TSMONDO IT-Security & Compliance

PRODUCT WALKTHROUGH

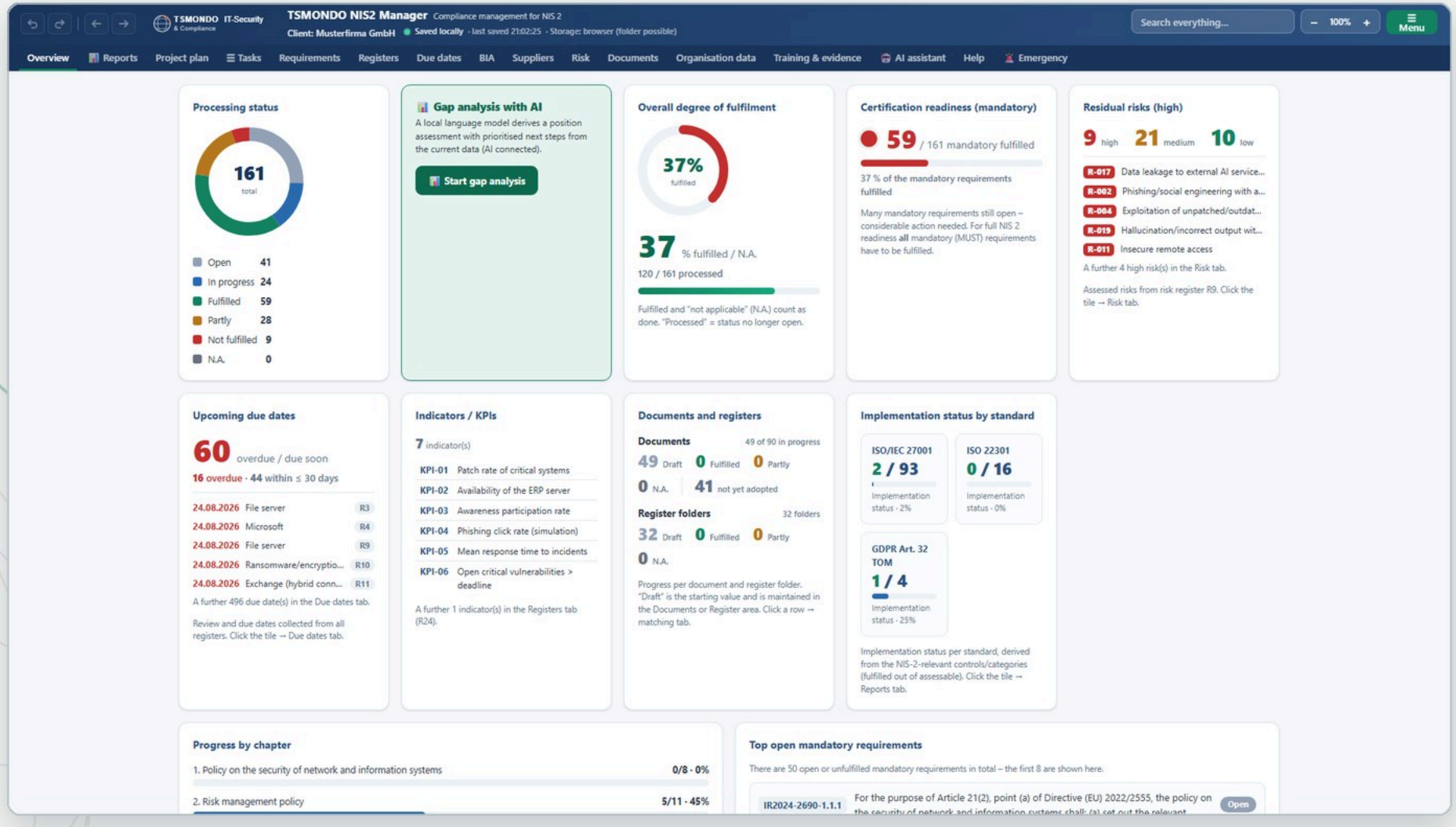
NIS2 Manager

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

TSMONDO · Münster

INTRODUCTION

What the application does

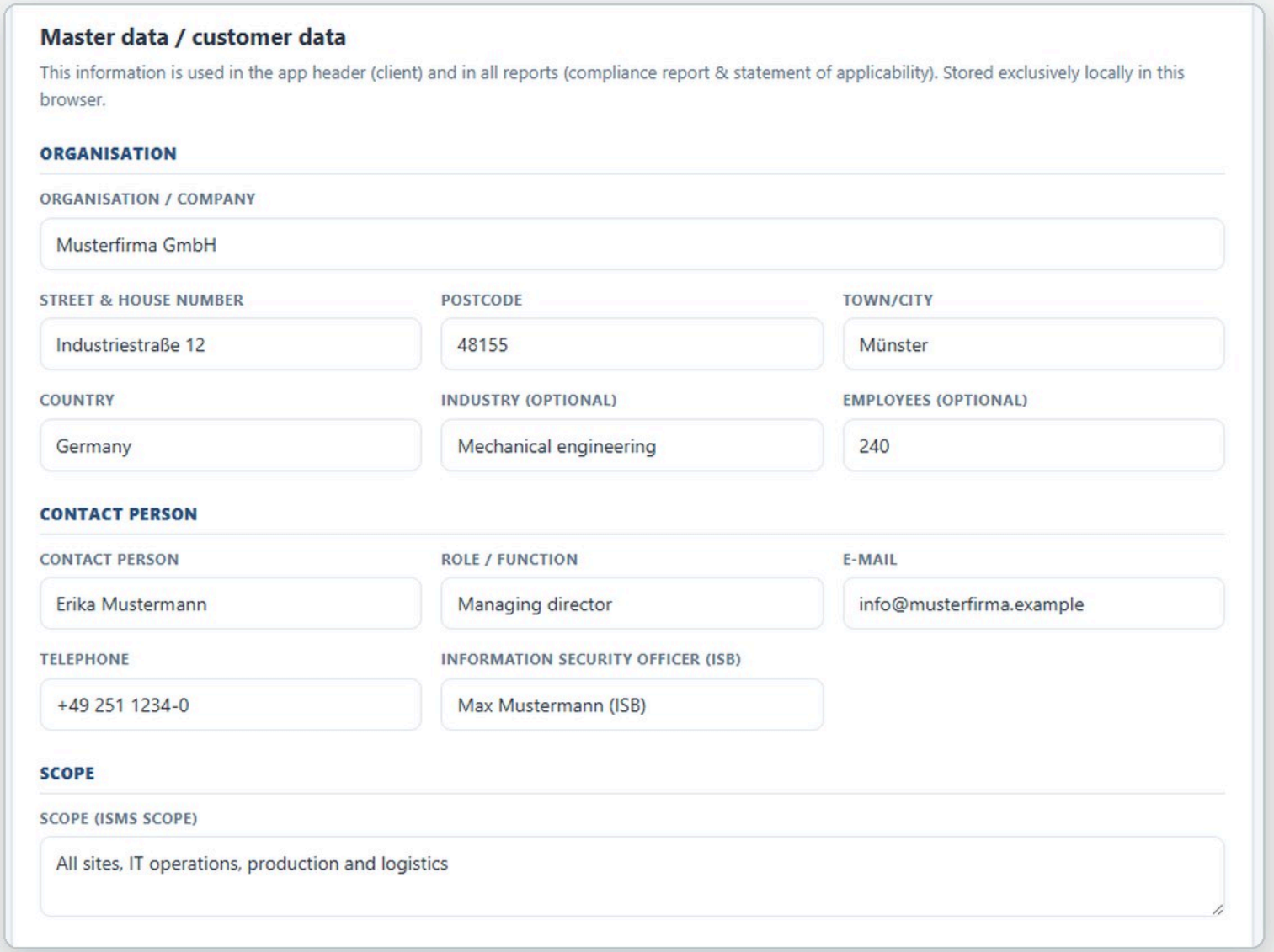


- Runs locally on your machine
- 161 requirements, 32 registers
- Over 80 document templates

ORGANISATION DATA

Enter once, used everywhere

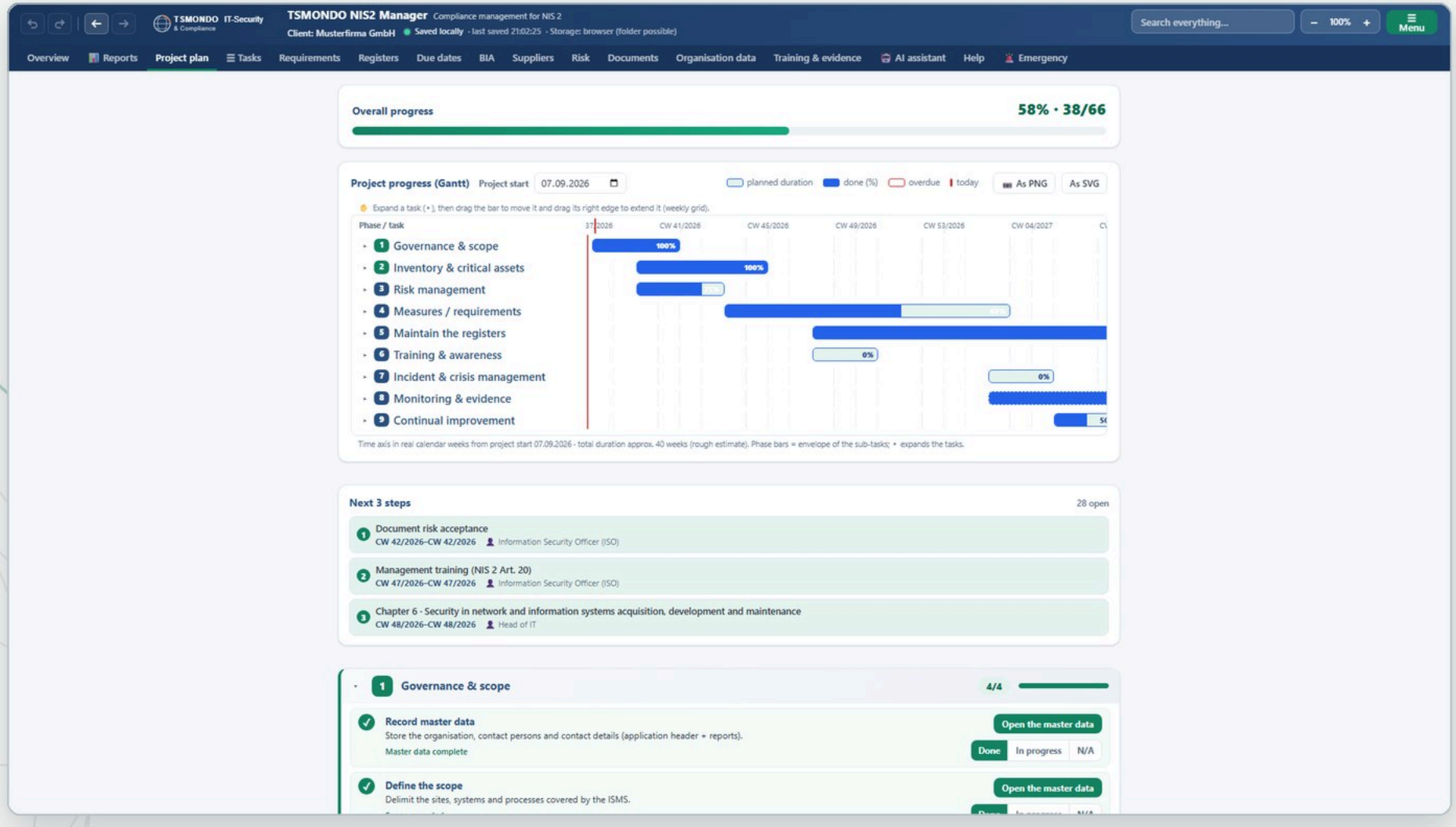
- Organisation and scope
- Feeds reports and templates
- Your own logo



PROJECT PLAN

The guided route

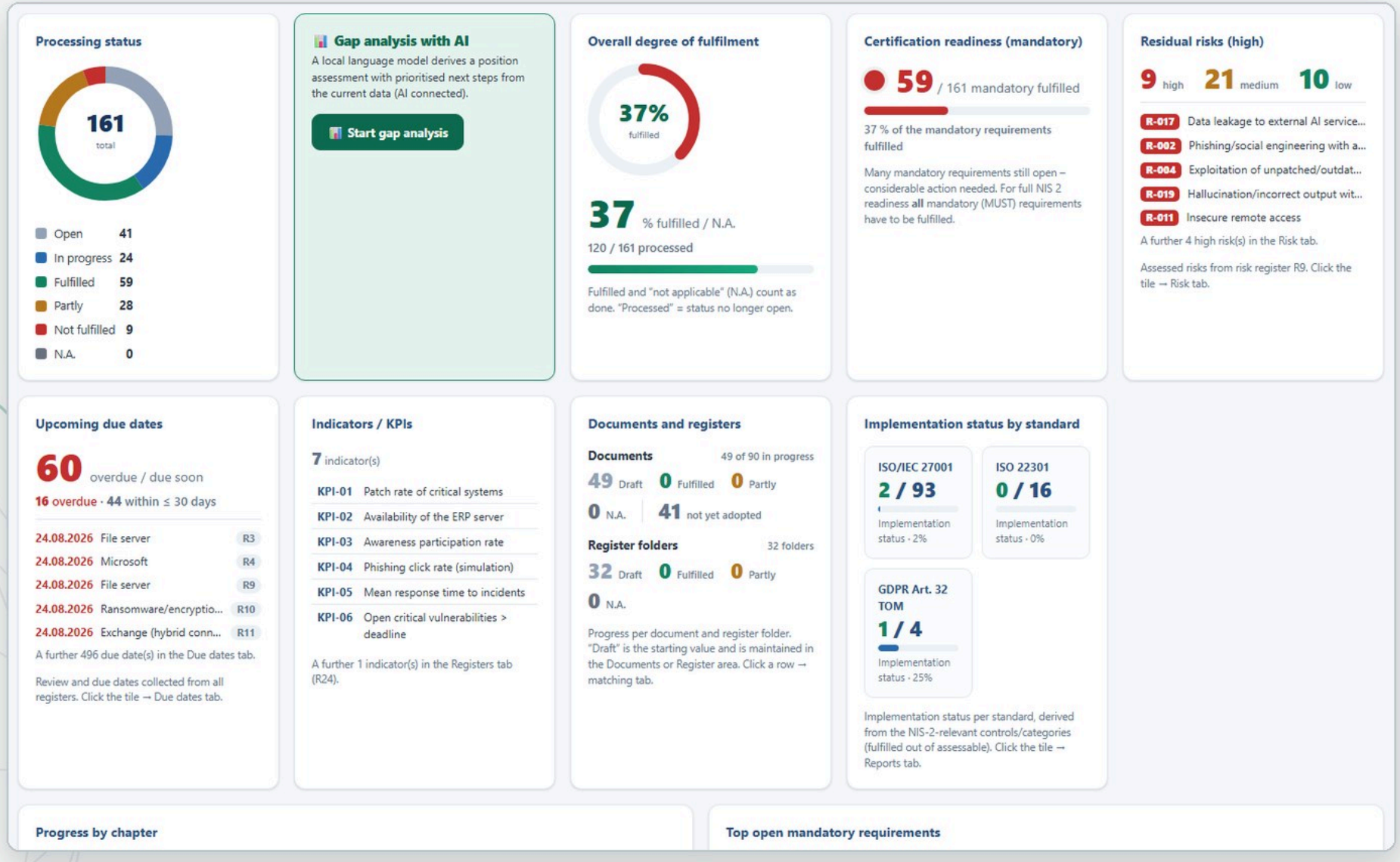
- 9 phases from start to evidence
- Every step jumps to its place
- Status is reported back



OVERVIEW

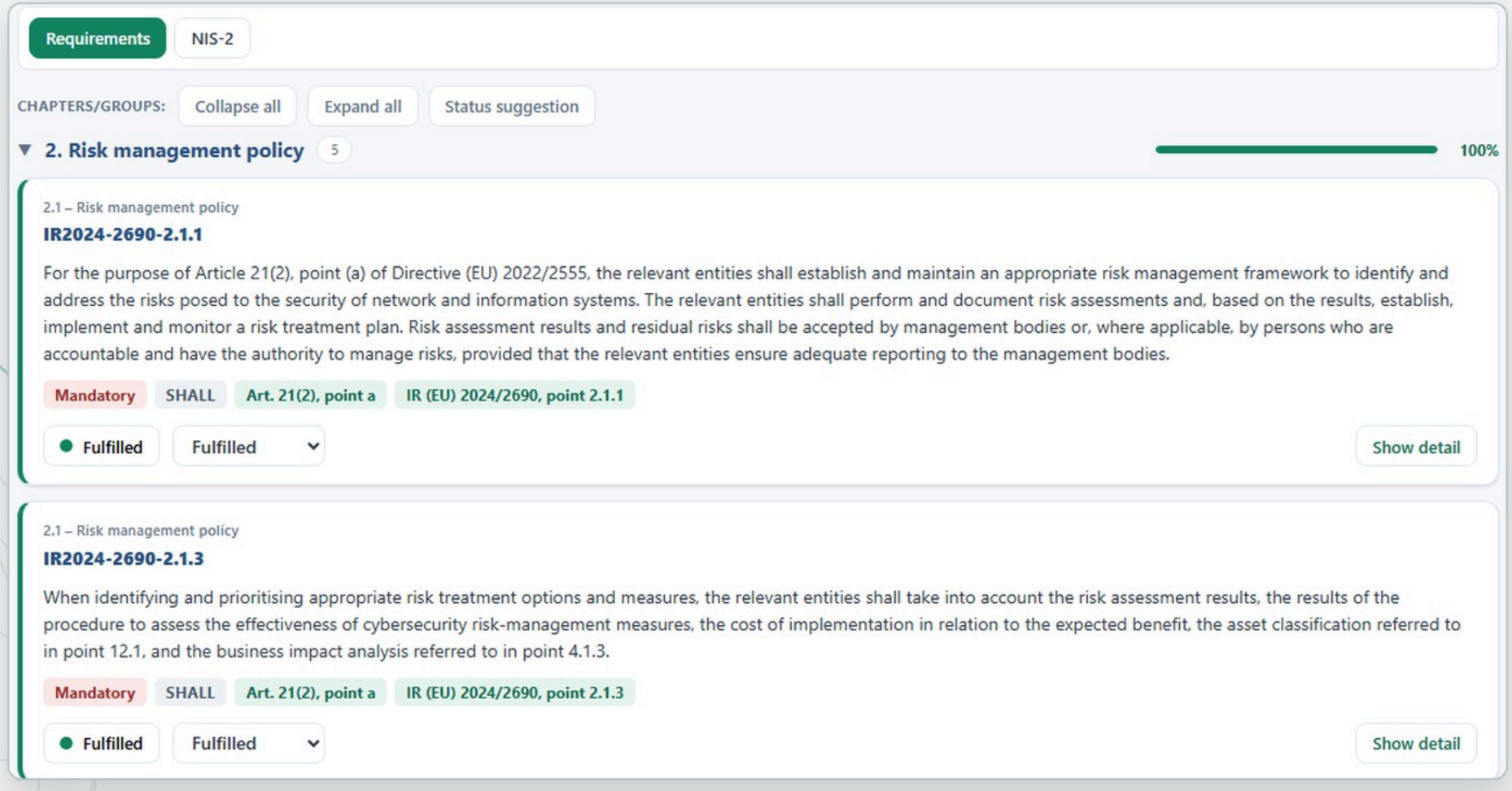
The current position at a glance

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



REQUIREMENTS

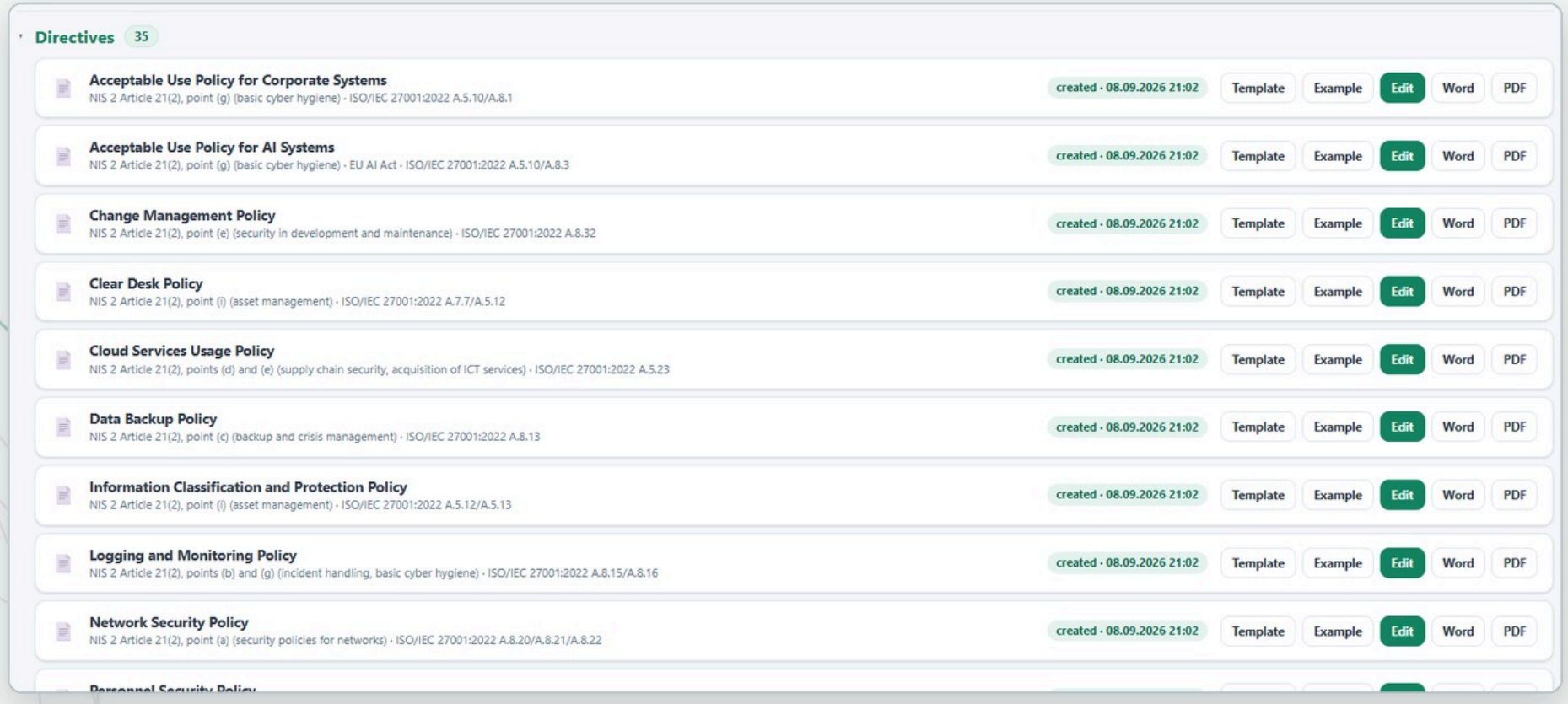
Assess and evidence



- 161 requirements
- Status, comment, evidence
- Reference to Article 21

DOCUMENTS

Templates with a worked example

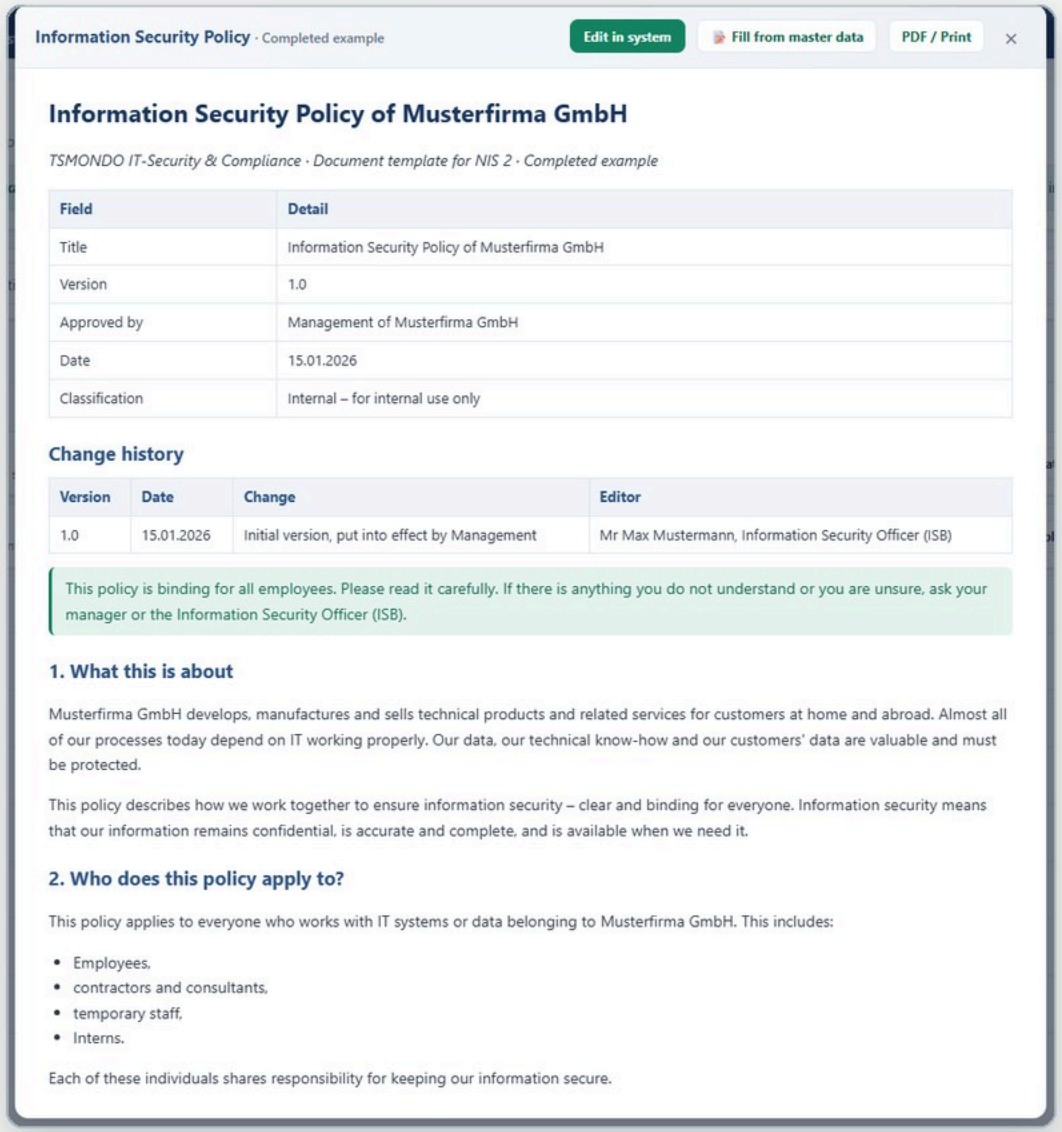


- Over 80 templates, sorted
- Each template names its requirement
- A completed example included

EDITOR

From template to your document

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



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

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

Risks – initial risk (R9)

9	21	10
HIGH	MEDIUM	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	15	24
HIGH	MEDIUM	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).

B I A

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	zentral	4 h	4 h	1 h	F high R medium Rep high 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	zentral	8 h	8 h	1 h	F high R medium Rep high 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	NOTIFICATION	FINAL REPORT
24 hours	**72 hours**	**1 month (or a progress report if the incident is ongoing)**
First short notification after becoming aware	Assessment: severity and impact	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

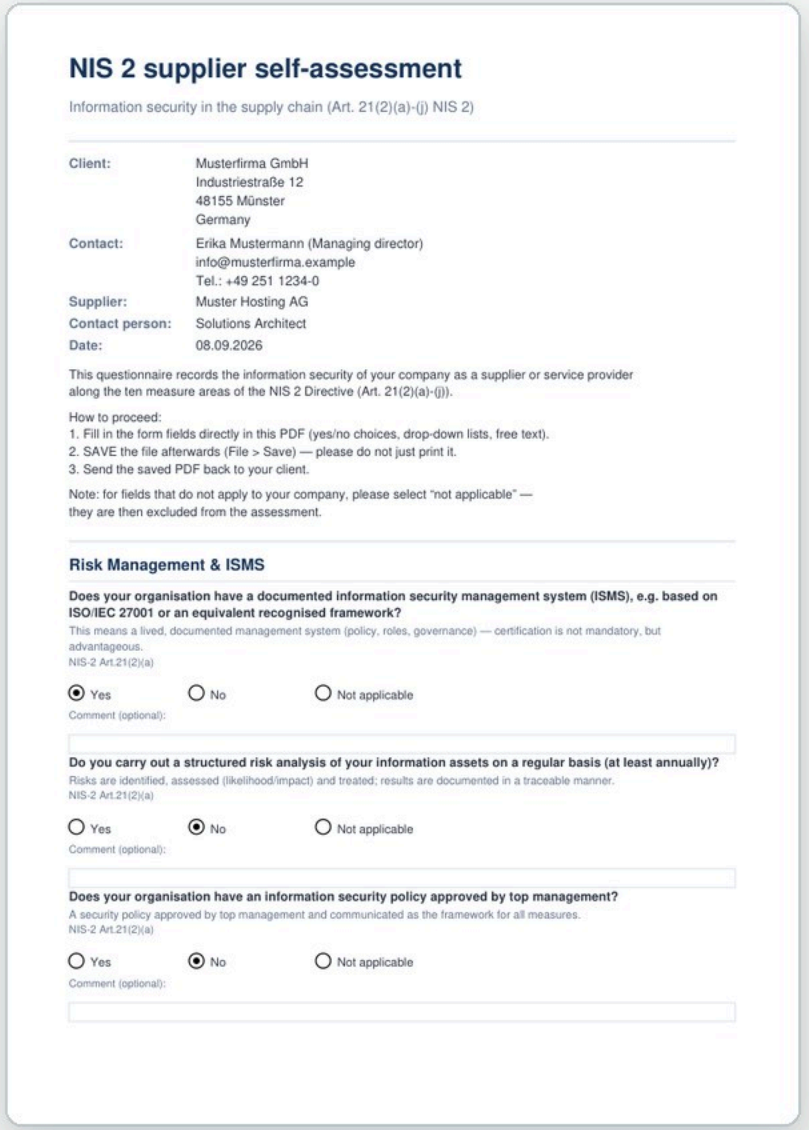
NAME / CATEGORY	CRITICALITY	LAST ASSESSMENT	SCORE	TRAFFIC LIGHT	ACTIONS
Muster Cloud Services GmbH Account team (partner) no data access	hoch	15.06.2026	**98**	Green	NIS 2 self-assessment · Questionnaire dispatch · Audit PDF
MusterIT GmbH Systeme GmbH E. Example no data access	hoch	15.06.2026	**71**	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):

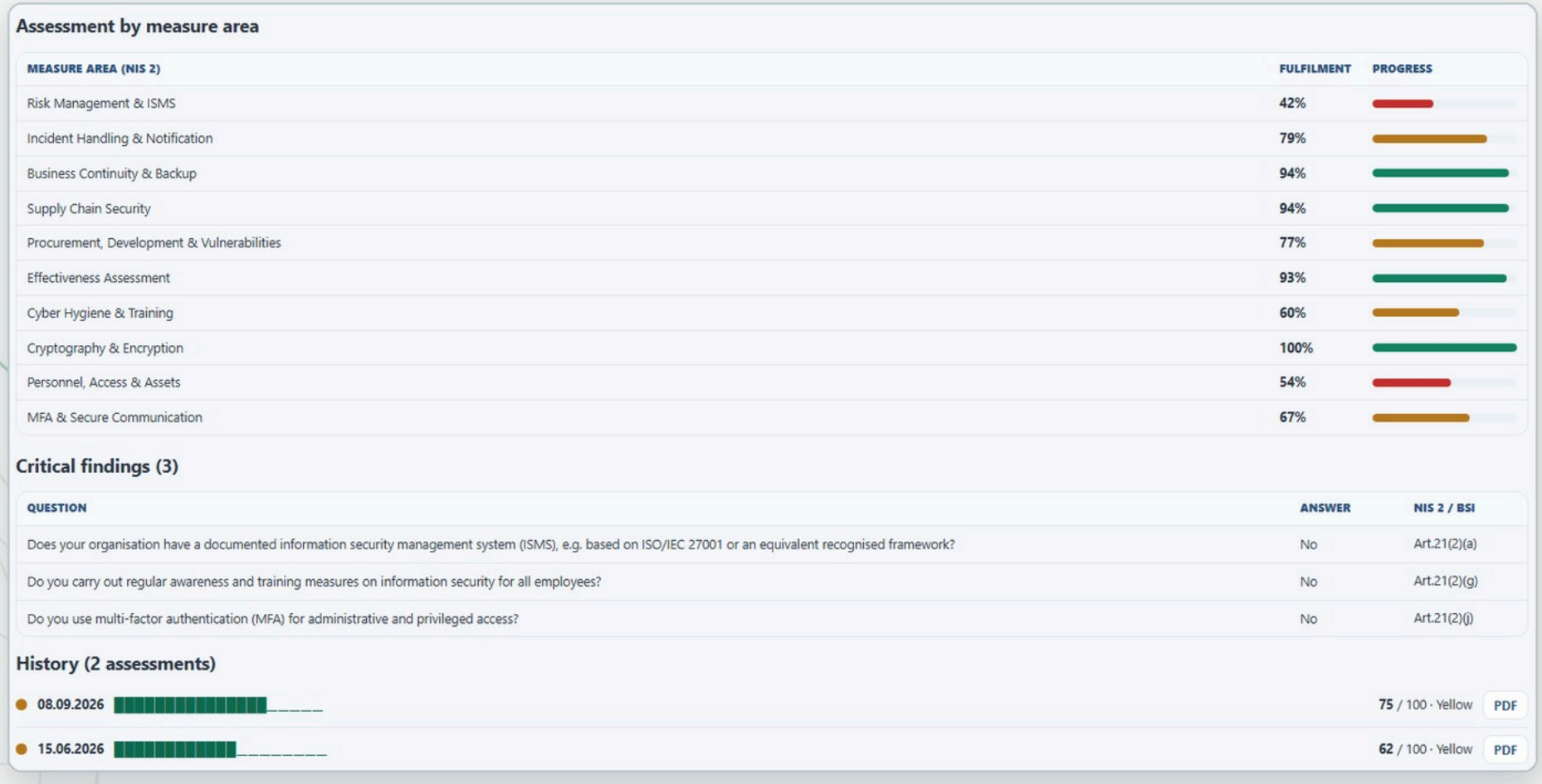
Does your organisation have an information security policy approved by top management?
A security policy approved by top management and communicated as the framework for all measures.
NIS-2 Art.21(2)(a)

○ 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)

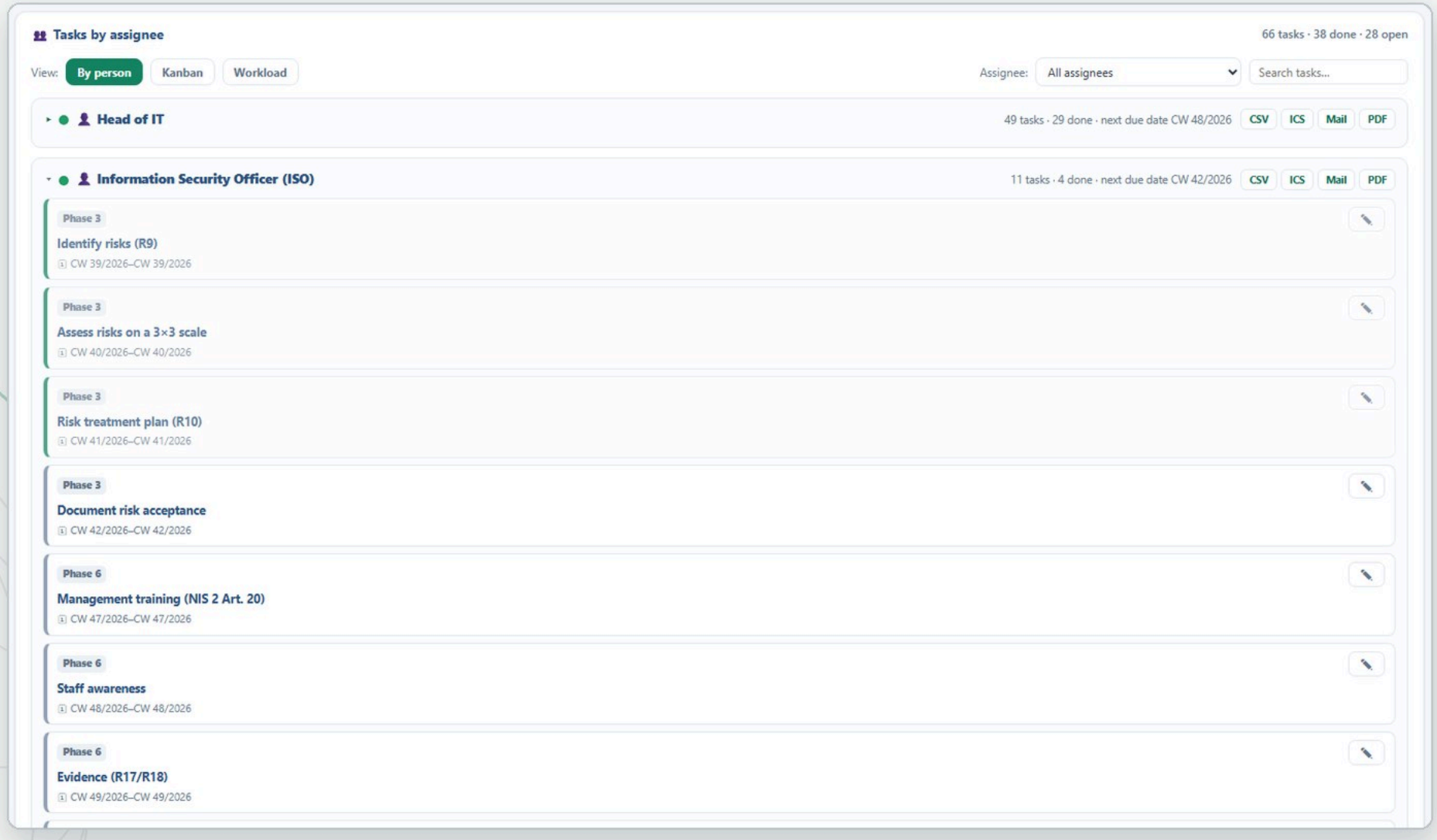
History (2 assessments)

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

TASKS

Who does what by when

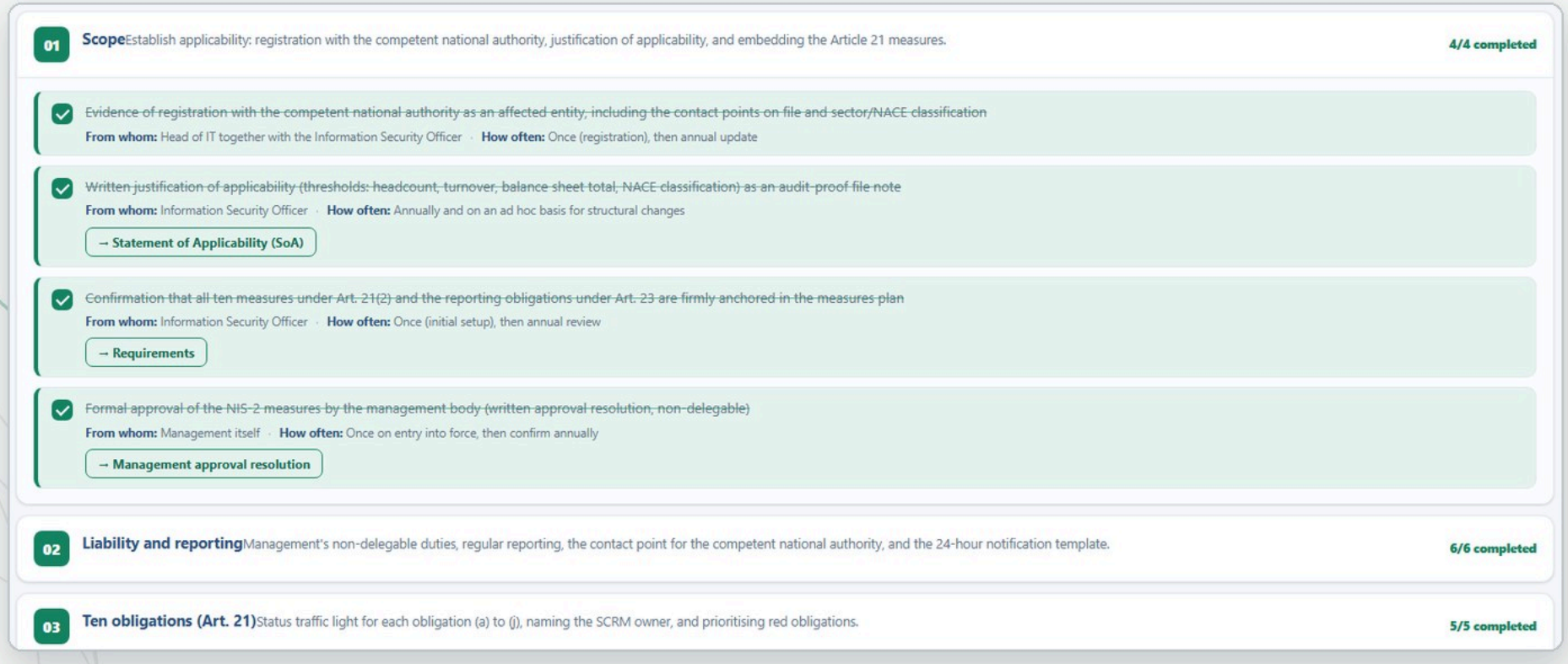
- Tasks from the project plan
- Board and bar chart
- Output per owner



TRAINING

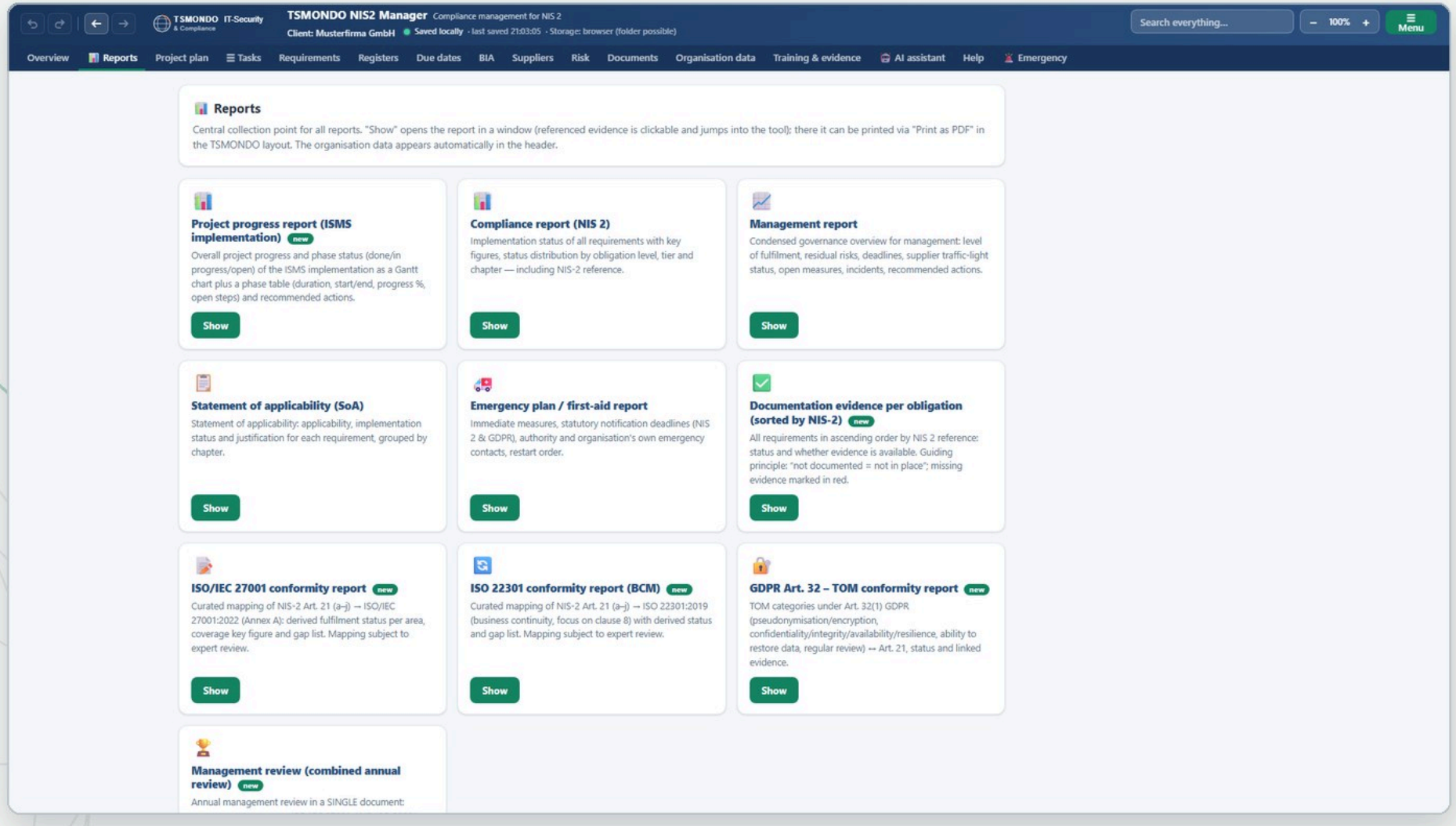
Management under obligation

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



REPORTS

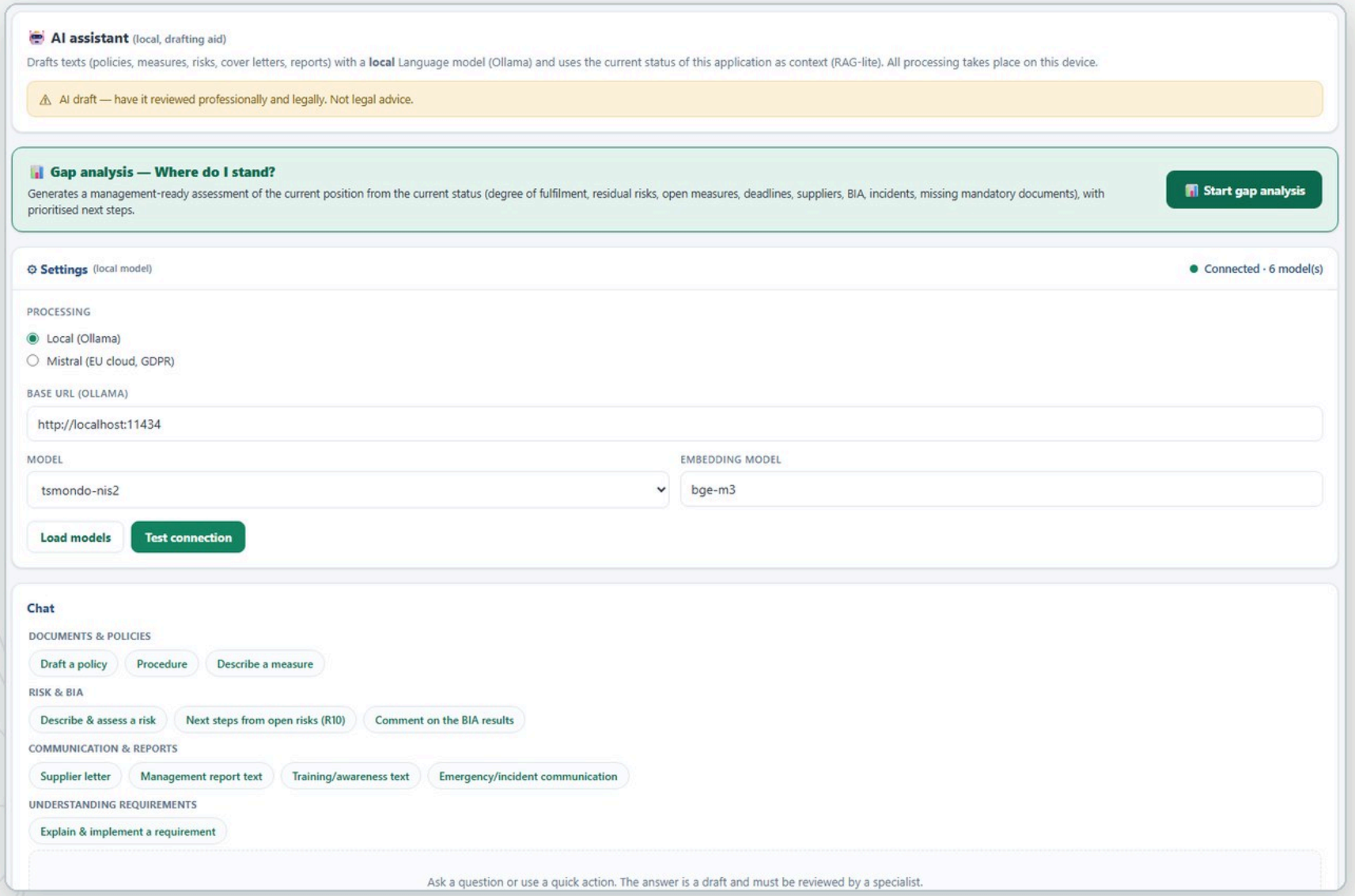
Evidence on paper



- 10 reports, one click
- Compliance report and statement of applicability
- Report for management

AI ASSISTANT

Drafting aid, not a substitute

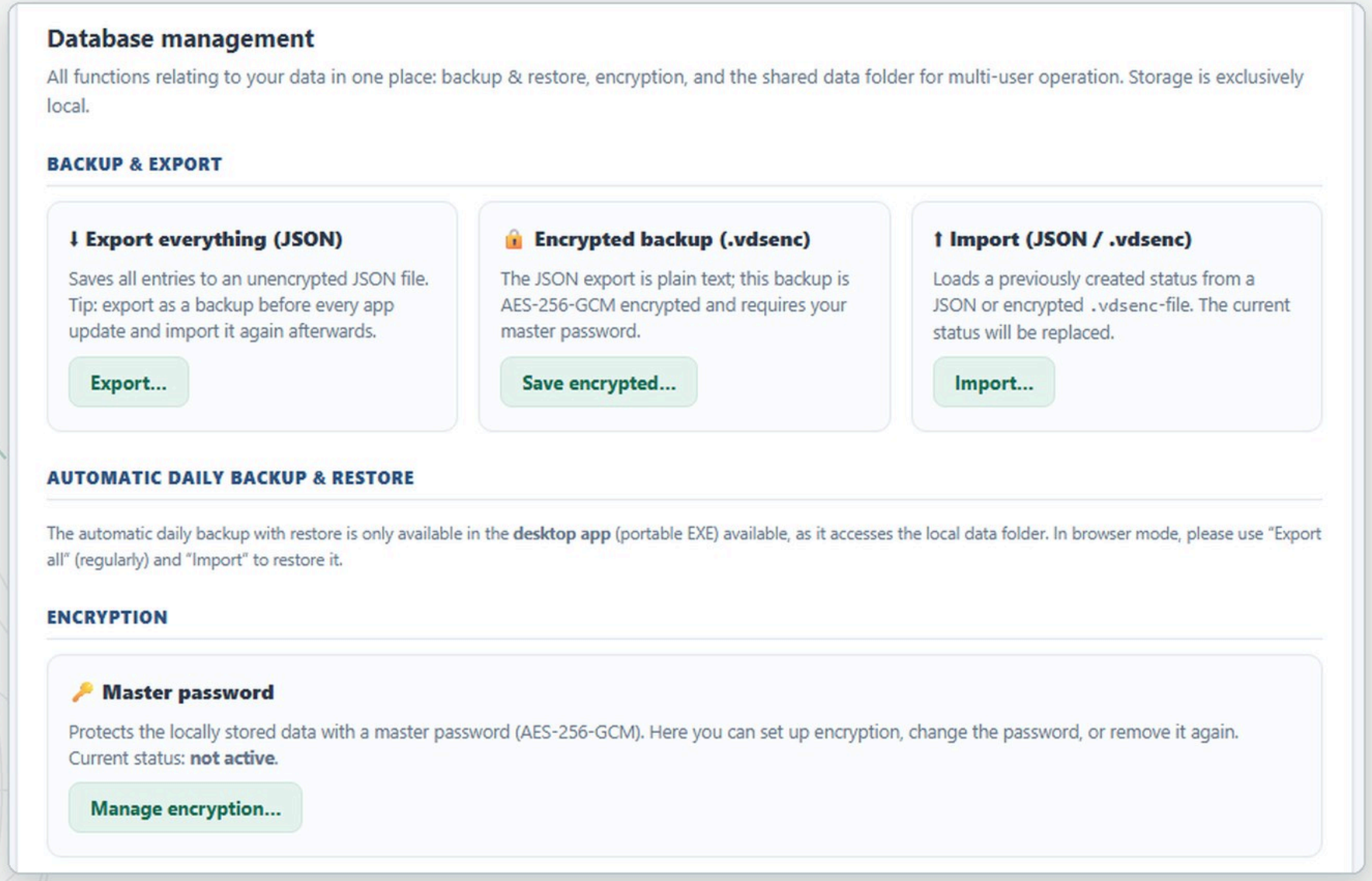


- Local model or EU provider
- A baseline assessment from your own data
- Every text stays a draft

CLOSING

Your data, your evidence

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



TSMONDO IT-Security & Compliance

Thank you.

tsmondo.eu · Münster

Compliance you can evidence, step by step.