment, residual risks, open measures, deadlines, suppliers, BIA, incidents, missing mandatory documents), with prioritised next steps.

Start gap analysis

Settings (local model) Connected · 6 model(s)

PROCESSING

☒ Local (Ollama)

☐ Mistral (EU cloud, GDPR)

BASE URL (OLLAMA)

MODEL

EMBEDDING MODEL

Load models **Test connection**

Chat

DOCUMENTS & POLICIES

RISK & BIA

COMMUNICATION & REPORTS

UNDERSTANDING REQUIREMENTS

Ask a question or use a quick action. The answer is a draft and must be reviewed by a specialist.

CLOSING

Your data, your evidence

- Your data stays local
- Encrypted backup
- Change log included

Database management

All functions relating to your data in one place: backup & restore, encryption, and the shared data folder for multi-user operation. Storage is exclusively local.

BACKUP & EXPORT

↓ Export everything (JSON)

Saves all entries to an unencrypted JSON file.
Tip: export as a backup before every app update and import it again afterwards.

[Export...](#)

🔒 Encrypted backup (.vdsenc)

The JSON export is plain text; this backup is AES-256-GCM encrypted and requires your master password.

[Save encrypted...](#)

↑ Import (JSON / .vdsenc)

Loads a previously created status from a JSON or encrypted .vdsenc-file. The current status will be replaced.

[Import...](#)

AUTOMATIC DAILY BACKUP & RESTORE

The automatic daily backup with restore is only available in the **desktop app** (portable EXE) available, as it accesses the local data folder. In browser mode, please use "Export all" (regularly) and "Import" to restore it.

ENCRYPTION

🔑 Master password

Protects the locally stored data with a master password (AES-256-GCM). Here you can set up encryption, change the password, or remove it again.
Current status: **not active**.

[Manage encryption...](#)



Thank you.

tsmondo.eu • Münster

Compliance you can evidence, step by step.