

COMPLIANCE GUIDE

DORA & NIS2 Testing Readiness

Two EU regimes — DORA for financial entities and NIS2 for essential and important entities — raise the bar on security testing. This is a plain-language primer on how they affect your testing, and how to prepare. It is guidance, not legal advice.

DORA (Digital Operational Resilience Act)

DORA applies to financial entities in the EU and their critical ICT providers. Alongside broad resilience requirements, it expects regular testing of ICT systems — and, for significant entities, advanced **threat-led penetration testing (TLPT)** aligned to the TIBER-EU framework.

- Maintain a testing programme covering your important ICT systems.
- Significant entities: periodic intelligence-led red teaming against live systems.
- Involve threat intelligence, control the risk, and document everything.

NIS2 (Network & Information Security Directive)

NIS2 widens the scope of EU cybersecurity rules to many more “essential” and “important” entities. It requires risk-management measures and the means to assess their effectiveness — which in practice means regular vulnerability assessment and penetration testing.

- Adopt risk-management measures appropriate to your exposure.
- Test and evaluate the effectiveness of those measures.
- Be ready to demonstrate this to regulators.

How to prepare

- ✓ Map which regime(s) apply to you, and to which systems.
- ✓ Establish a recurring testing cadence, not a one-off.
- ✓ For DORA TLPT, plan intelligence-led red teaming with careful risk controls.
- ✓ Keep testing reports and retest letters as evidence.
- ✓ Work with testers who can map findings to the specific obligations.

PXL Security delivers the penetration testing and threat-led red teaming these regimes call for, with audit-ready reporting. Talk to us at hello@pxlsec.com or pxlsec.com/services/compliance-penetration-testing. This document is informational and not legal advice.