NIS2 Gap Analysis Report

Prepared for: Mittelstand IT Services GmbH · **Prepared by:** NIS2Ready (Saevelis) · Marcos Leite · **Version:** 1.0
Confidentiality: CONFIDENTIAL: for internal use of Mittelstand IT Services GmbH and its board

43

out of 100 · NIS2 readiness score

Partial

Partial readiness: some controls exist, major gaps remain.

Borderline	**3**	**3–5**	**€3,000–8,000**
IN SCOPE OF NIS2	CRITICAL / TOP GAPS	MONTHS TO 70/100	EST. REMEDIATION COST

Executive Summary

Mittelstand IT Services GmbH has completed a NIS2 readiness assessment mapped to Article 21 of Directive (EU) 2022/2555 (NIS2) and the applicable national transposition. This report summarizes the current cybersecurity posture, identifies gaps against the 10 core security requirements of Art. 21(2), and provides a prioritized action plan with cost estimates.

In scope of NIS2?	**Borderline: confirm** — Important entity (confirm)
Applicable national law	Germany: NIS2UmsuCG (amended BSIG), in force. Registration in the BSI-Portal is mandatory and the deadline has already passed; new entities must register within 3 months. Authority: BSI.
Overall score	**43 / 100** (Partial)
Max. fine exposure	up to **€10M or 2%** of global turnover (essential) or **€7M or 1.4%** (important), Art. 34
Estimated effort to reach 70/100	3–5 months
Estimated remediation cost	€3,000–8,000 (mostly tools and time, not consulting)

> **Bottom line:** Mittelstand IT Services GmbH is partially prepared for NIS2. The most urgent gaps are Risk Analysis & Security Policy, Supply Chain Security, Effectiveness Assessment. With the action plan in section

> 6, the company can reach a demonstrably compliant posture within 3–5 months, for a fraction of the €5,000–15,000 a consulting firm would charge for the same assessment. A documented, prioritized gap analysis is the first evidence of good faith ("demonstrable progress") that regulators and customers ask for.

1. Scope Determination

CRITERION	COMPANY STATUS	IN SCOPE?
Employees (threshold: 50+)	50-249	Yes
Annual turnover / balance (threshold: 10M+)	lt10	No
Sector	IT / digital services (incl. managed services)	Yes (Annex I)
Supply chain to in-scope entity	IT / digital services (incl. managed services)	Check
Likely classification		**Important entity (confirm)**

Meets one threshold but not both. Member states may still include the entity (sector risk, Annex I). Confirm with the national competent authority. Sector is in Annex I (high criticality), which increases the likelihood of being considered in scope.

1.1 National transposition (applies to you)

Germany: NIS2UmsuCG (amended BSIG), in force. Registration in the BSI-Portal is mandatory and the deadline has already passed; new entities must register within 3 months. Authority: BSI.

1.2 Incident reporting readiness (Art. 23)

STAGE	DEADLINE	STATUS
Early warning	≤24h after becoming aware	**Not ready / verify**
Full notification	≤72h	**Not ready / verify**
Final report	≤1 month	Documented process required

A missed 72h notification can itself trigger sanctions, regardless of the incident's impact. Report to the national authority: [DE: BSI-Portal/MIP · NL: MijnNCSC · PT: CNCS · FR: ANSSI · ES: INCIBE/CNPIC].

1.3 Governance (Art. 20)

NIS2 holds **management personally liable** for non-compliance (Art. 20(2)). Documented board-level engagement (approvals, minutes, training records) is part of demonstrating good faith, and is the first thing an auditor or a large customer asks for.

2. Category Scores

#	CATEGORY		SCORE	SEVERITY
1	Risk Analysis & Security Policy		22/100	Critical
2	Incident Handling		44/100	Partial
3	Business Continuity & Backups		33/100	Critical

#	CATEGORY		SCORE	SEVERITY
4	Supply Chain Security		22/100	Critical
5	Secure Systems Acquisition & Development		56/100	Partial
6	Effectiveness Assessment		22/100	Critical
7	Cyber Hygiene & Training		56/100	Partial
8	Cryptography & Encryption		67/100	Partial
9	HR Security, Access Control & Asset Management		56/100	Partial
10	MFA & Secure Communications		67/100	Partial

Benchmark: an SME without prior ISMS work typically scores 30–50. Companies with ISO 27001 or mature GDPR processes typically score 60–80.

3. Gap Analysis

For each category: the legal requirement, the current state from your answers, and the risk of inaction.

Risk Analysis & Security Policy: 22/100 Critical Art. 21(2)(a)

Requirement (Art. 21(2)(a)): Policies on risk analysis and security of information systems and networks (documented, approved, reviewed at least annually and after major changes).

Current state (from your answers): 0 of 3 controls fully in place, 2 partial, 1 missing. Responses:

- **Missing** Does the company have a documented cybersecurity risk analysis?
- **Partially** Is there a formally approved information security policy covering NIS2 areas?
- **Partially** Is the risk analysis reviewed at least annually and after major changes?

Risk of inaction: This is the first thing regulators and customers ask for. Without a documented risk analysis, compliance cannot be demonstrated regardless of technical controls, and management exposure begins here (Art. 20 personal liability).

Incident Handling: 44/100 Partial Art. 21(2)(b)

Requirement (Art. 21(2)(b)): Incident prevention, detection and handling, including notification obligations (24h early warning / 72h notification / 1 month final report, Art. 23).

Current state (from your answers): 0 of 3 controls fully in place, 2 partial, 0 missing. Responses:

- **Partially** Is there a documented incident response plan?
- **Partially** Are security incidents detected and logged in a systematic way?
- Not answered Are staff aware of how and to whom to report a security incident?

Risk of inaction: In an incident, the company would likely exceed the 72h notification deadline, triggering supervisory follow-up on top of the incident itself. Untested response also means longer downtime.

Business Continuity & Backups: 33/100 Critical Art. 21(2)(c)

Requirement (Art. 21(2)(c)): Business continuity, backup management and disaster/crisis recovery, with tested restores and defined RTO/RPO.

Current state (from your answers): 0 of 3 controls fully in place, 1 partial, 1 missing. Responses:

- **Missing** Are critical data and systems backed up regularly, stored separately?
- **Partially** Has the company tested restoring from backup in the last 12 months?
- Not answered Is there a basic disaster recovery / crisis management plan?

Risk of inaction: A ransomware attack or fire destroying primary data and backups together is a single point of failure, with contractual and regulatory consequences on top of the operational ones.

Supply Chain Security: 22/100 Critical Art. 21(2)(d)

Requirement (Art. 21(2)(d)): Security of the supply chain and relationships with direct suppliers, including security requirements in contracts and risk evaluation before onboarding.

Current state (from your answers): 0 of 3 controls fully in place, 2 partial, 1 missing. Responses:

- **Missing** Does the company assess the security of its main suppliers?
- **Partially** Do supplier contracts include security requirements?
- **Partially** Is there a process for evaluating third-party security risks before onboarding?

Risk of inaction: NIS2 explicitly requires supply chain measures, and customer contracts will start demanding evidence. A breach via a contractor is attributed to the company.

Secure Systems Acquisition & Development: 56/100 Partial Art. 21(2)(e)

Requirement (Art. 21(2)(e)): Security in the acquisition, development and maintenance of systems, including vulnerability handling and disclosure.

Current state (from your answers): 0 of 3 controls fully in place, 1 partial, 0 missing. Responses:

- **Partially** Are new systems evaluated for security before deployment?
- Not answered Is there a process to test and approve changes to production systems?
- Not answered Does the company track and patch known vulnerabilities in time?

Risk of inaction: Unpatched or unvetted systems are the most common entry point for attacks; vulnerability management is a core NIS2 expectation.

Effectiveness Assessment: 22/100 Critical Art. 21(2)(f)

Requirement (Art. 21(2)(f)): Policies and procedures to assess the effectiveness of cybersecurity measures (audits, tests, reviews, KPIs).

Current state (from your answers): 0 of 3 controls fully in place, 2 partial, 1 missing. Responses:

- **Missing** Does the company regularly test whether security measures actually work?
- **Partially** Are security decisions based on documented evidence?
- **Partially** Are there defined metrics / KPIs for security?

Risk of inaction: Without testing and KPIs, controls decay silently and compliance cannot be evidenced to the regulator, customers or insurers.

Cyber Hygiene & Training: 56/100 Partial Art. 21(2)(g)

Requirement (Art. 21(2)(g)): Basic cyber hygiene practices and cybersecurity training, with completion records and company-specific risks.

Current state (from your answers): 0 of 3 controls fully in place, 1 partial, 0 missing. Responses:

- **Partially** Are all staff trained on basic cyber hygiene at least annually?
- Not answered Is there a clear process for phishing / suspicious email handling?
- Not answered Is training mandatory for new employees and company-specific?

Risk of inaction: Staff are the first line of defense; without training and phishing awareness, most incidents start with a single click.

Cryptography & Encryption: 67/100 Partial Art. 21(2)(h)

Requirement (Art. 21(2)(h)): Policies and procedures regarding the use of cryptography and encryption (devices, communications, key management).

Current state (from your answers): 0 of 3 controls fully in place, 0 partial, 0 missing. Responses:

- Not answered Are company devices' hard drives encrypted?
- Not answered Are communication channels with sensitive data encrypted?
- Not answered Is there a policy on encryption and key management?

Risk of inaction: Unencrypted devices and channels expose client and company data; lack of a policy makes the posture hard to evidence.

HR Security, Access Control & Asset Management: 56/100 Partial Art. 21(2)(i)

Requirement (Art. 21(2)(i)): Human resources security, access control policies and asset management (need-to-know, reviews, leavers, inventory).

Current state (from your answers): 0 of 3 controls fully in place, 1 partial, 0 missing. Responses:

- **Partially** Is access granted on a need-to-know basis and reviewed?
- Not answered Is there an up-to-date asset inventory?
- Not answered Are accounts of leavers revoked promptly?

Risk of inaction: Unreviewed access and missing inventory create hidden exposure; leavers with active accounts are a classic audit finding.

MFA & Secure Communications: 67/100 Partial Art. 21(2)(j)

Requirement (Art. 21(2)(j)): Multi-factor authentication (or continuous authentication), secured voice/video/text communications and secured emergency communication systems.

Current state (from your answers): 0 of 3 controls fully in place, 0 partial, 0 missing. Responses:

- Not answered Is MFA enforced on email, cloud and VPN for all users?
- Not answered Are privileged / admin accounts protected with MFA?
- Not answered Are emergency communication channels defined and tested?

Risk of inaction: MFA is the single most effective control against credential theft; missing it is the first question any auditor asks.

4. Prioritized Action Plan

Prioritization: impact × effort, quick wins first. Total estimated year-1 budget: €3,000–8,000 (versus €28k–150k if done by external consultants, 2026 market benchmarks).

4.1 Quick wins (0–4 weeks)

#	ACTION	CAT.	EFFORT	EST. COST
1	Enforce MFA on all email / cloud / VPN accounts	10	1–2 days	€0 (licenses may apply)
2	Enable disk encryption on all laptops	8	1 day	€0
3	Schedule automated off-site backups + test a restore	3	1 day	€30–80/mo
4	Document incident response roles (2-page plan) with 24h/72h notification path	2	half day	€0
5	Run annual phishing awareness training for all staff	7	1 day	€0–500
6	Document the access review process; schedule first quarterly review	9	half day	€0

4.2 Short term (1–3 months)

#	ACTION	CAT.	EFFORT	EST. COST
1	Formalize and approve the information security policy	1	1–2 days	€0 (template)
2	Create asset inventory + access review process	9	2–3 days	€0
3	Add security clauses to top 5 supplier contracts	4	2 days	Legal €500–1,500
4	Establish patch management process (14-day critical deadline)	5	1 day	€0
5	Draft the 24h / 72h incident notification template	2	half day	€0

4.3 Strategic (3–12 months)

#	ACTION	CAT.	EFFORT	EST. COST
1	Annual risk analysis process + documented management review	1, 6	Ongoing	€0–3,000/yr
2	Incident response tabletop exercise	2	1 day	€0–1,500
3	Vendor security assessment framework for new suppliers	4	1 week	€0–2,000
4	Security KPIs dashboard reviewed quarterly	6	1 week	€0–500
5	Management cybersecurity training (Art. 20 governance)	Gov	1 day	€0–1,000
6	Consider ISO 27001-aligned controls	All	6–12 months	€8k–15k

5. Compliance Roadmap (12 months)

MONTH	MILESTONE	EST. SCORE
M1	Quick wins implemented; security policy drafted; MFA verified	**51**
M2	Training completed; backups tested; notification template ready	**57**
M3	Asset inventory + access controls in place; first risk analysis started	**63**
M6	First documented risk analysis; supplier clauses signed; KPIs defined	**69**
M9	Incident response exercise performed; management reviews on schedule	**73**
M12	Re-assessment with evidence pack (target: 70+)	**70**

Re-take the free assessment at any time to measure progress. Many companies run it quarterly and share the delta with their board, insurer or customers as evidence of continuous improvement.

6. What Good Looks Like (evidence checklist)

- **1.** A documented, annually reviewed risk analysis (signed by management)
- **2.** An approved security policy covering all 10 categories of Art. 21(2)
- **3.** Incident response plan with defined roles and tested escalation + 24h/72h notification template
- **4.** Backup logs with tested restores and an off-site copy
- **5.** Supplier security requirements in contracts
- **6.** MFA enforced everywhere, with a compliance report
- **7.** Annual training with completion records
- **8.** Device and communication encryption
- **9.** Access reviews with records; revoked leavers
- **10.** KPIs and management review minutes (continuous improvement)

7. Crosswalk (existing frameworks)

If you already operate ISO 27001 or GDPR processes, map your existing evidence to this table instead of starting from zero.

NIS2 ART. 21(2)	ISO 27001:2022	NIST CSF 2.0
(a) Risk analysis & policy	5.2, 6.1, 8.2	GV.RM, GV.PO
(b) Incident handling	5.24–5.28	DE, RS
(c) Business continuity	5.29, 5.30, 8.5	RC, PR
(d) Supply chain	5.19–5.22	ID.SC, GV.SC
(e) Secure acquisition/dev	8.25–8.31	PR.PS
(f) Effectiveness assessment	9.1, 9.2, 9.3	GV, ME
(g) Hygiene & training	6.3, 7.2–7.4	PR.AT
(h) Cryptography	8.24	PR.DS
(i) HR, access, assets	5.2, 5.9–5.18, 8.1–8.3	PR.AA, ID.AM
(j) MFA & secure comms	8.5, 8.6	PR.AA, PR.DS

8. Market Context (2026)

- ~160,000 entities are estimated to be in scope of NIS2 across the EU (16× NIS1).
- ECSO estimates 1,400–2,800 person-hours for first-year compliance for a typical entity.
- 64% of incidents reported under NIS2 also involve personal data (GDPR overlap).
- Enforcement is active: Germany's BSI registration window has closed; the Netherlands' Cyberbeveiligingswet entered into force on 15 August 2026; the Commission referred Spain and France to the CJEU in July 2026.
- The Commission's proposed 2026 simplification package would ease some obligations, but it is not yet law. Plan against the current text.

9. Disclaimer & Confidentiality

This report is provided for information purposes only and does not constitute legal advice or a certification of compliance with the NIS2 Directive or any national implementing legislation. Companies should consult their national competent authority and, where appropriate, legal counsel. Self-reported answers have not been independently verified. This report contains confidential information of Mittelstand IT Services GmbH and is intended solely for its internal use.