



DORA Compliance Explainer

Understanding the Digital
Operational Resilience Act



03

What is DORA

04

Why it matters
Who needs to comply

05

Manual compliance burden

06

Time and cost of
achieving compliance

10

Breakdown of DORA
requirements and how we help

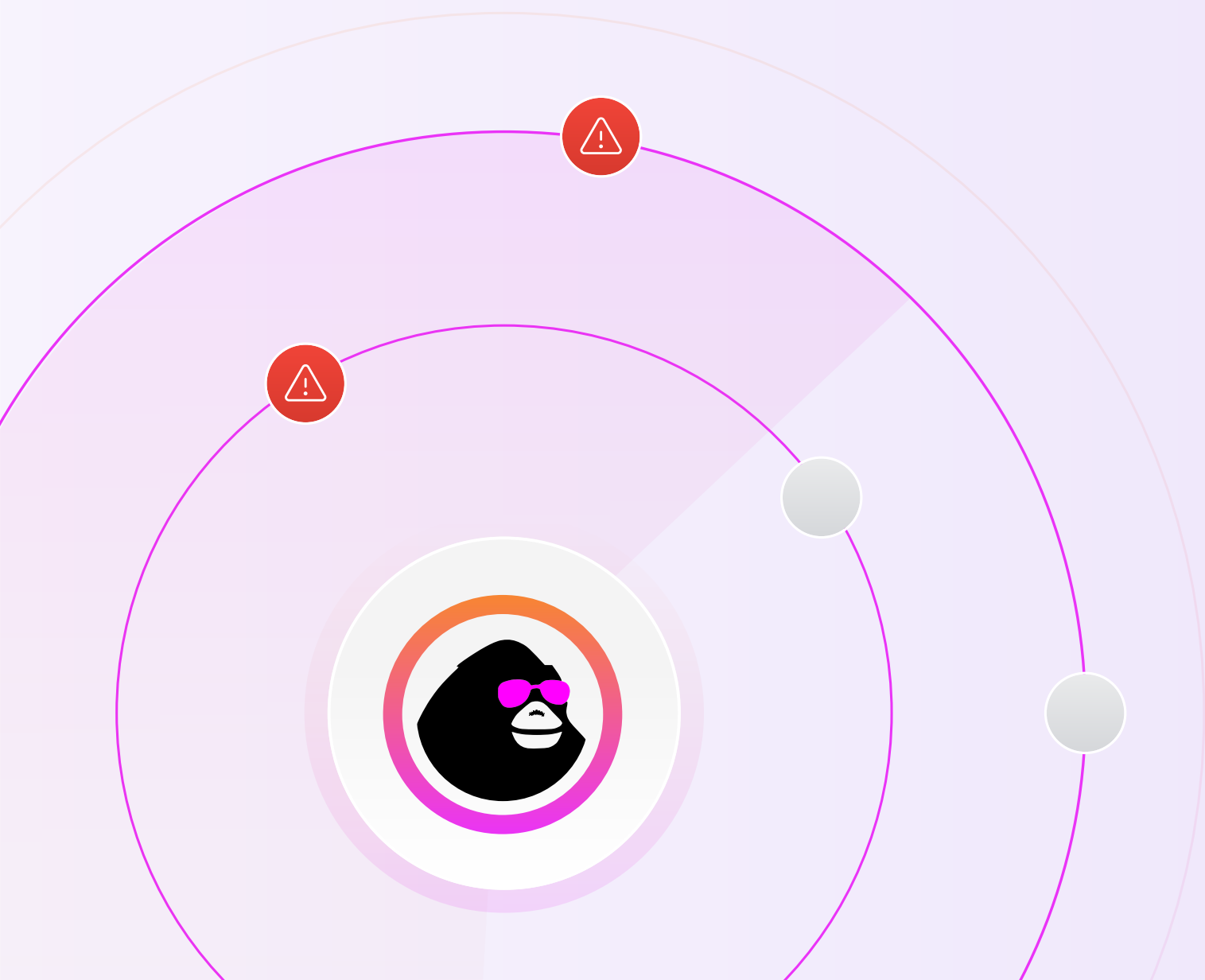
13

Why to use an automated
compliance tool

14

Resources and next steps





What is **DORA**

The Digital Operational Resilience Act (DORA) is an EU regulation that mandates how financial entities must manage digital risk.



**It entered into force on
January 17, 2025, aiming to:**

Unify ICT risk management across
the EU's financial sector

Close regulatory gaps between sectors

Ensure companies can resist, respond
to, and recover from ICT disruptions

DORA applies
alongside other
frameworks (e.g.
NIS2, GDPR, ISO
27001), but is
laser-focused
on operational
resilience
for financial
institutions.

Who needs to comply

DORA applies broadly to regulated financial entities and their critical ICT providers:



Banks, insurance firms, investment funds



Crypto-asset providers and crowdfunding platforms



Payment and account information service providers



ICT third-party service providers (subject to European Supervisory Authorities oversight)



Micro and small enterprises may be eligible for proportionality reductions, but are not exempt

Why it matters

DORA introduces a unified regulatory baseline across the EU, addressing growing digital interdependence and cyber risks in the financial sector.

It matters because it:

- Enhances trust among customers, regulators, and partners
- Protects financial stability by reducing ICT-related disruptions
- Aligns operational practices with EU expectations

In short, DORA isn't just another set of documents you need to provide — it's a strategic imperative.



Manual compliance burden

Achieving DORA compliance without automation is **resource-intensive**. On average, companies may spend:

200+ hours

for business
impact analysis

150+ hours

on vendor assessments

120+ hours

preparing incident
reporting mechanisms

100+ hours

setting up continuity and
disaster recovery policies

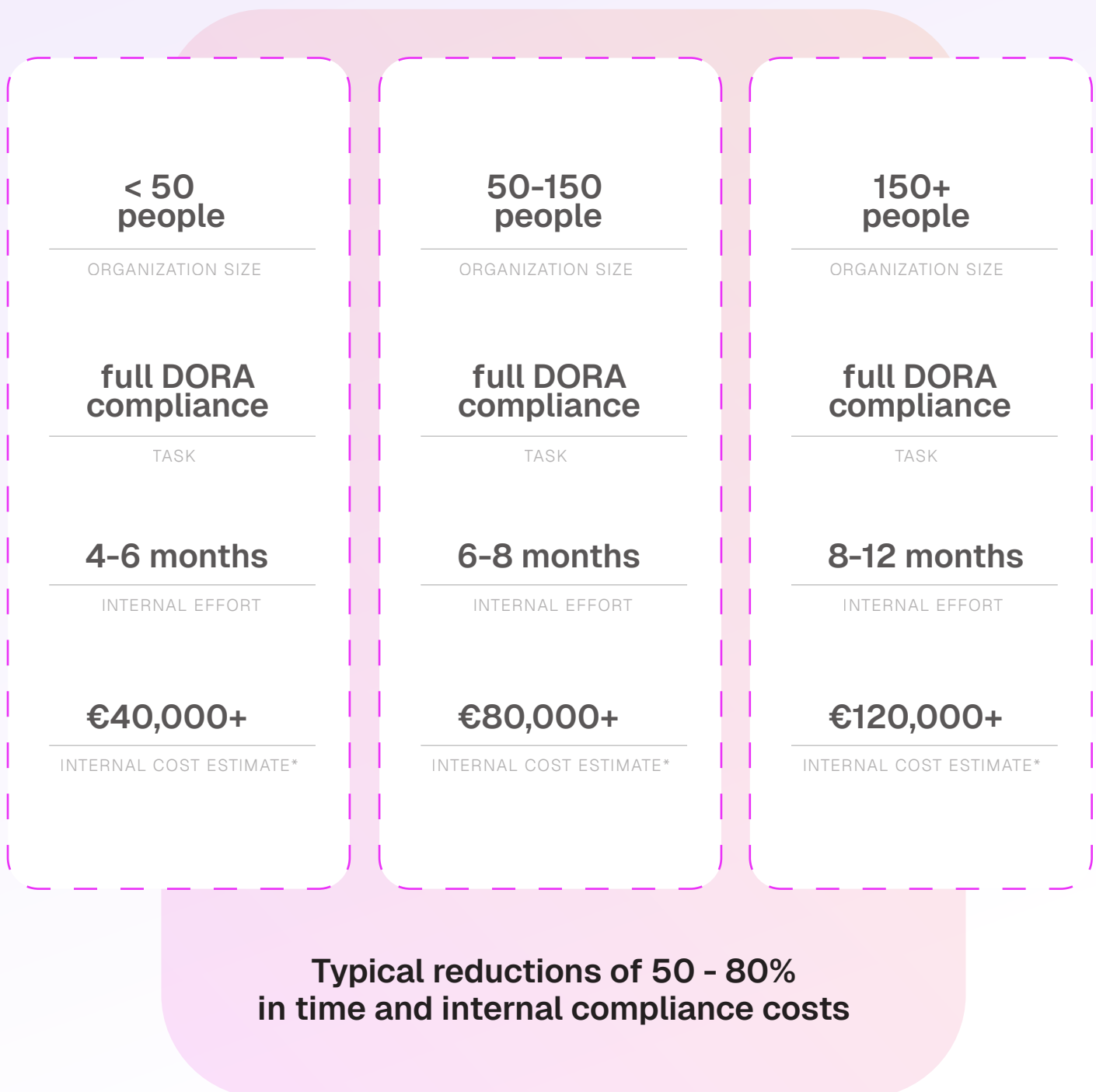


This **excludes** actual **testing, training, and audit** preparations. For many teams, compliance becomes a full-time job.

Time and cost of achieving compliance

Depending on your company size and approach, getting to DORA compliance readiness can range from a few months to an entire year.

Below is a general phased approach:



*INTERNAL COST BASED ON AVERAGE €7K/MONTH FTE. MAY VARY BASED ON INTERNAL AVAILABILITY, SCOPE, AND MATURITY.

Based on our experience with clients like FMPay, internal DORA compliance programs can cost over €120,000—especially when accounting for full-time CISO involvement and cross-departmental time.

Copla helps reduce that by up to 50%,
without compromising audit-readiness or control coverage.



Case study

“Ensuring compliance with DORA would have required significant internal resources, but by leveraging Copla expertise, we streamlined the process while **saving over €60K**. Copla’s CISO-as-a-Service not only reduced our compliance burden but also strengthened our cybersecurity posture, allowing us to focus on scaling our business across Europe.”

Roman Loban, Managing Director @FMpay



Detailed breakdown of DORA time investment (without Copla)

The hours your team would typically spend to independently plan, implement, and document each requirement.

ICT Risk Management (Articles 5–14):

250–400 hours

Establish risk management framework (Article 6)	60–90 hours
Asset classification (Article 8)	30–40 hours
Implement technical controls (Article 9)	60–80 hours
Threat monitoring and detection (Article 10)	40–60 hours
Business continuity and disaster recovery (Article 11)	80–100 hours
Post-incident review (Article 13)	20–30 hours per incident

ICT Incident Reporting (Articles 17–20):

80–120 hours

Incident classification and severity (Article 17)	30–40 hours
Reporting preparation and templates (Article 19)	50–80 hours

Digital Operational Resilience Testing (Articles 21–24):

100–150 hours

Vulnerability scanning and reporting	40–60 hours
Penetration testing preparation and response	50–80 hours

ICT Third-Party Risk Management (Articles 25–28):

200–300 hours

Governance and oversight (Article 25)	50–70 hours
Pre-contract due diligence (Article 26)	40–60 hours
Contractual clauses and legal work (Articles 27 and 28(4)–(6))	60–100 hours
Ongoing monitoring and register of information (Articles 28(1)–(3))	60–80 hours

Breakdown of **DORA** requirements and how we help

This explainer begins with Article 5, where the actionable compliance requirements under DORA start. Articles 1–4 cover regulatory background — including the **regulation’s scope, legal definitions, and other principles.**

DORA breaks down into several core domains:



01

ICT Risk Management (Articles 5–14)

DORA requires financial entities to formalize ICT governance and implement capabilities to detect, prevent, and recover from digital disruptions. This includes risk management frameworks, technical controls, business continuity planning, and incident response.

Copla supports this area by:

- ✓ Designing ICT risk frameworks tailored to governance structures
- ✓ Facilitating asset identification and classification
- ✓ Providing control templates for access, encryption, and MFA
- ✓ Defining monitoring baselines and threat detection strategies
- ✓ Delivering editable business continuity and disaster recovery plans
- ✓ Supporting post-incident documentation and review workflows

02

ICT-Related Incident Reporting (Articles 17–20)

Companies must classify incidents, notify regulators within 4 hours, and follow structured reporting processes. Documentation, clarity, and repeatability are critical.

Copla enables teams to:

- ✓ Build decision trees for classifying ICT incidents
- ✓ Prepare notification templates for initial and follow-up reporting
- ✓ Automate workflows to assign roles and pre-fill forms during crises

03

Digital Operational Resilience Testing (Articles 21–24)

Resilience must be tested regularly using proportionate methods such as vulnerability scanning, penetration testing, and (in some cases) threat-led red teaming.

With Copla, clients can:

- ✓ Run quarterly vulnerability scans & phishing simulations
- ✓ Receive prioritized technical reports and audit-ready summaries
- ✓ Conduct tailored penetration tests to meet supervisory expectations
- ✓ Bundle testing services with scenario planning and remediation tracking

04

Third-Party Risk and Vendor Governance (Articles 25–28)

Managing ICT third parties requires documented governance, risk-based onboarding, mandatory contract clauses, continuous oversight, and a full Register of Information.

Copla supports this end-to-end by:



Developing third-party risk policies aligned with ICT frameworks



Maintaining a dynamic, regulator-ready Register of Information



Coordinating due diligence and contract reviews



Designing vendor exit strategies integrated into continuity plans



Offering pre-approved legal clause templates

Why to use an automated compliance tool

Using a compliance partner like Copla streamlines the process:



- ✓ Provides document templates and fast customization
- ✓ Offers advisory support on controls, tools, and best practices
- ✓ Designs vendor scenarios and continuity planning
- ✓ Delivers pre-audit support, evidence collection, and remediation

“Copla has a model that every company should consider when dealing with DORA compliance. They act as an extension of our team, allowing us to focus on what we do best. Trusting them with our compliance processes has helped us optimize resources, delivering both cost savings and efficiency.”

Audrius Dumbliauskas, Product Manager @ HeavyFinance



Assess Your DORA Readiness

Not sure where your organization stands with DORA compliance?
Utilize Copla's **free**, user-friendly DORA Self-Assessment tool
to evaluate your operational resilience and identify areas for improvement.

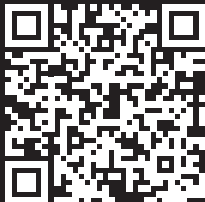
Choose between:

01 Fast Track

A quick 5-minute
overview for a high-
level snapshot

02 Full Scope

An in-depth 25-minute
assessment for
comprehensive insights



No prior DORA knowledge is required. Upon completion, receive
a detailed report highlighting your strengths and areas needing
attention. **Scan to find out more and begin your assessment.**

Not available on mobile. For the best experience, please use
your desktop to complete the DORA Self Assessment.



Resources and Next Steps

Copla offers a complete DORA com-
pliance pack, including:



Mapped requirements
with solution guidance



Vendor management
and testing frameworks



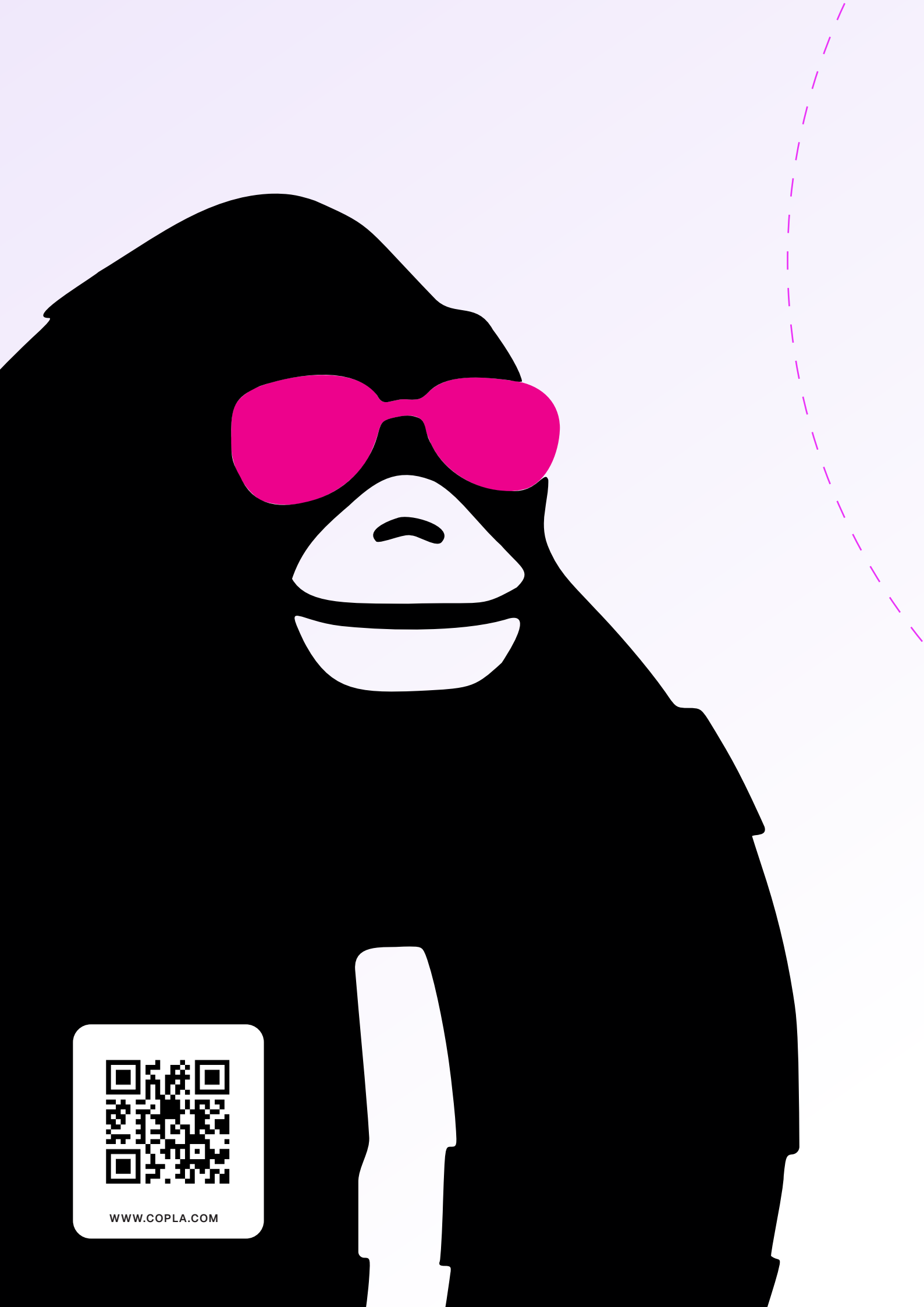
Document templates and
implementation checklists



Pre-audit reviews
and reporting support



Visit our website to explore the DORA Resource Hub, where you'll
find webinars, eBooks, case studies, and infographics.



WWW.COPLA.COM