aign.os

NIS2
DEUTSCHLAND 2026

Wie **AIGN OS** als betriebliches Governance-Betriebssystem Unternehmen unterstützt, die Anforderungen der NIS2-Richtlinie strukturiert, nachvollziehbar und zukunftsfähig umzusetzen.

Eine strategische Analyse zur Umsetzung der NIS2-Richtlinie, der neuen Management-Haftungsnormen und der entstehenden Risiken durch Agentic AI.

Autor:
Patrick Upmann
Architect of Systemic AI Governance
Founder & Creator of AIGN OS – The Operating System for Responsible AI Governance

Offizielles Länder-Dossier | Version 2026

EXECUTIVE SUMMARY

Mit der **NIS2-Richtlinie (EU 2022/2555)** entsteht erstmals ein europaweit harmonisiertes Sicherheitsniveau für Netz- und Informationssysteme. Betroffene Unternehmen müssen Maßnahmen zu Risikomanagement, Incident Response, Business Continuity, Lieferkettenüberwachung, Zugriffssicherheit, Kryptografie und Managementverantwortung umsetzen und dokumentieren.

Die Richtlinie definiert was zu tun ist – sie legt nicht fest, wie Unternehmen diese Vielzahl an Pflichten organisatorisch, technisch und dokumentarisch integrieren sollen.

Damit entsteht in der Praxis ein strukturelles Problem:
NIS2 betrifft viele Bereiche gleichzeitig, setzt hohe Nachweis- und Reportingpflichten und fordert klare Verantwortlichkeiten. Die BDSV/Detecon-Handreichung betont, dass Unternehmen eigenverantwortlich prüfen, registrieren und nachweisen müssen, welche Pflichten sie betreffen und wie diese umgesetzt sind.

Genau hier setzt **AIGN OS** an:

- AIGN OS ist kein Tool, keine Software, keine Plattform.
- AIGN OS ist ein Betriebssystem für Governance, das Rollen, Verantwortlichkeiten, Risiken, Kontrollen, Vorfälle, Meldeketten, Lieferkettensicherheit und Nachweise in eine konsistente, prüfbare Struktur bringt.

AIGN OS erfüllt keine einzelnen NIS2-Pflichten automatisch – aber es schafft die Governance-Umgebung, in der Organisationen diese Pflichten effektiv, nachvollziehbar und zukunftsfähig erfüllen können.

AIGN.OS

DIE NIS2-RICHTLINIE:

KONTEXT UND ANFORDERUNGEN

Die NIS2-Richtlinie verfolgt das Ziel, ein hohes gemeinsames Sicherheitsniveau innerhalb der EU zu schaffen. Sie verpflichtet Unternehmen zu organisatorischen, technischen und strategischen Maßnahmen, die eine ganzheitliche Widerstandsfähigkeit sicherstellen sollen.

Risikomanagement

Nach Art. 21 müssen Unternehmen ein umfassendes Risikomanagement etablieren, das mindestens umfasst:

- Risikoanalysen
- Sicherheitsrichtlinien
- Wiederherstellungs- und Betriebsfortführungspläne
- Incident-Management
- Kryptografische Maßnahmen
- Zugangskontrollen
- Überwachung der Lieferketten
- Schwachstellenmanagement
- Business Continuity
- Notfallpläne
- Backup- und Restore-Prozesse
- Krisenmanagement

Ein zentraler Aspekt ist die Dokumentierbarkeit: Unternehmen müssen jederzeit nachweisen können, dass die erforderlichen Maßnahmen existieren, funktionieren und überprüfbar sind.

Meldepflichten

NIS2 definiert strenge und zeitkritische Meldevorgaben:

- 24 Stunden: Frühwarnung
- 72 Stunden: Incident-Bericht
- 1 Monat: Abschlussbericht

Diese Anforderungen bedeuten, dass Unternehmen ein automatisiertes und durchgängiges Incident-Governance-System benötigen.

DIE NIS2-RICHTLINIE:

KONTEXT UND ANFORDERUNGEN

Die NIS2-Richtlinie verfolgt das Ziel, ein hohes gemeinsames Sicherheitsniveau innerhalb der EU zu schaffen. Sie verpflichtet Unternehmen zu organisatorischen, technischen und strategischen Maßnahmen, die eine ganzheitliche Widerstandsfähigkeit sicherstellen sollen.

Managementhaftung

Die Geschäftsleitung trägt die volle Verantwortung für die ordnungsgemäße Umsetzung. Sie ist verpflichtet:

- Schulungen wahrzunehmen
- Governance-Strukturen zu überwachen
- Verstöße zu verantworten

Bußgelder können bis zu 10 Mio. € oder 2 % des Umsatzes betragen.

Betroffene Sektoren

Die Richtlinie gilt für 18 kritische Sektoren, darunter:

- Energie
- Gesundheit
- Transport
- Produktion
- Digitale Infrastruktur
- Öffentliche Verwaltung
- Forschung
-

Damit betrifft **NIS2** de facto den Großteil der deutschen Kernwirtschaft**.**

DIE GOVERNANCE HERAUSFORDERUNG IN DEUTSCHLAND

Deutschland startet nicht bei null. Viele betroffene Unternehmen – insbesondere in KRITIS-Sektoren – verfügen bereits über etablierte Informationssicherheits-Managementsysteme (z. B. ISO/IEC 27001), branchenspezifische Sicherheitsstandards, Notfallhandbücher und Incident-Prozesse. In zahlreichen Häusern existieren zudem Datenschutz- und Compliance-Strukturen sowie ein gewisses Maß an Rollen- und Verantwortlichkeitsdefinition.

Die eigentliche Herausforderung durch NIS2 liegt daher weniger im völligen Fehlen von Sicherheit, sondern in drei anderen Dimensionen:

Harmonisierung und Integration

NIS2 kommt nicht isoliert, sondern on top zu bestehenden Vorgaben wie GDPR, KRITIS-Verordnung, branchenspezifischen Standards, teilweise auch DORA und dem EU AI Act. Unternehmen müssen diese Regelwerke kohärent umsetzen, ohne parallel laufende Silos, doppelte Prozesse oder widersprüchliche Zuständigkeiten zu erzeugen. Bitkom weist explizit darauf hin, dass unterschiedliche Zeitpläne, nationale Zusatzanforderungen und überlappende Pflichten zu erheblichem Mehraufwand und Unsicherheit führen.

Nachweis- und Dokumentationsfähigkeit

NIS2 verknüpft technische und organisatorische Maßnahmen mit strenger Managementhaftung und formalen Meldepflichten. Das bedeutet: Es reicht nicht, „irgendetwas“ zu tun – Unternehmen müssen belegen können, welche Risiken identifiziert, welche Maßnahmen getroffen, welche Vorfälle wie bewertet und gemeldet wurden. Die BDSV/Detecon-Handreichung betont, dass betroffene Einrichtungen sich selbst identifizieren, registrieren und gegenüber Behörden den Umgang mit Cyberrisiken, Zwischenfällen und Geschäftskontinuität nachvollziehbar darlegen müssen.

Koordination über Organisationseinheiten und Lieferketten hinweg

NIS2 zieht nicht nur zentrale IT, sondern auch Fachbereiche, Geschäftsleitung und Lieferkette in die Verantwortung. Viele Unternehmen verfügen zwar über Security-Tools und punktuelle Prozesse, aber keine übergreifende Governance-Architektur, die Verantwortlichkeiten, Entscheidungswege, Eskalationen, Lieferantenabhängigkeiten und Berichtswege systemisch zusammenführt. Gerade die Verzahnung von interner Sicherheit und externer Abhängigkeit (Dienstleister, Cloud, Plattformen) bleibt oft fragmentiert.

In vielen Unternehmen existieren bereits Security- und Compliance-Elemente.
Was fehlt, ist eine konsistente, architekturgetriebene Governance-Infrastruktur,
die NIS2-Anforderungen, bestehende Standards und neue digitale Risiken – insbesondere durch autonome Systeme – in einem einzigen, nachvollziehbaren System zusammenführt.

aign.os

Access Control and Authentication

System & Network Protection

Data Security and Encryption

User Awareness and Best Practices

WIE AIGN OS UNTERNEHMEN BEI NIS2 UNTERSTÜTZT

AIGN OS ist kein Tool, keine Software und kein einzelnes Produkt.
Es ist eine Governance-Infrastruktur, die Organisationen hilft:

- Verantwortlichkeiten klar zuzuordnen
- Risiken, Kontrollen und Maßnahmen einheitlich zu strukturieren
- Incident-Prozesse konsistent abzubilden
- Meldeketten nachvollziehbar zu gestalten
- Lieferkettenanforderungen und Risiken zentral zu organisieren
- Dokumentation für Behörden und Auditoren bereitzustellen
- autonome Systemhandlungen (Agentic AI) nachvollziehbar zu machen
- Führungskräfte in die Lage zu versetzen, ihre Pflichten evidenzbasiert wahrzunehmen

AIGN OS ersetzt keine NIS2-Pflicht, sondern schafft die systemische Ordnung, in der Pflichten erfüllt werden können.

AIGN OS: DIE GOVERNANCE-ARCHITEKTUR FÜR NIS2

NIS2-Pflichten

- Risikomanagement
- Sicherheitsvorfälle & Incident-Respons
- Meldepflichten (24 h / 72 h / 30 Tage)
- Business Continuity
- Lieferkettensicherheit
- Technische & organisatorische Maßnahmen
- Managementhaftung & Bußgelder

🔹 LAYER - GOVERNANCE TOOLCHAIN
NIS2-Bezug:
- Incident-Response & Meldepflichten (Art. 23-24)
- Supply-Chain Security (Art. 21 Abs. 2d)

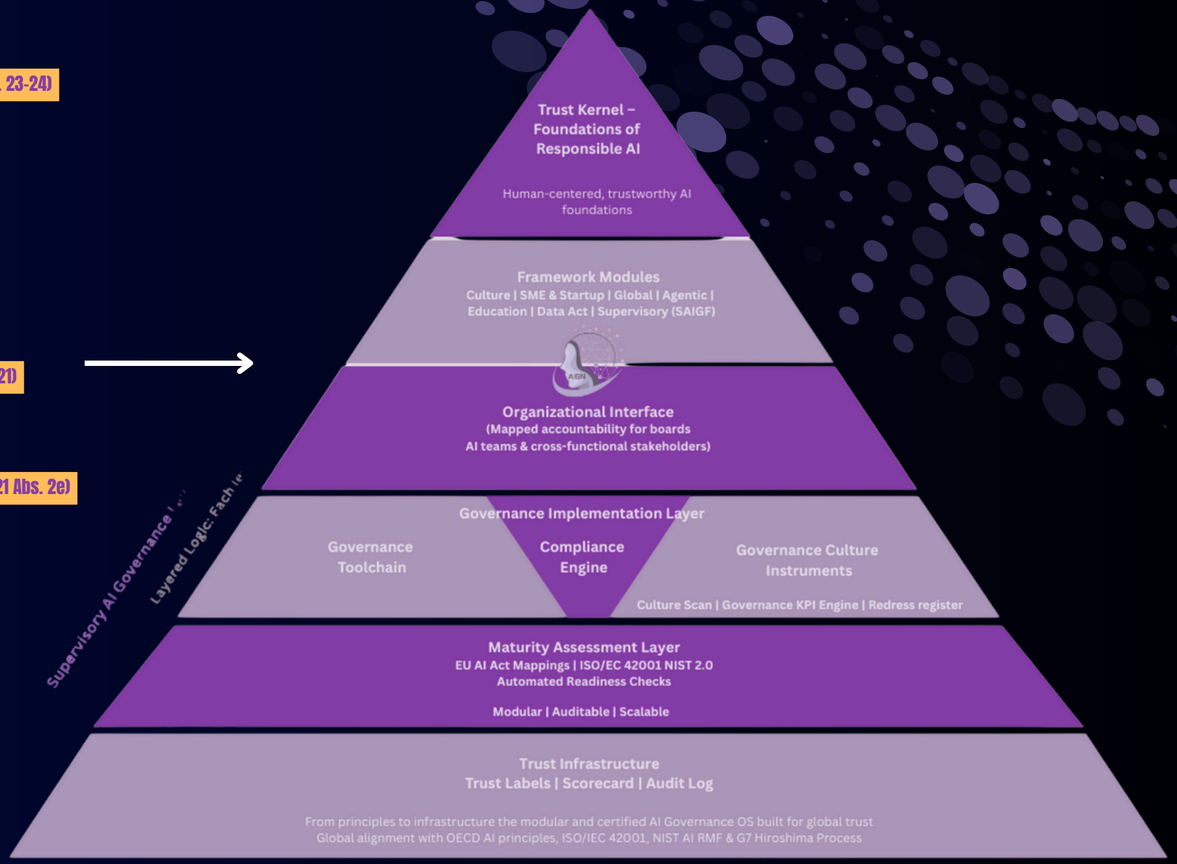
🔹 LAYER - GOVERNANCE KERNEL
NIS2-Bezug:
- Risiko-Management (Art. 21)
- Sicherheitsmaßnahmen (Art. 21 Abs. 2)

🔹 LAYER - ORGANIZATIONAL INTERFACE
NIS2-Bezug:
- Governance-Regeln
- Rollen & Verantwortlichkeiten (Art. 20-21)

🔹 LAYER - MATURITY ASSESSMENT LAYER
NIS2-Bezug:
- Business Continuity & Resilience (Art. 21 Abs. 2e)

🔹 LAYER - COMPLIANCE ENGINE
NIS2-Bezug:
- Dokumentation
- Auditierbarkeit
- Compliance-Pflichten (Art. 21, Art. 2d)

🔹 LAYER - TRUST & CERTIFICATION LAYER
NIS2-Bezug:
- Managementhaftung
- Aufsichtspflichten (Art. 20)



AIGN.OS

AIGN OS LAYER - MAPPING ZU NIS2

01

Layer 1 – Governance Foundations
Unterstützt:
- Verantwortlichkeiten
- Policies
- Governance-Strukturen

02

Layer 2 – Roles & Accountability
Unterstützt:
- Zugriffskonzepte
- Verantwortlichkeitsketten

03

Layer 3 – Risk & Control Engine
Unterstützt:
- Risikomanagement
- Wirksamkeitsprüfung
- Cyberhygiene

04

Layer 4 – Oversight & Incident Governance
Unterstützt:
- Incident Response
- 24h / 72h / 1-Monats-Dokumentation
- Auditfähigkeit

05

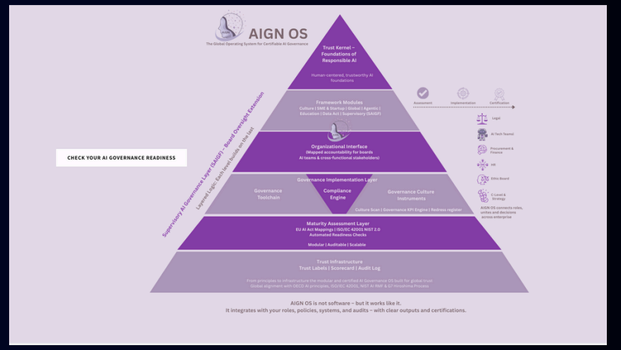
Layer 5 – Supply Chain Governance
Unterstützt:
- Bewertungen von Drittparteien
- Kontrolle kritischer Abhängigkeiten

06

Layer 6 – Resilience & Continuity
Unterstützt:
- Notfallplanung
- Business Continuity
- Wiederherstellungsprozesse

07

Layer 7 – Agentic Governance
Unterstützt:
- Nachvollziehbarkeit von maschinellen Entscheidungen
- Governance von automatisierten Abläufen
- Risikoanalyse für KI-Systeme



aign.os

NIS2-READINESS: EIN STRUKTURIERTER ANSATZ

AIGN OS ermöglicht:

- Reifegradbewertung
- Gap-Analyse
- Maßnahmenkatalog
- Governance-Dokumentation
- Prüfpfade für Behörden

SCHLUSSFOLGERUNG

NIS2 bringt ein neues Sicherheitsniveau nach Europa – aber kein Unternehmen erhält eine Anleitung, wie die Vielzahl an Pflichten organisatorisch zusammengeführt werden soll.

AIGN OS füllt genau diese Lücke:
Es ist das Betriebssystem für Governance, das Unternehmen befähigt:

- Risiken strukturiert zu bewerten
- Maßnahmen nachzuweisen
- Vorfälle korrekt zu melden
- Lieferketten kontrollierbar zu gestalten
- Führungspflichten evidenzbasiert wahrzunehmen
- neue technologische Risiken – einschließlich KI-basierter Automatismen – in eine verantwortliche Struktur einzubetten.
-

Damit macht **AIGN OS** die Umsetzung von NIS2 tragfähig, transparent und zukunftssicher.

aig.os

Allianz für Cyber-Sicherheit
Partner

VIELEN DANK

+49 1787770800

message@now.digital

aign.global