Copla

A FIELD GUIDE FROM COPLA

DORA in Practice.

Lessons from the first reporting cycle, and what to prepare for in the next supervisory wave.

WRITTEN BY

Ričardas Brogys

Chief Information Security Officer, Copla

PUBLISHED

May 2026

First edition

IN THIS GUIDE

What's inside.

ABOUT THIS GUIDE

This is a practitioner's reference for compliance leaders, CISOs, and operational risk owners working through DORA. It is written from inside regulated institutions, not from a vendor pitch deck. Every section is structured to be readable in under five minutes and actionable inside a working week.

FOREWORD

From preparation to practice.

The first DORA reporting cycle closed at the end of March. Across 23 countries, we watched our clients move from preparation to live submission. What followed was instructive.

Gaps surfaced. Supervisors began asking sharper questions. Patterns started to separate firms ready for ongoing scrutiny from those still treating DORA as a one-off project.

This guide collects what we have learned from that cycle. It is written by Ričardas Brogys, who has implemented these frameworks inside regulated institutions before joining Copla. It is intended for compliance leaders, CISOs, and operational risk owners who want a practitioner's view rather than a vendor's marketing brochure.

It is also a forward-looking document. The first cycle is closed. The next one is already underway. The supervisory wave that follows will reward firms who treat compliance as living infrastructure, maintained continuously, rather than annual housekeeping.

We hope it helps.

Aurimas Bakas

Chief Executive Officer, Copla

CHAPTER 01

Are you in scope, and at what level?

> DORA applies to a wide range of financial entities, but the obligations differ by category. Knowing where you sit is the foundation for everything that follows.

The default: full ICT risk management framework (Articles 5–15)

Most financial entities operate under the full ICT risk management framework set out in Articles 5–15. This covers credit institutions, payment institutions, e-money institutions, investment firms, crypto-asset service providers, crowdfunding service providers, and the wider list of 20+ financial entity categories named in Article 2. Incident management, testing, and third-party risk obligations in Chapters III–V apply on top of this.

The carve-out: simplified framework (Article 16)

Article 16 disapplies Articles 5–15 and substitutes a lighter set of obligations for a closed list of small or already-exempted entities:

- Small and non-interconnected investment firms
- Payment institutions exempted under PSD2
- Credit institutions exempted under CRD
- Electronic money institutions exempted under EMD
- Small institutions for occupational retirement provision

If your entity isn't on this list, the simplified framework does not apply to you, regardless of size. The simplified framework still requires a documented ICT risk management framework, continuous monitoring, business continuity, and regular testing. It is lighter, not absent.

Three questions to self-assess scope

1. **What is your authorisation type?** Your licence category under EU financial law is the primary scope determinant. Business model and portfolio size are secondary signals.
2. **Are you on the Article 16 list?** The simplified framework is a closed list of entity types. If your category isn't named there, you're under the full framework. Size alone does not move you to the simplified track.
3. **Are you in a grey zone?** If your situation involves multiple activities, novel structures, or cross-border complexity, calibrate directly with your competent authority before making assumptions.

ONCE SCOPE IS CONFIRMED

Three things must be in place:

1. ICT risk management framework, documented and board-approved.
2. ICT third-party contract register, prepared for submission and maintained continuously.
3. Incident classification procedure, in place and rehearsed before an incident occurs.

> ***Scope clarity is the first finding supervisors catch. Misclassification at this stage cascades into every subsequent obligation.***

CHAPTER 02

What regulators actually care about.

> The most useful summary of DORA's supervisory posture: substance over form. A 50-page ICT policy that nobody follows carries less weight than a five-page document that reflects daily operations. Three priorities have surfaced consistently in first-cycle supervisory engagement.

Substance over form

Policies need to reflect operational reality. The test supervisors apply is whether the people on the front line can describe their responsibilities in the same terms as the policy.

Board accountability

Article 5 places ICT risk ownership at management body level. Supervisors look for board minutes that approve the ICT risk framework, risk appetite statements, and evidence that senior management receives regular ICT risk reporting outside of audit cycles.

Where the board cannot articulate ICT risk appetite in its own words, that finding follows. If the answer comes only from the CISO, supervisors will record it.

Documented proportionality

DORA explicitly allows smaller firms to adapt requirements to their size and complexity. The condition is that the rationale is written down. "We are a small team" is not a rationale. A statement that describes the ICT environment (X systems, Y third parties, Z critical processes) and explains the chosen approach against that environment is.

THE LENS FOR EVERYTHING THAT FOLLOWS

Governance, testing, third-party risk, and reporting all need to demonstrate substance, board ownership, and proportionality at the same time. Every chapter that follows assumes this lens is applied.

CHAPTER 03

Governance: what regulators look for.

> DORA does not prescribe headcount or org charts. It prescribes outcomes. The structure a firm chooses must deliver three things and document the reasoning behind them.

Named ownership

Every ICT risk function, control function, and audit function needs a clearly identified owner. Supervisors will ask who is responsible, and the answer must be a person and a role. "The team" is not an answer. Ambiguity here is an early finding.

Functional independence

Control and audit functions must be able to escalate findings without conflict of interest. The way this is implemented depends on the organisation. Document how independence is maintained in the specific structure chosen.

Board-level accountability

The management body approves the ICT risk framework, sets risk appetite, and receives regular ICT risk reporting. This is not delegatable downward. Supervisors review board minutes to verify this is happening in practice.

THREE LINES OF DEFENCE, OR AN EQUIVALENT

Article 6(4) requires segregation between ICT risk management, control, and internal audit functions according to the three-lines-of-defence model **or an equivalent internal risk management and control model**. Microenterprises are exempt from this requirement. For non-microenterprise firms, proportionality allows combined first and second line roles where independence can still be demonstrated, with the third line covered by outsourced internal audit. Whatever structure is chosen, it must be justified, documented, and board-approved.

CHAPTER 04

ICT testing: your minimum viable programme.

> Article 25(1) lists 12 testing techniques as examples of what a digital operational resilience testing programme may include. DORA doesn't designate a fixed "minimum five." In our practice, five of these form a defensible floor for smaller entities with limited ICT complexity.

What Article 25 actually lists

The 12 techniques named in Article 25(1) are: vulnerability assessments and scans, open-source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing, and penetration testing. The list is non-exhaustive and the selection should follow a risk-based approach.

The five we recommend as a practitioner floor

1. **Vulnerability assessments and scans.** At least annually, and after significant changes to the ICT environment.
2. **Network security assessments.** Annually, or following major infrastructure change.
3. **Gap analyses against DORA requirements.** Documented with a remediation plan, reviewed annually.
4. **Scenario-based tests.** A minimum of one per year. Ransomware recovery is the most common starting point and a defensible choice for first-cycle programmes.
5. **Penetration testing.** At least once a year. More frequent testing applies if the risk profile or recent incidents warrant it.

What can be deferred

Open-source analysis, source code reviews, and physical security reviews are required only where feasible and proportionate to the ICT environment. If deferred, document the reasoning.

Threat-led penetration testing (TLPT)

Article 26 requires TLPT only for financial entities identified by their competent authority, based on impact, financial stability, and ICT risk profile criteria set out in Article 26(8). Simplified-framework entities (Article 16) and microenterprises are excluded from TLPT entirely. The vast majority of fintechs are not designated for TLPT and operate under standard penetration testing requirements only.

Documentation is non-negotiable

Test results, remediation tracking, and evidence of board-level reporting must be retained and produced on request. This is typically what supervisors ask for first.

> **PRACTITIONER NOTE**
>
> The most common gap in first-cycle testing programmes is not the testing itself. It is the audit trail. Firms run the tests, then fail to capture the remediation closure, the board acknowledgement, and the change record that connects the test result to the next iteration of the programme.

CHAPTER 05

Third-party risk: the oversight framework.

> Articles 28–30 apply to all ICT third-party service providers, not only those classified as critical. Building the foundation begins with inventory.

Start with the register

Before working through the obligations, list every tool and service the business depends on. Provider name, service type, criticality classification, contract status. That inventory is the foundation for everything else in the third-party regime.

Five obligations for every ICT provider relationship

1. **ICT provider register.** Documented inventory of providers, services, criticality, and contract status.
2. **Preliminary risk assessment.** Conducted before onboarding. Covers security posture, financial stability, and substitutability.
3. **Contractual provisions.** Article 30 mandatory clauses in every ICT contract (see Chapter 06).
4. **Exit strategy.** A documented transition plan covering who takes over, expected duration, and the data portability mechanism.
5. **Ongoing monitoring.** Periodic review of SLA performance, security incidents at provider level, and sub-outsourcing changes.

Concentration risk

If a single provider failure would cause material disruption, that exposure must be documented as concentration risk in the ICT Annual Risk Assessment and reported to the management body. The same provider can appear as concentration risk under multiple service categories.

The hyperscaler problem

AWS, Azure, and Google Cloud offer standardised contracts that cannot realistically be negotiated. DORA was written knowing this. The expectation is that firms know what they have accepted, identify the gaps against Article 30, implement compensating controls on their own side, and maintain an exit plan.

> ***The supervisory question is not "did you negotiate AWS?" It is "do you know what you accepted, and what you have done about it?"***

PRACTICAL TOOL: THE COMPENSATING CONTROLS REGISTER

For hyperscalers, maintain a register with one row per Article 30 clause. Each row documents the gap between the standard provider contract and the DORA requirement, and the firm-side mitigation that closes it.

This is what a supervisor will want to see. It demonstrates that the firm has read its own contracts, understood the obligations, and made conscious decisions about residual risk.

CHAPTER 06

The Article 30 contract checklist.

> Article 30 sets two tiers of mandatory contractual clauses. Paragraph 2 lists nine clauses required in every ICT contract. Paragraph 3 adds six more for contracts supporting critical or important functions.

Article 30(2) — required in every ICT contract

Required clause	What it covers (and the workaround for non-negotiable contracts)
(a) Service description & subcontracting	Complete description of ICT services; whether subcontracting of critical/important services is permitted and the conditions. For standard contracts: extract from the master services agreement.
(b) Data processing locations	Regions/countries where services are provided and data is processed and stored. Advance notification of location changes. For non-negotiable: extract from the DPA; request written confirmation.
(c) Data protection provisions	Availability, authenticity, integrity, confidentiality of data, including personal data. Usually in the DPA and security schedule.
(d) Data return on insolvency or termination	Access, recovery, and return of personal and non-personal data in accessible format on insolvency, resolution, or termination. Document the data portability mechanism on your side.
(e) Service level descriptions	SLAs including updates and revisions. Reference the provider's published SLA; attach as an annex to your internal record.
(f) Incident assistance from provider	Provider assistance during ICT incidents at no additional cost (or at a price agreed in advance). Usually in the master agreement's support terms.
(g) Cooperation with competent authorities	Provider obligation to cooperate fully with your competent authority and resolution authority.
(h) Termination rights	Right to terminate with minimum notice periods, in line with supervisory expectations. Supplement with your own internal termination procedure.
(i) Security training participation	Conditions for provider staff to participate in your ICT security awareness programmes and resilience training (Article 13(6)).

Article 30(3) — additional, for contracts supporting critical or important functions

Additional clause	What it covers (and the workaround for non-negotiable contracts)
(a) Full quantitative SLAs	Precise quantitative and qualitative performance targets allowing effective monitoring and corrective action.
(b) Material change notifications	Notice periods and reporting from the provider on developments materially affecting service delivery.
(c) Business continuity testing	Provider obligation to implement and test BCPs and to maintain appropriate ICT security measures. Map to your own BCM framework; document where provider RTO exceeds your tolerance.
(d) Cooperation in TLPT	Provider participation in your threat-led penetration tests under Articles 26–27.
(e) Audit & inspection rights	Unrestricted audit, inspection, and copy-taking rights for you, your appointed third party, and the competent authority. For non-negotiable: SOC 2 Type II or ISO 27001 may substitute by agreement; obtain annually.
(f) Exit strategy & transition	Mandatory transition period during which the provider continues service to allow migration to another provider or in-house. Document your own migration plan independently.

THE RULE

Article 30(2) applies to every active ICT contract. Article 30(3) applies on top, for contracts supporting critical or important functions. Hyperscaler contracts don't exempt the firm from either tier; they shift the obligation from negotiation to compensating controls on the firm's side.

CHAPTER 07

Supervisory reporting: what goes to the regulator.

> Three deliverables anchor DORA's supervisory reporting cycle. The first cycle is closed. Maintaining each of them continuously is what separates first-cycle survivors from second-cycle success.

Annual ICT risk report

A summary covering:

- ICT risk profile, risk appetite, and control effectiveness
- Significant incidents and near-misses from the reporting period
- Testing programme outcomes and open remediation items
- Overview of ICT third-party dependencies and concentration risks

Register of ICT contracts

The hardest deliverable in the first cycle, and the area with the largest first-cycle gaps. Three things to know:

- The register must be submitted to your competent authority on request and maintained continuously.
- The ESAs published a standardised template. Your register must map to it precisely.
- It covers all ICT third-party arrangements, not only those classified as critical or material.

The most common issues in first-cycle submissions: missing sub-outsourcing entries, no exit strategy documented, SLA data not recorded at contract level.

Incident reporting timelines

Article 19 establishes the requirement to submit an initial notification, an intermediate report, and a final report. Article 20 delegates the precise time limits to the European Supervisory Authorities. The actual 4h / 72h / 1-month cadence is set in the Commission Delegated Regulation (EU) 2025/302 (RTS on major incident reporting). Critically, these timelines start from the moment an incident is **classified as major**, not from when the incident occurred. Classification speed determines whether the reporting clock can be met.

4h

Initial notification to the competent authority

72h

Intermediate report with updated impact assessment

1mo

Final report with root cause and remediation

WHY CLASSIFICATION SPEED MATTERS

The four-hour window is short. If classification happens in hour three of an incident, the notification window is one hour, not four. Firms who treat classification as the first step of incident response, run in parallel with technical triage, are the ones who consistently meet the timeline.

The classification decision log (see Chapter 08) is the artefact supervisors will ask for when reviewing reporting timeliness.

> ***The clock starts at classification, not at incident. Build the classification flow before you need it.***

CHAPTER 08

Incident classification: is this a major incident?

A "major" ICT incident triggers mandatory reporting to the national competent authority. Article 18 sets six classification criteria; the quantitative thresholds that turn an incident into a "major" one are defined in the Commission Delegated Regulation (EU) 2025/301 (RTS on incident classification). Classification paralysis is the most common failure mode at this point in the lifecycle.

Article 18 criterion	What it covers	Practical guidance
(a) Clients, counterparts, transactions, reputation	Number/relevance of clients or financial counterparts affected, transactions affected, and reputational impact.	Define your own internal thresholds in advance (RTS sets the regulatory ones). Document them. Don't decide under pressure.
(b) Duration & service downtime	How long the incident and the service disruption last.	The RTS sets the quantitative threshold. Partial degradation counts: if core services are impaired the clock is running, even if some users are unaffected.
(c) Geographical spread	Particularly relevant if the incident affects more than two Member States.	"More than two" means three or more, not "multiple." A two-country shared infrastructure outage may still be major under other criteria, but not under (c) alone.
(d) Data losses	Loss in relation to availability, authenticity, integrity, or confidentiality of data.	Broader than data breaches. Unavailability of critical data (transaction records, KYC files) also qualifies.
(e) Criticality of services affected	Whether the affected service supports a critical or important function of the entity.	An outage of a non-critical internal tool is unlikely to be major. An outage of a payment or trading function almost certainly is.
(f) Economic impact	Direct and indirect costs and losses, in absolute and relative terms.	Report proactively if economic impact alone would meet the RTS threshold, even if other criteria don't.

Source: DORA Article 18(1). Quantitative thresholds: Commission Delegated Regulation (EU) 2025/301.

Two principles for the classification flow

PRINCIPLE 01

Build a classification decision log. Every incident, whether ultimately classified as major or not, should have a recorded classification decision with rationale. This protects the firm if a supervisor later questions a non-report.

PRINCIPLE 02

When in doubt, report early. An initial notification can be updated. A missed four-hour window cannot be undone. Supervisors are more concerned by delayed or absent reporting than by over-reporting.

> ***Classification speed is what determines whether the reporting clock can be met. Build the decision tree before you need it, not during the incident.***

What "rehearsed" looks like

The most efficient way to surface gaps in the classification flow is to walk a hypothetical incident through the criteria and the timeline before a real one arrives. A 90-minute tabletop exercise once a quarter, with the incident commander, the legal counsel, and a board observer, will catch the issues that documentation alone cannot.

Common gaps surfaced in tabletops: unclear escalation paths to the management body outside business hours, ambiguity about who signs off the initial notification, missing contact details for the competent authority.

CHAPTER 09

Practitioner Q&A.

> Selected questions from a live audience of compliance and security leaders working through their first DORA reporting cycle.

Q1 · Scope

A crowdfunding service provider has asked whether the simplified framework applies to them. Does it?

A. No. Article 16's simplified framework is a closed list of entity types: small and non-interconnected investment firms, exempted payment institutions, exempted credit institutions, exempted e-money institutions, and small IORPs. Crowdfunding service providers aren't on that list, so they operate under the full ICT risk management framework in Articles 5–15 regardless of size.

Q2 · Governance

What structure is acceptable for smaller entities that cannot implement a full three-lines-of-defence model?

A. Article 6(4) accepts the three-lines-of-defence model or an equivalent internal risk management and control model, and exempts microenterprises entirely. For non-microenterprise smaller firms, combined first and second line roles are workable where functional independence can be demonstrated. Outsourced internal audit can cover the third line. Document the rationale for proportionality and obtain board sign-off.

Q3 · Testing

What's a defensible minimum testing set for an entity with limited ICT complexity?

A. DORA Article 25 doesn't prescribe a fixed minimum. It lists 12 techniques as examples and requires a risk-based selection. In our practice, vulnerability scans, network assessments, gap analyses, scenario-based tests, and penetration testing at annual cadence form a defensible floor. TLPT is required only for entities identified by their competent authority under Article 26(8); most fintechs are not designated.

Q4 · Third-party risk

How do you meet Articles 28–30 when large providers offer non-negotiable contracts?

A. Document what was accepted. Identify the gaps against Article 30. Implement compensating controls on the firm's own side. Maintain an independent exit plan. The compensating controls register is the defence.

CHAPTER 10

What to prepare for in the next supervisory wave.

> The first DORA reporting cycle closed at the end of March 2026. Supervisors are now reviewing submissions, issuing clarification requests, and beginning to set expectations for the cycle ahead. Three areas are likely to attract the most attention in the months to come.

01 · Continuity, not completion

The first cycle rewarded firms who could submit on time. The second will reward firms who can demonstrate that the register, the risk framework, and the testing programme have continued to evolve since submission. Supervisors will look for evidence of updates: new vendors added to the register, retired contracts removed, classification decisions logged during the year, and board engagement that continued past March.

The practical response is to schedule monthly maintenance of the contract register and quarterly board reporting on ICT risk. Firms that treated the submission as a project will have the largest gap to close here.

02 · Sub-outsourcing depth

Sub-outsourcing entries were one of the most commonly incomplete fields in first-cycle submissions. The next wave is likely to test whether firms know who their providers' providers are, particularly for cloud-hosted services where the chain can extend several layers.

The practical response is to extend the register schema to capture sub-outsourcing relationships explicitly, and to subscribe to provider change notification channels so that updates in the chain reach the register automatically.

03 · Classification rigour and reporting cadence

Where firms reported incidents in the first cycle, supervisors will assess whether the classification decision was timely and defensible. Where firms did not report, supervisors will want to see classification decision logs that justify the absence of a report.

The practical response is to rehearse the classification flow before an incident occurs. Tabletop exercises that walk a hypothetical incident through the criteria and timeline are the most efficient way to surface gaps in the decision process.

LOOKING FURTHER · THE UK REGIME

For firms with UK exposure, the FCA's PS26/2 and PRA's PS7/26 introduce a comparable material third-party reporting regime that takes effect in March 2027. The underlying mechanics are similar to DORA's third-party regime. Firms that have built strong contract registers under DORA will find the lift to UK compliance manageable, provided the schema is designed with multi-jurisdiction reporting in mind from the start.

The next supervisory wave will reward firms who treat compliance as living infrastructure, maintained continuously, rather than annual housekeeping.

Copla

Let's continue the conversation.

ABOUT COPLA

Copla is a guided compliance engine for licensed financial institutions and fintechs. We help payment institutions, e-money firms, crypto-asset providers, investment firms, and crowdfunding platforms build real, auditable security posture alongside their compliance obligations.

We are EU-based, framework-agnostic across DORA, NIS2, and MiCA, and serve clients in 23 countries.

COPLA REGISTRY

Copla Registry is our dedicated tool for ICT third-party contract registers. Structured directly to the ESAs' template, with guided data capture, automatic gap flagging, and export-ready output.

What takes weeks in a spreadsheet takes hours in the Registry.

Try Copla Registry →

copla.com/dora-register-of-information

AUTHOR

Ričardas Brogys

CISO, Copla

ricardas.brogys@copla.com

FOREWORD

Aurimas Bakas

CEO, Copla

EDITION

May 2026

First edition