

WHITEPAPER · OCTOBER 2026

Threat-Led Penetration Testing under DORA

A practical guide for financial entities preparing
for TLPT under DORA, TIBER-EU and Regulation (EU) 2025/1190

EXECUTIVE SUMMARY

TLPT in one page

The Digital Operational Resilience Act (DORA) has applied since 17 January 2025. For the financial entities most important to the system, it requires **threat-led penetration testing (TLPT)** at least every three years: a covert, intelligence-led red team attack on the live production systems that support critical or important functions.

The detailed rules sit in **Commission Delegated Regulation (EU) 2025/1190**, the regulatory technical standards (RTS) on TLPT, adopted on 13 February 2025 and in force since 8 July 2025. They follow the TIBER-EU framework, which the Eurosystem updated on 11 February 2025 to align with DORA.

What this means in practice:

- Your TLPT authority decides whether you must test, using criteria in Article 2 of the RTS.
- Once notified, you have **3 months** to submit initiation information and **6 months** to submit a scope specification approved by your management body.
- The active red team phase lasts **at least 12 weeks** on live production systems, without the blue team knowing.
- Closure is tightly timed: red team report within 4 weeks, blue team report, replay and mandatory purple teaming within 10 weeks.
- Threat intelligence providers and testers must meet minimum experience, reference and insurance requirements (DORA Article 27, RTS Article 7).
- A remediation plan and the TLPT authority's attestation close the cycle. The attestation supports mutual recognition across EU authorities.

Bottom line: a DORA TLPT is a regulated programme, not a one-off test. Most of the risk to your timeline sits in preparation and procurement, so the earlier you start, the smoother the test.

1. THE BASICS

What threat-led penetration testing is

DORA defines TLPT as a framework that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat. It delivers a controlled, bespoke, intelligence-led red team test of the financial entity's critical live production systems.

The difference from a standard penetration test is purpose. A penetration test finds as many vulnerabilities as possible in a defined scope. A TLPT asks whether a realistic attacker could compromise your critical or important functions, and whether your people, processes and technology would detect and stop them.

	Penetration test	Threat-led penetration test (TLPT)
Goal	Find vulnerabilities in a defined system	Test resilience of critical or important functions against a realistic attacker
Scope	One application, network or cloud environment	People, processes and technology behind one or more critical functions
Basis	Checklists and testing methodologies	Targeted threat intelligence about actors likely to attack you
Environment	Often test or staging	Live production systems
Blue team aware?	Usually yes	No, only the control team knows
Duration	Days to weeks	Months, with at least 12 weeks of active red teaming
Oversight	Internal	TLPT authority, test managers and attestation

Source: DORA Article 3(17) and Article 26; RTS Article 11(5).

2. SCOPE

Who must perform TLPT

Under DORA Article 26, competent authorities identify the financial entities required to perform TLPT, based on their impact, financial stability concerns and ICT risk profile. Microenterprises and entities under the simplified ICT risk management framework (Article 16) are excluded. Authorities can also raise or lower the three-year frequency.

Article 2 of the RTS gives two sets of criteria for that assessment:

Impact and systemic factors	ICT risk factors
Size, interconnectedness, importance of services, substitutability, complexity of the business model, membership of a systemically important group sharing ICT systems	Risk profile and threat landscape, ICT dependence of critical functions, complexity of ICT architecture, reliance on ICT third-party providers, supervisory findings, maturity of business continuity and of detection and response

Entities presumed to be in scope

Unless the assessment shows otherwise, the RTS presumes the following entities must perform TLPT:

- Credit institutions identified as G-SIIs or O-SIIs, or part of such groups.
- Payment institutions with payment transactions above EUR 150 billion in each of the two preceding years.
- Electronic money institutions above EUR 150 billion in payment transactions or EUR 40 billion in outstanding e-money in each of the two preceding years.
- Central securities depositories and central counterparties.
- Trading venues with the largest national market share, or above 5% of EU turnover, in specified instrument categories.
- Insurance and reinsurance undertakings above defined premium, technical provision and asset thresholds.

Not designated? Many firms run voluntary TLPT-style red team exercises to raise detection maturity, prepare for possible future designation and reassure boards and clients.

Source: DORA Article 26(1) and (8); RTS Article 2. Thresholds summarised; check the Official Journal text for exact definitions.

3. THE FRAMEWORKS

DORA, TIBER-EU and national programmes

Framework	What it is	Status
DORA (EU) 2022/2554	EU regulation on digital operational resilience. Articles 26 and 27 set the TLPT obligation and tester requirements.	Applies since 17 January 2025
RTS on TLPT (EU) 2025/1190	Detailed methodology: identification, phases, deadlines, roles, provider requirements, internal testers, remediation, mutual recognition.	Adopted 13 Feb 2025; in force 8 Jul 2025
TIBER-EU	Eurosystem framework for threat intelligence-based ethical red teaming, on which the RTS is based.	Updated 11 Feb 2025 to align with DORA: mandatory purple teaming, "white team" renamed "control team"
National TIBER (e.g. TIBER-IE)	National implementations run by central banks, now covering DORA-mandated TLPT in many Member States.	E.g. the Central Bank of Ireland is the designated TIBER and DORA TLPT authority in Ireland
CBEST and STAR-FS (UK)	Intelligence-led testing frameworks for UK financial services (Bank of England, PRA, FCA; STAR-FS developed with CREST).	Outside DORA; relevant to groups operating in both the EU and UK

For cross-border groups, the attestation issued at the end of a TLPT supports mutual recognition between competent authorities, so one well-run test can serve several jurisdictions where the scope allows.

Sources: ECB, Eurosystem updates TIBER-EU framework (11 Feb 2025); Central Bank of Ireland, TIBER-IE; CREST, STAR-FS launch; DORA Article 26(6)–(7).

4. WHO DOES WHAT

Roles in a DORA TLPT

Role	Responsibility
Management body	Approves the scope specification document and owns the risk of the test.
Control team and control team lead	A small group inside the entity that runs the TLPT in secret: procurement, scoping, risk management, leg-ups and day-to-day decisions. Formerly the TIBER "white team".
Test managers (TLPT authority)	Supervisory staff who validate initiation information, approve the scope, the threat intelligence report and the red team test plan, and oversee the test.
Threat intelligence provider	External provider that produces the targeted threat intelligence report and attack scenarios. Must be external even when internal testers are used.
Testers (red team)	Plan and execute the attack scenarios on live production systems and write the red team test report.
Blue team	The entity's defenders (SOC, incident response, IT). Not informed during the active phase; writes the blue team test report afterwards.
ICT third-party providers	Must participate where their services are in scope. Pooled testing is possible in defined cases.

Sources: RTS Articles 9–13; DORA Articles 26(4) and 27(2).

5. THE LIFECYCLE

Phases and deadlines

The RTS sets hard deadlines, counted from the TLPT authority's notification or from the end of the active red team phase. Planning backwards from these dates is the single most useful thing a control team can do.

Phase	Key steps and deliverables	Deadline (RTS)
Preparation	Initiation information: project charter, control team lead, use of internal or external testers, communication channels, code name	Within 3 months of notification (Art. 9(2))
	Control team set-up; procurement of threat intelligence provider and testers; risk assessment	Before testing begins (Art. 9)
	Scope specification document, approved by the management body	Within 6 months of notification (Art. 9(6))
Testing: threat intelligence	Targeted threat intelligence report and scenarios; at least three scenarios selected	Approved by TLPT authority (Art. 10)
Testing: red team	Red team test plan approved by control team and TLPT authority; active red team testing on live production; weekly progress reporting; leg-ups as planned	At least 12 weeks of active testing (Art. 11(5))
Closure	Red team test report	Within 4 weeks of end of active phase (Art. 12(2))
	Blue team test report; replay; purple teaming exercise	Within 10 weeks of end of active phase (Art. 12(4)–(5))
	Test summary report	Within 8 weeks of authority notification (Art. 12(7))
Remediation and attestation	Remediation plans per finding; documentation to the authority; attestation issued	Within 8 weeks (Art. 13(1)); DORA Art. 26(7)

Recital 18 of the RTS indicates the threat intelligence phase typically takes around four weeks; this is guidance, not a legal deadline.

6. PROCUREMENT

Choosing threat intelligence providers and testers

DORA Article 27 requires testers of the highest suitability and reputability, with proven technical and organisational capabilities in threat intelligence, penetration testing and red teaming. They must be certified by an accreditation body in a Member State or follow formal codes of conduct or ethical frameworks, provide independent assurance on how they manage TLPT risks, and hold professional indemnity insurance covering misconduct and negligence.

Article 7 of the RTS adds minimum team requirements:

Requirement	Threat intelligence provider	External red team testers
Lead	5+ years in threat intelligence	5+ years in penetration testing and red teaming
Team	At least 1 more member with 2+ years	At least 2 more testers with 2+ years each
References	At least 3 from previous assignments	At least 5 from previous assignments
Evidence	CVs, recognised certifications, insurance	CVs, recognised certifications, insurance
Independence	No blue team or conflicting services for the entity	Separated from TI staff of the same provider

Internal testers

Internal testers are allowed only with the authority's approval, sufficient dedicated resources, no conflicts of interest and an external threat intelligence provider. Entities using internal testers must contract external testers every third test. Significant credit institutions supervised by the ECB must use external testers only.

Sources: DORA Articles 26(8) and 27; RTS Articles 7 and 9. In exceptional circumstances the RTS allows deviation from Article 7(1) with documented risk-mitigating measures.

7. CONTROLLING RISK

Testing live production safely

TLPT is performed on live systems, so the RTS requires the control team to assess and keep reviewing the risks of the test. Article 5 names six areas the assessment must cover at a minimum:

- Giving the threat intelligence provider and external testers access to sensitive information.
- Non-compliance with DORA or the RTS that could prevent attestation, including confidentiality breaches or unethical conduct.
- Crisis and incident escalation.
- The active red team phase, including interruption of critical activities and data corruption.
- Blue team activity, including possible effects on third parties.
- Incomplete restoration of systems affected by the test.

Practical safeguards include agreed rules of engagement, pre-approved **leg-ups** that let the red team continue when a step would take too long in a real attack, a clear escalation route if the test is detected, and the control team lead's power to suspend the test. In exceptional cases, and with prior validation by the authority, testing can continue as a limited purple teaming exercise.

Sources: RTS Articles 5 and 11(8)–(10).

8. GETTING READY

A preparation checklist

From experience of red team engagements, these are the steps that most often decide whether a TLPT runs on time:

Before notification

- ☐ Map your critical or important functions and the ICT systems, people and third parties behind them.
- ☐ Identify a control team lead with authority and time, and a small, discreet control team.
- ☐ Check your ICT third-party contracts allow participation in TLPT.
- ☐ Brief the management body: it must approve the scope.

First 3 months

- ☐ Prepare the project charter and initiation information.
- ☐ Start procurement early; ask providers for CVs, certifications, references and insurance evidence against RTS Article 7.
- ☐ Agree secure communication channels and a code name.

Months 3–6

- ☐ Draft the scope specification with flags (objectives) for each critical function.
- ☐ Complete the TLPT risk assessment and agree rules of engagement and leg-ups.
- ☐ Plan blue team availability for the closure phase without revealing the test.

After testing

- ☐ Book the replay and purple teaming within 10 weeks.
- ☐ Assign owners and dates to each remediation measure, with root causes.
- ☐ Feed lessons into detection engineering and your next resilience testing cycle.

9. LESSONS FROM THE FIELD

Common pitfalls

Pitfall	How to avoid it
Starting procurement after notification	Shortlist qualified providers in advance; the 3- and 6-month deadlines leave little slack.
A scope that is too broad or too vague	Tie each flag to a specific critical function and realistic attacker objective.
Leaks that end secrecy	Keep the control team small, use code names and plan cover stories for unusual activity.
Third parties not prepared	Agree participation, contacts and escalation routes with ICT providers before testing.
Treating the report as the finish line	The value lies in the replay, purple teaming and remediation; plan time and budget for them.
Underestimating the blue team effort	The blue team report and replay need people and logs; protect their time after the active phase.

10. HOW WE HELP

PenTest Hub and TLPT

PenTest Hub is a specialist offensive security company founded in 2017. We deliver penetration testing, red teaming, AI/ML red teaming and threat-led penetration testing for organisations across Europe and worldwide. Our consultants individually hold certifications including CREST, OSCP+, PNPT, CARTE and AI red teaming certifications.

- **Red team testing for DORA TLPT, TIBER-EU and national TIBER programmes**, working alongside your chosen threat intelligence provider and control team.
- **TLPT readiness**: TLPT-style red team and assumed-breach exercises that build blue team maturity before a mandated test.
- **Purple teaming and replay support** that turns findings into improved detection and response.
- **Complementary testing** of applications, networks, cloud environments and AI systems in scope of your critical functions.

Talk to a senior tester about your TLPT timeline, scope or readiness.
pentest-hub.com/tlpt-dora-tiber-eu · info@pentest-hub.com

Sources

- Regulation (EU) 2022/2554 (DORA), Articles 3, 26 and 27, Official Journal L 333, 27.12.2022.
- Commission Delegated Regulation (EU) 2025/1190 on threat-led penetration testing, eur-lex.europa.eu/eli/reg_del/2025/1190/oj.
- European Central Bank, "Eurosysteem updates TIBER-EU framework to align with DORA", 11 February 2025.
- Central Bank of Ireland, Threat Intelligence-based Ethical Red Teaming (TIBER-IE).
- CREST, "Launch of STAR-FS brings greater resilience to financial services sector".
- Bank of England, CBEST threat intelligence-led assessments.

Disclaimer. This guide summarises public regulatory texts as of October 2026 for general information. It is not legal advice. Always refer to the authentic texts published in the Official Journal of the European Union and to guidance from your competent or TLPT authority.