DORA Compliance Checklist Guide 2026

EU Regulation 2022/2554 — Digital Operational Resilience Act

A practical guide to assessing and achieving DORA compliance across all five pillars of digital operational resilience

Prepared by **DORA GRC** | doragrc.com

March 2026

95 checklist items • 5 pillars • 11 RTS/ITS references

Table of Contents

1. Introduction

The Digital Operational Resilience Act (DORA), formally Regulation (EU) 2022/2554, establishes a comprehensive framework for ICT risk management across the EU financial sector. It has applied since **17 January 2025** and covers **21 categories of financial entities**, including banks, insurers, investment firms, payment institutions, crypto-asset service providers, and ICT third-party service providers designated as critical.

DORA is structured around five pillars: ICT governance and risk management, incident management and reporting, digital operational resilience testing, third-party ICT risk management, and information sharing. Each pillar is supported by Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS) published by the European Supervisory Authorities (EBA, ESMA, EIOPA).

This guide provides a structured self-assessment tool covering **95 checklist items** across all five pillars, mapped to specific DORA articles and technical standards. It is designed to be used alongside the companion Excel template, which provides editable fields for maturity scoring, evidence tracking, ownership assignment, and remediation planning.

The proportionality principle (Art. 4) applies throughout. Not every requirement applies at the same depth to every entity. Microenterprises and less complex entities may meet some requirements at a reduced level, particularly under the simplified ICT risk management framework (Art. 16). If you are uncertain about the expected level of compliance for your entity, consult your National Competent Authority (NCA).

2. How to Use This Guide

• **Step 1: Review each pillar section.** Read the overview and understand which articles apply to your entity. Pay attention to the priority levels: Critical items are likely to be reviewed by your NCA.

• **Step 2: Self-assess each requirement.** Use the 1–5 maturity scale (see Section 3) to rate your current compliance posture for each checklist item.

• **Step 3: Record in the companion Excel template.** Enter your maturity score, target maturity, status, and supporting evidence for each item. The Excel template auto-calculates your compliance posture per pillar.

• **Step 4: Identify gaps and prioritise remediation.** Focus on Critical items that are below maturity level 3. These represent the highest regulatory exposure.

• **Step 5: Assign ownership and deadlines.** Each gap should have a named owner and a clear target date. DORA compliance requires coordination between ICT, risk, compliance, legal, and the management body.

• **Step 6: Track progress and review quarterly.** Compliance is not a one-time exercise. Schedule quarterly reviews to update your assessment and track remediation progress.

The Proportionality Principle (Art. 4)

DORA applies proportionally to the size, risk profile, nature, scale and complexity of the financial entity's services, activities and operations. Smaller entities may apply a simplified ICT risk management framework under Art. 16 and have reduced testing obligations under Art. 25. However, all in-scope entities must comply with the core requirements for incident reporting (Pillar 2), the Register of Information (Pillar 4), and governance accountability (Pillar 1).

3. Maturity Assessment Framework

Maturity Scale (1–5)

Level	Name	Description
1	**Initial / Ad Hoc**	No formal processes. Activities are reactive, undocumented and dependent on individuals. No evidence of compliance.
2	**Developing / Basic**	Basic processes exist but are inconsistent, partially documented or incomplete. Some awareness but significant gaps.
3	**Defined / Established**	Documented, standardised and consistently followed. Meets minimum DORA requirement. Evidence exists and is retrievable.
4	**Managed / Measured**	Monitored with KPIs, regularly reviewed and improving. Full compliance with comprehensive audit trail.
5	**Optimized / Leading**	Continuous improvement embedded, automated where possible. Exceeds DORA requirements. Best-in-class.

Priority Levels

Priority	Description
Critical	Must be addressed for regulatory compliance. Likely to be reviewed during NCA supervisory engagement.
Important	Expected for proportionate compliance. Should be in place for most entities.
Supplementary	Best practice or conditionally applicable. Lower regulatory exposure but recommended.

Status Values

Not Started — No work begun on this requirement.
In Progress — Work is underway but not yet meeting the requirement.
Partially Compliant — Some aspects are met but gaps remain.
Fully Compliant — Requirement is fully met with supporting evidence.
N/A — Not applicable to this entity (document justification).

4. Pillar 1: ICT Governance & Risk Management

Articles 5–16 | RTS: CDR 2024/1774

Governance is the foundation of DORA. The management body bears ultimate responsibility for ICT risk management and must formally approve the ICT risk management framework, define risk appetite, allocate resources, and receive regular reporting. This pillar covers the full lifecycle: asset identification and classification (Art. 8), protection controls (Art. 9), detection and monitoring (Art. 10), business continuity and disaster recovery (Art. 11–12), learning and communication (Art. 13–14), and the simplified framework for smaller entities (Art. 16).

Key articles: Art. 5 (Governance accountability), Art. 6 (Framework), Art. 7 (Systems), Art. 8 (Asset identification), Art. 9 (Protection), Art. 10 (Detection), Art. 11 (Business continuity), Art. 12 (Backup), Art. 13 (Learning), Art. 14 (Communication), Art. 16 (Simplified framework).

Ref	Requirement	Article	Priority
1.01	Management body has formally approved the ICT risk management framework	Art. 5(2)	**Critical**
1.02	Management body bears ultimate responsibility for ICT risk management	Art. 5(1)	**Critical**
1.03	ICT risk appetite and tolerance defined and documented by management body	Art. 5(2)(a)	**Critical**
1.04	Clear roles and responsibilities for ICT risk management assigned at all levels	Art. 5(2)(b)	**Critical**
1.05	Adequate budget and resources allocated to ICT security and operational resilience	Art. 5(2)(d)	**Important**
1.06	Management body members receive regular ICT risk training (at least annually)	Art. 5(4)	**Critical**
1.07	Management body receives regular ICT risk reporting (at least quarterly)	Art. 5(4)	**Important**
1.08	Documented framework includes a digital operational resilience strategy	Art. 6(1), 6(8)	**Critical**
1.09	Framework reviewed at least annually and after major ICT-related incidents	Art. 6(5)	**Critical**
1.10	Independent internal audit reviews the framework at least annually	Art. 6(6)	**Critical**
1.11	Multi-vendor ICT strategy defined with documented procurement rationale	Art. 6(9)	Supplementary
1.12	Dedicated ICT security function or officer appointed with clear reporting lines	Art. 6(4)	**Important**
1.13	ICT systems, protocols and tools are appropriate, reliable and resilient	Art. 7	**Important**
1.14	All business functions, roles, information and ICT assets identified and classified	Art. 8(1)	**Critical**
1.15	Complete, continuously maintained register of all ICT assets with criticality classification	Art. 8(1)	**Critical**
1.16	Dependencies between business functions, ICT assets and providers fully mapped	Art. 8(4)	**Critical**
1.17	Legacy ICT systems identified and subject to documented risk assessment	Art. 8(7)	**Important**
1.18	Asset classification and documentation reviewed at least annually	Art. 8(1)	**Important**
1.19	ICT security policies documented and enforced (access, encryption, patching)	Art. 9(1-2)	**Critical**
1.20	Strong authentication mechanisms implemented for access to critical systems	Art. 9(4)(c)	**Important**
1.21	Automated isolation of information assets in the event of cyber-attacks	Art. 9(4)(b)	**Important**
1.22	Change management procedures with risk assessment and rollback for critical changes	Art. 9(4)(e)	**Important**
1.23	Patch and update policies defined, implemented and tracked	Art. 9(4)(f)	**Important**
1.24	Detection and monitoring mechanisms for anomalous activities (logging, alerting)	Art. 10(1)	**Critical**

Ref	Requirement	Article	Priority
1.25	Sufficient capacity to investigate vulnerabilities, threats and incidents	Art. 10(2)	**Important**
1.26	Business continuity policy defined covering all critical and important functions	Art. 11(1)	**Critical**
1.27	Disaster recovery plans with defined RTO, RPO and MTPD for critical functions	Art. 11(2)	**Critical**
1.28	BCP and disaster recovery plans tested at least annually with documented results	Art. 11(5)	**Critical**
1.29	Crisis management function established with clear activation criteria	Art. 11(7)	**Important**
1.30	Backup policies defined (scope, frequency, retention) for all critical systems	Art. 12(1)	**Critical**
1.31	Backup systems physically and logically separated from primary production	Art. 12(3)	**Important**
1.32	Restoration and recovery procedures tested regularly with verified success	Art. 12(2)	**Critical**
1.33	Post-incident review process with lessons learned fed into risk assessments	Art. 13	**Important**
1.34	All staff receive ICT security awareness training appropriate to their role	Art. 13(6)	**Important**
1.35	Crisis communication plans for internal escalation, clients and external parties	Art. 14	**Important**
1.36	Responsible individual assigned for incident communication strategy	Art. 14(2)	Supplementary
1.37	Simplified ICT risk management framework assessed for applicability	Art. 16	Supplementary

Tip: Items 1.01–1.04 (management body accountability) are typically the first area reviewed during a supervisory engagement. Ensure these are documented and evidenced before addressing operational items.

5. Pillar 2: Incident Management & Reporting

Articles 17–23 | RTS: CDR 2024/1772, CDR 2025/301 | ITS: CIR 2025/302

Incident management under DORA is defined by strict classification criteria and reporting timelines. Financial entities must classify incidents using the criteria in CDR 2024/1772 (clients affected, duration, data loss, geographic spread, economic impact) and submit reports in three phases: initial notification within 4 hours of classification, intermediate report within 72 hours, and final report within 1 month.

Key articles: Art. 17 (Process), Art. 18 (Classification), Art. 19 (Reporting obligations), Art. 20 (Templates), Art. 23 (Payment-related incidents).

Ref	Requirement	Article	Priority
2.01	Documented incident management process with roles, responsibilities and escalation paths	Art. 17(1)	**Critical**
2.02	Procedures to identify, track, log, categorise and classify all ICT-related incidents	Art. 17(2)	**Critical**
2.03	Early warning indicators defined for ICT incidents	Art. 17(3)	**Important**
2.04	Root cause analysis process established for all ICT-related incidents	Art. 17(3)	**Important**
2.05	Incident classification framework implemented using CDR 2024/1772 criteria	Art. 18(1)	**Critical**
2.06	Major incident thresholds defined (clients, duration, data loss, geography, economic impact)	Art. 18(1)	**Critical**
2.07	Initial notification within 4 hours of classifying a major incident	Art. 19(4)(a)	**Critical**
2.08	Intermediate report within 72 hours of initial notification	Art. 19(4)(a)	**Critical**
2.09	Final report within 1 month of initial notification	Art. 19(4)(a)	**Critical**
2.10	ITS reporting templates prepared and pre-filled for rapid submission	Art. 20	**Critical**
2.11	Management body informed of each major ICT-related incident	Art. 17	**Important**
2.12	Client notification process defined for incidents affecting financial interests	Art. 19(3)	**Important**
2.13	All incidents logged and classified (not only major), supporting trend analysis	Art. 17(2)	**Important**
2.14	Voluntary reporting process defined for significant cyber threats	Art. 19(2)	Supplementary
2.15	Aggregated annual cost/loss reporting capability for major incidents	Art. 11(10)	Supplementary
2.16	Payment-related incident reporting aligned with PSD2 (if applicable)	Art. 23	Supplementary

Tip: The 4-hour initial notification deadline (item 2.07) is the most operationally demanding requirement. Pre-filled templates and a rehearsed escalation process are essential to meet this timeline.

6. Pillar 3: Digital Resilience Testing

Articles 24–27 | RTS: CDR 2025/1190

Testing validates everything else. Without a structured testing programme, your risk management framework, BCP plans and security controls provide only theoretical assurance. DORA requires a proportionate testing programme covering all critical ICT systems, including vulnerability assessments, scenario-based testing, penetration testing, and — for designated entities — Threat-Led Penetration Testing (TLPT) at least every three years.

Key articles: Art. 24 (Testing programme), Art. 25 (Testing types), Art. 26–27 (TLPT). Items marked Critical* are critical only if your entity has been designated for TLPT by your NCA.

Ref	Requirement	Article	Priority
3.01	Documented, proportionate testing programme covering all critical ICT systems	Art. 24(1)	**Critical**
3.02	Testing programme reviewed and updated at least annually	Art. 24(2)	**Critical**
3.03	Vulnerability assessments and scans at least annually on all critical systems	Art. 25(1)	**Critical**
3.04	Network security reviews performed regularly	Art. 25(1)	**Important**
3.05	Scenario-based testing validating BCP and disaster recovery plans	Art. 25(1)	**Critical**
3.06	Gap analyses conducted to identify compliance shortfalls	Art. 25(1)	**Important**
3.07	Source code reviews conducted on critical systems where proportionate	Art. 25(1)	Supplementary
3.08	Performance and load testing on critical systems	Art. 25(1)	**Important**
3.09	Penetration testing conducted on critical ICT systems	Art. 25(1)	**Important**
3.10	Testing conducted by independent parties (internal or external)	Art. 25(3)	**Important**
3.11	All findings prioritised, classified and tracked to remediation	Art. 24(5)	**Critical**
3.12	Testing results feed back into ICT risk management framework updates	Art. 24(5)	**Critical**
3.13	TLPT applicability assessed with NCA and documented	Art. 26(1)	**Important**
3.14	TLPT performed at least every 3 years on live production systems (if designated)	Art. 26(1-2)	**Critical***
3.15	TLPT scope covers all critical functions including outsourced services	Art. 26(2)	**Critical***
3.16	Qualified external testers engaged meeting Art. 27 requirements	Art. 27	**Critical***
3.17	At least every third TLPT conducted by an external tester	Art. 27(1)(a)	**Critical***
3.18	TLPT results and remediation plans shared with NCA	Art. 26(8)	**Critical***

7. Pillar 4: Third-Party ICT Risk Management

Articles 28–44 | RTS: CDR 2024/1773, CDR 2025/532 | ITS: CIR 2024/2956

Third-party oversight is one of DORA's most distinctive requirements. The Register of Information (ROI), mandatory contract clauses, concentration risk assessment and exit strategies go beyond existing financial regulation. The ROI must be maintained in the ITS 2024/2956 format and submitted annually to the NCA by 30 April. Sub-contracting chains must be documented. Exit plans must be actionable.

Key articles: Art. 28 (Strategy, ROI, due diligence), Art. 29 (Sub-contracting, concentration risk), Art. 30 (Mandatory contractual clauses), Art. 31–44 (CTPP oversight framework).

Ref	Requirement	Article	Priority
4.01	Strategy on ICT third-party risk adopted by management body and regularly reviewed	Art. 28(2)	**Critical**
4.02	Register of Information maintained continuously in ITS 2024/2956 format	Art. 28(3)	**Critical**
4.03	Register available at entity, sub-consolidated and consolidated levels	Art. 28(3)	**Important**
4.04	Register ready for annual NCA submission (deadline: 30 April)	Art. 28(3)	**Critical**
4.05	Only contracting with providers meeting appropriate security standards	Art. 28(4)	**Important**
4.06	Pre-contract risk assessment for all providers supporting critical functions	Art. 28(4)	**Critical**
4.07	Due diligence conducted before entering ICT third-party arrangements	Art. 28(4)	**Critical**
4.08	Concentration risk assessed across provider base and reported to management body	Art. 28(5), 29	**Critical**
4.09	Annual NCA reporting on new ICT arrangements, provider categories and service types	Art. 28(3)	**Important**
4.10	Timely NCA notification of planned arrangements for critical functions	Art. 28(3)	**Important**
4.11	Contracts include all mandatory Art. 30(2) clauses (SLAs, exit, audit, security)	Art. 30(2)	**Critical**
4.12	Exit strategies defined for all critical ICT provider arrangements	Art. 28(8)	**Critical**
4.13	Transition plans documented and actionable if provider relationship must end	Art. 28(8)	**Important**
4.14	Sub-contracting chains identified, documented and in Register of Information	Art. 29, 30(2)(a)	**Critical**
4.15	Sub-contracting risk assessment for providers of critical functions	Art. 29	**Important**
4.16	Ongoing monitoring of provider performance, incidents and contractual compliance	Art. 28(2)	**Critical**
4.17	Audit rights over ICT providers exercised periodically	Art. 30(2)(e)	**Important**
4.18	Provider contractual obligation to participate in TLPT where applicable	Art. 30(3)(d)	**Important**
4.19	LEI used for entity identification in Register of Information and incident reporting	Art. 28(3)	**Important**
4.20	Cooperation with Lead Overseer for designated CTPPs	Art. 31-44	Supplementary

Tip: The Register of Information (items 4.02–4.04) has a hard annual submission deadline of 30 April. Start data collection well in advance and validate using the EBA's 85-rule validation engine.

8. Pillar 5: Information Sharing

Article 45

DORA encourages — but does not mandate — the sharing of cyber threat intelligence between financial entities. Participation in information sharing arrangements (such as ISACs) is voluntary but should be formally evaluated. Where sharing takes place, it must be within trusted arrangements that protect commercially sensitive and personal data.

Ref	Requirement	Article	Priority
5.01	Cyber threat information sharing arrangements evaluated and considered	Art. 45(1)	**Important**
5.02	Participation in relevant industry forums or ISACs for threat intelligence	Art. 45(1)	Supplementary
5.03	Information shared only within trusted arrangements with appropriate safeguards	Art. 45(2)	**Important**
5.04	Sharing arrangements protect commercially sensitive, personal and confidential data	Art. 45(2)	**Important**

9. RTS/ITS Quick Reference

The following Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS) have been published by the European Supervisory Authorities to support DORA implementation.

Reference	Full Title	Pillar	DORA Article
CDR 2024/1774	RTS on ICT risk management framework and simplified framework	Pillar 1	Art. 15, 16(3)
CDR 2024/1772	RTS on incident classification criteria and materiality thresholds	Pillar 2	Art. 18(3)
CDR 2025/301	RTS on incident reporting content and time limits	Pillar 2	Art. 20(a)
CIR 2025/302	ITS on incident reporting templates and procedures	Pillar 2	Art. 20(b)
CDR 2025/1190	RTS on threat-led penetration testing (TLPT)	Pillar 3	Art. 26–27
CDR 2024/1773	RTS on ICT third-party contractual policy	Pillar 4	Art. 28(10)
CIR 2024/2956	ITS on Register of Information templates	Pillar 4	Art. 28(9)
CDR 2025/532	RTS on sub-contracting conditions for critical functions	Pillar 4	Art. 30(5)
CDR 2024/1502	Delegated act on CTPP designation criteria	Pillar 4	Art. 31(6)
CDR 2024/1505	Delegated act on oversight fees for CTPPs	Pillar 4	Art. 43(2)
CDR 2025/420	RTS on joint examination team composition	Pillar 4	Art. 41(1)(c)

10. Next Steps

Download the Companion Excel Template

The editable Excel template includes all 95 checklist items with dropdown fields for maturity scoring, status tracking, evidence documentation and remediation planning. The Summary Dashboard auto-calculates your compliance posture per pillar.

doragrc.com/downloads/dora-compliance-checklist-2026.xlsx

Take the Free DORA Gap Analysis

For a quick, automated assessment, take the free DORA gap analysis. It scores your maturity across all five pillars on a weighted scale and identifies your weakest areas. The assessment takes approximately 3 minutes and requires no account.

doragrc.com/dora-gap-analysis

Explore the DORA GRC Platform

DORA GRC is a purpose-built compliance platform for EU financial entities. It automates the data collection, linkage and reporting across all five pillars — including the Register of Information, incident reporting, risk assessment, testing programme management and 360° intelligence across assets, providers and functions.

doragrc.com/features

Contact

For questions, feedback or to start a free trial:
mail@doragrc.com
doragrc.com