NEXUS
MANAGEMENT CONSULTING

# NIS2-Compliance

Der pragmatische Umsetzungsleitfaden für Geschäftsführung und IT-Verantwortliche

Whitepaper | März 2026

**Simon Schilling**
Geschäftsführer & Principal Consultant
Nexus Management Consulting GmbH | nexuscon.net

# Management Summary

Die NIS2-Richtlinie ist seit Dezember 2025 in deutsches Recht überführt. Rund 29.500 Unternehmen sind betroffen. Die Geschäftsleitung haftet persönlich. Bußgelder bis 10 Mio. EUR oder 2 % des Jahresumsatzes drohen.

> Dieses Whitepaper beantwortet vier Kernfragen: Wer ist betroffen? Was bedeutet die persönliche Haftung? Wie sieht ein pragmatischer Umsetzungsfahrplan aus? Und welche Quick Wins können Sie sofort umsetzen?

# 1. NIS2 im Überblick

NIS2 (Richtlinie (EU) 2022/2555) ist die Nachfolgerin der NIS-Richtlinie von 2016 und stellt einen Paradigmenwechsel in der europäischen Cybersicherheitsregulierung dar. Die Richtlinie wurde am 27. Dezember 2022 im Amtsblatt der EU veröffentlicht und musste bis zum 17. Oktober 2024 in nationales Recht umgesetzt werden. In Deutschland erfolgte die Umsetzung durch das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG), das im Dezember 2025 in Kraft getreten ist.

Der Anwendungsbereich wurde massiv erweitert: Von ca. 4.500 auf rund 29.500 betroffene Unternehmen allein in Deutschland – eine Steigerung um über 550 %. Viele Unternehmen, die bisher nicht unter die KRITIS-Regulierung fielen, sind nun erstmals von umfassenden Cybersicherheitspflichten betroffen.

## 1.1 Was hat sich gegenüber NIS1 geändert?

| Aspekt | NIS1 (2016) | NIS2 (seit 2025) |
|---|---|---|
| Betroffene (DE) | ca. 4.500 | ca. 29.500 (+550 %) |
| Sektoren | 7 | 18 |
| Meldepflichten | 72 Stunden | 24h + 72h + 1 Monat |
| Haftung | Unternehmen | Persönlich (Geschäftsleitung) |
| Bußgelder | Bis 100.000 EUR | Bis 10 Mio. EUR oder 2 % Umsatz |
| Supply Chain | Kaum | Explizite Anforderungen |
| Durchsetzung | Begrenzt | Aktive BSI-Prüfungen |

## 1.2 Betroffene Sektoren

| Sektor | Beispiele | Kategorie |
|---|---|---|
| Energie | Strom, Gas, Öl, Fernwärme | Besonders wichtig |
| Gesundheitswesen | Krankenhäuser, Labore, Pharma | Besonders wichtig |
| Transport | Luftfahrt, Schiene, Wasser, Straße | Besonders wichtig |
| Digitale Infrastruktur | Rechenzentren, Cloud, DNS | Besonders wichtig |
| Finanzmarkt | Banken, Versicherungen | Besonders wichtig |
| Öffentliche Verwaltung | Bundes-/Landesbehörden | Besonders wichtig |
| Lebensmittel | Großhandel, Verarbeitung | Wichtig |
| Abfallwirtschaft | Entsorgung, Recycling | Wichtig |

# 2. Persönliche Haftung der Geschäftsführung

> **Persönliche Haftung**
> Die Geschäftsleitung haftet persönlich für die Umsetzung der Cybersicherheitsmaßnahmen. Diese Pflicht ist nicht delegierbar.

## 2.1 Konkrete Pflichten

- **Billigung und Überwachung:** Die GF muss Risikomanagementmaßnahmen billigen und überwachen
- **Cybersicherheitsschulungen:** Nachweisliche, regelmäßige Teilnahme
- **Persönliche Haftung:** Bei Pflichtverletzung gegenüber dem Unternehmen
- **Nicht delegierbar:** Auch die Bestellung eines CISO entbindet die GF nicht

## 2.2 Sanktionen

| Kategorie | Bußgeld | Weitere Konsequenzen |
|---|---|---|
| Bes. wichtige Einr. | 10 Mio. EUR oder 2 % Umsatz | Schadensersatz, Aufsichtsmaßnahmen |
| Wichtige Einrichtungen | 7 Mio. EUR oder 1,4 % Umsatz | Schadensersatz, Prüfungen |
| GF persönlich | Persönliche Haftung | D&O, ggf. Untersagung der GF-Tätigkeit |

## 2.3 Absicherung

- **Dokumentation:** Alle Beschlüsse und Schulungsteilnahmen schriftlich festhalten
- **D&O-Versicherung:** Auf NIS2-Kompatibilität prüfen
- **Regelmäßiges Reporting:** Mindestens quartalsweise an die GF
- **Incident-Response testen:** Regelmäßige Tabletop-Exercises der 24h/72h-Meldekette

# 3. Die 10 NIS2-Anforderungsdomänen

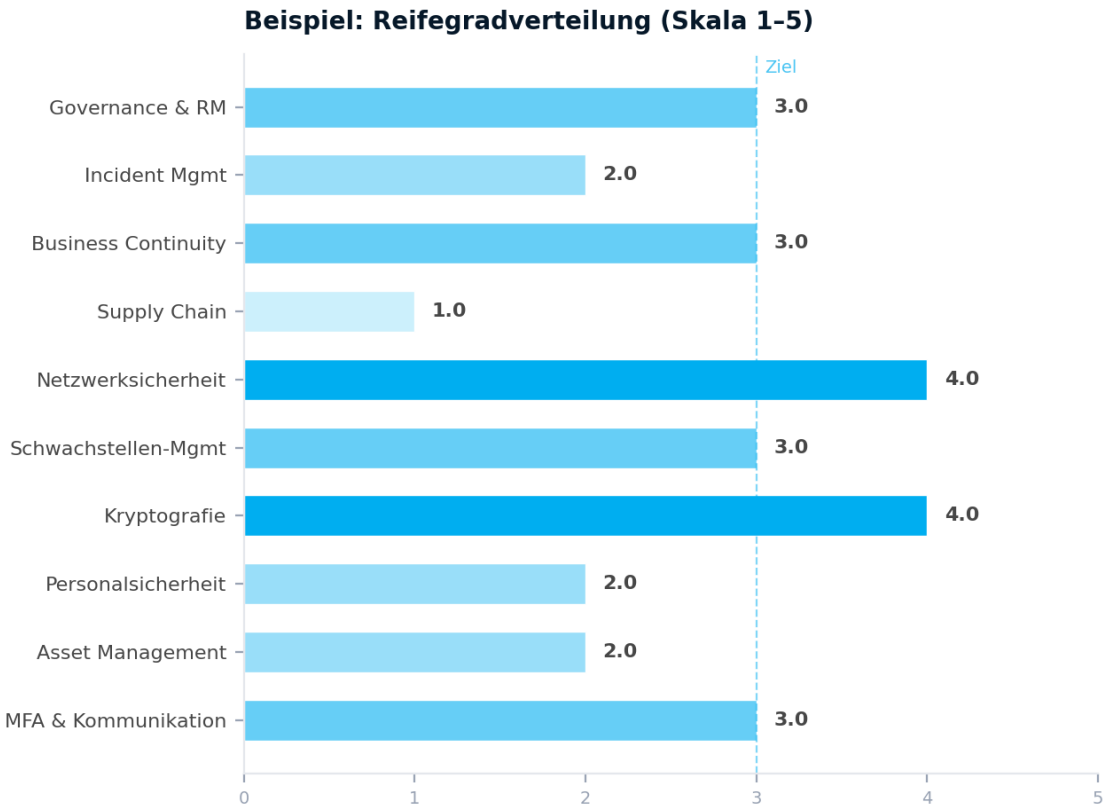
NIS2 fordert Maßnahmen in 10 zentralen Bereichen. Ein professionelles Assessment prüft über 125 Punkte systematisch in diesen Domänen:

| # | Domäne | Prüfpunkte | Kernfrage |
|---|---|---|---|
| 1 | Governance & Risikomanagement | 15 | Cyberstrategie, ISMS, GF-Einbindung? |
| 2 | Incident Management | 15 | 24h/72h-Meldekette, CSIRT, Übungen? |
| 3 | Business Continuity | 15 | BIA, BCP, DRP, RTO/RPO? |
| 4 | Supply Chain Security | 12 | Lieferantenbewertung, Verträge? |
| 5 | Netzwerksicherheit | 15 | Segmentierung, SIEM, Pentests? |
| 6 | Schwachstellenmanagement | 11 | Patch-SLAs, Vulnerability |

| | | | |
|---|---|---|---|
| | | | Disclosure? |
| 7 | Kryptografie | 10 | Verschlüsselung, Key Management? |
| 8 | Personalsicherheit | 11 | Least Privilege, PAM, Access Reviews? |
| 9 | Asset Management | 10 | Inventar, Klassifizierung, Shadow IT? |
| 10 | MFA & Kommunikation | 11 | MFA, SSO, sichere Kanäle? |

## 3.1 Typische Reifegradverteilung

Die folgende Grafik zeigt eine typische Reifegradverteilung, wie wir sie bei Assessments häufig antreffen:




## 3.2 Meldepflichten im Detail

Bei erheblichen Sicherheitsvorfällen gelten strikte Fristen:

| Frist | Pflicht | Inhalt |
|---|---|---|
| 24 Stunden | Frühwarnung an BSI | Erste Einschätzung des Vorfalls |
| 72 Stunden | Vorfallbericht | Bewertung, Schwere, Indikatoren |
| 1 Monat | Abschlussbericht | Ursache, Maßnahmen, grenzüberschreitende Auswirkungen |

# 4. Pragmatischer Umsetzungsfahrplan

Ein NIS2-Compliance-Programm lässt sich in vier Phasen umsetzen:


| Phase | Dauer | Ziel | Deliverables |
|---|---|---|---|
| 1. Assessment | 3–4 Tage | Standortbestimmung | Gap-Analyse, Risikomatrix, Maßnahmenplan, Bericht (40–60 S.) |
| 2. Framework | 3–4 Wochen | Konzeption | ISMS, Policies, Incident-Response-Plan, Risikomanagement-Methodik |
| 3. Implementierung | 8–24 Wochen | Umsetzung | Technische Controls, Schulungsprogramm, KPI-Framework |
| 4. Audit-Readiness | 2–4 Wochen | Nachweis | Pre-Audit, Dokumentationslandkarte, Betriebshandbuch |

# 5. Quick Wins: Sofort umsetzbar

Diese sechs Maßnahmen können Sie sofort umsetzen – ohne große Budgets:

> 1. MFA aktivieren für alle Remote-Zugänge und privilegierte Konten. Die wichtigste Einzelmaßnahme gegen Credential-basierte Angriffe.

> 2. Incident-Response-Plan erstellen mit BSI-Meldekette. Auch ein einfacher 2-Seiten-Plan ist besser als keiner.

> 3. Asset-Inventar anlegen – Sie können nur schützen, was Sie kennen.

- **4. Geschäftsleitung schulen:** Die persönliche Haftung verlangt nachweisliche Teilnahme
- **5. Lieferantenverträge prüfen:** Cybersicherheitsanforderungen vertraglich aufnehmen
- **6. Meldeprozess definieren:** Wer meldet in 24 Stunden an wen?

# 6. Kosten und Aufwand: Was NIS2 kostet

Die Kosten einer NIS2-Umsetzung variieren stark je nach Ausgangslage, Unternehmensgröße und IT-Komplexität. Laut einer Studie des Bundesverbands IT-Sicherheit (TeleTrusT, 2024) kalkulieren mittelständische Unternehmen im Schnitt 150.000–500.000 EUR für die vollständige NIS2-Implementierung. Dem stehen potenzielle Bußgelder von bis zu 10 Mio. EUR gegenüber.

Ein pragmatischer Ansatz mit klarer Priorisierung kann die Kosten erheblich senken:

| Phase | Typischer Aufwand | Was Sie bekommen |
|---|---|---|
| Readiness Assessment | 7.500–9.500 EUR | Gap-Analyse, Risikomatrix, Maßnahmenplan (40–60 S.) |
| Framework & Konzeption | 18.000–25.000 EUR | ISMS, Policies, Incident-Response-Plan |
| Implementierung | 30.000–150.000 EUR | Abhängig von Gaps: Controls, Schulungen, Tools |
| Audit-Readiness | 10.000–20.000 EUR | Pre-Audit, Dokumentation, Betriebshandbuch |
| Laufend: Virtual CISO | ab 5.000 EUR/Monat | Governance, Monitoring, Audit-Vorbereitung |

Der wichtigste Kostentreiber ist die Ausgangslage: Unternehmen mit bestehender ISO 27001-Zertifizierung können bis zu 60 % der Implementierungskosten sparen, weil viele Anforderungen bereits erfüllt sind.

# 7. Fazit & nächste Schritte

NIS2 ist geltendes Recht mit persönlicher Haftung der Geschäftsleitung. Die Anforderungen sind umfassend, aber mit einem strukturierten Vorgehen pragmatisch umsetzbar. Der wichtigste erste Schritt: Eine fundierte Standortbestimmung, die zeigt, wo Sie stehen und was priorisiert werden muss.

Kostenloser NIS2-Selbstcheck (10 Min.): nexuscon.net/nis2-selbstcheck

Professionelles Assessment (3–4 Tage, Festpreis): nexuscon.net/nis2-readiness-assessment

**→ Jetzt Erstgespräch vereinbaren**

# Quellen & Referenzen

Die folgenden Quellen wurden für dieses Whitepaper herangezogen:


- Europäisches Parlament (2022): Richtlinie (EU) 2022/2555 – NIS2-Richtlinie, Amtsblatt der EU, 27. Dezember 2022. → Quelle
- Bundesministerium des Innern (2025): NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG), Bundesgesetzblatt. → Quelle
- BSI (2025): „Betroffenheitsprüfung NIS-2" – Bundesamt für Sicherheit in der Informationstechnik. → Quelle
- BSI (2024): „IT-Grundschutz-Kompendium", Edition 2024. → Quelle
- ENISA (2024): „NIS2 Directive – Implementing Guidance", European Union Agency for Cybersecurity. → Quelle
- TeleTrusT (2024): „IT-Sicherheitslage und NIS2-Readiness im deutschen Mittelstand". → Quelle
- Bitkom (2024): „Wirtschaftsschutz 2024 – Spionage, Sabotage und Datendiebstahl", Bitkom Research. → Quelle
- ISO/IEC 27001:2022 – Informationssicherheitsmanagementsysteme – Anforderungen. → Quelle
- ISO 22301:2019 – Business Continuity Management Systems – Requirements. → Quelle
- DSGVO: Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung. → Quelle


*Stand: März 2026. Alle Angaben ohne Gewähr. Dieses Whitepaper stellt keine Rechtsberatung dar.*

# Über den Autor

## Simon Schilling

**Geschäftsführer & Principal Consultant**

Nexus Management Consulting GmbH | Stuttgart

AWS Solutions Architect | PRINCE2 | Azure Architect | TOGAF 9 | ITIL v3

Mit über 13 Jahren Erfahrung in der IT-Beratung hat Simon komplexe Transformationsprojekte bei T-Systems, Wipro und Q_PERIOR begleitet, bevor er 2023 Nexus gründete. Sein Fokus liegt auf der Integration von KI-Agenten in regulierte Geschäftsprozesse – von der Strategie über den PoC bis zum compliant-by-design Rollout.

Er verbindet technische Tiefe mit strategischer Beratung und Compliance-Expertise (EU AI Act, NIS2, DSGVO). Aktuelle Referenzprojekte: KI-Agenten für Anliegenmanagement (GKV/KRITIS), Workplace Architecture (Versicherung), SW-Lifecycle-Management (IT-Dienstleister), Sovereign Cloud Vergabe (öffentliche Verwaltung).

## Über Nexus Management Consulting

*„Nexus integriert KI-Agenten in regulierte Geschäftsprozesse – von der Strategie über den PoC bis zum compliant-by-design Rollout."*

Nexus Management Consulting ist eine spezialisierte Unternehmensberatung für regulierte Umfelder mit Sitz in Stuttgart. Wir unterstützen Unternehmen in den Bereichen Gesundheitswesen, Versicherung, KRITIS und öffentliche Verwaltung bei der Einführung von KI-Agenten und der Umsetzung regulatorischer Anforderungen.

### Leistungsportfolio

- **KI-Readiness Assessment** (5–7 Tage) – Reifegrad, Use Cases, Compliance-Check
- **Agentic AI Design Sprint** (3–4 Tage) – Agenten-Architektur und PoC-Spezifikation
- **KI-Agenten-Programm** (3–12 Monate) – End-to-End Steuerung
- **NIS2 / EU AI Act Compliance** – Vom Assessment bis zur Audit-Readiness
- **Fractional AI Officer / Virtual CISO** – Laufende Steuerung auf Abruf

## Kontakt aufnehmen

| | |
|---|---|
| **E-Mail** | simon.schilling@nexuscon.net |
| **Telefon** | +49 151 5472 6609 |
| **Web** | nexuscon.net |

Im Kaisemer 11 | 70191 Stuttgart | Nexus Management Consulting GmbH

**→ Jetzt Erstgespräch buchen**