BATTKE GRÜNBERG

battke-gruenberg.de

1. September 2026

9 Monate NIS2 - Wo Unternehmen jetzt stehen

NIS2 ist in der Unternehmenspraxis angekommen – aber wie weit sind betroffene Unternehmen tatsächlich?

Josephine Klawon, LL.M. || Ron Klas

IHRE ANSPRECHPARTNERIN

Josephine Klawon LL.M.
Rechtsanwältin

klawon@battke-gruenberg.de
+49 351 563 90 20

- Marken- und Designrecht
- Urheber- und Medienrecht
- Wettbewerbsrecht
- IT-/Softwarevertragsrecht

UNSER IT-KOOPERATIONSPARTNER

Ihr Ansprechpartner:

Ron Klas

Sales4C

Projekt- und Programm-Management

IT-Service Management

HCM Clouds, Recruiting & Talent Management

IT-Infrastruktur, IT-Multivendor-Support

Spezialisierungen:
Change-Management, OutTasking und Managed Services, Personalentwicklung und Modernes Führen, KRITIS, NIS2, IT-Security, IT-Vergabe, Mitbestimmungen (BetrVG)

Die Rechtslage ist klar – der eigene Stand oft nicht.

- **Seit 6. Dezember 2025 gilt NIS2 in Deutschland.**
- **Rund 29.500 Unternehmen und Einrichtungen stehen unter BSI-Aufsicht.**
- **Registrierung, Risikomanagement und Meldefähigkeit sind operative Pflichten.**
- **Die Registrierungsfrist ist abgelaufen.**

Wer ist betroffen?

1 Welcher Sektor?

- Energie
- Trink-/Abwasser
- Sozialversicherung
- Gesundheit
- Abfallentsorgung
- Industrie/Chemie/ Maschinenbau
- Digitale Dienste
- Verkehr
- Lebensmittel
- Finanzmarkt
- Digitale Infrastruktur
- Forschung
- Bankwesen/Finanz markt
- Post-/Kurierdienste

2 Welche Größe?

≥ 50 Mitarbeitende *oder*

> 10 Mio. EUR Jahresumsatz

und Bilanzsumme

3 Ausnahmen?

- Nebentätigkeit?
- Spezialbereiche?
- Faktische Unabhängigkeit von Partnerunternehmen?
- Öffentliche Verwaltung?

PFLICHTENKATALOG

Pflichtenkatalog	wichtige / besonders wichtige Einrichtungen	KRITIS-Betreiber
Risikomanagementmaßnahmen	✓	✓
Registrierung	✓	✓
Meldung von Sicherheitsvorfällen	✓	✓
Schulungen & Prävention	✓	✓
Besonderer Pflichtenmaßstab		✓
Systeme zur Angriffserkennung		✓
24/7 Erreichbarkeit		✓
Aktive Nachweispflicht		✓

Praxislücke beim Einstieg

Nicht mit Bußgeldern starten, sondern mit der Frage: „Können wir unseren aktuellen Stand erklären, priorisieren und belegen?“

Die entscheidende Frage lautet heute nicht mehr:

- *„Kommt NIS2?“*
- Sondern: *„Können wir unseren aktuellen Stand erklären und belegen?“*

NIS2 ist nicht mehr primär ein Gesetzgebungsthema, sondern eine Frage der betrieblichen Steuerungs- und Nachweisfähigkeit.

„Wir machen doch schon IT-Sicherheit“ – aber reicht das als Nachweis?

22%	71%	26%
haben ihre Betroffenheit eindeutig geklärt	der potenziell Betroffenen halten sich für „ready“	verfügen über ein ISMS

Typische Lücke:
Maßnahmen sind teilweise vorhanden – aber Verantwortlichkeit, Priorisierung, Dokumentation und Wirksamkeitsnachweis fehlen.

Verweis: Die ENISA-Auswertung unterstreicht > besonders anspruchsvoll sind Patch- und Schwachstellenmanagement, Betriebsfortführung und Wiederherstellung sowie Lieferkettenrisiken; zugleich haben KMU über alle betrachteten Dimensionen hinweg größere Schwierigkeiten als größere Organisationen.

In 30 Minuten vom Nebel zur belastbaren Startlinie

1. Orientieren

Welche Anforderungen treffen uns?
Wer übernimmt Verantwortung?

2. Bewerten

Wo stehen wir tatsächlich?
Was ist belegt, was nur angenommen?

3. Priorisieren

Welche Lücken haben zuerst Wirkung?
Wer macht was bis wann?

COMPLIANCE-PLATTFORM

Entrasec Comply

Regulatorische Klarheit in 30 Minuten.

Alle Pflichtfelder des Mittelstands — bewerten, nachweisen, prüfen lassen.

NIS2 · CRA · ISO 27001 · ISO 42001 · EU AI Act · DORA · TISAX

Made in Germany · EU-Hosting · DSGVO-konform

AUSGANGSLAGE

Die Regulierungswelle trifft alle gleichzeitig

NIS2, CRA, DORA, EU AI Act, ISO 27001 — jedes Regelwerk mit eigener Logik, eigenen Fristen, eigenen Nachweisen.

1

Jedes Regelwerk als Insel

NIS2 im Excel, ISO im Ordner, DSGVO beim DSB. Keine Sicht auf das Ganze.

2

Dieselbe Frage dreimal beantwortet

Zugriffskontrolle, Backup, Lieferkette — inhaltlich identisch, dreimal erhoben.

3

Nachweise, die keiner findet

Beim Audit beginnt die Suche nach Belegen von vorn — ohne Versionsstand.

4

Beraterkosten, die wiederkehren

Jede Erhebung von außen eingekauft. Wissen bleibt nicht im Haus.

Das Ergebnis: viel Aufwand, wenig Aussage. Und beim nächsten Regelwerk beginnt alles von vorn.

DIE LÖSUNG

Eine Plattform statt sieben Insellösungen

Bewerten, umsetzen, kontinuierlich betreiben — in einem System, auf einer Datenbasis.

01

Bewerten

Strukturierte Prüffragen statt Paragrafen. Reifegrad 0–4 mit Konfidenz und Evidenz — je Domäne und im Gesamtbild.

Assessment

02

Umsetzen

Aus den Lücken wird ein priorisierter Maßnahmenplan: Wirkung, Aufwand, Phase. Verantwortliche und Fristen inklusive.

Maßnahmen

03

Betreiben

Risiken, Lieferanten, Assets, Prozesse, Audits — mit Review-Zyklen und Audit-Trail dauerhaft gepflegt.

IMS-Plattform

Und das über alle Pflichtfelder hinweg — nicht nur für den einen Standard, der gerade drängt.

ABDECKUNG

12 Regelwerke — vorbereitet, nicht selbstgebaut

Fragen, Controls und Hilfetexte sind fachlich ausgearbeitet und gepflegt. Sie starten am Tag 1, nicht nach dem Katalogbau.

NIS2 EU/EWR · 84 Fragen	**CRA** Cyber Resilience Act	**ISO 27001** Informationssicherheit	**ISO 42001** KI-Management	**ISO 27701** Datenschutz-MS	**EU AI Act** KI-Governance
DORA Finanzsektor EU	**TISAX** Automotive	**BSI Grundschutz** Deutschland	**LkSG** Lieferkette DE	**BACS IKT** Schweiz	**AT-ISH** Österreich

792
Prüffragen gesamt

708
hinterlegte Controls

DE · EN
Katalog vollständig zweisprachig

Orange umrandet: die Regelwerke mit dem größten Zulauf im Mittelstand. Je Assessment sind 40–92 Fragen zu beantworten.

VOLLSTÄNDIGKEIT

Alles, wozu ein Mittelständler heute verpflichtet ist

Nicht ein Standard, sondern jedes Feld, in dem Ihr Unternehmen nachweispflichtig ist — in einem System, auf einer Datenbasis.

Informationssicherheit

ISO 27001 · BSI IT-Grundschutz · TISAX

Reifegrad je Domäne, Controls, Erklärung zur Anwendbarkeit.

Cyber-Regulierung

NIS2 · CRA · DORA

Betroffenheit, Pflichten und Umsetzungsstand je Regelwerk.

Datenschutz

ISO 27701 · VVT · DSFA · Betroffenenanträge

Verzeichnis nach Art. 30, Folgenabschätzung, Fristen für Anträge.

KI-Governance

EU AI Act · ISO 42001

Use-Cases mit Risikoklasse, Rolle und Auswirkungsbewertung.

Lieferkette

LkSG · Lieferanten-Fragebögen

Kritikalität, Selbstauskünfte, Nachweise mit Wiedervorlage.

Meldepflichten

NIS2 24 h / 72 h · BSI · DORA 4 h

Fristen laufen ab dem richtigen Zeitpunkt, Kontakte hinterlegt.

Interne Prüfung

Audit-Workspace · Feststellungen

Vom Review zum Audit bis zum geprüften Reifegrad.

Steuerung & Nachweis

Risiken · Maßnahmen · Prozesse · Schulungen

Verantwortliche, Fristen, Versionen, Audit-Trail.

Bewusst nicht abgedeckt: Qualitäts- und Umweltmanagement (ISO 9001 / 14001) sowie ESG- und CSRD-Berichterstattung.

BELASTBARKEIT

Vom Selbstcheck zum geprüften Nachweis

Selbsteinschätzung ist der Anfang, nicht das Ergebnis. Zwei Bausteine machen daraus einen Nachweis, der einer Prüfung standhält.

Audit-Workspace

Ihre eigene Prüfung

- Review im Vier-Augen-Prinzip: Antworten werden geprüft, bevor sie zählen.
- Aus dem Review entsteht per Wizard ein Audit mit Prüfpositionen und Evidenzliste.
- Je Position ein Prüfergebnis — bestätigt oder Abweichung, mit Feststellung.
- Ergebnis ist ein geprüfter Reifegrad, nicht mehr nur eine Selbstauskunft.
- Externe Prüfer kommen als Gast-Auditor: befristet, ohne festen Nutzerplatz.

Lieferanten-Fragebögen

Die Prüfung Ihrer Kette

- Eigener Fragenkatalog je Projekt — passend zu Kritikalität und Branche.
- Versand an den Lieferanten über ein externes Portal, ohne Benutzerkonto.
- KI-Vorprüfung der Antworten markiert Lücken und Widersprüche.
- Rückfrageschleife mit gesperrten Feldern und vollständiger Antworthistorie.
- Das Ergebnis landet direkt im Lieferantenregister, mit Wiedervorlage.

Wer nachweisen muss, braucht eine Prüfspur — keine Excel-Tabelle mit grünen Häkchen.

EFFIZIENZ

Und die Vollständigkeit bleibt bezahlbar

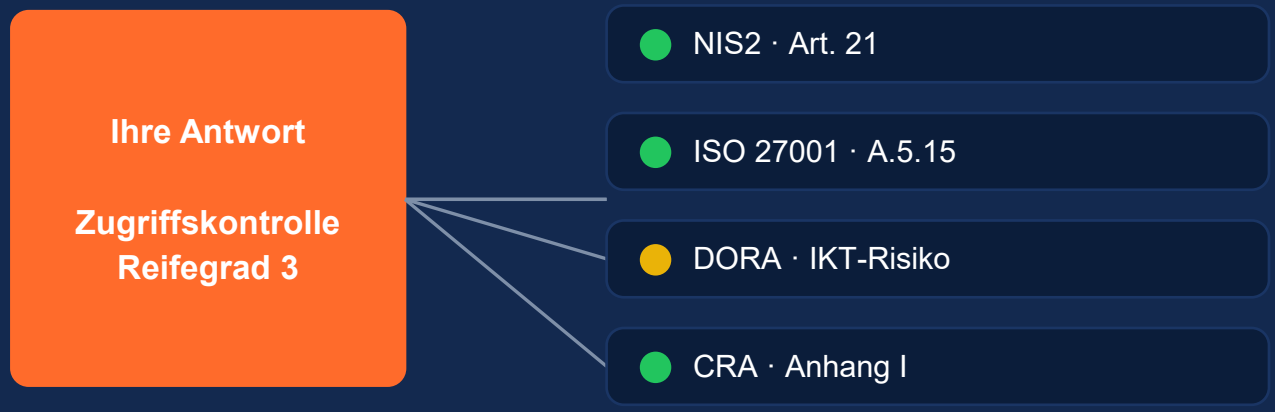
644 fachliche Verknüpfungen sorgen dafür, dass das zweite und dritte Regelwerk nicht den doppelten Aufwand bedeuten.

644

Cross-Mappings zwischen den Regelwerken

Beantworten Sie „Zugriffskontrolle“ für NIS2, ist dieselbe Aussage in ISO 27001, DORA und CRA sichtbar — inklusive Nachweis.

Eine Antwort — vier Wirkungen



Breite Abdeckung ohne Mehrfacharbeit — bis zu 60 % weniger Aufwand ab dem zweiten Regelwerk.

Die Mappings sind fachlich gepflegt, nicht per Stichwortsuche erzeugt — jede Verknüpfung ist im Assessment nachvollziehbar.

SO LÄUFT ES AB

Vom ersten Login zum Audit-Nachweis

Kein Implementierungsprojekt. Der erste belastbare Reifegrad steht am selben Tag.

1 — 10 Min.

Scope klären

Zwei-Stufen-Wizard: Profil und Checkliste. Ergebnis: nur die Normen, die Sie wirklich treffen.

2 — 30–90 Min.

Assessment

40–92 Prüffragen je Regelwerk, mit Hilfetext, Kommentar und Evidenz-Upload.

3 — sofort

Auswertung

Reifegrad je Domäne, Gesamtscore, Delta zum Vormonat, Management-Report als PDF.

4 — laufend

Maßnahmen

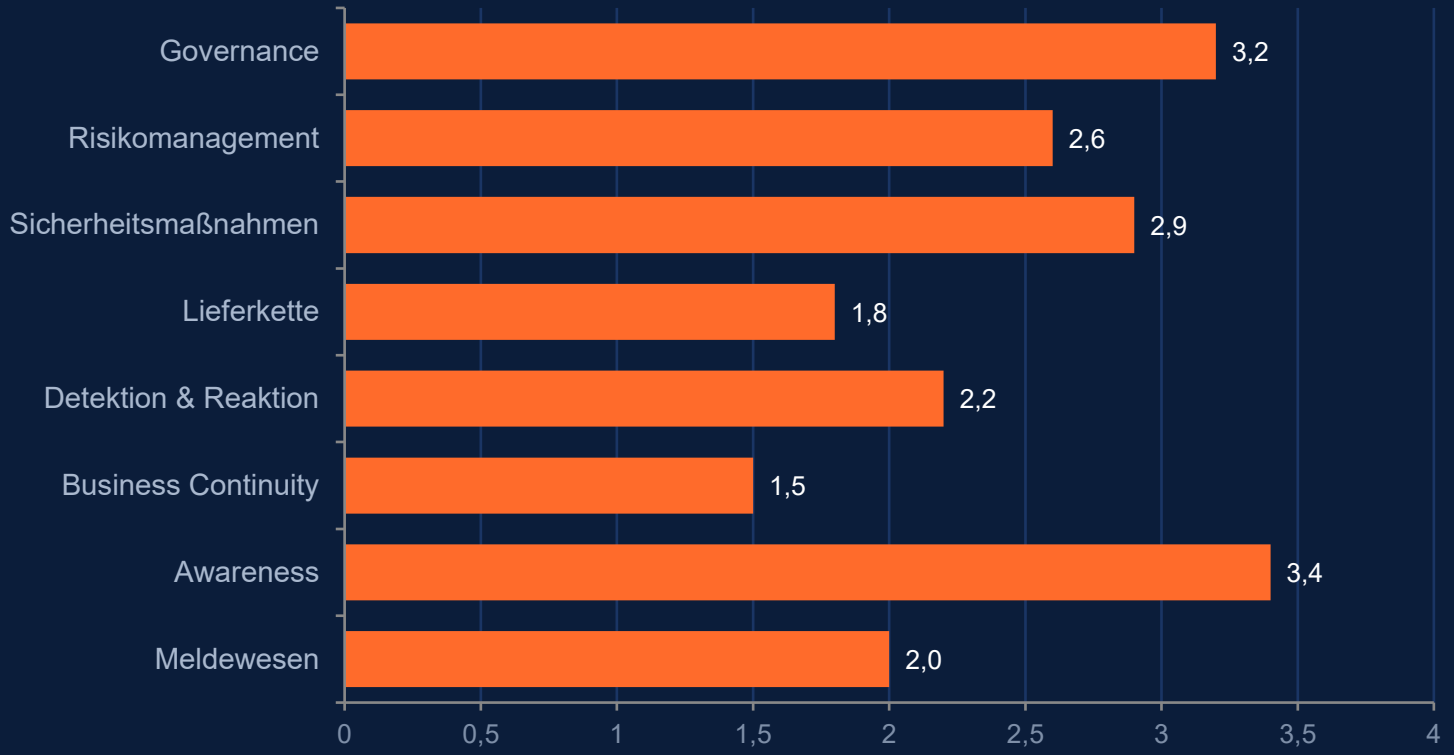
Priorisierter Plan nach Wirkung und Aufwand — mit Verantwortlichen und Wiedervorlage.

Danach: Wiederholung im Zyklus. Jedes Folge-Assessment zeigt das Delta — der Fortschritt wird belegbar, nicht behauptet.

DAS ERGEBNIS

Ein Reifegrad, den die Geschäftsführung versteht

Score je Domäne auf einer Skala von 0 bis 4 — mit Konfidenz und hinterlegtem Nachweis je Antwort.



Was daraus entsteht

Business Continuity
Kritische Lücke — Phase 1, hohe Wirkung

Lieferkette
Kritische Lücke — Nachweise fehlen

Meldewesen
Prozess vorhanden, nicht geübt

Awareness
Belegt, im Review-Zyklus

Export als Management-Report (PDF) — für Vorstand, Auditor und Kunde.

Beispieldarstellung mit fiktiven Werten.

KONTINUIERLICH BETREIBEN

Compliance endet nicht mit dem Assessment

Ein Prozess, ein Lieferant, ein KI-Use-Case existiert einmal — und ist zugleich DSGVO-, ISMS-, NIS2- und AI-Act-relevant.

Risiken

Bewertung, Behandlung, Review-Zyklus

Maßnahmen

Verantwortliche, Fristen, Status

Lieferanten

Kritikalität, Fragebögen, Wiedervorlage

Assets & Systeme

Schutzbedarf, Abhängigkeiten

Prozesse & VVT

Verarbeitungstätigkeiten nach Art. 30

DSFA & Anträge

Folgenabschätzung, Betroffenenrechte

KI-Use-Cases

Risikoklasse und Auswirkungsbewertung

Audits & Findings

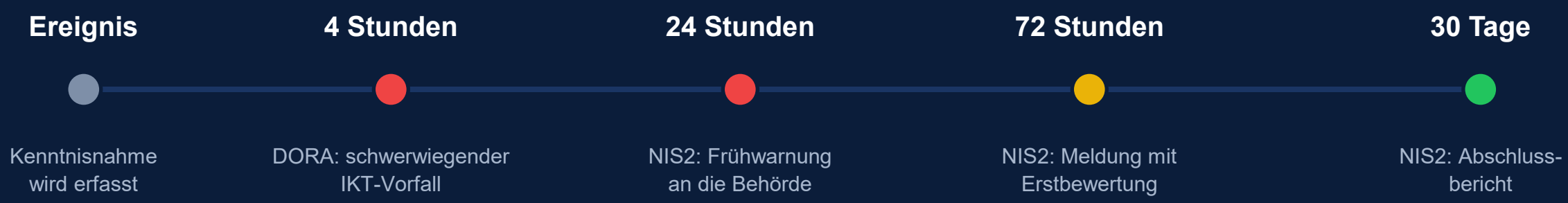
Feststellungen bis zur Erledigung

Dazu: Erklärung zur Anwendbarkeit (SoA), Nachweisverknüpfung und Audit-Trail. Die Compliance-Sicht zeigt je Anforderung, was bereits erfüllt ist.

ERNSTFALL

Wenn es passiert, laufen die Fristen sofort

Der Meldepflichten-Manager kennt die Fristen aus NIS2, BSI und DORA — und rechnet sie ab dem richtigen Zeitpunkt.



Meldekontakte mit Rollen

Melder, Incident-Lead, DSB, CISO, Management, extern — vorab hinterlegt.

KRITIS-Anlagen

BSI-Anlagennummer je Anlage, im Ernstfall sofort zur Hand.

Lückenloses Protokoll

Jede Aktion im Audit-Log — für die Nachbereitung mit der Behörde.

KI-UNTERSTÜTZUNG

KI hilft. Sie entscheiden.

Der Assistent kennt Ihre Branche, Ihre Antworten und den regulatorischen Kontext — und ist zu 100 % optional.

Advisor

Erklärt jede Prüffrage im Kontext Ihres Unternehmens und schlägt eine Einstufung vor.

Compliance-Chat

Rückfragen zum laufenden Assessment — mit Verlauf, je Assessment gespeichert.

Management-Report

Executive Summary aus den Ergebnissen — in der Sprache der Geschäftsführung.

Maßnahmenplan

Priorisierte Roadmap aus Ihren Lücken, nach Wirkung und Aufwand sortiert.

Ihre Kontrolle

- Die Plattform funktioniert vollständig ohne KI — kein Feature hängt davon ab.
- Prompt-Vorschau: Sie sehen vor dem Absenden, was übermittelt wird.
- Anbieterwahl: Anthropic, Mistral (EU) oder ein eigenes Modell im Haus.
- Vorschlag bleibt Vorschlag: Jede Einstufung bestätigt ein Mensch.

Keine Rechtsberatung — die Plattform zeigt, wo Sie stehen, und dokumentiert Ihre Entscheidungen.

VERTRAUEN

Eine Compliance-Plattform muss selbst sauber sein

Sicherheit, Datenstandort und Ausstiegsfähigkeit sind Produktbestandteil — nicht Verhandlungssache.

✓ EU-Hosting

Betrieb in der EU, AVV vorhanden, DSGVO-konforme Verarbeitung.

✓ Made in Germany

Entwicklung und Support aus Deutschland, deutsche Fachlogik.

✓ Authentisierung

MFA (TOTP), Account-Sperre, SSO via OIDC je Organisation.

✓ Feine Rechte

Rollen je Register — niemand vergibt mehr Rechte, als er selbst hat.

✓ Verschlüsselung

AES-256-GCM für Geheimnisse, eigener Schlüssel in der Produktion.

✓ Uploads geprüft

Jeder Nachweis läuft vor der Ablage durch den Virenscanner.

✓ Mandantentrennung

Alle Abfragen organisationsgebunden, vollständiger Audit-Trail.

✓ Datenexport

Vollständiger Export (EU Data Act, Art. 5) — kein Lock-in.

Audit-Trail über alle Änderungen · versionierte Nachweise · rollenbasierte Freigaben