Crosswalk NIS2 / DORA / ISO 27001 / Cyber Risk

Vergleichende Übersicht der Anforderungen und Kontrollen über alle relevanten Rahmenwerke. Quelle: resilience.amartens.com/crosswalk

Stand: 03.06.2026

Thema	NIS2	DORA	ISO 27001	Cyber Risk
Governance	Art. 20 NIS2 — Leitungsorgan-Verantwortung	Art. 5 DORA — Governance-Regelungen	A.5.1 — Führung und Verpflichtung	Management-Verantwortung, Schulungspflicht
Risikomanagement	Art. 21 NIS2 — Risikomanagement-Maßnahmen	Art. 6–14 DORA — IKT-Risikomanagementrahmen	A.5–A.8 — Risikobeurteilung und -behandlung	Risikoregister, Bedrohungsanalyse, Schutzbedarf
Incident Response	Art. 23 NIS2 — Meldepflichten bei Sicherheitsvorfällen	Art. 17–19 DORA — IKT-Vorfallsmanagement & Meldung	A.5.24–A.5.28 — Incident Management	Incident-Log, Meldeprotokoll, Playbooks
Lieferkette	Art. 21 II d NIS2 — Lieferkettensicherheit	Art. 28–33 DORA — IKT-Drittparteienrisiko	A.5.19–A.5.23 — Lieferantenbeziehungen	Lieferantenbewertung, Exit-Strategien, Konzentrationsrisiko
IKT-Sicherheit	Art. 21 II a, e NIS2 — Sicherheit der Netz- und Informationssysteme	Art. 7–9 DORA — IKT-Systeme, Schutz und Prävention	A.8 — Technische Maßnahmen (Annex A Controls)	Sicherheitskonzept, BSI-Grundschutz, KRITIS
Business Continuity	Art. 21 II c NIS2 — Business Continuity & Krisenmanagement	Art. 11 DORA — Backup-Policies und -Verfahren, Wiederherstellung	A.5.29–A.5.30 — Aufrechterhaltung, IKT-Bereitschaft	BCM-Plan, RTO-Definition, Failover-Tests
Audit / Prüfung	Art. 21 II f NIS2 — Überprüfung der Cybersicherheit	Art. 24–27 DORA — Testprogramm, TLPT, externe Prüfung	A.5.35 — Internes Audit, A.5.36 — Managementbewertung	Audit-Tracker, Jahresabschlussprüfung, SREP
Meldepflichten	Art. 23 NIS2 — Meldepflicht (24h/72h/1M)	Art. 19 DORA — Meldung schwerwiegender IKT-Vorfälle	— (nicht direkt, über ISMS-Prozesse abgedeckt)	Meldeprotokoll, Vorlagen, Fristen-Tracker
Management Review	Art. 20 NIS2 — Jährliche Überprüfung & Berichterstattung	Art. 6 VIII DORA — Überprüfung des IKT-Risikorahmens	A.5.36 — Managementbewertung des ISMS	Review Pack, Decision Log, Management-Beschlüsse
Evidence / Nachweise	Art. 21 NIS2 — Dokumentation der Maßnahmen	Art. 6, 25 DORA — Nachweisführung, Testdokumentation	A.5.37 — Dokumentierte Information (Annex A)	Evidence-Kategorien, Vollständigkeits-Checkliste