REGULAMENTUL DELEGAT (UE) 2025/1190 AL COMISIEI

din 13 februarie 2025

de completare a Regulamentului (UE) 2022/2554 al Parlamentului European și al Consiliului în ceea ce privește standardele tehnice de reglementare în care se precizează criteriile utilizate pentru identificarea entităților financiare care trebuie să efectueze teste de penetrare bazate pe amenințări, cerințele și standardele care reglementează utilizarea entităților interne de testare, cerințele referitoare la sfera de aplicare, metodologia și abordarea de testare pentru fiecare fază a testării, rezultatele, încheierea și etapele procesului de remediere și tipul de cooperare în materie de supraveghere și alt tip de cooperare relevant care sunt necesare pentru punerea în aplicare a TLPT și pentru facilitarea recunoașterii reciproce

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 ([1]), în special articolul 26 alineatul (11) al patrulea paragraf,

întrucât:

(1) Prezentul regulament a fost elaborat conform cadrului TIBER-UE și reflectă metodologia, procesul și structura testelor de penetrare bazate pe amenințări (TLPT), astfel cum sunt descrise în TIBER-EU. Entitățile financiare care fac obiectul TLPT pot face trimitere la cadrul TIBER-UE sau la una dintre modalitățile de punere în aplicare ale acestuia la nivel național și îl (o) pot aplica, în măsura în care cadrul sau modalitatea respectivă de punere în aplicare este în concordanță cu cerințele prevăzute la articolele 26 și 27 din Regulamentul (UE) 2022/2554 și în prezentul regulament. Desemnarea unei autorități publice unice în sectorul financiar care să fie responsabilă de aspectele legate de TLPT la nivel național în conformitate cu articolul 26 alineatul (9) din Regulamentul (UE) 2022/2554 nu ar trebui să aducă atingere competenței încredințate autorităților de resort la nivelul Uniunii pentru supravegherea anumitor entități financiare în conformitate cu articolul 46 din regulamentul respectiv, cum ar fi, de exemplu, Banca Centrală Europeană pentru instituțiile de credit semnificative care trebuie considerate competente în ceea ce privește aspectele legate de TLPT. În cazul în care numai unele dintre sarcinile legate de TLPT-uri sunt delegate unei alte autorități naționale din sectorul financiar în temeiul articolului 26 alineatul (10) din Regulamentul (UE) 2022/2554, autoritatea competentă a entității financiare menționate la articolul 46 din regulamentul respectiv ar trebui să rămână autoritatea pentru sarcinile legate de TLPT care nu au fost delegate.

(2) Având în vedere complexitatea TLPT și riscurile aferente, utilizarea acestuia ar trebui să fie limitată la entitățile financiare pentru care este justificat. Prin urmare, autoritățile responsabile de aspecte legate de TLPT (autoritățile TLPT, fie la nivelul Uniunii, fie la nivel național) ar trebui să excludă din sfera de aplicare a TLPT acele entități financiare care își desfășoară activitatea în subsectoare de servicii financiare de bază pentru care nu este justificat un TLPT. Aceasta înseamnă că instituțiile de credit, instituțiile de plată și instituțiile emitente de monedă electronică, depozitarii centrali de titluri de valoare, contrapărțile centrale, locurile de tranzacționare, întreprinderile de asigurare și de reasigurare ar putea fi scutite de cerința de a efectua TLPT în lumina unei evaluări globale a profilului lor de risc TIC și a maturității lor, a impactului asupra sectorului financiar și a preocupărilor conexe legate de stabilitatea financiară, chiar dacă îndeplinesc criteriile cantitative.

(3) Autoritățile TLPT ar trebui să evalueze, în lumina unei evaluări globale a profilului de risc TIC și a maturității, a impactului asupra sectorului financiar și a preocupărilor conexe legate de stabilitatea financiară, dacă orice tip de entitate financiară, alta decât instituțiile de credit, instituțiile de plată, instituțiile emitente de monedă electronică, contrapărțile centrale, depozitarii centrali de titluri de valoare, locurile de tranzacționare, întreprinderile de asigurare și de reasigurare, ar trebui să facă obiectul TLPT. Evaluarea măsurii în care respectivele entități financiare îndeplinesc aceste criterii calitative ar trebui să vizeze identificarea entităților financiare pentru care TLPT este adecvat prin utilizarea unor indicatori transsectoriali și obiectivi. În același timp, evaluarea îndeplinirii de către o entitate

([1]) JO L 333, 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

financiară a acestor criterii calitative ar trebui să limiteze entitățile care fac obiectul TLPT la cele pentru care testarea este justificată. Ar trebui să se evalueze, de asemenea, dacă o entitate financiară îndeplinește aceste criterii calitative în lumina noilor evoluții ale pieței și a importanței tot mai mari a noilor participanți pe piață pentru sectorul financiar în viitor, inclusiv a furnizorilor de servicii de criptoactive autorizați în conformitate cu articolul 59 din Regulamentul (UE) 2023/1114 al Parlamentului European și al Consiliului ([2]).

(4) Entitățile financiare pot avea același furnizor de servicii TIC intragrup sau pot aparține aceluiași grup și se pot baza pe utilizarea de sisteme TIC partajate. În acest caz, este important ca autoritățile TLPT să ia în considerare structura și caracterul sistemic sau importanța pentru sectorul financiar a entității financiare respective la nivel național sau la nivelul Uniunii atunci când evaluează dacă o entitate financiară ar trebui să facă obiectul TLPT și dacă TLPT ar trebui efectuat la nivel de entitate sau la nivel de grup (prin intermediul unui TLPT comun).

(5) Pentru a reflecta cadrul TIBER-UE, este necesar ca metodologia de testare să prevadă implicarea următorilor participanți principali: entitatea financiară, cu o echipă de control (care reflectă „echipa de control" TIBER-EU) și o echipă albastră (care reflectă „echipa albastră" TIBER-EU), și autoritatea TLPT, sub forma unei echipe cibernetice TLPT (care reflectă „echipele cibernetice TIBER" din cadrul TIBER-EU), a unui furnizor de date operative privind amenințările și sub formă de entități de testare (prin care entitățile de testare reflectă „furnizorul de tipul «echipa roșie»" TIBER-EU).

(6) Pentru a se asigura că TLPT beneficiază de experiența dobândită în cadrul punerii în aplicare a TIBER-UE și pentru a reduce riscurile asociate efectuării TLPT, ar trebui să se asigure faptul că responsabilitățile echipelor cibernetice TLPT care urmează să fie înființate la nivelul autorităților TLPT corespund cât mai mult posibil celor ale echipelor cibernetice TIBER-UE. Prin urmare, echipele cibernetice TLPT ar trebui să aibă manageri de testare responsabili cu supravegherea TLPT-urilor individuale și cu planificarea și coordonarea testelor individuale. Echipele cibernetice TLPT ar trebui să servească drept punct unic de contact pentru comunicarea legată de testare cu părțile interesate interne și externe, pentru colectarea și prelucrarea feedbackului și a învățămintelor desprinse din testele efectuate anterior, precum și pentru sprijinirea entităților financiare care fac obiectul testării TLPT.

(7) Pentru a reflecta metodologia cadrului TIBER-UE, managerii de testare ar trebui să aibă competențele și capacitățile necesare pentru a oferi consiliere și pentru a contesta propunerile entităților de testare. Experiența în cadrul TIBER-UE a dovedit că ar fi mai utilă o echipă alcătuită din cel puțin doi manageri de testare desemnați pentru fiecare test. Pentru a reflecta faptul că TLPT este utilizat în scopul încurajării experienței de învățare, pentru a proteja confidențialitatea testelor și exceptând cazurile în care întâmpină probleme legate de resurse sau de expertiză, autoritățile TLPT sunt puternic încurajate să ia în considerare faptul că, pe durata unui TLPT, managerii de testare nu ar trebui să desfășoare activități de supraveghere asupra aceleiași entități financiare care face obiectul unui TLPT.

(8) Pentru a asigura coerența cu cadrul TIBER-UE, este important ca autoritatea TLPT să urmărească îndeaproape fiecare dintre etapele testării. Având în vedere natura testării și riscurile asociate acesteia, este esențial ca autoritatea TLPT să fie implicată în fiecare fază specifică a testării. În special, autoritatea TLPT ar trebui consultată și ar trebui să valideze acele evaluări sau decizii ale entităților financiare care, pe de o parte, pot influența eficacitatea testului și, pe de altă parte, pot avea un impact asupra riscurilor asociate testului. Printre etapele fundamentale în care este necesară o implicare specifică a autorității TLPT se numără validarea anumitor documente fundamentale ale testării, precum și selectarea furnizorilor de date operative privind amenințările și a entităților de testare și a măsurilor de gestionare a riscurilor. Implicarea autorităților TLPT, în special în ceea ce privește validările, nu ar trebui să genereze o sarcină excesivă pentru autoritățile respective și, prin urmare, ar trebui să se limiteze la documentele și deciziile care afectează în mod direct desfășurarea TLPT. Prin participarea activă la fiecare fază a testării, autoritățile TLPT pot evalua în mod eficace respectarea de către entitățile financiare a cerințelor relevante, ceea ce ar trebui să permită autorităților respective să elibereze adeverințe în temeiul articolului 26 alineatul (7) din Regulamentul (UE) 2022/2554.

([2]) Regulamentul (UE) 2023/1114 al Parlamentului European și al Consiliului din 31 mai 2023 privind piețele criptoactivelor și de modificare a Regulamentelor (UE) nr. 1093/2010 și (UE) nr. 1095/2010 și a Directivelor 2013/36/UE și (UE) 2019/1937 (JO L 150, 9.6.2023, p. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj).

(9) Caracterul secret al TLPT este extrem de important pentru a asigura condiții de testare realiste. Din acest motiv, testarea ar trebui să fie ascunsă și ar trebui luate măsuri de precauție pentru a păstra confidențialitatea TLPT, inclusiv alegerea numelor de cod care ar trebui să fie concepute pentru a împiedica identificarea TLPT de către terți. În cazul în care membrii personalului responsabili cu securitatea echipei financiare au cunoștință de planificarea sau desfășurarea unui TLPT, este probabil ca aceștia să fie mai atenți și mai vigilenți decât în condiții normale de activitate, ceea ce ar duce la o modificare a rezultatului testării. Prin urmare, membrii personalului entității financiare care nu fac parte din echipa de control ar trebui să fie informați cu privire la orice TLPT planificat sau aflat în desfășurare numai în cazul în care există motive convingătoare și sub rezerva acordului prealabil al managerilor de testare, printre altele pentru a asigura caracterul secret al testului în cazul în care un membru al echipei albastre a detectat testarea.

(10) După cum reiese din experiența acumulată în cadrul TIBER-UE în ceea ce privește „echipa de control”, selectarea unui șef de echipă de control adecvat este indispensabilă pentru desfășurarea TLPT în condiții de siguranță. Șeful echipei de control ar trebui să aibă mandatul necesar în cadrul entității financiare pentru a orienta toate aspectele testării, fără a compromite confidențialitatea acesteia. Din același motiv, membrii echipei de control ar trebui să aibă cunoștințe aprofundate despre entitatea financiară, postul șefului echipei de control și poziționarea strategică, ar trebui să aibă vechimea necesară și ar trebui să aibă acces la consiliul de conducere. Pentru a reduce riscul de compromitere a TLPT, echipa de control ar trebui să fie cât mai mică posibil.

(11) Există elemente inerente ale riscurilor asociate TLPT, deoarece funcțiile critice sunt testate într-un mediu de producție în timp real, cu posibilitatea de a provoca incidente de blocare a accesului, defecțiuni neașteptate ale sistemului, deteriorarea sistemelor critice de producție în timp real sau pierderea, modificarea sau divulgarea datelor. Aceste riscuri evidențiază necesitatea unor măsuri solide de gestionare a riscurilor. Pentru a se asigura că TLPT se desfășoară în mod controlat pe tot parcursul testării, este foarte important ca entitățile financiare să aibă cunoștință în orice moment de riscurile specifice care apar în cadrul unui TLPT și ca aceste riscuri să fie atenuate. În acest sens, fără a aduce atingere proceselor interne ale entității financiare și responsabilității și delegărilor deja atribuite șefului echipei de control, ar putea fi adecvate informații cu privire la măsurile de gestionare a riscurilor asociate TLPT sau, în cazuri speciale, aprobarea măsurilor respective de gestionare a riscurilor chiar de către organul de conducere al entității financiare. Pentru a putea furniza servicii profesionale eficace și cu cel mai înalt nivel de calificare și pentru a reduce aceste riscuri, este, de asemenea, esențial ca entitățile de testare și furnizorii de date operative privind amenințările (denumiți împreună „furnizorii de TLPT”) să dispună de cel mai înalt nivel de competențe, expertiză și experiență adecvată în domeniul datelor operative privind amenințările și al TLPT în sectorul serviciilor financiare.

(12) Testele convenționale de penetrare oferă adesea o evaluare detaliată și utilă a vulnerabilităților tehnice și de configurare ale unui singur sistem sau ale unui singur mediu în mod izolat, dar, spre deosebire de testul de tipul „echipa roșie” bazat pe date operative, acestea nu evaluează întregul scenariu al unui atac direcționat împotriva unei întregi entități, inclusiv sfera completă a persoanelor, proceselor și tehnologiilor sale. Prin urmare, în cursul procesului de selecție a furnizorilor de TLPT, entitățile financiare ar trebui să se asigure că respectivii furnizori au competențele necesare pentru a efectua teste de tipul „echipa roșie” bazate pe date operative, și nu doar teste de penetrare. Prin urmare, este necesar să se stabilească criterii cuprinzătoare pentru entitățile de testare, atât interne, cât și externe, precum și pentru furnizorii de date operative privind amenințările, care sunt întotdeauna externi. În cazul în care furnizorii de TLPT fac parte din aceeași întreprindere, membrii personalului alocat pentru un TLPT ar trebui să fie separați în mod corespunzător.

(13) Pot exista circumstanțe excepționale în care entitățile financiare nu pot contracta furnizori de TLPT care îndeplinesc criteriile cuprinzătoare. Prin urmare, atunci când dovedesc indisponibilitatea unor astfel de furnizori de date operative privind amenințările, entitățile financiare ar trebui să aibă posibilitatea de a implica persoane care nu îndeplinesc toate criteriile cuprinzătoare, cu condiția ca acestea să atenueze în mod corespunzător oricare riscuri suplimentare rezultate și ca autoritatea TLPT să evalueze toate aceste criterii.

(14) În cazul în care într-un TLPT sunt implicate mai multe entități financiare și mai multe autorități TLPT, rolurile tuturor părților în procesul TLPT ar trebui specificate pentru a efectua testul cel mai eficient și mai sigur. În scopul testării grupate, sunt necesare cerințe specifice pentru a preciza rolul entității financiare desemnate, și anume că aceasta ar trebui să fie responsabilă de furnizarea întregii documentații necesare autorității TLPT principale și de monitorizarea procesului de testare. Entitatea financiară desemnată ar trebui, de asemenea, să fie responsabilă cu aspectele comune ale evaluării privind gestionarea riscurilor. În pofida rolului entității financiare desemnate, obligațiile fiecărei entități financiare care participă la procesul TLPT grupat nu ar trebui să fie afectate în cursul testului grupat. Același principiu ar trebui să se aplice în cazul TLPT-urilor comune.

(15) După cum reiese din experiența dobândită în urma punerii în aplicare a cadrului TIBER-UE, organizarea de reuniuni cu prezență fizică sau virtuale care să cuprindă toate părțile interesate vizate (entități financiare, autorități, entități de testare și furnizori de date operative privind amenințările) este cea mai eficientă modalitate de a asigura desfășurarea corespunzătoare a testelor. Prin urmare, reuniunile cu prezență fizică și cele virtuale ar trebui să aibă loc în diferite etape ale procesului și, în special, în faza de pregătire la lansarea TLPT și pentru a finaliza sfera de aplicare a acestuia, în timpul fazei de testare, pentru a finaliza raportul de date operative privind amenințările și planul testării de tipul „echipa roșie” și pentru informările săptămânale, precum și în timpul fazei de încheiere pentru reluarea acțiunilor entităților de testare și a acțiunilor de tipul „echipa albastră”, pentru activitățile de tipul „echipa violet” și pentru a face schimb de feedbackuri cu privire la TLPT.

(16) Pentru a asigura buna funcționare a TLPT, autoritatea TLPT ar trebui să prezinte în mod clar entității financiare așteptările sale în ceea ce privește testarea. În acest sens, managerii de testare ar trebui să se asigure că se stabilește un flux adecvat de informații cu echipa de control din cadrul entității financiare și cu furnizorii de TLPT.

(17) Entitatea financiară ar trebui să selecteze funcțiile critice sau importante care vor intra în sfera de aplicare a TLPT. Atunci când selectează aceste funcții, entitatea financiară ar trebui să se bazeze pe diferite criterii legate de importanța fiecărei funcții pentru entitatea financiară însăși și pentru sectorul financiar, la nivelul Uniunii și la nivel național, nu numai din punct de vedere economic, ci și având în vedere statutul simbolic sau politic al funcției. Pentru a facilita o tranziție lină către faza de colectare a datelor operative privind amenințările, echipa de control ar trebui să furnizeze entităților de testare și furnizorului de date operative privind amenințările care nu sunt implicați în procesul de definire a sferei de aplicare informații detaliate cu privire la stabilirea sferei de aplicare convenite.

(18) Pentru a furniza entităților de testare informațiile necesare pentru a simula un atac real și realist asupra sistemelor în timp real ale entității financiare care stau la baza funcțiilor sale critice sau importante, furnizorul de date operative privind amenințările ar trebui să colecteze date operative sau informații care acoperă cel puțin două domenii-cheie de interes: țintele, prin identificarea posibilelor suprafețe de atac din cadrul entității financiare, și amenințările, prin identificarea actorilor relevanți care reprezintă amenințări și a scenariilor probabile de amenințare. Pentru a se asigura că furnizorul de date operative privind amenințările ia în considerare amenințările relevante pentru entitatea financiară, entitățile de testare, echipa de control și managerii de testare ar trebui să furnizeze feedback în proiectul de raport privind datele operative privind amenințările. Dacă este disponibil, furnizorul de date operative privind amenințările poate utiliza un peisaj generic al amenințărilor furnizat de autoritatea TLPT pentru sectorul financiar al unui stat membru ca referință pentru peisajul amenințărilor la nivel național. Pe baza aplicării cadrului TIBER-UE, procesul de colectare a datelor operative privind amenințările durează, de regulă, aproximativ patru săptămâni.

(19) Pentru a permite entităților de testare să obțină informații și să revizuiască în continuare documentul privind specificarea sferei de aplicare și raportul referitor la datele operative privind amenințările specifice în vederea finalizării planului testării de tipul „echipa roșie”, este esențial ca, înainte de faza de testare de tipul „echipa roșie” a TLPT, entitățile de testare să primească de la furnizorul de date operative privind amenințările explicații detaliate cu privire la raportul referitor la datele operative privind amenințările specifice și analiza posibilelor scenarii de amenințare.

(20) Pentru a permite entităților de testare să efectueze o testare realistă și cuprinzătoare, în care să fie executate toate fazele de atac și să se atingă semnalele de alarmă, ar trebui să se aloce timp suficient fazei de testare activă de tipul „echipa roșie”. Pe baza experienței acumulate în cadrul TIBER-UE, timpul alocat ar trebui să fie de cel puțin 12 săptămâni și ar trebui stabilit ținând seama de numărul de părți implicate, de sfera de aplicare a TLPT, de resursele entității sau entităților financiare implicate, de cerințele externe și de disponibilitatea informațiilor justificative furnizate de entitatea financiară.

(21) În timpul fazei de testare activă de tipul „echipa roșie”, entitățile de testare ar trebui să aplice o serie de tactici, tehnici și proceduri (TTP) pentru a testa în mod adecvat sistemele de producție în timp real ale entității financiare. Tacticile, tehnicile și procedurile ar trebui să conțină, după caz, recunoașterea (și anume colectarea unui volum cât mai mare de informații cu privire la o țintă), instrumentalizarea (și anume analizarea informațiilor privind infrastructura, instalațiile și angajații și pregătirea pentru operațiunile specifice țintei), livrarea (și anume lansarea activă a operațiunii complete asupra țintei), exploatarea (și anume în cazul în care obiectivul entităților de testare este de a compromite serverele, rețelele entității financiare și de a exploata personalul acesteia prin inginerie socială); controlul și circulația (și anume încercările de a trece de la sistemele compromise la alte sisteme vulnerabile sau de mare valoare) și acțiunile asupra țintei (și anume obținerea unui acces suplimentar la sistemele compromise și obținerea accesului la informațiile și datele țintă convenite anterior, astfel cum s-a stabilit anterior în planul testării de tipul „echipa roșie”).

(22) Atunci când efectuează un TLPT, entitățile de testare ar trebui să acționeze ținând seama de timpul disponibil pentru desfășurarea atacului, de resursele și limitele de natură etică și juridică. În cazul în care entitățile de testare nu sunt în măsură să avanseze către următoarea etapă programată a atacului, echipa de control ar trebui să ofere asistență ocazională, cu acordul autorității TLPT, sub forma unor „ajutoare". Ajutoarele pot fi clasificate în linii mari în informații și acces și pot consta în furnizarea de acces la sistemele TIC sau la rețelele interne pentru a continua testarea și a se concentra asupra următoarelor etape ale atacului.

(23) În timpul activității de tipul „echipa roșie" în faza de testare, dacă este necesar pentru a permite continuarea TLPT în ultimă instanță, în circumstanțe excepționale și după epuizarea tuturor opțiunilor alternative, ar trebui să se utilizeze o activitate de testare în colaborare care să implice atât entitățile de testare, cât și echipa albastră. În contextul unui astfel de exercițiu limitat de tipul „echipa violet", se pot utiliza următoarele metode: „capturare și eliberare", atunci când entitățile de testare încearcă să continue scenariile, sunt detectate și apoi reiau testarea, „jocuri de război", care permit scenarii mai complexe pentru a testa procesul decizional strategic, sau „validarea în colaborare a conceptului", care permite entităților de testare și membrilor din echipa albastră să valideze în comun măsuri, instrumente sau tehnici de securitate specifice într-un mediu controlat și de cooperare.

(24) TLPT ar trebui utilizat ca experiență de învățare pentru a spori reziliența operațională digitală a entităților financiare. În acest sens, echipa albastră și entitățile de testare ar trebui să reia atacul și să revizuiască măsurile luate pentru a învăța din experiența de testare în colaborare cu entitățile de testare. În acest scop și pentru a permite o pregătire adecvată, raportul testării de tipul „echipa roșie" și raportul testării de tipul „echipa albastră" ar trebui să fie puse la dispoziția tuturor părților implicate în activitățile de reluare, înainte de desfășurarea activităților de reluare. În plus, în faza de încheiere, ar trebui să se efectueze un exercițiu de testare de tipul „echipa violet" pentru a maximiza experiența de învățare. Metodele care pot fi utilizate pentru activitatea de tipul „echipa violet" în faza de încheiere ar trebui să includă discuții privind scenarii alternative de atac, explorarea de scenarii alternative privind sistemele în timp real sau reexplorarea scenariilor planificate privind sistemele în timp real pe care entitățile de testare nu au fost în măsură să le finalizeze sau să le execute în timpul fazei de testare.

(25) Pentru a facilita și mai mult experiența de învățare a tuturor părților implicate în TLPT, în beneficiul testelor viitoare, și pentru a spori reziliența operațională digitală a entităților financiare, părțile în cauză ar trebui să își ofere reciproc feedback cu privire la procesul general și, în special, să identifice activitățile care au evoluat bine sau ar fi putut fi îmbunătățite și aspectele procesului TLPT care au funcționat bine sau ar putea fi îmbunătățite.

(26) Autoritățile competente menționate la articolul 46 din Regulamentul (UE) 2022/2554 și autoritățile TLPT, în cazul în care acestea sunt diferite, ar trebui să coopereze pentru a include testarea avansată prin intermediul TLPT în procesele de supraveghere existente. În acest sens și pentru a împărtăși înțelegerea corectă a constatărilor TLPT și a modului în care acestea ar trebui interpretate, este oportun să se stabilească, în special în ceea ce privește raportul de sinteză al testelor și planurile de remediere, o cooperare strânsă între managerii de testare care au fost implicați în TLPT și supraveghetorii responsabili.

(27) Articolul 26 alineatul (8) primul paragraf din Regulamentul (UE) 2022/2554 prevede că entitățile financiare au obligația de a contracta entități externe de testare la fiecare trei teste. În cazul în care entitățile financiare includ în echipa de entități de testare atât entități interne, cât și entități externe de testare, ar trebui să se considere că se efectuează un TLPT cu entități interne de testare în sensul articolului respectiv.

(28) Prezentul regulament are la bază proiectul de standarde tehnice de reglementare prezentat Comisiei de către Autoritatea Bancară Europeană, Autoritatea Europeană de Asigurări și Pensii Ocupaționale și Autoritatea Europeană pentru Valori Mobiliare și Piețe (autoritățile europene de supraveghere), în acord cu Banca Centrală Europeană.

(29) Autoritățile europene de supraveghere au desfășurat consultări publice deschise cu privire la proiectele de standarde tehnice de reglementare pe care se bazează prezentul regulament, au analizat costurile și beneficiile potențiale aferente și au solicitat avizul Grupului părților interesate din domeniul bancar, instituit în conformitate cu articolul 37 din Regulamentul (UE) nr. 1093/2010 al Parlamentului European și al Consiliului ([3]), al Grupului părților interesate din domeniul asigurărilor și reasigurărilor și al Grupului părților interesate din domeniul pensiilor ocupaționale, instituite în conformitate cu articolul 37 din Regulamentul (UE) nr. 1094/2010 al Parlamentului European și al Consiliului ([4]), și al Grupului părților interesate din domeniul valorilor mobiliare și pieței, instituit în conformitate cu articolul 37 din Regulamentul (UE) nr. 1095/2010 al Parlamentului European și al Consiliului ([5]).

(30) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ([6]) și a emis un aviz la 20 august 2024,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

1. „echipă de control” înseamnă echipa compusă din personalul entității financiare testate și, după caz, având în vedere sfera de aplicare a TLPT, personalul furnizorilor săi terți de servicii și orice altă parte care gestionează testul;

2. „șeful echipei de control” înseamnă membrul personalului entității financiare responsabil cu desfășurarea tuturor activităților legate de TLPT pentru entitatea financiară în contextul unui anumit test;

3. „echipa albastră” înseamnă personalul entității financiare și, după caz, personalul furnizorilor terți de servicii ai entității financiare și al oricărei alte părți considerate relevante având în vedere sfera de aplicare a TLPT, al furnizorilor terți de servicii ai entității financiare, care protejează utilizarea de către o entitate financiară a rețelelor și a sistemelor informatice prin menținerea posturii sale de securitate împotriva atacurilor simulate sau reale și care nu are cunoștință de TLPT;

4. „sarcini de tipul «echipa albastră»” înseamnă sarcini care sunt efectuate de obicei de echipa albastră, cum ar fi centrul de operațiuni de securitate (SOC), serviciile de infrastructură TIC, serviciile de asistență, serviciile de gestionare a incidentelor la nivel operațional;

5. „echipa roșie” înseamnă entitățile interne sau externe de testare, contractate pentru un TLPT sau desemnate pentru efectuarea unui TLPT;

6. „activitate de tipul «echipa violet»” înseamnă o activitate de testare în colaborare care implică atât entitățile de testare, cât și echipa albastră;

([3]) Regulamentul (UE) nr. 1093/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea bancară europeană), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/78/CE a Comisiei (JO L 331, 15.12.2010, p. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Regulamentul (UE) nr. 1094/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea europeană de asigurări și pensii ocupaționale), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/79/CE a Comisiei (JO L 331, 15.12.2010, p. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Regulamentul (UE) nr. 1095/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea europeană pentru valori mobiliare și piețe), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/77/CE a Comisiei (JO L 331, 15.12.2010, p. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

7. „autoritate TLPT” înseamnă oricare dintre următoarele:

   (a) autoritatea publică unică din sectorul financiar desemnată în conformitate cu articolul 26 alineatul (9) din Regulamentul (UE) 2022/2554;

   (b) autoritatea din sectorul financiar căreia îi este delegată exercitarea unora sau a tuturor sarcinilor legate de TLPT în conformitate cu articolul 26 alineatul (10) din Regulamentul (UE) 2022/2554;

   (c) oricare dintre autoritățile competente menționate la articolul 46 din Regulamentul (UE) 2022/2554;

8. „echipa cibernetică TLPT” sau „TCT” înseamnă personalul din cadrul autorităților TLPT care este responsabil de aspectele legate de TLPT;

9. „manageri de testare” înseamnă personalul desemnat să conducă activitățile autorității TLPT pentru un anumit TLPT în vederea monitorizării respectării prezentului regulament;

10. „furnizor de date operative privind amenințările” înseamnă experții, contractați de entitatea financiară pentru fiecare TLPT și care nu fac parte din entitatea financiară și nici dintre furnizorii de servicii TIC intragrup, după caz, care colectează și analizează date operative privind amenințările specifice relevante pentru entitățile financiare care intră în sfera de aplicare a unui anumit exercițiu TLPT și elaborează scenarii de amenințare relevante și realiste corespunzătoare;

11. „furnizori de TLPT” înseamnă entități de testare și furnizori de date operative privind amenințările;

12. „ajutor” înseamnă asistența sau informațiile furnizate de echipa de control entităților de testare pentru a permite acestora să continue executarea unei căi de atac în cazul în care acestea nu sunt în măsură să avanseze pe cont propriu și în cazul în care nu există nicio alternativă rezonabilă, inclusiv din cauza timpului sau a resurselor insuficiente pentru anumit TLPT;

13. „cale de atac” înseamnă ruta urmată de entitățile de testare în timpul fazei de testare activă de tipul „echipa roșie” a TLPT pentru a ajunge la semnalele de alarmă specificate pentru TLPT-ul respectiv;

14. „semnale de alarmă” sunt obiective-cheie ale sistemelor TIC care sprijină funcțiile critice sau importante ale unei entități financiare pe care entitățile de testare încearcă să le atingă prin intermediul testului;

15. „informații sensibile” înseamnă informații care pot fi mobilizate cu ușurință pentru a comite atacuri împotriva sistemelor TIC ale entității financiare, asupra proprietății intelectuale, asupra datelor confidențiale ale unei întreprinderi sau asupra datelor cu caracter personal, care pot afecta direct sau indirect entitatea financiară și ecosistemul său dacă ar intra în posesia unor actori rău-intenționați;

16. „grup” înseamnă toate entitățile financiare care participă la un TLPT grupat în temeiul articolului 26 alineatul (4) din Regulamentul (UE) 2022/2554;

17. „stat membru gazdă” înseamnă statul membru gazdă în conformitate cu dreptul sectorial al Uniunii aplicabil fiecărei entități financiare;

18. „TLPT comun” înseamnă un TLPT, altul decât un TLPT grupat, astfel cum se menționează la articolul 26 alineatul (4) din Regulamentul (UE) 2022/2554, care implică mai multe entități financiare care utilizează același furnizor de servicii TIC intragrup sau care aparțin aceluiași grup și care utilizează în comun sisteme TIC.

Articolul 2

Identificarea entităților financiare care trebuie să efectueze TLPT

(1) Autoritățile TLPT evaluează dacă o entitate financiară este obligată să efectueze TLPT, ținând seama de impactul entităților financiare respective, de caracterul lor sistemic și de profilul lor de risc TIC, pe baza tuturor criteriilor următoare:

(a) factori legați de impact și de caracterul sistemic:

   (i) dimensiunea entității financiare, stabilită pe baza faptului dacă entitatea financiară furnizează servicii financiare în unul sau mai multe state membre și prin compararea activităților entității financiare cu cele ale altor entități financiare care furnizează servicii similare;

   (ii) amploarea și natura interconectării entității financiare cu alte entități financiare din sectorul financiar din unul sau mai multe state membre;

   (iii) caracterul critic sau importanța serviciilor pe care entitatea financiară le furnizează sectorului financiar;

(iv) posibilitatea de substituire a serviciilor furnizate de entitatea financiară;

(v) complexitatea modelului de afaceri al entității financiare și a serviciilor și proceselor conexe;

(vi) dacă entitatea financiară face parte dintr-un grup cu caracter sistemic la nivelul Uniunii sau la nivel național în sectorul financiar și partajează sistemele TIC;

(b) factori legați de riscurile TIC:

(i) profilul de risc al entității financiare;

(ii) peisajul amenințărilor cu care se confruntă entitatea financiară;

(iii) gradul de dependență a funcțiilor critice sau importante ori a funcțiilor de sprijin ale entității financiare de sistemele și procesele TIC;

(iv) complexitatea arhitecturii TIC a entității financiare;

(v) serviciile și funcțiile TIC sprijinite de furnizori terți de servicii TIC, precum și cantitatea și tipul de acorduri contractuale cu furnizorii terți de servicii TIC sau cu furnizorii de servicii TIC intragrup;

(vi) rezultatele analizelor de supraveghere relevante pentru evaluarea maturității TIC a entității financiare;

(vii) maturitatea planurilor de continuitate a activității TIC și a planurilor de răspuns și de recuperare în domeniul TIC;

(viii) maturitatea măsurilor operaționale de detectare și atenuare în domeniul securității TIC, inclusiv capacitatea de:

1. monitorizare a infrastructurii TIC a entității financiare în mod permanent;

2. detectare a evenimentelor legate de TIC în timp real;

3. analiză a evenimentelor menționate la punctul 2;

4. răspuns la evenimentele menționate la punctul 2 în timp util și în mod eficace;

(ix) dacă entitatea financiară face parte dintr-un grup activ în sectorul financiar la nivelul Uniunii sau la nivel național care partajează sisteme TIC.

În sensul literei (a) punctul (i), autoritatea TLPT ia în considerare, atunci când este posibil:

(a) poziția cotei de piață a entității financiare la nivelul Uniunii și la nivel național;

(b) gama de activități oferite de entitatea financiară;

(c) cota de piață a serviciilor furnizate de entitatea financiară sau a activităților întreprinse la nivelul Uniunii și la nivel național.

În sensul literei (a) punctul (v), autoritatea TLPT ia în considerare, atunci când este posibil:

(a) dacă entitatea financiară desfășoară mai multe modele de afaceri;

(b) interconectarea diferitelor procese operaționale și a serviciilor conexe.

(2) Autoritățile TLPT impun tuturor entităților financiare următoare să efectueze TLPT, cu excepția cazului în care evaluarea menționată la alineatul (1) în ceea ce privește o entitate financiară indică faptul că impactul său, preocupările privind stabilitatea financiară legate de entitatea financiară respectivă sau profilul său de risc TIC nu justifică efectuarea unui TLPT:

(a) instituții de credit care îndeplinesc oricare dintre următoarele condiții:

(i) au fost identificate ca instituții de importanță sistemică globală (G-SII) în conformitate cu articolul 131 din Directiva 2013/36/UE a Parlamentului European și a Consiliului ([7]);

(ii) au fost identificate ca alte instituții de importanță sistemică (O-SII) în conformitate cu articolul 131 din Directiva 2013/36/UE;

(iii) fac parte dintr-o G-SII sau O-SII;

([7]) Directiva 2013/36/UE a Parlamentului European și a Consiliului din 26 iunie 2013 cu privire la accesul la activitatea instituțiilor de credit și supravegherea prudențială a instituțiilor de credit, de modificare a Directivei 2002/87/CE și de abrogare a Directivelor 2006/48/CE și 2006/49/CE (JO L 176, 27.6.2013, p. 338, ELI: http://data.europa.eu/eli/dir/2013/36/oj).

(b) instituțiile de plată care au depășit în fiecare dintre cei doi ani calendaristici anteriori evaluării de către autoritatea TLPT 150 de miliarde EUR din valoarea totală a operațiunilor de plată, astfel cum sunt definite la articolul 4 punctul 5 din Directiva (UE) 2015/2366 a Parlamentului European și a Consiliului ([8]);

(c) instituțiile emitente de monedă electronică care au depășit, în fiecare dintre cei doi ani calendaristici anteriori evaluării de către autoritatea TLPT, fie 150 de miliarde EUR din valoarea totală a operațiunilor de plată, astfel cum sunt definite la articolul 4 punctul 5 din Directiva (UE) 2015/2366, fie 40 de miliarde EUR din valoarea totală a volumului de monedă electronică în circulație;

(d) depozitarii centrali de titluri de valoare;

(e) contrapărțile centrale;

(f) locurile de tranzacționare cu un sistem electronic de tranzacționare care îndeplinesc oricare dintre următoarele criterii:

(i) locul de tranzacționare are cea mai mare cotă de piață în ceea ce privește cifra de afaceri la nivel național în fiecare dintre cei doi ani calendaristici anteriori evaluării de către autoritatea TLPT în oricare dintre următoarele:

1. valori mobiliare, astfel cum sunt definite la articolul 4 alineatul (1) punctul 44 litera (a) din Directiva 2014/65/UE a Parlamentului European și a Consiliului ([9]);

2. valori mobiliare, astfel cum sunt definite la articolul 4 alineatul (1) punctul 44 litera (b) din Directiva 2014/65/UE;

3. instrumente financiare derivate, astfel cum sunt definite la articolul 2 alineatul (1) punctul 29 din Regulamentul (UE) nr. 600/2014 ([10]);

4. produse financiare structurate, astfel cum sunt definite la articolul 2 alineatul (1) punctul 28 din Regulamentul (UE) nr. 600/2014;

5. certificate de emisii menționate în secțiunea C punctul 11 din anexa I la Directiva 2014/65/UE;

(ii) locul de tranzacționare are o cotă de piață în ceea ce privește cifra de afaceri la nivelul Uniunii care depășește 5 % în fiecare dintre cei doi ani calendaristici anteriori evaluării de către autoritatea TLPT în oricare dintre următoarele:

1. acțiuni la întreprinderi și alte titluri de valoare echivalente acțiunilor la întreprinderi, la întreprinderi de tip parteneriat sau la alte entități, precum și certificatele de depozit referitoare la acțiuni;

2. obligațiuni sau alte titluri de creanță, inclusiv certificatele de depozit referitoare la astfel de titluri;

3. instrumente financiare derivate, astfel cum sunt definite la articolul 2 alineatul (1) punctul 29 din Regulamentul (UE) nr. 600/2014 al Parlamentului European și al Consiliului;

4. produse financiare structurate, astfel cum sunt definite la articolul 2 alineatul (1) punctul 28 din Regulamentul (UE) nr. 600/2014;

5. certificate de emisii menționate în secțiunea C punctul 11 din anexa I la Directiva 2014/65/UE;

([8]) Directiva (UE) 2015/2366 a Parlamentului European și a Consiliului din 25 noiembrie 2015 privind serviciile de plată în cadrul pieței interne, de modificare a Directivelor 2002/65/CE, 2009/110/CE și 2013/36/UE și a Regulamentului (UE) nr. 1093/2010, și de abrogare a Directivei 2007/64/CE (JO L 337, 23.12.2015, p. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

([9]) Directiva 2014/65/UE a Parlamentului European și a Consiliului din 15 mai 2014 privind piețele instrumentelor financiare și de modificare a Directivei 2002/92/CE și a Directivei 2011/61/UE (JO L 173, 12.6.2014, p. 349, ELI: http://data.europa.eu/eli/dir/2014/65/oj).

([10]) Regulamentul (UE) nr. 600/2014 al Parlamentului European și al Consiliului din 15 mai 2014 privind piețele instrumentelor financiare și de modificare a Regulamentului (UE) nr. 648/2012 (JO L 173, 12.6.2014, p. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

(g) întreprinderile de asigurare și de reasigurare care îndeplinesc toate criteriile următoare:

(i) au o primă brută subscrisă (GWP) care depășește 1 500 000 000 EUR;

(ii) au rezerve tehnice care depășesc 10 000 000 000 EUR;

(iii) întreprinderile de asigurare care desfășoară numai activități de asigurare de viață sau care desfășoară atât activități de asigurare de viață, cât și activități de asigurare generală și care au active totale care depășesc 3,5 % din suma activelor totale evaluate în conformitate cu articolul 75 din Directiva 2009/138/CE a Parlamentului European și a Consiliului ([11]) ale întreprinderilor de asigurare și de reasigurare stabilite în statul membru.

În sensul literei (f) punctul (ii), în cazul în care locul de tranzacționare face parte dintr-un grup care partajează sisteme TIC sau același furnizor de servicii TIC intragrup, se ia în considerare cifra de afaceri a contractelor privind titlurile de valoare și instrumentele financiare derivate din toate locurile de tranzacționare care aparțin aceluiași grup și sunt stabilite în Uniune.

În sensul literei (g), autoritățile TLPT identifică un subset al tuturor întreprinderilor de asigurare și de reasigurare prin aplicarea criteriilor prevăzute la litera (g) punctele (i), (ii) și (iii). Întreprinderile de asigurare și de reasigurare incluse în subsetul respectiv au obligația de a efectua TLPT în cazul în care îndeplinesc, de asemenea, oricare dintre următoarele criterii:

(a) prime brute subscrise (GWP) care depășesc 3 000 000 000 EUR;

(b) rezerve tehnice care depășesc 30 000 000 000 EUR;

(c) active totale care depășesc 10 % din suma activelor totale evaluate în conformitate cu articolul 75 din Directiva 2009/138/CE ale întreprinderilor de asigurare și de reasigurare stabilite în statul membru respectiv.

(3) În cazul în care mai multe entități financiare care aparțin aceluiași grup și care partajează sisteme TIC sau mai multe entități financiare care utilizează același furnizor de servicii TIC intragrup îndeplinesc criteriile prevăzute la alineatul (2), autoritățile TLPT ale entităților financiare respective decid, în conformitate cu articolul 16 alineatul (2), dacă cerința de a efectua TLPT pe bază individuală este relevantă pentru entitățile financiare respective.

În cazul în care autoritatea TLPT a întreprinderii-mamă a unui grup de entități financiare menționate la primul paragraf este diferită de autoritățile TLPT ale entităților financiare ale grupului, autoritatea respectivă este consultată de autoritățile TLPT ale entităților financiare care aparțin grupului respectiv cu privire la oportunitatea efectuării TLPT pe bază individuală.

Articolul 3

TCT și managerii de testare TLPT

(1) O autoritate TLPT atribuie unei TCT responsabilitatea pentru coordonarea activităților legate de TLPT. O TCT este alcătuită din manageri de testare care sunt însărcinați să supravegheze un TLPT individual.

(2) Pentru fiecare test, autoritatea TLPT desemnează un manager de testare și cel puțin un supleant.

(3) Managerii de testare monitorizează dacă sunt respectate cerințele prevăzute în prezentul regulament și se asigură că acestea sunt respectate.

([11]) Directiva 2009/138/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 privind accesul la activitate și desfășurarea activității de asigurare și de reasigurare (Solvabilitate II) (JO L 335, 17.12.2009, p. 1, ELI: http://data.europa.eu/eli/dir/2009/138/oj).

(4) Managerul de testare comunică entității financiare datele de contact ale TCT prin notificarea menționată la articolul 9 alineatul (1).

(5) Autoritatea TLPT participă la toate fazele TLPT.

Articolul 4

Măsuri organizatorice pentru entitățile financiare

(1) Entitățile financiare desemnează un șef de echipă de control care este responsabil de gestionarea curentă a TLPT și de deciziile și acțiunile echipei de control.

(2) Entitățile financiare stabilesc măsuri organizatorice și procedurale pentru a se asigura că:

(a) accesul la informațiile referitoare la orice TLPT planificat sau aflat în desfășurare este limitat, pe baza principiului necesității de a cunoaște, la echipa de control, la organul de conducere, la entitățile de testare, la furnizorul de date operative privind amenințările și la autoritatea TLPT;

(b) echipa de control consultă managerii de testare înainte de a implica orice membru al echipei albastre într-un TLPT;

(c) echipa de control este informată cu privire la orice detectare a TLPT de către membrii personalului entității financiare sau de către furnizorii terți de servicii ai acesteia; în cazul escaladării răspunsului la incident rezultat, dacă este necesar, echipa de control ține sub control această escaladare;

(d) există acorduri referitoare la caracterul secret al TLPT, aplicabil personalului entității financiare, personalului furnizorilor terți de servicii TIC în cauză, entităților de testare și furnizorului de date operative privind amenințările;

(e) echipa de control furnizează managerilor de testare, la cerere, informații referitoare la TLPT;

(f) atunci când este posibil, părțile implicate în TLPT fac trimitere la acesta numai folosind denumirea codului.

Articolul 5

Gestionarea riscurilor pentru TLPT

(1) În cursul fazei de pregătire menționate la articolul 9, echipa de control evaluează riscurile asociate testării sistemelor de producție în timp real a funcțiilor critice sau importante ale entității financiare, inclusiv impactul potențial asupra:

(a) sectorului financiar;

(b) stabilității financiare la nivelul Uniunii sau la nivel național.

Echipa de control examinează aceste impacturi pe tot parcursul testării.

(2) În scopul evaluării și gestionării riscurilor, echipa de control ia în considerare cel puțin următoarele tipuri de riscuri legate de:

(a) acordarea accesului furnizorului de date operative privind amenințările și entităților externe de testare, după caz, la informații sensibile privind entitatea financiară;

(b) nerespectarea de către TLPT a Regulamentului (UE) 2022/2554 și a prezentului regulament în cazul în care această nerespectare duce la o lipsă a adeverinței menționate la articolul 26 alineatul (7) din Regulamentul (UE) 2022/2554, inclusiv în cazul în care această nerespectare este cauzată de încălcări ale confidențialității privind TLPT sau de absența unei conduite etice;

(c) escaladarea crizelor și a incidentelor;

(d) faza activă de tipul „echipa roșie”, inclusiv riscurile legate de întreruperea activităților critice și de coruperea datelor din cauza activităților entităților de testare, precum și impactul potențial al acesteia asupra terților;

(e) activitatea de tipul „echipa albastră”, inclusiv riscurile legate de întreruperea activităților critice și de coruperea datelor din cauza activităților echipei albastre, precum și impactul potențial al acesteia asupra terților;

(f) refacerea incompletă a sistemelor afectate de TLPT.

Articolul 6

Gestionarea riscurilor pentru TLPT-uri grupate sau comune

(1) În cazul unui TLPT comun sau al unui TLPT grupat, echipa de control a fiecărei entități financiare efectuează propria evaluare a riscurilor și își stabilește propriile măsuri de gestionare a riscurilor.

(2) Echipa de control a entității financiare desemnate menționate la articolul 16 alineatul (3) litera (b) din prezentul regulament sau a entității financiare desemnate în conformitate cu articolul 26 alineatul (4) din Regulamentul (UE) 2022/2554 evaluează riscurile legate de participarea la TLPT a mai multor entități financiare. Echipele de control ale entităților financiare implicate cooperează cu echipa de control a entității financiare desemnate pentru a identifica posibilele riscuri comune.

Articolul 7

Selectarea furnizorilor de TLPT

(1) Echipa de control ia măsuri pentru gestionarea riscurilor legate de TLPT și se asigură, în special, că, pentru fiecare TLPT:

(a) furnizorul de date operative privind amenințările și entitățile externe de testare furnizează echipei de control un *curriculum vitae* detaliat și copii ale certificărilor care, în conformitate cu standardele de piață recunoscute, sunt adecvate pentru desfășurarea activităților lor;

(b) furnizorul de date operative privind amenințările și entitatea externă de testare sunt acoperite în mod corespunzător și integral de asigurări adecvate de răspundere civilă profesională, inclusiv împotriva riscurilor de abatere și neglijență;

(c) furnizorul de date operative privind amenințările furnizează cel puțin trei referințe din misiuni anterioare în contextul testelor de penetrare și al testării de tipul „echipa roșie”;

(d) entitățile externe de testare furnizează cel puțin cinci referințe din misiuni anterioare legate de testele de penetrare și testarea de tipul „echipa roșie”;

(e) personalul furnizorului de date operative privind amenințările repartizat pentru TLPT:

(i) este alcătuit din cel puțin un manager cu cel puțin cinci ani de experiență în domeniul datelor operative privind amenințările și cel puțin un membru suplimentar cu cel puțin doi ani de experiență în domeniul datelor operative privind amenințările;

(ii) prezintă o gamă largă și un nivel adecvat de cunoștințe și competențe profesionale, inclusiv:

1. tactici, tehnici și proceduri de colectare a datelor operative;

2. cunoștințe geopolitice, tehnice și sectoriale;

3. competențe de comunicare adecvate pentru a prezenta în mod clar și a raporta cu privire la rezultatul angajamentului;

(iii) are o participare combinată la cel puțin trei misiuni anterioare de date operative privind amenințările în contextul testelor de penetrare și al testării de tipul „echipa roșie”;

(iv) nu îndeplinește simultan sarcini de tipul „echipa albastră” sau alte servicii care pot prezenta un conflict de interese în ceea ce privește entitatea financiară, furnizorul terț de servicii TIC sau un furnizor de servicii TIC intragrup implicat în TLPT la care este repartizat;

(v) este separat de personalul aceluiași furnizor de TLPT care pune la dispoziție entități externe de testare pentru același TLPT și nu este subordonat acestuia;

(f) pentru entitățile externe de testare, echipa roșie desemnată pentru TLPT:

(i) este alcătuită din cel puțin un manager, cu cel puțin cinci ani de experiență în testarea de penetrare și testarea de tipul „echipa roșie”, precum și din cel puțin două entități de testare suplimentare, fiecare cu teste de penetrare și testare de tipul „echipa roșie” de cel puțin doi ani;

(ii) prezintă o gamă largă și un nivel adecvat de cunoștințe și competențe profesionale, inclusiv cunoștințe despre activitatea entității financiare, recunoaștere, gestionarea riscurilor, dezvoltarea exploatării, penetrare fizică, inginerie socială, analiză a vulnerabilității, precum și competențe de comunicare adecvate pentru a prezenta în mod clar și a raporta cu privire la rezultatul angajamentului;

(iii) are o participare combinată la cel puțin cinci misiuni anterioare în legătură cu teste de penetrare și testare de tipul „echipa roșie”;

(iv) nu este angajată de un furnizor de date operative privind amenințările și nici nu furnizează servicii unui furnizor de date operative privind amenințările care îndeplinește simultan sarcini de tipul „echipa albastră” pentru o entitate financiară, un furnizor terț de servicii TIC sau un furnizor de servicii TIC intragrup care este implicat în TLPT;

(v) este separată de orice personal al aceluiași furnizor de TLPT care furnizează simultan servicii de date operative privind amenințările pentru același TLPT.

(g) entitățile de testare și furnizorul de date operative privind amenințările efectuează proceduri de restaurare la sfârșitul testării, inclusiv ștergerea securizată a informațiilor referitoare la parole, acreditări și alte chei secrete compromise în timpul TLPT, comunicarea securizată către entitățile financiare cu privire la conturile compromise, colectarea, stocarea, gestionarea și eliminarea în condiții de siguranță a altor date colectate în timpul testării;

(h) pe lângă procedurile de restaurare la sfârșitul testării menționate la litera (g), entitățile de testare efectuează următoarele proceduri de restaurare:

(i) dezactivarea comenzilor și a controalelor;

(ii) mecanisme de dezactivare automată în funcție de sfera de aplicare și de dată;

(iii) îndepărtarea ușilor secrete și a altor programe malware;

(iv) potențiala notificare a încălcării;

(v) proceduri de restaurare de rezervă viitoare care pot viza programe malware sau instrumente instalate în timpul testului;

(vi) monitorizarea activităților de tipul „echipa albastră” și informarea echipei de control cu privire la oricare detectări posibile;

(i) entitățile de testare și furnizorul de date operative privind amenințările nu desfășoară și nu participă la niciuna dintre următoarele activități:

(i) distrugerea neautorizată a echipamentelor entității financiare și ale furnizorilor săi terți de servicii TIC, dacă este cazul;

(ii) modificarea necontrolată a informațiilor și a activelor TIC ale entității financiare și ale furnizorilor săi terți de servicii TIC, dacă este cazul;

(iii) compromiterea intenționată a continuității funcțiilor critice sau importante ale entității financiare;

(iv) includerea neautorizată a sistemelor care nu intră în sfera de aplicare;

(v) divulgarea neautorizată a rezultatelor testelor.

(2) Echipa de control ține evidența documentației furnizate de entitățile de testare și de furnizorii de date operative privind amenințările pentru a demonstra conformitatea cu alineatul (1) literele (a)-(f).

În circumstanțe excepționale, entitățile financiare pot contracta entități externe de testare și furnizori externi de date operative privind amenințările care nu îndeplinesc una sau mai multe dintre cerințele prevăzute la alineatul(1) literele (a)-(f), cu condiția ca entitățile financiare respective să adopte măsuri adecvate pentru a atenua riscurile legate de nerespectarea acestor puncte și să înregistreze măsurile respective.

Articolul 8

Particularități pentru TLPT-uri grupate sau comune

(1) Cu excepția cazului în care autoritatea TLPT principală decide altfel, în cazul în care mai multe entități financiare, identificate în conformitate cu articolul 16 alineatul (2) sau (4), sunt implicate într-un TLPT grupat sau comun, fiecare entitate financiară urmează fiecare dintre etapele prevăzute la articolele 9-15.

(2) Cu excepția cazului în care se prevede altfel în prezentul regulament, în cazul în care mai multe autorități TLPT sunt implicate într-un TLPT comun sau într-un TLPT grupat, astfel cum se menționează la articolul 16 alineatul (3) sau (5), trimiterile de la articolele 9-15 la „autoritatea TLPT” se interpretează ca trimiteri la autoritatea TLPT principală pentru un astfel de TLPT grupat sau comun.

Articolul 9

Faza de pregătire

(1) O entitate financiară identificată în temeiul articolului 26 alineatul (8) al treilea paragraf din Regulamentul (UE) 2022/2554 inițiază un TLPT în urma unei notificări din partea autorității TLPT cu privire la efectuarea unui TLPT.

(2) În termen de trei luni de la primirea notificării menționate la alineatul (1), o entitate financiară transmite managerilor de testare toate informațiile următoare referitoare la inițierea TLPT:

(a) o cartă a proiectului care include un plan de proiect la nivel înalt, care conține informațiile prevăzute în anexa I;

(b) datele de contact ale șefului echipei de control;

(c) informații privind utilizarea preconizată a entităților interne sau externe de testare sau a ambelor tipuri de entități, după caz, astfel cum se detaliază la articolul 15;

(d) informații privind canalele de comunicare care urmează să fie utilizate în timpul TLPT;

(e) numele de cod pentru TLPT.

(3) În cazul în care informațiile menționate la alineatul (2) literele (a)-(e) sunt complete și asigură adecvarea și executarea eficace a TLPT, autoritatea TLPT validează informațiile de inițiere a TLPT ale entității financiare și notifică acest lucru entității financiare.

(4) În urma validării informațiilor privind inițierea TLPT de către autoritatea TLPT, entitatea financiară înființează o echipă de control pentru a sprijini șeful echipei de control în sarcinile sale de:

(a) specificare a canalelor și a proceselor de comunicare în cadrul echipei de control, cu entitățile de testare și cu furnizorii de date operative privind amenințările cu privire la toate aspectele legate de TLPT;

(b) informare a organului de conducere al entității financiare cu privire la evoluția TLPT și la riscurile asociate;

(c) luare de decizii pe baza expertizei în materie în cadrul TLPT;

(d) executare a TLPT în conformitate cu prezentul regulament;

(e) selectare a furnizorului de date operative privind amenințările pentru TLPT;

(f) selectare a entităților externe de testare, a entităților interne de testare sau a ambelor;

(g) elaborare a documentului privind specificarea sferei de aplicare.

(5) În cazul în care autoritatea TLPT consideră că atât componența inițială a echipei de control, cât și modificările ulterioare ale acesteia sunt adecvate pentru îndeplinirea sarcinilor menționate la alineatul (4), autoritatea TLPT validează echipa de control și notifică acest lucru șefului echipei de control.

(6) În termen de șase luni de la primirea notificării din partea autorității TLPT menționate la alineatul (1), entitatea financiară transmite managerilor de testare un document privind specificarea sferei de aplicare care conține toate informațiile prevăzute în anexa II. Organul de conducere al entității financiare aprobă documentul privind specificarea sferei de aplicare.

(7) Entitățile financiare iau în considerare următoarele criterii pentru includerea funcțiilor critice sau importante în sfera de aplicare a TLPT:

(a) caracterul critic sau importanța funcției și posibilul impact al acesteia asupra sectorului financiar și asupra stabilității financiare la nivelul Uniunii și la nivel național;

(b) importanța funcției pentru operațiunile curente ale entității financiare;

(c) posibilitatea de substituire a funcției;

(d) interconectarea cu alte funcții;

(e) amplasamentul geografic al funcției;

(f) dependența sectorială a altor entități de această funcție;

(g) în cazul în care sunt disponibile, date operative privind amenințările cu privire la funcție.

(8) Echipa de control transmite entităților de testare și furnizorilor de date operative privind amenințările, odată ce aceștia sunt contractați, informațiile privind inițierea TLPT și documentul privind specificarea sferei de aplicare. Echipa de control informează entitățile de testare și furnizorii de date operative privind amenințările cu privire la procesul de testare care trebuie urmat.

(9) Entitatea financiară se asigură că achiziția sau desemnarea entităților de testare și a furnizorilor de date operative privind amenințările este finalizată înainte de inițierea fazei de testare.

(10) Înainte de inițierea fazei de testare, echipa de control consultă managerii de testare cu privire la evaluarea riscurilor TLPT și la măsurile de gestionare a riscurilor. Echipa de control analizează evaluarea riscurilor sau măsurile de gestionare a riscurilor în cazul în care autoritatea TLPT consideră că acestea nu abordează în mod adecvat riscurile TLPT.

(11) Echipa de control evaluează dacă furnizorii de date operative privind amenințările și entitățile de testare pe care intenționează să îi includă în TLPT îndeplinesc cerințele prevăzute la articolul 27 din Regulamentul (UE) 2022/2554 și respectă dispozițiile articolului 7 alineatul (1) din prezentul regulament și documentează rezultatul evaluării respective. Echipa de control selectează furnizorii de date operative privind amenințările în conformitate cu evaluarea respectivă și cu practicile sale de gestionare a riscurilor. Înainte de a contracta furnizorii de date operative privind amenințările și entitățile externe de testare selectate, echipa de control furnizează managerilor de testare dovezi ale conformității respectivilor furnizori de date operative privind amenințările și respectivelor entități de testare cu cerințele prevăzute la articolul 27 din Regulamentul (UE) 2022/2554 și cu articolul 7 alineatul (1) din prezentul regulament. Echipa de control nu încheie contracte cu furnizorii de date operative privind amenințările selectați și cu entitățile externe de testare selectate în cazul în care autoritatea TLPT consideră că furnizorii de date operative privind amenințările selectați și entitățile externe de testare selectate nu respectă cerințele prevăzute la articolul 27 din Regulamentul (UE) 2022/2554 sau cerințele prevăzute la articolul 7 alineatul (1) din prezentul regulament sau cerințele suplimentare care decurg din legislațiile naționale în materie de securitate în conformitate cu dreptul Uniunii sau în cazul în care entitatea financiară nu respectă articolul 7 alineatul (2) primul paragraf din prezentul regulament sau în cazul în care nu sunt îndeplinite circumstanțele menționate la articolul 7 alineatul (2) al doilea paragraf din prezentul regulament.

(12) În cazul în care documentul privind specificarea sferei de aplicare este complet și asigură executarea unui TLPT adecvat și eficace, autoritatea TLPT aprobă documentul respectiv și informează șeful echipei de control cu privire la acest lucru.

Articolul 10

Faza de testare: date operative privind amenințările

(1) În urma aprobării documentului privind specificarea sferei de aplicare de către autoritatea TLPT, furnizorul de date operative privind amenințările analizează datele operative privind amenințările generice și specifice sectorului relevante pentru entitatea financiară. În cazul în care autoritatea TLPT a furnizat un peisaj generic al amenințărilor pentru sectorul financiar al unui stat membru, furnizorul de date operative privind amenințările poate utiliza acest peisaj ca referință pentru peisajul amenințărilor naționale. Furnizorul de date operative privind amenințările identifică amenințările cibernetice și vulnerabilitățile existente sau potențiale în ceea ce privește entitatea financiară. În plus, furnizorul de date operative privind amenințările colectează informații privind entitatea financiară și analizează date operative concrete, executabile și contextualizate privind amenințările vizând entitatea financiară, inclusiv prin consultarea echipei de control și a managerilor de testare.

(2) Furnizorul de date operative privind amenințările prezintă amenințările relevante și datele operative specifice privind amenințările și propune scenariile necesare echipei de control, entităților de testare și managerilor de testare. Scenariile propuse diferă în ceea ce privește actorii de amenințare identificați și tacticile, tehnicile și procedurile asociate și vizează fiecare funcție critică sau importantă din sfera de aplicare a TLPT.

(3) Șeful echipei de control selectează cel puțin trei scenarii pentru efectuarea TLPT pe baza tuturor elementelor următoare:

(a) recomandarea furnizorului de date operative privind amenințările și natura bazată pe amenințări a fiecărui scenariu;

(b) contribuțiile furnizate de managerii de testare;

(c) fezabilitatea scenariilor propuse pentru executare, pe baza opiniei experților entităților de testare;

(d) dimensiunea, complexitatea și profilul general de risc al entității financiare, precum și natura, amploarea și complexitatea serviciilor, activităților și operațiunilor sale.

(4) Cel mult unul dintre scenariile selectate poate să nu se bazeze pe amenințări și se poate baza pe o amenințare prospectivă și potențial fictivă cu o valoare predictivă, anticipativă, oportunistă sau prospectivă ridicată, având în vedere evoluțiile anticipate ale peisajului amenințărilor în ceea ce privește entitatea financiară.

Pentru TLPT-urile grupate, fără a aduce atingere scenariilor care vizează în mod direct funcțiile critice sau importante ale entităților financiare implicate în testare, cel puțin un scenariu include sistemele, procesele și tehnologiile TIC subiacente relevante ale furnizorului terț de servicii TIC care sprijină funcțiile critice sau importante ale entităților financiare care intră în sfera de aplicare.

În cazul în care testul este un TLPT comun care implică un furnizor de servicii TIC intragrup, fără a aduce atingere scenariilor care vizează în mod direct funcțiile critice sau importante ale entităților financiare implicate în testare, cel puțin un scenariu include sistemele, procesele și tehnologiile TIC subiacente relevante ale furnizorului de servicii TIC intragrup care sprijină funcțiile critice sau importante ale entităților financiare care intră în sfera de aplicare.

(5) Furnizorul de date operative privind amenințările furnizează echipei de control raportul referitor la date operative specifice privind amenințările, inclusiv scenariile selectate în conformitate cu alineatele (3) și (4). Raportul referitor la datele operative privind amenințările conține informațiile prevăzute în anexa III.

(6) Echipa de control prezintă managerului de testare, spre aprobare, raportul referitor la datele operative privind amenințările specifice. În cazul în care raportul referitor la datele operative privind amenințările specifice este complet și asigură executarea unui TLPT adecvat și eficace, autoritatea TLPT aprobă raportul referitor la datele operative privind amenințările specifice și informează șeful echipei de control cu privire la acest lucru.

Articolul 11

Faza de testare: testul de tipul „echipa roșie”

(1) În urma aprobării raportului referitor la datele operative privind amenințările specifice de către autoritatea TLPT, entitățile de testare pregătesc planul testării de tipul „echipa roșie” care conține informațiile prevăzute în anexa IV. Entitățile de testare utilizează documentul privind specificarea sferei de aplicare și raportul referitor la datele operative privind amenințările specifice ca bază pentru elaborarea scenariilor de atac.

(2) Entitățile de testare consultă echipa de control, furnizorul de date operative privind amenințările și managerii de testare cu privire la planul testării de tipul „echipa roșie”, inclusiv modalitățile de comunicare, de procedură și de management de proiect, pregătirea și cazurile de utilizare pentru activarea ajutorului, precum și acordurile de raportare către echipa de control și managerii de testare.

(3) În cazul în care planul testării de tipul „echipa roșie” este complet și asigură efectuarea unui TLPT eficace, echipa de control și autoritatea TLPT aprobă planul testării de tipul „echipa roșie”, iar TLPT informează șeful echipei de control cu privire la acest lucru.

(4) După aprobarea planului testării de tipul „echipa roșie” în conformitate cu alineatul (3), entitățile de testare efectuează TLPT în timpul fazei de testare activă de tipul „echipa roșie”.

(5) Durata fazei de testare activă de tipul „echipa roșie” este proporțională cu sfera de aplicare a TLPT, cu amploarea, activitatea, complexitatea și numărul entităților financiare și al furnizorilor terți de servicii TIC sau al furnizorilor de servicii TIC intragrup implicați în TLPT și, în orice caz, durează cel puțin 12 săptămâni. Scenariile de atac pot fi executate succesiv sau în același timp. Echipa de control, furnizorul de date operative privind amenințările, entitățile de testare și managerii de testare convin asupra încheierii fazei de testare activă de tipul „echipa roșie”.

(6) Sub rezerva asigurării faptului că planul testării de tipul „echipa roșie” rămâne complet și permite efectuarea unui TLPT eficace, șeful echipei de control și managerii de testare aprobă orice modificare a planului testării de tipul „echipa roșie” după aprobarea acestuia, inclusiv în ceea ce privește calendarul, sfera de aplicare, sistemele țintă sau semnalele de alarmă.

(7) Pe parcursul întregii faze de testare activă de tipul „echipa roșie”, entitățile de testare raportează cel puțin săptămânal echipei de control și managerilor de testare progresele înregistrate în cadrul TLPT, iar furnizorul de date operative privind amenințările rămâne disponibil pentru consultare și date operative suplimentare privind amenințările atunci când echipa de control solicită acest lucru.

(8) Echipa de control furnizează în timp util ajutoare concepute pe baza planului testării de tipul „echipa roșie”. Ajutoarele pot fi adăugate sau adaptate în urma aprobării de către echipa de control și de către managerii de testare.

(9) În cazul detectării activităților de testare de către orice membru al personalului entității financiare sau de către furnizorii terți de servicii TIC ai acesteia sau de către furnizorul său de servicii TIC intragrup, după caz, atunci, în consultare cu entitățile de testare și fără a aduce atingere alineatului (10), echipa de control propune și prezintă managerilor de testare, în vederea validării, măsuri care să permită continuarea TLPT, asigurând în același timp caracterul secret al acestuia.

(10) În circumstanțe excepționale care generează riscuri de impact asupra datelor, daune aduse activelor și perturbări ale funcțiilor, serviciilor sau operațiunilor critice sau importante ale entității financiare înseși, ale furnizorilor săi terți de servicii TIC sau ale furnizorilor săi de servicii TIC intragrup sau perturbări ale contrapărților sale sau ale sectorului financiar, șeful echipei de control poate suspenda TLPT sau, în ultimă instanță, în cazul în care continuarea TLPT nu este posibilă în alt mod și sub rezerva validării prealabile de către autoritatea TLPT, poate continua TLPT utilizând un exercițiu limitat de tipul „echipa violet”. Durata exercițiului limitat de tipul „echipa violet” se ia în considerare în sensul duratei minime de 12 săptămâni a fazei de testare activă de tipul „echipa roșie” menționate la alineatul (5).

Articolul 12

Faza de încheiere

(1) După încheierea fazei de testare activă de tipul „echipa roșie”, șeful echipei de control informează echipa albastră că a avut loc un TLPT.

(2) În termen de patru săptămâni de la sfârșitul fazei de testare activă de tipul „echipa roșie”, entitățile de testare prezintă echipei de control un raport privind testarea de tipul „echipa roșie” care conține informațiile prevăzute în anexa V.

(3) Echipa de control furnizează fără întârzieri nejustificate echipei albastre și managerilor de testare raportul testării de tipul „echipa roșie”.

La cererea managerilor de testare, raportul menționat la primul paragraf nu conține informații sensibile.

(4) La primirea raportului testării de tipul „echipa roșie” și în termen de cel mult 10 săptămâni de la încheierea fazei de testare activă de tipul „echipa roșie”, echipa albastră prezintă echipei de control un raport al testării de tipul „echipa albastră” care conține informațiile prevăzute în anexa VI. Echipa de control furnizează fără întârzieri nejustificate raportul testării de tipul „echipa albastră” entităților de testare și managerilor de testare.

La cererea managerilor de testare, raportul menționat la primul paragraf nu conține informații sensibile.

(5) În termen de cel mult 10 săptămâni de la încheierea fazei de testare activă de tipul „echipa roșie”, echipa albastră și entitățile de testare reiau acțiunile ofensive și defensive desfășurate în timpul TLPT. Echipa de control efectuează, de asemenea, un exercițiu de tipul „echipa violet” pe teme identificate în comun de echipa albastră și de entitățile de testare, pe baza vulnerabilităților identificate în timpul testului și, după caz, a aspectelor care nu au putut fi testate în timpul fazei de testare activă de tipul „echipa roșie”.

(6) După încheierea exercițiilor de reluare și a celor de tipul „echipa violet”, echipa de control, echipa albastră, entitățile de testare și furnizorii de date operative privind amenințările își oferă reciproc feedback cu privire la procesul TLPT. Managerii de testare pot oferi feedback.

(7) După ce autoritatea TLPT a notificat șefului echipei de control că a constatat că raportul testării de tipul „echipa albastră” și raportul testării de tipul „echipa roșie” conțin informațiile prevăzute în anexele V și VI, entitatea financiară transmite autorității TLPT, în termen de opt săptămâni, în vederea aprobării, raportul care sintetizează constatările relevante ale TLPT, astfel cum se menționează la articolul 26 alineatul (6) din Regulamentul (UE) 2022/2554, care conține elementele prevăzute în anexa VII.

La cererea autorității TLPT, raportul menționat la primul paragraf nu conține informații sensibile.

Articolul 13

Planul de remediere

(1) În termen de opt săptămâni de la notificarea menționată la articolul 12 alineatul (7) din prezentul regulament, entitatea financiară furnizează autorității TLPT și, dacă sunt diferite, autorității competente a entității financiare planurile de remediere și documentația menționată la articolul 26 alineatul (6) din Regulamentul (UE) 2022/2554.

(2) Planul de remediere menționat la alineatul (1) include, pentru fiecare constatare efectuată în cadrul TLPT:

(a) o descriere a deficiențelor identificate;

(b) o descriere a măsurilor de remediere propuse și a stabilirii priorităților acestora și a finalizării preconizate a acestora, inclusiv, după caz, măsuri de îmbunătățire a capacităților de identificare, protecție, detectare și răspuns;

(c) analiza cauzelor principale;

(d) personalul sau funcțiile entității financiare responsabile cu punerea în aplicare a măsurilor de remediere sau a îmbunătățirilor propuse;

(e) riscurile asociate nepunerii în aplicare a măsurilor menționate la litera (b) și, după caz, riscurile asociate punerii în aplicare a acestor măsuri.

Articolul 14

Adeverință

1. Adeverința menționată la articolul 26 alineatul (7) din Regulamentul (UE) 2022/2554 conține informațiile prevăzute în anexa VIII.

2. În cazul în care mai multe autorități TLPT au fost implicate într-un TLPT, autoritatea TLPT principală furnizează entităților financiare testate adeverința menționată la articolul 26 alineatul (7) din Regulamentul (UE) 2022/2554.

Articolul 15

Utilizarea entităților interne de testare

(1) Entitățile financiare stabilesc toate modalitățile următoare pentru utilizarea entităților interne de testare:

(a) instituirea și punerea în aplicare a unei politici de gestionare a entităților interne de testare în cadrul unui TLPT;

(b) măsuri prin care să se asigure că utilizarea entităților interne de testare pentru a efectua un TLPT nu are un impact negativ asupra capacităților generale de apărare sau de reziliență ale entității financiare în ceea ce privește incidentele legate de TIC sau nu are un impact semnificativ asupra disponibilității resurselor dedicate sarcinilor legate de TIC pe durata unui TLPT;

(c) măsuri pentru a se asigura că entitățile interne de testare dispun de resurse și capacități suficiente pentru a efectua un TLPT.

Politica menționată la litera (a):

(a) conține criterii de evaluare a caracterului adecvat, a competenței și a potențialelor conflicte de interese ale entităților interne de testare și specifică responsabilitățile de gestionare în procesul de testare;

(b) este documentată și revizuită periodic;

(c) prevede că entitatea internă de testare include un conducător al testului și cel puțin doi membri suplimentari;

(d) impune ca toți membrii echipei de testare să fi fost angajați de entitatea financiară sau de un furnizor de servicii TIC intragrup în ultimele 12 luni;

(e) include dispoziții privind formarea cu privire la modul de efectuare a testelor de penetrare și a testării de tipul „echipa roșie” de către entitățile interne de testare.

(2) În cazul în care o autoritate TLPT aprobă utilizarea entităților interne de testare în conformitate cu articolul 27 alineatul (2) litera (a) din Regulamentul (UE) 2022/2554, autoritatea TLPT ia în considerare cerințele prevăzute la articolul 7 alineatul (1) din prezentul regulament.

(3) Atunci când utilizează entități interne de testare, entitatea financiară se asigură că această utilizare este menționată în următoarele documente:

(a) informațiile referitoare la inițierea testului menționate la articolul 9;

(b) raportul testării de tipul „echipa roșie” menționat la articolul 12 alineatul (2);

(c) raportul care sintetizează constatările relevante ale TLPT menționate la articolul 26 alineatul (6) din Regulamentul (UE) 2022/2554.

(4) Entitățile de testare angajate de un furnizor de servicii TIC intragrup sunt considerate entități interne de testare ale entității financiare.

Articolul 16

Cooperare și recunoaștere reciprocă

(1) În scopul efectuării unui TLPT în legătură cu o entitate financiară care furnizează servicii în mai multe state membre, inclusiv prin intermediul unei sucursale, autoritatea TLPT:

(a) stabilește autoritățile TLPT din statele membre gazdă care sunt implicate, luând în considerare dacă una sau mai multe funcții critice sau importante sunt desfășurate sau partajate în statele membre gazdă;

(b) informează autoritățile TLPT identificate în conformitate cu litera (a) cu privire la decizia de a efectua un test TLPT asupra entității financiare;

(c) cu excepția cazului în care autoritățile TLPT convin altfel, autoritatea TLPT a entității financiare conduce TLPT.

Autoritățile TLPT din statele membre gazdă pot, în termen de 20 de zile lucrătoare de la primirea interesul de a observa TLPT în calitate de observatori, fie să desemneze un manager de testare care să participe la TLPT. Autoritatea TLPT principală furnizează tuturor autorităților TLPT care acționează în calitate de observatori în TLPT documentul privind specificarea sferei de aplicare, raportul de sinteză al testului, planul de remediere și adeverința.

Autoritatea TLPT principală coordonează toate autoritățile TLPT participante pe tot parcursul testului și adoptă toate deciziile necesare pentru a efectua TLPT în mod corespunzător și eficace. Autoritatea TLPT principală poate stabili un număr maxim de autorități informațiilor privind efectuarea în viitor a unui TLPT, fie să își exprime TLPT participante, în caz contrar desfășurarea eficientă a TLPT putând fi compromisă.

(2) În cazul în care o entitate financiară utilizează același furnizor de servicii TIC intragrup ca entitățile financiare stabilite în alte state membre sau aparține unui grup și partajează sisteme TIC cu entități financiare din același grup stabilite în alte state membre, autoritatea TLPT a entității financiare contactează autoritățile TLPT ale celorlalte entități financiare care utilizează același furnizor de servicii TIC intragrup sau care partajează sisteme TIC ca parte a grupului și evaluează împreună cu acestea fezabilitatea și caracterul adecvat al efectuării unui TLPT comun în privința acestora. Un TLPT comun este preferat unui TLPT individual în cazul în care poate duce la reducerea costurilor și a resurselor pentru entitățile financiare și pentru autoritățile TLPT, cu condiția să nu se aducă atingere rigurozității și eficacității testării.

(3) În scopul efectuării unui TLPT comun:

(a) autoritățile TLPT ale entităților financiare convin asupra entității financiare care va fi desemnată să efectueze TLPT, având în vedere structura grupului și eficiența testului;

(b) autoritatea TLPT a entității financiare desemnate în conformitate cu litera (a) conduce TLPT, cu excepția cazului în care autoritățile TLPT ale entităților financiare care participă la TLPT comun convin altfel;

(c) autoritățile TLPT ale entităților financiare, altele decât entitatea financiară desemnată să conducă TLPT comun, pot fie să își exprime interesul de a observa TLPT în calitate de observatori, fie să desemneze un manager de testare pentru TLPT în cauză.

Autoritatea TLPT principală coordonează toate autoritățile TLPT implicate în TLPT comun și adoptă toate deciziile necesare pentru efectuarea TLPT comun în mod riguros și eficient.

(4) În cazul în care o entitate financiară intenționează să efectueze un TLPT grupat, astfel cum se menționează la articolul 26 alineatul (4) din Regulamentul (UE) 2022/2554, care ar putea implica entități financiare stabilite în alte state membre, autoritatea TLPT a acesteia contactează autoritățile TLPT ale celorlalte entități financiare și evaluează împreună cu acestea fezabilitatea și caracterul adecvat al efectuării unui TLPT grupat în privința acestora, în conformitate cu articolul 26 alineatul (4) din Regulamentul (UE) 2022/2554.

(5) În scopul efectuării unui TLPT grupat, astfel cum se menționează la articolul 26 alineatul (4) din Regulamentul (UE) 2022/2554:

(a) autoritățile TLPT ale entităților financiare convin asupra entității financiare care este desemnată să efectueze TLPT grupat, având în vedere serviciile TIC furnizate de furnizorul terț de servicii TIC entităților financiare și eficiența testului;

(b) autoritatea TLPT a entității financiare desemnate în conformitate cu litera(a) conduce TLPT, cu excepția cazului în care autoritățile TLPT ale entităților financiare care participă la TLPT grupat convin altfel;

(c) autoritățile TLPT ale entităților financiare, altele decât entitatea financiară desemnată să conducă TLPT grupat, pot fie să își exprime interesul de a observa TLPT în calitate de observatori, fie să desemneze un manager de testare pentru TLPT în cauză.

Autoritatea TLPT principală coordonează toate autoritățile TLPT implicate în TLPT grupat și adoptă toate deciziile necesare pentru efectuarea TLPT grupat în mod riguros și eficient.

(6) În cazul în care, în ceea ce privește o entitate financiară care trebuie să efectueze un TLPT, autoritatea TLPT a acesteia diferă de autoritatea sa competentă, astfel cum se menționează la articolul 46 din Regulamentul (UE) 2022/2554, autoritățile respective fac schimb de informații relevante cu privire la toate aspectele legate de TLPT în scopul efectuării TLPT sau al îndeplinirii sarcinilor care le revin în conformitate cu regulamentul respectiv.

Articolul 17

Intrarea în vigoare

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 13 februarie 2025.

Pentru Comisie
Președinta
Ursula VON DER LEYEN

ANEXA I

Conținutul cartei proiectului [articolul 9 alineatul (2) litera (a)]

Informație	Informații necesare
Persoana responsabilă cu planul de proiect, și anume șeful echipei de control	Nume Date de contact
Entități de testare	☐ interne ☐ externe ☐ ambele
Canalele de comunicare selectate în conformitate cu articolul 9 alineatul (2) litera (d) și cu articolul 9 alineatul (4) litera (a), inclusiv: (a) criptarea e-mailurilor care urmează să fie utilizată (b) camerele de date online care urmează să fie utilizate (c) mesageria instantanee care urmează să fie utilizată	
Numele de cod pentru TLPT	
Dacă există, funcții critice sau importante pe care le desfășoară entitatea financiară în alte state membre	1. lista funcțiilor critice sau importante desfășurate într-un alt stat membru 2. pentru fiecare funcție critică sau importantă, indicarea statului membru sau a statelor membre în care se desfășoară
Dacă există, funcții critice sau importante sprijinite de furnizori terți de servicii TIC	3. lista funcțiilor critice sau importante sprijinite de furnizori terți de servicii TIC 4. pentru fiecare funcție, identificarea furnizorului terț de servicii TIC
Termene preconizate pentru finalizarea:	
1. fazei de pregătire, în conformitate cu articolul 9	aaaa-ll-zz
2. fazei de testare, în conformitate cu articolele 10 și 11	aaaa-ll-zz
3. fazei de încheiere, în conformitate cu articolul 12	aaaa-ll-zz
4. planului de remediere în conformitate cu articolul 13	aaaa-ll-zz

ANEXA II

Conținutul documentului privind specificarea sferei de aplicare [articolul 9 alineatul (6)]

1. Documentul privind specificarea sferei de aplicare conține o listă a tuturor funcțiilor critice sau importante identificate de entitatea financiară.

2. Pentru fiecare funcție critică sau importantă identificată, se includ următoarele informații:
   (a) în cazul în care funcția critică sau importantă nu este inclusă în sfera de aplicare a TLPT, explicarea motivelor pentru care nu este inclusă;
   (b) în cazul în care funcția critică sau importantă este inclusă în sfera de aplicare a TLPT:
      (i) explicarea motivelor includerii sale;
      (ii) sistemul (sistemele) TIC identificat(e) care sprijină respectiva funcție critică sau importantă;
      (iii) pentru fiecare sistem TIC identificat:
         1. dacă este externalizat și, în caz afirmativ, numele furnizorului terț de servicii TIC;
         2. jurisdicțiile în care este utilizat sistemul TIC;
         3. o descriere de nivel înalt a semnalului (semnalelor) de alarmă preliminar(e), indicând aspectul de securitate a confidențialității, a integrității, a autenticității sau a disponibilității care este vizat de fiecare semnal de alarmă.

ANEXA III

Conținutul raportului referitor la datele operative specifice privind amenințările [articolul 10 alineatul (5)]

Raportul referitor la datele operative specifice privind amenințările conține informații cu privire la toate elementele următoare:

1. Sfera de aplicare generală a cercetării în domeniul datelor operative, incluzând cel puțin următoarele:
   (a) funcții critice sau importante din sfera de aplicare;
   (b) amplasamentul geografic;
   (c) limba oficială a UE utilizată;
   (d) furnizorii terți de servicii TIC relevanți;
   (e) perioada în care se realizează cercetarea.
2. Evaluarea generală a datelor operative executabile concrete care pot fi găsite cu privire la entitatea financiară, inclusiv:
   (a) numele de utilizator și parolele angajaților;
   (b) domeniile similare care pot fi confundate cu domeniile oficiale ale entității financiare;
   (c) recunoașterea tehnică: software, sisteme și tehnologii vulnerabile sau exploatabile;
   (d) informații publicate de angajați pe internet, referitoare la entitatea financiară, care ar putea fi utilizate în scopul unui atac;
   (e) informații de vânzare pe *dark net*;
   (f) alte informații relevante disponibile pe internet sau în rețelele publice;
   (g) după caz, informații de direcționare fizică, inclusiv modalități de acces la sediul entității financiare.
3. Analiza datelor operative privind amenințările, având în vedere peisajul general al amenințărilor și situația specifică a entității financiare, inclusiv, cel puțin:
   (a) mediul geopolitic;
   (b) mediul economic;
   (c) tendințele tehnologice și alte tendințe legate de activitățile din sectorul serviciilor financiare.
4. Profilurile de amenințare ale actorilor rău-intenționați (o anumită persoană/un anumit grup sau o clasă generică) care pot viza entitatea financiară, inclusiv sistemele entității financiare care sunt susceptibile de a fi compromise sau vizate de actorii rău-intenționați, posibila motivație, intenție și justificare pentru potențiala direcționare și modul de operare posibil al atacatorilor.
5. Scenarii de amenințare: cel puțin trei scenarii de amenințare de la un capăt la altul pentru profilurile de amenințare identificate în conformitate cu punctul 4, care prezintă cele mai mari punctaje în ceea ce privește gravitatea amenințării. Scenariile de amenințare descriu calea de atac de la un capăt la altul și includ cel puțin:
   (a) un scenariu care include, dar nu se limitează la compromiterea disponibilității serviciului;
   (b) un scenariu care include, dar nu se limitează la compromiterea integrității datelor;
   (c) un scenariu care include, dar nu se limitează la compromiterea confidențialității informațiilor.
6. După caz, o descriere a scenariului care nu este bazat pe amenințări menționat la articolul 10 alineatul (4).

ANEXA IV

Conținutul planului testării de tipul „echipa roșie” [articolul 11 alineatul (1)]

Planul testării de tipul „echipa roșie” conține informații cu privire la toate elementele următoare:

(a) canalele și procedurile de comunicare;

(b) tacticile, tehnicile și procedurile permise și nepermise a fi utilizate în atac, inclusiv limitele de natură etică pentru ingineria socială;

(c) măsurile de gestionare a riscurilor pe care trebuie să le urmeze entitățile de testare;

(d) o descriere pentru fiecare scenariu, inclusiv:

  (i) actorul de amenințare simulat;

  (ii) intenția, motivația și obiectivele sale;

  (iii) funcția (funcțiile) țintă și sistemul sau sistemele TIC de sprijin;

  (iv) aspectele vizate legate de confidențialitate, integritate, disponibilitate și autenticitate;

  (v) semnale de alarmă;

(e) o descriere detaliată a fiecărei căi de atac preconizate, inclusiv condițiile prealabile și eventualele ajutoare care urmează să fie furnizate de echipa de control, inclusiv termenele pentru furnizarea acestora și utilizarea potențială a acestora;

(f) programarea activităților de tipul „echipa roșie”, inclusiv planificarea cronologică pentru executarea fiecărui scenariu, defalcată cel puțin în funcție de cele trei faze pe care le parcurge entitatea de testare pe parcursul fazei de testare, și anume intrarea în sistemele TIC ale entităților financiare, trecerea prin sistemele TIC și, în cele din urmă, executarea acțiunilor privind obiectivele urmată, ca ultim punct, de extragerea din sistemele TIC (fazele de intrare, trecere și ieșire);

(g) particularitățile infrastructurii entităților financiare care trebuie luate în considerare în cursul testării;

(h) dacă este cazul, informații suplimentare sau alte resurse necesare entităților de testare pentru executarea scenariilor.

ANEXA V

Conținutul raportului testării de tipul „echipa roșie” [articolul 12 alineatul (2)]

Raportul testării de tipul „echipa roșie” conține informații cu privire la cel puțin toate elementele următoare:

(a) informații privind atacul efectuat, inclusiv:

  (i) funcțiile critice sau importante vizate și sistemele, procesele și tehnologiile TIC identificate care sprijină funcția critică sau importantă, astfel cum sunt identificate în planul testării de tipul „echipa roșie”;

  (ii) rezumatul fiecărui scenariu;

  (iii) semnalele de alarmă atinse și neatinse;

  (iv) căi de atac urmate cu succes și fără succes;

  (v) tactici, tehnici și proceduri utilizate cu succes și fără succes;

  (vi) abateri de la planul testării de tipul „echipa roșie”, dacă este cazul;

  (vii) ajutoare acordate, dacă este cazul;

(b) toate acțiunile cunoscute entităților de testare care au fost efectuate de echipa albastră pentru a reconstrui atacul și a atenua efectele acestuia;

(c) vulnerabilitățile descoperite și alte constatări, inclusiv:

  (i) descrierea vulnerabilității și a altor constatări, inclusiv caracterul critic al acestora;

  (ii) analiza cauzelor principale ale atacurilor reușite;

  (iii) recomandări pentru remediere, inclusiv indicarea priorității de remediere.

ANEXA VI

Conținutul raportului testării de tipul „echipa albastră” [articolul 12 alineatul (4)]

Raportul testării de tipul „echipa albastră” conține informații cu privire la cel puțin toate elementele următoare:

1. pentru fiecare etapă de atac descrisă de entitățile de testare în raportul testării de tipul „echipa roșie”:
   (a) lista acțiunilor de atac detectate;
   (b) înregistrări în registru corespunzătoare acestor detectări;
2. evaluarea constatărilor și a recomandărilor entităților de testare;
3. dovezi ale atacului din partea entităților de testare, colectate de echipa albastră;
4. analiza echipei albastre privind cauzele principale ale atacurilor reușite ale entităților de testare;
5. lista învățămintelor desprinse și potențialul de îmbunătățire identificat;
6. lista subiectelor care urmează să fie abordate în cadrul activității de tipul „echipa violet”.

ANEXA VII

Detalii ale raportului care sintetizează constatările relevante ale TLPT menționate la articolul 26 alineatul (6) din Regulamentul (UE) 2022/2554

Raportul de sinteză al testului conține informații cu privire la cel puțin toate elementele următoare:

(a) părțile implicate;

(b) planul proiectului;

(c) sfera de aplicare validată, inclusiv justificarea includerii sau a excluderii funcțiilor critice sau importante și a sistemelor, proceselor și tehnologiilor TIC identificate care sprijină funcțiile critice sau importante vizate de TLPT;

(d) scenarii selectate și orice abatere semnificativă de la raportul referitor la datele operative specifice privind amenințările;

(e) căile de atac executate și tactici, tehnici și proceduri utilizate;

(f) semnale de alarmă capturate și necapturate;

(g) abateri de la planul testării de tipul „echipa roșie”, dacă este cazul;

(h) detectările realizate de echipa albastră, dacă este cazul;

(i) activități de tipul „echipa violet” în faza de testare, în cazul în care sunt efectuate, și condițiile aferente;

(j) ajutoarele utilizate, dacă este cazul;

(k) măsurile de gestionare a riscurilor luate;

(l) vulnerabilitățile identificate și alte constatări, inclusiv caracterul critic al acestora;

(m) analiza cauzelor principale ale atacurilor reușite;

(n) plan la nivel înalt pentru remediere, corelând vulnerabilitățile și alte constatări, cauzele principale ale acestora și prioritatea remedierii;

(o) învățămintele desprinse din feedbackul primit.

ANEXA VIII

Detalii privind adeverința TLPT menționată la articolul 26 alineatul (7) din Regulamentul (UE) 2022/2554

Adeverința trebuie să includă cel puțin toate informațiile următoare:

(a) în ceea ce privește TLPT efectuat:

(i) datele de începere și de încheiere a TLPT;

(ii) funcțiile critice sau importante care intră în sfera de aplicare a testului;

(iii) după caz, informații privind funcțiile critice sau importante care intră în sfera de aplicare a testului în legătură cu care nu a fost efectuat TLPT;

(iv) după caz, alte entități financiare care au fost implicate în TLPT;

(v) după caz, furnizorii terți de servicii TIC care au participat la TLPT;

(vi) în ceea ce privește entitățile de testare:

1. dacă au fost utilizate entități interne de testare;

2. dacă entitatea financiară a utilizat articolul 5 alineatul (3) al doilea paragraf;

(vii) durata, în zile calendaristice, a fazei de testare activă de tipul „echipa roșie”;

(b) în cazul în care mai multe autorități TLPT au fost implicate în TLPT, celelalte autorități TLPT și calitatea acestora;

(c) lista documentelor examinate de autoritatea TLPT în scopul eliberării adeverinței.