DORA on One Page, Quick Reference Cheat Sheet

Null-Packet · Free DORA resource · v1.0 · Regulation (EU) 2022/2554 · *Not legal advice*

Who's in scope

Named list, not sector × size. Article 2(1) lists ~20 financial-entity types (banks, payment & e-money institutions, investment firms, crypto-asset service providers, CSDs, CCPs, trading venues, fund managers, insurers, IORPs, rating agencies, crowdfunding platforms, and more). If you match a named type, you're in, DORA runs no general size test first.

	Full regime	Simplified framework (Art. 16)
Who	Most financial entities	Small/non-interconnected investment firms; exempted payment/e-money institutions; small IORPs (<15 members); proportionality-scaled microenterprise obligations
ICT risk management	Full Chapter II	Lighter, proportionate version
Incident reporting, testing, third-party rules	Apply in full	Apply, proportionately

Separately: ESAs can **designate** certain ICT providers (cloud, data, software) as **critical**, placing them under direct EU oversight (Title V) - a different regime from the one this toolkit covers.

The 5 pillars (Chapters II-VI)

Ch.	Pillar	The one thing to get right
II	ICT risk management (Art. 5-16)	A board-owned framework, tested, not a document that sits on a shelf
III	ICT incident management, classification & reporting (Art. 17-23)	Classify fast, the reporting clock runs from awareness, not resolution
IV	Digital operational resilience testing (Art. 24-27)	Test like an attacker would, not a checklist audit; TLPT for the entities it applies to
V	ICT third-party risk management (Art. 28-44)	The Register of Information, kept live, not built once for a submission
VI	Information sharing (Art. 45)	Voluntary, join a sharing arrangement if your sector has one

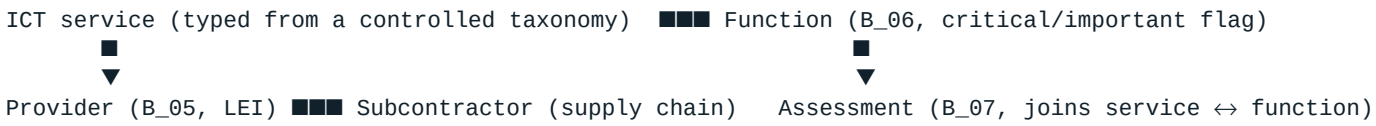
Governance (Art. 5), the personal one

The **management body** bears ultimate responsibility, **approves** the ICT risk management framework, **oversees** it, maintains knowledge to assess ICT risk, and **allocates budget**. → Keep a **dated management-body approval** on record, same discipline as NIS2 Article 20.

The Register of Information (Art. 28(3)), DORA's distinctive artifact

Unlike NIS2 and CIS, DORA **prescribes the format**: Commission Implementing Regulation (EU) 2024/2956 sets out interlinked templates (the `B_xx` series), not a free-form spreadsheet.

```
Financial entity (B_01, keyed by LEI)
        ■
        ▼
Contractual arrangement (B_02, arrangement reference no.)
        ■
        ▼
```



Every arrow is a foreign key the ESA collection validates before a human reads a single field. Get the **Legal Entity Identifier of the exact contracting entity** (not the brand, not the ultimate parent) from GLEIF, and reconcile the register against your contract repository and your third-party risk register on a fixed cycle, those three drift apart otherwise.

The incident reporting clock (Art. 19), from AWARENESS

```
Initial notification  →  as soon as possible, no later than 24h after classifying as "major"
Intermediate report   →  within 72h of the initial notification
Final report          →  within 1 month of the intermediate report
```

Classify using the criteria in the RTS on incident classification (clients/ counterparts/transactions affected, duration, geographical spread, data losses, economic impact, reputational impact, service criticality). **Major** incidents trigger the clock; lesser incidents are logged but not reported on this schedule. *If personal data is involved, the GDPR 72h DPA notification runs in parallel as a separate obligation.*

Do this first (in order)

1. Confirm your entity type and regime (full / simplified) · identify your competent authority
2. Stand up governance, management-body approval + oversight cadence
3. Start the Register of Information (entity, arrangements, providers, functions, assessment)
4. Tier third-party ICT services by criticality; flag critical/important functions with a documented method
5. Incident classification criteria + reporting templates + authority contact
6. Build the testing programme (proportionate to size and criticality)
7. Evidence pack + management report

Framework shortcut

Already run one of these? DORA's ICT risk management measures map onto them, don't start over: **ISO/IEC 27001:2022** · **NIST CSF 2.0** · **CIS Controls v8**. The Register of Information itself has no equivalent in any of the three, it is DORA's own prescribed artifact.

DORA vs NIS2, the one rule to remember

For a financial entity in DORA's scope, DORA is **lex specialis**: for ICT risk management, ICT third-party risk, and incident matters, apply DORA's rules, including the Register of Information, rather than the equivalent NIS2 provisions for the same subject. You do not run both in parallel for the same requirement.

---

*Get the full build kit: the **DORA Compliance Toolkit**, implementation guide, ICT risk framework mapping, Register of Information templates, third-party risk register, incident classification & reporting playbook, 10-policy pack, roadmap and board pack. shop.null-packet.com*

© null-packet, free to share unmodified. Implementation guidance, not legal advice.