sosafe

DORA Mapping Overview: Orientation Along the Five Pillars

A practical allocation of DORA requirements to ISO 27001 and NIS2, focused on recommended evidence rather than on lists of articles.

This overview shows where your existing ISO 27001 or NIS2 implementation already overlaps with the five DORA pillars, and what type of evidence an audit typically expects for each requirement. It is not legal advice and not a complete, article-by-article gap analysis. What it does offer is a quick sense of which topic areas to prioritise and where you are likely to be starting from scratch. This overview does not claim to be exhaustive. It draws on Regulation (EU) 2022/2554 (DORA), ISO/IEC 27001:2022 and Directive (EU) 2022/2555 (NIS2) together with its national transpositions.

1 ICT risk management (DORA Art. 5–15)

The core area, and the one that overlaps most with existing management systems.

DORA requirement	ISO 27001 reference	NIS2 reference	Recommended evidence	Example measure
Governance and responsibility of the management body (Art. 5)	Context of the organisation, leadership (clauses 4–5)	Governance obligations (Art. 20)	Management body decision or minutes covering the ICT risk strategy	Annual sign-off of the ICT risk strategy by the executive board
ICT risk management framework (Art. 6)	Risk assessment and treatment (clause 6, Annex A.5)	Risk management measures (Art. 21(2)(a))	Current risk register, review cycles	Documented ISMS with a defined review interval
ICT systems, protocols and tools (Art. 7)	Annex A.8.9 (configuration management)	Art. 21(2)(e)	Configuration standards, change logs	Standardised system configuration under version control
Identification of assets and risks (Art. 8)	Annex A.5.9, A.5.12 (asset inventory, classification)	Art. 21(2)(i)	Current asset register with criticality classification	Annual inventory of all ICT assets, including an assessment of protection requirements
Protection and prevention (Art. 9)	Annex A.8.7, A.8.24 (malware protection, cryptography)	Art. 21(2)(h)	Evidence of the protective measures in use and of encryption standards	Endpoint protection and encrypted data transmission

DORA requirement	ISO 27001 reference	NIS2 reference	Recommended evidence	Example measure
Detection of anomalies (Art. 10)	Annex A.8 (monitoring, logging)	Art. 21(2)(b)	Monitoring concept, alerting records	SIEM-based anomaly detection with defined thresholds
Response and recovery, BCM (Art. 11)	Annex A.5.29–5.30 (business continuity)	Art. 21(2)(c)	BCM plans, test records, recovery times	Annual BCM test with documented recovery times (RTO/RPO)
Backup policies and restoration (Art. 12)	Annex A.8.13 (backup)	Art. 21(2)(c)	Backup concept, restore test records	Regular restore tests from backup systems
Learning and evolving, including awareness (Art. 13)	Annex A.6.3 (security awareness, competence)	Art. 21(2)(g)	Training records by role, tracking of knowledge levels	Role-based awareness programme with learning progress tracking
Communication during incidents and crises (Art. 14)	Annex A.5.26 (response to information security incidents)	Art. 21(2)(b)	Communication plan, internal and external reporting channels	Defined escalation and communication plan for crisis situations
Further harmonisation through regulatory technical standards, RTS (Art. 15)	No direct equivalent (RTS requirements vary by topic)	No direct equivalent	Evidence that published RTS requirements have been implemented	Ongoing comparison of internal standards against newly published ESA RTS

2 ICT-related incident reporting (DORA Art. 17–23)

This is where DORA diverges most from ISO 27001: the staggered deadlines are specific to DORA.

DORA requirement	ISO 27001 reference	NIS2 reference	Recommended evidence	Example measure
ICT-related incident management process (Art. 17)	Annex A.5.24 (incident management planning)	Art. 23(1)	Documented incident management process	Defined process from detection through to post-incident review
Classification of incidents (Art. 18)	Annex A.5.25 (assessment of security events)	Art. 23(4)	Classification scheme with a defined set of criteria	Severity matrix based on impact and on who is affected
Reporting within staggered deadlines: initial, intermediate and final report (Art. 19)	No direct equivalent (general reporting channels only)	Early warning 24h / notification 72h	Escalation process with documented deadlines, reporting records	Templates for the initial, intermediate and final report to the supervisory authority
Harmonised reporting content and formats (Art. 20)	No direct equivalent	No direct equivalent	Use of the ESA reporting templates	Standardised reporting forms in line with the ITS

3 ICT third-party risk (DORA Art. 28–30)

Applies to every provider. How far the requirements reach depends on the criticality classification.

DORA requirement	ISO 27001 reference	NIS2 reference	Recommended evidence	Example measure
Strategy on ICT third-party risk (Art. 28(2))	Annex A.5.19 (supplier relationships, principles)	Art. 21(2)(d) (supply chain)	Documented third-party risk strategy	Outsourcing strategy approved by the management body
Register of information covering all third-party providers (Art. 28(3))	Annex A.5.19–5.20 (supplier relationships)	Art. 21(2)(d)	Central, current register including criticality tier	Register of information following the ESA template, updated annually
Due diligence before entering into a contract (Art. 28(4))	Annex A.5.20 (supplier agreements)	Art. 21(2)(d)	Due diligence documentation for each provider	Standardised due diligence questionnaire before contract signature
Assessment of concentration risk (Art. 29)	No direct equivalent	No direct equivalent	Portfolio-wide concentration risk analysis	Annual analysis of provider concentration by criticality
Mandatory contractual provisions for critical functions (Art. 30)	Annex A.5.20, A.5.22	No direct equivalent at this level of detail	Contract clause checklist, evidence of renegotiation	Standard clause catalogue covering audit, termination and exit rights
Ongoing monitoring (Art. 28(6))	Annex A.5.22 (monitoring of supplier performance)	Art. 21(2)(d)	Review records by criticality tier	Regular supplier review scheduled by risk tier

4 Resilience testing (DORA Art. 24–27)

No direct equivalent in either ISO 27001 or NIS2.

DORA requirement	ISO 27001 reference	NIS2 reference	Recommended evidence	Example measure
General testing requirements (Art. 24)	Annex A.5.35 (independent review, as an approximation)	No direct equivalent	Annual test plan setting out test types by criticality	Risk-based test plan covering all ICT systems
Testing of ICT tools and systems (Art. 25)	Annex A.8.29 (security testing in development and acceptance, as an approximation)	No direct equivalent	Test records, vulnerability reports	Regular vulnerability scans and penetration tests
Threat-led penetration testing, TLPT (Art. 26)	No direct equivalent	No direct equivalent	TLPT test report following the TIBER-EU methodology	TLPT carried out at the prescribed interval by significant institutions
Requirements for testers (Art. 27)	No direct equivalent	No direct equivalent	Evidence of tester qualification or accreditation	Engagement of accredited TLPT testers only

Threat-led penetration testing under Art. 24–27 is a DORA-specific obligation for significant institutions, and existing penetration testing routines will not cover it: scope, methodology (TIBER-EU) and frequency are all prescribed separately.

5 Information sharing (DORA Art. 45)

Again without a direct equivalent in ISO 27001 or NIS2, and voluntary rather than mandatory.

DORA requirement	ISO 27001 reference	NIS2 reference	Recommended evidence	Example measure
Voluntary sharing of cyber threat information (Art. 45)	No direct equivalent	No direct equivalent	Evidence of participation in sharing arrangements (optional)	Voluntary participation in threat intelligence sharing forums

Sharing information on cyber threats has no counterpart in either framework and remains a standalone DORA measure that carries no obligation.

Where DORA goes beyond ISO 27001 and NIS2

Even with substantial coverage, three areas remain where existing certifications fall short: the short, staggered deadlines for incident reporting (Art. 19), the mandatory minimum contractual provisions for providers supporting critical functions (Art. 30), and threat-led penetration testing (Art. 24–27). Focusing your mapping on those three gaps covers the largest audit risks in practice.

The human factor in your mapping: DORA Art. 13(6) requires documented, role-based awareness and training measures for staff and management, as a line of its own with evidence attached. SoSafe's **Human Risk Management Dashboard** supplies the role-based learning content and the audit-ready records that go with it.

Request a demo

This overview is intended as an initial orientation and does not constitute legal advice. Legal sources: Regulation (EU) 2022/2554 (DORA), ISO/IEC 27001:2022, Directive (EU) 2022/2555 (NIS2). Last updated: August 2026