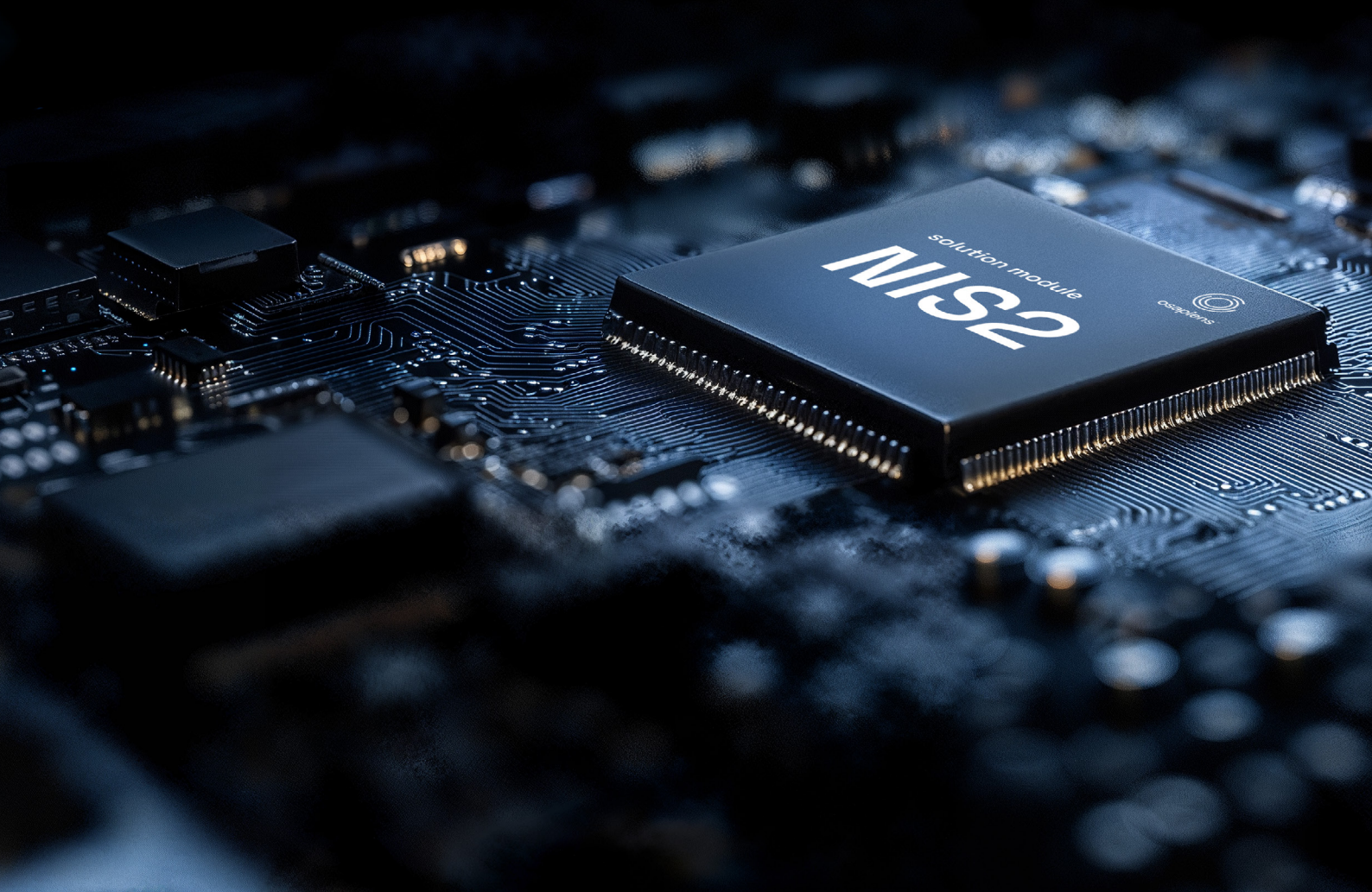
VICCON CONSULTING

osapiens® for sustainable growth

OSAPIENS GUIDE

NIS2 strukturiert umsetzen

Praxisleitfaden für Einordnung, Pflichten und Roadmap der Cyber- und Risikosteuerung



Dieser Leitfaden ordnet NIS2 ein und zeigt, warum die Richtlinie nicht nur IT, sondern auch Governance, Risiko- und Compliance-Management betrifft. Er erklärt, welche Unternehmen betroffen sind, welche Pflichten daraus folgen und welche Fristen für Planung und Umsetzung gelten. Die Anforderungen werden in fünf praxisnahe Themenblöcke übersetzt, die sich direkt als Struktur für ein NIS2-Programm nutzen lassen. Außerdem beschreibt der Leitfaden typische Stolpersteine und Anforderungen an Prozesse und Tools und zeigt, wie das gemeinsam mit VICCON entwickelte NIS2-Modul im osapiens HUB for Supplier Intelligence Unternehmen dabei unterstützt, diese Anforderungen systematisch und prüfungsfest umzusetzen. So wird aus der abstrakten Regulierung ein konkreter Fahrplan für rechtssichere, integrierte Cyber- und Risikosteuerung.

Inhalt

01. Einleitung: Was NIS2 für Unternehmen jetzt bedeutet 03

02. NIS2 im Überblick: Hintergrund, Ziele, Einordnung 04

03. Zeitplan & Rechtsrahmen: EU-Richtlinie und Umsetzung in Deutschland 05

04. Wer ist betroffen? Scope, Sektoren, Schwellenwerte 06

05. Konkrete Pflichten: Was Unternehmen umsetzen müssen 08

06. Typische Herausforderungen in der Praxis 12

07. Anforderungen an NIS2-Tools und -Prozesse 13

08. Wie osapiens unterstützt: osapiens HUB for NIS2 im Kontext des osapiens HUB for Supplier Intelligence 14

09. NIS2 umsetzen: Fahrplan in 5 Schritten 16

01.

Einleitung: Was NIS2 für Unternehmen jetzt bedeutet

NIS2 ist kein weiteres Spezialthema, das man „bei IT parken" kann. Die Richtlinie rückt die Unternehmensleitung stärker in die Verantwortung: Informationssicherheit, Resilienz und der Umgang mit Cyberrisiken werden zu Fragen der Governance, des unternehmensweiten Risiko- und Compliance-Managements und betreffen damit auch Strategie, Einkauf, Lieferkette und Operations.

Viele Unternehmen haben in den vergangenen Jahren bereits Strukturen für Compliance, Risikomanagement oder Lieferkettentransparenz aufgebaut – etwa im Kontext von LkSG, CSDDD oder anderen Nachhaltigkeits- und Sorgfaltspflichten. Genau hier setzt NIS2 an: Die Richtlinie verlangt keinen kompletten Neustart, sondern den konsequenten Ausbau bestehender Prozesse. Gefordert ist ein integrierter Blick auf Risiken, kritische Prozesse, Dienstleister und Lieferanten – mit klar definierten Zuständigkeiten und nachweisbarer Wirksamkeit der Maßnahmen.

Digitale Plattformen wie der osapiens HUB for Supplier Intelligence schaffen dafür eine zentrale Datengrundlage. Sie bündeln Lieferketten-, Risiko- und Compliance-Informationen und machen diese steuerbar, über Gesellschaften, Standorte, Lieferanten und Dienstleister hinweg. NIS2 lässt sich darauf als zusätzlicher Use Case aufsetzen: Unternehmen können bestehende Due-Diligence-Prozesse (z. B. für LkSG oder CSDDD) gezielt erweitern und so Synergien nutzen, statt parallele Strukturen aufzubauen.

Gleichzeitig bietet NIS2 für viele Organisationen einen sinnvollen Einstiegspunkt, um ein solches systematisches Setup überhaupt erst zu etablieren – mit klaren Prozessen, Verantwortlichkeiten und einer skalierbaren Plattform, die regulatorische Anforderungen nachhaltig abbildet.

Der Guide liefert damit drei Dinge: eine klare Einordnung der eigenen Betroffenheit, eine strukturierte Übersicht über die zentralen Handlungsfelder und einen pragmatischen Umsetzungsweg – einschließlich der Frage, wie sich bestehende Due-Diligence- und Lieferkettenstrukturen, insbesondere im osapiens HUB for Supplier Intelligence, gezielt für NIS2 nutzen lassen, ohne eine zusätzliche Insellösung aufzubauen.

02.

NIS2 im Überblick: Hintergrund, Ziele, Einordnung

Mit der ersten NIS-Richtlinie wurden 2016 erstmals EU-weit Mindestvorgaben zur Cybersicherheit definiert. NIS1 fokussierte sich dabei vor allem auf Betreiber kritischer Infrastrukturen; digitale Diensteanbieter waren nur in einem deutlich engeren Rahmen erfasst. Gleichzeitig machte die Richtlinie auf EU-Ebene keine einheitlichen, konkretisierten Vorgaben dazu, wie Sicherheits- und Risikomanagementmaßnahmen genau auszugestalten sind. Das Ergebnis war in der Praxis ein Flickenteppich nationaler Anforderungen.

NIS2 setzt genau hier an: Die Richtlinie soll die Cybersicherheit in Europa harmonisieren und das Schutzniveau deutlich erhöhen. Statt vager Mindeststandards formuliert sie klare Anforderungen an Risikomanagement, organisatorische und technische Sicherheitsmaßnahmen sowie Meldeprozesse, die Unternehmen künftig verbindlich umsetzen müssen.
Ein weiterer zentraler Schritt ist die **Ausweitung des Anwendungsbereichs.** Im Fokus stehen nicht mehr nur Betreiber kritischer Infrastrukturen, sondern mittelgroße und große Unternehmen aus 18 klar definierten Sektoren, von Energie, Transport und Gesundheitswesen über digitale Infrastruktur und Finanzsektor bis hin zu öffentlichen Verwaltungen, Post und Kurierdiensten sowie Entsorgung. Besonders unterschätzt wird dabei der Blick in die industrielle Breite: NIS2 erfasst auch Teile des verarbeitenden Gewerbes, in denen digitale Systeme und vernetzte Produktionsprozesse geschäftskritisch sind. Dazu zählen insbesondere Unternehmen aus der Produktion von Medizinprodukten und In vitro Diagnostika, der Fertigung von Computern sowie elektronischen und optischen Erzeugnissen, der Herstellung elektrischer Ausrüstungen, dem Maschinenbau sowie der Fahrzeug und sonstigen Transportmittelproduktion. In diesen Branchen sind IT und OT eng verzahnt, etwa über vernetzte Anlagen, Fernwartung, zentrale Produktions und Qualitätsdaten oder integrierte Logistikprozesse. Entsprechend kann ein Sicherheitsvorfall nicht nur die Büro IT, sondern unmittelbar Produktion, Lieferfähigkeit und Produktsicherheit beeinträchtigen und damit erhebliche Auswirkungen auf Wirtschaft und Gesellschaft haben.

Besonders im Blick hat NIS2 dabei die zunehmenden Angriffe auf die Lieferkette. Sie gelten als besonders kritisch, weil sie oft erst spät erkannt werden und sich über Lieferanten und Dienstleister schnell vervielfachen können. Gerade in vernetzten Betriebs- und Produktionsumgebungen reichen einzelne Schwachstellen bei externen Partnern oft aus, um ganze Prozesse zu beeinträchtigen. Um diese Risiken zu begrenzen, verlangt NIS2, Dienstleister und Lieferanten systematisch in das Risikomanagement einzubeziehen.

Dahinter steht die Notwendigkeit einer anderen Form der Zusammenarbeit mit Geschäftspartnern: Unternehmen müssen Anforderungen an Informationssicherheit, Transparenz und Kooperation vertraglich und organisatorisch in ihre Lieferbeziehungen integrieren – überall dort, wo Partner einen Einfluss auf die eigene Informationssicherheit haben.

Das übergeordnete Zielbild ist ein **hoher gemeinsamer Cybersicherheitsstandard in der EU,** mit Fokus auf Resilienz und Verfügbarkeit kritischer und wesentlicher Dienste. Dazu gehört auch eine engere Zusammenarbeit der Behörden: Die dreistufige Meldepflicht soll nicht nur die Aufsicht über einzelne Unternehmen verbessern, sondern vor allem eine schnelle Frühwarnung und Koordination zwischen den Mitgliedstaaten ermöglichen.

NIS2 steht nicht isoliert, sondern fügt sich in bestehende nationale und sektorspezifische Vorgaben ein. In Deutschland wird die Richtlinie im Kern durch das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) umgesetzt, das insbesondere das BSI-Gesetz (BSIG) umfassend anpasst. Daneben bleibt die KRITIS-Verordnung relevant, die Schwellenwerte dafür festlegt, ab wann ein Unternehmen als Betreiber kritischer Infrastrukturen gilt. In einzelnen Sektoren kommen weitere Spezialvorgaben hinzu, etwa das Energiewirtschaftsgesetz (EnWG) im Energiesektor oder die IT-Sicherheitskataloge (IT-SiKat) für Energie- und Telekommunikationsunternehmen. NIS2 bildet damit den übergeordneten Rahmen, in den sich diese Regelungen einordnen und wird zu einem zentralen Baustein des deutschen Regulierungsgefüges zur Informationssicherheit.

03.

Zeitplan & Rechtsrahmen: EU-Richtlinie und Umsetzung in Deutschland

NIS2 auf EU-Ebene: die wichtigsten Meilensteine

JANUAR 2023
NIS2 tritt als EU-Richtlinie in Kraft

OKTOBER 2024
Durchführungsverordnung (EU) zu NIS2 tritt in Kraft
Sie richtet sich vor allem an den digitalen Sektor (z. B. DNS-Dienste, TLD-Register, Cloud- und Rechenzentrumsdienste, Content-Delivery-Netze, Managed (Security) Services, Online-Marktplätze, Suchmaschinen, soziale Netzwerke, Vertrauensdienste). Sie konkretisiert:

- wann ein „erheblicher Sicherheitsvorfall" vorliegt und meldepflichtig ist und
- welche sehr detaillierten technischen und organisatorischen Maßnahmen diese Unternehmen umsetzen müssen, um ein angemessenes Risikomanagement und Sicherheitsniveau nachzuweisen.

OKTOBER 2024
Umsetzungsfrist für die Überführung der NIS2 in nationales Recht in allen Mitgliedsstaaten
(Deutschland verfehlt diese Frist, der EU-Rechtsrahmen steht aber vollständig).

Nationale Umsetzung in Deutschland

In Deutschland erfolgt die Umsetzung über das **NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG).** Kern ist eine umfassende Anpassung des **BSI-Gesetzes (BSIG-neu).**

13. NOVEMBER 2025
Der Bundestag verabschiedet das NIS2UmsuCG

6. DEZEMBER 2025
Inkrafttreten nach Verkündung im Bundesgesetzblatt

06.MÄRZ 2026
Einrichtungen müssen sich spätestens innerhalb von drei Monaten registrieren, nachdem sie erstmals oder erneut **NIS2-betroffen** sind (maßgeblich ist der Zeitpunkt, ab dem die Betroffenheit tatsächlich eintritt – z. B. nach Einstufung/Prüfung oder durch Größen-, Struktur- oder Tätigkeitsänderungen – nicht pauschal das Inkrafttreten).

Für Unternehmen wichtig:

- **Betroffenheit wird oft übersehen:** Besonders mittelgroße und große Unternehmen aus NIS2-Sektoren außerhalb der klassischen KRITIS-Welt unterschätzen ihren Scope, etwa Teile des verarbeitenden Gewerbes wie Medizinprodukte, Elektronik, elektrische Ausrüstung sowie Maschinen und Anlagenbau.
- **Nachweise sind je nach Kategorie unterschiedlich geregelt:** Betreiber kritischer Anlagen müssen die Umsetzung regelmäßig durch Sicherheitsaudits, Prüfungen oder Zertifizierungen nachweisen. Für wichtige und besonders wichtige Einrichtungen sieht das Gesetz dagegen keinen festen turnusmäßigen Nachweiszyklus vor, sondern ermöglicht dem BSI, Prüfungen und Nachweise im Einzelfall anzuordnen.
- **Audit-Scope ist nicht gleich Umsetzungsscope:** Bei KRITIS bleibt der Audit-Scope grundsätzlich an der kritischen Dienstleistung orientiert. Die NIS2-Anforderungen an Risikomanagement sowie organisatorische und technische Maßnahmen sind jedoch unternehmensweit umzusetzen und dürfen nicht im isolierten „KRITIS-Kasten" stehen bleiben.

Praxisrelevante Fristen für Unternehmen

Mit Inkrafttreten des deutschen Umsetzungsgesetzes zählen für betroffene Unternehmen vor allem drei Punkte:

1. Registrierung und Betroffenheitsprüfung
Ab Inkrafttreten haben Unternehmen **drei Monate Zeit,** ihre NIS2-Betroffenheit zu prüfen und sich anschließend beim BSI zu registrieren, inklusive Benennung einer 24/7-Erreichbarkeitsstelle. Dabei geht es nicht um „Abstufungen" der Anforderungen, sondern um die klare Klärung, ob das Unternehmen in den Anwendungsbereich fällt und damit registrierungs- und umsetzungspflichtig ist.

2. Sofortige Umsetzungsverpflichtung
Die inhaltlichen Anforderungen (Risikomanagement, technische und organisatorische Maßnahmen, Meldeprozesse) gelten **grundsätzlich ab Inkrafttreten.** Es gibt keine komfortable Übergangsphase, in der man „abwarten" könnte.

3. Nachweise und faktische „Schonfrist“

Für Betreiber kritischer Infrastrukturen ist der erste formale Nachweis nach neuem Recht nicht am Tag X fällig, sondern turnusmäßig. Der Nachweiszyklus liegt bei drei Jahren (das BSI weist darauf hin, dass sich der Nachweiszyklus von zwei auf drei Jahre verlängert; bereits registrierte KRITIS-Betreiber haben vom BSI neue Nachweisfristen mitgeteilt bekommen). De facto entsteht damit eine **begrenzte Schonfrist,** allerdings nur in dem Sinne, dass Prüfungen später kommen. Unternehmen sollten in diesem Zeitraum bereits

- ein **Grobkonzept,**
- eine belastbare **Projektplanung** und
- erste zentrale Maßnahmen

nachweisen können, um gegenüber Aufsicht und Prüfern und insbesondere nach einem Sicherheitsvorfall zeigen zu können, dass sie NIS2 aktiv und strukturiert umsetzen.

Tipp an den Leser

Rechtlich mag der Prüfungsdruck zeitversetzt kommen, inhaltlich ist NIS2 mit Inkrafttreten jedoch sofort relevant. Wer da erst anfängt zu planen, ist zu spät dran.

04.

Wer ist betroffen? Scope, Sektoren, Schwellenwerte

Einrichtungsarten und Größenkriterien

NIS2 unterscheidet (in Deutschland über § 28 BSIG) zwei Kategorien von Unternehmen:

Besonders wichtige Einrichtungen (essential entities)

In der Regel große Unternehmen aus den NIS2 Sektoren der Anlage 1, z. B. Energie und Wasserwirtschaft, Verkehr, Banken und Finanzmarktinfrastrukturen, Gesundheitswesen sowie digitale Infrastruktur und IT Dienste wie Cloud und Rechenzentrumsdienste, DNS Dienste und TLD Register oder Managed Service Provider und Managed Security Service Provider. Typisch: mindestens **250 Beschäftigte** und **> 50 Mio. € Jahresumsatz** und **> 43 Mio. € Jahresbilanzsumme**

Wichtige Einrichtungen (important entities)

Meist mittlere Unternehmen aus den Sektoren der Anlagen 1 und 2, z. B. Abfallwirtschaft, Post und Kurierdienste, Lebensmittelproduktion und verarbeitung sowie Teile des verarbeitenden Gewerbes wie Medizinprodukte, Elektronik und Optik, elektrische Ausrüstungen und Maschinenbau. Auch Anbieter digitaler Dienste wie Online Marktplätze, Online Suchmaschinen und soziale Netzwerke können darunter fallen: mindestens **50 Beschäftigte** und **> 10 Mio. € Jahresumsatz** und **> 10 Mio. € Jahresbilanzsumme**

Hinzu kommen **größenunabhängige Sonderfälle,** etwa bestimmte Betreiber kritischer Anlagen oder Unternehmen mit besonderer Bedeutung für Versorgungssicherheit oder öffentliche Sicherheit.

Für den schnellen Reality-Check:

	besonders wichtige Einrichtungen	**wichtige** Einrichtungen
Anlage	1	1 oder 2
	UND	**UND**
Mitarbeitende	≥ 250	≥ 50
	ODER	**ODER**
Jahresumsatz	> 50 Mio. €	> 10 Mio. €
	UND	**UND**
Jahresbilanzsumme	> 43 Mio. €	> 10 Mio. €
	ODER*	
	Betreiber kritischer Anlagen	

Sektoren und Teilsektoren

Die unten gezeigten Sektoren basieren direkt auf den Anlagen 1 und 2 der deutschen NIS2-Umsetzungsverordnung. Dort sind die betroffenen Bereiche nach **Sektor, Branche und Einrichtungsart** gegliedert.

DORA im Finanzsektor

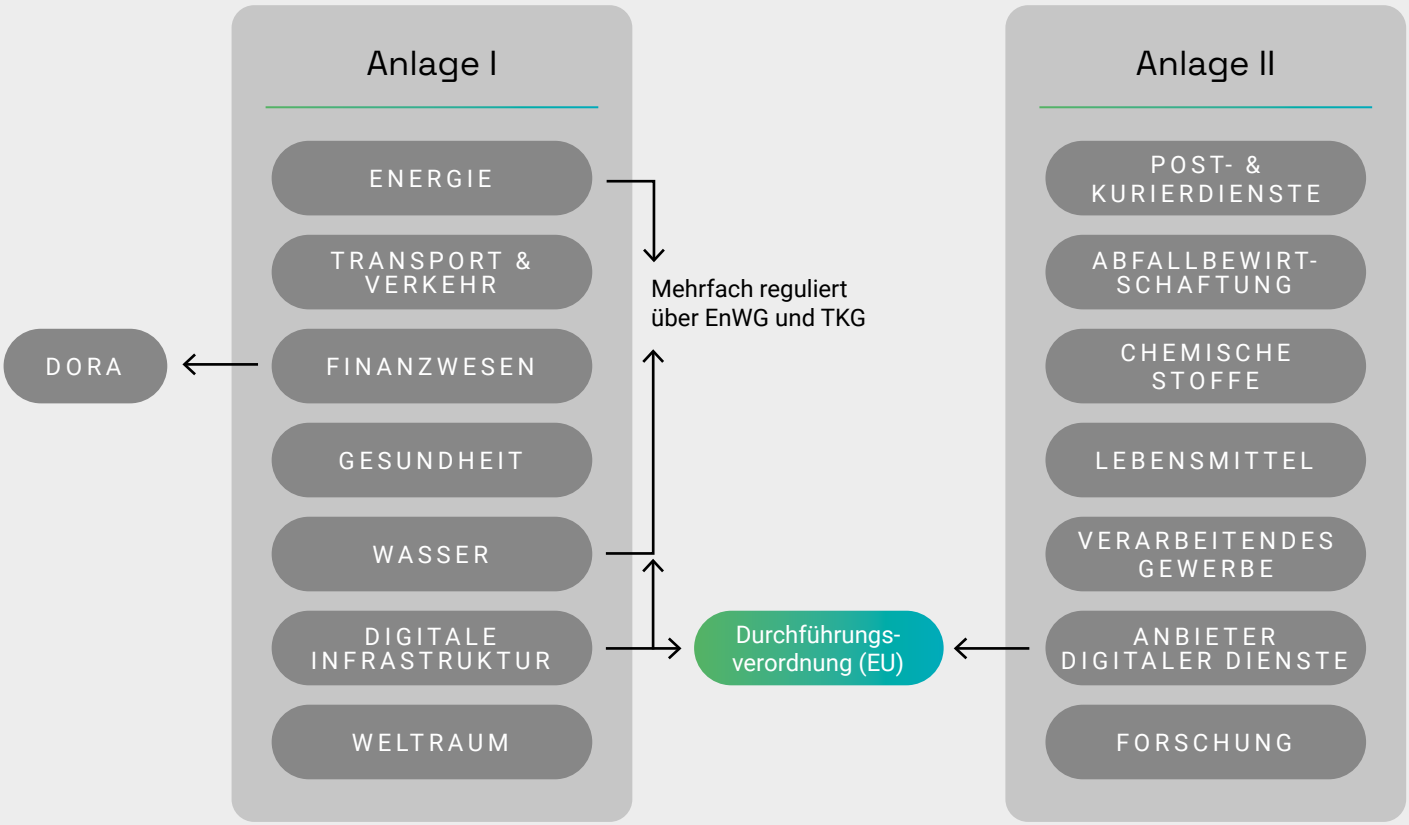
DORA (Digital Operational Resilience Act) ist die spezielle EU-Verordnung für die digitale Resilienz von Finanzunternehmen. Sie regelt u. a. IKT-Risikomanagement, Vorfallmeldungen, Tests und den Umgang mit IKT-Dienstleistern. Für Banken, Wertpapierfirmen, Börsen & Co. ist DORA die zentrale Cyber-/IKT-Regulierung; NIS2 setzt den übergeordneten Rahmen und kommt ergänzend hinzu.

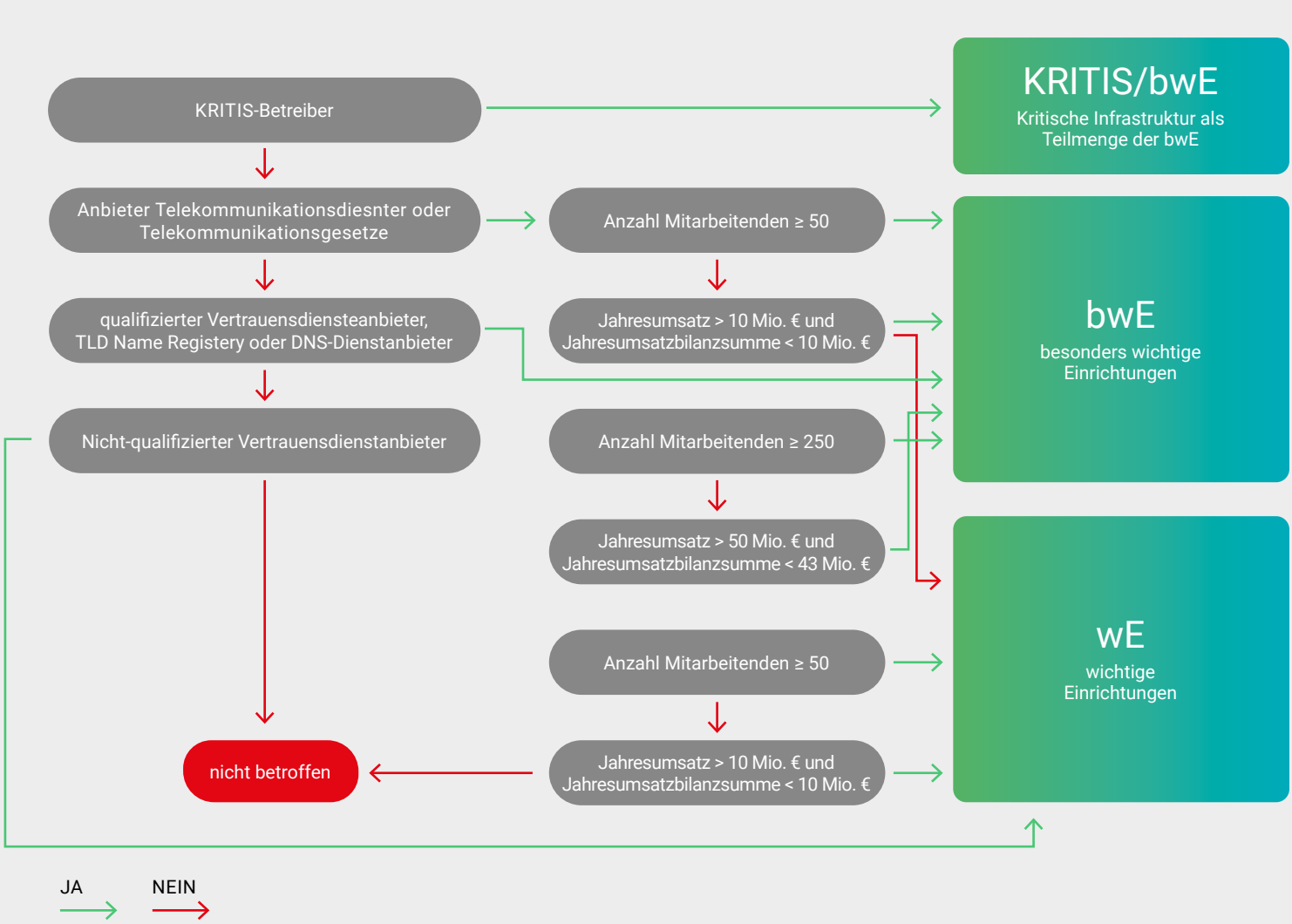
Für die Praxis heißt das:

- **Zuordnung zu Anlage 1 oder 2 prüfen:** Anhand der Anlagen 1 und 2 klären, ob eine wirtschaftliche Tätigkeit im Unternehmen NIS2-relevant ist. Entscheidend ist nicht das Kerngeschäft, sondern jede Tätigkeit: Betreibt z. B. ein Schokoladenhersteller ein eigenes Rechenzentrum nur für sich selbst, ist das meist unkritisch. Versorgt dieses Rechenzentrum jedoch konzernweit weitere Gesellschaften oder Standorte, wird die Rolle als Rechenzentrumsbetreiber relevant und kann die NIS2-Betroffenheit auslösen.
- **Einstufung über Größenkriterien vornehmen:** Wenn das der Fall ist, mit den im Gesetz genannten Schwellenwerten für Mitarbeitende, Jahresumsatz und Bilanzsumme bestimmen, ob das Unternehmen als besonders wichtige Einrichtung, wichtige Einrichtung oder nicht betroffen gilt.

Der BSI-Entscheidungsbaum zur NIS2-Betroffenheitsprüfung zeigt diese Schritte als einfachen Ablauf:

Betroffene Sektoren





Mehrländerszenarien

Bei Konzernen mit Standorten in **mehreren EU-Staaten** stellt sich zusätzlich die Frage, welcher Mitgliedstaat als Aufsicht zuständig ist und wie ausländische Tochtergesellschaften einzuordnen sind (eigenständige Unternehmen, verbundene Unternehmen, Partnerunternehmen).

Zusätzlich relevant sind Konstellationen mit Gesellschaften außerhalb der EU: Auch wenn diese Nicht-EU-Einheiten nicht automatisch unter NIS2 fallen, können sie die Betroffenheitsanalyse und den Scope der Umsetzung in der EU spürbar beeinflussen, etwa über Verbund- und Größenbetrachtungen, über konzernweite IT-/Security-Shared-Services (z. B. SOC, IAM, Patch- und Asset-Management), oder über operative Abhängigkeiten in kritischen Prozessen.

Je nach Zuordnung können strengere Anforderungen eines bestimmten Mitgliedstaats greifen, zusätzliche Nachweispflichten entstehen oder der Staat des Mutterkonzerns als primär zuständige Aufsicht auftreten. Für einfache Unternehmensstrukturen ist die Einordnung meist schnell erledigt; bei international aufgestellten Konzernen kann eine saubere Betroffenheitsanalyse dagegen leicht zu einem eigenen Projekt werden.

05.

Konkrete Pflichten: Was Unternehmen umsetzen müssen

NIS2 beschreibt keine einzelnen „Technikmaßnahmen“, sondern ein Gesamtbild: Governance, Risikomanagement, Incident-Handling, Steuerung von Dienstleistern und eine saubere Dokumentation müssen zusammenpassen. Die folgenden fünf Themenblöcke können direkt als Struktur für das eigene NIS2-Projekt genutzt werden.

1. Governance & Verantwortung

NIS2 rückt die **Geschäftsleitung und Leitungsorgane** klar in die Verantwortung. Sie müssen Cybersicherheit aktiv steuern, Rollen definieren und deren Wirksamkeit überwachen.

Kernanforderungen:

Rolle der Geschäftsleitung

- Wahrnehmung von Haftungs- und Überwachungspflichten im Bereich Netz- und Informationssicherheit.
- Billigung und Überwachung zentraler Cybersicherheitsmaßnahmen.
- Teilnahme an regelmäßigen Schulungen, um Cyber-Risiken sowie deren Erhebung und Bewertung nachvollziehen und wirksam steuern zu können.

Einbindung zentraler Funktionen

- Systematische Einbindung von CISO/IT-Security, Datenschutz, Compliance und Legal in Entscheidungsprozesse.

Klare Rollen- und Verantwortlichkeitsstruktur

- Definition und Zuordnung klarer Verantwortlichkeiten und Weisungsbefugnisse für Netz- und Informationssicherheit an spezifische Rollen.
- Mitteilung dieser Rollen- und Entscheidungsstruktur an die Leitungsorgane, um Transparenz über Hierarchien und Zuständigkeiten sicherzustellen.
- Schaffung dedizierter Rollen für Cybersicherheit oder Erweiterung bestehender Rollen – abhängig von Größe und Komplexität des Unternehmens.

Interessenskonflikte vermeiden

- Trennung widerstrebender Pflichten und Vermeidung widersprüchlicher oder überschneidender Verantwortlichkeiten (z. B. Kontrollfunktion und operativer Betrieb in einer Hand).

Regelmäßige Überprüfung

- Turnusmäßige Überprüfung und Anpassung der Rollen, insbesondere nach Vorfällen oder bei geänderter Risikolage, durch die Leitungsorgane.

2. Risikomanagement & Sicherheitsmaßnahmen

Im Zentrum von NIS2 steht ein **systematisches, dokumentiertes Risikomanagement** für Netz- und Informationssicherheit. Technische Maßnahmen allein genügen nicht, sie müssen aus einer Risikobetrachtung abgeleitet und gesteuert werden.

Kernanforderungen:

ISMS und Allgefahren-Ansatz

- Etablierung eines Informationssicherheitsmanagementsystems (ISMS) im Sinne von NIS2.
- Regelmäßige, dokumentierte Risikobewertungen nach dem Allgefahren-Ansatz (inkl. Cyberangriffe, technische Störungen, menschliche Fehler, physische Risiken und umweltbedingte Bedrohungen).

Risikobewertung & -akzeptanz

- Identifikation und Analyse von Risiken für Verfügbarkeit, Integrität und Vertraulichkeit wesentlicher Systeme und Daten.

Festlegung von Risikokriterien und Risikotoleranzen.

- Definition von Risikobehandlungsplänen mit klaren Verantwortlichkeiten, Prioritäten und Zeitplänen.
- Dokumentierte Akzeptanz von Restrisiken durch Leitungsorgane bzw. definierte Risk Owner.

Umsetzung & Monitoring von Maßnahmen

- Ableitung technischer und organisatorischer Sicherheitsmaßnahmen (u. a. Netzwerksicherheit, Zugangskontrollen, Backup/Recovery, Härtung von Systemen, Security Awareness).
- Fortlaufende Überwachung der Umsetzung von Risikomaßnahmen und regelmäßiges Reporting an die Leitungsorgane.

Schwachstellenmanagement

- Systematische Schwachstellenidentifikation (z. B. Scans, Pen-Tests, externe Hinweise).
- Etablierung von Prozessen für Vulnerability Disclosure und koordinierte Behebung identifizierter Schwachstellen.

Verzahnung mit BCM und Krisenmanagement

- Integration der Ergebnisse des Risikomanagements in die Betriebskontinuitätsplanung (Business Continuity Management).
- Abstimmung mit Notfall- und Krisenmanagementprozessen, damit Sicherheitsvorfälle auch organisatorisch beherrscht werden können.

3. Meldepflichten & Incident Management

NIS2 sieht ein **dreistufiges Meldeverfahren für erhebliche Sicherheitsvorfälle** vor. Dieses Verfahren muss in bestehende Incident- und Krisenprozesse integriert werden.

Kernanforderungen:

Fristen und Schwellen der Meldungen

- **Erstmeldung innerhalb von 24 Stunden** nach Kenntniserlangung eines erheblichen Sicherheitsvorfalls.
- **Detailmeldung innerhalb von 72 Stunden** mit Bewertung von Schweregrad, Auswirkungen und möglicher Kompromittierung von Systemen oder Daten.
- **Abschlussbericht innerhalb eines Monats** mit Ursachenanalyse, dokumentierten Abhilfemaßnahmen und ggf. grenzüberschreitenden Effekten (bei noch laufender Bewältigung: Abschlussbericht, sobald ausreichend gesicherte Erkenntnisse vorliegen).

Verzahnung mit internen Prozessen

- Anbindung an bestehende Prozesse und Funktionen wie Incident Response Plan (IRP), Security Operations Center (SOC), CERT/CSIRT, Notfall- und Krisenmanagement.

Kommunikationswege definieren

- Interne Informationskette festlegen: wer bei einem Vorfall wann informiert wird (z. B. IT und Security, Management, Recht, Kommunikation, betroffene Fachbereiche).
- Externe Informationskette festlegen: wer wann Behörden (z. B. BSI), Kunden, Dienstleister und weitere relevante Stakeholder informiert und wer dafür kommunikations und meldebefugt ist.

4. Drittrisiko & Lieferketten

NIS2 verlangt, **Dienstleister und Lieferanten mit Einfluss auf die Informationssicherheit** systematisch zu steuern. Das ist kein „Nice to have“, sondern ein zentraler Risikofaktor.

Kernanforderungen:

Relevante Lieferanten identifizieren

- Festlegung von Kriterien, welche Lieferanten und Dienstleister einen Einfluss auf die eigene Informationssicherheit haben (z. B. Hosting, Wartung, Remote-Zugriff, kritische Services).
- Pragmatischer Ansatz zur Eingrenzung: Relevante Lieferanten lassen sich effizient vorsortieren, etwa über Filterkriterien wie den NACE Code.
- Regelmäßige Bewertung dieser Lieferanten nach einem definierten Konzept.
- Gesonderte, vertiefte Risikobewertung für als kritisch identifizierte Lieferanten.

Integration in Due Diligence & Lieferkettenprozesse

- Einbindung der NIS2-Anforderungen in bestehende Due-Diligence-Prozesse und Lieferkettensteuerung.

→ **Für Bestandskunden des osapiens HUB for Supplier Intelligence heißt das:** NIS2 kann als Add-on zum Supplier Intelligence Modul hinzugefügt werden und kommt nicht als zusätzliche Insellösung ins Haus, sondern als weiterer Anwendungsfall auf derselben Plattform, auf der Lieferanten, Risiken und Maßnahmen bereits zentral gesteuert werden.

Kriterien für Auswahl, Vergabe und Vertragsgestaltung

- Cybersicherheitsanforderungen bereits bei Auswahl und Auftragsvergabe berücksichtigen.
- Vertragliche Sicherheitsklauseln und Mindestanforderungen entlang der gesamten Lieferkette verankern (z. B. zu Patch-Management, Meldepflichten, Audit-Rechten).

Kontinuierliche Überwachung

- Regelmäßige Überprüfung von Cybersicherheitsverfahren bei Anbietern, bei Bedarf auch durch Audits oder Nachweisanforderungen – insbesondere nach Vorfällen.
- Berücksichtigung sowohl koordinierter als auch individueller Risikobewertungen für IKT-Produkte und -Dienste.
- Laufendes Monitoring risikobehafteter Lieferanten und dokumentierte Reaktionen auf erkannte Mängel.

5. Dokumentation, Reporting & Auditfähigkeit

Ohne belastbare Dokumentation fehlt die Grundlage, um bei Sicherheitsvorfällen, Audits oder behördlichen Nachfragen Entscheidungen zu begründen, Maßnahmen nachzuweisen und aus Vorfällen zu lernen. NIS2 verlangt deshalb nachvollziehbare **Nachweise, Entscheidungsgrundlagen und Reports** – auch wenn in Deutschland formale Nachweispflichten primär KRITIS-Unternehmen und Fälle mit expliziter BSI-Anforderung betreffen.

Kernanforderungen:

Nachweispflichten gegenüber Aufsichtsbehörden

- In Deutschland insbesondere für KRITIS-Unternehmen sowie Unternehmen, von denen das BSI aktiv einen Nachweis einfordert.

Vollständige Dokumentation zentraler Prozesse

- Dokumentation aller Risikobewertungen, Risikobehandlungspläne, Testergebnisse (z. B. Pen-Tests, Notfallübungen) und Anpassungen.
- Prüfpfade zu Policies, Richtlinien, technischen Standards, Schulungsunterlagen und Schulungsnachweisen.

Regelmäßiges Reporting

- Regelmäßige Berichterstattung zum Stand der Cybersicherheit an Geschäftsleitung und Leitungsorgane (z. B. Status von Maßnahmen, Risiken, Vorfällen, KPIs).

Nachverfolgung von Schwachstellen und Vorfällen

- Systematisches Tracking identifizierter Schwachstellen, Maßnahmenumsetzung und Fristen.
- Dokumentation relevanter Sicherheitsvorfälle, inklusive Ursachen, Auswirkungen und Lessons Learned.

Dokumentation von Drittbeziehungen

- Nachvollziehbare Dokumentation von Entscheidungen, Maßnahmen und Leistungsvereinbarungen mit Dritten, soweit sie Informationssicherheitsrisiken beeinflussen.

06.

Typische Herausforderungen in der Praxis

Auf dem Papier wirkt NIS2 oft klar geregelt. In der Realität scheitert die Umsetzung selten an fehlenden Vorgaben, sondern an Strukturen, Zuständigkeiten und Systembrüchen im Unternehmen. Die folgenden Herausforderungen begegnen uns in der Praxis immer wieder und erklären, warum viele Organisationen trotz vorhandener Maßnahmen nicht wirklich sicher sind, ob sie NIS2-konform sind.

In Summe entsteht so ein Muster: nicht der einzelne Paragraph macht NIS2 schwierig, sondern das Zusammenspiel aus Betroffenheit, Governance, Prozessen, Tools und Daten. Genau hier entsteht der Bedarf nach einer **strukturierten und möglichst integrierten Lösung.**

Herausforderungen in der NIS2 Umsetzung

Unklare Betroffenheit

Viele Unternehmen können nicht klar beurteilen, ob sie unter NIS2 fallen. Entscheidend ist nicht nur das Kerngeschäft, sondern jede wirtschaftliche Tätigkeit, auch Neben- und Konzernfunktionen. Unklare Zuständigkeiten zwischen Mutter- und Tochtergesellschaften führen zusätzlich zu Verzögerungen und Fehlpriorisierungen.

Datenlücken bei Dienstleistern & Lieferkette

Wer erbringt welche kritische Leistung, mit welchen Systemen und Zugriffsrechten? Häufig unklar, schlecht dokumentiert oder veraltet. Genau dort, wo NIS2 den Fokus hinlegt, fehlen Transparenz und belastbare Daten.

Unklare Verantwortung

IT, Informationssicherheit, Compliance, Datenschutz, Risk und Fachbereiche sind alle irgendwie beteiligt, aber Ownership ist unklar. Entscheidungen versanden, Maßnahmen bleiben unvollständig, und im Zweifel ist Verantwortung so verteilt, dass sich niemand wirklich zuständig fühlt.

Regulierungs-Overload ohne Harmonisierung

NIS2, LkSG/CSDDD, KRITIS, DORA und andere Branchenanforderungen laufen in separaten Projekten, mit unterschiedlichen Fragebögen, Scorings und Reports. Das kostet Ressourcen und produziert trotzdem Widersprüche.

Tool-Chaos statt durchgängiger Steuerung

Risikoregister im GRC-System, ISMS in einer eigenen Lösung, Lieferanten im ERP, Vorfälle im Ticketsystem, Verträge im DMS, Auswertungen in Excel: Technisch ist vieles vorhanden, aber kaum durchgängig verbunden. Jede NIS2-Fragestellung wird zum manuellen Auswertungsprojekt – aufwendig und anfällig.

Ressourcenknappheit & Zeitdruck

Security- und Compliance-Teams sind meist knapp besetzt, NIS2 läuft dann häufig zusätzlich zum Tagesgeschäft. Spätestens mit ersten Prüfungen, Nachweisforderungen oder größeren Vorfällen zeigt sich, dass es an Struktur, Priorisierung und integrierten Lösungen fehlt.

07.

Anforderungen an NIS2-Tools und -Prozesse

Damit NIS2 nicht in zusätzlichen Insellösungen endet, braucht es Prozesse und Tools, die die gesetzlichen Anforderungen wirklich abbilden und nicht nur ein generisches ISMS „drüberstülpen".

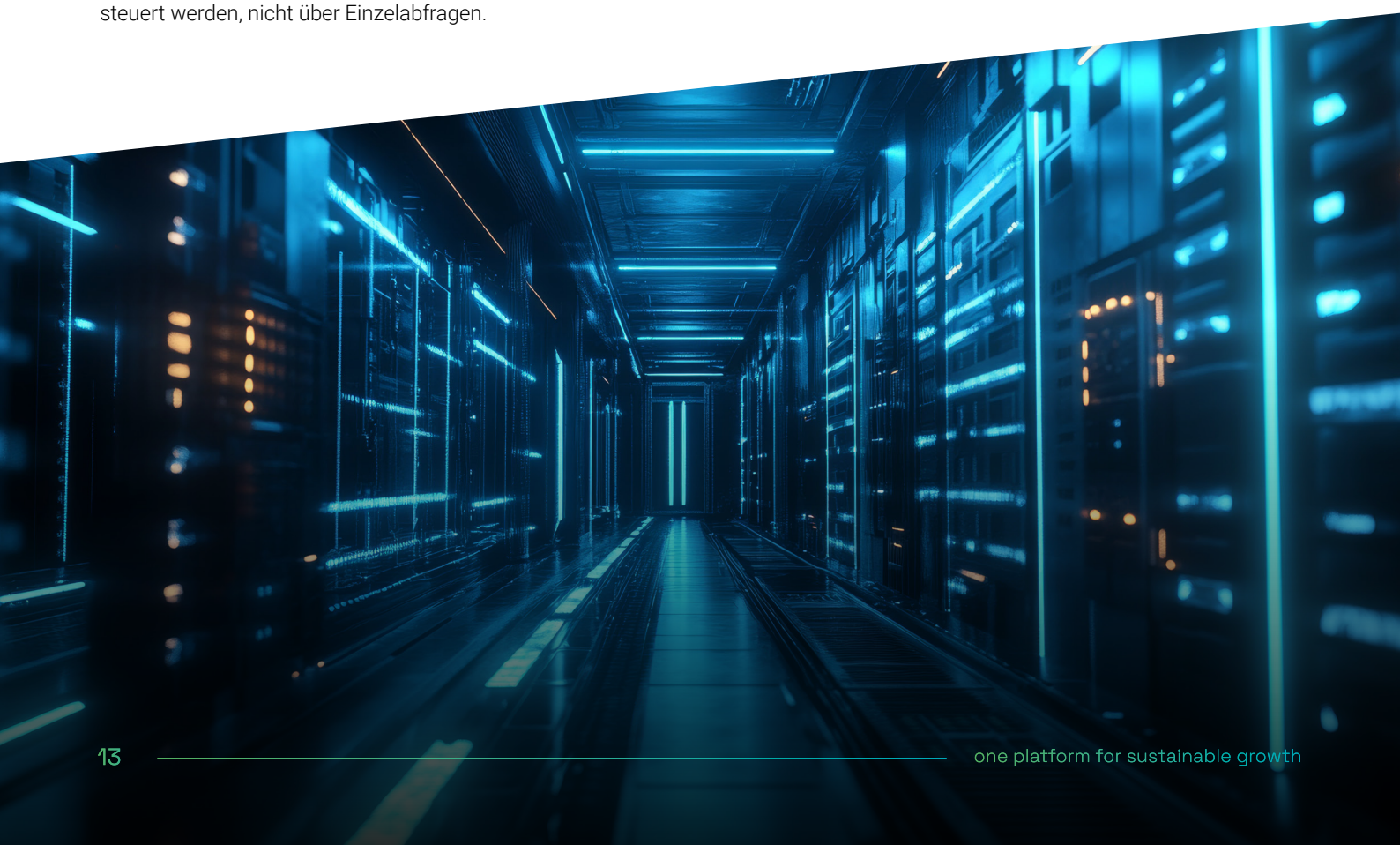
Ein zentraler Baustein ist ein NIS2-spezifisches **Risikomodell** mit einem passenden **Fragenkatalog** und definierten Nachweisarten. Es reicht nicht, irgendein ISMS zu betreiben. Die Lösung sollte Risiken entlang der geforderten Themen (Governance, Risikomanagement, Meldepflichten, Drittrisiko) strukturiert erfassen und bewerten – so, dass Ergebnisse und Nachweise prüffähig auf NIS2 referenzieren und als fachliche Grundlage für die weitere Umsetzung dienen.

Darauf aufbauend braucht es **durchgängige Workflows und sinnvolle Automatisierung.** Risiken müssen systematisch erfasst, bewertet und behandelt werden – inklusive klarer Zuständigkeiten und Fristen. Sicherheitsvorfälle sollten von der ersten Erkennung über die interne Bearbeitung bis hin zur fristgerechten Meldung an die Behörde in einem einheitlichen Incident-Prozess laufen. Dasselbe gilt für die Bewertung von Lieferanten und Dienstleistern: Third-Party-Risiken sollten über standardisierte Bewertungslogiken und wiederverwendbare Fragebögen gesteuert werden, nicht über Einzelabfragen.

Wesentlich ist außerdem eine **saubere Integration in die bestehende Systemlandschaft.** NIS2-Prozesse sollten mit vorhandenen ISMS-Lösungen, SIEM/SOC-Systemen, ERP, GRC-Tools und bestehenden Due-Diligence-Plattformen zusammenspielen. Idealerweise werden Stammdaten, Ereignisse und Maßnahmen übernommen, statt parallel gepflegt. Nur so entsteht ein konsistentes Bild über Risiken, Vorfälle und Abhängigkeiten.

Ein gutes NIS2-Setup kommt ohne **stabiles Reporting und lückenlosen Audit-Trail** nicht aus. Aufsichtsbehörden, Revision und Management wollen nachvollziehen können, welche Risiken identifiziert wurden, welche Maßnahmen beschlossen und umgesetzt sind, wie Vorfälle behandelt wurden und wer welche Entscheidung getroffen hat. Eine geeignete Lösung sollte diese Nachweise ohne großen manuellen Aufwand erzeugen können.

Schließlich hilft eine **zentrale Dokumentenbibliothek,** die notwendigen Richtlinien und Regelwerke im Unternehmen zu verankern. Darin sollten Vorlagen für die zentralen Richtlinien bereitstehen, die im Sinne der NIS2-Anforderungen im Unternehmen notwendig sind, etwa zu Rollen und Verantwortlichkeiten, Incident Management, Schwachstellenmanagement oder Lieferantenmanagement. Diese Templates sind so aufgebaut, dass sie konkrete Vorschläge für unternehmensinterne Regelungen machen, gleichzeitig aber an die jeweiligen Gegebenheiten und Strukturen des Unternehmens angepasst werden können.



08.

Wie osapiens unterstützt: osapiens HUB for NIS2 im Kontext des osapiens HUB for Supplier Intelligence

NIS2-Modul als Teil des osapiens HUB

Das NIS2-Modul im osapiens HUB bildet die Anforderungen der Richtlinie in klaren Prozessen, Kontrollen und Fragebögen ab. Scope, Einrichtungsarten und betroffene Gesellschaften werden strukturiert erfasst; der Umsetzungsstand lässt sich über eine Reifegradsteuerung gezielt planen und nachverfolgen.

Automatisierte Transparenz & AI-Unterstützung

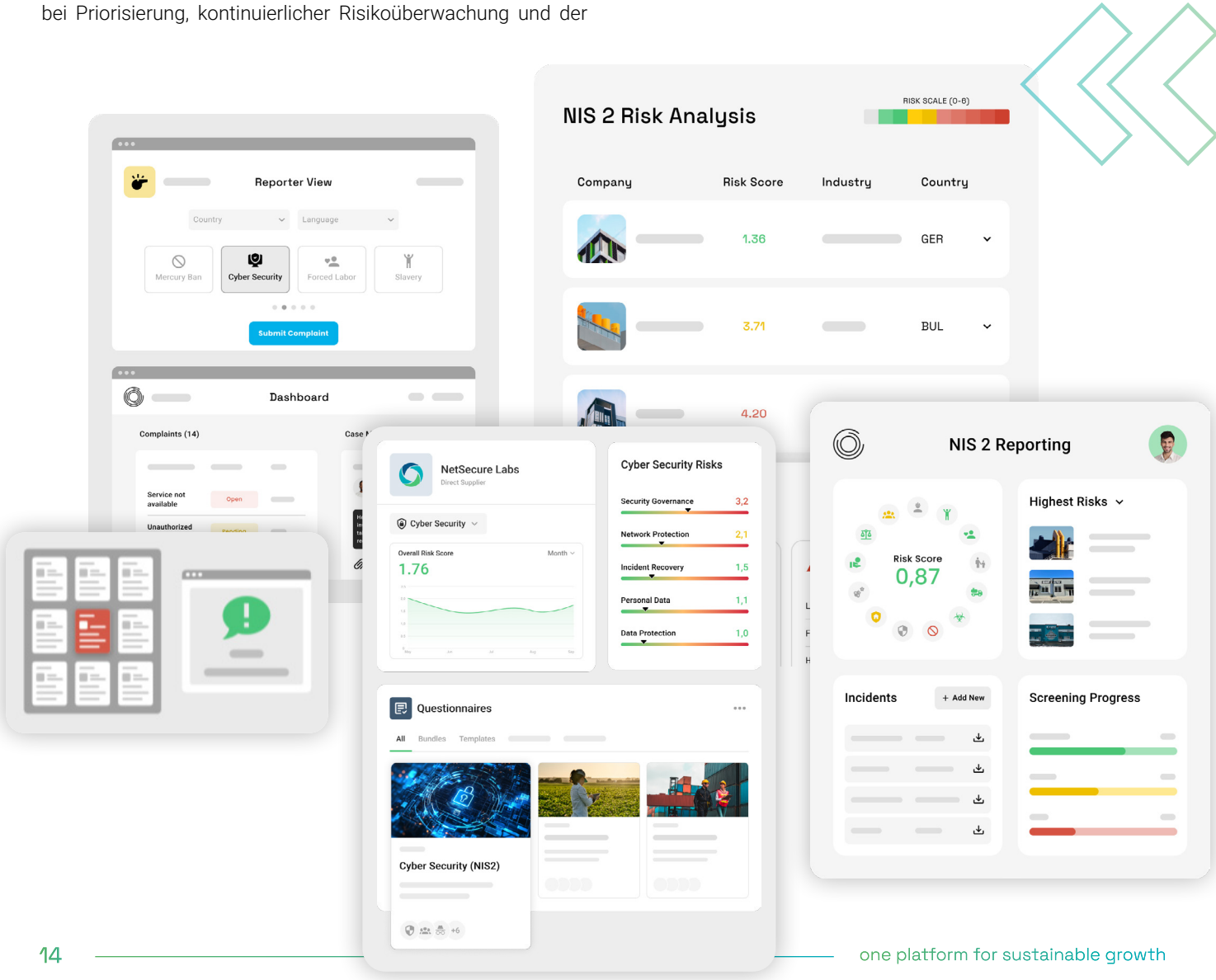
Für NIS2-Risikobewertungen nutzt der osapiens HUB vorhandene Unternehmens- und Lieferantendaten. Darauf aufbauend unterstützen automatisierte Auswertungen und KI-Funktionen bei Priorisierung, kontinuierlicher Risikoüberwachung und der Ableitung konkreter Handlungsempfehlungen. Dazu gehört auch ein KI-gestütztes News Monitoring, das relevante Meldungen scannt und Alerts auslöst, sobald risikorelevante Ereignisse oder Hinweise zu Unternehmen und Lieferanten erscheinen.

Richtlinien Templates & ISMS Starthilfe

Für Unternehmen ohne etabliertes ISMS stellt das NIS2 Modul praxiserprobte Vorlagen für zentrale Richtlinien und Regelwerke bereit. So lassen sich grundlegende ISMS Bausteine schnell aufsetzen und unternehmensspezifisch anpassen, ohne bei Null zu starten.

Incident- & Meldeprozesse

Sicherheitsvorfälle werden in standardisierten Workflows erfasst, bewertet und eskaliert. Die Lösung unterstützt bei der strukturierten Aufbereitung der Informationen, die für Meldungen an die zuständigen Behörden nach NIS2 erforderlich sind. Plattformvorteile: NIS2 integriert in der osapiens HUB for Supplier Intelligence Lösung



Unternehmen mit **bestehendem Einsatz des osapiens HUB for Supplier Intelligence (LkSG / CSDDD):**

- **Wiederverwendung vorhandener Daten**
  Lieferanten-, Dienstleister- und Gesellschaftsstammdaten sowie bestehende Risikobewertungen aus dem osapiens HUB for Supplier Intelligence werden für NIS2 mitgenutzt. Zusätzliche Datenerhebung und Pflege bleiben auf das notwendige Minimum beschränkt.
- **Vordefinierte NIS2-Fragebögen & Evidenz-Templates**
  Standardisierte Fragebögen für NIS2-relevante Lieferanten (und perspektivisch auch für eigene Gesellschaften) sowie klar definierte Nachweisarten, die strukturiert hochgeladen werden können (z. B. ISO 27001/22301, ISIS12). Die Nachweise fließen inklusive Scope-Betrachtung in die Bewertung ein und machen Ergebnisse konsistent nachvollziehbar.
- **Gemeinsame Plattform-Logik**
  Gleiches Rollen- und Berechtigungskonzept, gleiche UI, gleiche Workflow-Engine für LkSG/CSDDD und NIS2. Das reduziert Einarbeitungsaufwand und erleichtert die Steuerung über mehrere Regime hinweg.
- **Modulares Andocken statt Neu-Einführung**
  Das NIS2-Modul kann als Add-on zur bestehenden Lösung hinzugefügt werden. Bereits angebundene Systeme (z. B. ERP, HR, Ticketing, SIEM/SOC, GRC) können weiterverwendet werden, zusätzliche Schnittstellen bleiben überschaubar.
- **Single Source of Truth für Compliance & Risiko**
  Risiken, Maßnahmen, Vorfälle und lieferantenbezogene Informationen werden einheitlich geführt – über NIS2, LkSG, CSDDD und weitere Anwendungsfälle hinweg. Das erleichtert konsistente Auswertungen für Management, Aufsicht und Revision.

Für **Neueinsteiger**

- **Einstieg über ein klar strukturiertes NIS2-Setup,** das von Anfang an auf spätere Erweiterung ausgelegt ist, etwa um Supply Chain Risk Management und weitere Anforderungen wie CSDDD.
- **Vermeidung von Insellösungen,** die in 1–2 Jahren wieder abgelöst oder integriert werden müssen.

09.

NIS2 umsetzen: Fahrplan in 5 Schritten

01 **Betroffenheit und Governance klären**
Einstufung als besonders wichtige bzw. wichtige Einrichtung, Abgrenzung der betroffenen Gesellschaften und Dienste, Festlegung von Verantwortlichkeiten, Gremien und Berichtslinien.

02 **Ist-Analyse und Lückenbewertung**
Bestehende Sicherheits-, Risiko- und Compliance-Strukturen systematisch gegen die NIS2-Pflichten spiegeln: Governance, ISMS, Incident Management, Dienstleistersteuerung, Dokumentation.

03 **Zielbild und Maßnahmenplan festlegen**
Zielbild für NIS2 definieren und in einen priorisierten Maßnahmenplan überführen: mit Meilensteinen, Verantwortlichkeiten und Ressourcen. Wo möglich Maßnahmen so wählen, dass sie gleichzeitig andere Regulierungen (z. B. LkSG, CSDDD) adressieren.

04 **Prozesse und Tools implementieren**
Bestehende Prozesse anpassen, fehlende Workflows für Risiko, Vorfälle und Lieferanten aufsetzen und geeignete Tools bzw. eine Plattformlösung (z. B. NIS2-Modul im osapiens HUB) in die bestehende Systemlandschaft integrieren.

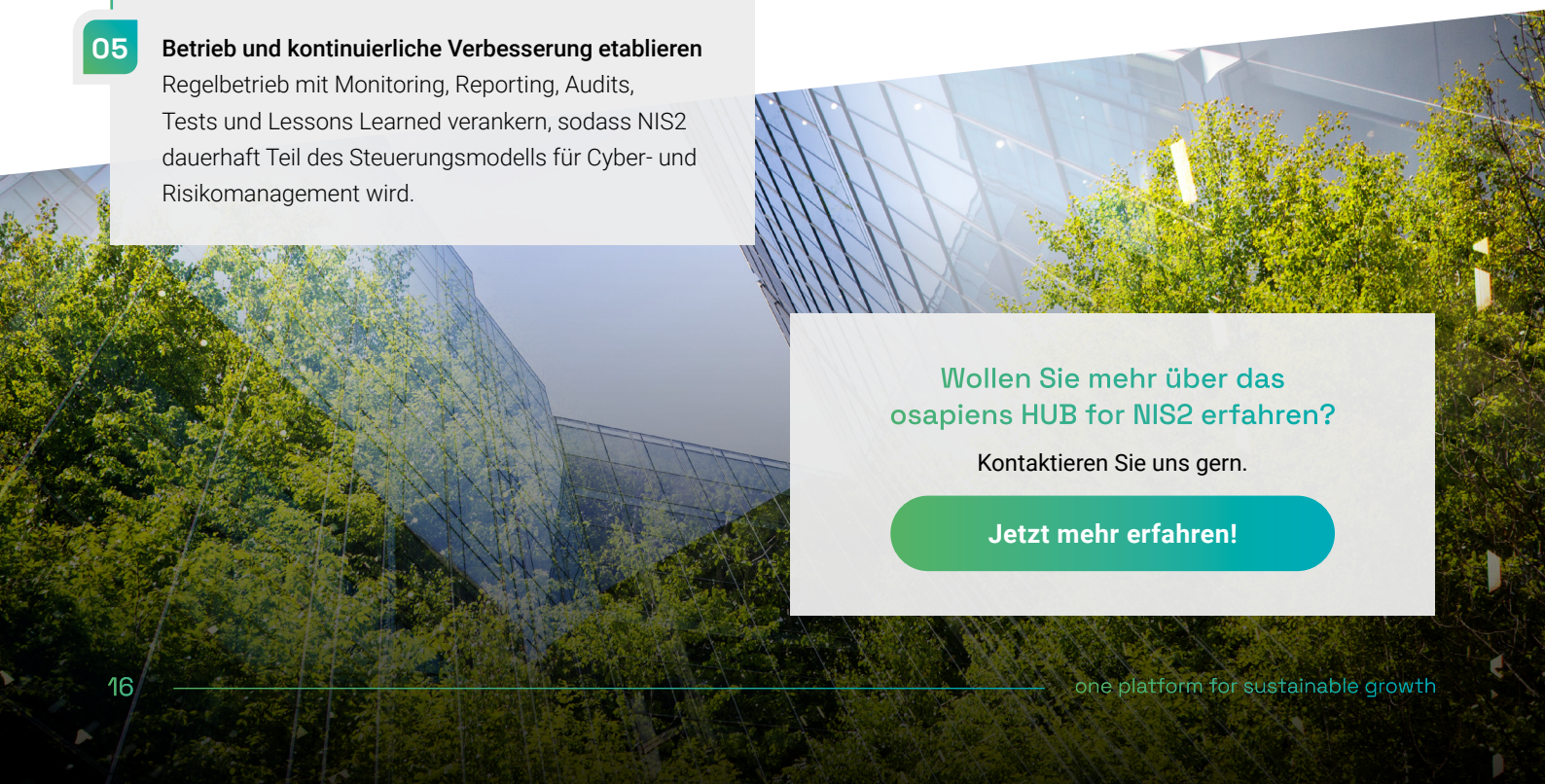
05 **Betrieb und kontinuierliche Verbesserung etablieren**
Regelbetrieb mit Monitoring, Reporting, Audits, Tests und Lessons Learned verankern, sodass NIS2 dauerhaft Teil des Steuerungsmodells für Cyber- und Risikomanagement wird.

→ Hinweis für Unternehmen mit **bestehendem osapiens Setup**

Wenn Sie für die Umsetzung von LkSG und/oder CSDDD bereits mit dem osapiens HUB for Supplier Intelligence arbeiten, sind viele Bausteine aus den Schritten 1–3 bereits vorhanden: Lieferanten- und Dienstleisterstammdaten, Due-Diligence-Prozesse und Teile des Risikomanagements liegen im System vor. Der lieferkettenbezogene Teil von NIS2 ist damit weitgehend vorbereitet.

Wichtig ist dennoch eine saubere Betroffenheitsprüfung über das gesamte Unternehmen hinweg: Für die NIS2-Einstufung zählt die gesamte wirtschaftliche Tätigkeit der Organisation, im Zweifel kann auch eine Nebentätigkeit die NIS2 Betroffenheit auslösen. Auf dieser Basis unterstützt das NIS2-Modul insbesondere bei den zusätzlichen Anforderungen rund um Governance, Incident Management und die erforderlichen Nachweise.

Wer diesen Fahrplan konsequent umsetzt, stellt die rechtssichere Erfüllung der NIS2-Pflichten sicher – und hebt zugleich Cyber- und Risikomanagement auf ein Niveau, das klare Zuständigkeiten, belastbare Daten und nachvollziehbare Entscheidungen im Alltag ermöglicht.



Wollen Sie mehr über das osapiens HUB for NIS2 erfahren?

Kontaktieren Sie uns gern.

Jetzt mehr erfahren!

osapiens – one platform for sustainable growth

osapiens entwickelt cloudbasierte Softwarelösungen, die Unternehmen dabei unterstützen, nachhaltiges Wachstum entlang ihrer gesamten Wertschöpfungskette zu fördern. Durch leistungsstarke Datenintegration und Echtzeitanalysen hilft osapiens, komplexe operative Daten und Nachhaltigkeitskennzahlen zu konsolidieren, auszuwerten und zielgerichtete Maßnahmen abzuleiten.

Der osapiens HUB, eine skalierbare, KI-basierte Plattform, vereint über 25 Lösungen zur Optimierung der operativen Effizienz und des nachhaltigen Wirtschaftens in zwei Kernbereichen: **Transparency Solutions** ermöglichen die Abbildung und Überwachung der gesamten Wertschöpfungskette, um Lieferkettenrisiken zu minimieren und regulatorische Anforderungen wie EUDR, CSRD und CSDDD zu erfüllen. **Efficiency Solutions** sorgen für reibungslose und effiziente Abläufe – von der digitalen Instandhaltung über das Asset Management bis hin zur Planung und Umsetzung von Field Service Tätigkeiten.

Mit Hauptsitz in Mannheim unterstützt osapiens mit einem internationalen Team von über 550 Mitarbeitenden mehr als 2.500 Kunden weltweit.

2.500 + Kunden
60 + Länder
550 + Mitarbeitende
60 + Nationalitäten

Kontakt

Julius-Hatry-Straße 1
68163 Mannheim

info@osapiens.com
+49 (0) 621 15020690
www.osapiens.com

Besuchen Sie uns auf LinkedIn