Beispiel-Auswertung

NIS-2 Reifegrad-Check

Musterfirma GmbH · Maschinenbau · 180 Mitarbeitende

BERICHTSDATUM	NIS-2-EINSTUFUNG	GESAMT-REIFEGRAD
11.06.2026	Wichtige Einrichtung	Teilweise (38 %)

Management-Summary

Die Musterfirma GmbH fällt als produzierendes Unternehmen mit 180 Mitarbeitenden und einem Jahresumsatz über 50 Mio. € in den Anwendungsbereich des NIS2UmsuCG als **wichtige Einrichtung**. Damit greifen die Sicherheitsanforderungen nach Art. 21, die Meldepflichten nach Art. 23 sowie die Aufsichts- und Sanktionsregime. Die persönliche Verantwortung der Geschäftsführung gemäß § 38 NIS2UmsuCG ist gegeben.

Der Gesamt-Reifegrad liegt bei **38 %** — drei der zehn Pflichtbereiche sind **kritisch**, sechs **teilweise umgesetzt**, einer **gut**. Ohne fokussierte Maßnahmen ist eine fristgerechte Compliance bis zum nationalen Stichtag nicht erreichbar. Mit den drei vorgeschlagenen Schwerpunkt-Maßnahmen (Top-3) lassen sich die größten Risiken in einem Zeitraum von ca. 4–6 Monaten und einem Budgetrahmen von **40.000–70.000 €** adressieren.

Wir empfehlen, die Roadmap in einem 90-Tage-Sprint zu starten — Schwerpunkt: Incident-Response und Meldewesen, Lieferketten-Sicherheit, sowie Schulung von Geschäftsführung und Schlüsselrollen.

Reifegrad-Übersicht — Pflichtmaßnahmen Art. 21

Bewertung in drei Stufen: ● **Kritisch** (sofortiger Handlungsbedarf), ● **Teilweise** (Konzept vorhanden, Umsetzung lückenhaft), ● **Gut** (im Soll oder darüber).

#	Pflichtmaßnahme Art. 21 NIS-2	Reifegrad	Bemerkung
1	Risikoanalyse und Konzepte für die Sicherheit der Informationssysteme	● Teilweise	ISO-27001-Risikobewertung vorhanden, NIS-2-Kontext-Erweiterung fehlt
2	Bewältigung von Sicherheitsvorfällen (Incident Response)	● Kritisch	Kein dokumentierter Prozess, keine 24/72-h-Meldekette etabliert
3	Aufrechterhaltung des Betriebs (Backup, Wiederherstellung, BCM)	● Teilweise	Backup-Konzept produktiv, BCM/ITSCM nur fragmentarisch

#	Pflichtmaßnahme Art. 21 NIS-2	Reifegrad	Bemerkung
4	Sicherheit der Lieferkette	● Kritisch	Lieferanten-Risiko-Inventar fehlt, keine Security-Klauseln in Verträgen
5	Sicherheit in Beschaffung, Entwicklung und Wartung	● Teilweise	Härtungs-Standards vorhanden, Patch-Compliance bei 73 %
6	Maßnahmen zur Bewertung der Wirksamkeit	● Kritisch	Kein internes Audit-Programm, kein Wirksamkeits-Reporting
7	Grundlegende Cyberhygiene-Praktiken und Schulungen	● Teilweise	GF nicht geschult, jährliche MA-Schulung läuft (LV-Quote 81 %)
8	Konzepte und Verfahren für Kryptografie und Verschlüsselung	● Teilweise	BitLocker + TLS aktiv, keine zentrale Schlüsselverwaltung
9	Sicherheit des Personals, Zugriffskontrolle, Asset-Management	● Gut	Tier-Modell + JML-Prozess + CMDB-Pflege im Soll
10	Einsatz von Mehrfaktor-Authentifizierung	● Teilweise	MFA in M365 aktiv, jedoch nicht für VPN/IRM/SAP-Backend erzwungen

Top-3-Maßnahmen — Empfohlene Reihenfolge

Die folgenden Maßnahmen schließen die größten Lücken aus der Ampel-Übersicht. Reihenfolge ergibt sich aus dem Verhältnis Risiko-Reduktion zu Umsetzungs-Aufwand und der Abhängigkeit untereinander.

1. Incident-Response und 24/72-h-Meldewesen aufbauen ● Kritisch

• Incident-Response-Prozess (Detection → Triage → Eskalation → Behebung → Lessons-Learned) dokumentieren

• Meldekette an BSI für signifikante Sicherheitsvorfälle inkl. Vorlagen für 24-h-Frühwarnung, 72-h-Erstmeldung und 1-Monats-Abschlussbericht etablieren

• On-Call-Roster für IT-Leitung + Stellvertretung + externer SOC/MDR, technische Eskalationswege getestet

• Vorfall-Tabletop-Übung mit Geschäftsführung als Wirksamkeits-Nachweis durchführen

Aufwand: ca. 12–18 Personentage über 6 Wochen | **Kostenkorridor:** 14.000–22.000 € (eigene Aufwände + 1 Tabletop-Workshop extern)

2. Lieferketten-Sicherheit strukturieren ● Kritisch

• Lieferanten-Risiko-Inventar erstellen: alle kritischen IKT-Lieferanten + Cloud-Dienste + Wartungs-Verträge

• Risiko-Klassifizierung in 4 Stufen (Tier 1–4) abhängig von Schutzbedarf und Datenzugriff

• Standard-Security-Klausel inkl. AVV, Sub-Auftragnehmer-Regelung und Meldepflicht in Verträge integrieren

• Jährliche Reassessment-Kadenz für Tier-1- und Tier-2-Lieferanten, Onboarding-Check für neue Lieferanten

Aufwand: ca. 15–20 Personentage über 8 Wochen | **Kostenkorridor:** 16.000–24.000 € (eigene Aufwände + Vertrags-Reviews durch externe Beratung)

3. Cyberhygiene-Schulung Geschäftsführung und Schlüsselrollen ● Teilweise

• Geschäftsführungs-Briefing zu NIS-2-Pflichten, Organhaftung und Aufsichtsrechten des BSI (2 Stunden, dokumentiert)

• Vertiefungs-Schulung für IT-Leitung, ISB, Datenschutzbeauftragten und Notfall-Stab (1 Tag)

• Awareness-Programm für alle Mitarbeitenden ausbauen (Phishing-Simulation, Quartals-Mikrolearnings)

• Wirksamkeits-Messung über Phishing-Klick-Rate, Trainings-Abdeckung und Stichproben

Aufwand: ca. 6–10 Personentage über 4 Wochen | **Kostenkorridor:** 8.000–12.000 € (Schulungs-Materialien, Awareness-Lizenzen, Trainer-Tag)

Detail-Befunde (Auszug)

Bereich 2 — Bewältigung von Sicherheitsvorfällen

Soll-Anforderung: Art. 21 Abs. 2 lit. b NIS-2 fordert ein Konzept zur Bewältigung von Sicherheitsvorfällen einschließlich Detektion, Eindämmung, Behebung und Nachbereitung. Art. 23 ergänzt die Meldepflichten an das BSI in den Zeitfenstern 24 h (Frühwarnung), 72 h (Erstmeldung) und 1 Monat (Abschlussbericht).

Ist-Zustand: Es existieren technische Detektions-Werkzeuge (SIEM bei MSP, Defender für Endpoint im M365 E5-Tenant). Ein dokumentierter Prozess für die Bewältigung von Vorfällen, klare Verantwortlichkeiten und eine getestete Meldekette an das BSI fehlen. Ein Vorfall in Q4/2025 wurde ad-hoc bearbeitet, ohne dass eine Lessons-Learned-Dokumentation entstanden ist.

Risiko: Eine Versäumung der 24- oder 72-Stunden-Meldepflicht führt zu Bußgeldern bis 7 Mio. € (wichtige Einrichtung), zusätzlich zur persönlichen Haftung der Geschäftsführung. Eine fehlende Wiederherstellungs-Fähigkeit erhöht den finanziellen Schaden bei einem Ransomware-Vorfall.

Empfehlung: siehe Top-3-Maßnahme 1.

Bereich 4 — Sicherheit der Lieferkette

Soll-Anforderung: Art. 21 Abs. 2 lit. d NIS-2 verlangt Sicherheits-Anforderungen für Lieferanten und Dienstleister, die direkt oder indirekt Zugriff auf die Netz- und Informationssysteme der Einrichtung haben. Lieferanten-Risiken müssen identifiziert und behandelt werden.

Ist-Zustand: Es gibt eine Liste aktiver Lieferanten in der Buchhaltung. Eine Inventarisierung der IKT-Lieferanten mit Schutzbedarf-Bewertung und Sub-Auftragnehmer-Mapping existiert nicht. Vertragsstandards enthalten keine Security-Klauseln oder Meldepflichten der Lieferanten.

Risiko: Lieferketten-Angriffe sind statistisch die häufigste Eintrittstür in mittelständische Industrieunternehmen. Ohne strukturiertes Lieferanten-Management können Schwachstellen in Wartungs-Zugängen oder bei Software-Lieferanten unerkannt bleiben — siehe SolarWinds, Kaseya, MOVEit-Wellen.

Empfehlung: siehe Top-3-Maßnahme 2.

Bereich 6 — Maßnahmen zur Bewertung der Wirksamkeit

Soll-Anforderung: Art. 21 Abs. 2 lit. f NIS-2 fordert Konzepte und Verfahren, um die Wirksamkeit der Risikomanagement-Maßnahmen zu bewerten. In der Praxis bedeutet das ein internes Audit-Programm, KPIs und ein Management-Review.

Ist-Zustand: Externe Pen-Tests werden alle 24 Monate beauftragt. Ein internes Audit-Programm über die Risikomanagement-Maßnahmen existiert nicht. Kennzahlen werden nicht systematisch erhoben oder an die Geschäftsführung berichtet.

Empfehlung: Aufbau eines schlanken internen Audit-Programms (jährlich, themen-rotierend), Definition von 6–8 KPIs (Patch-Compliance, MFA-Abdeckung, Phishing-Klick-Rate, Vorfall-Meldungen, Wiederanlauf-Übung, Lieferanten-Reassessments, MA-Schulungs-Quote, Stichprobe Zutritts-Berechtigungen).

Methodik und Grundannahmen

Die Bewertung basiert auf Selbstauskunft im strukturierten NIS-2-Fragebogen (87 Items) sowie einem Erstgespräch mit Geschäftsführung und IT-Leitung am 03.06.2026 (60 min). Die Aussagen wurden plausibilitätsgestützt eingeordnet, jedoch nicht durch Evidence-Stichproben überprüft. Die Bewertung stellt ein Self-Assessment mit qualifizierter Außensicht dar, kein formales Audit nach ISO 27001 oder BSI IT-Grundschutz.

Mapping: Jede Pflichtmaßnahme nach Art. 21 NIS-2 wurde gegen ISO 27001:2022 Annex A (Maßnahmen-Katalog A.5–A.8) und gegen BSI IT-Grundschutz-Bausteine gespiegelt. Bestehende ISO-27001-Implementierungen werden anerkannt und nicht doppelt verlangt.

Reifegrad-Stufen: Kritisch (0–25 % Umsetzung), Teilweise (26–75 %), Gut (76–100 %). Die Stufen orientieren sich an der CMMI-Logik (Initial, Repeatable, Defined, Managed, Optimizing).

Quellen und Referenzen

• NIS2UmsuCG — Gesetzentwurf der Bundesregierung, Drucksache 20/13184
• Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie) — ABl. EU L 333/80 vom 27.12.2022
• BSI-Standard 200-2 (IT-Grundschutz-Methodik)
• ISO/IEC 27001:2022 — Information security management systems
• ISO/IEC 27002:2022 — Information security controls
• BSI-Standard 200-4 (Business Continuity Management)

Hinweis zu diesem Beispiel-Dokument: Dieser Bericht ist eine anonymisierte Beispiel-Auswertung. Daten, Befunde und Empfehlungen sind plausibilitätsgestützt konstruiert und beziehen sich nicht auf ein reales Unternehmen. Ihr eigener Reifegrad-Bericht wird auf Basis Ihres Fragebogen-Rücklaufs erstellt und kann inhaltlich, strukturell und in Tonalität abweichen.

Erstellt von: **Thorsten Schmitz-Hübsch** · ISO 27001 Lead Auditor · ISACA CISM · TSMONDO UG (haftungsbeschränkt) · Münster · t@tsmondo.de · +49 162 9691436