NIS2-Compliance-Checkliste

Die zentralen Pflichten nach dem NIS2-Umsetzungsgesetz (NIS2UmsuCG) zum Abhaken · Stand: Oktober 2026

Diese Checkliste führt Sie durch die Pflichten des NIS2UmsuCG, das seit dem 6. Dezember 2025 in Kraft ist. Arbeiten Sie die Abschnitte der Reihe nach durch und halten Sie fest, wer bis wann zuständig ist. Die Liste ersetzt keine Rechtsberatung – sie sorgt dafür, dass nichts übersehen wird.

UNTERNEHMEN	STANDORT / BETRIEBSSTÄTTE
DATUM	VERANTWORTLICH (NAME)

1 Betroffenheit klären

NIS2 erfasst rund 29.500 Unternehmen in 18 Sektoren. Ob Sie dazugehören, entscheidet sich an Sektor und Größe.

	PRÜFPUNKT	ERGEBNIS	WER	BIS
☐	Gehört unser Hauptgeschäft zu einem der 18 NIS2-Sektoren (Anlage 1 oder 2)?			
☐	Erreichen wir die Schwelle: mindestens 50 Mitarbeitende **oder** mehr als 10 Mio. € Jahresumsatz?			
☐	Einstufung bestimmt: besonders wichtige (BEI) oder wichtige Einrichtung (WEI)?			
☐	Konzernstrukturen geprüft – gelten Zurechnungsregeln für Tochtergesellschaften?			
☐	Separat geprüft, ob zusätzlich das KRITIS-Dachgesetz greift (eigenes Verfahren, eigene Behörde)			

Grenzfall? Bei Konzernsachverhalten und Zulieferer-Konstellationen lohnt eine rechtliche Einzelfallprüfung – die Einstufung entscheidet über Aufsichtsdichte und Bußgeldrahmen.

2 Registrierung beim BSI

Die reguläre Frist lief am 6. März 2026 ab, die BSI-Nachfrist endete am 31. Juli 2026. Die Pflicht besteht unverändert fort.

	PRÜFPUNKT	ERGEBNIS	WER	BIS
☐	Registrierung über das BSI-Meldeportal erfolgt (bzw. umgehend nachgeholt)			
☐	Registrierungsbestätigung abgelegt und auffindbar			
☐	Kontaktstelle benannt, jederzeit erreichbar und im Portal hinterlegt			
☐	Prozess festgelegt, wie Änderungen (Kontakt, Sektor, Größe) nachgemeldet werden			

Achtung: Die fehlende Registrierung ist ein **eigenständiger** Bußgeldtatbestand mit bis zu 500.000 € – unabhängig davon, ob alle übrigen Pflichten erfüllt sind, und unabhängig davon, wie lange das Versäumnis andauert.

3 Risikomanagement – die zehn Pflichtbereiche

Das NIS2UmsuCG verlangt Risikomanagementmaßnahmen in zehn Bereichen. Halten Sie je Bereich fest, wo Sie stehen.

	BEREICH	STAND	WER	BIS
☐	1 · Risikoanalyse & Sicherheitskonzepte			
☐	2 · Bewältigung von Sicherheitsvorfällen			
☐	3 · Business Continuity, Backup & Krisenmanagement			
☐	4 · Sicherheit der Lieferkette			
☐	5 · Sicherheit bei Erwerb & Wartung von IT-Systemen			
☐	6 · Wirksamkeitsprüfung von Sicherheitsmaßnahmen			
☐	7 · Cyberhygiene & Schulungen			
☐	8 · Kryptografie & Verschlüsselung			
☐	9 · Personalsicherheit & Zugriffskontrolle			
☐	10 · Multi-Faktor-Authentifizierung & sichere Kommunikation			

Orientierung: Wer bereits ein ISMS nach ISO 27001 oder BSI IT-Grundschutz betreibt, deckt einen großen Teil dieser Bereiche ab und muss vor allem Lücken schließen und Nachweise ordnen.

4 Meldeprozess für Sicherheitsvorfälle

Bei erheblichen Vorfällen gilt eine gestufte Meldepflicht. Die Uhr läuft ab Kenntnisnahme – nicht ab Behebung.

	PRÜFPUNKT	STAND	WER	BIS
☐	**24 Stunden:** Frühwarnung an das BSI – Prozess definiert und erprobt			
☐	**72 Stunden:** Folgemeldung mit Bewertung und bisherigen Maßnahmen			
☐	**1 Monat:** Abschlussbericht			
☐	Rufbereitschaft geklärt: Wer meldet außerhalb der Geschäftszeiten und am Wochenende?			
☐	Meldeweg einmal im Trockenlauf geübt (Zugangsdaten, Ansprechpartner, Formulare)			
☐	Kriterien dokumentiert, wann ein Vorfall als „erheblich" gilt			

5 Geschäftsleitung: Pflichten und Haftung

NIS2 adressiert die Leitungsebene ausdrücklich. Diese Pflichten lassen sich nicht vollständig delegieren.

	PRÜFPUNKT	STAND	WER	BIS
☐	Geschäftsleitung hat die Risikomanagementmaßnahmen förmlich gebilligt			
☐	Überwachung der Umsetzung ist geregelt (Turnus, Berichtsweg, Protokoll)			
☐	Schulung der Leitungsebene absolviert und dokumentiert			
☐	Regelmäßige Schulungen für Mitarbeitende eingeplant			
☐	Versicherungsschutz und Haftungsfragen mit Rechtsberatung geklärt			

Bußgeldrahmen: Besonders wichtige Einrichtungen bis zu 10 Mio. € oder 2 % des weltweiten Jahresumsatzes, wichtige Einrichtungen bis zu 7 Mio. € oder 1,4 % – es gilt jeweils der höhere Betrag. Hinzu kommt die persönliche Verantwortung der Leitungsebene.

6 Nachweise und Dokumentation

Im Prüfungsfall zählt, was belegbar ist. Legen Sie die Nachweise an einem Ort ab, der auch ohne IT erreichbar ist.

	PRÜFPUNKT	STAND	WER	BIS
☐	Registrierungsnachweis, Risikoanalyse und Konzepte zentral abgelegt			
☐	Schulungsnachweise und Teilnehmerlisten vorhanden			
☐	Vorfalls- und Meldedokumentation wird fortlaufend geführt			
☐	Lieferantenverträge um Sicherheitsanforderungen ergänzt			
☐	Wiedervorlage gesetzt: jährliche Überprüfung der gesamten Checkliste			

Nächster Schritt: Unter blackout-check-industrie.de prüfen Sie mit dem kostenlosen Betroffenheits-Check in zwei Minuten, welche Regelwerke für Sie gelten – NIS2, KRITIS-Dachgesetz, CRA, DORA und TISAX in einem Durchgang.

Alle Angaben ohne Gewähr · Stand Oktober 2026 · Diese Checkliste dient der allgemeinen Orientierung und ersetzt keine Rechtsberatung. Grundlage: NIS2UmsuCG (BGBl. 2024 I Nr. 307), BSI.