DORA

DORA (whole Part)

Audit Checklist

237 audit questions across **26** sections.

HOW TO USE THIS CHECKLIST

Each question has three boxes the auditor fills in during the audit:

1. **Compliance** — the binary headline: Compliant / Non-compliant.
2. **Classification** — where the gap is, four-state grid: Documented / Implemented matrix.
3. **Finding level** — severity: Maj / Min / Obs (Major nonconformity / Minor nonconformity / Observation).

Severity is the auditor's call on the day, against the real finding — no severity is pre-suggested per question.

auditchecklists.org Audit Checklist Licence

Product:	DORA (whole Part) (237 questions)
Regulation:	
Issued:	[YYYY-MM-DD — STAMPED AT ISSUE]

Licensed to:	[ORG NAME — STAMPED AT ISSUE]
Licensee email:	[EMAIL — STAMPED AT ISSUE]
Order:	[AVI-YYYY-NNNNN — STAMPED AT ISSUE]

Licence terms

This audit checklist is licensed for use within the organisation named above by the licensee email named above. Use is permitted by employees and contractors of the named organisation in the course of their work for that organisation, including printing, internal distribution within the organisation, annotation during audits, and incorporation into the organisation's management-system documentation as a working reference.

Not for redistribution. Sharing this document, or any derivative or extract of it, with any party outside the named organisation is a breach of this licence. This includes posting to file-sharing networks, internal wikis or knowledge bases accessible to other organisations, vendor portals, supplier-facing GRC systems, and email forwarding to colleagues at other firms. Quoting individual audit questions in regulator submissions or internal training materials is permitted; reproducing the structured checklist as a whole is not.

Each additional organisation or operating site requires a separate licence. If a sister organisation in the same group, or a separate operating entity, requires the same checklist, contact licences@auditchecklists.org for a multi-site licence quote. Holding companies licensing for multiple subsidiaries are eligible for group-licence pricing.

Licence transfers. This licence does not transfer with sale, merger, or organisational restructure without written consent. auditchecklists.org may, at its discretion, transfer the licence to the successor organisation on request — usually a formality, contact licences@auditchecklists.org.

Defects and amendments. If you identify a defect in this checklist — wrong content, mistranscribed regulation, factual error — email support@auditchecklists.org. We will verify the defect, correct it, and reissue the affected artefacts to you within a reasonable timeframe at no further charge. Regulatory amendments published during your 12-month update

§Article 2

Scope

Q1 ARTICLE DORA Art.2(1)

Has the entity self-classified under one or more of the §2(1)(a)–(u) entity classes — and confirmed the classification with reference to the underlying sectoral definitions (CRR, MiFID II, PSD2, EMD2, MiCA, Solvency II, AIFMD, UCITS, etc.)?

SOURCE VERBATIM

> 1. Without prejudice to paragraphs 3 and 4, this Regulation applies to the following entities:
>
> (a) credit institutions; (b) payment institutions, including payment institutions exempted pursuant to Directive (EU) 2015/2366; (c) account information service providers; (d) electronic money institutions, including electronic money institutions exempted pursuant to Directive 2009/110/EC; (e) investment firms; (f) crypto-asset service providers [...]; (g) central securities depositories; (h) central counterparties; (i) trading venues; (j) trade repositories; (k) managers of alternative investment funds; (l) management companies; (m) data reporting service providers; (n) insurance and reinsurance undertakings; (o) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries; (p) institutions for occupational retirement provision; (q) credit rating agencies; (r) administrators of critical benchmarks; (s) crowdfunding service providers; (t) securitisation repositories; (u) ICT third-party service providers.
>
> — Regulation (EU) 2022/2554 Article 2(1), Original 2022-12-14 (DORA)

COMPLIANCE

☐ Compliant ☐ Non-compliant

CLASSIFICATION (FOUR-STATE)

☐ Documented and Implemented
☐ Documented Not Implemented
☐ Not Documented but Implemented
☐ Not Documented and Not Implemented

FINDING LEVEL

☐ Maj ☐ Min ☐ Obs

Maj = Major nonconformity · Min = Minor nonconformity · Obs = Observation

SUGGESTED EVIDENCE TO REQUEST

- §2(1) self-classification record per class
- Underlying licence / authorisation documents
- For multi-class entities: per-class assessment

MANAGEMENT SYSTEM REFERENCE: _____

FINDINGS / NOTES:

Q2 ARTICLE DORA Art.2(3)

After §2(1) self-classification, has the entity assessed whether any §2(3) exclusion applies — and recorded the conclusion (in scope, or excluded under a specific named ground)?

SOURCE VERBATIM

> 1. This Regulation does not apply to:
>
> (a) managers of alternative investment funds as referred to in Article 3(2) of Directive 2011/61/EU; (b) insurance and reinsurance undertakings as referred to in Article 4 of Directive 2009/138/EC; (c) institutions for occupational retirement provision which operate pension schemes which together do not have more than 15 members in total; (d) natural or legal persons exempted pursuant to Articles 2 and 3 of Directive 2014/65/EU; (e) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries which are microenterprises or small or medium-sized enterprises; (f) post office giro institutions as referred to in Article 2(5), point (3), of Directive 2013/36/EU.
>
> — Regulation (EU) 2022/2554 Article 2(3), Original 2022-12-14 (DORA)

COMPLIANCE

☐ Compliant ☐ Non-compliant

CLASSIFICATION (FOUR-STATE)

☐ Documented and Implemented
☐ Documented Not Implemented
☐ Not Documented but Implemented
☐ Not Documented and Not Implemented

FINDING LEVEL

☐ Maj ☐ Min ☐ Obs

Maj = Major nonconformity · Min = Minor nonconformity · Obs = Observation

SUGGESTED EVIDENCE TO REQUEST

- Per claimed exclusion: the named §2(3) ground and the underlying threshold check
- For sub-threshold AIFMs: AuM evidence
- For small IORPs: member-count evidence
- For micro/SME insurance intermediaries: SME classification record

MANAGEMENT SYSTEM REFERENCE: _____

FINDINGS / NOTES:

§Article 4

Proportionality principle

Q1 ARTICLE DORA Art.4(1)

Has the entity calibrated its Ch II ICT risk-management implementation to its size, overall risk profile, and the nature/scale/complexity of its services, activities and operations — and recorded the calibration?

SOURCE VERBATIM

> 1. Financial entities shall implement the rules laid down in Chapter II in accordance with the principle of proportionality, taking into account their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations.
>
> — Regulation (EU) 2022/2554 Article 4(1), Original 2022-12-14 (DORA)

COMPLIANCE

☐ Compliant ☐ Non-compliant

CLASSIFICATION (FOUR-STATE)

☐ Documented and Implemented
☐ Documented Not Implemented
☐ Not Documented but Implemented
☐ Not Documented and Not Implemented

FINDING LEVEL

☐ Maj ☐ Min ☐ Obs
Maj = Major nonconformity · Min = Minor nonconformity · Obs = Observation

SUGGESTED EVIDENCE TO REQUEST

- Per Ch II article: calibration record (size/risk-profile/complexity inputs)
- Sample of measures with explicit depth choice
- Periodic recalibration on material change

MANAGEMENT SYSTEM REFERENCE: _____

FINDINGS / NOTES: