HORIZONSHIELD

Securing Your Digital Future, Today.

FINANCIAL REGULATORY COMPLIANCE · BOOK 04 OF 16

DORA Compliance Guide 2026

Digital Operational Resilience Act — Complete Implementation

The practitioner's guide to DORA compliance for EU financial entities. All five pillars covered: ICT risk management, incident reporting, TLPT, third-party risk, and information sharing — with gap assessment checklists and implementation timelines.

PILLARS	EFFECTIVE	MAX FINE
5	17 Jan 2025	2% global turnover

SCOPE

EU Financial Entities

Contents

DORA COMPLIANCE GUIDE 2026

CHAPTER 01

DORA Overview

EU Regulation 2022/2554 — directly applicable from January 17, 2025. No national transposition required. No grace period.

REGULATION SCOPE PENALTIES ENFORCEMENT

What Is DORA and What Does It Require

DORA establishes a single, harmonised, legally binding ICT risk management framework for the entire EU financial sector. Unlike previous guidance-based frameworks, DORA is a directly applicable EU regulation — it does not require national transposition and applies with full legal force since **January 17, 2025**.

17 Jan
2025 — ENFORCEMENT DATE
No grace period granted

5
COMPLIANCE PILLARS — ALL MANDATORY
64 articles + 13 RTS/ITS

2%
GLOBAL ANNUAL TURNOVER MAX FINE
Per violation, per NCA

4hrs
INITIAL MAJOR INCIDENT NOTIFICATION
Most stringent requirement globally

Entities in Scope — Classification

Entity	Examples	DORA Regime	Key Note
Credit institutions	Banks, building societies, mortgage lenders	Full DORA — all 5 pillars	Central bank oversight — early supervisory focus
Payment institutions	PSPs, e-money institutions, PISP/AISP	Full DORA	PSD2-licensed entities — DORA adds ICT requirements

Entity	Examples	DORA Regime	Key Note
Investment firms	Brokers, asset managers, trading firms	Full DORA	TLPT required for significant entities
Insurance undertakings	Insurers, reinsurers, intermediaries	Full DORA	Solvency II entities — DORA additive requirement
Crypto-asset service providers	MiCA-licensed CASPs	Full DORA from MiCA authorization date	New entrant — DORA compliance from day of authorization
Critical ICT third-party providers	Cloud providers, data services designated critical by ESAs	Chapter V oversight	Directly subject to ESA regulatory oversight and inspections
Microenterprises	<10 staff AND <€2M turnover AND <€2M balance sheet (ALL three)	Simplified DORA	Proportionate requirements — reduced incident reporting burden

DORA IS BEING ACTIVELY ENFORCED

National Competent Authorities published their DORA supervisory priorities for 2025-2026. Key focus areas: (1) ICT incident classification procedures — can you actually classify within 4 hours?, (2) Third-party registers — complete, current, in RTS format?, (3) Board ICT governance — genuine oversight or rubber stamp? Thematic reviews are underway.

Five DORA Pillars

PILLAR 1 — ART. 5-16

ICT Risk Management Framework

Board-approved ICT risk management framework. ICT risk appetite statement. Asset inventory. Security policies for all domains. Business continuity with ICT component. Backup and recovery with tested restoration. Annual review and board sign-off.

PILLAR 2 — ART. 17-23

ICT Incident Reporting

Classify major ICT incidents per RTS criteria. Initial notification to NCA within 4 hours. Intermediate report within 72 hours. Final report within 1 month. Voluntary cyber threat reporting channel. Harmonised reporting forms across EU.

PILLAR 3 — ART. 24-27

Digital Operational Resilience Testing

Annual vulnerability assessments for all entities. Threat-Led Penetration Testing (TLPT) every 3 years for significant entities. TLPT uses live red team testing against actual production

PILLAR 4 — ART. 28-44

ICT Third-Party Risk Management

Due diligence on all ICT providers supporting critical/important functions. DORA-compliant contract terms. Register of ICT third-party services in RTS format. Concentration risk analysis. Exit strategies for critical providers.

systems using threat intelligence-driven scenarios.

CHAPTER 02

Pillar 1 — ICT Risk Management

The foundation: a board-approved, documented, annually reviewed ICT risk management framework covering all domains.

GOVERNANCE | RISK FRAMEWORK | BCP | ASSET INVENTORY

ICT Risk Management Framework Requirements

Management Body Obligations — Article 5

DORA places ultimate responsibility with the management body. The board cannot fully delegate this to the CISO or CTO.

- **Define and approve** the ICT risk management framework — the board sets the framework, not merely receives briefings
- **Annual review and approval** — framework reviewed minimum annually, board sign-off documented in board minutes
- **Ultimate accountability** — management body is responsible for ICT risk regardless of operational delegation
- **Adequate ICT risk knowledge** — DORA requires board-level understanding of ICT risk, driving cybersecurity training requirements
- **Budget allocation** — board must ensure sufficient financial and human resources for ICT security and resilience

Required Framework Components

Component	Article	Requirement	Evidence Required	Common Gap
ICT Risk Appetite Statement	Art. 6(8)	Defined tolerable ICT risk levels with quantitative thresholds triggering management escalation	Board-approved document with thresholds. Board minutes showing approval.	Generic risk appetite, no ICT specificity, no quantitative thresholds
ICT Asset Inventory	Art. 8	Complete inventory of ALL ICT assets supporting critical/important functions, with dependencies	Maintained database with criticality classification, not annual spreadsheet	Incomplete — shadow IT excluded. No criticality tiering.
Data Classification	Art. 8(1)	Classification by sensitivity and criticality. Data flow map.	Classification policy + data map showing where each level resides	Policy on paper but not operationally implemented
BCP with ICT Component	Art. 11	Documented BCP covering ICT scenarios with RTO/RPO for all critical functions	Tested plan with documented test results and actual vs target performance	Plan exists but never tested. No quantitative RTO/RPO.
Backup & Recovery Tested	Art. 12	Regular backups with tested recovery. Backup isolated from production.	Backup logs + restoration test results with timestamps	Backups never tested. No offline/isolated copy.
Vulnerability Management	Art. 9(3)	Risk-based patching with defined SLAs. Scanning programme. Remediation tracking.	Patch SLA policy + compliance reports + open vulnerability tracking	No patch SLAs. Scanning infrequent. No remediation tracking.

CHAPTER 03

Pillar 2 — Incident Reporting

The most operationally demanding DORA requirement. The 4-hour initial notification window requires pre-built infrastructure.

4 HOURS | 72 HOURS | 1 MONTH | MAJOR INCIDENT CRITERIA

Major Incident Classification & Reporting

THE 4-HOUR CLOCK STARTS AT AWARENESS — NOT INVESTIGATION COMPLETION

DORA Article 19: initial notification must be submitted within 4 hours of classifying as a major incident — not 4 hours after completing your investigation. Submit even if investigation is incomplete. This requires pre-built reporting templates, pre-identified NCA contacts, and a tested classification procedure that works under crisis pressure.

1

Initial Notification — T+4 Hours

MANDATORY — HARDEST DEADLINE

Submit to NCA. Required: incident nature and classification, date/time of occurrence, initial severity assessment, whether ongoing, geographic areas affected, cross-border impact. Incomplete information is acceptable — timeliness is paramount.

2

Intermediate Report — T+72 Hours

MANDATORY

Updated detailed report: classification update, containment status, preliminary root cause, actions taken/planned, customer impact (number and type), financial impact estimate, external notifications (law enforcement, other regulators).

3

Final Report — T+1 Month

MANDATORY (T+3 MONTHS FOR COMPLEX)

Complete root cause analysis, full timeline, total financial and operational impact, all remediation measures implemented, preventive measures, lessons learned, changes to ICT risk framework, follow-up resilience testing planned/completed.

Major Incident Classification Criteria — DORA RTS

Criterion	Threshold	Assessment Method	Trigger Rule
Clients affected	> 10% of total client base OR > 10,000 clients	Count of clients unable to access service per hour	Either threshold met = major incident candidate
Service unavailability	Critical ICT service unavailable > 30 minutes OR degraded > 2 hours	Service monitoring — define "unavailable" vs "degraded" in advance	Duration threshold for critical service = major incident candidate
Reputational impact	Media coverage in national/international outlets OR regulatory inquiry	Communications team assessment. Google Alert monitoring.	Any media coverage or regulatory contact = assess for major
Economic impact	Direct losses > €100,000 OR potential losses > €500,000	Finance team assessment within 72 hours	Either threshold = major incident candidate
Duration	3+ similar incidents in 12 months OR single incident > 24 hours	Incident management system tracking	Third similar incident in 12 months = automatic major classification
Geographic spread	Affects 2+ EU Member States	Operational scope assessment	Multi-jurisdiction = major with cross-border notification obligation

TWO OR MORE CRITERIA = REPORT OBLIGATION

An incident meeting thresholds in two or more criteria must be classified as major. When in doubt — report. Voluntary over-reporting is viewed favorably. Under-reporting is a compliance failure. Note: the reporting obligation survives rapid containment — if criteria were met at any point, you must report.

CHAPTER 07

DORA Gap Assessment Checklist

Where are you today vs. where DORA requires? Complete self-assessment checklist for all five pillars.

ALL PILLARS | EVIDENCE | PRIORITY | ACTIONS

DORA Gap Assessment — Pillar by Pillar

Pillar 1 — ICT Risk Management

Status	Requirement	Article	Priority	Evidence Required
☐	ICT risk management framework documented and board-approved	Art. 5-6	CRITICAL	Board-approved document + board minutes showing approval date
☐	ICT risk appetite statement with quantitative thresholds	Art. 6(8)	CRITICAL	Risk appetite document, board-approved
☐	Board ICT risk training completed and documented	Art. 5	CRITICAL	Training records, board resolution on ICT responsibilities
☐	ICT asset inventory complete and current	Art. 8	HIGH	Maintained inventory with criticality classification, last-updated date
☐	Data classification scheme implemented operationally	Art. 8(1)	HIGH	Classification policy + data map
☐	Security policies for all ICT domains documented	Art. 9	HIGH	Policy library with version history, annual review records

Status	Requirement	Article	Priority	Evidence Required
☐	BCP with ICT component documented and tested	Art. 11	CRITICAL	BCP document + test results with actual vs target RTO/RPO
☐	Backup tested — restoration verified with timestamps	Art. 12	CRITICAL	Backup logs + restoration test results
☐	Patch management with defined SLAs and tracking	Art. 9(3)	HIGH	Policy + compliance reporting + open vulnerability tracking

Pillar 2 — Incident Management

Status	Requirement	Article	Priority	Evidence Required
☐	Major incident classification procedure documented and tested	Art. 18	CRITICAL	Classification tool/decision tree aligned to RTS. Test results.
☐	4-hour notification capability confirmed via tabletop exercise	Art. 19	CRITICAL	Tabletop exercise result showing notification possible in <4 hours
☐	NCA contact list current with out-of-hours numbers	Art. 19	CRITICAL	Contact list, last verified date
☐	Pre-written notification templates ready — all three stages	Art. 19-20	HIGH	Completed template examples for initial, intermediate, final
☐	Incident management system with classification tracking	Art. 17	HIGH	System demo or documentation

Pillars 3-5

Status	Requirement	Pillar	Priority	Evidence
☐	Annual vulnerability assessment programme in place	3	HIGH	Scan results + remediation tracking from last 12 months
☐	Annual penetration testing completed by qualified provider	3	HIGH	Pentest report, scope, findings, remediation status
☐	TLPT conducted if significant entity designation applies	3	CRITICAL	TLPT report from DORA-qualified threat intelligence red team
☐	ICT third-party register complete in RTS format	4	CRITICAL	Register with all providers supporting critical/important functions

Status	Requirement	Pillar	Priority	Evidence
☐	All ICT contracts reviewed for DORA mandatory clauses	4	HIGH	Contract review log with DORA clause status per provider
☐	Exit strategies documented for critical ICT providers	4	HIGH	Exit strategy per critical/important ICT provider
☐	ICT third-party concentration risk analysis completed	4	MEDIUM	Analysis of concentration by provider, geography, service type
☐	Information sharing arrangement decision documented	5	LOW	Board decision document on participation in sharing arrangements

HS

HORIZONSHIELD

Securing Your Digital Future, Today.

DORA Compliance Guide 2026

Part of the HorizonShield Security Series — 16 comprehensive professional cybersecurity manuals covering every domain of modern enterprise security.