LEITFADEN · SELBST-CHECK

ITS AG

NIS2-Quick-Check für mittelständische IT-Verantwortliche

In 30 Minuten klären, ob Ihr Unternehmen unter NIS2 fällt – und welche Maßnahmen dann konkret zu erwarten sind.

Lesezeit	Format	Rechtsstand
30 Minuten	**Selbst-Check**	**Dez. 2025**

Ein Praxis-Leitfaden der ITS AG. Rechtsstand: NIS2-Umsetzungsgesetz, in Kraft seit 06.12.2025. Keine Rechtsberatung.

WORUM ES GEHT

01 NIS2 ist kein Zukunftsthema mehr – das Gesetz gilt

Viele Unternehmen warten noch auf NIS2. Das Warten ist vorbei: Das deutsche Umsetzungsgesetz wurde verabschiedet und ist in Kraft. Die zentralen Pflichten gelten unmittelbar – ohne komfortable Übergangsfrist.

~29.500

Einrichtungen in Deutschland fallen voraussichtlich unter NIS2 – statt bisher rund 4.500 unter der alten KRITIS-Regelung.

18

betroffene Sektoren in zwei Anlagen – von Energie und Gesundheit bis zu produzierendem Gewerbe und IKT-Diensten.

10Mio€

Bußgeld-Rahmen für besonders wichtige Einrichtungen – plus persönliche Haftung der Geschäftsleitung.

Rechtsstand kurz & konkret

Das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) wurde im November 2025 von Bundestag und Bundesrat beschlossen, im Dezember 2025 verkündet und ist **seit dem 06.12.2025 in Kraft**. Es reformiert das BSI-Gesetz (BSIG). Die materiellen Sicherheitsanforderungen gelten unmittelbar; Unternehmen werden **nicht automatisch benachrichtigt** – die Selbsteinschätzung ist Pflicht.

Auch wenn Sie nicht direkt betroffen sind: NIS2 verpflichtet betroffene Unternehmen, ihre Lieferkette abzusichern (§30). Als Zulieferer oder IT-Dienstleister werden diese Anforderungen vertraglich an Sie weitergereicht. Cybersicherheit wird so zum Wettbewerbsfaktor – nicht nur zur Pflicht.

SCHRITT 1–3

02 Sind Sie betroffen? In drei Schritten klären

Die Betroffenheit ergibt sich aus drei Fragen, die Sie nacheinander beantworten: Gehören Sie zu einem regulierten Sektor? Überschreiten Sie die Größenschwellen? Und in welche Kategorie fallen Sie damit?

Schritt 1 · Sektor

Gehört Ihre Tätigkeit zu einem der 18 Sektoren in zwei Anlagen?

Anlage 1 – Sektoren hoher Kritikalität	Anlage 2 – weitere kritische Sektoren
Energie · Transport/Verkehr · Bankwesen	Post- und Kurierdienste
Finanzmarktinfrastruktur · Gesundheit	Abfallwirtschaft · Chemie
Trinkwasser · Abwasser	Lebensmittel (Produktion/Handel)
Digitale Infrastruktur · IKT-Dienste (B2B)	Verarbeitendes / produzierendes Gewerbe
Öffentliche Verwaltung · Weltraum	Digitale Dienste · Forschung

Schritt 2 · Größe

Überschreiten Sie mindestens eine dieser Schwellen (Mitarbeitende verbundener Unternehmen zählen mit)?

Kriterium	Schwelle
Beschäftigte	ab 50
Jahresumsatz	> 10 Mio. €
… und Jahresbilanzsumme	> 10 Mio. €

Schritt 3 · Einstufung

Kategorie	Schwelle (vereinfacht)	Aufsicht	Bußgeld bis
Besonders wichtig (bwE)	Anlage 1 & ab 250 MA oder > 50 Mio. € Umsatz	proaktiv	10 Mio. € / 2 %
Wichtig (wE)	übrige oberhalb der Größenschwelle	anlassbezogen	7 Mio. € / 1,4 %
Größenunabhängig	u. a. TK-/DNS-/Vertrauensdiensteanbieter, Betreiber kritischer Anlagen		—

Prozentwerte beziehen sich auf den weltweiten Jahresumsatz; es gilt der höhere Betrag. Vereinfachte Darstellung.

Tipp

Das BSI stellt eine (nicht rechtsverbindliche) Betroffenheitsprüfung bereit. Sie ersetzt keine belastbare Einordnung – nutzen Sie sie als Einstieg und lassen Sie Grenzfälle fachlich prüfen.

DIE PFLICHTEN

03 Die 10 Risikomanagement-Maßnahmen (§30 BSIG)

NIS2 verlangt einen „All-Gefahren-Ansatz“: Die Maßnahmen müssen angemessen, verhältnismäßig und wirksam sein und auch physische Risiken berücksichtigen. Bewerten Sie jede Maßnahme ehrlich per Ampel – das ist Ihr persönlicher Gap-Check.

	Maßnahme nach §30 Abs. 2 BSIG	Status (selbst eintragen)
1	Risikoanalyse und Sicherheitskonzepte für Informationssysteme	🔴🟡🟢
2	Bewältigung von Sicherheitsvorfällen (Incident Management)	🔴🟡🟢
3	Aufrechterhaltung des Betriebs: Backup-Management, Wiederherstellung, Krisenmanagement	🔴🟡🟢
4	Sicherheit der Lieferkette (Zulieferer, Dienstleister)	🔴🟡🟢
5	Sicherheit bei Beschaffung, Entwicklung und Wartung inkl. Schwachstellenmanagement	🔴🟡🟢
6	Verfahren zur Bewertung der Wirksamkeit der Maßnahmen	🔴🟡🟢
7	Cyberhygiene und regelmäßige Schulungen	🔴🟡🟢
8	Kryptografie und Verschlüsselung	🔴🟡🟢
9	Personalsicherheit, Zugriffskontrolle, Asset-Management	🔴🟡🟢
10	MFA / kontinuierliche Authentifizierung, gesicherte (Notfall-)Kommunikation	🔴🟡🟢

Gute Nachricht

Ein etabliertes Informationssicherheits-Managementsystem (ISMS) nach ISO 27001 deckt einen großen Teil dieser Anforderungen bereits ab. Die typischen verbleibenden Lücken sind die **BSI-Registrierung**, das formale **Meldeverfahren** und die **Pflichten der Geschäftsleitung**.

FRISTEN & HAFTUNG

04 Melden, registrieren, haften

Meldepflicht bei Sicherheitsvorfällen (§32 BSIG) – dreistufig

1. **Erstmeldung / Frühwarnung – binnen 24 Stunden**
   Unverzüglich ab Kenntnis eines erheblichen Sicherheitsvorfalls an das BSI.

2. **Bestätigung / Detailbericht – binnen 72 Stunden**
   Aktualisierte Bewertung, erste Erkenntnisse zu Ursache und Auswirkungen.

3. **Abschlussbericht – binnen 1 Monat**
   Ausführliche Beschreibung, Ursachen, ergriffene und geplante Maßnahmen.

Registrierung beim BSI

Betroffene Einrichtungen müssen sich über das BSI-Portal registrieren (mit ELSTER-Organisationszertifikat). Eine erste Frist lief im Frühjahr 2026 ab – eine verspätete Registrierung ist weiterhin möglich und dringend ratsam. Fehlende Registrierung ist ein eigener Bußgeldtatbestand.

Pflicht der Geschäftsleitung (§38)

Die Geschäftsleitung muss die Risikomaßnahmen **billigen und überwachen** – das ist nicht delegierbar – und an Schulungen teilnehmen. Bei Pflichtverletzung droht **persönliche Haftung**.

Bußgeldrahmen (§65)

Kategorie	Maximum	Auslöser (Beispiele)
Besonders wichtige Einrichtung	10 Mio. € / 2 %	fehlende Maßnahmen, fehlende Dokumentation
Wichtige Einrichtung	7 Mio. € / 1,4 %	Verstöße gegen Pflichten nach §30/§32
Ultima Ratio	**vorübergehende Untersagung der Geschäftstätigkeit möglich**	

IN 30 MINUTEN

05 Ihr Quick-Check – Schritt für Schritt

Mit dieser Zeiteinteilung kommen Sie in einer halben Stunde zu einer belastbaren Ersteinschätzung.

5' PHASE 1	**Sektor-Check**	Ordnen Sie Ihre Tätigkeit den 18 Sektoren zu (Schritt 1). Im Zweifel: eher zuordnen und genauer prüfen.
5' PHASE 2	**Größe prüfen**	Beschäftigte, Umsatz, Bilanzsumme – inklusive verbundener und Partnerunternehmen.
5' PHASE 3	**Einstufung**	Besonders wichtig, wichtig oder größenunabhängig? Damit kennen Sie Aufsichtsregime und Bußgeldrahmen.
15' PHASE 4	**Gap-Schnellcheck**	Gehen Sie die 10 Maßnahmen aus Abschnitt 03 per Ampel durch. Notieren Sie Ihre drei größten roten Punkte.

Sofort-Maßnahmen (Quick Wins)

- BSI-Registrierung anstoßen
- Mehr-Faktor-Authentifizierung flächendeckend aktivieren
- Meldewege und Notfallplan festlegen
- Awareness-Schulung für alle Mitarbeitenden

Mit 3–6 Monaten Vorlauf: Risikoanalyse, Backup-/Wiederanlauftests, Bewertung der Lieferkette und Aufbau eines ISMS.

Quellen (Auswahl): NIS2UmsuCG / BSIG-neu (BGBl. 2025 I Nr. 301, in Kraft seit 06.12.2025) · BSI, Informationen zu NIS-2-Risikomanagementmaßnahmen · EU-Richtlinie (EU) 2022/2555 · EU-Empfehlung 2003/361/EG (KMU-Definition).