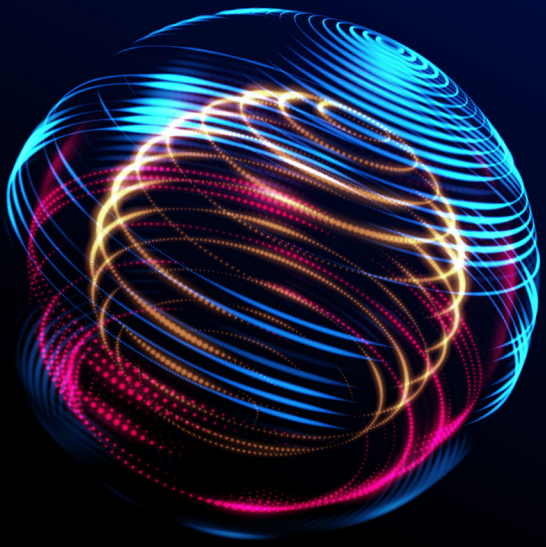
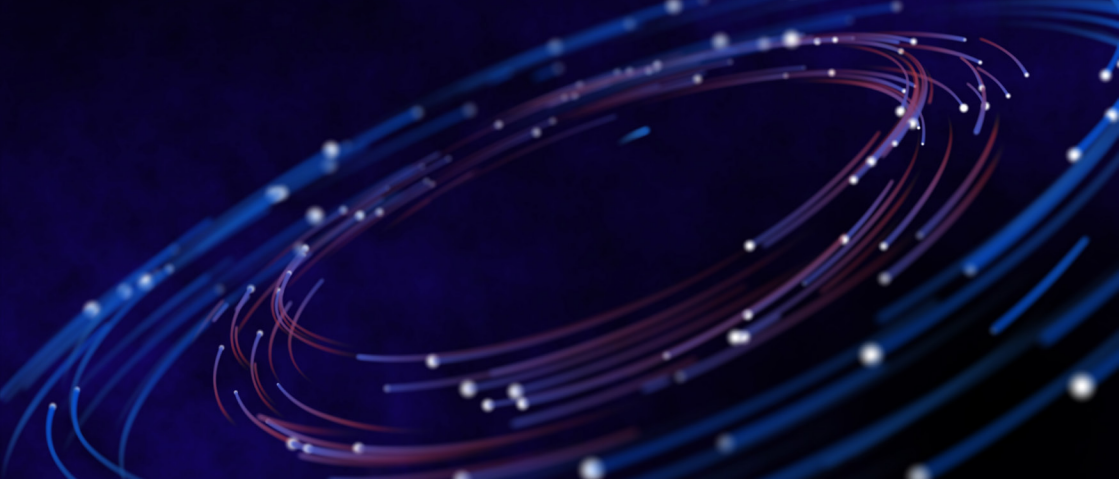


CMS
law·tax·future

Digital Finance Papers N.2

I Threat-Led Penetration Test: tra normativa e criticità

Gennaio 2026



Al fine di garantire un elevato livello di resilienza operativa digitale nel settore finanziario, il Regolamento (UE) 2022/2554, noto come Regolamento **DORA (Digital Operational Resilience Act)**, entrato in vigore a gennaio 2025, ha introdotto un quadro normativo armonizzato che impone alle entità finanziarie specifici obblighi in materia di gestione dei rischi informatici e di segnalazione degli incidenti connessi alle **TIC**.

In funzione del perseguimento dell'obiettivo della resilienza operativa digitale, l'art. 26 del Regolamento DORA introduce l'obbligo di sottoporre le funzioni essenziali o importanti delle entità finanziarie a test avanzati di cibersicurezza guidati dalla minaccia o **Threat-Led Penetration Test (TLPT)**, che vengono svolti secondo le norme tecniche di regolamentazione **(Regulatory Technical Standards – RTS)** elaborate dall'autorità europee di vigilanza .

Siffatti test sono volti a valutare l'impatto delle minacce informatiche attuali e verosimili sulle funzioni aziendali essenziali o importanti, nonché a verificare la capacità dell'entità di prevenire, individuare, rispondere e ripristinare le proprie operazioni in presenza di attacchi informatici complessi.

Il Regolamento prevede che le entità finanziarie individuate dalle autorità competenti siano tenute a svolgere test di penetrazione guidati dalla minaccia sulle funzioni essenziali o importanti con una frequenza almeno triennale.

Tale periodicità può essere modulata dall'autorità competente che, sulla base del profilo di rischio dell'entità finanziaria e delle specifiche circostanze operative, può richiedere un aumento o una riduzione della frequenza dei TLPT.

Ai sensi dell'art. 27 del Regolamento DORA, per l'esecuzione dei TLPT, le entità finanziarie devono avvalersi

esclusivamente di soggetti incaricati altamente qualificati e affidabili, dotati di comprovate competenze tecniche e organizzative in materia di analisi delle minacce, penetration testing e red teaming, nonché adeguatamente certificati o aderenti a codici di condotta ed etici riconosciuti. Tali soggetti devono inoltre garantire un'adeguata copertura assicurativa e fornire garanzia sulla corretta gestione dei rischi connessi allo svolgimento dei TLPT, inclusa la tutela delle informazioni riservate.

Qualora i test siano svolti da soggetti interni, ciò è consentito solo previa autorizzazione dell'autorità competente, a condizione che siano assicurate risorse dedicate sufficienti, l'assenza di conflitti di interesse e il ricorso a un fornitore esterno per l'analisi delle minacce.

Le fasi del TLPT

I Threat-Led Penetration Test (TLPT) costituiscono attività complesse e articolate, finalizzate a valutare in modo realistico la resilienza delle funzioni essenziali o importanti di un'entità finanziaria di fronte a minacce informatiche sofisticate.

La loro efficacia dipende dalle competenze tecniche dei team coinvolti e da una pianificazione accurata, che assicuri l'identificazione, la documentazione e la mitigazione delle vulnerabilità individuate.

I TLPT, come puntualmente disciplinati dalle norme tecniche di regolamentazione (RTS) di riferimento, si articolano in tre fasi principali: la fase di preparazione (preparation), la fase di esecuzione dei test (testing) e la fase di chiusura (closure).

La fase di preparation prende avvio con la notifica, da parte dell'autorità competente per i TLPT, della necessità di condurre un test. Entro tre mesi dal ricevimento di tale comunicazione, l'entità finanziaria è tenuta a trasmettere la documentazione relativa al TLPT, comprensiva delle informazioni sul team di controllo, nonché a definire l'ambito del test, individuando le funzioni essenziali o importanti da sottoporre a verifica sulla base di criteri quali l'impatto sul settore finanziario e la stabilità del sistema.

La fase di testing ha inizio con l'analisi mirata delle minacce. Il soggetto incaricato di fornire tale analisi esamina le minacce informatiche generiche e settoriali rilevanti per l'entità finanziaria, anche facendo riferimento, ove necessario, al scenario delle minacce per il settore finanziario dello Stato membro.

In tale contesto, vengono individuate le minacce informatiche e le vulnerabilità esistenti o potenziali dell'entità, raccogliendo informazioni concrete, fruibili e contestualizzate sui possibili bersagli e scenari di attacco, anche mediante il confronto con il team di controllo e i responsabili dei test.

La relazione sull'analisi mirata delle minacce è sottoposta all'approvazione dell'autorità competente.

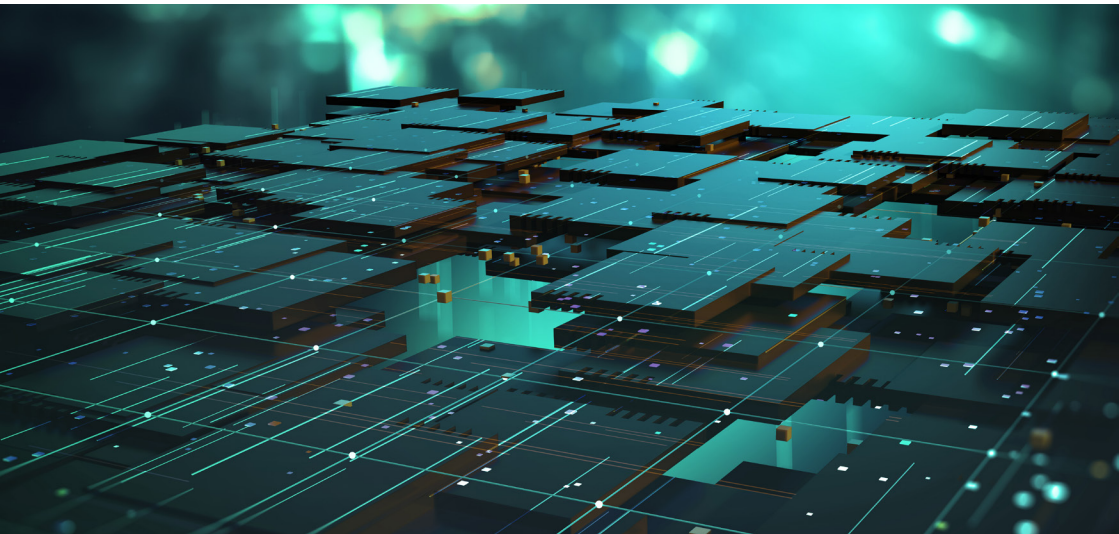
Sulla base delle risultanze dell'analisi delle minacce, ha luogo la fase di red team testing, nella quale i soggetti incaricati dell'esecuzione dei test elaborano un piano operativo dettagliato.

Qualora tale piano risulti completo e idoneo a garantire lo svolgimento efficace del TLPT, esso viene approvato dal team di controllo e dall'autorità competente, che ne dà comunicazione al responsabile del team di controllo. La fase attiva di test ha una durata minima di dodici settimane.

La fase di closure si apre con l'informativa al personale dell'entità finanziaria (c.d. blue team) dell'avvenuta esecuzione del TLPT.

Entro quattro settimane dalla conclusione della fase attiva, il red team, ovvero il team che pianifica, sviluppa ed esegue degli scenari di attacco sulle persone, processi, sistemi e servizi inclusi nel perimetro del test, trasmette la relazione sui test effettuati, cui segue, entro le successive dieci settimane, la relazione del blue team.

Entro dieci settimane dalla fine della fase di red team testing, il blue team e i soggetti incaricati dello svolgimento dei test procedono alla replica delle azioni offensive e difensive eseguite durante il TLPT. Il team di controllo svolge inoltre un esercizio di purple teaming su specifici ambiti individuati congiuntamente dal blue team e dai soggetti incaricati dei test, sulla base delle vulnerabilità emerse e, ove necessario, su aspetti non testati nella fase attiva.



Al termine degli esercizi di replica e di purple teaming, tutti i soggetti coinvolti nel processo — team di controllo, blue team, red team e fornitori dell'analisi delle minacce — procedono a uno scambio strutturato di riscontri sull'intero processo di TLPT.

Concluso il test, l'entità finanziaria è tenuta a presentare, entro otto settimane dalla notifica delle risultanze, un piano correttivo che dettagli le carenze individuate, le misure di remediation proposte, le cause profonde e le responsabilità.

Al termine del processo, l'autorità competente per i TLPT rilascia un attestato che sintetizza gli elementi essenziali e gli esiti del test.

Coinvolgimento dei fornitori terzi di servizi TIC nei test di penetrazione guidati dalla minaccia (TLPT)

Lo svolgimento dei Threat-Led Penetration Test (TLPT) può coinvolgere anche i fornitori terzi di servizi TIC qualora i servizi da questi prestati siano a supporto di funzioni essenziali o importanti delle entità finanziarie.

In tali circostanze, le entità finanziarie sono tenute ad adottare tutte le misure organizzative, contrattuali e tecniche necessarie a garantire l'effettiva partecipazione dei fornitori terzi di servizi TIC allo svolgimento dei TLPT, assicurando al contempo un adeguato livello di controllo, coordinamento e tutela delle informazioni sensibili.

A tal fine, il Regolamento consente che l'entità finanziaria e il fornitore terzo di servizi TIC concordino espressamente, in forma scritta, che quest'ultimo stipuli direttamente accordi contrattuali con un soggetto esterno incaricato dello svolgimento dei test.

Tali accordi sono finalizzati alla conduzione, sotto la direzione di un'entità finanziaria designata, di un TLPT congiunto (pooled testing), che può coinvolgere più entità finanziarie servite dal medesimo fornitore terzo di servizi TIC.

Tuttavia, il coinvolgimento dei fornitori terzi di servizi TIC nei TLPT solleva delicate questioni sotto il profilo della concorrenza e della tutela del segreto industriale. In particolare, il soggetto incaricato dello svolgimento dei test potrebbe essere un operatore che, direttamente o indirettamente, compete con il fornitore TIC oggetto del test sul medesimo mercato.

In tali circostanze, l'accesso a informazioni altamente sensibili — quali architetture di sistema, configurazioni di sicurezza, processi operativi e vulnerabilità — potrebbe determinare rischi di concorrenza sleale, indebita appropriazione di know-how o distorsioni del mercato, anche in assenza di un utilizzo intenzionalmente illecito delle informazioni acquisite.

Ciò impone una particolare attenzione nella selezione dei soggetti incaricati dello svolgimento dei test e nella predisposizione di presidi contrattuali rafforzati, volti a prevenire conflitti di interesse, assicurare l'indipendenza del tester e garantire la rigorosa segregazione delle informazioni.

È prevedibile che, nella prassi applicativa, emerga una tensione strutturale tra gli interessi delle entità finanziarie e quelli dei fornitori terzi di servizi TIC. Da un lato, le banche e gli intermediari finanziari saranno tenderanno a coinvolgere anche i fornitori di servizi TIC nell'ambito dei TLPT, in quanto tali test rappresentano uno strumento particolarmente efficace per rafforzare la resilienza operativa digitale e per dimostrare la propria compliance regolamentare nei confronti delle autorità di vigilanza.

Dall'altro lato, i fornitori di servizi TIC potrebbero manifestare una maggiore resistenza, considerato il carattere intrinsecamente invasivo dei TLPT, l'elevato impatto operativo, nonché i rischi connessi alla divulgazione di informazioni sensibili e al possibile pregiudizio competitivo.

In questo contesto, il mercato sarà chiamato a individuare un punto di equilibrio tra l'esigenza di sicurezza e resilienza perseguita dal Regolamento DORA e la necessità di tutelare l'operatività, il know-how e la posizione concorrenziale dei fornitori di servizi TIC.

Tale equilibrio potrà essere raggiunto solo attraverso un progressivo affinamento delle prassi contrattuali, della governance dei test e dei meccanismi di salvaguardia, nonché mediante un dialogo costante tra entità finanziarie, fornitori e autorità di vigilanza, volto a garantire un'applicazione proporzionata ed efficace dei TLPT.

Matia Campo
Partner / TMC
T +39 06478151
E matia.campo@cms-aacs.com

Veronica Mazzaferro
Counsel / TMC
T +39 06478151
E veronica.mazzaferro@cms-aacs.com

Alice Dal Bello
Trainee / TMC
T +39 06478151
E alice.dalbello@cms-aacs.com

Digital Finance Team

Emiliano La Sala
Partner/Debt Capital Markets
E emiliano.lasala@cms-aacs.com

Paolo Bonolis
Partner/Banking & Finance
E paolo.bonolis@cms-aacs.com

Italo De Feo
Partner/TMC
E italo.defeo@cms-aacs.com

Domenico Gaudiello
Partner/Banking & Finance
E domenico.gaudiello@cms-aacs.com

Matia Campo
Partner/TMC
E matia.campo@cms-aacs.com

CMS Law-Now™

Your free online legal information service.

A subscription service for legal articles on a variety of topics delivered by email.
cms-lawnow.com

CMS locations:
Aberdeen, Abu Dhabi, Amsterdam, Antwerp, Barcelona, Beijing, Belgrade, Bengaluru, Bergen, Berlin, Bogotá, Bratislava, Brisbane, Bristol, Brussels, Bucharest, Budapest, Casablanca, Chennai, Cologne, Dubai, Dublin, Duesseldorf, Ebene, Edinburgh, Frankfurt, Funchal, Geneva, Glasgow, Gothenburg, Gurugram, Hamburg, Hong Kong, Hyderabad, Istanbul, Johannesburg, Kyiv, Leipzig, Lima, Lisbon, Liverpool, Ljubljana, London, Luanda, Luxembourg, Lyon, Madrid, Manchester, Maputo, Mexico City, Milan, Mombasa, Monaco, Mumbai, Munich, Muscat, Nairobi, New Delhi, Oslo, Paris, Podgorica, Poznan, Prague, Reading, Rio de Janeiro, Riyadh, Rome, Santiago de Chile, São Paulo, Sarajevo, Shanghai, Sheffield, Silicon Valley, Singapore, Skopje, Sofia, Stavanger, Stockholm, Strasbourg, Stuttgart, Sydney, Tel Aviv, Tirana, Vienna, Warsaw, Zagreb and Zurich.

Further information can be found at **cms.law**