2025/1190

18.6.2025

REGOLAMENTO DELEGATO (UE) 2025/1190 DELLA COMMISSIONE

del 13 febbraio 2025

che integra il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che specificano i criteri utilizzati per identificare le entità finanziarie che hanno l'obbligo di svolgere test di penetrazione guidati dalla minaccia, i requisiti e le norme che disciplinano il ricorso a soggetti incaricati dello svolgimento dei test interni, i requisiti concernenti l'ambito, l'approccio e la metodologia da seguire per i test in ciascuna fase dei test, i risultati, la chiusura e le fasi correttive e il tipo di cooperazione di vigilanza e altri tipi di cooperazione pertinenti necessari per svolgere i TLPT e per la facilitazione del riconoscimento reciproco

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 ([1]), in particolare l'articolo 26, paragrafo 11, quarto comma,

considerando quanto segue:

(1) Il presente regolamento è stato redatto conformemente al quadro di riferimento TIBER-EU e rispecchia la metodologia, il processo e la struttura dei test di penetrazione guidati dalla minaccia (*threat-led penetration testing*, TLPT) descritti in detto quadro. Le entità finanziarie soggette a TLPT possono fare riferimento al quadro TIBER-EU, o a una delle sue implementazioni nazionali, e applicarlo nella misura in cui tale quadro o implementazione sia coerente con i requisiti di cui agli articoli 26 e 27 del regolamento (UE) 2022/2554 e con il presente regolamento. La designazione di un'autorità pubblica unica nel settore finanziario responsabile delle questioni relative ai TLPT a livello nazionale a norma dell'articolo 26, paragrafo 9, del regolamento (UE) 2022/2554 dovrebbe lasciare impregiudicata la competenza delle autorità competenti affidata a livello dell'Unione per la vigilanza di talune entità finanziarie a norma dell'articolo 46 di tale regolamento, come ad esempio la Banca centrale europea per gli enti creditizi significativi che devono essere considerati competenti per le questioni relative ai TLPT. Se solo alcuni dei compiti relativi ai TLPT sono delegati a un'altra autorità nazionale nel settore finanziario a norma dell'articolo 26, paragrafo 10, del regolamento (UE) 2022/2554, l'autorità competente dell'entità finanziaria di cui all'articolo 46 del medesimo regolamento dovrebbe continuare a essere l'autorità responsabile dei compiti relativi ai TLPT che non sono stati delegati.

(2) Tenuto conto della complessità del TLPT e dei rischi connessi, il relativo utilizzo dovrebbe essere limitato alle entità finanziarie per le quali è giustificato. Pertanto le autorità responsabili delle questioni relative ai TLPT (autorità competenti per i TLPT, a livello dell'Unione o nazionale) dovrebbero escludere dall'ambito di applicazione dei TLPT le entità finanziarie che operano in sottosettori chiave dei servizi finanziari per i quali un TLPT non è giustificato. Ciò significa che gli enti creditizi, gli istituti di pagamento e di moneta elettronica, i depositari centrali di titoli, le controparti centrali, le sedi di negoziazione, le imprese di assicurazione e di riassicurazione, anche se soddisfano i criteri quantitativi, potrebbero essere dispensati dall'obbligo di svolgere TLPT alla luce di una valutazione globale del loro profilo dei rischi informatici e della maturità delle TIC, dell'impatto sul settore finanziario e dei relativi problemi di stabilità finanziaria.

(3) Le autorità competenti per i TLPT dovrebbero valutare, alla luce di una valutazione globale del profilo dei rischi informatici e della maturità delle TIC, dell'impatto sul settore finanziario e dei relativi problemi di stabilità finanziaria, se qualsiasi tipo di entità finanziaria diversa dagli enti creditizi, dagli istituti di pagamento, dagli istituti di moneta elettronica, dalle controparti centrali, dai depositari centrali di titoli, dalle sedi di negoziazione e dalle imprese di assicurazione e di riassicurazione debba essere soggetta a TLPT. La valutazione del rispetto dei suddetti criteri qualitativi da parte di tali entità finanziarie dovrebbe mirare a individuare le entità finanziarie per le quali il TLPT è appropriato utilizzando indicatori intersettoriali e oggettivi. Allo stesso tempo, la valutazione del rispetto di tali

([1]) GU L 333 del 27.12.2022, pag. 1, ELI: https//data.europa.eu/eli/reg/2022/2554/oj.

criteri qualitativi da parte di un'entità finanziaria dovrebbe limitare le entità soggette a TLPT a quelle per le quali il test è giustificato. È opportuno valutare se un'entità finanziaria soddisfa tali criteri qualitativi anche alla luce dello sviluppo di nuovi mercati e della crescente importanza di nuovi partecipanti al mercato per il settore finanziario in futuro, compresi i prestatori di servizi per le cripto-attività autorizzati a norma dell'articolo 59 del regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio ([2]).

(4) Le entità finanziarie possono avere lo stesso fornitore intragruppo di servizi di TIC o appartenere allo stesso gruppo e fare affidamento sull'uso di sistemi di TIC condivisi. In tal caso, è importante che le autorità competenti per i TLPT tengano conto della struttura e del carattere sistemico o dell'importanza per il settore finanziario di tale entità finanziaria a livello nazionale o dell'Unione nel valutare se un'entità finanziaria debba essere soggetta a TLPT e se il TLPT debba essere condotto a livello di entità o di gruppo (attraverso un TLPT comune).

(5) Per rispecchiare il quadro di riferimento TIBER-EU, è necessario che la metodologia da seguire per i test preveda il coinvolgimento dei seguenti partecipanti principali: l'entità finanziaria, con un team di controllo (che rispecchia il «team di controllo» di TIBER-EU) e un blue team (che rispecchia il «blue team» di TIBER-EU), e l'autorità competente per il TLPT, sotto forma di un team informatico TLPT (che rispecchia i «TIBER cyber team» di TIBER-EU), un soggetto che fornisce analisi delle minacce e soggetti incaricati dello svolgimento dei test (questi ultimi rispecchiano il «red team provider» di TIBER-EU).

(6) Per garantire che il TLPT tragga vantaggio dall'esperienza acquisita nel quadro dell'attuazione di TIBER-EU e per ridurre i rischi associati allo svolgimento dei TLPT, è opportuno garantire che le responsabilità dei team informatici TLPT da istituire a livello delle autorità competenti per i TLPT corrispondano il più possibile a quelle dei «TIBER-EU cyber team». Pertanto i team informatici TLPT dovrebbero disporre di responsabili dei test incaricati della supervisione dei singoli TLPT nonché della pianificazione e del coordinamento dei singoli test. I team informatici TLPT dovrebbero fungere da punto di contatto unico per la comunicazione relativa ai test ai portatori di interessi interni ed esterni, per la raccolta e il trattamento dei riscontri e degli insegnamenti tratti dai test condotti in precedenza e per il sostegno alle entità finanziarie sottoposte a TLPT.

(7) Per rispecchiare la metodologia del quadro di riferimento TIBER-EU, i responsabili dei test dovrebbero disporre delle competenze e delle capacità necessarie per fornire consulenza e per contestare le proposte dei soggetti incaricati dello svolgimento dei test. L'esperienza acquisita nell'ambito del quadro di riferimento TIBER-EU ha dimostrato che è utile disporre di un team composto da almeno due responsabili dei test assegnati a ciascun test. Per riflettere il fatto che il TLPT è utilizzato per incoraggiare l'esperienza di apprendimento, per salvaguardare la riservatezza dei test e, a meno che non sussistano problematiche relative alle risorse o alle competenze, le autorità competenti per i TLPT sono fortemente incoraggiate a considerare che, per la durata di un TLPT, i responsabili dei test non dovrebbero svolgere attività di vigilanza sulla stessa entità finanziaria sottoposta a TLPT.

(8) Ai fini della coerenza con il quadro di riferimento TIBER-EU, è importante che l'autorità competente per il TLPT segua da vicino il test in ciascuna delle sue fasi. In considerazione della natura del test e dei rischi ad esso associati, è fondamentale che l'autorità competente per il TLPT sia coinvolta in ciascuna fase specifica del test. In particolare, l'autorità competente per il TLPT dovrebbe essere consultata e dovrebbe convalidare le valutazioni o le decisioni delle entità finanziarie che possono, da un lato, influenzare l'efficacia del test e, dall'altro, avere un impatto sui rischi associati al test. Le fasi fondamentali durante le quali è necessario il coinvolgimento specifico dell'autorità competente per il TLPT comprendono la convalida di alcuni documenti fondamentali del test, la selezione dei soggetti che forniscono analisi delle minacce e dei soggetti incaricati dello svolgimento dei test nonché le misure di gestione dei rischi. Il coinvolgimento delle autorità competenti per i TLPT, in particolare per le convalide, non dovrebbe comportare un onere eccessivo per tali autorità e dovrebbe pertanto essere limitato alla documentazione e alle decisioni che incidono direttamente sullo svolgimento del TLPT. Attraverso la partecipazione attiva a ciascuna fase del test, le autorità competenti per i TLPT possono valutare efficacemente la conformità delle entità finanziarie ai requisiti pertinenti, il che dovrebbe consentire a tali autorità di rilasciare attestati a norma dell'articolo 26, paragrafo 7, del regolamento (UE) 2022/2554.

([2]) Regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle cripto-attività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937 (GU L 150 del 9.6.2023, pag. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj).

(9) La segretezza del TLPT è di fondamentale importanza affinché le condizioni del test siano realistiche. Per tale motivo, il test dovrebbe essere segreto e dovrebbero essere adottate precauzioni affinché il TLPT resti riservato, compresa la scelta dei nomi in codice che dovrebbero essere concepiti in modo da impedire l'identificazione del TLPT da parte di terzi. Se i membri del personale responsabili della sicurezza della divisione finanziaria sono a conoscenza di un TLPT pianificato o in corso, è probabile che siano più accorti e attenti rispetto alle normali condizioni di lavoro, alterando così l'esito del test. I membri del personale dell'entità finanziaria al di fuori del team di controllo dovrebbero pertanto essere informati di eventuali TLPT pianificati o in corso solo se vi sono motivi validi e previo accordo dei responsabili dei test, anche al fine di garantire la segretezza del test nel caso in cui un membro del blue team abbia rilevato il test.

(10) Come dimostrato dall'esperienza acquisita nell'ambito del quadro di riferimento TIBER-EU per quanto riguarda il «team di controllo», la selezione di un responsabile adeguato del team di controllo è indispensabile affinché il TLPT sia condotto in sicurezza. Il responsabile del team di controllo dovrebbe disporre dell'autorità necessaria all'interno dell'entità finanziaria per dirigere tutti gli aspetti del test, senza comprometterne la riservatezza. Per lo stesso motivo, i membri del team di controllo dovrebbero avere una conoscenza approfondita dell'entità finanziaria, delle mansioni e del posizionamento strategico del responsabile del team di controllo, avere l'anzianità richiesta e avere accesso al consiglio di amministrazione. Per ridurre il rischio di compromettere il TLPT, il team di controllo dovrebbe essere il più ristretto possibile.

(11) Sono presenti elementi intrinseci di rischio associati ai TLPT, in quanto le funzioni essenziali sono sottoposte a test in un ambiente di produzione attivo, per cui sussiste la possibilità di causare incidenti legati alla negazione del servizio, guasti imprevisti del sistema, danni a sistemi di produzione attivi e critici oppure la perdita, la modifica o la divulgazione di dati. Tali rischi evidenziano la necessità di solide misure di gestione dei rischi. Per garantire che il TLPT sia condotto in maniera controllata durante l'intero processo di test, è molto importante che le entità finanziarie siano consapevoli in ogni momento dei rischi specifici che insorgono durante un TLPT e che tali rischi siano attenuati. A tale riguardo, fatti salvi i processi interni dell'entità finanziaria e la responsabilità e le deleghe già attribuite al responsabile del team di controllo, può risultare opportuno fornire informazioni sulle misure di gestione dei rischi connessi al TLPT o, in casi particolari, sottoporre tali misure di gestione dei rischi all'approvazione dell'organo di gestione stesso dell'entità finanziaria. Per poter fornire servizi professionali efficaci e più qualificati e ridurre tali rischi, è altresì essenziale che i soggetti incaricati dello svolgimento dei test e i soggetti che forniscono analisi delle minacce (denominati congiuntamente «fornitori di TLPT») possiedano il massimo livello di competenze, conoscenze e un'esperienza adeguata nel campo dell'analisi delle minacce e dei TLPT nel settore dei servizi finanziari.

(12) Spesso i test di penetrazione convenzionali forniscono una valutazione dettagliata e utile delle vulnerabilità tecniche e di configurazione di un singolo sistema o ambiente in maniera isolata, ma a differenza di un test red team basato sull'analisi della minaccia, non valutano lo scenario complessivo di un attacco mirato nei confronti di un'intera entità, compreso l'ambito di applicazione completo delle rispettive persone, procedure e tecnologie. Durante il processo di selezione dei fornitori di TLPT, le entità finanziarie dovrebbero pertanto garantire che tali fornitori dispongano delle competenze necessarie per eseguire test red team basati sull'analisi della minaccia e non solo test di penetrazione. È pertanto necessario stabilire criteri esaustivi per i soggetti incaricati dello svolgimento dei test, sia interni che esterni, nonché per i soggetti che forniscono analisi delle minacce, che sono sempre esterni. Qualora i fornitori di TLPT appartengano alla stessa impresa, il personale assegnato a un TLPT dovrebbe essere adeguatamente separato.

(13) Possono verificarsi circostanze eccezionali in cui le entità finanziarie non sono in grado di avvalersi di fornitori di TLPT che soddisfano tutti i criteri. Le entità finanziarie, dopo aver dimostrato l'indisponibilità di tali soggetti che forniscono analisi delle minacce, dovrebbero essere pertanto autorizzate a coinvolgere persone che non soddisfano tutti i criteri, a condizione che provvedano ad attenuare adeguatamente eventuali rischi aggiuntivi che ne conseguono e che l'autorità competente per il TLPT valuti tutti i criteri in questione.

(14) Qualora più entità finanziarie e diverse autorità competenti per i TLPT siano coinvolte in un TLPT, dovrebbero essere specificati i ruoli di tutte le parti coinvolte nel processo di TLPT affinché il test possa essere condotto nel modo più efficiente e sicuro possibile. Ai fini dei test congiunti, sono necessari requisiti specifici volti a specificare il ruolo dell'entità finanziaria designata; nello specifico essa dovrebbe essere incaricata di fornire tutta la documentazione necessaria all'autorità capofila competente per il TLPT e di monitorare il processo di test. L'entità finanziaria designata dovrebbe inoltre essere responsabile degli aspetti comuni della valutazione della gestione del rischio. Nonostante il ruolo dell'entità finanziaria designata, gli obblighi di ciascuna entità finanziaria che partecipa al processo di TLPT congiunto dovrebbero rimanere inalterati durante il test congiunto. Lo stesso principio dovrebbe applicarsi ai TLPT comuni.

(15) Come dimostrato dall'esperienza acquisita nell'attuazione del quadro di riferimento TIBER-EU, l'organizzazione di riunioni in presenza o virtuali che coinvolgano tutti i portatori di interessi (entità finanziarie, autorità, soggetti incaricati dello svolgimento dei test e soggetti che forniscono analisi delle minacce) rappresenta il modo più efficiente per garantire lo svolgimento adeguato dei test. Si dovrebbero pertanto tenere riunioni in presenza e virtuali in varie fasi del processo, in particolare durante la fase di preparazione all'avvio del TLPT e per perfezionarne l'ambito di applicazione, durante la fase di test, per ultimare la relazione sull'analisi delle minacce e il piano relativo al test red team e per gli aggiornamenti settimanali, nonché durante la fase di chiusura per la replica delle azioni dei soggetti incaricati dello svolgimento dei test e del blue team, il purple teaming e lo scambio di riscontri sul TLPT.

(16) Per garantire il corretto svolgimento del TLPT, l'autorità competente per il TLPT dovrebbe esporre chiaramente all'entità finanziaria quali sono le sue aspettative in merito al test. A tale riguardo, i responsabili dei test dovrebbero garantire che sia instaurato un adeguato flusso di informazioni con il team di controllo all'interno dell'entità finanziaria e con i fornitori di TLPT.

(17) L'entità finanziaria dovrebbe selezionare le funzioni essenziali o importanti che rientreranno nell'ambito di applicazione del TLPT. Nel selezionare tali funzioni, l'entità finanziaria dovrebbe basarsi su vari criteri relativi all'importanza di ciascuna funzione per l'entità finanziaria stessa e per il settore finanziario, a livello dell'Unione e nazionale, non solo in termini economici, ma anche in considerazione dello status simbolico o politico della funzione. Per facilitare una transizione agevole verso la fase di raccolta delle analisi delle minacce, il team di controllo dovrebbe fornire ai soggetti incaricati dello svolgimento dei test e ai soggetti che forniscono analisi delle minacce che non sono coinvolti nel processo di definizione dell'ambito di applicazione informazioni dettagliate sull'ambito di applicazione concordato.

(18) Per fornire ai soggetti incaricati dello svolgimento dei test le informazioni necessarie per simulare un attacco reale e realistico ai sistemi attivi dell'entità finanziaria che sono alla base delle sue funzioni essenziali o importanti, il soggetto che fornisce analisi delle minacce dovrebbe raccogliere informazioni riguardanti almeno due settori chiave di interesse: i bersagli, individuando potenziali superfici di attacco in tutta l'entità finanziaria, e le minacce, identificando i pertinenti autori della minaccia e i probabili scenari della minaccia. Per garantire che il soggetto che fornisce analisi delle minacce prenda in considerazione le minacce pertinenti per l'entità finanziaria, i soggetti incaricati dello svolgimento dei test, il team di controllo e i responsabili dei test dovrebbero fornire riscontri sul progetto di relazione sull'analisi delle minacce. Il soggetto che fornisce analisi delle minacce può utilizzare, se disponibile, un panorama delle minacce generico fornito dall'autorità competente per il TLPT per il settore finanziario di uno Stato membro come base di riferimento per il panorama delle minacce nazionale. Sulla base dell'applicazione del quadro di riferimento TIBER-EU, il processo di raccolta delle analisi delle minacce generalmente dura all'incirca quattro settimane.

(19) Per consentire ai soggetti incaricati dello svolgimento dei test di acquisire informazioni e riesaminare ulteriormente il documento relativo alle specifiche dell'ambito di applicazione e la relazione sull'analisi mirata delle minacce al fine di ultimare il piano relativo al test red team, è essenziale che, prima della fase di test red team del TLPT, i soggetti incaricati dello svolgimento dei test ricevano dal soggetto che fornisce analisi delle minacce spiegazioni dettagliate in merito alla relazione sull'analisi mirata delle minacce e l'analisi dei possibili scenari di minaccia.

(20) Per consentire ai soggetti incaricati dello svolgimento dei test di svolgere un test realistico e completo in cui tutte le fasi di attacco siano eseguite e siano raggiunti gli obiettivi (*flag*), alla fase attiva di test red team dovrebbe essere assegnato un tempo sufficiente. Sulla base dell'esperienza acquisita con il quadro di riferimento TIBER-EU, il tempo assegnato dovrebbe essere di almeno 12 settimane e dovrebbe essere determinato tenendo conto del numero di parti coinvolte, dell'ambito di applicazione del TLPT, delle risorse dell'entità o delle entità finanziarie coinvolte, di eventuali requisiti esterni e della disponibilità di informazioni di supporto fornite dall'entità finanziaria.

(21) Durante la fase attiva di test red team, i soggetti incaricati dello svolgimento dei test dovrebbero utilizzare una serie di tattiche, tecniche e procedure per sottoporre adeguatamente a test i sistemi di produzione attivi dell'entità finanziaria. Le tattiche, tecniche e procedure dovrebbero prevedere, se del caso, la ricognizione (reconnaissance, ossia la raccolta del maggior numero di informazioni possibili su un bersaglio), l'armamento (weaponization, ossia l'analisi delle informazioni sulle infrastrutture, sugli impianti e sui dipendenti e la preparazione delle operazioni specifiche per il bersaglio), la consegna (delivery, ossia l'avvio attivo dell'intera operazione indirizzata verso il bersaglio), lo sfruttamento (exploitation, ossia quando l'obiettivo dei soggetti incaricati dello svolgimento dei test è quello di compromettere i server, le reti dell'entità finanziaria e di sfruttarne il personale attraverso l'ingegneria sociale), il controllo e il movimento (ossia tentativi di passare dai sistemi compromessi ad altri sistemi vulnerabili o di elevato valore) e le azioni sul bersaglio (ossia l'ottenimento di un ulteriore accesso ai sistemi compromessi e l'acquisizione dell'accesso alle informazioni e ai dati sul bersaglio precedentemente concordato, come stabilito in precedenza nel piano relativo al test red team).

(22) Durante l'esecuzione di un TLPT, i soggetti incaricati dello svolgimento dei test dovrebbero agire tenendo conto del tempo a disposizione per eseguire l'attacco, delle risorse e dei confini etici e giuridici. Qualora i soggetti incaricati dello svolgimento dei test non fossero in grado di progredire verso la successiva fase programmata dell'attacco, il team di controllo dovrebbe fornire assistenza occasionale, previo accordo dell'autorità competente per il TLPT, sotto forma di «*leg-up*». I *leg-up* possono essere genericamente classificati in *leg-up* in materia di informazioni e di accesso e possono consistere nell'offerta di accesso a sistemi di TIC o a reti interne per proseguire il test e concentrarsi sulle successive fasi di attacco.

(23) Durante il red teaming attivo nella fase di test, se necessario per consentire il proseguimento del TLPT come ultima risorsa in circostanze eccezionali e una volta esaurite tutte le opzioni alternative, dovrebbe essere utilizzata un'attività di test collaborativa che coinvolga sia i soggetti incaricati dello svolgimento dei test che il blue team. Nel contesto di tale esercizio limitato di purple teaming, è possibile utilizzare i metodi seguenti: «catch-and-release», in cui i soggetti incaricati dello svolgimento dei test tentano di proseguire gli scenari, essere rilevati e poi riprendere i test; «war gaming», che consente scenari più complessi per sottoporre a test il processo decisionale strategico; oppure «dimostrazione di concetto collaborativa», che consente ai soggetti incaricati dello svolgimento dei test e ai membri del blue team di convalidare congiuntamente misure, strumenti o tecniche di sicurezza specifici in un ambiente controllato e cooperativo.

(24) Il TLPT dovrebbe essere utilizzato come esperienza di apprendimento per rafforzare la resilienza operativa digitale delle entità finanziarie. A tale riguardo, il blue team e i soggetti incaricati dello svolgimento dei test dovrebbero replicare l'attacco e riesaminare le misure adottate per trarre insegnamenti dall'esperienza dei test in collaborazione con i soggetti incaricati dello svolgimento dei test. A tal fine e per consentire un'adeguata preparazione, la relazione sul test del red team e la relazione sul test del blue team dovrebbero essere messe a disposizione di tutte le parti coinvolte nelle attività di replica, prima di svolgere eventuali attività di riproduzione. Inoltre, per trarre il massimo dall'esperienza di apprendimento, dovrebbe essere effettuato un esercizio di purple teaming durante la fase di chiusura. I metodi che possono essere utilizzati per il purple teaming nella fase di chiusura dovrebbero includere la discussione di scenari di attacco alternativi, l'esplorazione di scenari alternativi su sistemi attivi oppure la ri-esplorazione di scenari pianificati su sistemi attivi che i soggetti incaricati dello svolgimento dei test non erano stati in grado di completare o eseguire durante la fase di test.

(25) Per agevolare ulteriormente l'esperienza di apprendimento di tutte le parti coinvolte nel TLPT, a vantaggio dei test futuri, e per rafforzare la resilienza operativa digitale delle entità finanziarie, le parti interessate dovrebbero fornire riscontri reciproci sul processo nel suo complesso e, in particolare, individuare quali attività hanno registrato buoni progressi o avrebbero potuto essere migliorate e quali aspetti del processo di TLPT hanno funzionato bene o potrebbero essere migliorati.

(26) Le autorità competenti di cui all'articolo 46 del regolamento (UE) 2022/2554 e le autorità competenti per i TLPT, se diverse, dovrebbero cooperare per integrare i test avanzati mediante TLPT all'interno delle procedure di vigilanza esistenti. A tale riguardo e per condividere la corretta comprensione delle risultanze del TLPT e del modo in cui dovrebbero essere interpretate, è opportuno che, in particolare per quanto riguarda la relazione di sintesi sul test e i piani correttivi, sia instaurata una stretta cooperazione tra i responsabili dei test che hanno partecipato al TLPT e le autorità di vigilanza responsabili.

(27) L'articolo 26, paragrafo 8, primo comma, del regolamento (UE) 2022/2554 impone alle entità finanziarie di avvalersi di un soggetto incaricato dello svolgimento dei test esterno ogni tre test. Se le entità finanziarie includono nel gruppo di soggetti incaricati dello svolgimento dei test soggetti sia interni che esterni, ai fini del suddetto articolo il TLPT dovrebbe essere considerato come eseguito con soggetti incaricati dello svolgimento dei test interni.

(28) Il presente regolamento si basa sul progetto di norme tecniche di regolamentazione presentato alla Commissione dall'Autorità bancaria europea, dall'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali e dall'Autorità europea degli strumenti finanziari e dei mercati (autorità europee di vigilanza), in accordo con la Banca centrale europea.

(29) Le autorità europee di vigilanza hanno condotto consultazioni pubbliche aperte sui progetti di norme tecniche di regolamentazione su cui si basa il presente regolamento, hanno analizzato i relativi costi e benefici potenziali e hanno chiesto la consulenza del gruppo delle parti interessate nel settore bancario istituito in conformità dell'articolo 37 del regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio ([3]), del gruppo delle parti interessate nel settore dell'assicurazione e della riassicurazione e nel settore dei fondi pensionistici aziendali e professionali istituito a norma dell'articolo 37 del regolamento (UE) n. 1094/2010 del Parlamento europeo e del Consiglio ([4]) e del gruppo delle parti interessate nel settore degli strumenti finanziari e dei mercati istituito ai sensi dell'articolo 37 del regolamento (UE) n. 1095/2010 del Parlamento europeo e del Consiglio ([5]).

(30) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([6]), il Garante europeo della protezione dei dati è stato consultato e ha espresso un parere il 20 agosto 2024,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

(1) «team di controllo»: il team composto dal personale dell'entità finanziaria sottoposta a test e, se pertinente in considerazione dell'ambito di applicazione del TLPT, dal personale dei suoi fornitori terzi di servizi e da qualsiasi altra parte, che gestisce il test;

(2) «responsabile del team di controllo»: il membro del personale dell'entità finanziaria responsabile della conduzione di tutte le attività relative al TLPT per l'entità finanziaria nel contesto di un determinato test;

(3) «blue team»: il personale dell'entità finanziaria e, se del caso, il personale dei fornitori terzi di servizi dell'entità finanziaria e di qualsiasi altra parte ritenuta pertinente in considerazione dell'ambito di applicazione del TLPT, e dei fornitori terzi di servizi dell'entità finanziaria, che difende l'uso dei sistemi informatici e di rete da parte di un'entità finanziaria mantenendo la propria posizione di sicurezza contro attacchi simulati o reali e che non è a conoscenza del TLPT;

(4) «compiti del blue team»: compiti generalmente svolti dal blue team, quali attività del centro operativo di sicurezza, servizi di infrastruttura delle TIC, servizi di helpdesk, servizi di gestione degli incidenti a livello operativo;

(5) «red team»: i soggetti incaricati dello svolgimento dei test, interni o esterni, di cui ci si avvale per un TLPT o assegnati a un TLPT;

(6) «purple teaming»: un'attività di test collaborativa che coinvolge sia i soggetti incaricati dello svolgimento dei test che il blue team;

([3]) Regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità bancaria europea), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/78/CE della Commissione (GU L 331 del 15.12.2010, pag. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Regolamento (UE) n. 1094/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità europea delle assicurazioni e delle pensioni aziendali e professionali), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/79/CE della Commissione (GU L 331 del 15.12.2010, pag. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Regolamento (UE) n. 1095/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità europea degli strumenti finanziari e dei mercati), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/77/CE della Commissione (GU L 331 del 15.12.2010, pag. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(7) «autorità competente per il TLPT»: una delle autorità seguenti:

a) l'autorità pubblica unica nel settore finanziario designata conformemente all'articolo 26, paragrafo 9, del regolamento (UE) 2022/2554;

b) l'autorità nel settore finanziario alla quale è delegato l'esercizio di alcuni o di tutti i compiti relativi ai TLPT conformemente all'articolo 26, paragrafo 10, del regolamento (UE) 2022/2554;

c) una qualsiasi delle autorità competenti di cui all'articolo 46 del regolamento (UE) 2022/2554;

(8) «team informatico TLPT»: il personale delle autorità competenti per il TLPT che ha la responsabilità delle questioni relative ai TLPT;

(9) «responsabili dei test»: il personale designato a dirigere le attività dell'autorità competente per il TLPT per uno specifico TLPT al fine di monitorare la conformità con il presente regolamento;

(10) «soggetti che forniscono analisi delle minacce»: gli esperti, incaricati dall'entità finanziaria per ciascun TLPT, ed esterni all'entità stessa e agli eventuali fornitori intragruppo di servizi TIC, che raccolgono ed esaminano analisi mirate sulle minacce pertinenti per le entità finanziarie nell'ambito di uno specifico esercizio di TLPT e sviluppano corrispondenti scenari di minaccia pertinenti e realistici;

(11) «fornitori di TLPT»: soggetti incaricati dello svolgimento dei test e soggetti che forniscono analisi delle minacce;

(12) «*leg-up*»: gli aiuti o le informazioni forniti dal team di controllo ai soggetti incaricati dello svolgimento dei test per consentire a questi ultimi di proseguire l'esecuzione di un percorso di attacco qualora non siano in grado di avanzare da soli e non esistano altre alternative ragionevoli, anche in caso di tempo o risorse insufficienti in un dato TLPT;

(13) «percorso di attacco»: il percorso seguito dai soggetti incaricati dello svolgimento dei test durante la fase attiva di test red team del TLPT per raggiungere i *flag* specificati per tale TLPT;

(14) «*flag*»: obiettivi chiave nei sistemi di TIC a supporto di funzioni essenziali o importanti di un'entità finanziaria che i soggetti incaricati dello svolgimento dei test cercano di conseguire attraverso il test;

(15) «informazioni sensibili»: informazioni che possono essere facilmente sfruttate per compiere attacchi contro i sistemi di TIC dell'entità finanziaria, la proprietà intellettuale, i dati commerciali riservati o i dati personali, che possono danneggiare, direttamente o indirettamente, l'entità finanziaria e il suo ecosistema qualora finissero nelle mani di soggetti malintenzionati;

(16) «*pool*»: tutte le entità finanziarie che partecipano a un TLPT congiunto a norma dell'articolo 26, paragrafo 4, del regolamento (UE) 2022/2554;

(17) «Stato membro ospitante»: lo Stato membro ospitante conformemente al diritto settoriale dell'Unione applicabile a ciascuna entità finanziaria;

(18) «TLPT comune»: un TLPT, diverso da un TLPT congiunto di cui all'articolo 26, paragrafo 4, del regolamento (UE) 2022/2554, che coinvolge più entità finanziarie che utilizzano lo stesso fornitore intragruppo di servizi TIC oppure che appartengono allo stesso gruppo e condividono sistemi di TIC.

Articolo 2

Identificazione delle entità finanziarie che hanno l'obbligo di svolgere TLPT

1. Le autorità competenti per i TLPT valutano se un'entità finanziaria ha l'obbligo di svolgere TLPT, tenendo conto dell'impatto di tali entità finanziarie, del loro carattere sistemico e del loro profilo dei rischi informatici, sulla base di tutti i criteri seguenti:

a) fattori correlati all'impatto e al carattere sistemico:

i) le dimensioni dell'entità finanziaria, determinate in base al fatto che l'entità finanziaria fornisca servizi finanziari in uno o più Stati membri e confrontando le attività dell'entità finanziaria con quelle di altre entità finanziarie che forniscono servizi analoghi;

ii) la portata e la natura dell'interconnessione dell'entità finanziaria con altre entità finanziarie del settore finanziario in uno o più Stati membri;

iii) la criticità o l'importanza dei servizi che l'entità finanziaria fornisce al settore finanziario;

iv) la sostituibilità dei servizi che l'entità finanziaria fornisce;

v) la complessità del modello aziendale dell'entità finanziaria e dei relativi servizi e processi;

vi) se l'entità finanziaria fa parte di un gruppo di carattere sistemico a livello dell'Unione o nazionale nel settore finanziario e che condivide sistemi di TIC;

b) fattori correlati ai rischi informatici:

i) il profilo di rischio dell'entità finanziaria;

ii) il panorama delle minacce dell'entità finanziaria;

iii) il grado di dipendenza delle funzioni essenziali o importanti o delle relative funzioni di supporto dell'entità finanziaria da processi e sistemi di TIC;

iv) la complessità dell'architettura delle TIC dell'entità finanziaria;

v) le funzioni e i servizi TIC supportati da fornitori terzi di servizi TIC nonché la quantità e il tipo di accordi contrattuali con i fornitori terzi di servizi TIC o con i fornitori intragruppo di servizi TIC;

vi) i risultati di eventuali esami di vigilanza pertinenti per la valutazione della maturità delle TIC dell'entità finanziaria;

vii) la maturità dei piani di continuità operativa delle TIC e dei piani di risposta e ripristino relativi alle TIC;

viii) la maturità delle misure operative di individuazione e attenuazione per la sicurezza delle TIC, compresa la capacità di:

1) monitorare l'infrastruttura delle TIC dell'entità finanziaria in maniera permanente;

2) individuare gli eventi connessi alle TIC in tempo reale;

3) analizzare gli eventi di cui al punto 2);

4) reagire agli eventi di cui al punto 2) in modo tempestivo ed efficace;

ix) se l'entità finanziaria fa parte di un gruppo attivo nel settore finanziario a livello dell'Unione o nazionale che condivide sistemi di TIC.

Ai fini della lettera a), punto i), l'autorità competente per il TLPT prende in considerazione, ove possibile:

a) la posizione in termini di quota di mercato dell'entità finanziaria a livello dell'Unione e nazionale;

b) la gamma di attività offerte dall'entità finanziaria;

c) la quota di mercato dei servizi forniti dall'entità finanziaria o delle attività intraprese a livello dell'Unione e nazionale.

Ai fini della lettera a), punto v), l'autorità competente per il TLPT prende in considerazione, ove possibile:

a) se l'entità finanziaria gestisce più di un modello aziendale;

b) l'interconnessione dei diversi processi aziendali e dei relativi servizi.

2. Le autorità competenti per i TLPT impongono a tutte le seguenti entità finanziarie di svolgere TLPT, a meno che dalla valutazione di cui al paragrafo 1 in relazione a un'entità finanziaria emerga che il suo impatto, i problemi di stabilità finanziaria relativi a tale entità finanziaria o il suo profilo dei rischi informatici non giustificano lo svolgimento di un TLPT:

a) enti creditizi che soddisfano una delle condizioni seguenti:

i) sono stati individuati come enti a rilevanza sistemica a livello globale (G-SII) conformemente all'articolo 131 della direttiva 2013/36/UE del Parlamento europeo e del Consiglio ([7]);

ii) sono stati individuati come altri enti a rilevanza sistemica («O-SII») conformemente all'articolo 131, paragrafi 1 e 3, della direttiva 2013/36/UE;

iii) fanno parte di G-SII o O-SII;

([7]) Direttiva 2013/36/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE (GU L 176 del 27.6.2013, pag. 338, ELI: http:/data.europa.eu/eli/dir/2013/36/oj).

b) istituti di pagamento che, in ciascuno dei due anni civili precedenti la valutazione da parte dell'autorità competente per il TLPT, hanno superato i 150 miliardi di EUR di valore complessivo delle operazioni di pagamento quali definite all'articolo 4, punto 5), della direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio ([8]);

c) istituti di moneta elettronica che, in ciascuno dei due anni civili precedenti la valutazione da parte dell'autorità competente per il TLPT, hanno superato i 150 miliardi di EUR di valore complessivo delle operazioni di pagamento quali definite all'articolo 4, punto 5), della direttiva (UE) 2015/2366 oppure i 40 miliardi di EUR di valore complessivo dell'importo della moneta elettronica in circolazione;

d) depositari centrali di titoli;

e) controparti centrali;

f) sedi di negoziazione dotate di un sistema elettronico di negoziazione che soddisfano uno dei criteri seguenti:

i) la sede di negoziazione detiene la quota di mercato più elevata in termini di volume degli scambi a livello nazionale in ciascuno dei due anni civili precedenti la valutazione da parte dell'autorità competente per il TLPT in relazione a uno degli elementi seguenti:

(1) valori mobiliari quali definiti all'articolo 4, paragrafo 1, punto 44), lettera a), della direttiva 2014/65/UE del Parlamento europeo e del Consiglio ([9]);

(2) valori mobiliari quali definiti all'articolo 4, paragrafo 1, punto 44), lettera b), della direttiva 2014/65/UE;

(3) strumenti derivati quali definiti all'articolo 2, paragrafo 1, punto 29), del regolamento (UE) n. 600/2014 del Parlamento europeo e del Consiglio ([10]);

(4) strumenti finanziari strutturati quali definiti all'articolo 2, paragrafo 1, punto 28), del regolamento (UE) n. 600/2014;

(5) quote di emissioni quali definite all'allegato I, sezione C, punto 11), della direttiva 2014/65/UE del Parlamento europeo e del Consiglio;

ii) la sede di negoziazione detiene una quota di mercato in termini di volume degli scambi a livello dell'Unione superiore al 5 % in ciascuno dei due anni civili precedenti la valutazione da parte dell'autorità competente per il TLPT, in relazione a uno degli elementi seguenti:

(1) azioni di società e altri titoli equivalenti ad azioni di società, di partnership o di altri soggetti e certificati di deposito azionario;

(2) obbligazioni o altri titoli di debito, compresi i certificati di deposito relativi a tali titoli;

(3) strumenti derivati quali definiti all'articolo 2, paragrafo 1, punto 29), del regolamento (UE) n. 600/2014;

(4) strumenti finanziari strutturati quali definiti all'articolo 2, paragrafo 1, punto 28), del regolamento (UE) n. 600/2014;

(5) quote di emissioni quali definite all'allegato I, sezione C, punto 11), della direttiva 2014/65/UE;

([8]) Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE (GU L 337 del 23.12.2015, pag. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

([9]) Direttiva 2014/65/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE (rifusione) (GU L 173 del 12.6.2014, pag. 349, ELI: http://data.europa.eu/eli/dir/2014/65/oj).

([10]) Regolamento (UE) n. 600/2014 del Parlamento europeo e del Consiglio, del 15 maggio 2014, sui mercati degli strumenti finanziari e che modifica il regolamento (UE) n. 648/2012 (GU L 173 del 12.6.2014, pag. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

g) imprese di assicurazione e di riassicurazione che soddisfano tutti i criteri seguenti:

i) hanno un premio lordo contabilizzato superiore a 1 500 000 000 EUR;

ii) hanno riserve tecniche superiori a 10 000 000 000 EUR;

iii) imprese di assicurazione che svolgono attività solo nel settore vita o che svolgono attività in entrambi i settori vita e non-vita e che detengono attività totali superiori al 3,5 % della somma delle attività totali, valutate conformemente all'articolo 75 della direttiva 2009/138/CE del Parlamento europeo e del Consiglio ([11]), delle imprese di assicurazione e di riassicurazione stabilite nello Stato membro.

Ai fini della lettera f), punto ii), se la sede di negoziazione fa parte di un gruppo che condivide sistemi di TIC oppure lo stesso fornitore intragruppo di servizi TIC, si considera il volume degli scambi relativi a titoli e contratti derivati in tutte le sedi di negoziazione appartenenti allo stesso gruppo e stabilite nell'Unione.

Ai fini della lettera g), le autorità competenti per i TLPT individuano un sottoinsieme di tutte le imprese di assicurazione e di riassicurazione applicando i criteri di cui alla lettera g), punti i), ii) e iii). Le imprese di assicurazione e di riassicurazione incluse in tale sottoinsieme hanno l'obbligo di svolgere TLPT se anch'esse soddisfano uno dei criteri seguenti:

a) premio lordo contabilizzato superiore a 3 000 000 000 EUR;

b) riserve tecniche superiori a 30 000 000 000 EUR;

c) attività totali che superano il 10 % della somma delle attività totali, valutate conformemente all'articolo 75 della direttiva 2009/138/CE, delle imprese di assicurazione e di riassicurazione stabilite nello Stato membro.

3. Se più di un'entità finanziaria appartenente allo stesso gruppo e che condivide sistemi di TIC o se più di un'entità finanziaria che utilizza lo stesso fornitore intragruppo di servizi TIC soddisfano i criteri di cui al paragrafo 2, le autorità competenti per i TLPT di tali entità finanziarie decidono, conformemente all'articolo 16, paragrafo 2, se l'obbligo di svolgere TLPT su base individuale sia pertinente per tali entità finanziarie.

Se l'autorità competente per il TLPT dell'impresa madre di un gruppo di entità finanziarie di cui al primo comma è diversa dalle autorità competenti per i TLPT delle entità finanziarie del gruppo, tale autorità è consultata dalle autorità competenti per i TLPT delle entità finanziarie appartenenti a tale gruppo in merito all'opportunità di svolgere TLPT su base individuale.

Articolo 3

Team informatico TLPT e responsabili dei test nell'ambito dei TLPT

1. Un'autorità competente per il TLPT attribuisce a un team informatico TLPT la responsabilità di coordinare le attività relative ai TLPT. Un team informatico TLPT è composto da responsabili dei test incaricati di supervisionare un singolo TLPT.

2. Per ogni test, l'autorità competente per il TLPT designa un responsabile del test e almeno un sostituto.

3. I responsabili dei test controllano e garantiscono che siano rispettate le prescrizioni di cui al presente regolamento.

([11]) Direttiva 2009/138/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, in materia di accesso ed esercizio delle attività di assicurazione e di riassicurazione (solvibilità II) (GU L 335 del 17.12.2009, pag. 1, ELI: http://data.europa.eu/eli/dir/2009/138/oj).

4. Il responsabile del test comunica i dati di contatto del team informatico TLPT all'entità finanziaria mediante la notifica di cui all'articolo 9, paragrafo 1.

5. L'autorità competente per il TLPT partecipa a tutte le fasi del TLPT.

Articolo 4

Disposizioni organizzative per le entità finanziarie

1. Le entità finanziarie nominano un responsabile del team di controllo che ha la responsabilità della gestione quotidiana del TLPT e delle decisioni e azioni del team di controllo.

2. Le entità finanziarie definiscono misure organizzative e procedurali per garantire che:

a) l'accesso alle informazioni relative a qualsiasi TLPT pianificato o in corso sia limitato, in base alla necessità di sapere, al team di controllo, all'organo di gestione, ai soggetti incaricati dello svolgimento dei test, al soggetto che fornisce analisi delle minacce e all'autorità competente per il TLPT;

b) il team di controllo consulti i responsabili dei test prima di coinvolgere qualsiasi membro del blue team in un TLPT;

c) il team di controllo sia informato di qualsiasi rilevamento del TLPT da parte di membri del personale dell'entità finanziaria o dei suoi fornitori terzi di servizi; in caso di escalation della conseguente risposta all'incidente, se necessario, il team di controllo contenga tale escalation;

d) siano presenti disposizioni relative alla segretezza del TLPT, applicabili al personale dell'entità finanziaria, al personale dei fornitori terzi di servizi TIC interessati, ai soggetti incaricati dello svolgimento dei test e al soggetto che fornisce analisi delle minacce;

e) il team di controllo fornisca ai responsabili dei test, su richiesta, tutte le informazioni relative al TLPT;

f) ove possibile, le parti coinvolte nel TLPT facciano riferimento a quest'ultimo utilizzando solo il nome in codice.

Articolo 5

Gestione dei rischi per i TLPT

1. Durante la fase di preparazione di cui all'articolo 9, il team di controllo valuta i rischi associati al sottoporre a test sistemi di produzione attivi di funzioni essenziali o importanti dell'entità finanziaria, compresi i potenziali impatti su quanto segue:

a) il settore finanziario:

b) la stabilità finanziaria a livello dell'Unione o nazionale.

Il team di controllo esamina tali impatti per tutta la durata del test.

2. Ai fini della valutazione e della gestione dei rischi, il team di controllo tiene conto almeno dei seguenti tipi di rischi riguardanti:

a) la concessione dell'accesso a informazioni sensibili sull'entità finanziaria al soggetto che fornisce analisi delle minacce e ai soggetti incaricati dello svolgimento dei test esterni, se del caso;

b) la mancata conformità del TLPT al regolamento (UE) 2022/2554 e al presente regolamento qualora tale mancata conformità si traduca nell'assenza dell'attestato di cui all'articolo 26, paragrafo 7, del regolamento (UE) 2022/2554, anche quando tale mancata conformità è dovuta a violazioni della riservatezza del TLPT o a una condotta non etica;

c) l'escalation di crisi e incidenti;

d) la fase attiva del red team, compresi i rischi connessi all'interruzione delle attività critiche e alla corruzione dei dati dovuta alle attività dei soggetti incaricati dello svolgimento dei test, e il suo potenziale impatto su terzi;

e) l'attività del blue team, compresi i rischi connessi all'interruzione delle attività critiche e alla corruzione dei dati dovuta alle attività del blue team, e il suo potenziale impatto su terzi;

f) il ripristino incompleto dei sistemi interessati dal TLPT.

Articolo 6

Gestione dei rischi per i TLPT congiunti o comuni

1. Nel caso di un TLPT comune o di un TLPT congiunto, il team di controllo di ciascuna entità finanziaria effettua la propria valutazione dei rischi e definisce le proprie misure di gestione dei rischi.

2. Il team di controllo dell'entità finanziaria designata di cui all'articolo 16, paragrafo 3, lettera b), del presente regolamento, o l'entità finanziaria designata a norma dell'articolo 26, paragrafo 4, del regolamento (UE) 2022/2554, valuta i rischi relativi al coinvolgimento di più entità finanziarie nel TLPT. I team di controllo delle entità finanziarie coinvolte cooperano con il team di controllo dell'entità finanziaria designata al fine di identificare potenziali rischi comuni.

Articolo 7

Selezione dei fornitori di TLPT

1. Il team di controllo adotta misure per gestire i rischi relativi al TLPT e garantisce in particolare che, per ciascun TLPT:

a) il soggetto che fornisce analisi delle minacce e i soggetti incaricati dello svolgimento dei test esterni forniscano al team di controllo un curriculum vitae dettagliato e copie di certificazioni che, secondo gli standard di mercato riconosciuti, sono adeguate allo svolgimento delle loro attività;

b) il soggetto che fornisce analisi delle minacce e i soggetti incaricati dello svolgimento dei test esterni siano debitamente e pienamente coperti da un'assicurazione di responsabilità professionale adeguata, anche contro i rischi di colpa e negligenza;

c) il soggetto che fornisce analisi delle minacce fornisca almeno tre referenze relative a precedenti incarichi nel contesto dei test di penetrazione e dei test red team;

d) i soggetti incaricati dello svolgimento dei test esterni forniscano almeno cinque referenze relative a precedenti incarichi riguardanti test di penetrazione e test red team;

e) il personale del soggetto che fornisce analisi delle minacce assegnato al TLPT:

   i) sia composto da almeno un responsabile con minimo cinque anni di esperienza nell'analisi delle minacce e da almeno un altro membro con minimo due anni di esperienza nell'analisi delle minacce;

   ii) presenti un'ampia gamma e un livello adeguato di conoscenze e competenze professionali, tra cui:

      1) tattiche, tecniche e procedure per la raccolta di informazioni;

      2) conoscenze geopolitiche, tecniche e settoriali;

      3) adeguate capacità di comunicazione per presentare chiaramente i risultati dell'impegno e riferire in merito;

   iii) abbia partecipato in totale ad almeno tre precedenti incarichi di analisi delle minacce nel contesto dei test di penetrazione e dei test red team;

   iv) non svolga simultaneamente compiti appartenenti al blue team o altri servizi che possono presentare un conflitto di interessi nei confronti dell'entità finanziaria, del fornitore terzo di servizi di TIC o di un fornitore intragruppo di servizi TIC coinvolto nel TLPT cui è assegnato;

   v) sia separato dal personale dello stesso fornitore di TLPT che fornisce soggetti incaricati dello svolgimento dei test esterni per lo stesso TLPT, e non faccia capo a tale personale;

f) per i soggetti incaricati dello svolgimento dei test esterni, il red team assegnato al TLPT:

i) sia composto da almeno un responsabile, con minimo cinque anni di esperienza in test di penetrazione e test red team, nonché da almeno due ulteriori soggetti incaricati dello svolgimento dei test, ciascuno con minimo due anni di esperienza in test di penetrazione e test red team;

ii) presenti un'ampia gamma e un livello adeguato di conoscenze e competenze professionali, comprese conoscenze sull'attività dell'entità finanziaria, in materia di ricognizione (*reconnaissance*), gestione dei rischi, sviluppo di *exploit*, penetrazione fisica, ingegneria sociale, analisi delle vulnerabilità, nonché adeguate capacità di comunicazione per presentare chiaramente i risultati dell'impegno e riferire in merito;

iii) abbia partecipato in maniera combinata ad almeno cinque precedenti incarichi riguardanti test di penetrazione e test red team;

iv) non sia alle dipendenze di un soggetto che fornisce analisi delle minacce che svolge simultaneamente compiti appartenenti al blue team per un'entità finanziaria, un fornitore terzo di servizi TIC o un fornitore intragruppo di servizi TIC coinvolto nel TLPT, né fornisca servizi a tale soggetto;

v) sia separato dal personale dello stesso fornitore di TLPT che fornisce contemporaneamente servizi di analisi delle minacce per lo stesso TLPT;

g) i soggetti incaricati dello svolgimento dei test e il soggetto che fornisce analisi delle minacce eseguano procedure di ripristino al termine dei test, anche per quanto riguarda la cancellazione sicura delle informazioni relative a password, credenziali e altre chiavi segrete compromesse durante il TLPT, la comunicazione sicura alle entità finanziarie dei conti compromessi, la raccolta, l'archiviazione, la gestione e l'eliminazione sicure di altri dati raccolti durante il test;

h) i soggetti incaricati dello svolgimento dei test, oltre alle procedure di ripristino al termine dei test di cui alla lettera g), eseguano le procedure di ripristino seguenti:

i) disattivazione del comando e del controllo;

ii) attivazione di meccanismi di emergenza (*kill switch*) riguardanti ambito di applicazione e data;

iii) rimozione di *backdoor* e altri malware;

iv) notifica della potenziale violazione;

v) procedure per il ripristino futuro di back-up che possono riguardare malware o strumenti installati durante il test;

vi) monitoraggio delle attività del blue team e comunicazione al team di controllo di eventuali rilevamenti;

i) i soggetti incaricati dello svolgimento dei test e il soggetto che fornisce analisi delle minacce non svolgano alcuna delle attività seguenti, né vi prendano parte:

i) distruzione non autorizzata delle attrezzature dell'entità finanziaria e degli eventuali fornitori terzi di servizi TIC;

ii) modifica incontrollata delle informazioni e delle risorse TIC dell'entità finanziaria e degli eventuali fornitori terzi di servizi TIC;

iii) compromissione intenzionale della continuità di funzioni essenziali o importanti dell'entità finanziaria;

iv) inclusione non autorizzata di sistemi esterni all'ambito di applicazione;

v) divulgazione non autorizzata dei risultati dei test.

2. Il team di controllo registra la documentazione fornita dai soggetti incaricati dello svolgimento dei test e dai soggetti che forniscono analisi delle minacce per dimostrare la conformità con il paragrafo 1, lettere da a) a f).

In circostanze eccezionali, le entità finanziarie possono avvalersi di soggetti incaricati dello svolgimento dei test esterni e di soggetti che forniscono analisi delle minacce che non soddisfano uno o più dei requisiti di cui al paragrafo 1, lettere da a) a f), a condizione che tali entità finanziarie adottino misure adeguate per attenuare i rischi connessi alla mancata conformità con tali punti e registrino tali misure.

Articolo 8

Specificità per i TLPT comuni o congiunti

1. Salvo diversa decisione dell'autorità capofila competente per il TLPT, se più entità finanziarie, identificate a norma dell'articolo 16, paragrafo 2 o 4, sono coinvolte in un TLPT comune o congiunto, ciascuna entità finanziaria segue ognuna delle fasi di cui agli articoli da 9 a 15.

2. Salvo disposizione contraria del presente regolamento, se diverse autorità competenti per i TLPT sono coinvolte in un TLPT comune o in un TLPT congiunto di cui all'articolo 16, paragrafo 3 o 5, i riferimenti contenuti negli articoli da 9 a 15 all'«autorità competente per il TLPT» sono da intendersi come riferimenti all'autorità capofila competente per il TLPT per tale TLPT comune o congiunto.

Articolo 9

Fase di preparazione

1. Un'entità finanziaria identificata a norma dell'articolo 26, paragrafo 8, terzo comma, del regolamento (UE) 2022/2554 avvia un TLPT a seguito di una notifica circa la necessità di condurre un TLTP da parte dell'autorità competente per il TLPT.

2. Entro tre mesi dal ricevimento della notifica di cui al paragrafo 1, l'entità finanziaria trasmette ai responsabili dei test tutte le informazioni seguenti relative all'avvio del TLPT:

a) una carta del progetto comprendente un piano di progetto ad alto livello, contenente le informazioni di cui all'allegato I;

b) i recapiti del responsabile del team di controllo;

c) informazioni sull'uso previsto di soggetti incaricati dello svolgimento dei test interni o esterni o di entrambi, se del caso come specificato all'articolo 15;

d) informazioni sui canali di comunicazione da utilizzare durante il TLPT;

e) il nome in codice del TLPT.

3. Se le informazioni di cui al paragrafo 2, lettere da a) a e), sono complete e garantiscono l'idoneità e lo svolgimento efficace del TLPT, l'autorità competente per il TLPT convalida le informazioni di avvio del TLPT dell'entità finanziaria e ne informa quest'ultima.

4. A seguito della convalida delle informazioni relative all'avvio del TLPT da parte dell'autorità competente per il TLPT, l'entità finanziaria istituisce un team di controllo per coadiuvare il responsabile del team di controllo nei compiti seguenti:

a) specificare i canali e i processi di comunicazione all'interno del team di controllo, con i soggetti incaricati dello svolgimento dei test e i soggetti che forniscono analisi delle minacce in tutte le questioni relative al TLPT;

b) informare l'organo di gestione dell'entità finanziaria in merito ai progressi del TLPT e ai rischi connessi;

c) adottare decisioni basate sulle competenze in materia durante tutto il TLPT;

d) eseguire il TLPT conformemente al presente regolamento;

e) selezionare il soggetto che fornisce analisi delle minacce per il TLPT;

f) selezionare i soggetti incaricati dello svolgimento dei test esterni, i soggetti incaricati dello svolgimento dei test interni o entrambi;

g) preparare il documento contenente le specifiche relative all'ambito di applicazione.

5. Se ritiene che la composizione iniziale del team di controllo e le eventuali modifiche successive siano adeguate per lo svolgimento dei compiti di cui al paragrafo 4, l'autorità competente per il TLPT convalida il team di controllo e ne informa il relativo responsabile.

6. L'entità finanziaria presenta ai responsabili dei test un documento relativo alle specifiche dell'ambito di applicazione contenente tutte le informazioni di cui all'allegato II entro sei mesi dal ricevimento della notifica da parte dell'autorità competente per il TLPT di cui al paragrafo 1. L'organo di gestione dell'entità finanziaria approva il documento relativo alle specifiche dell'ambito di applicazione.

7. Ai fini dell'inclusione di funzioni essenziali o importanti nell'ambito di applicazione del TLPT, le entità finanziarie prendono in considerazione i criteri seguenti:

a) l'essenzialità o l'importanza della funzione e il suo possibile impatto sul settore finanziario e sulla stabilità finanziaria a livello dell'Unione e nazionale;

b) l'importanza della funzione per l'operatività quotidiana dell'entità finanziaria;

c) l'intercambiabilità della funzione;

d) l'interconnessione con altre funzioni;

e) l'ubicazione geografica della funzione;

f) la dipendenza settoriale di altre entità dalla funzione;

g) se disponibili, analisi delle minacce riguardanti la funzione.

8. Dopo che i soggetti incaricati dello svolgimento dei test e i soggetti che forniscono analisi delle minacce hanno ricevuto l'incarico, il team di controllo condivide con loro le informazioni sull'avvio del TLPT e il documento relativo alle specifiche dell'ambito di applicazione. Il team di controllo informa i soggetti incaricati dello svolgimento dei test e i soggetti che forniscono analisi delle minacce in merito al processo di test da seguire.

9. L'entità finanziaria garantisce che l'acquisizione o l'assegnazione di soggetti incaricati dello svolgimento dei test e di soggetti che forniscono analisi delle minacce sia ultimata prima dell'inizio della fase di test.

10. Prima dell'inizio della fase di test, il team di controllo consulta i responsabili dei test in merito alla valutazione dei rischi relativi al TLPT e alle relative misure di gestione dei rischi. Se l'autorità competente per il TLPT ritiene che la valutazione dei rischi o le misure di gestione dei rischi non affrontino adeguatamente i rischi relativi al TLPT, il team di controllo provvede a riesaminarle.

11. Il team di controllo valuta se i soggetti che forniscono analisi delle minacce e i soggetti incaricati dello svolgimento dei test che si intende coinvolgere nel TLPT soddisfano i requisiti di cui all'articolo 27 del regolamento (UE) 2022/2554 e all'articolo 7, paragrafo 1, del presente regolamento e documenta l'esito di tale valutazione. Il team di controllo seleziona i soggetti che forniscono analisi delle minacce conformemente a tale valutazione e alle sue pratiche di gestione dei rischi. Prima di avvalersi dei soggetti che forniscono analisi delle minacce e dei soggetti incaricati dello svolgimento dei test esterni selezionati, il team di controllo fornisce ai responsabili dei test prove del fatto che tali soggetti che forniscono analisi delle minacce e soggetti incaricati dello svolgimento dei test soddisfano i requisiti di cui all'articolo 27 del regolamento (UE) 2022/2554 e all'articolo 7, paragrafo 1, del presente regolamento. Il team di controllo non si avvale dei soggetti che forniscono analisi delle minacce e dei soggetti incaricati dello svolgimento dei test esterni selezionati se l'autorità competente per il TLPT ritiene che i soggetti che forniscono analisi delle minacce e i soggetti incaricati dello svolgimento dei test esterni selezionati non soddisfino i requisiti di cui all'articolo 27 del regolamento (UE) 2022/2554, i requisiti di cui all'articolo 7, paragrafo 1, del presente regolamento o requisiti supplementari derivanti da normative nazionali in materia di sicurezza conformemente al diritto dell'Unione, o qualora l'entità finanziaria non rispetti l'articolo 7, paragrafo 2, primo comma, del presente regolamento, o qualora non siano soddisfatte le circostanze di cui all'articolo 7, paragrafo 2, secondo comma, del presente regolamento.

12. Se il documento relativo alle specifiche dell'ambito di applicazione è completo e garantisce lo svolgimento di un TLPT adeguato ed efficace, l'autorità competente per il TLPT approva tale documento e ne informa il responsabile del team di controllo.

Articolo 10

Fase di test: analisi delle minacce

1. A seguito dell'approvazione del documento relativo alle specifiche dell'ambito di applicazione da parte dell'autorità competente per il TLPT, il soggetto che fornisce analisi delle minacce esamina le analisi delle minacce generiche e settoriali pertinenti per l'entità finanziaria. Se l'autorità competente per il TLPT ha fornito un panorama delle minacce generico per il settore finanziario di uno Stato membro, il soggetto che fornisce analisi delle minacce può utilizzare tale panorama come base di riferimento per il panorama delle minacce nazionale. Il soggetto che fornisce analisi delle minacce individua le minacce informatiche nonché le vulnerabilità esistenti o potenziali riguardanti l'entità finanziaria. Inoltre il soggetto che fornisce analisi delle minacce raccoglie informazioni in merito ad analisi delle minacce e dei bersagli riguardanti l'entità finanziaria che siano concrete, fruibili e contestualizzate e provvede ad esaminarle, anche consultando il team di controllo e i responsabili dei test.

2. Il soggetto che fornisce analisi delle minacce presenta le minacce e le analisi mirate delle minacce pertinenti e propone gli scenari necessari al team di controllo, ai soggetti incaricati dello svolgimento dei test e ai responsabili dei test. Gli scenari proposti differiscono per quanto riguarda gli autori identificati delle minacce nonché le tattiche, tecniche e procedure associate e sono rivolti a ciascuna funzione essenziale o importante nell'ambito di applicazione del TLPT.

3. Il responsabile del team di controllo seleziona almeno tre scenari per condurre il TLPT sulla base di tutti gli elementi seguenti:

a) la raccomandazione del soggetto che fornisce analisi delle minacce e la natura guidata dalla minaccia di ciascuno scenario;

b) il contributo fornito dai responsabili dei test;

c) la fattibilità degli scenari proposti per l'esecuzione, sulla base del giudizio esperto dei responsabili dei test;

d) le dimensioni, la complessità e il profilo di rischio complessivo dell'entità finanziaria nonché la natura, la portata e la complessità dei suoi servizi, delle sue attività e della sua operatività.

4. Al massimo uno degli scenari selezionati può non essere guidato dalla minaccia e può basarsi su una minaccia futura e potenzialmente fittizia con un elevato valore predittivo, anticipativo, opportunistico o prospettico, in considerazione degli sviluppi previsti del panorama delle minacce riguardante l'entità finanziaria.

Per i TLPT congiunti, fatti salvi gli scenari che riguardano direttamente le funzioni essenziali o importanti delle entità finanziarie coinvolte nei test, almeno uno scenario comprende i pertinenti sistemi, processi e tecnologie TIC sottostanti del fornitore terzo di servizi TIC a supporto delle funzioni essenziali o importanti delle entità finanziarie che rientrano nell'ambito di applicazione.

Se il test è un TLPT comune che coinvolge un fornitore intragruppo di servizi TIC, fatti salvi gli scenari che riguardano direttamente le funzioni essenziali o importanti delle entità finanziarie coinvolte nel test, almeno uno scenario comprende i pertinenti sistemi, processi e tecnologie TIC sottostanti del fornitore intragruppo di servizi TIC a supporto delle funzioni essenziali o importanti delle entità finanziarie che rientrano nell'ambito di applicazione.

5. Il soggetto che fornisce analisi delle minacce trasmette la relazione sull'analisi mirata delle minacce al team di controllo, compresi gli scenari selezionati conformemente ai paragrafi 3 e 4. La relazione sull'analisi delle minacce contiene le informazioni di cui all'allegato III.

6. Il team di controllo sottopone la relazione sull'analisi mirata delle minacce all'approvazione del responsabile dei test. Se la relazione sull'analisi mirata delle minacce è completa e garantisce lo svolgimento di un TLPT efficace, l'autorità competente per il TLPT approva la relazione sull'analisi mirata delle minacce e il responsabile del team di controllo

Articolo 11

Fase di test: test red team

1. A seguito dell'approvazione della relazione sull'analisi mirata delle minacce da parte dell'autorità competente per il TLPT, i soggetti incaricati dello svolgimento dei test preparano il piano relativo al test red team che contiene le informazioni di cui all'allegato IV. I soggetti incaricati dello svolgimento dei test utilizzano il documento relativo alle specifiche dell'ambito di applicazione e la relazione sull'analisi mirata delle minacce come base per l'elaborazione degli scenari di attacco.

2. I soggetti incaricati dello svolgimento dei test consultano il team di controllo, il soggetto che fornisce analisi delle minacce e i responsabili dei test in merito al piano relativo al test red team, comprese le disposizioni in materia di comunicazione, procedure e gestione del progetto, la preparazione e i casi d'uso per l'attivazione dei *leg-up* e gli accordi di comunicazione al team di controllo e ai responsabili dei test.

3. Se il piano relativo al test red team è completo e garantisce lo svolgimento di un TLPT efficace, il team di controllo e l'autorità competente per il TLPT approvano il piano relativo al test red team e l'autorità competente per il TLPT ne informa il responsabile del team di controllo.

4. Una volta approvato il piano relativo al test red team conformemente al paragrafo 3, i responsabili dei test conducono il TLPT durante la fase attiva di test red team.

5. La durata della fase attiva di test red team è proporzionata all'ambito di applicazione del TLPT, alla portata, all'attività, alla complessità e al numero delle entità finanziarie e dei fornitori terzi o intragruppo di servizi TIC coinvolti nel TLPT e, in ogni caso, è di minimo 12 settimane. Gli scenari di attacco possono essere eseguiti in sequenza o contemporaneamente. Il team di controllo, il soggetto che fornisce analisi delle minacce, i soggetti incaricati dello svolgimento dei test e i responsabili dei test concordano la fine della fase attiva di test red team.

6. Fermo restando il presupposto che il piano relativo al test red team debba rimanere completo e consentire lo svolgimento di un TLPT efficace, il responsabile del team di controllo e i responsabili dei test approvano eventuali modifiche al piano relativo al test red team in seguito alla sua approvazione, anche per quanto riguarda le tempistiche, l'ambito di applicazione, i sistemi di bersagli o i *flag*.

7. Durante l'intera fase attiva di test red team, i soggetti incaricati dello svolgimento dei test riferiscono con cadenza almeno settimanale al team di controllo e ai responsabili dei test in merito ai progressi compiuti nel TLPT e il soggetto che fornisce analisi delle minacce rimane a disposizione a fini di consultazione e per fornire ulteriori analisi delle minacce su richiesta del team di controllo.

8. Il team di controllo fornisce tempestivamente *leg-up* concepiti sulla base del piano relativo al test red team. I *leg-up* possono essere aggiunti o adattati previa approvazione del team di controllo e dei responsabili dei test.

9. In caso di rilevamento delle attività di test da parte di qualsiasi membro del personale dell'entità finanziaria o dei suoi fornitori terzi di servizi di TIC o del suo fornitore intragruppo di servizi TIC, se del caso, il team di controllo, in consultazione con i soggetti incaricati dello svolgimento dei test e fatto salvo il paragrafo 10, propone e presenta ai responsabili dei test misure che consentano di proseguire il TLPT, garantendone nel contempo la segretezza, affinché possano convalidarle.

10. In circostanze eccezionali che comportano rischi di impatti sui dati, danni alle attività e perturbazioni delle funzioni essenziali o importanti, delle operazioni o dei servizi dell'entità finanziaria stessa, dei suoi fornitori terzi di servizi TIC o fornitori intragruppo di servizi TIC, oppure perturbazioni delle sue controparti o del settore finanziario, il responsabile del team di controllo può sospendere il TLPT o, in ultima istanza, qualora il proseguimento del TLPT non sia altrimenti possibile e previa convalida da parte dell'autorità competente per il TLPT, può proseguire il TLPT utilizzando un esercizio limitato di purple teaming. La durata dell'esercizio limitato di purple teaming è conteggiata ai fini del rispetto della durata minima di 12 settimane della fase attiva di test red team di cui al paragrafo 5.

Articolo 12

Fase di chiusura

1. Al termine della fase attiva di test red team, il responsabile del team di controllo informa il blue team dell'avvenuto TLPT.

2. Entro quattro settimane dalla fine della fase attiva di test red team, i soggetti incaricati dello svolgimento dei test presentano al team di controllo una relazione sul test red team contenente le informazioni di cui all'allegato V.

3. Il team di controllo fornisce senza indebito ritardo la relazione sul test red team al blue team e ai responsabili dei test.

Dietro richiesta dei responsabili dei test, la relazione di cui al primo comma non contiene informazioni sensibili.

4. Una volta ricevuta la relazione sul test red team ed entro 10 settimane dalla fine della fase attiva di test red team, il blue team presenta al team di controllo una relazione sul test blue team contenente le informazioni di cui all'allegato VI. Il team di controllo fornisce senza indebito ritardo la relazione sul test blue team ai soggetti incaricati dello svolgimento dei test e ai responsabili dei test.

Dietro richiesta dei responsabili dei test, la relazione di cui al primo comma non contiene informazioni sensibili.

5. Entro 10 settimane dalla fine della fase attiva di test red team, il blue team e i soggetti incaricati dello svolgimento dei test replicano le azioni offensive e difensive eseguite durante il TLPT. Il team di controllo esegue inoltre un esercizio di purple teaming su temi individuati di concerto dal blue team e dai soggetti incaricati dello svolgimento dei test, sulla base delle vulnerabilità individuate durante il test e, se del caso, su questioni che non hanno potuto essere sottoposte a test durante la fase attiva di test red team.

6. Al termine degli esercizi di replica e di purple teaming, il team di controllo, il blue team, i soggetti incaricati dello svolgimento dei test e i soggetti che forniscono analisi delle minacce scambiano reciprocamente riscontri sul processo di TLPT. I responsabili dei test possono fornire riscontri.

7. Dopo che l'autorità competente per il TLPT ha notificato al responsabile del team di controllo di aver accertato che la relazione sul test blue team e la relazione sul test red team contengono le informazioni di cui agli allegati V e VI, entro otto settimane l'entità finanziaria sottopone all'approvazione dell'autorità competente per il TLPT la relazione di sintesi delle pertinenti risultanze di cui all'articolo 26, paragrafo 6, del regolamento (UE) 2022/2554, contenente gli elementi di cui all'allegato VII.

Dietro richiesta dell'autorità competente per il TLPT, la relazione di cui al primo comma non contiene informazioni sensibili.

Articolo 13

Piano correttivo

1. Entro otto settimane dalla notifica di cui all'articolo 12, paragrafo 7, del presente regolamento, l'entità finanziaria trasmette i piani correttivi e la documentazione di cui all'articolo 26, paragrafo 6, del regolamento (UE) 2022/2554 all'autorità competente per il TLPT e, se diversa, all'autorità competente dell'entità finanziaria.

2. Il piano correttivo di cui al paragrafo 1 comprende, per ciascuna risultanza ottenuta nel quadro del TLPT:

a) una descrizione delle carenze individuate;

b) una descrizione delle misure correttive proposte, indicandone l'ordine di priorità e il completamento previsto, comprese, se del caso, misure volte a migliorare le capacità di identificazione, protezione, rilevamento e risposta;

c) un'analisi delle cause di fondo;

d) l'indicazione del personale o delle funzioni dell'entità finanziaria responsabili dell'attuazione delle misure correttive o dei miglioramenti proposti;

e) l'indicazione dei rischi associati alla mancata attuazione delle misure di cui alla lettera b) e, se del caso, dei rischi associati all'attuazione di tali misure.

Articolo 14

Attestato

1. L'attestato di cui all'articolo 26, paragrafo 7, del regolamento (UE) 2022/2554 contiene le informazioni di cui all'allegato VIII.

2 Se in un TLPT sono state coinvolte più autorità competenti per i TLPT, l'autorità capofila competente per il TLPT fornisce l'attestato di cui all'articolo 26, paragrafo 7, del regolamento (UE) 2022/2554 alle entità finanziarie sottoposte a test.

Articolo 15

Ricorso a soggetti incaricati dello svolgimento dei test interni

1. Le entità finanziarie mettono in atto tutte le modalità seguenti per il ricorso a soggetti incaricati dello svolgimento dei test interni:

a) l'istituzione e l'attuazione di una politica per la gestione dei soggetti incaricati dello svolgimento dei test interni in un TLPT;

b) l'adozione di misure volte a garantire che il ricorso a soggetti incaricati dello svolgimento dei test interni per eseguire un TLPT non abbia un impatto negativo sulle capacità generali di difesa o resilienza dell'entità finanziaria per quanto riguarda gli incidenti connessi alle TIC o non incida in modo significativo sulla disponibilità di risorse destinate a compiti connessi alle TIC durante un TLPT;

c) l'adozione di misure volte a garantire che i soggetti incaricati dello svolgimento dei test interni dispongano di risorse e capacità sufficienti per eseguire un TLPT.

La politica di cui alla lettera a):

a) contiene criteri per valutare l'idoneità, la competenza e i potenziali conflitti di interesse dei soggetti incaricati dello svolgimento dei test interni e specifica le responsabilità di gestione nel processo di test;

b) è documentata e riesaminata periodicamente;

c) prevede che il team interno incaricato dello svolgimento del test comprenda un responsabile del test e almeno altri due membri;

d) impone che tutti i membri del team incaricato dello svolgimento del test siano dipendenti dell'entità finanziaria o di un fornitore intragruppo di servizi TIC da almeno 12 mesi;

e) contiene disposizioni in materia di formazione sulle modalità di esecuzione dei test di penetrazione e dei test di red team per i soggetti incaricati dello svolgimento dei test interni.

2. Qualora approvi il ricorso a soggetti incaricati dello svolgimento dei test interni conformemente all'articolo 27, paragrafo 2, lettera a), del regolamento (UE) 2022/2554, l'autorità competente per il TLPT tiene conto dei requisiti di cui all'articolo 7, paragrafo 1, del presente regolamento.

3. Quando ricorre a soggetti incaricati dello svolgimento dei test interni, l'entità finanziaria garantisce che tale ricorso sia indicato nei documenti seguenti:

a) le informazioni relative all'avvio del test di cui all'articolo 9;

b) la relazione sul test red team di cui all'articolo 12, paragrafo 2;

c) la relazione di sintesi delle pertinenti risultanze del TLPT di cui all'articolo 26, paragrafo 6, del regolamento (UE) 2022/2554.

4. I soggetti incaricati dello svolgimento dei test che sono dipendenti di un fornitore intragruppo di servizi TIC sono considerati soggetti incaricati dello svolgimento dei test interni dell'entità finanziaria.

Articolo 16

Cooperazione e riconoscimento reciproco

1. Ai fini dello svolgimento di un TLPT in relazione a un'entità finanziaria che fornisce servizi in più di uno Stato membro, anche attraverso una succursale, la rispettiva autorità competente per il TLPT:

a) determina quali autorità competenti per i TLPT negli Stati membri ospitanti sono coinvolte, prendendo in considerazione se una o più funzioni essenziali o importanti sono svolte o condivise negli Stati membri ospitanti;

b) informa le autorità competenti per i TLPT identificate conformemente alla lettera a) della decisione di svolgere un TLPT sull'entità finanziaria;

c) salvo diversamente concordato dalle autorità competenti per i TLPT, l'autorità competente per il TLPT dell'entità finanziaria dirige il TLPT.

Entro 20 giorni lavorativi dal ricevimento delle informazioni sul futuro svolgimento di un TLPT, le autorità competenti per i TLPT degli Stati membri ospitanti possono manifestare il proprio interesse a seguire il TLPT in qualità di osservatori oppure incaricare un responsabile dei test affinché partecipi al TLPT. L'autorità capofila competente per il TLPT fornisce a tutte le autorità competenti per i TLPT che agiscono in qualità di osservatori nel TLPT il documento relativo alle specifiche dell'ambito di applicazione, la relazione di sintesi sul test, il piano correttivo e l'attestato.

L'autorità capofila competente per il TLPT coordina tutte le autorità competenti per i TLPT partecipanti durante l'intero test e adotta tutte le decisioni necessarie per svolgere il TLPT in modo adeguato ed efficace. L'autorità capofila competente per il TLPT può stabilire un numero massimo di autorità competenti per i TLPT partecipanti, qualora lo svolgimento del TLPT in maniera efficiente potrebbe risultare altrimenti compromesso.

2. Se un'entità finanziaria utilizza lo stesso fornitore intragruppo di servizi TIC di entità finanziarie stabilite in altri Stati membri, o appartiene a un gruppo e condivide sistemi di TIC con entità finanziarie dello stesso gruppo stabilite in altri Stati membri, l'autorità competente per il TLPT dell'entità finanziaria contatta le autorità competenti per i TLPT delle altre entità finanziarie che utilizzano lo stesso fornitore intragruppo di servizi TIC o condividono sistemi di TIC appartenenti al gruppo e valuta con esse la fattibilità e l'idoneità di svolgere un TLPT comune nei loro confronti. Un TLPT comune è da preferire a un TLPT individuale se consente una riduzione dei costi e delle risorse per le entità finanziarie e per le autorità competenti per i TLPT, purché la solidità e l'efficacia del test non siano compromesse.

3. Ai fini dello svolgimento di un TLPT comune:

a) le autorità competenti per i TLPT delle entità finanziarie concordano quale entità finanziaria è designata per condurre il TLPT, tenendo conto della struttura del gruppo e dell'efficienza del test;

b) l'autorità competente per il TLPT dell'entità finanziaria designata conformemente alla lettera a) dirige il TLPT, salvo diversamente concordato dalle autorità competenti per i TLPT delle entità finanziarie che partecipano al TLPT comune;

c) le autorità competenti per i TLPT delle entità finanziarie diverse dall'entità finanziaria designata per dirigere il TLPT comune possono manifestare il proprio interesse a seguire il TLPT in qualità di osservatori o assegnare un responsabile dei test a tale TLPT.

L'autorità capofila competente per il TLPT coordina tutte le autorità competenti per i TLPT coinvolte nel TLPT comune e adotta tutte le decisioni necessarie per svolgere il TLPT comune in modo corretto ed efficace.

4. Qualora un'entità finanziaria intenda condurre un TLPT congiunto di cui all'articolo 26, paragrafo 4, del regolamento (UE) 2022/2554, che potrebbe coinvolgere entità finanziarie stabilite in altri Stati membri, la rispettiva autorità competente per il TLPT contatta le autorità competenti per i TLPT delle altre entità finanziarie e valuta con esse la fattibilità e l'idoneità di svolgere un TLPT congiunto che le riguardi a norma dell'articolo 26, paragrafo 4, del regolamento (UE) 2022/2554.

5. Ai fini dello svolgimento di un TLPT congiunto di cui all'articolo 26, paragrafo 4, del regolamento (UE) 2022/2554:

a) le autorità competenti per i TLPT delle entità finanziarie concordano quale entità finanziaria designare per condurre il TLPT congiunto, tenendo conto dei servizi TIC forniti dal fornitore terzo di servizi TIC alle entità finanziarie e dell'efficienza del test;

b) l'autorità competente per il TLPT dell'entità finanziaria designata conformemente alla lettera a) dirige il TLPT, salvo diversamente concordato dalle autorità competenti per i TLPT delle entità finanziarie che partecipano al TLPT congiunto;

c) le autorità competenti per i TLPT delle entità finanziarie diverse dall'entità finanziaria designata per dirigere il TLPT congiunto possono manifestare il proprio interesse a seguire il TLPT in qualità di osservatori o assegnare un responsabile dei test a tale TLPT.

L'autorità capofila competente per il TLPT coordina tutte le autorità competenti per i TLPT coinvolte nel TLPT congiunto e adotta tutte le decisioni necessarie per svolgere il TLPT congiunto in modo corretto ed efficace.

6. Se, in relazione a un'entità finanziaria che ha l'obbligo di svolgere un TLPT, la rispettiva autorità competente per il TLPT è diversa dalla rispettiva autorità competente di cui all'articolo 46 del regolamento (UE) 2022/2554, tali autorità condividono tutte le informazioni pertinenti riguardanti tutte le questioni relative al TLPT ai fini dello svolgimento del TLPT o dell'esercizio delle loro funzioni conformemente a detto regolamento.

Articolo 17

Entrata in vigore

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 13 febbraio 2025

Per la Commissione
La presidente
Ursula VON DER LEYEN

ALLEGATO I

Contenuto della carta del progetto [articolo 9, paragrafo 2, lettera a)]

Tipo di informazione	Informazioni richieste
Responsabile del piano di progetto, ossia il responsabile del team di controllo	Nome Recapiti
Soggetti incaricati dello svolgimento dei test	☐ interni ☐ esterni ☐ entrambi
Canali di comunicazione selezionati conformemente all'articolo 9, paragrafo 2, lettera d), e all'articolo 9, paragrafo 4, lettera a), tra cui: a) cifratura delle e-mail da utilizzare b) sale dati (*data room*) online da utilizzare c) messaggistica istantanea da utilizzare	
Nome in codice per il TLPT	
Eventuali funzioni essenziali o importanti che l'entità finanziaria svolge in altri Stati membri	1. Elenco delle funzioni essenziali o importanti svolte in un altro Stato membro 2. Per ciascuna funzione essenziale o importante, indicazione dello Stato membro o degli Stati membri in cui è svolta
Eventuali funzioni essenziali o importanti supportate da fornitori terzi di servizi TIC	3. Elenco delle funzioni essenziali o importanti supportate da fornitori terzi di servizi TIC 4. Per ciascuna funzione, identificazione del fornitore terzo di servizi TIC
Termini previsti per il completamento di:	
(1) fase di preparazione, conformemente all'articolo 9	aaaa-mm-gg
(2) fase di test, conformemente agli articoli 10 e 11	aaaa-mm-gg
(3) fase di chiusura, conformemente all'articolo 12	aaaa-mm-gg
(4) piano correttivo, conformemente all'articolo 13	aaaa-mm-gg

ALLEGATO II

Contenuto del documento relativo alle specifiche dell'ambito di applicazione (articolo 9, paragrafo 6)

1. Il documento relativo alle specifiche dell'ambito di applicazione contiene un elenco di tutte le funzioni essenziali o importanti identificate dall'entità finanziaria.

2. Per ciascuna funzione essenziale o importante identificata sono incluse le informazioni seguenti:
   a) se la funzione essenziale o importante non è inclusa nell'ambito di applicazione del TLPT, la spiegazione dei motivi per cui non è inclusa;
   b) se la funzione essenziale o importante è inclusa nell'ambito di applicazione del TLPT:
      i) la spiegazione dei motivi dell'inclusione;
      ii) il sistema o i sistemi di TIC identificati che supportano tale funzione essenziale o importante;
      iii) per ciascun sistema di TIC identificato:
         1. se è esternalizzato e, in caso affermativo, il nome del fornitore terzo di servizi TIC;
         2. le giurisdizioni in cui è utilizzato il sistema di TIC;
         3. una descrizione ad alto livello dei *flag* preliminari, che indichi l'aspetto relativo alla sicurezza della riservatezza, dell'integrità, dell'autenticità o della disponibilità coperto da ciascun *flag*.

ALLEGATO III

Contenuto della relazione sull'analisi mirata delle minacce (articolo 10, paragrafo 5)

La relazione sull'analisi mirata delle minacce contiene informazioni su tutti gli aspetti seguenti:

1. l'ambito generale della ricerca relativa all'analisi delle minacce, che comprende almeno gli elementi seguenti:
   a) le funzioni essenziali o importanti che rientrano nell'ambito di applicazione;
   b) la relativa ubicazione geografica;
   c) la lingua ufficiale dell'UE utilizzata;
   d) i fornitori terzi di servizi TIC pertinenti;
   e) il periodo di tempo durante il quale sono raccolti dati per la ricerca;
2. la valutazione complessiva delle informazioni concrete e fruibili che possono essere reperite sull'entità finanziaria, tra cui:
   a) i nomi utente e le password dei dipendenti;
   b) i domini somiglianti che possono essere confusi per domini ufficiali dell'entità finanziaria;
   c) la ricognizione tecnica: software, sistemi e tecnologie vulnerabili o sfruttabili;
   d) le informazioni pubblicate dai dipendenti su Internet, relative all'entità finanziaria, che potrebbero essere utilizzate ai fini di un attacco;
   e) le informazioni messe in vendita sul dark web;
   f) qualsiasi altra informazione pertinente disponibile su Internet o su reti pubbliche;
   g) se del caso, le informazioni relative all'identificazione fisica del bersaglio (*targeting*), comprese le modalità di accesso ai locali dell'entità finanziaria;
3. un esame dell'analisi delle minacce che tenga conto del panorama generale delle minacce e della situazione particolare dell'entità finanziaria, comprendente almeno:
   a) il contesto geopolitico;
   b) il contesto economico;
   c) le tendenze tecnologiche e qualsiasi altra tendenza relativa alle attività nel settore dei servizi finanziari;
4. i profili di minaccia dei soggetti malintenzionati (soggetti/gruppi specifici o categorie generiche) che possono prendere di mira l'entità finanziaria, compresi i sistemi dell'entità finanziaria che hanno maggiori probabilità di essere compromessi o presi di mira da soggetti malintenzionati, le possibili motivazione, intenzione e logica alla base del potenziale *targeting* e il possibile modus operandi dei responsabili dell'attacco;
5. gli scenari di minaccia: almeno tre scenari di minaccia *end-to-end* per i profili di minaccia identificati conformemente al punto 4 che presentano i punteggi di gravità della minaccia più elevati. Gli scenari di minaccia descrivono il percorso di attacco *end-to-end* e comprendono almeno:
   a) uno scenario che include, tra l'altro, la compromissione della disponibilità del servizio;
   b) uno scenario che include, tra l'altro, la compromissione dell'integrità dei dati;
   c) uno scenario che include, tra l'altro, la compromissione della riservatezza delle informazioni;
6. se del caso, una descrizione dello scenario non guidato dalla minaccia di cui all'articolo 10, paragrafo 4.

ALLEGATO IV

Contenuto del piano relativo al test red team (articolo 11, paragrafo 1)

Il piano relativo al test red team contiene informazioni su tutti gli aspetti seguenti:

a) i canali e le procedure di comunicazione;

b) le tattiche, le tecniche e le procedure che possono o non possono essere utilizzate nell'attacco, compresi i confini etici per l'ingegneria sociale;

c) le misure di gestione dei rischi che i soggetti incaricati dello svolgimento dei test devono adottare;

d) una descrizione per ciascuno scenario, che indichi:

   i) l'autore della minaccia simulata;

   ii) le relative intenzioni, motivazione e finalità;

   iii) la funzione o le funzioni bersaglio e il sistema o i sistemi di TIC di supporto;

   iv) gli aspetti relativi alla riservatezza, all'integrità, alla disponibilità e all'autenticità presi di mira;

   v) i *flag*;

e) una descrizione dettagliata di ciascun percorso di attacco previsto, compresi i prerequisiti e gli eventuali *leg-up* che il team di controllo deve fornire, inclusi i termini per la relativa fornitura e il potenziale utilizzo;

f) la programmazione delle attività di red teaming, compresa la pianificazione temporale per l'esecuzione di ciascuno scenario, suddivisa almeno in base alle tre fasi che un soggetto incaricato dello svolgimento dei test intraprende durante l'intera fase di test, entrando rispettivamente nei sistemi di TIC delle entità finanziarie, spostandosi attraverso i sistemi di TIC e, in ultima battuta, eseguendo azioni sugli obiettivi e infine abbandonando i sistemi di TIC (fasi di ingresso, attraversamento e uscita);

g) le particolarità dell'infrastruttura delle entità finanziarie da prendere in considerazione durante il test;

h) se del caso, informazioni supplementari o altre risorse necessarie ai soggetti incaricati dello svolgimento dei test per l'esecuzione degli scenari.

ALLEGATO V

Contenuto della relazione sul test red team (articolo 12, paragrafo 2)

La relazione sul test red team contiene informazioni su almeno tutti gli aspetti seguenti:

a) i dati relativi all'attacco eseguito, tra cui:

   i) le funzioni essenziali o importanti prese di mira e i sistemi, i processi e le tecnologie TIC identificati a supporto della funzione essenziale o importante, come indicato nel piano relativo al test red team;

   ii) la sintesi di ciascuno scenario;

   iii) i *flag* raggiunti o non raggiunti;

   iv) i percorsi di attacco seguiti con successo e senza successo;

   v) le tattiche, tecniche e procedure utilizzate con successo e senza successo;

   vi) gli eventuali scostamenti dal piano relativo al test red team;

   vii) gli eventuali *leg-up* forniti;

b) tutte le azioni, di cui i soggetti incaricati dello svolgimento dei test sono a conoscenza, che sono state eseguite dal blue team per ricostruire l'attacco e attenuarne gli effetti;

c) le vulnerabilità rilevate e altre risultanze, tra cui:

   i) la descrizione della vulnerabilità e delle altre risultanze, compresa la relativa criticità;

   ii) l'analisi delle cause di fondo degli attacchi riusciti;

   iii) raccomandazioni per la correzione, compresa l'indicazione della priorità delle correzioni.

ALLEGATO VI

Contenuto del piano relativo al test blue team (articolo 12, paragrafo 4)

La relazione sul test blue team contiene informazioni su almeno tutti gli aspetti seguenti:

1. per ogni fase di attacco descritta dai soggetti incaricati dello svolgimento dei test della relazione sul test red team:
   a) l'elenco delle azioni di attacco rilevate;
   b) le voci di registrazione corrispondenti a tali rilevamenti;
2. la valutazione delle risultanze e raccomandazioni dei soggetti incaricati dello svolgimento dei test;
3. le prove dell'attacco da parte dei soggetti incaricati dello svolgimento dei test raccolte dal blue team;
4. l'analisi delle cause di fondo, effettuata dal blue team, degli attacchi riusciti da parte dei soggetti incaricati dello svolgimento dei test;
5. l'elenco degli insegnamenti tratti e dei potenziali miglioramenti individuati;
6. l'elenco dei temi da trattare nell'ambito del purple teaming.

ALLEGATO VII

Dettagli della relazione di sintesi delle pertinenti risultanze del TLPT di cui all'articolo 26, paragrafo 6, del regolamento (UE) 2022/2554

La relazione di sintesi sul test contiene informazioni su almeno tutti gli aspetti seguenti:

a) le parti coinvolte;

b) il piano di progetto;

c) l'ambito di applicazione convalidato, compresa la logica alla base dell'inclusione o dell'esclusione di funzioni essenziali o importanti e di sistemi, processi e tecnologie di TIC identificati a supporto delle funzioni essenziali o importanti coperte dal TLPT;

d) gli scenari selezionati ed eventuali scostamenti significativi dalla relazione sull'analisi mirata delle minacce;

e) i percorsi di attacco eseguiti e le tattiche, tecniche e procedure utilizzate;

f) i *flag* raggiunti e non raggiunti;

g) gli eventuali scostamenti dal piano relativo al test red team;

h) gli eventuali rilevamenti da parte del blue team;

i) il purple teaming nella fase di test, se avvenuto e relative condizioni;

j) gli eventuali *leg-up* utilizzati;

k) le misure di gestione dei rischi adottate;

l) le vulnerabilità identificate e altre risultanze, compresa la relativa criticità;

m) l'analisi delle cause di fondo degli attacchi riusciti;

n) un piano correttivo ad alto livello, che colleghi le vulnerabilità e altre risultanze, le relative cause di fondo e la priorità delle correzioni;

o) gli insegnamenti tratti dai riscontri ricevuti.

ALLEGATO VIII

Dettagli dell'attestato del TLPT di cui all'articolo 26, paragrafo 7, del regolamento (UE) 2022/2554

L'attestato contiene almeno tutte le informazioni seguenti:

a) sul TLPT svolto:
   - i) le date di inizio e di fine del TLPT;
   - ii) le funzioni essenziali o importanti incluse nell'ambito di applicazione del test;
   - iii) se del caso, informazioni sulle funzioni essenziali o importanti incluse nell'ambito di applicazione del test in relazione alle quali il TLPT non è stato svolto;
   - iv) se del caso, le altre entità finanziarie coinvolte nel TLPT;
   - v) se del caso, i fornitori terzi di servizi TIC che hanno partecipato al TLPT;
   - vi) per quanto riguarda i soggetti incaricati dello svolgimento dei test:
     1. se sono stati utilizzati soggetti incaricati dello svolgimento dei test interni;
     2. se l'articolo 5, paragrafo 3, secondo comma, è stato utilizzato dall'entità finanziaria;
   - vii) la durata, in giorni di calendario, della fase attiva di test red team;
b) nel caso in cui nel TLPT siano state coinvolte più autorità competenti per il TLPT, le altre autorità competenti per il TLPT e in quale veste sono state coinvolte;
c) l'elenco dei documenti esaminati dall'autorità competente per il TLPT ai fini dell'attestato.