

TLPT

Threat-led penetration testing is the advanced red team test that DORA makes mandatory for designated financial entities. Here is what it is, who it covers and how to get ready.

WHAT IT IS

TLPT, or threat-led penetration testing, uses real threat intelligence to mimic how genuine attackers would target your organisation, then has an external red team run that attack covertly against your live systems. Under DORA it is a legal duty for designated financial entities, run at least every three years to prove their defences hold.

WHY IT MATTERS

~1 in 5

of all reported cyber incidents in two decades have hit the financial sector

IMF, April 2024

\$12 billion

in direct losses to financial firms from cyber incidents since 2004

IMF, April 2024

4x+

growth in extreme financial-sector cyber losses since 2017, to at least \$2.5 billion

IMF, April 2024

WHAT HAPPENED

In February 2016 attackers linked by the US government to North Korea's Lazarus Group reached Bangladesh Bank's payment environment and sent fraudulent SWIFT instructions for roughly \$951 million. They moved \$81 million out before a misspelled order and a routine review at the New York Fed stopped the rest. Most of the \$81 million was never recovered, and a threat-led test is built to catch exactly this kind of quiet access to a critical function.

RED FLAGS TO WATCH FOR

You may be behind on TLPT if any of these are true.

- You rely on annual penetration tests alone
- You have never mapped your critical or important functions
- You have no external threat intelligence provider or red team lined up
- Your detection and response have never been tested by a live adversary
- You assume outsourcing the systems moves the duty to your provider

THE ONE RULE THAT STOPS IT

Map your critical or important functions and fix detection and response now, before your authority ever notifies you.

THEN BUILD THE HABIT AROUND IT

- Keep baseline vulnerability assessments and annual penetration tests current (DORA Articles 24 to 25)

- Procure a compliant external threat intelligence provider and red team early
- Budget for a 12-week active phase plus closure and remediation
- Use the purple-teaming replay to train your blue team

MYTHS AND FACTS

MYTH

TLPT is just a bigger penetration test.

FACT

It is an intelligence-led red team exercise against your live critical functions, run covertly and overseen by a regulator.

MYTH

Every financial firm has to run TLPT.

FACT

Only entities a competent authority designates must run it, and microenterprises are excluded. All in-scope firms still owe baseline testing.

MYTH

TLPT is pass or fail.

FACT

It is not scored pass or fail. The point is to find the gaps a real attacker would use, then close them.

THE LEGAL DUTY

Under DORA (Regulation (EU) 2022/2554), Articles 26 and 27, designated financial entities must run TLPT at least every three years on live systems. The detailed rules sit in Commission Delegated Regulation (EU) 2025/1190, in force since 8 July 2025. In Sweden this runs through TIBER-SE, coordinated by Sveriges Riksbank.

GET HELP

**Preparing for a DORA TLPT, or need the baseline penetration testing that comes first?
eBuilder Security can help you get ready.**

[Read the Full Article →](#)