NIS2-Compliance-Checkliste — Artikel 21(2)

Alle zehn Risikomanagementmaßnahmen mit ISMS-Lückenbewertung — v1.0 · 2026-07-16

#	Maßnahme (Art. 21(2))	ISMS-Abdeckung	Die Lücke	Was zu tun ist	Priorität
(a)	**Konzepte für Risikoanalyse und Sicherheit von Informationssystemen**	Durch ISMS abgedeckt	—	Stellen Sie sicher, dass die Risikoanalyse die NIS2-spezifischen operativen Aspekte abdeckt: Vorfallsmeldung, Lieferkette, Wirksamkeitsnachweis.	**Niedrig**
(b)	**Bewältigung von Sicherheitsvorfällen**	Fundament — operative Ergänzung nötig	Operative 24h/72h-Fähigkeit unter Zeitdruck — Koordination zwischen Security, Legal, Kommunikation und Geschäftsleitung.	Bauen Sie ein Incident-Management über den Plan hinaus auf: Tabletop-Übungen gegen die 24-Stunden-Frist; Vorlagen für alle drei Meldestufen.	**Hoch**
(c)	**Aufrechterhaltung des Betriebs und Krisenmanagement**	Durch ISMS abgedeckt	—	Prüfen Sie, ob die BCM-Pläne Cybervorfälle mit gleichzeitigen Meldepflichten nach Artikel 23 abdecken.	**Niedrig**
(d)	**Sicherheit der Lieferkette**	Fundament — operative Ergänzung nötig	Kontinuierliche Überwachung statt Jahres-Momentaufnahmen; anlassbezogene Neubewertungen; abrufbare Lieferantennachweise.	Monitoring-Fähigkeit aufbauen; von zyklischen zu anlassbezogenen Bewertungen wechseln; NIS2-Klauseln in Verträge aufnehmen; Nachweise abrufbar machen.	**Hoch**
(e)	**Sicherheit bei Erwerb, Entwicklung und Wartung**	Durch ISMS abgedeckt	Vulnerability Disclosure gegen die ENISA-Umsetzungsleitlinien prüfen.	Prüfen Sie, ob die Offenlegungsprozesse den NIS2-/ENISA-Erwartungen entsprechen — diese gehen über typische ISMS-Implementierungen hinaus.	**Mittel**
(f)	**Bewertung der Wirksamkeit der Risikomanagementmaßnahmen**	Fundament — operative Ergänzung nötig	Kontinuierlich verfügbare Evidenz statt Audit-Zyklus-Dokumentation.	Stellen Sie das Nachweismanagement auf kontinuierliche Verfügbarkeit um: Versionierung, Gültigkeitszeiträume, Verantwortlichkeiten; Behördenanfragen binnen Tagen beantworten können.	**Hoch**
(g)	**Grundlegende Cyberhygiene und Schulungen**	Durch ISMS abgedeckt	Nachweisbare Schulungsteilnahme der Geschäftsleitung.	Stellen Sie sicher, dass die Geschäftsleitung nachweislich an Cybersicherheitsschulungen teilnimmt — dieser Nachweis ist unmittelbar haftungsrelevant.	**Niedrig**
(h)	**Kryptographie und Verschlüsselung**	Durch ISMS abgedeckt	—	Halten Sie die Kryptographie-Konzepte aktuell und am Stand der Technik ausgerichtet.	**Niedrig**
(i)	**Personalsicherheit, Zugriffskontrolle und Asset-Management**	Durch ISMS abgedeckt	—	Bestätigen Sie die MFA-Abdeckung dort, wo NIS2 sie verlangt (siehe Maßnahme (j)).	**Niedrig**

#	Maßnahme (Art. 21(2))	ISMS-Abdeckung	Die Lücke	Was zu tun ist	Priorität
(j)	**MFA, gesicherte Kommunikation und Notfallkommunikation**	Teilweise abgedeckt	Gesicherte Notfallkommunikationskanäle, die unabhängig von der regulären (möglicherweise kompromittierten) Infrastruktur funktionieren.	MFA-Abdeckung auditieren; Notfallkanäle unabhängig von der regulären Infrastruktur etablieren; verschlüsselte Kommunikation für die Vorfallskoordination sicherstellen.	**Mittel**

Pflichten Art. 23 & Art. 20

Pflicht	Frist / Regel	Rechtsgrundlage
Frühwarnung an das CSIRT bzw. die zuständige Behörde	Innerhalb von 24 Stunden nach Kenntnis eines erheblichen Sicherheitsvorfalls	Art. 23(4)(a)
Meldung des Sicherheitsvorfalls	Innerhalb von 72 Stunden nach Kenntnis — Bewertung inkl. Schweregrad, Auswirkungen, Kompromittierungsindikatoren	Art. 23(4)(b)
Abschlussbericht	Innerhalb eines Monats nach der Vorfallsmeldung	Art. 23(4)(d)
Billigung und Überwachung der Risikomanagementmaßnahmen durch die Geschäftsleitung	Laufend — die Geschäftsleitung billigt die Maßnahmen, überwacht die Umsetzung und haftet persönlich	Art. 20(1)
Cybersicherheitsschulung der Geschäftsleitung	Regelmäßig — Mitglieder der Geschäftsleitung sind verpflichtet, an Schulungen teilzunehmen	Art. 20(2)

So nutzen Sie diese Checkliste

1. Gehen Sie jede der zehn Maßnahmen aus Artikel 21(2) durch und bewerten Sie ehrlich: nicht 'Haben wir einen Prozess?', sondern 'Können wir das unter Zeitdruck, gegenüber externen Parteien und mit belastbaren Nachweisen operativ ausführen?'

2. Nutzen Sie die Prioritätsspalte als Ausgangspunkt: Die drei Hoch-Lücken (Vorfallsbewältigung, Lieferkette, Wirksamkeitsnachweis) haben die höchste regulatorische Dringlichkeit.

3. Planen Sie für jede Lücke den operativen Ausbau: Welches System, welcher Prozess, welche Fähigkeit wird konkret benötigt?

4. Behalten Sie das ISMS als interne Kontrollebene und ergänzen Sie es um die operative Ebene, die NIS2 zusätzlich verlangt.

5. Verfolgen Sie Status, Verantwortliche und Nachweise je Maßnahme im Checklisten-Blatt — Aufsichtsbehörden können Nachweise jederzeit anfordern.

Vollständige Erläuterungen je Maßnahme, Quellen und die ISMS-Lückenanalyse: https://www.orbiqhq.com/de/eu-vorschriften/nis2-checkliste-artikel-21