THREAT-LED PENETRATION TESTING (TLPT) UNDER DORA: WHAT FINANCIAL INSTITUTIONS NEED TO KNOW

CREST

Contents

Introduction

Financial institutions across the EU are facing new cyber security mandates under the Digital Operational Resilience Act (DORA). One key requirement is to conduct Threat-Led Penetration Testing (TLPT) – essentially, advanced Red Team exercises that simulate real cyberattacks on live systems. In this whitepaper, we'll break down what TLPT entails as mandated by DORA, how it fits into broader operational resilience, why using accredited service providers (especially CREST-accredited firms) is so important, and the benefits of doing so. We'll also compare CREST with other well-known certifications like OSCP and GIAC and highlight the risks of choosing unaccredited or unvetted testing providers. The goal is to provide clarity for cyber security managers, CISOs, and procurement leads on navigating TLPT in a compliant and effective manner.

What is TLPT and Why DORA Mandates It

Threat-Led Penetration Testing (TLPT) is an intelligence-driven form of penetration testing – essentially a controlled cyber "red team" attack designed to mimic the tactics and techniques of real threat actors. Unlike a regular vulnerability scan or traditional pentest, a TLPT is a full-scale stealth attack simulation on an organisation's critical live systems, conducted without the defenders knowing it's a test. This approach provides an authentic measure of the institution's ability to detect, respond to, and recover from a sophisticated attack in real time. TLPT exercises are bespoke to each institution's threat profile, guided by threat intelligence about adversaries that would realistically target them. Financial entities identified as significant (e.g. major banks, payment providers above certain size thresholds) must conduct a TLPT at least every three years – or more often if the regulator deems necessary. This ensures that no institution goes too long without a rigorous check of its cyber defenses. DORA's Article 26 defines TLPT as the pinnacle of operational resilience testing, and Article 27 lays out strict criteria for who can perform these tests, emphasising that the testing must be carried out by highly qualified, reputable professionals.

In the broader operational resilience context, TLPT is one component of DORA's comprehensive requirements. DORA covers everything from risk management processes and incident reporting to oversight of third-party ICT providers. Regular penetration testing and vulnerability assessments are expected of all in-scope firms, but TLPT is reserved for the largest or most systemically important institutions with mature cyber defences. Think of TLPT as the "advanced level" test of an organisation's cyber resilience – DORA essentially forces critical financial entities to prove their cyber resilience in a real-world scenario, not just on paper. By doing so, regulators aim to identify weaknesses before real attackers do, and to promote continuous improvement in defences. The inclusion of TLPT in DORA underscores how vital it is for the financial sector to be prepared for sophisticated cyber threats as part of overall operational continuity.

TLPT: A High-Stakes Cyber Resilience Exercise

To put TLPT in perspective, it helps to understand what such a test looks like in practice. A TLPT engagement usually involves two specialised teams from a provider: a Threat Intelligence team (to study relevant threat actors and craft realistic attack scenarios) and a Red Team (to execute the simulated attack). The test spans multiple phases – from initial reconnaissance and scenario planning to active exploitation and, finally, a closure phase that includes debrief and remediation. Notably, DORA's TLPT standards even mandate a "purple teaming" element in the closure phase, meaning the attacking Red Team and the institution's defending Blue Team come together after the simulation to share insights and improve detection capabilities

Because TLPT exercises run on live production systems, they carry inherent risk. During the test, Red Team operators attempt to bypass security controls, pivot through networks, and achieve predefined objectives (for example, accessing crown-jewel data or performing fraudulent transactions) – all without causing unintended disruption. The risks of a poorly executed TLPT are real: there's a possibility of causing outages, corrupting data, or inadvertently exposing sensitive information if the test isn't carefully controlled. For this reason, both DORA and frameworks like TIBER-EU put a strong emphasis on risk management and tester qualifications. As the ECB notes in the TIBER-EU guidance, testing on critical live systems must be handled by the most competent, qualified, and trusted professionals, with robust risk controls in place always.

Threat-led penetration tests simulate real cyberattacks on an institution's live systems, revealing how well its defences hold up. These "ethical hackers" operate covertly during a TLPT, mimicking advanced threat actors to test detection and response capabilities under fire. The exercise is intelligence-led and carefully scoped to ensure a controlled, yet realistic, challenge to the organisation's resilience. In summary, TLPT is a double-edged sword: incredibly valuable for uncovering gaps and improving cyber resilience, but only if conducted in a safe and professional manner. That's why DORA doesn't just mandate that you do a TLPT – it effectively mandates that you do it right, with the right people.

Why You Should Use Accredited Service Providers for TLPT

Given the high stakes of TLPT, DORA explicitly requires financial entities to engage suitable and accredited testers for these exercises. In fact, Article 27 of DORA stipulates that those institutions "shall only use testers" that meet strict criteria, including: having the highest suitability and reputability, possessing proven technical and organisational capabilities in threat intelligence and Red Team testing, and being certified by an accreditation body or adhering to formal codes of conduct. Testers must also provide assurance of sound risk management and carry professional indemnity insurance. In plain terms, this means you can't just hire a random self-proclaimed hacker for a TLPT – you need to choose a provider that is recognised and vetted by industry or authorities for their quality and integrity.

Using accredited providers offers trust and assurance, as their personnel, processes, and methodologies are independently validated by a recognised body or standard. This assures you (and your regulators) that the provider follows industry best practices for conducting such sensitive tests. For example, an accredited firm will have strict protocols for handling your confidential data, a well-defined testing methodology, experienced staff with certified skills, and adherence to a code of ethics. DORA's emphasis on accreditation is about reducing the risk that something will go wrong in the test,
and ensuring the results can be trusted. As one industry analysis put it, without recognised standards and professional oversight, critical vulnerabilities could easily be overlooked or mishandled by unqualified testers.

By choosing an accredited provider, you gain confidence that the test will be carried out safely, thoroughly, and with proper accountability.

Another angle to consider is that regulators and stakeholders will expect the TLPT to be performed by a reputable firm. In many EU jurisdictions, financial regulators maintain lists of approved testing providers or explicitly require certain accreditations. Using an accredited firm thus helps with regulatory compliance. It demonstrates to regulators that you took due care in vendor selection, as the firm meets formal criteria of competence. In fact, some sectors (like parts of the public sector and banking industry) already require CREST-accredited suppliers or similar for any penetration testing engagements. DORA is creating a similar expectation across the EU financial sector.

In short, engaging an accredited service provider is not just a best practice – it's fast becoming a regulatory must for TLPT. It's the concrete way to meet DORA's tester requirements around suitability, expertise, and ethical conduct.

The Benefits of Using CREST-Accredited Companies for TLPT

When it comes to accreditation in the penetration testing and red teaming world, CREST is one of the most respected names. CREST is an international non-profit accreditation body that certifies cyber security firms and professionals to rigorous standards. Many financial institutions choose CREST-accredited providers for conducting TLPTs, and for good reason. Here are some specific benefits of using a CREST-accredited company for your DORA TLPT engagement:

- Proven Expertise and Skill: CREST requires that member companies employ highly skilled testers who have passed rigorous exams and logged thousands of hours of relevant experience. Individuals must progress through tough certification tiers (practitioner, registered, certified) by demonstrating hands-on proficiency and knowledge of the latest threats. This means a CREST-accredited Red Team is staffed by experts who know what they're doing – exactly what you need for a high-calibre TLPT. In contrast, if you rely on providers without such credentialed staff, you risk the test being done by less-qualified personnel.

- Quality Methodology and Standards: A CREST accreditation is often seen as a "stamp of approval" for the provider's methodology and processes. CREST-assessed companies must demonstrate they follow industry best practices throughout the engagement lifecycle – from scoping and rules-of-engagement, to testing procedures, to reporting. Their internal processes (including data security and reporting quality) are reviewed to ensure consistency and thoroughness. For a TLPT, which can be complex and lengthy, having a structured, standardised approach is crucial. CREST firms will deliver the test in a controlled and safe manner, adhering to a code of conduct that aligns with ethical red teaming. This gives you confidence that the TLPT won't devolve into a chaotic or dangerous exercise.

- Professionalism and Ethics: By choosing a CREST company, you are engaging a team that is bound by CREST's code of ethics and professional conduct. Members are expected to perform work responsibly, confidentially, and with integrity. There's an inherent commitment to professional standards and ethical behaviour that comes with the accreditation. This is especially important for TLPT, where testers may obtain highly sensitive access during the simulation – you need to trust that they will handle information appropriately and not overstep agreed boundaries. CREST's oversight and disciplinary processes help enforce that trust.

The Benefits of Using CREST-Accredited Companies for TLPT Continued

- Recognition and Accountability: CREST is globally recognised, and its accreditation is respected by regulators and industry bodies. In the context of threat-led testing, CREST was instrumental in standards like CBEST (the Bank of England's framework) and works with many national authorities. A CREST-accredited provider likely has experience with regulatory programs and understands the compliance reporting aspects of TLPT. Using a CREST firm can thus give regulators assurance that your TLPT was conducted by a qualified professional. Moreover, should any issues arise, accredited firms are accountable to CREST – an extra layer of recourse beyond just your contract with the provider.

- Alignment with Threat Intelligence & Red Teaming Best Practices: Unlike general IT testing certifications, CREST offers specific programs for Intelligence-Led Penetration Testing (the CREST STAR scheme) and Threat Intelligence services. This means CREST-accredited providers are often uniquely equipped for exactly the kind of combined threat intel and Red Team engagement that TLPT requires. Their teams might include CREST-certified threat intelligence analysts as well as Red Team operators, ensuring both sides of the TLPT (intel gathering and attack execution) meet high standards. Certifications like OSCP or GIAC focus mainly on technical penetration skills of individuals, but CREST encompasses the full spectrum of a threat-led exercise, from scenario design to execution to analysis. This comprehensive scope sets CREST-accredited companies apart when it comes to delivering TLPTs.

In essence, a CREST-accredited company brings assurance of quality, methodology, and professionalism to a TLPT engagement. As one 2025 industry guide put it, opting for a CREST provider offers benefits ranging from highly trained experts to improved customer assurance, and even a competitive edge in meeting security expectations. Especially under the scrutiny of DORA, these benefits are invaluable.

CREST vs. Other Certifications (OSCP, GIAC): What Sets CREST Apart

It's worth distinguishing CREST accreditation from other well-known cyber security certifications like OSCP or GIAC. Many people in the industry have OSCP (Offensive Security Certified Professional) or various GIAC certifications (from the SANS Institute) – these are indeed respected individual qualifications. An OSCP holder, for example, has proven their ability to penetration test by completing a rigorous practical exam, and GIAC offers specialist certs (like GPEN for pen testing, or GCTI for threat intel) that indicate strong knowledge. However, these certifications alone do not equate to a provider being accredited or necessarily having the structured capabilities required for TLPT:

- Individual Cert vs Company Accreditation: OSCP/GIAC certify an individual's skill, whereas CREST accredits both individuals and the service provider organisation. Having team members with OSCP or GIAC is a plus, but when you hire a firm to do a TLPT, you need confidence in the firm's overall process, governance, and track record – not just one or two star employees. CREST accreditation addresses this by auditing the company's policies, data security, and quality assurance processes in delivering testing services. In contrast, two different OSCP-certified freelancers might conduct tests in completely different ways; the certification doesn't enforce a consistent standard or methodology across an engagement.

- Scope of Skills (Threat Intel and Red Teaming): OSCP is mainly focused on network/web penetration testing techniques and exploiting vulnerabilities. GIAC offers a wider range of certs (including some red teaming and threat intel ones), but each is siloed to a specific domain of knowledge. CREST, through its programs like CREST STAR (Simulated Targeted Attack & Response) and threat intelligence certifications, ensures that accredited providers can integrate threat intelligence with Red Team operations effectively. Essentially, CREST ties the pieces together – its accredited companies have demonstrated they can perform intelligence-led attacks (not just hack systems in a vacuum). This ability to simulate realistic threat actors (as required by TLPT) is a key differentiator. Someone who holds the OSCP might be excellent at finding vulnerabilities, but not necessarily experienced in crafting attack scenarios based on specific threat actors or working under covert Red Team conditions.

CREST vs. Other Certifications (OSCP, GIAC): What Sets CREST Apart - Continued

- Industry Recognition and Requirements: While OSCP and GIAC are well-recognised in the cyber security community, they are not typically named by regulators as required qualifications for performing regulated tests. CREST and similar bodies (like the UK's NCSC CHECK scheme, or other national accreditation programs) are often explicitly required or recommended by regulators for engagements like TLPT. For example, the European Central Bank and many national authorities encourage using frameworks aligned with CREST standards for threat-led tests. Thus, in the context of DORA compliance, citing that your TLPT provider is CREST-accredited likely carries more weight than saying "Our tester has the OSCP." The latter speaks to an individual's ability; the former speaks to the organisation's overall credibility.

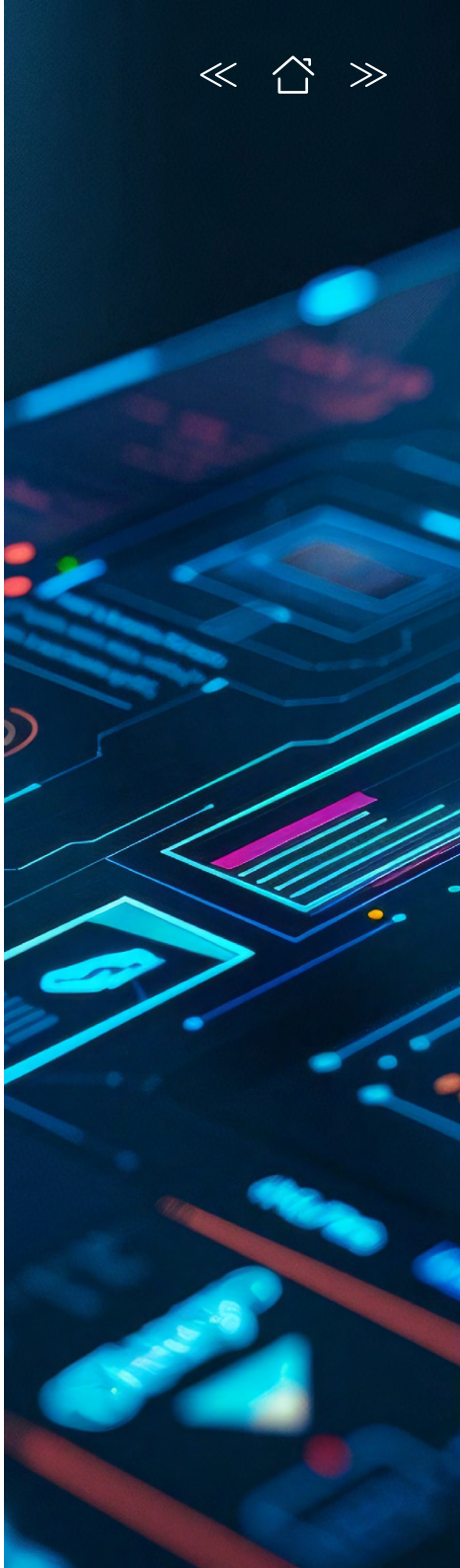
To be clear, OSCP, GIAC, and other certifications are great benchmarks for technical talent – and you'll often find CREST member companies employ many OSCPs and GIAC-certified professionals. They complement each other. But what sets CREST apart is that it provides an external assurance of quality and consistency at the service delivery level, which individual certifications alone do not. In a high-level red teaming engagement governed by DORA, that external assurance is crucial.

Risks of Using Non-Accredited or Poorly Vetted Providers

Choosing the wrong provider for a TLPT isn't just a minor inconvenience – it can introduce serious reputational, operational, and regulatory risks for a financial institution. Let's examine these risks:

- Reputational Risk: Your institution's reputation is on the line during a TLPT. By its nature, a TLPT might expose sensitive weaknesses or even result in notable disruptions if mishandled. An unaccredited or poorly vetted provider may lack adequate safeguards, potentially leading to a public incident (e.g. if the test accidentally takes down online services or if news leaks that customer data was accessed during the exercise). Furthermore, if word gets out in industry circles or to clients that you engaged a sub-par security firm, it could reflect poorly on your due diligence. In contrast, using a renowned, accredited firm shows stakeholders that you take cyber resilience seriously and have done your homework in hiring experts.

- Operational Risk: As discussed, an incompetent Red Team test can cause real damage. Imagine a tester triggering a major outage in core banking systems or failing to contain the test such that it impacts actual business operations. There's also the risk of false sense of security – a less skilled team might overlook crucial vulnerabilities or not actually test your detection/response effectively, leaving you blind to real dangers. Essentially, a bad TLPT is not just wasted effort; it can actively make you less secure (either by causing incidents or by giving you an inaccurate assessment). Accredited providers significantly mitigate this risk because they follow strict procedures to prevent uncontrolled events and ensure findings are valid. They carry insurance for a reason – but ideally will never have to use it because of their professionalism. With an unvetted provider, you are taking a gamble on their operational discipline.



Risks of Using Non-Accredited or Poorly Vetted Providers Continued

- Regulatory Risk: Non-compliance with DORA is a serious matter. If you choose a provider that doesn't meet DORA's criteria (for example, they're not accredited/certified as required, or they lack the necessary expertise), you could fail to satisfy the TLPT requirement. Regulators could reject the test results or, worse, impose sanctions for not conducting the TLPT properly within mandated timelines. DORA empowers authorities to enforce penalties for non-compliance, just as they would for failures in other risk management obligations. At the very least, you might be required to redo the TLPT with an acceptable provider – incurring additional cost and effort. Furthermore, regulators across the EU are likely to share information about the quality of TLPT exercises; a poor report or incident in one country could attract scrutiny elsewhere. In short, skimping on provider vetting isn't worth the risk. Using an accredited firm directly supports compliance by fulfilling the "tester requirements" that DORA set out, whereas an unaccredited firm puts you on legally thin ice.

It's also worth noting that cyber security is ultimately about trust. Financial institutions are entrusting external testers with the keys to their kingdom during a TLPT (at least in a limited scope). If the provider is not well vetted, you risk that trust being broken – perhaps through data mishandling, conflicts of interest, or even malicious behaviour. While rare, there have been cases in the broader industry of "penetration testers" who turned out to be unscrupulous, causing breaches or extortion. Accredited providers are not immune to wrongdoing, but the accreditation process and community oversight make such scenarios far less likely.

In summary, choosing a credible, accredited TLPT provider greatly reduces your risk. It provides assurance that the test will be meaningful and safe, and that your organisation will emerge from the exercise with improved resilience rather than new problems. As one 2025 industry guide put it, even if some non-accredited firms can do a decent job, if you want assurance that the engagement meets recognised standards and has been properly vetted, going with an accredited provider "is best".

Conclusion

The Digital Operational Resilience Act is raising the bar for cyber security in the EU financial sector, and Threat-Led Penetration Testing is a prime example of this elevated standard. By requiring TLPT, regulators are effectively asking institutions to prove their cyber resilience under fire – to show that they can withstand the kinds of sophisticated attacks that real-world adversaries might throw at them. Meeting this challenge means not only conducting TLPTs as a checkbox exercise but doing them with the right approach and partners.

For financial entities gearing up for DORA compliance, the key takeaways are clear: plan your TLPT early, budget for doing it at least every three years, and select your testing partner with extreme care. Engaging an accredited provider (ideally a CREST-accredited company with a strong track record in red teaming and threat intelligence) will provide confidence that the test is executed expertly and in line with regulatory expectations. It will also yield more reliable results that you can use to fortify your defences and demonstrate improvements to regulators and stakeholders.

TLPT, when done properly, is not just a compliance hurdle – it's an invaluable tool for continuous improvement. It can reveal unseen vulnerabilities in your systems, processes, and people, and it can pressure-test your incident response in a way no theoretical drill can. By partnering with a top-notch, accredited red team, you gain an honest view of your cyber resilience and a roadmap to enhance it. In contrast, cutting corners with unqualified testers could leave you with a false sense of security or land you in hot water.

As a CISO or security manager, you should treat the TLPT provider selection as seriously as you would a critical technology vendor. Ask for certifications, check for CREST (or equivalent) accreditation, inquire about their experience with frameworks like TIBER-EU or CBEST, and ensure they understand DORA's specific requirements. A good provider will be able to walk you through their methodology and how it maps to DORA's process (preparation, testing phases, closure/purple team, etc.) and deliverables. They will also emphasise safety and clear rules of engagement to protect your production environment during the test.

At the end, TLPT under DORA is as much about building trust as it is about testing. By undergoing a threat-led penetration test, a financial institution signals to regulators, customers, and itself that it is taking cyber threats seriously and is willing to learn and improve from realistic challenges. By choosing the right accredited partner to perform that test, the institution further ensures that this trust is well placed – that the results of the TLPT will be credible and actionable.

Author: Zoja Antuchevic, CEO, SolutionLab and a CREST EU Council Member