



2025/1190

18.6.2025.

DELEGIRANA UREDBA KOMISIJE (EU) 2025/1190

od 13. veljače 2025.

o dopuni Uredbe (EU) 2022/2554 Europskog parlamenta i Vijeća u pogledu regulatornih tehničkih standarda kojima se utvrđuju kriteriji za određivanje koji su financijski subjekti dužni provoditi penetracijsko testiranje vođeno prijetnjama, zahtjevi i standardi koji se primjenjuju na angažiranje unutarnjih provoditelja testiranja, zahtjevi povezani s opsegom i metodologijom testiranja i pristupom svakoj pojedinačnoj fazi testiranja, rezultatima, završetkom testiranja i fazama testiranja koje se odnose na ispravljanje nedostataka te vrsta nadzorne suradnje i drugi relevantni oblici suradnje koji su potrebni za provedbu TLPT-a i olakšavanje njegova uzajamnog priznavanja

(Tekst značajan za EGP)

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 ⁽¹⁾, a posebno njezin članak 26. stavak 11. četvrti podstavak,

budući da:

- (1) Ova je Uredba izrađena u skladu s okvirom TIBER-EU i sadržava metodologiju, postupak i strukturu penetracijskog testiranja vođenog prijetnjama (TLPT) kako je opisano u tom okviru. Financijski subjekti koji imaju obvezu provedbe TLPT-a mogu primjenjivati i upućivati na okvir TIBER-EU ili jedan od oblika njegove provedbe na nacionalnoj razini pod uvjetom da su taj okvir ili provedba u skladu sa zahtjevima utvrđenima u člancima 26. i 27. Uredbe (EU) 2022/2554 i ovoj Uredbi. Imenovanje jedinstvenog tijela javne vlasti u financijskom sektoru koje je odgovorno za pitanja povezana s TLPT-om na nacionalnoj razini u skladu s člankom 26. stavkom 9. Uredbe (EU) 2022/2554 ne bi trebalo dovoditi u pitanje nadležnost tijela za nadzor određenih financijskih subjekata na razini Unije u skladu s člankom 46. te uredbe, kao što je, na primjer, nadležnost Europske središnje banke za značajne kreditne institucije koje se smatraju nadležnima za pitanja povezana s TLPT-om. Ako su samo neke zadaće koje su povezane s TLPT-ima delegirane drugom nacionalnom tijelu u financijskom sektoru u skladu s člankom 26. stavkom 10. Uredbe (EU) 2022/2554, tijelo nadležno nad financijskim subjektom iz članka 46. te uredbe trebalo bi ostati tijelo nadležno za zadaće povezane s TLPT-om koje nisu delegirane.
- (2) S obzirom na složenost TLPT-a i s njim povezane rizike, njegova bi primjena trebala biti ograničena na one financijske subjekte za koje je opravdana. Stoga bi tijela odgovorna za pitanja TLPT-a (tijela za TLPT na razini Unije ili na nacionalnoj razini) trebala iz opsega TLPT-a isključiti one financijske subjekte koji posluju u podsektorima ključnih financijskih usluga za koje TLPT nije opravdan. To znači da bi kreditne institucije, institucije za platni promet i elektronički novac, središnji depozitoriji vrijednosnih papira, središnje druge ugovorne strane, mjesta trgovanja, društva za osiguranje i društva za reosiguranje, iako ispunjavaju kvantitativne kriterije, mogli biti oslobođeni obveze provedbe TLPT-a na temelju opće procjene njihova profila IKT rizičnosti i stupnja zrelosti, učinka na financijski sektor i povezanih pitanja financijske stabilnosti.
- (3) Tijela za TLPT trebala bi na temelju opće procjene profila IKT rizičnosti i stupnja zrelosti, učinka na financijski sektor i povezanih pitanja financijske stabilnosti procijeniti bi li bilo koja vrsta financijskog subjekta osim kreditnih institucija, institucija za platni promet, institucija za elektronički novac, središnjih drugih ugovornih strana, središnjih depozitorija vrijednosnih papira, mjesta trgovanja, društava za osiguranje i društava za reosiguranje trebala imati obvezu provedbe TLPT-a. Procjena toga ispunjavaju li takvi financijski subjekti navedene kvalitativne kriterije trebala bi služiti za određivanje za koje je financijske subjekte TLPT primjeren korištenjem međusektorskih i objektivnih pokazatelja. Istodobno bi na temelju procjene toga ispunjava li financijski subjekt predmetne kvalitativne

⁽¹⁾ SL L 333, 27.12.2022., str. 1., ELI: <http://data.europa.eu/eli/reg/2022/2554/oj>.

kriterije trebalo ograničiti obvezu provedbe TLPT-a na subjekte za koje je takvo testiranje opravdano. Ispunjava li financijski subjekt navedene kvalitativne kriterije trebalo bi procijeniti i s obzirom na razvoj novih tržišta i sve veću važnost novih sudionika na tržištu za financijski sektor u budućnosti, uključujući pružatelje usluga povezanih s kriptoinovinom koji imaju odobrenje za rad u skladu s člankom 59. Uredbe (EU) 2023/1114 Europskog parlamenta i Vijeća ⁽²⁾.

- (4) Financijski subjekti mogu imati istog pružatelja IKT usluga unutar grupe ili mogu pripadati istoj grupi i oslanjati se na upotrebu zajedničkih IKT sustava. U tom je slučaju važno da tijela za TLPT pri procjeni bi li financijski subjekt trebao imati obvezu provedbe TLPT-a i bi li se TLPT trebao provoditi na razini subjekta ili na razini grupe (u okviru zajedničkog TLPT-a) uzmu u obzir strukturu i sistemsku prirodu ili značaj tog financijskog subjekta za financijski sektor na nacionalnoj razini ili na razini Unije.
- (5) Kako bi se preslikao okvir TIBER-EU, u metodologiji testiranja treba predvidjeti sudjelovanje sljedećih glavnih sudionika: financijskog subjekta, s kontrolnim timom (koji odgovara „kontrolnom timu” iz okvira TIBER-EU) i plavim timom (koji odgovara „plavom timu” iz okvira TIBER-EU) te tijela za TLPT, u obliku kibernetičkog tima za TLPT (koji odgovara „kibernetičkim timovima TIBER-a” iz okvira TIBER-EU), pružatelja saznanja o prijetnjama i provoditelja testiranja (koji odgovaraju „pružatelju crvenog tima” iz okvira TIBER-EU).
- (6) Kako bi se pri provedbi TLPT-a iskoristilo iskustvo stečeno u provedbi okvira TIBER-EU i kako bi se smanjili rizici povezani s provedbom TLPT-a, trebalo bi osigurati da se odgovornosti kibernetičkih timova za TLPT koji će se osnovati na razini tijela za TLPT što više podudaraju s odgovornostima kibernetičkih timova iz okvira TIBER-EU. Stoga bi kibernetički timovi za TLPT trebali imati voditelje testiranja koji su odgovorni za nadzor pojedinačnih TLPT-a te za planiranje i koordinaciju pojedinačnih testova. Kibernetički timovi za TLPT trebali bi funkcionirati kao jedinstvena kontaktna točka za komunikaciju s unutarnjim i vanjskim dionicima o testiranju, prikupljanju i obradi povratnih informacija i iskustava stečenih u prethodnim testiranjima te potpori financijskim subjektima koji se podvrgavaju TLPT-u.
- (7) Kako bi primjenjivali metodologiju iz okvira TIBER-EU, voditelji testiranja trebali bi imati vještine i sposobnosti potrebne za pružanje savjeta i odgovaranje na prijedloge provoditelja testiranja. Iskustvo stečeno u provedbi okvira TIBER-EU pokazalo je da je korisno imati tim od najmanje dva voditelja testiranja za svaki test. Kako bi se osiguralo da se TLPT upotrebljava za stjecanje iskustva i kako bi se zaštitila povjerljivost testova, tijelima za TLPT preporučuje se da, pod uvjetom da nemaju problema s resursima ili stručnošću, uzmu u obzir da tijekom trajanja TLPT-a voditelji testiranja ne bi trebali provoditi nadzorne aktivnosti nad financijskim subjektom koji se podvrgava TLPT-u.
- (8) Radi dosljednosti s okvirom TIBER-EU važno je da tijelo za TLPT pomno prati svaku fazu testiranja. S obzirom na prirodu testiranja i s njime povezane rizike, neophodno je da tijelo za TLPT sudjeluje u svakoj fazi testiranja. Konkretno, tijelo za TLPT trebalo bi biti dostupno za savjetovanje i potvrditi procjene ili odluke financijskih subjekata koje s jedne strane mogu utjecati na učinkovitost testiranja, a s druge na rizike povezane s testiranjem. Glavni koraci testiranja u kojima je potrebno posebno sudjelovanje tijela za TLPT jesu potvrđivanje određene temeljne dokumentacije o testiranju, odabir pružatelja saznanja o prijetnjama i provoditelja testiranja te donošenje mjera upravljanja rizicima. Sudjelovanje tijela za TLPT, posebno pri potvrđivanju dokumentacije, ne bi ih trebalo prekomjerno opteretiti te bi stoga trebala biti ograničena na dokumentaciju i odluke koje izravno utječu na provedbu TLPT-a. Aktivnim sudjelovanjem u svakoj fazi testiranja, tijela za TLPT mogu učinkovito procijeniti usklađenost financijskih subjekata s relevantnim zahtjevima, što bi tim tijelima trebalo omogućiti izdavanje potvrda u skladu s člankom 26. stavkom 7. Uredbe (EU) 2022/2554.

⁽²⁾ Uredba (EU) 2023/1114 Europskog parlamenta i Vijeća od 31. svibnja 2023. o tržištima kriptoinovine i izmjeni uredaba (EU) br. 1093/2010 i (EU) br. 1095/2010 te direktiva 2013/36/EU i (EU) 2019/1937 (SL L 150, 9.6.2023., str. 40., ELI: <http://data.europa.eu/eli/reg/2023/1114/oj>).

- (9) Tajnost TLPT-a od izuzetne je važnosti kako bi se osiguralo da su uvjeti testiranja realistični. Zbog toga bi testiranje trebalo biti prikriveno te bi trebalo poduzeti mjere opreza kako bi TLPT bio povjerljiv, što uključuje odabir kodnih naziva koji bi trebali biti osmišljeni tako da se trećim stranama onemogući prepoznavanje TLPT-a. Ako bi članovi osoblja koji su odgovorni za sigurnost financijskog tima bili svjesni planiranog ili tekućeg TLPT-a, vjerojatno bi bili pažljiviji i oprezniji nego u uobičajenim radnim uvjetima, što bi utjecalo na ishod testiranja. Članovi osoblja financijskog subjekta izvan kontrolnog tima trebali bi stoga biti upoznati sa svim planiranim ili tekućim TLPT-ima samo ako za to postoje uvjerljivi razlozi i uz prethodnu suglasnost voditelja testiranja, među ostalim kako bi se osigurala tajnost testiranja u slučaju da član plavog tima otkrije da se provodi testiranje.
- (10) Kao što je vidljivo iz iskustva stečenog u pogledu „kontrolnog tima” u provedbi okvira TIBER-EU, odabir prikladnog voditelja kontrolnog tima neophodan je za sigurnu provedbu TLPT-a. Voditelj kontrolnog tima trebao bi u okviru financijskog subjekta imati potrebne ovlasti koje mu omogućuju usmjeravanje svih aspekata testiranja a da se ne ugrozi njegova povjerljivost. Zbog istog bi razloga članovi kontrolnog tima trebali dobro poznavati financijski subjekt i ulogu i stratešku poziciju voditelja kontrolnog tima te imati potreban senioritet i pristup upravnom odboru. Kako bi se smanjio rizik od ugrožavanja TLPT-a, kontrolni tim treba biti što manji.
- (11) S TLPT-om se povezuju određeni inherentni elementi rizika jer se ključne funkcije testiraju u produkcijskom okruženju, što znači da postoji mogućnost uzrokovanja incidenata uskraćivanja usluge, neočekivanih padova sustava, oštećenja ključnih produkcijskih sustava ili gubitka, izmjene ili otkrivanja podataka. Zbog tih su rizika potrebne snažne mjere upravljanja rizicima. Kako bi se osiguralo da se TLPT kontrolirano provodi tijekom cijelog testiranja, vrlo je važno da financijski subjekti u svakom trenutku budu svjesni konkretnih rizika koji se javljaju u okviru TLPT-a i da se ti rizici ublaže. Za te bi potrebe, ne dovodeći u pitanje unutarnje procese financijskog subjekta te odgovornosti i delegirane ovlasti koje su već dodijeljene voditelju kontrolnog tima, mogle biti primjerene informacije o mjerama upravljanja rizicima koji proizlaze iz TLPT-a ili, u posebnim slučajevima, odobrenje tih mjera upravljanja rizicima od strane upravljačkog tijela financijskog subjekta. Kako bi mogli pružati učinkovite i stručne profesionalne usluge te smanjiti te rizike, neophodno je i da provoditelji testiranja i pružatelji saznanja o prijetnjama (zajedno „pružatelji usluga TLPT-a”) posjeduju najvišu razinu vještina, stručnosti i odgovarajućeg iskustva u području saznanja o prijetnjama i TLPT-a u industriji financijskih usluga.
- (12) Konvencionalna penetracijska testiranja omogućuju detaljnu i korisnu procjenu tehničkih i konfiguracijskih ranjivosti, često pojedinačnog sustava ili okruženja, ali za razliku od testiranja koja provodi crveni tim i koja se temelje na saznanjima, njima se ne procjenjuje potpuni scenarij ciljanog napada na cijeli subjekt te na sve njegovo osoblje, procese i tehnologije. Financijski subjekti stoga bi u postupku odabira pružatelja usluga TLPT-a trebali osigurati da oni imaju potrebne vještine za provedbu testiranja crvenog tima koja se temelje na saznanjima, a ne samo penetracijskih testova. Stoga je potrebno utvrditi sveobuhvatne kriterije za unutarnje i vanjske provoditelje testiranja te za pružatelje saznanja o prijetnjama, koji su uvijek vanjski. Ako pružatelji usluga TLPT-a pripadaju istom društvu, osoblje kojem je povjerena provedba TLPT-a trebalo bi biti na odgovarajući način odvojeno.
- (13) U iznimnim okolnostima financijski subjekti možda neće moći angažirati pružatelje usluga TLPT-a koji ispunjavaju sveobuhvatne kriterije. Stoga bi financijskim subjektima, nakon što dokažu nedostupnost takvih pružatelja saznanja o prijetnjama, trebalo dopustiti da angažiraju osobe koje ne ispunjavaju sve sveobuhvatne kriterije, pod uvjetom da na odgovarajući način ublaže sve povezane dodatne rizike i da tijelo za TLPT procijeni sve te kriterije.
- (14) Ako u TLPT-u sudjeluje nekoliko financijskih subjekata i nekoliko tijela za TLPT, trebalo bi odrediti uloge svih strana u postupku TLPT-a kako bi testiranje bilo što učinkovitije i sigurnije. Za skupno testiranje potrebno je utvrditi posebne zahtjeve kako bi se odredila uloga imenovanog financijskog subjekta, odnosno kako bi se utvrdilo da bi on trebao biti zadužen za dostavu sve potrebne dokumentacije vodećem tijelu za TLPT i za praćenje postupka testiranja. Imenovani financijski subjekt trebao bi biti zadužen i za zajedničke aspekte procjene upravljanja rizicima. Neovisno o ulozima imenovanog financijskog subjekta, obveze svakog financijskog subjekta koji sudjeluje u postupku skupnog TLPT-a trebale bi ostati nepromijenjene za vrijeme provedbe skupnog testiranja. Isto načelo trebalo bi se primjenjivati i na zajedničke TLPT-e.

- (15) Kao što je vidljivo iz iskustva stečenog u provedbi okvira TIBER-EU, održavanje sastanaka uživo ili virtualnim putem sa svim uključenim dionicima (financijskim subjektima, nadležnim tijelima, provoditeljima testiranja i pružateljima saznanja o prijetnjama) najučinkovitiji je način osiguravanja odgovarajuće provedbe testiranja. Stoga bi se sastanci uživo i virtualni sastanci trebali održavati u različitim fazama postupka, a posebno u pripremnoj fazi prije pokretanja TLPT-a radi utvrđivanja njegova opsega, u fazi testiranja radi dovršetka izvješća o saznanjima o prijetnjama i plana testiranja crvenog tima te tjednih razmjena novosti i u završnoj fazi radi ponavljanja testova i aktivnosti plavog tima, provedbe zajedničkih aktivnosti u okviru ljubičastog tima i razmjene povratnih informacija o TLPT-u.
- (16) Kako bi se osigurala neometana provedba TLPT-a, tijelo za TLPT trebalo bi financijskom subjektu jasno iznijeti svoja očekivanja u pogledu testiranja. U tom bi pogledu voditelji testiranja trebali osigurati uspostavu odgovarajućeg protoka informacija s kontrolnim timom unutar financijskog subjekta i s pružateljima usluga TLPT-a.
- (17) Financijski subjekt trebao bi odabrati ključne ili važne funkcije koje će biti obuhvaćene TLPT-om. Odabir tih funkcija trebao bi temeljiti na različitim kriterijima koji se odnose na važnost svake funkcije za financijski subjekt i financijski sektor, na razini Unije i na nacionalnoj razini, ne samo u gospodarskom smislu, nego uzimajući u obzir i simbolički ili politički status funkcije. Kako bi se omogućio neometan prijelaz na fazu prikupljanja saznanja o prijetnjama, kontrolni tim trebao bi provoditeljima testiranja i pružatelju saznanja o prijetnjama koji nisu uključeni u postupak utvrđivanja opsega testiranja pružiti detaljne informacije o dogovorenom opsegu.
- (18) Kako bi se provoditeljima testiranja pružile informacije potrebne za simulaciju stvarnog i realističnog napada na produkcijske sustave financijskog subjekta na kojima se temelje njegove ključne ili važne funkcije, pružatelj saznanja o prijetnjama trebao bi prikupljati saznanja ili informacije o najmanje dva ključna područja interesa: o metama utvrđivanjem potencijalnih površina napada u cijelom financijskom subjektu i o prijetnjama identifikacijom relevantnih aktera prijetnji i vjerojatnih scenarija prijetnji. Kako bi se osiguralo da pružatelj saznanja o prijetnjama razmatra prijetnje koje su relevantne za financijski subjekt, provoditelji testiranja, kontrolni tim i voditelji testiranja trebali bi dostaviti povratne informacije o nacrtu izvješća o saznanjima o prijetnjama. Ako je dostupno, pružatelj saznanja o prijetnjama kao osnovu za utvrđivanje stanja u pogledu prijetnji na nacionalnoj razini može iskoristiti opis općih prijetnji za financijski sektor države članice koje je dostavilo tijelo za TLPT. Na temelju primjene okvira TIBER-EU postupak prikupljanja saznanja o prijetnjama obično traje približno četiri tjedna.
- (19) Kako bi se provoditeljima testiranja omogućio uvid i dodatno preispitivanje dokumenta o utvrđivanju opsega testiranja i izvješća o posebnim saznanjima o prijetnjama radi dovršetka plana testiranja crvenog tima, ključno je da prije faze testiranja TLPT-a za koju je odgovoran crveni tim provoditelji testiranja od pružatelja saznanja o prijetnjama dobiju detaljna objašnjenja o izvješću o posebnim saznanjima o prijetnjama i analizi mogućih scenarija prijetnji.
- (20) Kako bi se provoditeljima testiranja omogućilo da provedu realistično i sveobuhvatno testiranje u kojem se izvode sve faze napada i ostvaruju utvrđene etape, za aktivnu fazu testiranja crvenog tima trebalo bi izdvojiti dovoljno vremena. Na temelju iskustva stečenog u provedbi okvira TIBER-EU izdvojeno razdoblje trebalo bi trajati najmanje 12 tjedana i trebalo bi ga utvrditi s obzirom na broj uključenih strana, opseg TLPT-a, resurse uključenog financijskog subjekta ili financijskih subjekata, sve vanjske zahtjeve i dostupnost popratnih informacija koje je dostavio financijski subjekt.
- (21) Tijekom aktivne faze testiranja crvenog tima provoditelji testiranja trebali bi primijeniti niz taktika, tehnika i postupaka kako bi na odgovarajući način testirali produkcijske sustave financijskog subjekta. Taktike, tehnike i postupci trebali bi, prema potrebi, obuhvaćati izviđanje (tj. prikupljanje što više informacija o meti), naoružanje (tj. analizu informacija o infrastrukturi, objektima i zaposlenicima te pripremu za operacije specifične za metu), provedbu (tj. aktivno pokretanje potpune operacije usmjerene na metu), otkrivanje i iskorištavanje ranjivosti (tj. radnje u kojima je cilj provoditelja testiranja ugroziti poslužitelje i mreže financijskog subjekta i iskoristiti njegovo osoblje uz pomoć socijalnog inženjeringa), kontrolu i kretanje (tj. pokušaje prelaska s kompromitiranih sustava na druge ranjive sustave ili sustave visoke vrijednosti) i izvođenje mjera protiv mete (tj. ostvarivanje daljnjeg pristupa kompromitiranim sustavima i ostvarivanje pristupa ciljnim informacijama i podacima kako je prethodno dogovoreno u planu testiranja crvenog tima).

- (22) Tijekom TLPT-a provoditelji testiranja trebali bi djelovati uzimajući u obzir vrijeme dostupno za izvođenje napada, resurse te etička i pravna ograničenja. Ako provoditelji testiranja ne mogu napredovati prema planiranoj sljedećoj fazi napada, kontrolni tim trebao bi, uz suglasnost tijela za TLPT, pružiti povremenu pomoć. Takva pomoć općenito može biti u obliku informacija i olakšanog pristupa te se može sastojati od pružanja pristupa IKT sustavima ili internim mrežama kako bi provoditelji mogli nastaviti testiranje i usmjeriti se na sljedeće korake napada.
- (23) Ako je to potrebno kako bi se omogućio nastavak TLPT-a i kao krajnja mjera u iznimnim okolnostima nakon što se iscrpe sve druge mogućnosti, tijekom aktivne faze testiranja crvenog tima trebalo bi provesti aktivnost zajedničkog testiranja koja podrazumijeva suradnju provoditelja testiranja i plavog tima. U kontekstu takve ograničene zajedničke aktivnosti u okviru ljubičastog tima mogu se primijeniti sljedeće metode: „hvatanje i puštanje”, pri čemu provoditelji testiranja pokušavaju nastaviti provoditi scenarije dok ih se ne otkrije i zatim nastaviti testiranje, „vojne vježbe”, koje omogućuju složenije scenarije u svrhu testiranja strateškog donošenja odluka, ili „zajedničku provjeru koncepta”, koja provoditeljima testiranja i članovima plavog tima omogućuje da zajednički potvrde konkretne sigurnosne mjere, alate ili tehnike u kontroliranom i suradničkom okruženju.
- (24) TLPT bi se trebao iskoristiti za stjecanje iskustva kako bi se poboljšala digitalna operativna otpornost financijskih subjekata. U tom smislu, plavi tim i provoditelji testiranja trebali bi ponoviti napad i preispitati korake koji su poduzeti kako bi članovi plavog tima stekli nova znanja iz iskustva testiranja u suradnji s provoditeljima testiranja. U tu svrhu i kako bi se omogućila odgovarajuća priprema, izvješća o testiranju crvenog i plavog tima trebala bi se staviti na raspolaganje svim stranama uključenima u aktivnosti ponavljanja testiranja prije njihove ponovne provedbe. Osim toga, u završnoj fazi trebalo bi provesti zajedničke aktivnosti ljubičastog tima kako bi se u najvećoj mjeri iskoristilo stečeno iskustvo. Metode koje se mogu primijeniti za zajedničke aktivnosti ljubičastog tima u završnoj fazi trebale bi uključivati rasprave o alternativnim scenarijima napada, istraživanje alternativnih scenarija na produkcijskim sustavima ili ponovno istraživanje planiranih scenarija na produkcijskim sustavima koje provoditelji testiranja nisu mogli dovršiti ili izvršiti tijekom faze testiranja.
- (25) Radi dodatnog stjecanja iskustva svih strana uključenih u TLPT, koje će se iskoristiti u budućim testovima, te kako bi se unaprijedila digitalna operativna otpornost financijskih subjekata, uključene strane trebale bi jedna drugoj dostaviti povratne informacije o cjelokupnom procesu, konkretno istaknuti aktivnosti koje su dobro napredovale i one koje se mogu poboljšati te koji su aspekti procesa TLPT-a dobro funkcionirali, a koji se mogu poboljšati.
- (26) Nadležna tijela iz članka 46. Uredbe (EU) 2022/2554 i tijela za TLPT, ako se razlikuju, trebala bi surađivati kako bi napredno testiranje TLPT-om uključila u postojeće nadzorne postupke. U tom pogledu i kako bi se podijelilo pravilno razumijevanje nalaza TLPT-a i načina na koji bi ih trebalo tumačiti, primjereno je uspostaviti blisku suradnju voditelja testiranja koji su sudjelovali u TLPT-u i odgovornih nadzornih tijela, posebno u vezi sa sažetim izvješćem o testiranju i planovima za ispravljanje nedostataka.
- (27) Člankom 26. stavkom 8. prvim podstavkom Uredbe (EU) 2022/2554 financijski se subjekti obvezuju na angažiranje vanjskih provoditelja testiranja za svaki treći test. Ako financijski subjekti u tim provoditelja testiranja uključe i unutarnje i vanjske provoditelje testiranja, to bi se trebalo smatrati TLPT-om koji provode unutarnji provoditelji testiranja za potrebe tog članka.
- (28) Ova Uredba se temelji na nacrtu regulatornih tehničkih standarda koji su Komisiji dostavili Europsko nadzorno tijelo za bankarstvo, Europsko nadzorno tijelo za osiguranje i strukovno mirovinsko osiguranje i Europsko nadzorno tijelo za vrijednosne papire i tržišta kapitala (europska nadzorna tijela) u dogovoru s Europskom središnjom bankom.

- (29) Europska nadzorna tijela provela su otvoreno javno savjetovanje o nacrtu regulatornih tehničkih standarda na kojem se temelji ova Uredba, analizirala moguće povezane troškove i koristi te zatražila mišljenje Interesne skupine za bankarstvo osnovane u skladu s člankom 37. Uredbe (EU) br. 1093/2010 Europskog parlamenta i Vijeća ⁽³⁾, Interesne skupine za osiguranje i reosiguranje i Interesne skupine za strukovno mirovinsko osiguranje osnovanih u skladu s člankom 37. Uredbe (EU) br. 1094/2010 Europskog parlamenta i Vijeća ⁽⁴⁾ te Interesne skupine za vrijednosne papire i tržišta kapitala osnovane u skladu s člankom 37. Uredbe (EU) br. 1095/2010 Europskog parlamenta i Vijeća ⁽⁵⁾.
- (30) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 42. stavkom 1. Uredbe (EU) 2018/1725 Europskog parlamenta i Vijeća ⁽⁶⁾ te je on dao mišljenje 20. kolovoza 2024.,

DONIJELA JE OVU UREDBU:

Članak 1.

Definicije

Za potrebe ove Uredbe primjenjuju se sljedeće definicije:

1. „kontrolni tim” znači tim koji čini osoblje financijskog subjekta nad kojim se provodi testiranje i, ako je to relevantno s obzirom na opseg TLPT-a, osoblje njegovih trećih strana pružatelja usluga i svih drugih strana koje upravljaju testom;
2. „voditelj kontrolnog tima” znači član osoblja financijskog subjekta koji je odgovoran za provedbu svih aktivnosti povezanih s TLPT-om za financijski subjekt u kontekstu određenog testa;
3. „plavi tim” znači osoblje financijskog subjekta i, prema potrebi, osoblje trećih strana pružatelja usluga financijskog subjekta i bilo koje druge strane koja se smatra relevantnom s obzirom na opseg TLPT-a trećih strana pružatelja usluga financijskog subjekta, koje štiti upotrebu mrežnih i informacijskih sustava financijskog subjekta tako što održava njegov sigurnosni status pod simuliranim ili stvarnim napadima i koje nije upoznato s TLPT-om;
4. „zadaci plavog tima” znači zadaci koje obično obavlja plavi tim, kao što su aktivnosti centra za sigurnosne operacije, usluge IKT infrastrukture, aktivnosti službe za korisnike i usluge upravljanja incidentima na operativnoj razini;
5. „crveni tim” znači unutarnji ili vanjski provoditelji testiranja, koji su angažirani za provedbu TLPT-a ili kojima je povjerena provedba TLPT-a;
6. „zajednička aktivnost u okviru ljubičastog tima” znači aktivnost zajedničkog testiranja u kojoj sudjeluju provoditelji testiranja i plavi tim;

⁽³⁾ Uredba (EU) br. 1093/2010 Europskog parlamenta i Vijeća od 24. studenog 2010. o osnivanju europskog nadzornog tijela (Europskog nadzornog tijela za bankarstvo), kojom se izmjenjuje Odluka br. 716/2009/EZ i stavlja izvan snage Odluka Komisije 2009/78/EZ (SL L 331, 15.12.2010., str. 12., ELI: <http://data.europa.eu/eli/reg/2010/1093/oj>).

⁽⁴⁾ Uredba (EU) br. 1094/2010 Europskog parlamenta i Vijeća od 24. studenog 2010. o osnivanju Europskog nadzornog tijela (Europsko nadzorno tijelo za osiguranje i strukovno mirovinsko osiguranje), o izmjeni Odluke br. 716/2009/EZ i o stavljanju izvan snage Odluke Komisije 2009/79/EZ (SL L 331, 15.12.2010., str. 48., ELI: <http://data.europa.eu/eli/reg/2010/1094/oj>).

⁽⁵⁾ Uredba (EU) br. 1095/2010 Europskog parlamenta i Vijeća od 24. studenog 2010. o osnivanju europskog nadzornog tijela (Europskog nadzornog tijela za vrijednosne papire i tržišta kapitala), izmjeni Odluke br. 716/2009/EZ i stavljanju izvan snage Odluke Komisije 2009/77/EZ (SL L 331, 15.12.2010., str. 84., ELI: <http://data.europa.eu/eli/reg/2010/1095/oj>).

⁽⁶⁾ Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ (SL L 295, 21.11.2018., str. 39., ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>).

7. „tijelo za TLPT” znači bilo koje od sljedećeg:
 - (a) jedinstveno tijelo javne vlasti u financijskom sektoru imenovano u skladu s člankom 26. stavkom 9. Uredbe (EU) 2022/2554;
 - (b) nadležno tijelo u financijskom sektoru kojem je delegirano izvršavanje nekih ili svih zadaća povezanih s TLPT-om u skladu s člankom 26. stavkom 10. Uredbe (EU) 2022/2554;
 - (c) bilo koje od nadležnih tijela iz članka 46. Uredbe (EU) 2022/2554;
8. „kibernetički tim za TLPT” ili „TCT” znači osoblje tijela za TLPT koje je odgovorno za pitanja povezana s TLPT-om;
9. „voditelji testiranja” znači osoblje kojem je povjereno vođenje aktivnosti tijela za TLPT za određeni TLPT radi praćenja usklađenosti s ovom Uredbom;
10. „pružatelj saznanja o prijetnjama” znači stručnjaci koje je financijski subjekt angažirao za određeni TLPT i koji djeluju kao vanjski suradnici financijskog subjekta i pružatelja IKT usluga unutar grupe, ako postoje, koji prikupljaju i analiziraju posebna saznanja o prijetnjama relevantna za financijske subjekte u okviru određenog TLPT-a te izrađuju odgovarajuće relevantne i realistične scenarije prijetnji;
11. „pružatelji usluga TLPT-a” znači provoditelji testiranja i pružatelji saznanja o prijetnjama;
12. „pomoć” znači pomoć ili informacije koje kontrolni tim pruža provoditeljima testiranja kako bi im omogućio daljnje izvršavanje puta napada ako ne mogu samostalno napredovati i ako ne postoji druga razumna alternativa, među ostalim zbog nedovoljno vremena ili resursa u određenom TLPT-u;
13. „put napada” znači put koji provoditelji testiranja slijede pri provedbi TPLT-a tijekom aktivne faze testiranja crvenog tima kako bi ostvarili etape utvrđene za taj TLPT;
14. „etape” su ključni ciljevi u IKT sustavima kojima se podupiru ključne ili važne funkcije financijskog subjekta koje provoditelji testiranja nastoje ostvariti u okviru testa;
15. „osjetljive informacije” znači informacije koje se mogu lako iskoristiti za napade na IKT sustave financijskog subjekta, intelektualno vlasništvo, povjerljivi poslovni podaci ili osobni podaci, koji mogu izravno ili neizravno naštetiti financijskom subjektu i njegovu ekosustavu ako ih se domognu zlonamjerni akteri;
16. „skup” znači svi financijski subjekti koji sudjeluju u skupnom TLPT-u u skladu s člankom 26. stavkom 4. Uredbe (EU) 2022/2554;
17. „država članica domaćin” znači država članica domaćin u skladu sa sektorskim pravom Unije koje se primjenjuje na svaki financijski subjekt;
18. „zajednički TLPT” znači TLPT, osim skupnog TLPT-a iz članka 26. stavka 4. Uredbe (EU) 2022/2554, koji uključuje nekoliko financijskih subjekata koji angažiraju istog pružatelja IKT usluga unutar grupe ili pripadaju istoj grupi i dijele IKT sustave.

Članak 2.

Određivanje koji su financijski subjekti dužni provoditi TLPT

1. Tijela za TLPT procjenjuju je li određeni financijski subjekt dužan provoditi TLPT uzimajući u obzir učinak tih financijskih subjekata, njihovu sistemsku prirodu i njihov profil IKT rizičnosti na temelju svih sljedećih kriterija:
 - (a) čimbenici povezani s učinkom i sistemskom prirodom:
 - i. veličina financijskog subjekta, utvrđena na temelju toga pruža li financijske usluge u jednoj ili više država članica i na temelju usporedbe njegovih djelatnosti s djelatnostima drugih financijskih subjekata koji pružaju slične usluge;
 - ii. opseg i priroda međusobne povezanosti financijskog subjekta s drugim financijskim subjektima u financijskom sektoru u jednoj ili više država članica;
 - iii. ključnost ili važnost usluga koje financijski subjekt pruža financijskom sektoru;

- iv. zamjenjivost usluga koje financijski subjekt pruža;
 - v. složenost poslovnog modela financijskog subjekta te povezanih usluga i procesa;
 - vi. činjenica je li financijski subjekt dio grupe od sistemskog značaja u financijskom sektoru na razini Unije ili na nacionalnoj razini i dijeli li IKT sustave s ostatkom grupe;
- (b) čimbenici povezani s IKT rizicima:
- i. profil rizičnosti financijskog subjekta;
 - ii. prijetnje s kojima se suočava financijski subjekt;
 - iii. stupanj ovisnosti ključnih ili važnih funkcija ili funkcija kojima se podupiru te funkcije financijskog subjekta o IKT sustavima i procesima;
 - iv. složenost IKT arhitekture financijskog subjekta;
 - v. IKT usluge i funkcije koje podupiru treće strane pružatelji IKT usluga te količina i vrsta ugovornih aranžmana s trećim stranama pružateljima IKT usluga ili pružateljima IKT usluga unutar grupe;
 - vi. ishodi svih nadzornih provjera relevantnih za procjenu IKT zrelosti financijskog subjekta;
 - vii. razrađenost planova kontinuiteta poslovanja u području IKT-a te planova odgovora i oporavka u području IKT-a;
 - viii. razrađenost operativnih mjera za otkrivanje i ublažavanje u području IKT sigurnosti, uključujući sposobnost:
 - 1. kontinuiranog praćenja IKT infrastrukture financijskog subjekta;
 - 2. otkrivanja događaja povezanih s IKT-om u stvarnom vremenu;
 - 3. analiziranja događaja iz točke 2.;
 - 4. pravodobnog i učinkovitog odgovaranja na događaje iz točke 2.;
 - ix. činjenica je li financijski subjekt dio grupe aktivne u financijskom sektoru na razini Unije ili na nacionalnoj razini koja dijeli IKT sustave.

Za potrebe točke (a) podtočke i. tijelo za TLPT, ako je to moguće, razmatra:

- (a) položaj financijskog subjekta s obzirom na tržišni udio na razini Unije i na nacionalnoj razini;
- (b) opseg aktivnosti koje nudi financijski subjekt;
- (c) tržišni udio usluga koje pruža financijski subjekt ili djelatnosti koje obavlja na razini Unije i na nacionalnoj razini.

Za potrebe točke (a) podtočke v. tijelo za TLPT, ako je to moguće, razmatra:

- (a) primjenjuje li financijski subjekt u poslovanju više od jednog poslovnog modela;
- (b) međusobnu povezanost različitih poslovnih procesa i povezanih usluga.

2. Tijela za TLPT sve sljedeće financijske subjekte obvezuju na provedbu TLPT-a, osim ako procjena iz stavka 1. u pogledu financijskog subjekta pokaže da njegov učinak, pitanja financijske stabilnosti povezana s tim financijskim subjektom ili njegov profil IKT rizičnosti ne opravdavaju provedbu TLPT-a:

- (a) kreditne institucije koje ispunjavaju bilo koji od sljedećih uvjeta:
 - i. smatraju se globalnim sistemski važnim institucijama (GSV institucije) u skladu s člankom 131. Direktive 2013/36/EU Europskog parlamenta i Vijeća (⁷);
 - ii. smatraju se ostalim sistemski važnim institucijama (OSV institucije) u skladu s člankom 131. Direktive 2013/36/EU;
 - iii. dio su GSV ili OSV institucija;

(⁷) Direktiva 2013/36/EU Europskog parlamenta i Vijeća od 26. lipnja 2013. o pristupanju djelatnosti kreditnih institucija i bonitetnom nadzoru nad kreditnim institucijama, izmjeni Direktive 2002/87/EZ te stavljanju izvan snage direktiva 2006/48/EZ i 2006/49/EZ (SL L 176, 27.6.2013., str. 338., ELI: <http://data.europa.eu/eli/dir/2013/36/oj>).

- (b) institucije za platni promet čije su platne transakcije, kako su definirane u članku 4. točki 5. Direktive (EU) 2015/2366 Europskog parlamenta i Vijeća ⁽⁸⁾, u svakoj od dvije kalendarske godine koje su prethodile procjeni tijela za TLPT premašile ukupnu vrijednost od 150 milijardi EUR;
- (c) institucije za elektronički novac čije su platne transakcije, kako su definirane u članku 4. točki 5. Direktive (EU) 2015/2366, u svakoj od dvije kalendarske godine koje su prethodile procjeni tijela za TLPT premašile ukupnu vrijednost od 150 milijardi EUR ili čiji je iznos elektroničkog novca u optjecaju premašio ukupnu vrijednost od 40 milijardi EUR;
- (d) središnje depozitorije vrijednosnih papira;
- (e) središnje druge ugovorne strane;
- (f) mjesta trgovanja s elektroničkim sustavom trgovanja koja ispunjavaju bilo koji od sljedećih kriterija:
 - i. mjesto trgovanja ima najveći tržišni udio u smislu prometa na nacionalnoj razini u svakoj od dvije kalendarske godine koje su prethodile procjeni tijela za TLPT u bilo kojem od sljedećeg:
 - 1. prenosivim vrijednosnim papirima kako su definirani u članku 4. stavku 1. točki 44. podtočki (a) Direktive 2014/65/EU Europskog parlamenta i Vijeća ⁽⁹⁾;
 - 2. prenosivim vrijednosnim papirima kako su definirani u članku 4. stavku 1. točki 44. podtočki (b) Direktive 2014/65/EU;
 - 3. izvedenicama kako su definirane u članku 2. stavku 1. točki 29. Uredbe (EU) br. 600/2014 Europskog parlamenta i Vijeća ⁽¹⁰⁾;
 - 4. strukturiranim financijskim proizvodima kako su definirani u članku 2. stavku 1. točki 28. Uredbe (EU) br. 600/2014;
 - 5. emisijskim jedinicama iz odjeljka C točke 11. Priloga I. Direktivi 2014/65/EU;
 - ii. mjesto trgovanja ima tržišni udio veći od 5 % u smislu prometa na razini Unije u svakoj od dvije kalendarske godine koje su prethodile procjeni tijela za TLPT u bilo kojem od sljedećeg:
 - 1. dionicama društava i drugim vrijednosnim papirima koji su jednakovrijedni udjelu u kapitalu ili članskim pravima u društvima ili drugim subjektima te potvrđama o deponiranim dionicama;
 - 2. obveznicama ili drugim oblicima sekuritiziranog duga, uključujući potvrde o deponiranim takvim vrijednosnim papirima;
 - 3. izvedenicama kako su definirane u članku 2. stavku 1. točki 29. Uredbe (EU) br. 600/2014;
 - 4. strukturiranim financijskim proizvodima kako su definirani u članku 2. stavku 1. točki 28. Uredbe (EU) br. 600/2014;
 - 5. emisijskim jedinicama iz odjeljka C točke 11. Priloga I. Direktivi 2014/65/EU;

⁽⁸⁾ Direktiva (EU) 2015/2366 Europskog parlamenta i Vijeća od 25. studenog 2015. o platnim uslugama na unutarnjem tržištu, o izmjeni direktiva 2002/65/EZ, 2009/110/EZ i 2013/36/EU te Uredbe (EU) br. 1093/2010 i o stavljanju izvan snage Direktive 2007/64/EZ (SL L 337, 23.12.2015., str. 35., ELI: <http://data.europa.eu/eli/dir/2015/2366/oj>).

⁽⁹⁾ Direktiva 2014/65/EU Europskog parlamenta i Vijeća od 15. svibnja 2014. o tržištu financijskih instrumenata i izmjeni Direktive 2002/92/EZ i Direktive 2011/61/EU (SL L 173, 12.6.2014., str. 349., ELI: <http://data.europa.eu/eli/dir/2014/65/oj>).

⁽¹⁰⁾ Uredba (EU) br. 600/2014 Europskog parlamenta i Vijeća od 15. svibnja 2014. o tržištima financijskih instrumenata i izmjeni Uredbe (EU) br. 648/2012 (SL L 173, 12.6.2014., str. 84., ELI: <http://data.europa.eu/eli/reg/2014/600/oj>).

- (g) društva za osiguranje i društva za reosiguranje koja ispunjavaju sve sljedeće kriterije:
- i. imaju zaračunanu bruto premiju (ZBP) koja premašuje 1 500 000 000 EUR;
 - ii. imaju tehničke pričuve koje premašuju 10 000 000 000 EUR;
 - iii. društva za osiguranje koja obavljaju samo djelatnosti životnog osiguranja ili djelatnosti životnog i neživotnog osiguranja i čija ukupna imovina premašuje 3,5 % zbroja ukupne imovine društava za osiguranje i društava za reosiguranje s poslovnim nastanom u državi članici vrednovane u skladu s člankom 75. Direktive 2009/138/EZ Europskog parlamenta i Vijeća ⁽¹⁾.

Za potrebe točke (f) podtočke ii., ako je mjesto trgovanja dio grupe koja dijeli IKT sustave ili istog pružatelja IKT usluga unutar grupe, uzima se u obzir promet u vrijednosnim papirima i ugovorima o izvedenicama na svim mjestima trgovanja koja pripadaju istoj grupi i imaju poslovni nastan u Uniji.

Za potrebe točke (g) tijela za TLPT utvrđuju podskup svih društava za osiguranje i društava za reosiguranje primjenom kriterija utvrđenih u točki (g) podtočkama i., ii. i iii. Društva za osiguranje i društva za reosiguranje uključena u taj podskup dužna su provoditi TLPT ako ispunjavaju i bilo koji od sljedećih kriterija:

- (a) zaračunana bruto premija (ZBP) premašuje 3 000 000 000 EUR;
- (b) tehničke pričuve premašuju 30 000 000 000 EUR;
- (c) ukupna imovina koja premašuje 10 % zbroja ukupne imovine društava za osiguranje i društava za reosiguranje s poslovnim nastanom u državi članici vrednovane u skladu s člankom 75. Direktive 2009/138/EZ.

3. Ako više financijskih subjekata koji pripadaju istoj grupi i dijele IKT sustave ili više financijskih subjekata koji angažiraju istog pružatelja IKT usluga unutar grupe ispunjava kriterije iz stavka 2., tijela za TLPT tih financijskih subjekata u skladu s člankom 16. stavkom 2. odlučuju je li obveza provedbe TLPT-a na pojedinačnoj osnovi primjenjiva na te financijske subjekte.

Ako se tijelo za TLPT matičnog društva grupe financijskih subjekata iz prvog podstavka razlikuje od tijela za TLPT financijskih subjekata grupe, tijela za TLPT financijskih subjekata koji pripadaju toj grupi savjetuju se s tim tijelom o tome je li primjereno provoditi TLPT na pojedinačnoj osnovi.

Članak 3.

TCT i voditelji TLPT-a

1. Tijelo za TLPT odgovornost za koordinaciju aktivnosti povezanih s TLPT-om dodjeljuje TCT-u. TCT se sastoji od voditelja testiranja kojima je povjereno nadziranje pojedinačnog TLPT-a.
2. Za svako testiranje tijelo za TLPT imenuje voditelja testiranja i najmanje jednog zamjenika.
3. Voditelji testiranja prate poštuju li se zahtjevi utvrđeni u ovoj Uredbi i osiguravaju njihovo poštovanje.

⁽¹⁾ Direktiva 2009/138/EZ Europskog parlamenta i Vijeća od 25. studenog 2009. o osnivanju i obavljanju djelatnosti osiguranja i reosiguranja (Solventnost II) (SL L 335, 17.12.2009., str. 1., ELI: <http://data.europa.eu/eli/dir/2009/138/oj>).

4. Voditelj testiranja financijskom subjektu dostavlja podatke za kontakt TCT-a u okviru obavijesti iz članka 9. stavka 1.
5. Tijelo za TLPT sudjeluje u svim fazama TLPT-a.

Članak 4.

Organizacijski ustroj u financijskim subjektima

1. Financijski subjekti imenuju voditelja kontrolnog tima koji je odgovoran za svakodnevno upravljanje TLPT-om te za odluke i aktivnosti kontrolnog tima.
2. Financijski subjekti uspostavljaju organizacijske i postupovne mjere kako bi osigurali sljedeće:
 - (a) da je pristup informacijama koje se odnose na bilo koji planirani ili tekući TLPT ograničen na temelju nužnosti i to na kontrolni tim, upravljačko tijelo, provoditelje testiranja, pružatelja saznanja o prijetnjama i tijelo za TLPT;
 - (b) da se kontrolni tim savjetuje s voditeljima testiranja prije uključivanja bilo kojeg člana plavog tima u TLPT;
 - (c) da članovi osoblja financijskog subjekta ili njegovih trećih strana pružatelja usluga obavješćuju kontrolni tim o svakom otkrivanju TLPT-a; da će u slučaju eskalacije odgovora na incident koji iz toga proizlazi kontrolni tim prema potrebi ograničiti eskalaciju;
 - (d) da su uspostavljeni aranžmani koji se odnose na tajnost TLPT-a i koji su primjenjivi na osoblje financijskog subjekta, osoblje uključenih trećih strana pružatelja IKT usluga, provoditelje testiranja i pružatelja saznanja o prijetnjama;
 - (e) da kontrolni tim voditeljima testiranja na zahtjev dostavlja sve informacije koje se odnose na TLPT;
 - (f) da, ako je moguće, strane uključene u TLPT upućuju na njega samo prema kodnom nazivu.

Članak 5.

Upravljanje rizicima za TLPT

1. Tijekom pripremne faze iz članka 9. kontrolni tim procjenjuje rizike povezane s testiranjem produkcijskih sustava ključnih ili važnih funkcija financijskog subjekta, uključujući moguće učinke na:

- (a) financijski sektor;
- (b) financijsku stabilnost na razini Unije ili na nacionalnoj razini.

Kontrolni tim preispituje te učinke tijekom cijelog testiranja.

2. Za potrebe procjene rizika i upravljanja rizicima kontrolni tim uzima u obzir barem sljedeće vrste rizika koji se odnose na:

- (a) odobravanje pristupa pružatelju saznanja o prijetnjama i vanjskim provoditeljima testiranja, ako je primjenjivo, osjetljivim informacijama o financijskom subjektu;
- (b) neusklađenost TLPT-a s Uredbom (EU) 2022/2554 i ovom Uredbom ako se takva neusklađenost dovede do uskraćivanja potvrde iz članka 26. stavka 7. Uredbe (EU) 2022/2554, među ostalim ako je takva neusklađenost posljedica kršenja povjerljivosti TLPT-a ili neetičnog postupanja;
- (c) eskalaciju kriza i incidenata;
- (d) aktivnu fazu crvenog tima, uključujući rizike povezane s prekidom ključnih aktivnosti i oštećenjem podataka zbog aktivnosti provoditelja testiranja, i njezine moguće učinke na treće strane;

- (e) aktivnost plavog tima, uključujući rizike povezane s prekidom ključnih aktivnosti i oštećenjem podataka zbog aktivnosti plavog tima, i njezine moguće učinke na treće strane;
- (f) nepotpunu ponovnu uspostavu sustava obuhvaćenih TLPT-om.

Članak 6.

Upravljanje rizicima za skupne ili zajedničke TLPT-e

1. U slučaju zajedničkog ili skupnog TLPT-a kontrolni tim svakog financijskog subjekta provodi vlastitu procjenu rizika i uspostavlja vlastite mjere upravljanja rizicima.
2. Kontrolni tim imenovanog financijskog subjekta iz članka 16. stavka 3. točke (b) ove Uredbe ili financijskog subjekta imenovanog u skladu s člankom 26. stavkom 4. Uredbe (EU) 2022/2554 procjenjuje rizike povezane sa sudjelovanjem više financijskih subjekata u TLPT-u. Kontrolni timovi uključenih financijskih subjekata surađuju s kontrolnim timom imenovanog financijskog subjekta kako bi utvrdili potencijalne zajedničke rizike.

Članak 7.

Odabir pružatelja usluga TLPT-a

1. Kontrolni tim poduzima mjere za upravljanje rizicima povezanim s TLPT-om i posebno osigurava da za svaki TLPT:
 - (a) pružatelj saznanja o prijetnjama i vanjski provoditelj testiranja kontrolnom timu dostave detaljan životopis i preslike potvrda koje, u skladu s priznatim tržišnim standardima, dokazuju primjerenost za obavljanje njihovih djelatnosti;
 - (b) pružatelj saznanja o prijetnjama i vanjski provoditelj testiranja imaju propisna i cjelovita osiguranja od profesionalne odgovornosti, što uključuje rizike od protupravnog i nemarnog postupanja;
 - (c) pružatelj saznanja o prijetnjama dostavi najmanje tri preporuke iz prethodnih angažmana u kontekstu penetracijskih testiranja i testiranja crvenog tima;
 - (d) vanjski provoditelji testiranja dostave najmanje pet preporuka iz prethodnih angažmana povezanih s penetracijskim testiranjem i testiranjem crvenog tima;
 - (e) osoblje pružatelja saznanja o prijetnjama koje radi na TLPT-u:
 - i. uključuje najmanje jednog voditelja s najmanje pet godina iskustva u području saznanja o prijetnjama i najmanje jednog dodatnog člana s najmanje dvije godine iskustva u području saznanja o prijetnjama;
 - ii. posjeduje širok raspon i odgovarajuću razinu stručnog znanja i vještina, uključujući:
 1. taktike, tehnike i postupke za prikupljanje saznanja;
 2. geopolitička, tehnička i sektorska znanja;
 3. odgovarajuće komunikacijske vještine za jasno iznošenje rezultata angažmana i izvješćivanje o njima;
 - iii. zajednički ima iskustva u sudjelovanju u najmanje tri prethodna angažmana u području prikupljanja saznanja o prijetnjama u kontekstu penetracijskog testiranja i testiranja crvenog tima;
 - iv. ne obavlja istodobno zadaće plavog tima niti pruža druge usluge koje bi mogle dovesti do sukoba interesa u odnosu na financijski subjekt, treću stranu pružatelja IKT usluga ili pružatelja IKT usluga unutar grupe koji je uključen u TLPT na kojem rade;
 - v. djeluje odvojeno od osoblja i ne odgovara osoblju pružatelja usluga TLPT-a ako je taj pružatelj usluga isti kao onaj koji osigurava vanjske provoditelje testiranja za isti TLPT;

- (f) kad je riječ o vanjskim provoditeljima testiranja, crveni tim dodijeljen TLPT-u:
- uključuje najmanje jednog voditelja s najmanje pet godina iskustva u području penetracijskog testiranja i testiranja crvenog tima te najmanje dva dodatna provoditelja testiranja, od kojih svaki ima najmanje dvije godine iskustva u području penetracijskog testiranja i testiranja crvenog tima;
 - posjeduje širok raspon i odgovarajuću razinu stručnog znanja i vještina, uključujući znanje o poslovanju financijskog subjekta, izviđanju, upravljanju rizicima, razvoju otkrivanja i iskorištavanja ranjivosti, fizičkoj penetraciji, socijalnom inženjeringu i analizi ranjivosti, kao i odgovarajuće komunikacijske vještine za jasno iznošenje rezultata angažmana i izvješćivanje o njima;
 - zajednički ima iskustva u sudjelovanju u najmanje pet prethodnih angažmana povezanih s penetracijskim testiranjem i testiranjem crvenog tima;
 - nije zaposlen u pružatelju saznanja o prijetnjama niti pruža usluge tom pružatelju koji istodobno obavlja zadaće plavog tima za financijski subjekt, treću stranu pružatelja IKT usluga ili pružatelja IKT usluga unutar grupe koji je uključen u TLPT;
 - djeluje odvojeno od osoblja pružatelja usluga TLPT-a koji istodobno pruža usluge saznanja o prijetnjama za isti TLPT;
- (g) provoditelji testiranja i pružatelj saznanja o prijetnjama provode postupke ponovne uspostave po završetku testiranja, među ostalim sigurno brisanje informacija povezanih s lozinkama, vjerodajnicama i drugim tajnim ključevima koji su kompromitirani tijekom TLPT-a, sigurnu komunikaciju s financijskim subjektima o kompromitiranim računima, sigurno prikupljanje, pohranu i uklanjanje drugih podataka prikupljenih tijekom testiranja te upravljanje njima;
- (h) provoditelji testiranja uz postupke ponovne uspostave po završetku testiranja iz točke (g) provode i sljedeće postupke ponovne uspostave:
- deaktivaciju sustava za upravljanje i kontrolu;
 - uspostavu mehanizama za prestanak testiranja na temelju opsega i datuma;
 - uklanjanje programa za neovlašten pristup sustavu („stražnji ulaz”) i drugog zlonamjernog softvera;
 - slanje obavijesti o mogućem upadu u sustav;
 - postupke za buduću ponovnu uspostavu na temelju sigurnosnih kopija koje se mogu odnositi na zlonamjerni softver ili alate instalirane tijekom testiranja;
 - praćenje aktivnosti plavog tima i obavješćivanje kontrolnog tima o mogućim otkrivanjima testiranja;
- (i) provoditelji testiranja i pružatelj saznanja o prijetnjama ne obavljaju nijednu od sljedećih aktivnosti niti u njima sudjeluju:
- neovlašteno uništenje opreme financijskog subjekta i njegovih trećih strana pružatelja IKT usluga, ako postoje;
 - nekontrolirane izmjene informacija i IKT imovine financijskog subjekta i njegovih trećih strana pružatelja IKT usluga, ako postoje;
 - namjerno ugrožavanje kontinuiteta ključnih ili važnih funkcija financijskog subjekta;
 - neovlašteno uključivanje sustava koji nisu obuhvaćeni testiranjem;
 - neovlašteno otkrivanje rezultata testiranja.

2. Kontrolni tim vodi evidenciju o dokumentaciji koju su dostavili provoditelji testiranja i pružatelji saznanja o prijetnjama kako bi dokazali usklađenost sa stavkom 1. točkama od (a) do (f).

U iznimnim okolnostima financijski subjekti mogu angažirati vanjske provoditelje testiranja i pružatelje saznanja o prijetnjama koji ne ispunjavaju jedan ili više zahtjeva iz stavka 1. točaka od (a) do (f), pod uvjetom da ti financijski subjekti donesu odgovarajuće mjere za ublažavanje rizika koji proizlaze iz neusklađenosti s tim točkama i evidentiraju te mjere.

Članak 8.

Specifičnosti skupnih ili zajedničkih TLPT-a

1. Ako vodeće tijelo za TLPT ne odluči drukčije, kad je u skupni ili zajednički TLPT uključeno nekoliko financijskih subjekata određenih u skladu s člankom 16. stavcima 2. ili 4., svaki financijski subjekt mora poduzeti sve korake utvrđene u člancima od 9. do 15.

2. Ako nije drukčije predviđeno ovom Uredbom, kad je u zajednički TLPT ili skupni TLPT uključeno nekoliko tijela za TLPT, kako je navedeno u članku 16. stavku 3. ili članku 16. stavku 5., upućivanja na „tijelo za TLPT” u člancima od 9. do 15. smatraju se upućivanjem na vodeće tijelo za TLPT za takav skupni ili zajednički TLPT.

Članak 9.

Pripremna faza

1. Financijski subjekt određen u skladu s člankom 26. stavkom 8. trećim podstavkom Uredbe (EU) 2022/2554 pokreće TLPT nakon primitka obavijesti od tijela za TLPT da se TLPT treba provesti.

2. Financijski subjekt u roku od tri mjeseca od primitka obavijesti iz stavka 1. voditeljima testiranja dostavlja sve sljedeće informacije o pokretanju TLPT-a:

- (a) projektni list koji sadržava plan projekta na visokoj razini s informacijama iz Priloga I.;
- (b) podatke za kontakt voditelja kontrolnog tima;
- (c) prema potrebi, informacije o namjeri angažiranja unutarnjih ili vanjskih provoditelja testiranja ili oboje, kako je utvrđeno u članku 15.;
- (d) informacije o komunikacijskim kanalima koji će se upotrebljavati tijekom TLPT-a;
- (e) kodni naziv TLPT-a.

3. Ako su informacije iz stavka 2. točaka (a) do (e) potpune i osiguravaju prikladnost i učinkovitu provedbu TLPT-a, tijelo za TLPT potvrđuje informacije financijskog subjekta o pokretanju TLPT-a i o tome obavješćuje financijski subjekt.

4. Nakon što tijelo za TLPT potvrdi informacije o pokretanju TLPT-a, financijski subjekt uspostavlja kontrolni tim za pružanje potpore voditelju kontrolnog tima u sljedećim zadaćama:

- (a) određivanju komunikacijskih kanala i postupaka unutar kontrolnog tima te s provoditeljima testiranja i pružateljima saznanja o prijetnjama za sva pitanja povezana s TLPT-om;
- (b) obavješćivanju upravljačkog tijela financijskog subjekta o napretku TLPT-a i povezanim rizicima;
- (c) donošenju odluka na temelju odgovarajućeg stručnog znanja tijekom cijelog TLPT-a;
- (d) provedbi TLPT-a u skladu s ovom Uredbom;
- (e) odabiru pružatelja saznanja o prijetnjama za TLPT;
- (f) odabiru vanjskih provoditelja testiranja, unutarnjih provoditelja testiranja ili oboje;
- (g) izradi dokumenta o utvrđivanju opsega testiranja.

5. Ako tijelo za TLPT smatra da su početni sastav kontrolnog tima i sve njegove naknadne promjene prikladni za obavljanje zadaća iz stavka 4., tijelo za TLPT potvrđuje kontrolni tim i o tome obavješćuje voditelja kontrolnog tima.

6. Financijski subjekt u roku od šest mjeseci od primitka obavijesti od tijela za TLPT iz stavka 1. dostavlja voditeljima testiranja dokument o utvrđivanju opsega testiranja koji sadržava sve informacije iz Priloga II. Upravljačko tijelo financijskog subjekta odobrava dokument o utvrđivanju opsega testiranja.

7. Financijski subjekti uzimaju u obzir sljedeće kriterije pri razmatranju uključivanja ključnih ili važnih funkcija u opseg TLPT-a:

- (a) ključnost ili važnost funkcije i njezin mogući učinak na financijski sektor i financijsku stabilnost na razini Unije i na nacionalnoj razini;
- (b) važnost funkcije za svakodnevno poslovanje financijskog subjekta;
- (c) zamjenjivost funkcije;
- (d) međusobnu povezanost s drugim funkcijama;
- (e) geografsku lokaciju funkcije;
- (f) sektorsku ovisnost drugih subjekata o funkciji;
- (g) prema potrebi, saznanja o prijetnjama u vezi s funkcijom.

8. Kontrolni tim dijeli informacije o pokretanju TLPT-a i dokument o utvrđivanju opsega testiranja s provoditeljima testiranja i pružateljima saznanja o prijetnjama nakon što ih se angažira. Kontrolni tim obavješćuje provoditelje testiranja i pružatelje saznanja o prijetnjama o načinu provedbe postupka testiranja.

9. Financijski subjekt osigurava da se povjeravanje zadaća ili angažiranje provoditelja testiranja i pružatelja saznanja o prijetnjama dovrši prije početka faze testiranja.

10. Prije početka faze testiranja kontrolni tim savjetuje se s voditeljima testiranja o procjeni rizika koji proizlaze iz TLPT-a i o mjerama upravljanja rizicima. Kontrolni tim preispituje procjenu rizika ili mjere upravljanja rizicima ako tijelo za TLPT smatra da se njima rizici koji proizlaze iz TLPT-a ne rješavaju na odgovarajući način.

11. Kontrolni tim procjenjuje usklađenost pružatelja saznanja o prijetnjama i provoditelja testiranja koje želi uključiti u TLPT sa zahtjevima utvrđenima u članku 27. Uredbe (EU) 2022/2554 i članku 7. stavku 1. ove Uredbe te dokumentira ishod te procjene. Kontrolni tim odabire pružatelje saznanja o prijetnjama u skladu s tom procjenom i svojim praksama upravljanja rizicima. Prije angažiranja odabranih pružatelja saznanja o prijetnjama i vanjskih provoditelja testiranja kontrolni tim voditeljima testiranja dostavlja dokaze o usklađenosti tih pružatelja saznanja o prijetnjama i provoditelja testiranja sa zahtjevima utvrđenima u članku 27. Uredbe (EU) 2022/2554 i članku 7. stavku 1. ove Uredbe. Kontrolni tim ne smije angažirati odabrane pružatelje saznanja o prijetnjama i vanjske provoditelje testiranja ako tijelo za TLPT smatra da odabrani pružatelji saznanja o prijetnjama i vanjski provoditelji testiranja ne ispunjavaju zahtjeve utvrđene u članku 27. Uredbe (EU) 2022/2554 ili zahtjeve utvrđene u članku 7. stavku 1. ove Uredbe ili dodatne zahtjeve koji proizlaze iz zakonodavstva o nacionalnoj sigurnosti u skladu s pravom Unije ili ako financijski subjekt ne ispunjava zahtjeve iz članka 7. stavka 2. prvog podstavka ove Uredbe ili ako ne postoje okolnosti iz članka 7. stavka 2. drugog podstavka ove Uredbe.

12. Ako je dokument o utvrđivanju opsega testiranja potpun i omogućuje provedbu odgovarajućeg i učinkovitog TLPT-a, tijelo za TLPT odobrava taj dokument i o tome obavješćuje voditelja kontrolnog tima.

Članak 10.

Faza testiranja: saznanja o prijetnjama

1. Nakon što tijelo za TLPT odobri dokument o utvrđivanju opsega testiranja pružatelj saznanja o prijetnjama analizira saznanja o općim i sektorskim prijetnjama relevantna za financijski subjekt. Ako je tijelo za TLPT dostavilo opis općih prijetnji za financijski sektor države članice, pružatelj saznanja o prijetnjama može te informacije upotrijebiti kao osnovu za utvrđivanje stanja u pogledu prijetnji na nacionalnoj razini. Pružatelj saznanja o prijetnjama utvrđuje kibernetičke prijetnje i postojeće ili moguće ranjivosti povezane s financijskim subjektom. Uz to, pružatelj saznanja o prijetnjama prikuplja informacije i analizira konkretna, provediva i kontekstualizirana saznanja o metama i prijetnjama koja se odnose na financijski subjekt, među ostalim u okviru savjetovanja s kontrolnim timom i voditeljima testiranja.

2. Pružatelj saznanja o prijetnjama iznosi relevantne prijetnje i posebna saznanja o prijetnjama te predlaže potrebne scenarije kontrolnom timu, provoditeljima testiranja i voditeljima testiranja. Predloženi scenariji razlikuju se s obzirom na utvrđene aktere prijetnji i povezane taktike, tehnike i postupke te su usmjereni na svaku ključnu ili važnu funkciju obuhvaćenu TLPT-om.

3. Voditelj kontrolnog tima odabire najmanje tri scenarija za provedbu TLPT-a na temelju svih sljedećih elemenata:

- (a) preporuke pružatelja saznanja o prijetnjama i prirode svakog scenarija vođenog prijetnjama;
- (b) informacija koje dostave voditelji testiranja;
- (c) izvedivosti predloženih scenarija na temelju stručne prosudbe provoditelja testiranja;
- (d) veličine, složenosti i ukupnog profila rizičnosti financijskog subjekta te prirode, opsega i složenosti njegovih usluga, aktivnosti i poslovanja.

4. Najviše jedan od odabranih scenarija ne mora biti vođen prijetnjama i može se temeljiti na budućoj i potencijalno fiktivnoj prijetnji s visokom prediktivnom, anticipativnom, oportunističkom ili prospektivnom vrijednošću s obzirom na očekivana kretanja prijetnji koje se odnose na financijski subjekt.

Kad je riječ o skupnim TPLT-ima, ne dovodeći u pitanje scenarije koji su usmjereni izravno na ključne ili važne funkcije financijskih subjekata uključenih u testiranje, barem jedan scenarij mora uključivati relevantne temeljne IKT sustave, procese i tehnologije treće strane pružatelja IKT usluga kojima se podupiru ključne ili važne funkcije obuhvaćenih financijskih subjekata.

Kad je riječ o zajedničkom TLPT-u koji uključuje pružatelja IKT usluga unutar grupe, ne dovodeći u pitanje scenarije koji su usmjereni izravno na ključne ili važne funkcije financijskih subjekata uključenih u testiranje, barem jedan scenarij mora uključivati relevantne temeljne IKT sustave, procese i tehnologije pružatelja IKT usluga unutar grupe kojima se podupiru ključne ili važne funkcije obuhvaćenih financijskih subjekata.

5. Pružatelj saznanja o prijetnjama dostavlja izvješće o posebnim saznanjima o prijetnjama kontrolnom timu, uključujući scenarije odabrane u skladu sa stavcima 3. i 4. Izvješće o saznanjima o prijetnjama sadržava informacije navedene u Prilogu III.

6. Kontrolni tim dostavlja izvješće o posebnim saznanjima o prijetnjama voditelju testiranja na odobrenje. Ako je izvješće o posebnim saznanjima o prijetnjama potpuno i omogućuje provedbu učinkovitog TLPT-a, tijelo za TLPT odobrava izvješće i o tome obavješćuje voditelja kontrolnog tima.

Članak 11.

Faza testiranja: test crvenog tima

1. Nakon što tijelo za TLPT odobri izvješće o posebnim saznanjima o prijetnjama, provoditelji testiranja izrađuju plan testiranja crvenog tima koji sadržava informacije utvrđene u Prilogu IV. Provoditelji testiranja temelje scenarij napada na dokumentu o utvrđivanju opsega testiranja i izvješću o posebnim saznanjima o prijetnjama.
2. Provoditelji testiranja savjetuju se s kontrolnim timom, pružateljem saznanja o prijetnjama i voditeljima testiranja o planu testiranja crvenog tima, što uključuje aranžmane za komunikaciju, upravljanje postupcima i projektima, pripremu i scenarije za aktivaciju pomoći te dogovore o izvješćivanju kontrolnog tima i voditelja testiranja.
3. Ako je plan testiranja crvenog tima potpun i omogućuje provedbu učinkovitog TLPT-a, kontrolni tim i tijelo za TLPT odobravaju plan testiranja crvenog tima, a TLPT o tome obavješćuje voditelja kontrolnog tima.
4. Nakon odobrenja plana testiranja crvenog tima u skladu sa stavkom 3. provoditelji testiranja provode TLPT tijekom aktivne faze testiranja crvenog tima.
5. Trajanje aktivne faze testiranja crvenog tima razmjerno je opsegu TLPT-a te prirodi, aktivnosti, složenosti i broju financijskih subjekata i trećih strana pružatelja IKT usluga ili pružatelja IKT usluga unutar grupe uključenih u TLPT, a faza u svakom slučaju mora trajati najmanje 12 tjedana. Scenariji napada mogu se izvoditi jedan za drugim ili istodobno. Kontrolni tim, pružatelj saznanja o prijetnjama, provoditelji testiranja i voditelji testiranja dogovaraju se o završetku aktivne faze testiranja crvenog tima.
6. Pod uvjetom da plan testiranja crvenog tima ostane potpun te i dalje omogućuje provedbu učinkovitog TLPT-a, voditelj kontrolnog tima i voditelji testiranja odobravaju sve izmjene plana testiranja crvenog tima nakon njegova odobrenja, uključujući rok, opseg, ciljne sustave ili etape.
7. Tijekom cijele aktivne faze testiranja crvenog tima provoditelji testiranja najmanje jednom tjedno izvješćuju kontrolni tim i voditelje testiranja o napretku TLPT-a, a pružatelj saznanja o prijetnjama mora biti na raspolaganju za savjetovanje i dodatna saznanja o prijetnjama na zahtjev kontrolnog tima.
8. Kontrolni tim pravodobno osigurava pomoć u skladu s planom testiranja crvenog tima. Vrste pomoći mogu se dodati ili prilagoditi nakon odobrenja kontrolnog tima i voditelja testiranja.
9. Ako bilo koji član osoblja financijskog subjekta ili njegovih trećih strana pružatelja IKT usluga ili pružatelja IKT usluga unutar grupe, ako je primjenjivo, otkrije aktivnosti testiranja, kontrolni tim, u savjetovanju s provoditeljima testiranja i ne dovodeći u pitanje stavak 10., predlaže i dostavlja voditeljima testiranja radi potvrde mjere kojima se omogućuje nastavak TLPT-a uz istodobno osiguravanje njegove tajnosti.
10. U iznimnim okolnostima u kojima nastaju rizici od učinka na podatke, štete na imovini i poremećaja u radu ključnih ili važnih funkcija, usluga ili operacija u okviru samog financijskog subjekta, njegovih trećih strana pružatelja IKT usluga ili pružatelja IKT usluga unutar grupe, ili poremećaja u radu njegovih partnerskih financijskih subjekata ili u financijskom sektoru, voditelj kontrolnog tima može suspendirati TLPT ili može, kao krajnju mjeru, ako nastavak TLPT-a nije moguć na drugi način i uz prethodnu potvrdu tijela za TLPT, nastaviti TLPT provedbom ograničenih zajedničkih aktivnosti u okviru ljubičastog tima. Trajanje ograničenih zajedničkih aktivnosti u okviru ljubičastog tima uračunava se u 12-tjedno minimalno trajanje aktivne faze testiranja crvenog tima iz stavka 5.

Članak 12.**Završna faza**

1. Nakon završetka aktivne faze testiranja crvenog tima voditelj kontrolnog tima obavješćuje plavi tim da je proveden TLPT.
2. U roku od četiri tjedna od završetka aktivne faze testiranja crvenog tima provoditelji testiranja kontrolnom timu podnose izvješće o testiranju crvenog tima koje sadržava informacije utvrđene u Prilogu V.
3. Kontrolni tim bez nepotrebne odgode dostavlja izvješće o testiranju crvenog tima plavom timu i voditeljima testiranja.

Izvješće iz prvog podstavka na zahtjev voditelja testiranja ne sadržava osjetljive informacije.

4. Po primitku izvješća o testiranju crvenog tima, a najkasnije 10 tjedana nakon završetka aktivne faze testiranja crvenog tima, plavi tim kontrolnom timu dostavlja izvješće o testiranju plavog tima koje sadržava informacije utvrđene u Prilogu VI. Kontrolni tim bez nepotrebne odgode dostavlja izvješće o testiranju plavog tima provoditeljima testiranja i voditeljima testiranja.

Izvješće iz prvog podstavka na zahtjev voditelja testiranja ne sadržava osjetljive informacije.

5. Najkasnije 10 tjedana nakon završetka aktivne faze testiranja crvenog tima plavi tim i provoditelji testiranja ponavljaju ofenzivne i defenzivne radnje provedene u okviru TLPT-a. Kontrolni tim provodi i zajedničke aktivnosti u okviru ljubičastog tima u vezi s temama koje su zajednički utvrdili plavi tim i provoditelji testiranja, na temelju ranjivosti utvrđenih tijekom testiranja i prema potrebi na temelju pitanja koja se nisu mogla testirati tijekom aktivne faze testiranja crvenog tima.
6. Nakon završetka ponovljenog testiranja i zajedničkih aktivnosti u okviru ljubičastog tima kontrolni tim, plavi tim, provoditelji testiranja i pružatelji saznanja o prijetnjama međusobno razmjenjuju povratne informacije o postupku TLPT-a. Voditelji testiranja mogu dostaviti povratne informacije.
7. Nakon što tijelo za TLPT obavijesti voditelja kontrolnog tima da je ocijenilo da izvješće o testiranju plavog tima i izvješće o testiranju crvenog tima sadržavaju informacije utvrđene u prilogima V. i VI. financijski subjekt u roku od osam tjedana tijelu za TLPT dostavlja na odobrenje izvješće sa sažetkom relevantnih nalaza TLPT-a, kako je navedeno u članku 26. stavku 6. Uredbe (EU) 2022/2554, koje sadržava elemente utvrđene u Prilogu VII.

Izvješće iz prvog podstavka na zahtjev tijela za TLPT ne sadržava osjetljive informacije.

Članak 13.**Plan za ispravljanje nedostataka**

1. Financijski subjekt u roku od osam tjedana od primitka obavijesti iz članka 12. stavka 7. ove Uredbe tijelu za TLPT i, ako se razlikuju, nadležnom tijelu financijskog subjekta dostavlja planove za ispravljanje nedostataka i dokumentaciju iz članka 26. stavka 6. Uredbe (EU) 2022/2554.
2. Plan za ispravljanje nedostataka iz stavka 1. za svaki nalaz TLPT-a uključuje:
 - (a) opis utvrđenih nedostataka;
 - (b) opis predloženih mjera za ispravljanje nedostataka te prijedlog za određivanje prioriteta među tim mjerama i njihov očekivani dovršetak, uključujući, prema potrebi, mjere za poboljšanje sposobnosti identifikacije, zaštite, otkrivanja i odgovora;
 - (c) analizu temeljnih uzroka;
 - (d) osoblje ili funkcije financijskog subjekta odgovorne za provedbu predloženih mjera za ispravljanje nedostataka ili poboljšanja;
 - (e) rizike povezane s neprovođenjem mjera iz točke (b) i, prema potrebi, rizike povezane s provedbom takvih mjera.

Članak 14.**Potvrda**

1. Potvrda iz članka 26. stavka 7. Uredbe (EU) 2022/2554 sadržava informacije utvrđene u Prilogu VIII.
2. Ako je u TLPT bilo uključeno nekoliko tijela za TLPT, potvrdu iz članka 26. stavka 7. Uredbe (EU) 2022/2554 financijskim subjektima nad kojima je provedeno testiranje dostavlja vodeće tijelo za TLPT.

Članak 15.**Angažiranje unutarnjih provoditelja testiranja**

1. Financijski subjekti dužni su uspostaviti sve sljedeće aranžmane za potrebe angažiranja unutarnjih provoditelja testiranja:
 - (a) oblikovanje i provedbu politike upravljanja unutarnjim provoditeljima testiranja u okviru TLPT-a;
 - (b) mjere kojima se osigurava da angažiranje unutarnjih provoditelja testiranja za provedbu TLPT-a ne utječe negativno na opće obrambene sposobnosti ili otpornost financijskog subjekta u pogledu IKT incidenata niti znatno utječe na dostupnost resursa namijenjenih zadaćama povezanim s IKT-om tijekom TLPT-a;
 - (c) mjere kojima se osigurava da unutarnji provoditelji testiranja imaju dostatne resurse i sposobnosti za provedbu TLPT-a.

Politika iz točke (a) mora ispunjavati sljedeće uvjete:

- (a) mora sadržavati kriterije za procjenu prikladnosti, stručnosti i mogućih sukoba interesa unutarnjih provoditelja testiranja te u njoj moraju biti utvrđene upravljačke odgovornosti u postupku testiranja;
- (b) mora se dokumentirati i redovito preispitivati;
- (c) u njoj se mora utvrditi da unutarnji tim za testiranje uključuje voditelja testiranja i najmanje dva dodatna člana;
- (d) njome se mora propisati da su svi članovi tima za testiranje moraju biti zaposleni u financijskom subjektu ili pružatelju IKT usluga unutar grupe tijekom prethodnih 12 mjeseci;
- (e) mora sadržavati odredbe o osposobljavanju za provedbu penetracijskog testiranja i testiranja crvenog tima unutarnjih provoditelja testiranja.

2. Ako tijelo za TLPT odobri angažiranje unutarnjih provoditelja testiranja u skladu s člankom 27. stavkom 2. točkom (a) Uredbe (EU) 2022/2554, ono razmatra zahtjeve utvrđene u članku 7. stavku 1. ove Uredbe.

3. Kad angažira unutarnje provoditelje testiranja, financijski subjekt dužan je osigurati da se to navede u sljedećim dokumentima:

- (a) informacijama o pokretanju testiranja iz članka 9.;
- (b) izvješću o testiranju crvenog tima iz članka 12. stavka 2.;
- (c) izvješću u kojem su sažeti relevantni nalazi TLPT-a iz članka 26. stavka 6. Uredbe (EU) 2022/2554.

4. Provoditelji testiranja koje angažira pružatelj IKT usluga unutar grupe smatraju se unutarnjim provoditeljima testiranja financijskog subjekta.

Članak 16.

Suradnja i uzajamno priznavanje

1. Za potrebe provedbe TLPT-a nad financijskim subjektom koji pruža usluge u više od jedne države članice, uključujući preko podružnice, njegovo tijelo za TLPT:

- (a) određuje koja tijela za TLPT u državama članicama domaćinima trebaju sudjelovati u testiranju, uzimajući u obzir djeluje li jedna ili više ključnih ili važnih funkcija u državama članicama domaćinima ili se dijeli među njima;
- (b) obavješćuje tijela za TLPT određena u skladu s točkom (a) o odluci o provedbi TLPT-a nad financijskim subjektom;
- (c) ako se tijela za TLPT ne dogovore drukčije, TLPT vodi tijelo za TLPT financijskog subjekta.

Tijela za TLPT država članica domaćina mogu u roku od 20 radnih dana od primitka obavijesti o budućoj provedbi TLPT-a izraziti interes za praćenje TLPT-a kao promatrači ili imenovati voditelja testiranja koji će sudjelovati u TLPT-u. Vodeće tijelo za TLPT svim tijelima za TLPT koja djeluju kao promatrači u okviru TLPT-a dostavlja dokument o utvrđivanju njegova opsega, sažeto izvješće o testiranju, plan za ispravljanje nedostataka i potvrdu.

Vodeće tijelo za TLPT za vrijeme cijelog testiranja koordinira sva tijela za TLPT koja sudjeluju u testiranju i donosi sve odluke potrebne za odgovarajuću i učinkovitu provedbu TLPT-a. Vodeće tijelo za TLPT može odrediti najveći broj tijela za TLPT koja mogu sudjelovati u testiranju ako bi se u suprotnom mogla ugroziti učinkovita provedba TLPT-a.

2. Ako financijski subjekt angažira istog pružatelja IKT usluga unutar grupe kao i financijski subjekti s poslovnim nastanom u drugim državama članicama, ili pripada grupi i dijeli IKT sustave s financijskim subjektima iz iste grupe s poslovnim nastanom u drugim državama članicama, tijelo za TLPT financijskog subjekta stupa u kontakt s tijelima za TLPT drugih financijskih subjekata koji su angažirali istog pružatelja IKT usluga unutar grupe ili koji dijele IKT sustave kao dio grupe te u suradnji s njima procjenjuje izvedivost i prikladnost provedbe zajedničkog TLPT-a. Zajednički TLPT ima prednost pred pojedinačnim TLPT-om ako može dovesti do smanjenja troškova i manje potrošnje resursa za financijske subjekte i tijela za TLPT, pod uvjetom da se ne dovedu u pitanje pouzdanost i učinkovitost testiranja.

3. Za potrebe provedbe zajedničkog TLPT-a:

- (a) tijela za TLPT financijskih subjekata dogovaraju koji će financijski subjekt biti imenovan za provedbu TLPT-a, uzimajući u obzir strukturu grupe i učinkovitost testa;
- (b) tijelo za TLPT financijskog subjekta imenovanog u skladu s točkom (a) vodi TLPT, osim ako se tijela za TLPT financijskih subjekata koji sudjeluju u zajedničkom TLPT-u dogovore drukčije;
- (c) tijela za TLPT financijskih subjekata koji nisu imenovani financijski subjekt koji će voditi zajednički TLPT mogu iskazati interes za praćenje TLPT-a kao promatrači ili imenovati voditelja testiranja za taj TLPT.

Vodeće tijelo za TLPT koordinira sva tijela za TLPT uključena u zajednički TLPT i donosi sve odluke potrebne za pouzdanu i učinkovitu provedbu zajedničkog TLPT-a.

4. Ako financijski subjekt namjerava provoditi skupni TLPT kako je navedeno u članku 26. stavku 4. Uredbe (EU) 2022/2554 koji može uključivati financijske subjekte s poslovnim nastanom u drugim državama članicama, njegovo tijelo za TLPT stupa u kontakt s tijelima za TLPT drugih financijskih subjekata i u suradnji s njima procjenjuje izvedivost i prikladnost provedbe skupnog TLPT-a u skladu s člankom 26. stavkom 4. Uredbe (EU) 2022/2554.

5. Za potrebe provedbe skupnog TLPT-a kako je navedeno u članku 26. stavku 4. Uredbe (EU) 2022/2554:
- (a) tijela za TLPT financijskih subjekata dogovaraju koji će financijski subjekt biti imenovan za vođenje skupnog TLPT-a, uzimajući u obzir IKT usluge koje treća strana pružatelj IKT usluga pruža financijskim subjektima i učinkovitost testa;
 - (b) tijelo za TLPT financijskog subjekta imenovanog u skladu s točkom (a) vodi TLPT, osim ako se tijela za TLPT financijskih subjekata koji sudjeluju u skupnom TLPT-u dogovore drukčije;
 - (c) tijela za TLPT financijskih subjekata koji nisu imenovani financijski subjekt koji će voditi skupni TLPT mogu iskazati interes za praćenje TLPT-a kao promatrači ili imenovati voditelja testiranja za taj TLPT.

Vodeće tijelo za TLPT koordinira sva tijela za TLPT uključena u skupni TLPT i donosi sve odluke potrebne za pouzdanu i učinkovitu provedbu skupnog TLPT-a.

6. Ako se tijelo za TLPT financijskog subjekta koji je dužan provoditi TLPT razlikuje od njegova nadležnog tijela iz članka 46. Uredbe (EU) 2022/2554, ta tijela razmjenjuju sve relevantne informacije o svim pitanjima povezanim s TLPT-om za potrebe provedbe TLPT-a ili izvršavanja svojih dužnosti u skladu s tom uredbom.

Članak 17.

Stupanje na snagu

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu 13. veljače 2025.

Za Komisiju
Predsjednica
Ursula VON DER LEYEN

PRILOG I.

Sadržaj projektnog lista (članak 9. stavak 2. točka (a))

Podatak	Podaci koji se traže
Osoba odgovorna za projektni plan, tj. voditelj kontrolnog tima	Ime i prezime Podaci za kontakt
Provođitelji testiranja	☐ unutarnji ☐ vanjski ☐ oboje
Komunikacijski kanali odabrani u skladu s člankom 9. stavkom 2. točkom (d) i člankom 9. stavkom 4. točkom (a), uključujući: (a) vrstu šifriranja e-pošte koja se primjenjuje; (b) internetske podatkovne sobe koje se upotrebljavaju; (c) aplikacije za trenutačnu razmjenu poruka koje se primjenjuju	
Kodni naziv TLPT-a	
Ako postoje, ključne ili važne funkcije koje financijski subjekt provodi u drugim državama članicama	1. popis ključnih ili važnih funkcija koje se provode u drugoj državi članici 2. za svaku ključnu ili važnu funkciju navesti državu članicu ili države članice u kojima se provode
Ako postoje, ključne ili važne funkcije koje podupiru treće strane pružatelji IKT usluga	3. popis ključnih ili važnih funkcija koje podupiru treće strane pružatelji IKT usluga 4. za svaku funkciju navesti treću stranu pružatelja IKT usluga
Očekivani rokovi dovršetka:	
1. pripremne faze, u skladu s člankom 9.	gggg-mm-dd
2. faze testiranja, u skladu s člancima 10. i 11.	gggg-mm-dd
3. završne faze, u skladu s člankom 12.	gggg-mm-dd
4. plana za ispravljanje nedostataka, u skladu s člankom 13.	gggg-mm-dd

PRILOG II.

Sadržaj dokumenta o utvrđivanju opsega testiranja (članak 9. stavak 6.)

1. Dokument o utvrđivanju opsega testiranja sadržava popis svih ključnih ili važnih funkcija koje je utvrdio financijski subjekt.
2. Za svaku se utvrđenu ključnu ili važnu funkciju navode sljedeće informacije:
 - (a) ako ključna ili važna funkcija nije obuhvaćena TLPT-om, objašnjenje razloga zbog kojih nije obuhvaćena;
 - (b) ako je ključna ili važna funkcija obuhvaćena TLPT-om:
 - i. objašnjenje razloga za njezino uključivanje u opseg testiranja;
 - ii. utvrđeni IKT sustavi kojima se podupire ta ključna ili važna funkcija;
 - iii. za svaki utvrđeni IKT sustav:
 1. informacija o tome je li eksternaliziran i, ako jest, naziv treće strane pružatelja IKT usluga;
 2. jurisdikcije u kojima se taj IKT sustav upotrebljava;
 3. opis preliminarne etape na visokoj razini, u kojem se navodi koji je sigurnosni aspekt povjerljivosti, cjelovitosti, vjerodostojnosti ili dostupnosti obuhvaćen pojedinom etapom.

PRILOG III.

Sadržaj izvješća o posebnim saznanjima o prijetnjama (članak 10. stavak 5.)

Izvješće o posebnim saznanjima o prijetnjama sadržava sljedeće informacije:

1. sveukupni opseg prikupljanja saznanja, uključujući barem sljedeće:
 - (a) obuhvaćene ključne ili važne funkcije;
 - (b) njihovu geografsku lokaciju;
 - (c) korišteni službeni jezik EU-a;
 - (d) relevantne treće strane pružatelje IKT usluga;
 - (e) razdoblje u kojem se prikupljanje provodi;
2. ukupnu procjenu konkretnih provedivih saznanja o financijskom subjektu, što uključuje:
 - (a) korisnička imena i lozinke zaposlenika;
 - (b) slične domene koje se mogu zamijeniti za službene domene financijskog subjekta;
 - (c) tehničko izviđanje: ranjivi softver, sustavi i tehnologije ili oni koje akteri prijetnje mogu iskoristiti;
 - (d) informacije koje zaposlenici objavljuju na internetu, a koje se odnose na financijski subjekt i koje bi se mogle upotrijebiti u svrhu napada;
 - (e) informacije za prodaju na mračnoj mreži;
 - (f) sve druge relevantne informacije dostupne na internetu ili javnim mrežama;
 - (g) prema potrebi informacije o fizičkim metama, među ostalim načine pristupa prostorima financijskog subjekta;
3. analizu saznanja o prijetnjama s obzirom na opće stanje u pogledu prijetnji i posebnu situaciju financijskog subjekta, uključujući barem:
 - (a) geopolitičko okruženje;
 - (b) gospodarsko okruženje;
 - (c) tehnološke trendove i sve druge trendove povezane s djelatnostima u sektoru financijskih usluga;
4. profile prijetnji zlonamjernih aktera (određeni pojedinac/skupina ili općenita kategorija) koji mogu napadati financijski subjekt, uključujući sustave financijskog subjekta za koje je najvjerojatnije da će ih zlonamjerni akteri pokušati ugroziti ili napasti, moguću motivaciju, namjeru i obrazloženje potencijalnog napada te mogući način djelovanja napadača;
5. scenarije prijetnji: najmanje tri sveobuhvatna scenarija prijetnji za profile prijetnji utvrđene u skladu s točkom 4. s najvišim ocjenama ozbiljnosti prijetnje; u scenarijima prijetnji opisuje se cjeloviti put napada i oni uključuju barem:
 - (a) jedan scenarij koji među ostalim obuhvaća ugroženu dostupnost usluge;
 - (b) jedan scenarij koji među ostalim obuhvaća ugroženu cjelovitost podataka;
 - (c) jedan scenarij koji među ostalim obuhvaća ugroženu povjerljivost podataka;
6. prema potrebi, opis scenarija koji nije vođen prijetnjama iz članka 10. stavka 4.

PRILOG IV.

Sadržaj plana testiranja crvenog tima (članak 11. stavak 1.)

Plan testiranja crvenog tima sadržava sljedeće informacije:

- (a) informacije o komunikacijskim kanalima i postupcima;
- (b) taktike, tehnike i postupke koji su dopušteni odnosno nisu dopušteni za upotrebu u napadu, uključujući etička ograničenja za socijalni inženjering;
- (c) mjere upravljanja rizicima kojih se moraju pridržavati provoditelji testiranja;
- (d) opise svakog scenarija, što uključuje:
 - i. simuliranog aktera prijetnje;
 - ii. njegove namjere, motivaciju i ciljeve;
 - iii. funkcije i IKT sustave kojima se one podupiru koji su meta napada;
 - iv. aspekte povjerljivosti, cjelovitosti, dostupnosti i vjerodostojnosti koji su meta napada;
 - v. etape;
- (e) detaljan opis svakog očekivanog puta napada, uključujući preduvjete i moguću pomoć koju treba osigurati kontrolni tim, uključujući rokove za njihovo pružanje i moguću upotrebu;
- (f) raspored aktivnosti crvenog tima, uključujući planiranje vremena za izvođenje svakog scenarija, barem u skladu s tri faze koje provoditelj testiranja provodi tijekom faze testiranja, odnosno ulazak u IKT sustave financijskih subjekata, kretanje kroz te IKT sustave te izvršavanje radnji u odnosu na mete te izlazak iz IKT sustava (faze ulaska, prolaska i izlaska);
- (g) posebnosti infrastrukture financijskih subjekata koje treba uzeti u obzir u okviru testiranja;
- (h) ako postoje, dodatne informacije ili informacije o drugim resursima koji su provoditeljima testiranja potrebni za izvođenje scenarija.

PRILOG V.

Sadržaj izvješća o testiranju crvenog tima (članak 12. stavak 2.)

Izvješće o testiranju crvenog tima sadržava barem sljedeće informacije:

- (a) informacije o izvedenom napadu, što obuhvaća:
 - i. ključne ili važne funkcije i utvrđene IKT sustave, procese i tehnologije kojima se podupire ključna ili važna funkcija koji su meta napada, kako je utvrđeno u planu testiranja crvenog tima;
 - ii. sažetak svakog scenarija;
 - iii. etape koje su ostvarene odnosno nisu ostvarene;
 - iv. putove napada koje se uspješno odnosno neuspješno slijedilo;
 - v. taktike, tehnike i postupke koji su uspješno odnosno neuspješno primijenjeni;
 - vi. odstupanja od plana testiranja crvenog tima, ako postoje;
 - vii. pruženu pomoć, ako postoji;
- (b) informacije o svim radnjama s kojima su provoditelji testiranja upoznati, a koje je izvršio plavi tim, radi rekonstruiranja napada i ublažavanja njegovih učinaka;
- (c) otkrivene ranjivosti i druge nalaze, uključujući:
 - i. opis ranjivosti i drugih nalaza, uključujući njihovu ključnost;
 - ii. analizu temeljnih uzroka uspješnih napada;
 - iii. preporuke za ispravljanje nedostataka, uključujući isticanje prioriteta ispravljanja.

PRILOG VI.

Sadržaj izvješća o testiranju plavog tima (članak 12. stavak 4.)

Izvješće o testiranju plavog tima sadržava barem sljedeće informacije:

1. za svaki korak napada koji provoditelji testiranja opisu u izvješću o testiranju crvenog tima:
 - (a) popis otkrivenih napadačkih radnji;
 - (b) unose u evidenciju koji odgovaraju otkrivenim radnjama;
2. procjenu nalaza i preporukama provoditelja testiranja;
3. dokaze o napadu provoditelja testiranja koje je prikupio plavi tim;
4. analizu temeljnih uzroka uspješnih napada provoditelja testiranja koju je proveo plavi tim;
5. popis stečenih iskustava i utvrđenih mogućnosti za poboljšanje;
6. popis tema koje treba razmotriti pri provedbi zajedničkih aktivnosti u okviru ljubičastog tima.

PRILOG VII.

Pojedinosti izvješća u kojem su sažeti relevantni nalazi TLPT-a iz članka 26. stavka 6. Uredbe (EU) 2022/2554

Sažeto izvješće o testiranju sadržava barem informacije o sljedećem:

- (a) uključenim stranama;
- (b) projektnom planu;
- (c) potvrđenom opsegu, uključujući razloge za uključivanje ili isključivanje ključnih ili važnih funkcija te utvrđenih IKT sustava, procesa i tehnologija kojima se podupiru ključne ili važne funkcije obuhvaćene TLPT-om;
- (d) odabranim scenarijima i svim bitnim odstupanjima od izvješća o posebnim saznanjima o prijetnjama;
- (e) izvršenim putovima napada i primijenjenim taktikama, tehnikama i postupcima;
- (f) etapama koje su ostvarene odnosno nisu ostvarene;
- (g) odstupanjima od plana testiranja crvenog tima, ako postoje;
- (h) činjenicama da je plavi tim otkrio testiranje, ako se to dogodilo;
- (i) zajedničkim aktivnostima u okviru ljubičastog tima u fazi testiranja, ako ih je bilo, i povezanim uvjetima;
- (j) iskorištenoj pomoći, ako je pomoć pružena;
- (k) poduzetim mjerama upravljanja rizicima;
- (l) utvrđenim ranjivostima i drugim nalazima, uključujući njihovu ključnost;
- (m) analizi temeljnih uzroka uspješnih napada;
- (n) planu na visokoj razini za ispravljanje nedostataka, u kojem se povezuju ranjivosti i drugi nalazi, njihovi temeljni uzroci i prioriteti ispravljanja;
- (o) iskustvima stečenima na temelju primljenih povratnih informacija.

PRILOG VIII.

Pojedinosti o potvrdi TLPT-a iz članka 26. stavka 7. Uredbe (EU) 2022/2554

Potvrda sadržava barem sljedeće informacije:

- (a) informacije o provedenom TLPT-u, odnosno:
 - i. datum početka i završetka TLPT-a;
 - ii. ključne ili važne funkcije obuhvaćene testom;
 - iii. prema potrebi, ključne ili važne funkcije obuhvaćene testom za koje TLPT nije proveden;
 - iv. prema potrebi, druge financijske subjekte koji su sudjelovali u TLPT-u;
 - v. prema potrebi, treće strane pružatelje IKT usluga koji su sudjelovali u TLPT-u;
 - vi. kad je riječ o provoditeljima testiranja:
 - 1. jesu li angažirani unutarnji provoditelji testiranja;
 - 2. je li financijski subjekt primijenio članak 5. stavak 3. drugi podstavak;
 - vii. trajanje aktivne faze testiranja crvenog tima u kalendarskim danima;
- (b) ako je nekoliko tijela za TLPT bilo uključeno u TLPT, informacije o tome o kojim je drugim tijelima za TLPT riječ i u kojem su svojstvu sudjelovala;
- (c) popis dokumenata koje je pregledalo tijelo za TLPT za potrebe izdavanja potvrde.
