sosafe

DORA-Mapping-Übersicht: Orientierung entlang der fünf Säulen

Eine praktische Zuordnung der DORA-Anforderungen zu ISO 27001 und NIS2, mit Fokus auf empfohlene Nachweise statt auf reine Artikellisten.

Diese Übersicht ordnet die fünf DORA-Säulen den Stellen zu, an denen sich Ihre bestehende ISO-27001- oder NIS2-Umsetzung bereits mit DORA überschneidet, und zeigt, welcher Nachweistyp im Audit typischerweise erwartet wird. Sie ersetzt keine Rechtsberatung und keine vollständige, artikelgenaue Gap-Analyse; dafür bietet sie eine schnelle Orientierung, mit welchen Themenblöcken Sie priorisiert arbeiten sollten und wo Sie eher neu ansetzen müssen. Alle Angaben ohne Gewähr auf Vollständigkeit. Grundlage sind Verordnung (EU) 2022/2554 (DORA), ISO/IEC 27001:2022 sowie die Richtlinie (EU) 2022/2555 (NIS2) und ihre nationale Umsetzung.

1 IKT-Risikomanagement (DORA Art. 5–15)

Der Kernbereich mit der größten Überschneidung zu bestehenden Managementsystemen.

DORA-Anforderung	ISO-27001-Bezug	NIS2-Bezug	Empfohlener Nachweis	Beispielmaßnahme
Governance & Verantwortung des Leitungsorgans (Art. 5)	Kontext der Organisation, Führung (Kap. 4–5)	Governance-Pflichten (Art. 20)	Beschluss/Protokoll des Leitungsorgans zur ICT-Risikostrategie	Jährliche Freigabe der IKT-Risikostrategie durch Vorstand/Geschäftsführung
IKT-Risikomanagement-Rahmenwerk (Art. 6)	Risikobeurteilung & -behandlung (Kap. 6, Annex A.5)	Risikomanagementmaßnahmen (Art. 21 Abs. 2 lit. a)	Aktuelle Risikoregister, Reviewzyklen	Dokumentiertes ISMS mit definiertem Reviewintervall
IKT-Systeme, Protokolle und Tools (Art. 7)	Annex A.8.9 (Konfigurationsmanagement)	Art. 21 Abs. 2 lit. e	Konfigurationsstandards, Change-Protokolle	Standardisierte Systemkonfiguration mit Versionskontrolle
Identifizierung von Assets und Risiken (Art. 8)	Annex A.5.9, A.5.12 (Asset-Inventar, Klassifizierung)	Art. 21 Abs. 2 lit. i	Aktuelles Asset-Register mit Kritikalitätsklassifizierung	Jährliche Inventur aller IKT-Assets inkl. Schutzbedarfsfeststellung
Schutz und Prävention (Art. 9)	Annex A.8.7, A.8.24 (Malware-Schutz, Kryptografie)	Art. 21 Abs. 2 lit. h	Nachweis über eingesetzte Schutzmaßnahmen und Verschlüsselungsstandards	Endpoint-Protection und verschlüsselte Datenübertragung

DORA-Anforderung	ISO-27001-Bezug	NIS2-Bezug	Empfohlener Nachweis	Beispielmaßnahme
Erkennung von Anomalien (Art. 10)	Annex A.8 (Monitoring, Logging)	Art. 21 Abs. 2 lit. b	Monitoring-Konzept, Alarmierungsprotokolle	SIEM-gestützte Anomalieerkennung mit definierten Schwellenwerten
Reaktion & Wiederherstellung, BCM (Art. 11)	Annex A.5.29–5.30 (Business Continuity)	Art. 21 Abs. 2 lit. c	BCM-Pläne, Testprotokolle, Wiederanlaufzeiten	Jährlicher BCM-Test mit dokumentierten Wiederanlaufzeiten (RTO/RPO)
Backup-Policies und Wiederherstellung (Art. 12)	Annex A.8.13 (Backup)	Art. 21 Abs. 2 lit. c	Backup-Konzept, Restore-Testprotokolle	Regelmäßige Restore-Tests aus Backup-Systemen
Lernen & Weiterentwicklung, inkl. Awareness (Art. 13)	Annex A.6.3 (Security Awareness, Kompetenz)	Art. 21 Abs. 2 lit. g	Schulungsnachweise je Rolle, Wissensstand-Tracking	Rollenbasiertes Awareness-Programm mit Lernfortschritts-Tracking
Kommunikation bei Vorfällen und Krisen (Art. 14)	Annex A.5.26 (Reaktion auf Sicherheitsvorfälle)	Art. 21 Abs. 2 lit. b	Kommunikationsplan, interne/externe Meldewege	Definierter Eskalations- und Kommunikationsplan für Krisenfälle
Weitere Harmonisierung durch technische Regulierungsstandards, RTS (Art. 15)	Kein direktes Äquivalent (RTS-Vorgaben variieren je Thema)	Kein direktes Äquivalent	Nachweis der Umsetzung veröffentlichter RTS-Vorgaben	Laufender Abgleich interner Standards mit neu veröffentlichten ESA-RTS

2 Meldepflichten bei IKT-Vorfällen (DORA Art. 17–23)

Hier weicht DORA am stärksten von ISO 27001 ab: Die gestaffelten Fristen sind DORA-spezifisch.

DORA-Anforderung	ISO-27001-Bezug	NIS2-Bezug	Empfohlener Nachweis	Beispielmaßnahme
IKT-Vorfallmanagementprozess (Art. 17)	Annex A.5.24 (Planung Incident Management)	Art. 23 Abs. 1	Dokumentierter Incident-Management-Prozess	Definierter Prozess von Erkennung bis Nachbereitung
Klassifizierung von Vorfällen (Art. 18)	Annex A.5.25 (Bewertung von Sicherheitsereignissen)	Art. 23 Abs. 4	Klassifizierungsschema mit Kriterienkatalog	Schweregrad-Matrix nach Auswirkung und Betroffenheit
Meldung in gestaffelten Fristen: Erst-, Zwischen-, Abschlussbericht (Art. 19)	Kein direktes Äquivalent (nur allgemeine Meldewege)	Frühwarnung 24h / Meldung 72h	Eskalationsprozess mit dokumentierten Fristen, Meldeprotokolle	Vorlagen für Erst-, Zwischen- und Abschlussmeldung an die Aufsicht
Harmonisierte Meldeinhalte und -formate (Art. 20)	Kein direktes Äquivalent	Kein direktes Äquivalent	Nutzung der ESA-Meldevorlagen	Einsatz standardisierter Meldeformulare gemäß ITS

3 IKT-Drittparteienrisiko (DORA Art. 28–30)

Betrifft alle Dienstleister. Die Tiefe der Anforderungen hängt von der Kritikalitätseinstufung ab.

DORA-Anforderung	ISO-27001-Bezug	NIS2-Bezug	Empfohlener Nachweis	Beispielmaßnahme
Strategie für IKT-Drittparteienrisiko (Art. 28 Abs. 2)	Annex A.5.19 (-Lieferantenbeziehungen, Grundsätze)	Art. 21 Abs. 2 lit. d (Lieferkette)	Dokumentierte Drittparteien-risiko-Strategie	Vom Leitungsorgan freigegebene Auslagerungsstrategie
Informationsregister aller Drittdienstleister (Art. 28 Abs. 3)	Annex A.5.19–5.20 (-Lieferantenbeziehungen)	Art. 21 Abs. 2 lit. d	Zentrales, aktuelles Register mit Kritikalitätsstufe	Register of Information nach ESA-Vorlage, jährlich aktualisiert
Sorgfaltsprüfung vor Vertragsschluss (Art. 28 Abs. 4)	Annex A.5.20 (-Lieferantenvereinbarungen)	Art. 21 Abs. 2 lit. d	Due-Diligence-Dokumentation je Anbieter	Standardisierter Due-Diligence-Fragebogen vor Vertragsabschluss
Konzentrationsrisiko-Bewertung (Art. 29)	Kein direktes Äquivalent	Kein direktes Äquivalent	Portfolioweite Konzentrationsrisiko-Analyse	Jährliche Analyse der Anbieterkonzentration nach Kritikalität
Pflichtvertragsinhalte bei kritischen Funktionen (Art. 30)	Annex A.5.20, A.5.22	Kein direktes Äquivalent in dieser Detailtiefe	Vertragsklausel-Checkliste, Nachweis der Nachverhandlung	Standardklauselkatalog für Audit-, Kündigungs- und Exit-Rechte
Fortlaufende Überwachung (Art. 28 Abs. 6)	Annex A.5.22 (Überwachung von Lieferantenleistungen)	Art. 21 Abs. 2 lit. d	Review-Protokolle nach Kritikalitätsstufe	Turnusmäßiges Lieferanten-Review nach Risikostufe

4 Resilienztests (DORA Art. 24–27)

Kein direktes Äquivalent in ISO 27001 oder NIS2.

DORA-Anforderung	ISO-27001-Bezug	NIS2-Bezug	Empfohlener Nachweis	Beispielmaßnahme
Allgemeine Testanforderungen (Art. 24)	Annex A.5.35 (Unabhängige Überprüfung, als Annäherung)	Kein direktes Äquivalent	Jährlicher Testplan mit Testarten je Kritikalität	Risikobasierter Testplan für alle IKT-Systeme
Testing von IKT-Tools und -Systemen (Art. 25)	Annex A.8.29 (-Sicherheitstests in Entwicklung/Abnahme, als Annäherung)	Kein direktes Äquivalent	Testprotokolle, Schwachstellenberichte	Regelmäßige Vulnerability-Scans und Penetrationstests
Bedrohungsgeleitete Penetrationstests, TLPT (Art. 26)	Kein direktes Äquivalent	Kein direktes Äquivalent	TLPT-Testbericht nach TIBER-EU-Methodik	Durchführung von TLPT im vorgeschriebenen Zyklus für bedeutende Institute
Anforderungen an Tester (Art. 27)	Kein direktes Äquivalent	Kein direktes Äquivalent	Nachweis der Testerqualifikation/-akkreditierung	Beauftragung ausschließlich akkreditierter TLPT-Tester

Bedrohungsgeleitete Penetrationstests (TLPT) nach Art. 24–27 sind eine DORA-spezifische Pflicht für bedeutende Institute und lassen sich nicht über bestehende Penetrationstest-Routinen abdecken, da Umfang, Methodik (TIBER-EU) und Frequenz eigens vorgegeben sind.

5 Informationsaustausch (DORA Art. 45)

Ebenfalls kein direktes Äquivalent in ISO 27001 oder NIS2, zudem freiwillig statt verpflichtend.

DORA-Anforderung	ISO-27001-Bezug	NIS2-Bezug	Empfohlener Nachweis	Beispielmaßnahme
Freiwilliger Informationsaustausch zu Cyberbedrohungen (Art. 45)	Kein direktes Äquivalent	Kein direktes Äquivalent	Teilnahmenachweis an Austauschformaten (optional)	Freiwillige Teilnahme an Threat-Intelligence-Sharing-Foren

Der Informationsaustausch zu Cyberbedrohungen hat keine Entsprechung in den beiden Rahmenwerken und bleibt eine eigenständige, nicht verpflichtende DORA-Maßnahme.

Wo DORA über ISO 27001 und NIS2 hinausgeht

Auch bei hoher Deckung bleiben drei Bereiche, in denen bestehende Zertifizierungen nicht ausreichen: die gestaffelten, kurzen Meldefristen bei Vorfällen (Art. 19), die verpflichtenden Mindestvertragsinhalte für Dienstleister mit kritischen Funktionen (Art. 30) und die bedrohungsgeleiteten Penetrationstests (Art. 24–27). Wer sein Mapping auf diese drei Lücken fokussiert, deckt in der Praxis die größten Auditrisiken ab.

Diese Übersicht dient der ersten Orientierung und ersetzt keine Rechtsberatung. Rechtsgrundlagen: Verordnung (EU) 2022/2554 (DORA), ISO/IEC 27001:2022, Richtlinie (EU) 2022/2555 (NIS2). Stand: August 2026