PENTESTERRA

DORA GAP ASSESSMENT

Is Your Digital Operational Resilience Actually Tested?

Gap assessment across 26 DORA controls spanning the 5 pillars - ICT risk management, incident management, digital operational resilience testing, ICT third-party risk - for EU financial entities.

IN SHORT

Covers DORA's 5 pillars: ICT risk management (Art. 5-16), ICT-incident management and reporting (Art. 17-23), digital operational resilience testing (Art. 24-27), ICT third-party risk (Art. 28-30), and information-sharing (Art. 45).

26
DORA controls covered across 5 pillars

Art. 24-27
Digital operational resilience testing

EU-Wide
Financial entities and critical ICT providers

THE SITUATION TODAY

WHO YOU ARE

You're the CISO or ICT risk lead of an EU financial entity - a bank, insurer, fund manager, or payment services provider - subject to DORA since January 2025.

WHAT HAPPENED

Your insurer, an institutional client, or the supervisory authority asks for evidence of the digital operational resilience testing required under Art. 24-27.

WHY IT HURTS

DORA requires periodic, documented resilience testing. An entity that cannot demonstrate it risks sanctions and, more concretely, the trust of partners and supervisors.

WHERE YOU WANT TO GET TO

DESIRED OUTCOME

You want to know, control by control, what's satisfied, what's partial, and what's missing - with real technical evidence attached to every answer, not an optimistic claim nobody has verified.

THE SOLUTION

Pentesterra's DORA Gap Assessment: a structured assessment across every control, with technical controls auto-filled from vulnerability scanning, penetration testing, OSINT and External Exposure monitoring wherever evidence exists.

WHY IT'S DIFFERENT

You're not buying another self-assessment questionnaire, and this isn't a legal opinion. You're working with [YOUR COMPANY NAME] - a certified provider with a long track record in information security. You've likely worked with us already, directly or through someone you know - a colleague, a supplier, a competitor. And the gap assessment doesn't stop at a paper checklist: technical controls are auto-filled from evidence already on file, with cross-standard mapping to the other 12 frameworks the platform supports, so a second audit never starts from zero.

CONCRETE PROOF

The result is a complete, ready-to-deliver PDF report covering every control, with a direct reference to the legal/regulatory basis. If gaps come up, we propose the additional services to close them: vulnerability assessment, network or application penetration testing, phishing training and simulation.

WHAT'S ACTUALLY INCLUDED

Not a generic checklist - the real controls of DORA, grouped the way you'll see them in the platform.

Pillar 1: ICT risk management (Art. 5-16)

The governance and ICT risk-management framework the management body must own.

- Management body accountability for ICT risk
- Identification, protection and prevention
- Detection, response and recovery

Pillar 2: ICT incident management (Art. 17-23)

Classification and reporting of major ICT-related incidents.

- Incident classification process
- Reporting to competent authorities
- Post-incident review and lessons learned

Pillar 3: Digital operational resilience testing (Art. 24-27)

The pillar where Pentesterra offers the most direct technical evidence.

- Risk-based testing programme
- Threat-led penetration testing (TLPT)
- Remediation of findings and retesting

Pillar 4-5: ICT third-party risk and sharing (Art. 28-30, 45)

The ICT supply-chain risk.

- Register of critical ICT third-party providers
- Mandatory contractual provisions
- Cyber threat information-sharing

PENTESTERRA

DORA GAP ASSESSMENT

WHAT YOU GET

- ✓ An exportable XLSX control matrix, with the status of every individual control
- ✓ An editable DOCX gap report, ready for your auditor or your board
- ✓ Technical controls auto-filled from evidence the platform already collected
- ✓ Guided applicability check by sector, country, and company size
- ✓ Cross-standard mapping to the other 12 frameworks the platform supports - answer once, reuse across standards
- ✓ A one-click auditor package: questionnaire, technical evidence and gap report together
- ✓ Prioritized remediation recommendations for the gaps found

HOW IT WORKS

1

We define the scope

Assessment boundary, systems and processes involved - we set the scope together.

2

We collect the evidence

Technical controls are auto-filled from evidence the platform already collected.

3

We complete the questionnaire

Non-technical controls are verified with your team.

4

We deliver the report

A complete PDF with the gaps found and the actions to take.

Find out how ready you are for DORA

A complete report, ready to present to clients, auditors, or your board.

Request your DORA Gap Assessment →

info@pentesterra.com · pentesterra.com/solutions/compliance