Úradný vestník
Európskej únie

SK
Séria L

2025/1190

18.6.2025

# DELEGOVANÉ NARIADENIE KOMISIE (EÚ) 2025/1190

## z 13. februára 2025,

## ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, v ktorých sa bližšie špecifikujú kritériá používané na identifikáciu finančných subjektov povinných vykonať penetračné testovanie na základe konkrétnej hrozby, požiadavky a normy, ktorými sa riadi využívanie interných testovacích subjektov, požiadavky týkajúce sa rozsahu pôsobnosti, metodiky testovania a prístupu pre každú fázu testovania, výsledkov, záverečného a nápravného štádia a druh spolupráce v oblasti dohľadu a v iných relevantných oblastiach potrebnej na vykonávanie TLPT a na uľahčenie vzájomného uznávania

**(Text s významom pre EHP)**

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011 ([1]), a najmä na jeho článok 26 ods. 11 štvrtý pododsek,

keďže:

(1) Toto nariadenie bolo vypracované v súlade s rámcom TIBER-EÚ a odzrkadľuje metodiku, proces a štruktúru penetračného testovania na základe konkrétnej hrozby (TLPT), ako sa opisuje v rámci TIBER-EÚ. Finančné subjekty, na ktoré sa vzťahuje TLPT, môžu odkazovať na rámec TIBER-EÚ alebo na jedno z jeho vnútroštátnych vykonávaní a uplatňovať ich, pokiaľ je tento rámec alebo vykonávanie v súlade s požiadavkami stanovenými v článkoch 26 a 27 nariadenia (EÚ) 2022/2554 a v tomto nariadení. Určením jedného verejného orgánu vo finančnom sektore, ktorý je zodpovedný za záležitosti súvisiace s TLPT na vnútroštátnej úrovni v súlade s článkom 26 ods. 9 nariadenia (EÚ) 2022/2554, by nemala byť dotknutá právomoc príslušných orgánov zverená na úrovni Únie v oblasti dohľadu nad určitými finančnými subjektmi v súlade s článkom 46 uvedeného nariadenia, ako je napríklad právomoc Európskej centrálnej banky v prípade významných úverových inštitúcií, ktoré sa majú považovať za príslušné v záležitostiach súvisiacich s TLPT. Ak sa na iný vnútroštátny orgán vo finančnom sektore delegujú len niektoré úlohy súvisiace s TLPT podľa článku 26 ods. 10 nariadenia (EÚ) 2022/2554, príslušný orgán finančného subjektu uvedený v článku 46 uvedeného nariadenia by mal zostať orgánom zodpovedným za úlohy súvisiace s TLPT, ktoré neboli delegované.

(2) Vzhľadom na zložitosť TLPT a s ním súvisiace riziká by sa jeho používanie malo obmedziť na tie finančné subjekty, pre ktoré je odôvodnené. Orgány zodpovedné za záležitosti TLPT (orgány TLPT buď na úrovni Únie alebo na vnútroštátnej úrovni) by preto mali z rozsahu pôsobnosti TLPT vylúčiť tie finančné subjekty, ktoré pôsobia v hlavných pododvetviach finančných služieb, pre ktoré TLPT nie je odôvodnené. To znamená, že aj keď úverové inštitúcie, platobné inštitúcie a inštitúcie elektronického peňažníctva, centrálne depozitáre cenných papierov, centrálne protistrany, obchodné miesta, poisťovne a zaisťovne spĺňajú kvantitatívne kritériá, mohli by byť oslobodené od požiadavky TLPT vzhľadom na celkové posúdenie ich rizikového profilu a vyspelosti v oblasti IKT, vplyvu na finančný sektor a súvisiacich obáv týkajúcich sa finančnej stability.

(3) Orgány TLPT by mali so zreteľom na celkové posúdenie rizikového profilu a vyspelosti v oblasti IKT, vplyvu na finančný sektor a súvisiacich obáv týkajúcich sa finančnej stability posúdiť, či by sa TLPT malo vzťahovať na akýkoľvek druh finančného subjektu iného než úverové inštitúcie, platobné inštitúcie, inštitúcie elektronického peňažníctva, centrálne protistrany, centrálne depozitáre cenných papierov, obchodné miesta, poisťovne a zaisťovne. Posúdenie, či takéto finančné subjekty spĺňajú uvedené kvalitatívne kritériá, by malo byť zamerané na identifikáciu finančných subjektov, pre ktoré je TLPT vhodné, a to použitím medzisektorových a objektívnych ukazovateľov. Zároveň by sa posudzovanie toho, či finančný subjekt spĺňa tieto kvalitatívne kritériá, malo zo skupiny subjektov, na ktoré sa vzťahuje TLPT, týkať len tých subjektov, pre ktoré je testovanie odôvodnené. To, či finančný subjekt spĺňa

([1]) Ú. v. EÚ L 333, 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

tieto kvalitatívne kritériá, by sa malo posudzovať aj so zreteľom na nový vývoj na trhoch a na rastúci význam nových účastníkov trhu pre finančný sektor v budúcnosti vrátane poskytovateľov služieb kryptoaktív, ktorým bolo udelené povolenie v súlade s článkom 59 nariadenia Európskeho parlamentu a Rady (EÚ) 2023/1114 ([2]).

(4) Finančné subjekty môžu mať toho istého vnútroskupinového poskytovateľa IKT služieb alebo môžu patriť do tej istej skupiny a využívať zdieľané IKT systémy. V takom prípade je dôležité, aby orgány TLPT pri posudzovaní toho, či by sa na finančný subjekt malo vzťahovať TLPT a či by sa TLPT malo vykonávať na úrovni subjektu alebo na úrovni skupiny (prostredníctvom spoločného TLPT), zohľadňovali štruktúru a systémový charakter alebo význam daného finančného subjektu pre finančný sektor na vnútroštátnej úrovni alebo na úrovni Únie.

(5) S cieľom kopírovať rámec TIBER-EÚ je nevyhnutné, aby metodika testovania zabezpečovala zapojenie týchto hlavných účastníkov: finančného subjektu s kontrolným tímom (kopírujúc „kontrolný tím“ TIBER-EÚ) a modrým tímom (kopírujúc „modrý tím“ TIBER-EÚ) a orgánu TLPT vo forme kybernetického tímu TLPT (kopírujúc „TIBER kybernetické tímy“ TIBER-EÚ), poskytovateľa spravodajských informácií o hrozbách a testovacích subjektov (kde testovacie subjekty kopírujú „poskytovateľa červeného tímu“ TIBER-EÚ).

(6) V snahe zabezpečiť, aby TLPT využívalo skúsenosti získané v rámci vykonávania TIBER-EÚ, a znížiť riziká spojené s vykonávaním TLPT by sa malo zabezpečiť, aby povinnosti kybernetických tímov TLPT, ktoré sa majú zriadiť na úrovni orgánov TLPT, čo najviac zodpovedali povinnostiam kybernetických tímov TIBER-EÚ. Kybernetické tímy TLPT by preto mali mať testovacích manažérov, ktorí sú zodpovední za dohľad nad jednotlivými TLPT a za plánovanie a koordináciu jednotlivých testov. Kybernetické tímy TLPT by mali slúžiť ako jednotné kontaktné miesto pre komunikáciu s internými a externými zainteresovanými stranami týkajúcu sa testov, pre získavanie a spracovávanie spätnej väzby a skúseností získaných z predchádzajúcich testov a pre podporu finančných subjektov, ktoré sa podrobujú testovaniu TLPT.

(7) S cieľom kopírovať metodiku rámca TIBER-EÚ by testovací manažéri mali mať zručnosti a schopnosti potrebné na poskytovanie poradenstva a na zaujatie stanoviska k návrhom testovacích subjektov. Skúsenosti z rámca TIBER-EÚ preukázali, že je cenné, aby bol ku každému testu pridelený tím zložený z najmenej dvoch testovacích manažérov. V snahe zohľadniť, že TLPT sa používa na podporu vzdelávacích skúseností, na ochranu dôvernosti testov, a pokiaľ orgány TLPT nemajú problémy so zdrojmi alebo odbornými znalosťami, dôrazne sa im odporúča, aby zvážili, že počas trvania TLPT by testovací manažéri testov nemali vykonávať činnosti dohľadu nad tým istým finančným subjektom, ktorý sa podrobuje testovaniu TLPT.

(8) Na účely konzistentnosti s rámcom TIBER-EÚ je dôležité, aby orgán TLPT dôsledne sledoval testovanie v každom z jeho štádií. Vzhľadom na povahu testovania a riziká s ním spojené je nevyhnutné, aby bol orgán TLPT zapojený do každej konkrétnej fázy testovania. Predovšetkým by mali s orgánom TLPT prebiehať konzultácie, mal by validovať tie posúdenia alebo rozhodnutia finančných subjektov, ktoré môžu na jednej strane ovplyvniť účinnosť testu a na druhej strane môžu mať vplyv na riziká spojené s testom. Medzi základné kroky, pri ktorých je potrebné konkrétne zapojenie orgánu TLPT, patrí validovanie určitej základnej dokumentácie testovania a výber poskytovateľov spravodajských informácií o hrozbách a testovacích subjektov, ako aj opatrení na riadenie rizík. Zapojenie orgánov TLPT a najmä validácie by nemali viesť k nadmernému zaťaženiu týchto orgánov, a preto by mali byť obmedzené na tie dokumenty a rozhodnutia, ktoré priamo ovplyvňujú vykonávanie TLPT. Prostredníctvom aktívnej účasti v každej fáze testovania môžu orgány TLPT účinne posúdiť súlad finančných subjektov s príslušnými požiadavkami, čo by týmto orgánom malo umožniť vydávať osvedčenia podľa článku 26 ods. 7 nariadenia (EÚ) 2022/2554.

([2]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1114 z 31. mája 2023 o trhoch s kryptoaktívami a o zmene nariadení (EÚ) č. 1093/2010 a (EÚ) č. 1095/2010 a smerníc 2013/36/EÚ a (EÚ) 2019/1937 (Ú. v. EÚ L 150, 9.6.2023, s. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj).

(9) Utajenie je pri TLPT mimoriadne dôležité, aby sa zabezpečilo, že podmienky testovania budú realistické. Z tohto dôvodu by testovanie malo byť tajné a mali by sa prijať preventívne opatrenia na zachovanie dôvernosti TLPT vrátane výberu kódových označení, ktoré by mali byť navrhnuté tak, aby sa zabránilo identifikácii TLPT tretími stranami. Ak by zamestnanci zodpovední za bezpečnosť finančného tímu vedeli o plánovanom alebo prebiehajúcom TLPT, je pravdepodobné, že by boli pozornejší a ostražitejší ako za bežných pracovných podmienok, čo by viedlo k zmene výsledku testovania. Zamestnanci finančného subjektu mimo kontrolného tímu by preto mali byť informovaní o akomkoľvek plánovanom alebo prebiehajúcom TLPT len vtedy, ak na to existujú presvedčivé dôvody a na základe predchádzajúceho súhlasu testovacích manažérov, aby sa okrem iného zabezpečilo utajenie testu v prípade, že člen modrého tímu odhalil testovanie.

(10) Ako vyplýva zo skúseností zhromaždených v rámci TIBER-EÚ v súvislosti s „kontrolným tímom“, výber primeraného vedúceho kontrolného tímu je nevyhnutný pre bezpečné vykonávanie TLPT. Vedúci kontrolného tímu by mal mať v rámci finančného subjektu potrebný mandát na usmerňovanie všetkých aspektov testovania bez toho, aby bola ohrozená jeho dôvernosť. Z rovnakého dôvodu by členovia kontrolného tímu mali mať dôkladné znalosti o finančnom subjekte, pracovných úlohách a strategickom postavení vedúceho kontrolného tímu, mali by mať požadovaný počet odpracovaných rokov a mali by mať prístup k správnej rade. V záujme zníženia rizika ohrozenia TLPT by mal byť kontrolný tím čo najmenší.

(11) Existujú inherentné prvky rizík spojených s TLPT, keďže kritické funkcie sa testujú v živom produkčnom prostredí s možnosťou spôsobiť incidenty odmietnutia služby, neočakávané zrútenia systému, poškodenie kritických živých produkčných systémov alebo stratu, zmenu alebo zverejnenie údajov. Tieto riziká poukazujú na potrebu spoľahlivých opatrení na riadenie rizík. V snahe zabezpečiť, aby sa TLPT počas celého testovania vykonávalo kontrolovaným spôsobom, je veľmi dôležité, aby si finančné subjekty boli vždy vedomé konkrétnych rizík, ktoré vznikajú pri TLPT, a aby sa tieto riziká zmierňovali. V tejto súvislosti a bez toho, aby boli dotknuté vnútorné procesy finančného subjektu a zodpovednosť a delegovanie, ktoré sa už poskytli vedúcemu kontrolného tímu, môžu byť vhodné informácie o opatreniach na riadenie rizík TLPT alebo v osobitných prípadoch schválenie týchto opatrení na riadenie rizík samotným riadiacim orgánom finančného subjektu. Na to, aby bolo možné poskytovať účinné a čo najkvalifikovanejšie odborné služby a znížiť tieto riziká, je takisto nevyhnutné, aby testovacie subjekty a poskytovatelia spravodajských informácií o hrozbách (spoločne poskytovatelia TLPT) mali čo najvyššiu úroveň zručností, odborných znalostí a primeraných skúseností v oblasti spravodajských informácií o hrozbách a TLPT v sektore finančných služieb.

(12) Konvenčné penetračné testy poskytujú podrobné a užitočné posúdenie technických a konfiguračných zraniteľných miest, ktoré sa často nachádzajú v jednom systéme alebo v izolovanom prostredí, ale na rozdiel od testu červeného tímu na základe spravodajských informácií neposudzujú úplný scenár cieleného útoku na celý subjekt vrátane úplného rozsahu jeho ľudí, procesov a technológií. Počas výberového procesu poskytovateľov TLPT by preto finančné subjekty mali zabezpečovať, aby títo poskytovatelia mali potrebné zručnosti na vykonanie testov červeného tímu na základe spravodajských informácií, a nielen penetračných testov. Preto je nevyhnutné stanoviť komplexné kritériá pre testovacie subjekty, a to interné aj externé, a poskytovateľov spravodajských informácií o hrozbách, ktorí sú vždy externí. Ak poskytovatelia TLPT patria k tej istej spoločnosti, zamestnanci pridelení na TLPT by mali byť primerane oddelení.

(13) Výnimočné okolnosti môžu nastať, keď finančné subjekty nedokážu uzavrieť zmluvu s poskytovateľmi TLPT, ktorí spĺňajú komplexné kritériá. Finančné subjekty by preto po preukázaní nedostupnosti takýchto poskytovateľov spravodajských informácií o hrozbách mali mať možnosť zapojiť osoby, ktoré nespĺňajú všetky komplexné kritériá, za predpokladu, že náležite zmiernia akékoľvek výsledné dodatočné riziká a že orgán TLPT všetky tieto kritériá posúdi.

(14) Ak je do TLPT zapojených viacero finančných subjektov a viacero orgánov TLPT, úlohy všetkých strán v procese TLPT by sa mali určiť s cieľom vykonať najúčinnejší a najbezpečnejší test. Na účely združeného testovania sú potrebné osobitné požiadavky na bližšie špecifikovanie úlohy určeného finančného subjektu, konkrétne to, že by mal byť zodpovedný za poskytovanie všetkej potrebnej dokumentácie vedúcemu orgánu TLPT a za monitorovanie procesu testovania. Určený finančný subjekt by mal byť zodpovedný aj za spoločné aspekty posudzovania riadenia rizík. Bez ohľadu na úlohu určeného finančného subjektu by povinnosti každého finančného subjektu, ktorý sa zúčastňuje na procese združeného TLPT, mali zostať počas združeného testu nedotknuté. Rovnaká zásada by sa mala uplatňovať na spoločné TLPT.

(15) Ako vyplýva zo skúseností s vykonávaním rámca TIBER-EÚ, najúčinnejším spôsobom na zabezpečenie primeraného vykonávania testovania je uskutočňovanie osobných alebo virtuálnych stretnutí so všetkými dotknutými zainteresovanými stranami (finančné subjekty, orgány, testovacie subjekty a poskytovatelia spravodajských informácií o hrozbách). Osobné a virtuálne stretnutia by sa preto mali uskutočniť v rôznych fázach procesu, a to najmä počas prípravnej fázy pri spustení TLPT s cieľom sfinalizovať jeho rozsah pôsobnosti, počas testovacej fázy s cieľom dokončiť správu o spravodajských informáciách o hrozbách a plán testu červeného tímu a na účely týždenných aktualizácií, ako aj v záverečnej fáze s cieľom znovu si prehrať kroky testovacích subjektov a modrého tímu, fialové tímové cvičenie a poskytovať spätnú väzbu o TLPT.

(16) V snahe zabezpečiť hladké fungovanie TLPT by mal orgán TLPT finančnému subjektu jasne predstaviť svoje očakávania týkajúce sa testovania. V tejto súvislosti by testovací manažéri mali zabezpečiť vytvorenie primeraného toku informácií s kontrolným tímom v rámci finančného subjektu a s poskytovateľmi TLPT.

(17) Finančný subjekt by mal vybrať kritické alebo dôležité funkcie, ktoré budú spadať do rozsahu pôsobnosti TLPT. Pri výbere týchto funkcií by mal finančný subjekt použiť rôzne kritériá týkajúce sa významu každej funkcie pre samotný finančný subjekt a pre finančný sektor na úrovni Únie aj na vnútroštátnej úrovni, a to nielen z hospodárskeho hľadiska, ale aj s ohľadom na symbolický alebo politický štatút funkcie. V záujme uľahčenia hladkého prechodu do fázy zhromažďovania spravodajských informácií o hrozbách by mal kontrolný tím poskytovať testovacím subjektom a poskytovateľovi spravodajských informácií o hrozbách, ktorí nie sú zapojení do procesu určovania rozsahu pôsobnosti, podrobné informácie o dohodnutom stanovení rozsahu pôsobnosti.

(18) S cieľom poskytnúť testovacím subjektom informácie potrebné na simuláciu reálneho a realistického útoku na živé systémy finančného subjektu, ktoré podporujú jeho kritické alebo dôležité funkcie, by mal poskytovateľ spravodajských informácií o hrozbách zhromažďovať spravodajské informácie alebo informácie, ktoré sa týkajú aspoň dvoch kľúčových oblastí záujmu: cieľov, a to identifikáciou potenciálnych plôch útoku v celom finančnom subjekte, a hrozieb, a to identifikáciou relevantných aktérov hrozieb a pravdepodobných scenárov hrozieb. S cieľom zabezpečiť, aby poskytovateľ spravodajských informácií o hrozbách zohľadnil relevantné hrozby pre finančný subjekt, by testovacie subjekty, kontrolný tím a testovací manažéri mali poskytovať spätnú väzbu k návrhu správy o spravodajských informáciách o hrozbách. Poskytovateľ spravodajských informácií o hrozbách môže použiť všeobecnú panorámu hrozieb, ktorú poskytol orgán TLPT pre finančný sektor členského štátu, ako základ pre vnútroštátnu panorámu hrozieb, ak je takáto panoráma k dispozícii. Na základe uplatňovania rámca TIBER-EÚ zvyčajne trvá proces zhromažďovania spravodajských informácií o hrozbách približne 4 týždne.

(19) V snahe umožniť testovacím subjektom získať prehľad a ďalej skúmať dokument so špecifikáciou rozsahu a cielenú správu o spravodajských informáciách o hrozbách s cieľom dokončiť plán testovania prostredníctvom červeného tímu je nevyhnutné, aby pred fázou testovania TLPT prostredníctvom červeného tímu testujúce subjekty dostali od poskytovateľa spravodajských informácií o hrozbách podrobné vysvetlenia k cielenej správe o spravodajských informáciách o hrozbách a analýzu možných scenárov hrozieb.

(20) V záujme umožnenia testovacím subjektom vykonať realistické a komplexné testovanie, v rámci ktorého sa vykonajú všetky fázy útoku a dosiahnu sa vlajky, by sa fáze aktívneho testovania prostredníctvom červeného tímu mal alokovať dostatočný čas. Na základe skúseností získaných s rámcom TIBER-EÚ by mal byť alokovaný čas v trvaní aspoň 12 týždňov a mal by sa určiť s prihliadnutím na počet zúčastnených strán, rozsah pôsobnosti TLPT, zdroje zapojeného finančného subjektu alebo subjektov, akékoľvek externé požiadavky a dostupnosť podporných informácií, ktoré poskytol finančný subjekt.

(21) Počas fázy aktívneho testovania prostredníctvom červeného tímu by testovacie subjekty mali na primerané otestovanie živých produkčných systémov finančného subjektu použiť celú škálu taktík, techník a postupov (TTP). TTP by mali podľa potreby obsahovať prieskum (t. j. zhromažďovanie čo najväčšieho množstva informácií o cieli), využívanie informácií ako zbraní (t. j. analýza informácií o infraštruktúre, zariadeniach a zamestnancoch a príprava na operácie špecifické pre daný cieľ), realizáciu (t. j. aktívne spustenie plnej operácie na cieľ), využitie (t. j. kde je cieľom testovacích subjektov napadnúť servery, siete finančného subjektu a využívať jeho zamestnancov prostredníctvom sociálneho inžinierstva), kontrolu a pohyb (t. j. pokusy o prechod od napadnutých systémov k ďalším zraniteľným systémom alebo systémom s vysokou hodnotou) a opatrenia zamerané na cieľ (t. j. získanie ďalšieho prístupu s cieľom napadnúť systémy a získanie prístupu k predtým dohodnutým cieľovým informáciám a údajom, ako sa predtým dohodlo v pláne testu červeného tímu).

(22) Pri vykonávaní TLPT by mali testovacie subjekty konať s prihliadnutím na čas, ktorý je k dispozícii na vykonanie útoku, zdroje a etické a právne hranice. Ak by testovacie subjekty nedokázali prikročiť k ďalšej naprogramovanej fáze útoku, kontrolný tím by im mal po dohode s orgánom TLPT príležitostne poskytnúť pomoc vo forme „opôr“. Opory môžu byť vo všeobecnosti kategorizované do informačných opôr a prístupových opôr a môžu spočívať v poskytovaní prístupu k systémom IKT alebo interným sieťam, aby sa mohlo pokračovať v teste a zamerať sa na nasledujúce kroky útoku.

(23) Počas aktívneho červeného tímového cvičenia v testovacej fáze, ak je to potrebné na umožnenie pokračovania TLPT ako poslednej možnosti za výnimočných okolností a po vyčerpaní všetkých alternatívnych možností, by sa mala použiť kolaboratívna testovacia činnosť, ktorá zahŕňa testovacie subjekty a modrý tím. V súvislosti s takýmto obmedzeným fialovým tímovým cvičením sa môžu použiť tieto metódy: „chyť a pusti“ (*catch-and-release*), kde sa testovacie subjekty pokúšajú pokračovať v scenároch, sú odhalení a potom obnovia testovanie, „vojnové hry“ (*war gaming*), ktoré počítajú so zložitejšími scenármi na testovanie strategického rozhodovania, alebo „kolaboratívne overovanie konceptu“ (*collaborative proof-of-concept*), ktoré umožňuje testovacím subjektom a členom modrého tímu spoločne validovať konkrétne bezpečnostné opatrenia, nástroje alebo techniky v kontrolovanom a kooperatívnom prostredí.

(24) TLPT by sa malo využívať ako vzdelávacia skúsenosť s cieľom zvýšiť digitálnu prevádzkovú odolnosť finančných subjektov. V tejto súvislosti by si modrý tím a testovacie subjekty mali znovu prehrať útok a preskúmať kroky prijaté s cieľom poučiť sa zo skúseností s testovaním v spolupráci s testovacími subjektmi. Na tento účel a s cieľom umožniť primeranú prípravu by sa mala správa o teste červeného tímu a správa o teste modrého tímu sprístupniť všetkým stranám zapojeným do činností opätovného prehrávania pred vykonaním akýchkoľvek činností opätovného prehrávania. Okrem toho by sa v záverečnej fáze malo uskutočniť fialové tímové cvičenie, aby sa maximalizovali vzdelávacie skúsenosti. Metódy, ktoré sa môžu použiť pri fialovom tímovom cvičení v záverečnej fáze, by mali zahŕňať diskusie o alternatívnych scenároch útoku, preskúmanie živých systémov v alternatívnych scenároch alebo opätovné preskúmanie plánovaných scenárov na živých systémoch, ktoré testovacie subjekty neboli schopné dokončiť alebo vykonať počas testovacej fázy.

(25) Na ďalšie uľahčenie vzdelávacích skúseností všetkých strán zapojených do TLPT v prospech budúcich testov a na podporu digitálnej prevádzkovej odolnosti finančných subjektov by si dotknuté strany mali navzájom poskytovať spätnú väzbu o celkovom procese, a najmä určiť, ktoré činnosti napredovali dobre alebo sa mohli zlepšiť a ktoré aspekty procesu TLPT fungovali dobre alebo by sa mohli zlepšiť.

(26) Príslušné orgány uvedené v článku 46 nariadenia (EÚ) 2022/2554 a, ak sú odlišné, orgány TLPT by mali spolupracovať s cieľom začleniť pokročilé testovanie prostredníctvom TLPT do existujúcich procesov dohľadu. V tejto súvislosti a s cieľom dosiahnuť správne pochopenie zistení TLPT a spôsobu ich výkladu je vhodné, aby sa najmä v prípade súhrnnej správy o teste a plánov nápravy nadviazala úzka spolupráca medzi testovacími manažérmi, ktorí boli zapojení do TLPT, a zodpovednými orgánmi dohľadu.

(27) V článku 26 ods. 8 prvom pododseku nariadenia (EÚ) 2022/2554 sa od finančných subjektov vyžaduje, aby uzatvárali zmluvy s externými testovacími subjektmi po každom treťom testovaní. Ak finančné subjekty zahŕňajú do tímu testovacích subjektov interné aj externé testovacie subjekty, malo by sa to na účely uvedeného článku považovať za TLPT vykonávané s internými testovacími subjektmi.

(28) Toto nariadenie vychádza z návrhu regulačných technických predpisov, ktorý Komisii predložili Európsky orgán pre bankovníctvo, Európsky orgán pre poisťovníctvo a dôchodkové poistenie zamestnancov a Európsky orgán pre cenné papiere a trhy (európske orgány dohľadu) so súhlasom Európskej centrálnej banky.

(29) Európske orgány dohľadu uskutočnili otvorené verejné konzultácie k návrhu regulačných technických predpisov, z ktorých toto nariadenie vychádza, analyzovali možné súvisiace náklady a prínosy a požiadali o poradenstvo Skupinu zainteresovaných strán v bankovníctve zriadenú v súlade s článkom 37 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1093/2010 ([3]), Skupinu zainteresovaných strán v poisťovníctve a zaisťovníctve zriadenú v súlade s článkom 37 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1094/2010 ([4]) a Skupinu zainteresovaných strán v oblasti cenných papierov a trhov zriadenú v súlade s článkom 37 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1095/2010 ([5]),

(30) V súlade s článkom 42 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 ([6]) sa konzultovalo s európskym dozorným úradníkom pre ochranu údajov, ktorý vydal 20. augusta 2024 svoje stanovisko,

PRIJALA TOTO NARIADENIE:

*Článok 1*

**Vymedzenie pojmov**

Na účely tohto nariadenia sa uplatňuje toto vymedzenie pojmov:

1. „kontrolný tím“ je tím zložený zo zamestnancov testovaného finančného subjektu a, ak je to relevantné vzhľadom na rozsah pôsobnosti TLPT, zo zamestnancov jeho externých poskytovateľov služieb a akejkoľvek inej strany, ktorá test riadi;

2. „vedúci kontrolného tímu“ je zamestnanec finančného subjektu zodpovedný za vykonávanie všetkých činností súvisiacich s TLPT pre finančný subjekt v kontexte daného testu;

3. „modrý tím“ sú zamestnanci finančného subjektu a prípadne zamestnanci externých poskytovateľov služieb finančného subjektu a akejkoľvek inej strany považovanej za relevantnú z hľadiska rozsahu pôsobnosti TLPT, externých poskytovateľov služieb finančného subjektu, ktorí bránia používanie sietí a informačných systémov finančného subjektu, a to udržiavaním stavu bezpečnosti pred simulovanými alebo skutočnými útokmi a ktorí nemajú vedomosť o TLPT;

4. „úlohy modrého tímu“ sú úlohy, ktoré zvyčajne vykonáva modrý tím, ako sú centrum bezpečnostných operácií (CBO), služby infraštruktúry IKT, služby helpdesku, služby riadenia incidentov na operačnej úrovni;

5. „červený tím“ sú interné alebo externé testovacie subjekty, ktoré sú zazmluvnené alebo pridelené na TLPT;

6. „fialové cvičenie“ je kolaboratívna testovacia činnosť, ktorá zahŕňa testovacie subjekty a modrý tím;

([3]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1093/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre bankovníctvo) a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/78/ES (Ú. v. EÚ L 331, 15.12.2010, s. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1094/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre poisťovníctvo a dôchodkové poistenie zamestnancov), a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/79/ES (Ú. v. EÚ L 331, 15.12.2010, s. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1095/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre cenné papiere a trhy) a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/77/ES (Ú. v. EÚ L 331, 15.12.2010, s. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

7. „orgán TLPT“ je ktorýkoľvek z týchto orgánov:

   a) jeden verejný orgán vo finančnom sektore určený v súlade s článkom 26 ods. 9 nariadenia (EÚ) 2022/2554;

   b) orgán vo finančnom sektore, na ktorý sa deleguje vykonávanie niektorých alebo všetkých úloh v súvislosti s TLPT v súlade s článkom 26 ods. 10 nariadenia (EÚ) 2022/2554;

   c) ktorýkoľvek príslušný orgán uvedený v článku 46 nariadenia (EÚ) 2022/2554;

8. „kybernetický tím TLPT“ alebo „KTT“ sú zamestnanci orgánov TLPT, ktorí sú zodpovední za záležitosti súvisiace s TLPT;

9. „testovací manažéri“ sú zamestnanci určení na vedenie činností orgánu TLPT pre konkrétne TLPT s cieľom monitorovať súlad s týmto nariadením;

10. „poskytovateľ spravodajských informácií o hrozbách“ sú odborníci, s ktorými finančný subjekt uzavrel zmluvu pre každé TLPT, a ktorí sú externí vo vzťahu k finančnému subjektu a prípadne vnútroskupinovým poskytovateľom IKT služieb, ktorí zhromažďujú a analyzujú cielené spravodajské informácie o hrozbách relevantné pre finančné subjekty v rozsahu pôsobnosti konkrétneho cvičenia TLPT a vypracúvajú zodpovedajúce relevantné a realistické scenáre hrozieb;

11. „poskytovatelia TLPT“ sú testovacie subjekty a poskytovatelia spravodajských informácií o hrozbách;

12. „opora“ je pomoc alebo informácie, ktoré kontrolný tím poskytuje testovacím subjektom s cieľom umožniť testovacím subjektom pokračovať vo vykonávaní dráhy útoku, ak nie sú schopní napredovať samostatne a ak neexistuje žiadna iná primeraná alternatíva, a to aj vzhľadom na nedostatočný čas alebo zdroje v danom TLPT;

13. „dráha útoku“ je trasa, ktorú nasledujú testovacie subjekty počas fázy aktívneho testovania prostredníctvom červeného tímu TLPT, aby dosiahli vlajky špecifikované pre dané TLPT;

14. „vlajky“ sú kľúčové ciele IKT systémov podporujúcich kritické alebo dôležité funkcie finančného subjektu, ktoré sa testovacie subjekty snažia dosiahnuť cez test;

15. „citlivé informácie“ sú informácie, ktoré možno ľahko využiť na vykonanie útokov na IKT systémy finančného subjektu, duševné vlastníctvo, dôverné obchodné údaje alebo osobné údaje, ktoré môžu priamo alebo nepriamo poškodiť finančný subjekt a jeho ekosystém, ak by boli v rukách aktérov s nekalými úmyslami;

16. „združené subjekty“ sú všetky finančné subjekty, ktoré sa zúčastňujú na združenom TLPT podľa článku 26 ods. 4 nariadenia (EÚ) 2022/2554;

17. „hostiteľský členský štát“ je hostiteľský členský štát v súlade s odvetvovým právom Únie uplatniteľným na každý finančný subjekt;

18. „spoločné TLPT“ je TLPT iné než združené TLPT uvedené v článku 26 ods. 4 nariadenia (EÚ) 2022/2554, do ktorého je zapojených viacero finančných subjektov, ktoré využívajú toho istého vnútroskupinového poskytovateľa IKT služieb alebo patria do tej istej skupiny a zdieľajú IKT systémy.

*Článok 2*

**Identifikácia finančných subjektov povinných vykonať TLPT**

1. Orgány TLPT posudzujú, či je akýkoľvek finančný subjekt povinný vykonať TLPT, pričom zohľadňujú vplyv týchto finančných subjektov, ich systémový charakter a ich rizikový profil v oblasti IKT, a to na základe všetkých týchto kritérií:

a) faktory súvisiace s vplyvom a systémovým charakterom:

   i) veľkosť finančného subjektu určená na základe toho, či finančný subjekt poskytuje finančné služby v jednom alebo viacerých členských štátoch, a porovnaním činností finančného subjektu s činnosťami iných finančných subjektov poskytujúcich podobné služby;

   ii) rozsah a povaha prepojenia finančného subjektu s inými finančnými subjektmi vo finančnom sektore v jednom alebo viacerých členských štátoch;

   iii) kritickosť alebo význam služieb, ktoré finančný subjekt poskytuje finančnému sektoru;

iv) nahraditeľnosť služieb, ktoré finančný subjekt poskytuje;

v) zložitosť obchodného modelu finančného subjektu a súvisiacich služieb a procesov;

vi) či je finančný subjekt súčasťou skupiny systémového charakteru na úrovni Únie alebo na vnútroštátnej úrovni vo finančnom sektore a zdieľa IKT systémy;

b) faktory súvisiace s IKT rizikom:

i) rizikový profil finančného subjektu;

ii) panoráma hrozieb finančného subjektu;

iii) stupeň závislosti kritických alebo dôležitých funkcií alebo ich podporných funkcií finančného subjektu od IKT systémov a procesov;

iv) zložitosť architektúry IKT finančného subjektu;

v) IKT služby a funkcie podporované externými poskytovateľmi IKT služieb a množstvo a typ zmluvných dojednaní s externými poskytovateľmi IKT služieb alebo vnútroskupinovými poskytovateľmi IKT služieb;

vi) výsledky všetkých preskúmaní orgánmi dohľadu, ktoré sú relevantné pre posúdenie vyspelosti finančného subjektu v oblasti IKT;

vii) vyspelosť plánov kontinuity činností v oblasti IKT a plánov reakcie a obnovy v oblasti IKT;

viii) vyspelosť operačných bezpečnostných opatrení v oblasti IKT na odhaľovanie a zmierňovanie vrátane schopnosti:

1. neustále monitorovať infraštruktúru IKT finančného subjektu;

2. v reálnom čase odhaľovať udalosti súvisiace s IKT;

3. analyzovať udalosti uvedené v bode 2;

4. včas a účinne reagovať na udalosti uvedené v bode 2;

ix) či je finančný subjekt súčasťou skupiny pôsobiacej vo finančnom sektore na úrovni Únie alebo na vnútroštátnej úrovni, v rámci ktorej sa zdieľajú IKT systémy.

Ak je to možné, orgán TLPT na účely písmena a) bodu i) berie do úvahy:

a) postavenie finančného subjektu z hľadiska trhového podielu na úrovni Únie a na vnútroštátnej úrovni;

b) rozsah činností, ktoré finančný subjekt ponúka;

c) trhový podiel služieb, ktoré poskytuje finančný subjekt, alebo činností vykonávaných na úrovni Únie a na vnútroštátnej úrovni.

Ak je to možné, orgán TLPT na účely písmena a) bodu v) berie do úvahy:

a) či finančný subjekt prevádzkuje viac než jeden obchodný model;

b) prepojenosť rôznych obchodných procesov a súvisiacich služieb.

2. Orgány TLPT vyžadujú, aby TLPT vykonávali všetky nasledujúce finančné subjekty, pokiaľ z posúdenia uvedeného v odseku 1 v súvislosti s finančným subjektom nevyplýva, že jeho vplyv, obavy o finančnú stabilitu týkajúce sa daného finančného subjektu alebo jeho rizikový profil v oblasti IKT neodôvodňujú vykonanie TLPT:

a) úverové inštitúcie, ktoré spĺňajú ktorúkoľvek z týchto podmienok:

i) boli identifikované ako globálne systémovo významné inštitúcie (G-SII) v súlade s článkom 131 smernice Európskeho parlamentu a Rady 2013/36/EÚ ([7]);

ii) boli identifikované ako inak systémovo významné inštitúcie (O-SII) v súlade s článkom 131 smernice 2013/36/EÚ;

iii) sú súčasťou G-SII alebo O-SII;

([7]) Smernica Európskeho parlamentu a Rady 2013/36/EÚ z 26. júna 2013 o prístupe k činnosti úverových inštitúcií a prudenciálnom dohľade nad úverovými inštitúciami, o zmene smernice 2002/87/ES a o zrušení smerníc 2006/48/ES a 2006/49/ES (Ú. v. EÚ L 176, 27.6.2013, s. 338, ELI: http://data.europa.eu/eli/dir/2013/36/oj).

b) platobné inštitúcie, ktoré v každom z dvoch kalendárnych rokov predchádzajúcich posúdeniu orgánom TLPT prekročili celkovú hodnotu platobných transakcií vo výške 150 miliárd EUR v zmysle vymedzenia v článku 4 bode 5 smernice Európskeho parlamentu a Rady (EÚ) 2015/2366 ([8]);

c) inštitúcie elektronického peňažníctva, ktoré v každom z dvoch kalendárnych rokov predchádzajúcich posúdeniu orgánom TLPT prekročili buď celkovú hodnotu platobných transakcií vo výške 150 miliárd EUR v zmysle vymedzenia v článku 4 bode 5 smernice (EÚ) 2015/2366 alebo celkovú hodnotu 40 miliárd EUR sumy vydaných elektronických peňazí;

d) centrálne depozitáre cenných papierov;

e) centrálne protistrany;

f) obchodné miesta s elektronickým systémom obchodovania, ktoré spĺňajú ktorékoľvek z týchto kritérií:

i) obchodné miesto má najvyšší trhový podiel z hľadiska obratu na vnútroštátnej úrovni v každom z dvoch kalendárnych rokov predchádzajúcich posúdeniu orgánom TLPT v ktoromkoľvek z týchto prípadov:

1. prevoditeľné cenné papiere v zmysle vymedzenia v článku 4 ods. 1 bode 44 písm. a) smernice Európskeho parlamentu a Rady 2014/65/EÚ ([9]);

2. prevoditeľné cenné papiere v zmysle vymedzenia v článku 4 ods. 1 bode 44 písm. b) smernice 2014/65/EÚ;

3. deriváty v zmysle vymedzenia v článku 2 ods. 1 bode 29 nariadenia Európskeho parlamentu a Rady (EÚ) č. 600/2014 ([10]);

4. štruktúrované finančné produkty v zmysle vymedzenia v článku 2 ods. 1 bode 28 nariadenia (EÚ) č. 600/2014;

5. emisné kvóty uvedené v oddiele C bode 11 prílohy I k smernici 2014/65/EÚ;

ii) obchodné miesto má trhový podiel z hľadiska obratu na úrovni Únie, ktorý presahuje 5 % v každom z dvoch kalendárnych rokov predchádzajúcich posúdeniu orgánom TLPT v ktoromkoľvek z týchto prípadov:

1. akcie spoločností a iné cenné papiere rovnocenné s akciami spoločností, osobných spoločností alebo iných subjektov a vkladové potvrdenky týkajúce sa akcií;

2. dlhopisy alebo iné formy sekuritizovaných dlhových cenných papierov vrátane vkladových potvrdeniek týkajúcich sa takýchto cenných papierov;

3. deriváty v zmysle vymedzenia v článku 2 ods. 1 bode 29 nariadenia (EÚ) č. 600/2014;

4. štruktúrované finančné produkty v zmysle vymedzenia v článku 2 ods. 1 bode 28 nariadenia (EÚ) č. 600/2014;

5. emisné kvóty uvedené v oddiele C bode 11 prílohy I k smernici 2014/65/EÚ;

([8]) Smernica Európskeho parlamentu a Rady (EÚ) 2015/2366 z 25. novembra 2015 o platobných službách na vnútornom trhu, ktorou sa menia smernice 2002/65/ES, 2009/110/ES a 2013/36/EÚ a nariadenie (EÚ) č. 1093/2010 a ktorou sa zrušuje smernica 2007/64/ES (Ú. v. EÚ L 337, 23.12.2015, s. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

([9]) Smernica Európskeho parlamentu a Rady 2014/65/EÚ z 15. mája 2014 o trhoch s finančnými nástrojmi, ktorou sa mení smernica 2002/92/ES a smernica 2011/61/EÚ (Ú. v. EÚ L 173, 12.6.2014, s. 349, ELI: http://data.europa.eu/eli/dir/2014/65/oj).

([10]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 600/2014 z 15. mája 2014 o trhoch s finančnými nástrojmi, ktorým sa mení nariadenie (EÚ) č. 648/2012 (Ú. v. EÚ L 173, 12.6.2014, s. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

g) poisťovne a zaisťovne, ktoré spĺňajú všetky tieto kritériá:

i) majú hrubé predpísané poistné, ktoré presahuje 1 500 000 000 EUR;

ii) majú technické rezervy, ktoré presahujú 10 000 000 000 EUR;

iii) poisťovne, ktoré vykonávajú len činnosti životného poistenia alebo činnosti životného aj neživotného poistenia a ktorých celkové aktíva presahujú 3,5 % súčtu celkových aktív poisťovní a zaisťovní usadených v členskom štáte ocenených v súlade s článkom 75 smernice Európskeho parlamentu a Rady ([11]) 2009/138/ES.

Na účely písmena f) bodu ii), ak je obchodné miesto súčasťou skupiny zdieľajúcej IKT systémy alebo toho istého vnútroskupinového poskytovateľa IKT služieb, zohľadňuje sa obrat zmlúv o cenných papieroch a derivátoch na všetkých obchodných miestach patriacich tej istej skupine a usadených v Únii.

Na účely písmena g) orgány TLPT identifikujú podskupinu všetkých poisťovní a zaisťovní tak, že uplatňujú kritériá stanovené v písmene g) bodoch i), ii) a iii). Poisťovne a zaisťovne zahrnuté do tejto podskupiny sú povinné vykonať TLPT, ak zároveň spĺňajú ktorékoľvek z týchto kritérií:

a) majú hrubé predpísané poistné, ktoré presahuje 3 000 000 000 EUR;

b) majú technické rezervy, ktoré presahujú 30 000 000 000 EUR;

c) celkové aktíva, ktoré presahujú 10 % súčtu celkových aktív poisťovní a zaisťovní usadených v členskom štáte ocenených v súlade s článkom 75 smernice 2009/138/ES.

3. Ak viac než jeden finančný subjekt, ktorý patrí do tej istej skupiny, v ktorej sa zdieľajú IKT systémy, alebo ak viac než jeden finančný subjekt používajúci toho istého vnútroskupinového poskytovateľa IKT služieb spĺňa kritériá stanovené v odseku 2, orgány TLPT týchto finančných subjektov v súlade s článkom 16 ods. 2 rozhodujú, či je požiadavka vykonať TLPT na individuálnom základe pre tieto finančné subjekty relevantná.

Ak je orgán TLPT materského podniku skupiny finančných subjektov uvedenej v prvom pododseku odlišný od orgánov TLPT finančných subjektov skupiny, orgány TLPT finančných subjektov patriacich do tejto skupiny konzultujú s týmto orgánom, či je vhodné vykonať TLPT na individuálnom základe.

*Článok 3*

**KTT a testovací manažéri TLPT**

1. Orgán TLPT prideľuje zodpovednosť za koordináciu činností súvisiacich s TLPT na KTT. KTT sa skladá z testovacích manažérov, ktorí sú poverení dohľadom nad jednotlivými TLPT.

2. Pre každý test určuje orgán TLPT testovacieho manažéra a aspoň jedného náhradníka.

3. Testovací manažéri monitorujú, či sú splnené požiadavky stanovené v tomto nariadení, a zabezpečujú, aby boli splnené.

([11]) Smernica Európskeho parlamentu a Rady 2009/138/ES z 25. novembra 2009 o začatí a vykonávaní poistenia a zaistenia (Solventnosť II) (Ú. v. EÚ L 335, 17.12.2009, s. 1 ELI: http://data.europa.eu/eli/dir/2009/138/oj).

4. Testovací manažér oznamuje kontaktné údaje KTT finančnému subjektu prostredníctvom oznámenia uvedeného v článku 9 ods. 1.

5. Orgán TLPT sa zúčastňuje na všetkých fázach TLPT.

*Článok 4*

**Organizačné opatrenia pre finančné subjekty**

1. Finančné subjekty menujú vedúceho kontrolného tímu, ktorý je zodpovedný za každodenné riadenie TLPT a za rozhodnutia a činnosti kontrolného tímu.

2. Finančné subjekty musia zaviesť organizačné a procesné opatrenia s cieľom zabezpečiť, aby:

a) bol prístup k informáciám týkajúcich sa akéhokoľvek plánovaného alebo prebiehajúceho TLPT obmedzený na kontrolný tím, riadiaci orgán, testovacie subjekty, poskytovateľa spravodajských informácií o hrozbách a orgán TLPT na základe „need-to-know“;

b) kontrolný tím konzultoval s testovacími manažérmi pred tým, než zapojí ktoréhokoľvek člena modrého tímu do TLPT;

c) bol kontrolný tím informovaný o každom odhalení TLPT zamestnancami finančného subjektu alebo jeho externými poskytovateľmi služieb; v prípade eskalácie výslednej reakcie na incident v prípade potreby kontrolný tím takúto eskaláciu zvládol;

d) boli zavedené opatrenia týkajúce sa utajenia TLPT, ktoré sa vzťahujú na zamestnancov finančného subjektu, zamestnancov dotknutých externých poskytovateľov IKT služieb, testovacích subjektov a poskytovateľa spravodajských informácií o hrozbách;

e) kontrolný tím na požiadanie poskytol testovacím manažérom všetky informácie týkajúce sa TLPT;

f) strany zapojené do TLPT odkazovali na toto testovanie len kódovým označením, ak je to možné.

*Článok 5*

**Riadenie rizík pre TLPT**

1. Kontrolný tím posudzuje počas prípravnej fázy uvedenej v článku 9 riziká spojené s testovaním živých produkčných systémov kritických alebo dôležitých funkcií finančného subjektu vrátane potenciálnych vplyvov na:

a) finančný sektor;

b) finančnú stabilitu na úrovni Únie alebo na vnútroštátnej úrovni.

Kontrolný tím skúma tieto vplyvy počas celého testovania.

2. Na účely posúdenia a riadenia rizík kontrolný tím zohľadňuje aspoň tieto druhy rizík súvisiacich s:

a) poskytovaním prístupu k citlivým informáciám o finančnom subjekte poskytovateľovi spravodajských informácií o hrozbách a v uplatniteľných prípadoch externým testovacím subjektom;

b) nesúladom TLPT s nariadením (EÚ) 2022/2554 a s týmto nariadením, ak má takýto nesúlad za následok neposkytnutie osvedčenia uvedeného v článku 26 ods. 7 nariadenia (EÚ) 2022/2554, a to aj vtedy, ak je takýto nesúlad spôsobený porušením dôvernosti TLPT alebo neetickým správaním;

c) eskaláciou krízy a incidentov;

d) aktívnou fázou červeného tímu vrátane rizík súvisiacich s prerušením kritických činností a poškodením údajov v dôsledku činností testovacích subjektov a jej možnými dôsledkami pre tretie strany;

e) činnosťou modrého tímu vrátane rizík súvisiacich s prerušením kritických činností a poškodením údajov v dôsledku činností modrého tímu a jej možnými dôsledkami pre tretie strany;

f) neúplnou obnovou systémov ovplyvnených TLPT.

*Článok 6*

**Riadenie rizík pre združené alebo spoločné TLPT**

1. V prípade spoločného TLPT alebo združeného TLPT kontrolný tím každého finančného subjektu vykonáva vlastné posúdenie rizík a stanovuje vlastné opatrenia na riadenie rizík.

2. Kontrolný tím určeného finančného subjektu uvedeného v článku 16 ods. 3 písm. b) tohto nariadenia alebo finančný subjekt určený v súlade s článkom 26 ods. 4 nariadenia (EÚ) 2022/2554 posudzuje riziká súvisiace so zapojením viacerých finančných subjektov do TLPT. Kontrolné tímy zapojených finančných subjektov spolupracujú s kontrolným tímom určeného finančného subjektu s cieľom identifikovať potenciálne spoločné riziká.

*Článok 7*

**Výber poskytovateľov TLPT**

1. Kontrolný tím prijíma opatrenia na riadenie rizík súvisiacich s TLPT a predovšetkým zabezpečuje, aby pri každom TLPT:

a) poskytovateľ spravodajských informácií o hrozbách a externé testovacie subjekty poskytli kontrolnému tímu podrobný životopis a kópie osvedčení, ktoré sú podľa uznávaných trhových noriem primerané pre výkon ich činností;

b) poskytovateľ spravodajských informácií o hrozbách a externý testovací subjekt boli riadne a v plnom rozsahu krytí príslušnými poisteniami zodpovednosti za škodu spôsobenú pri výkone povolania, a to aj pre prípad pochybenia a nedbanlivosti;

c) poskytovateľ spravodajských informácií o hrozbách poskytol aspoň tri referencie z predchádzajúcich zadaní v súvislosti s penetračným testovaním a testovaním prostredníctvom červeného tímu;

d) externé testovacie subjekty poskytli aspoň päť referencií z predchádzajúcich zadaní súvisiacich s penetračným testovaním a testovaním prostredníctvom červeného tímu;

e) zamestnanci poskytovateľa spravodajských informácií o hrozbách priradení k TLPT:

   i) pozostávali aspoň z manažéra s minimálne päťročnými skúsenosťami v oblasti spravodajských informácií o hrozbách a aspoň jedného ďalšieho člena s minimálne dvojročnými skúsenosťami v oblasti spravodajských informácií o hrozbách;

   ii) mali rozhľad a primeranú úroveň odborných znalostí a zručností vrátane:

      1. taktík, techník a postupov zhromažďovania spravodajských informácií;

      2. geopolitických, technických a sektorových znalostí;

      3. primeraných komunikačných zručností s cieľom jasne prezentovať svojho zapojenia a podávať o ňom správy;

   iii) mali kombinovanú účasť aspoň na troch predchádzajúcich zadaniach v oblasti spravodajských informácií o hrozbách v súvislosti s penetračným testovaním a testovaním prostredníctvom červeného tímu;

   iv) nevykonávali súčasne žiadne úlohy modrého tímu ani iné služby, ktoré by mohli predstavovať konflikt záujmov vo vzťahu k finančnému subjektu, externému poskytovateľovi IKT služieb alebo vnútroskupinovému poskytovateľovi IKT služieb zapojených do TLPT, ku ktorému sú priradení;

   v) boli oddelení od zamestnancov toho istého poskytovateľa TLPT, ktorý poskytuje externé testovacie subjekty pre ten istý TLPT, a neboli podriadení týmto zamestnancom;

f) v prípade externých testovacích subjektov červený tím priradený k TLPT:

i) pozostával aspoň z manažéra s minimálne päťročnými skúsenosťami s penetračným testovaním a testovaním prostredníctvom červeného tímu, ako aj aspoň z dvoch ďalších testovacích subjektov, pričom každý z nich má minimálne dvojročné skúsenosti s penetračným testovaním a testovaním prostredníctvom červeného tímu;

ii) mal rozhľad a primeranú úroveň odborných znalostí a zručností vrátane znalostí o podnikaní finančného subjektu, prieskume, riadení rizík, rozvoja využitia, fyzickom prieniku, sociálnom inžinierstve, analýze zraniteľnosti, ako aj primeraných komunikačných zručností s cieľom jasne prezentovať výsledok svojho zapojenia a podávať o ňom správy;

iii) mal kombinovanú účasť aspoň na piatich predchádzajúcich zadaniach súvisiacich s penetračným testovaním a testovaním prostredníctvom červeného tímu;

iv) nebol zamestnaný poskytovateľom spravodajských informácií o hrozbách, ktorý súčasne vykonáva úlohy modrého tímu pre finančný subjekt, externého poskytovateľa IKT služieb alebo vnútroskupinového poskytovateľa IKT služieb, ktorý je zapojený do TLPT, ani mu neposkytoval služby;

v) bol oddelený od všetkých zamestnancov toho istého poskytovateľa TLPT, ktorý súčasne poskytuje služby v oblasti spravodajských informáciách o hrozbách pre ten istý TLPT;

g) testovacie subjekty a poskytovateľ spravodajských informácií o hrozbách na konci testovania vykonali postupy obnovy vrátane bezpečného vymazania informácií týkajúcich sa hesiel, prihlasovacích údajov a iných tajných kľúčov, ktoré boli napadnuté počas TLPT, zabezpečenej komunikácie s finančnými subjektmi o napadnutých účtoch, bezpečného zhromažďovania, uchovania, správy a likvidácie iných údajov zhromaždených počas testovania;

h) testovacie subjekty okrem postupov obnovy na konci testovania uvedených v písmene g) vykonávali tieto postupy obnovy:

i) deaktiváciu velenia a riadenia;

ii) núdzové vypínače rozsahu a dátumu;

iii) odstránenie zadných dvierok a iného malvéru;

iv) oznámenie o možnom porušení;

v) postupy obnovy záloh v budúcnosti, ktoré sa môžu týkať malvéru alebo nástrojov nainštalovaných počas testu;

vi) monitorovanie činností modrého tímu a informovanie kontrolného tímu o všetkých možných odhaleniach;

i) testovacie subjekty a poskytovateľ spravodajských informácií o hrozbách nevykonávali žiadnu z nasledujúcich činností ani sa na nich nezúčastňovali:

i) prípadné neoprávnené zničenie vybavenia finančného subjektu a jeho prípadných externých poskytovateľov IKT služieb;

ii) nekontrolovaná zmena informácií a IKT aktív finančného subjektu a jeho prípadných externých poskytovateľov IKT služieb;

iii) úmyselné narušenie kontinuity kritických alebo dôležitých funkcií finančného subjektu;

iv) neoprávnené vkladanie systémov mimo rozsahu pôsobnosti;

v) neoprávnené zverejňovanie výsledkov testov.

2. Kontrolný tím vedie v záujme preukázania súladu s odsekom 1 písm. a) až f) záznamy o dokumentácii, ktorú poskytli testovacie subjekty a poskytovatelia spravodajských informácií o hrozbách.

Za výnimočných okolností môžu finančné subjekty uzavrieť zmluvu s externými testovacími subjektmi a poskytovateľmi spravodajských informácií o hrozbách, ktorí nespĺňajú jednu alebo viacero požiadaviek stanovených v odseku 1 písm. a) až f), za predpokladu, že tieto finančné subjekty prijímajú opatrenia vhodné na zmierňovanie rizík súvisiacich s nedodržiavaním takýchto bodov a tieto opatrenia zaznamenávajú.

*Článok 8*

**Osobitosti pre združené alebo spoločné TLPT**

1. Pokiaľ vedúci orgán TLPT nerozhodne inak, ak je do združeného alebo spoločného TLPT zapojených viacero finančných subjektov identifikovaných v súlade s článkom 16 ods. 2 alebo 4, každý finančný subjekt dodržiava každý z krokov stanovených v článkoch 9 až 15.

2. Pokiaľ nie je v tomto nariadení stanovené inak, ak je do spoločného TLPT alebo do združeného TLPT zapojených viacero orgánov TLPT, ako sa uvádza v článku 16 ods. 3 alebo ods. 5, odkazy v článkoch 9 až 15 na „orgán TLPT“ sa pokladajú za odkazy na hlavný orgán TLPT pre takýto združený alebo spoločný TLPT.

*Článok 9*

**Prípravná fáza**

1. Finančný subjekt identifikovaný podľa článku 26 ods. 8 tretieho pododseku nariadenia (EÚ) 2022/2554 spúšťa TLPT na základe oznámenia orgánu TLPT, že sa má vykonať TLPT.

2. Finančný subjekt do troch mesiacov od prijatia oznámenia uvedeného v odseku 1 predloží testovacím manažérom všetky tieto informácie o spustení TLPT:

a) projektový zámer vrátane projektového plánu na vysokej úrovni, ktorý obsahuje informácie uvedené v prílohe I;

b) kontaktné údaje vedúceho kontrolného tímu;

c) informácie o zamýšľanom využití interných alebo externých testovacích subjektov alebo prípadne oboch, ako sa podrobne uvádza v článku 15;

d) informácie o komunikačných kanáloch, ktoré sa majú použiť počas TLPT;

e) kódové označenie TLPT.

3. Ak sú informácie uvedené v odseku 2 písm. a) až e) úplné a zabezpečuje sa nimi vhodnosť a účinné vykonanie TLPT, orgán TLPT validuje informácie finančného subjektu týkajúce sa spustenia TLPT a oznámi to finančnému subjektu.

4. Finančný subjekt po potvrdení informácií o spustení TLPT orgánom TLPT zriadi kontrolný tím na podporu vedúceho kontrolného tímu pri plnení jeho úloh, a to konkrétne pri:

a) špecifikovaní komunikačných kanálov a procesov v kontrolnom tíme s testovacími subjektmi a poskytovateľmi spravodajských informácií o hrozbách vo všetkých záležitostiach týkajúcich sa TLPT;

b) informovaní riadiaceho orgánu finančného subjektu o pokroku TLPT a o súvisiacich rizikách;

c) prijímaní rozhodnutí na základe odborných znalostí v danej oblasti počas celého TLPT;

d) vykonávaní TLPT v súlade s týmto nariadením;

e) výbere poskytovateľa spravodajských informácií o hrozbách pre TLPT;

f) výbere externých testovacích subjektov, interných testovacích subjektov alebo oboch;

g) príprave dokumentu so špecifikáciou rozsahu.

5. Ak sa orgán TLPT domnieva, že počiatočné zloženie kontrolného tímu a všetky jeho následné zmeny sú primerané plneniu úloh uvedených v odseku 4, orgán TLPT potvrdí kontrolný tím a oznámi to vedúcemu kontrolného tímu.

6. Finančný subjekt predkladá testovacím manažérom dokument so špecifikáciou rozsahu obsahujúci všetky informácie uvedené v prílohe II do šiestich mesiacov od prijatia oznámenia od orgánu TLPT uvedeného v odseku 1. Riadiaci orgán finančného subjektu schvaľuje dokument so špecifikáciou rozsahu.

7. Finančné subjekty pri začleňovaní kritických alebo dôležitých funkcií do rozsahu pôsobnosti TLPT zohľadňujú tieto kritériá:

a) kritickosť alebo význam funkcie a jej možný vplyv na finančný sektor a na finančnú stabilitu na úrovni Únie a na vnútroštátnej úrovni;

b) význam funkcie pre každodenné obchodné operácie finančného subjektu;

c) zameniteľnosť funkcie;

d) prepojenosť s inými funkciami;

e) geografická poloha funkcie;

f) závislosť iných subjektov v sektore od funkcie;

g) spravodajské informácie o hrozbách týkajúce sa funkcie, ak sú k dispozícii.

8. Kontrolný tím poskytne informácie o spustení TLPT a dokument so špecifikáciou rozsahu testovacím subjektom a poskytovateľom spravodajských informácií o hrozbách hneď, ako sa s nimi uzatvoria zmluvy. Kontrolný tím informuje testovacie subjekty a poskytovateľov spravodajských informácií o hrozbách o testovacom procese, ktorým sa majú riadiť.

9. Finančný subjekt zabezpečuje, aby sa obstarávanie alebo priraďovanie testovacích subjektov a poskytovateľov spravodajských informácií o hrozbách dokončilo pred spustením testovacej fázy.

10. Pred spustením testovacej fázy kontrolný tím konzultuje s testovacími manažérmi posúdenie rizika TLPT a opatrenia na riadenie rizík. Kontrolný tím preskúmava posúdenie rizika alebo opatrenia na riadenie rizík, ak orgán TLPT zastáva názor, že sa nimi primerane nerieši riziká súvisiace s TLPT.

11. Kontrolný tím posudzuje plnenie požiadaviek stanovených v článku 27 nariadenia (EÚ) 2022/2554 a článku 7 ods. 1 tohto nariadenia poskytovateľmi spravodajských informácií o hrozbách a testovacími subjektmi, ktorých zapojenie do TLPT zvažuje, a dokumentuje výsledok tohto posúdenia. Kontrolný tím vyberá poskytovateľov spravodajských informácií o hrozbách v súlade s týmto posúdením a so svojimi postupmi riadenia rizík. Pred uzavretím zmluvy s vybranými poskytovateľmi spravodajských informácií o hrozbách a externými testovacími subjektmi poskytuje kontrolný tím testovacím manažérom dôkazy o plnení požiadaviek stanovených v článku 27 nariadenia (EÚ) 2022/2554 a článku 7 ods. 1 tohto nariadenia týmito poskytovateľmi spravodajských informácií o hrozbách a testovacími subjektmi. Kontrolný tím nesmie pokračovať v uzatváraní zmlúv s vybranými poskytovateľmi spravodajských informácií o hrozbách a externými testovacími subjektmi, ak orgán TLPT zastáva názor, že vybraní poskytovatelia spravodajských informácií o hrozbách a externé testovacie subjekty nespĺňajú požiadavky stanovené v článku 27 nariadenia (EÚ) 2022/2554 alebo požiadavky stanovené v článku 7 ods. 1 tohto nariadenia alebo dodatočné požiadavky vyplývajúce z vnútroštátnych právnych predpisov v oblasti bezpečnosti v súlade s právom Únie, alebo ak finančný subjekt nedodržiava článok 7 ods. 2 prvý pododsek tohto nariadenia, alebo ak nie sú splnené okolnosti uvedené v článku 7 ods. 2 druhom pododseku tohto nariadenia.

12. Ak je dokument so špecifikáciou rozsahu úplný a zabezpečuje sa ním vykonanie vhodného a účinného TLPT, orgán TLPT tento dokument schváli a oznámi to vedúcemu kontrolného tímu.

*Článok 10*

**Testovacia fáza: spravodajské informácie o hrozbách**

1. Poskytovateľ spravodajských informácií o hrozbách po schválení dokumentu so špecifikáciou rozsahu orgánom TLPT analyzuje všeobecné a sektorové spravodajské informácie o hrozbách relevantné pre finančný subjekt. Ak orgán TLPT poskytol všeobecnú panorámu hrozieb pre finančný sektor členského štátu, poskytovateľ spravodajských informácií o hrozbách môže túto panorámu použiť ako základ pre vnútroštátnu panorámu hrozieb. Poskytovateľ spravodajských informácií o hrozbách identifikuje kybernetické hrozby a existujúce alebo potenciálne zraniteľné miesta týkajúce sa finančného subjektu. Poskytovateľ spravodajských informácií o hrozbách okrem toho zhromažďuje informácie o konkrétnych, realizovateľných a situačných spravodajských informáciách o cieľoch a hrozbách týkajúcich sa finančného subjektu a analyzuje ich, a to aj prostredníctvom konzultácií s kontrolným tímom a testovacími manažérmi.

2. Poskytovateľ spravodajských informácií o hrozbách predkladá relevantné hrozby a cielené spravodajské informácie o hrozbách a navrhuje potrebné scenáre kontrolnému tímu, testovacím subjektom a testovacím manažérom. Navrhované scenáre sa líšia v závislosti od identifikovaných aktérov hrozieb a súvisiacich taktík, techník a postupov a sú cielené na každú kritickú alebo dôležitú funkciu v rozsahu pôsobnosti TLPT.

3. Vedúci kontrolnej skupiny vyberá aspoň tri scenáre na vykonanie TLPT na základe všetkých týchto prvkov:

a) odporúčania poskytovateľa spravodajských informácií o hrozbách a povahy každého scenára na základe konkrétnej hrozby;

b) vstupov poskytnutých testovacími manažérmi;

c) uskutočniteľnosti navrhovaných scenárov na vykonanie na základe odborného úsudku testovacích subjektov;

d) veľkosti, zložitosti a celkového rizikového profilu finančného subjektu a povahy, rozsahu a zložitosti jeho služieb, činností a operácií.

4. Najviac jeden z vybraných scenárov môže byť bez konkrétnej hrozby a môže byť založený na výhľadovej a potenciálne fiktívnej hrozbe s vysokou prediktívnou, anticipatívnou, oportunistickou alebo prospektívnou hodnotou vzhľadom na očakávaný vývoj panorámy hrozieb týkajúci sa finančného subjektu.

V prípade združených TLPT bez toho, aby boli dotknuté scenáre zacielené priamo na kritické alebo dôležité funkcie finančných subjektov zapojených do testovania, musí aspoň jeden scenár zahŕňať relevantné podkladové IKT systémy, procesy a technológie externého poskytovateľa IKT služieb podporujúce kritické alebo dôležité funkcie finančných subjektov v rozsahu pôsobnosti.

Ak ide o spoločné TLPT, do ktorého je zapojený vnútroskupinový poskytovateľ IKT služieb, bez toho, aby boli dotknuté scenáre zacielené priamo na kritické alebo dôležité funkcie finančných subjektov zapojených do testu, aspoň jeden scenár musí zahŕňať relevantné podkladové IKT systémy, procesy a technológie vnútroskupinového poskytovateľa IKT služieb podporujúce kritické alebo dôležité funkcie finančných subjektov v rozsahu pôsobnosti.

5. Poskytovateľ spravodajských informácií o hrozbách poskytuje kontrolnému tímu cielenú správu o spravodajských informáciách o hrozbách vrátane scenárov vybraných v súlade s odsekmi 3 a 4. Správa o spravodajských informáciách o hrozbách obsahuje informácie uvedené v prílohe III.

6. Kontrolný tím predkladá cielenú správu o spravodajských informáciách o hrozbách testovaciemu manažérovi na schválenie. Ak je cielená správa o spravodajských informáciách o hrozbách úplná a zabezpečuje sa ňou vykonanie účinného TLPT, orgán TLPT cielenú správu o spravodajských informáciách o hrozbách schváli a oznámi to vedúcemu kontrolného tímu.

*Článok 11*

**Testovacia fáza: test červeného tímu**

1. Testovacie subjekty po schválení cielenej správy o spravodajských informáciách o hrozbách orgánom TLPT vypracujú plán testu červeného tímu, ktorý obsahuje informácie stanovené v prílohe IV. Ako základ pre vypracovanie scenárov útoku používajú testovacie subjekty dokument so špecifikáciou rozsahu a cielenú správu o spravodajských informáciách o hrozbách.

2. Testovacie subjekty konzultujú s kontrolným tímom, poskytovateľom spravodajských informácií o hrozbách a testovacími manažérmi plán testu červeného tímu vrátane komunikácie, procedurálnych opatrení a opatrení projektového riadenia, prípravy a prípadov použitia aktivácie opôr a dohôd o podávaní správ kontrolnému tímu a testovacím manažérom.

3. Ak je plán testu červeného tímu úplný a zabezpečuje sa ním vykonanie účinného TLPT, kontrolný tím a orgán TLPT schvália plán testu červeného tímu a TLPT to oznámi vedúcemu kontrolného tímu.

4. Po schválení plánu testu červeného tímu v súlade s odsekom 3 testovacie subjekty vykonajú TLPT počas fázy aktívneho testovania prostredníctvom červeného tímu.

5. Trvanie fázy aktívneho testovania prostredníctvom červeného tímu musí byť primerané rozsahu pôsobnosti TLPT, rozsahu, činnosti, zložitosti a počtu finančných subjektov a externých poskytovateľov IKT služieb alebo vnútroskupinových poskytovateľov IKT služieb zapojených do TLPT a v každom prípade trvá aspoň 12 týždňov. Scenáre útoku sa môžu uskutočňovať postupne alebo súčasne. Kontrolný tím, poskytovateľ spravodajských informácií o hrozbách, testovacie subjekty a testovacie manažéri sa zhodnú na ukončení fázy aktívneho testovania prostredníctvom červeného tímu.

6. Pod podmienkou, že plán testu červeného tímu zostane úplný a umožní sa ním vykonanie účinného TLPT, vedúci kontrolného tímu a testovací manažéri schvália všetky zmeny plánu testu červeného tímu po jeho schválení vrátane harmonogramu, rozsahu pôsobnosti, cieľových systémov alebo vlajok.

7. Počas celej fázy aktívneho testovania prostredníctvom červeného tímu testovacie subjekty podávajú aspoň raz týždenne kontrolnému tímu a testovacím manažérom správu o pokroku dosiahnutom v rámci TLPT a poskytovateľ spravodajských informácií o hrozbách musí na požiadanie kontrolného tímu zostať k dispozícii na konzultácie a poskytnutie dodatočných spravodajských informácií o hrozbách.

8. Kontrolný tím včas poskytuje opory navrhnuté na základe plánu testu červeného tímu. Opory sa môžu pridávať alebo upravovať po schválení kontrolným tímom a testovacími manažérmi.

9. V prípade odhalenia testovacích činností ktorýmkoľvek zamestnancom finančného subjektu alebo jeho externých poskytovateľov IKT služieb, prípadne vnútroskupinového poskytovateľa IKT služieb, kontrolný tím po konzultácii s testovacími subjektmi a bez toho, aby bol dotknutý odsek 10, navrhne a predloží testovacím manažérom na validáciu opatrenia, ktoré umožnia pokračovať v TLPT, pričom zabezpečuje jeho utajenie.

10. Za výnimočných okolností, ktoré vyvolávajú riziká vplyvu na údaje, škody na aktívach a narušenia kritických alebo dôležitých funkcií, služieb alebo operácií samotného finančného subjektu, jeho externých poskytovateľov IKT služieb alebo vnútroskupinových poskytovateľov IKT služieb, alebo narušenia jeho protistrán alebo finančného sektora, môže vedúci kontrolného tímu pozastaviť TLPT, alebo v krajnom prípade, ak pokračovanie TLPT nie je inak možné a pod podmienkou predchádzajúceho potvrdenia orgánom TLPT, pokračovať v TLPT a použiť pritom obmedzené fialové tímové cvičenie. Trvanie obmedzeného fialového tímového cvičenia sa počíta na účely minimálneho 12-týždňového trvania fázy aktívneho testovania prostredníctvom červeného tímu uvedenej v odseku 5.

*Článok 12*

**Záverečná fáza**

1. Vedúci kontrolného tímu po skončení fázy aktívneho testovania prostredníctvom červeného tímu informuje modrý tím o tom, že sa uskutočnilo TLPT.

2. Do štyroch týždňov od ukončenia fázy aktívneho testovania prostredníctvom červeného tímu predložia testovacie subjekty kontrolnému tímu správu o teste červeného tímu obsahujúcu informácie uvedené v prílohe V.

3. Kontrolný tím bez zbytočného odkladu poskytne modrému tímu a testovacím manažérom správu o teste červeného tímu.

Na žiadosť testovacích manažérov nesmie správa uvedená v prvom pododseku obsahovať citlivé informácie.

4. Pro prijatí správy o teste červeného tímu a najneskôr do desiatich týždňov po ukončení fázy aktívneho testovania prostredníctvom červeného tímu predloží modrý tím kontrolnému tímu správu o teste modrého tímu obsahujúcu informácie uvedené v prílohe VI. Kontrolný tím bez zbytočného odkladu poskytne testovacím subjektom a testovacím manažérom správu o teste modrého tímu.

Na žiadosť testovacích manažérov nesmie správa uvedená v prvom pododseku obsahovať citlivé informácie.

5. Najneskôr desať týždňov po ukončení fázy aktívneho testovania prostredníctvom červeného tímu si modrý tím a testovacie subjekty prehrajú ofenzívne a obranné činnosti vykonané počas TLPT. Kontrolný tím vykonáva aj fialové tímové cvičenie týkajúce sa tém, ktoré identifikoval modrý tím spolu s testovacími subjektmi, a to na základe zraniteľných miest identifikovaných počas testu, a v relevantných prípadoch týkajúce sa problémov, ktoré nebolo možné otestovať počas fázy aktívneho testovania prostredníctvom červeného tímu.

6. Po skončení prehrávania a fialových tímových cvičení si kontrolný tím, modrý tím, testovacie subjekty a poskytovatelia spravodajských informácií o hrozbách navzájom poskytujú spätnú väzbu o procese TLPT. Testovací manažéri smú poskytovať spätnú väzbu.

7. Po tom, ako orgán TLPT oznámi kontrolnému tímu, že dospel k záveru, že správa o teste modrého tímu a správa o teste červeného tímu obsahujú informácie uvedené v prílohách V a VI, finančný subjekt do ôsmich týždňov predloží orgánu TLPT na schválenie správu obsahujúcu prvky uvedené v prílohe VII, pričom v správe zhrnie príslušné zistenia týkajúce sa TLPT, ako sa uvádza v článku 26 ods. 6 nariadenia (EÚ) 2022/2554.

Na žiadosť orgánu TLPT nesmie správa uvedená v prvom pododseku obsahovať citlivé informácie.

*Článok 13*

**Plán nápravy**

1. Finančný subjekt do ôsmich týždňov od oznámenia uvedeného v článku 12 ods. 7 tohto nariadenia poskytne plány nápravy a dokumentáciu uvedené v článku 26 ods. 6 nariadenia (EÚ) 2022/2554 orgánu TLPT a, ak je odlišný, príslušnému orgánu finančného subjektu.

2. Plán nápravy uvedený v odseku 1 obsahuje ku každému zisteniu, ku ktorému došlo v rámci TLPT:

a) opis identifikovaných nedostatkov;

b) opis navrhovaných nápravných opatrení a ich prioritizáciu a očakávané dokončenie vrátane prípadných opatrení na zlepšenie spôsobilostí v oblasti identifikácie, ochrany, odhaľovania a reakcie;

c) analýzu základnej príčiny;

d) zoznam zamestnancov alebo funkcií finančného subjektu zodpovedných za vykonávanie navrhovaných nápravných opatrení alebo zlepšení;

e) riziká spojené s nevykonávaním opatrení uvedených v písmene b) a v relevantných prípadoch riziká spojené s vykonávaním takýchto opatrení.

*Článok 14*

**Osvedčenie**

1. Osvedčenie uvedené v článku 26 ods. 7 nariadenia (EÚ) 2022/2554 musí obsahovať informácie stanovené v prílohe VIII.

2. Ak bolo do TLPT zapojených viacero orgánov TLPT, vedúci orgán TLPT poskytne testovaným finančným subjektom osvedčenie uvedené v článku 26 ods. 7 nariadenia (EÚ) 2022/2554.

*Článok 15*

**Využívanie interných testovacích subjektov**

1. Finančné subjekty musia zaviesť všetky nasledujúce opatrenia na využívanie interných testovacích subjektov:

a) zavedenie a vykonávanie politiky riadenia interných testovacích subjektov v rámci TLPT;

b) opatrenia na zabezpečenie toho, aby využívanie interných testovacích subjektov na vykonávanie TLPT nemalo negatívny vplyv na všeobecné spôsobilosti finančného subjektu v oblasti obrany alebo odolnosti, pokiaľ ide o incidenty súvisiace s IKT, ani aby výrazne neovplyvnilo dostupnosť zdrojov vyčlenených na úlohy súvisiace s IKT počas TLPT;

c) opatrenia na zabezpečenie toho, aby interné testovacie subjekty mali dostatočné zdroje a spôsobilosti na vykonanie TLPT.

Politika uvedená v písmene a) musí:

a) obsahovať kritériá na posúdenie vhodnosti, kompetencií, potenciálnych konfliktov záujmov interných testovacích subjektov a špecifikovať povinnosti manažmentu v procese testovania;

b) byť zdokumentovaná a pravidelne preskúmavaná;

c) zabezpečiť, aby interný testovací tím zahŕňal vedúceho testu a aspoň dvoch ďalších členov;

d) požadovať, aby všetci členovia testovacieho tímu boli zamestnaní finančným subjektom alebo vnútroskupinovým poskytovateľom IKT služieb počas predchádzajúcich 12 mesiacov;

e) zahŕňať ustanovenia o odbornej príprave interných testovacích subjektov k tomu, ako vykonávať penetračné testovanie a testovanie prostredníctvom červeného tímu.

2. Ak orgán TLPT schváli využívanie interných testovacích subjektov v súlade s článkom 27 ods. 2 písm. a) nariadenia (EÚ) 2022/2554, orgán TLPT berie do úvahy požiadavky stanovené v článku 7 ods. 1 tohto nariadenia.

3. Pri využívaní interných testovacích subjektov finančný subjekt zabezpečuje, aby sa takéto využitie uviedlo v týchto dokumentoch:

a) informáciách o spustení testu uvedených v článku 9;

b) správe o teste červeného tímu uvedenej v článku 12 ods. 2;

c) správe, v ktorej sú zhrnuté príslušné zistenia TLPT, uvedenej v článku 26 ods. 6 nariadenia (EÚ) 2022/2554.

4. Testovacie subjekty zamestnané vnútroskupinovým poskytovateľom IKT služieb sa považujú za interné testovacie subjekty finančného subjektu.

*Článok 16*

**Spolupráca a vzájomné uznávanie**

1. Na účely vykonávania TLPT vo vzťahu k finančnému subjektu poskytujúcemu služby vo viac než jednom členskom štáte, a to aj prostredníctvom pobočky, jeho orgán TLPT:

a) určuje, ktoré orgány TLPT v hostiteľských členských štátoch budú zapojené, pričom zohľadňuje, či sa v hostiteľských členských štátoch vykonáva jedna alebo viacero kritických alebo dôležitých funkcií alebo či sa medzi týmito členskými štátmi takéto funkcie zdieľajú;

b) oznamuje orgánom TLPT určeným v súlade s písmenom a) rozhodnutie vykonať test TLPT na finančnom subjekte;

c) pokiaľ sa orgány TLPT nedohodnú inak, orgán TLPT finančného subjektu vedie TLPT.

Orgány TLPT hostiteľských členských štátov môžu do 20 pracovných dní od prijatia informácií o budúcom uskutočnení TLPT buď vyjadriť svoj záujem o sledovanie TLPT ako pozorovatelia, alebo poveriť testovacieho manažéra, aby sa zúčastnil na TLPT. Vedúci orgán TLPT poskytuje všetkým orgánom TLPT v roli pozorovateľov v TLPT dokument so špecifikáciou rozsahu, súhrnnú správu o teste, plán nápravy a osvedčenie.

Vedúci orgán TLPT koordinuje všetky zúčastnené orgány TLPT počas celého testu a prijíma všetky rozhodnutia potrebné na riadne a účinné vykonanie TLPT. Vedúci orgán TLPT môže stanoviť maximálny počet zúčastnených orgánov TLPT, ak by inak mohlo byť ohrozené efektívne vykonanie TLPT.

2. Ak finančný subjekt používa rovnakého vnútroskupinového poskytovateľa IKT služieb ako finančné subjekty usadené v iných členských štátoch alebo ak patrí do skupiny a zdieľa IKT systémy s finančnými subjektmi tej istej skupiny usadenými v iných členských štátoch, orgán TLPT finančného subjektu kontaktuje orgány TLPT týchto iných finančných subjektov využívajúcich rovnakého vnútroskupinového poskytovateľa IKT služieb alebo zdieľajúcich IKT systémy ako súčasť skupiny, a v súvislosti s nimi posúdi uskutočniteľnosť a vhodnosť vykonania spoločného TLPT. Spoločný TLPT sa uprednostňuje pred individuálnym TLPT, ak môže viesť k zníženiu nákladov a zdrojov finančných subjektov a orgánov TLPT, za predpokladu, že tým nie je ohrozená spoľahlivosť a účinnosť testovania.

3. Na účely vykonania spoločného TLPT:

a) sa orgány TLPT finančných subjektov dohodnú na tom, ktorý finančný subjekt bude určený na vykonanie TLPT, pričom zohľadňujú štruktúru skupiny a efektívnosť testu;

b) orgán TLPT finančného subjektu určeného v súlade s písmenom a) vedie TLPT, pokiaľ sa orgány TLPT finančných subjektov zúčastňujúcich sa na spoločnom TLPT nedohodnú inak;

c) orgány TLPT iných finančných subjektov, než je určený finančný subjekt, ktorý má viesť spoločný TLPT, môžu buď vyjadriť svoj záujem o sledovanie TLPT ako pozorovatelia, alebo prideliť pre daný TLPT testovacieho manažéra.

Vedúci orgán TLPT koordinuje všetky orgány TLPT zapojené do spoločného TLPT a prijíma všetky rozhodnutia potrebné na riadne a účinné vykonanie spoločného TLPT.

4. Ak má finančný subjekt v úmysle vykonať združený TLPT, ako sa uvádza v článku 26 ods. 4 nariadenia (EÚ) 2022/2554, s možnosťou zapojenia finančných subjektov usadených v iných členských štátoch, jeho orgán TLPT kontaktuje orgány TLPT iných finančných subjektov a posúdi s nimi uskutočniteľnosť a vhodnosť vykonania združeného TLPT v súvislosti nimi v súlade s článkom 26 ods. 4 nariadenia (EÚ) 2022/2554.

5. Na účely vykonania združeného TLPT, ako sa uvádza v článku 26 ods. 4 nariadenia (EÚ) 2022/2554:

a) orgány TLPT finančných subjektov sa dohodnú na tom, ktorý finančný subjekt bude určený na vykonanie združeného TLPT, pričom zohľadňujú IKT služby, ktoré externý poskytovateľ IKT služieb poskytuje finančným subjektom a efektívnosť testu;

b) orgán TLPT finančného subjektu určeného v súlade s písmenom a) vedie TLPT, pokiaľ sa orgány TLPT finančných subjektov zúčastňujúcich sa na združenom TLPT nedohodnú inak;

c) orgány TLPT iných finančných subjektov, než je určený finančný subjekt, ktorý má viesť združený TLPT, môžu buď vyjadriť svoj záujem o sledovanie TLPT ako pozorovatelia, alebo prideliť na daný TLPT testovacieho manažéra.

Vedúci orgán TLPT koordinuje všetky orgány TLPT zapojené do združeného TLPT a prijíma všetky rozhodnutia potrebné na riadne a účinné vykonanie združeného TLPT.

6. Ak sa vo vzťahu k finančnému subjektu povinného vykonať TLPT jeho orgán TLPT líši od jeho príslušného orgánu uvedeného v článku 46 nariadenia (EÚ) 2022/2554, tieto orgány si vymieňajú všetky relevantné informácie týkajúce sa všetkých záležitostí súvisiacich s TLPT na účely vykonania TLPT alebo plnenia svojich povinností v súlade s uvedeným nariadením.

*Článok 17*

**Nadobudnutie účinnosti**

Toto nariadenie nadobúda účinnosť dvadsiatym dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 13. februára 2025

*Za Komisiu*
*predsedníčka*
Ursula VON DER LEYEN

*PRÍLOHA I*

**Obsah projektového zámeru [článok 9 ods. 2 písm. a)]**

| Informačná položka | Požadované informácie |
|---|---|
| Osoba zodpovedná za projektový plán, t. j. vedúci kontrolného tímu | meno<br>kontaktné údaje |
| Testovacie subjekty | ☐ interné<br>☐ externé<br>☐ oboje |
| Komunikačné kanály vybrané v súlade s článkom 9 ods. 2 písm. d) a článkom 9 ods. 4 písm. a) vrátane:<br>a) šifrovania e-mailov, ktoré sa má použiť;<br>b) online dátových priestorov, ktoré sa majú použiť;<br>c) rýchlych správ, ktoré sa majú použiť | |
| Kódové označenie TLPT | |
| Prípadné kritické alebo dôležité funkcie, ktoré finančný subjekt vykonáva v iných členských štátoch | 1. zoznam kritických alebo dôležitých funkcií vykonávaných v inom členskom štáte<br>2. pre každú kritickú alebo dôležitú funkciu uvedenie členského štátu alebo štátov, v ktorých sa vykonávajú |
| Prípadné kritické alebo dôležité funkcie podporované externými poskytovateľmi IKT služieb | 3. zoznam kritických alebo dôležitých funkcií podporovaných externými poskytovateľmi IKT služieb<br>4. identifikácia externého poskytovateľa IKT služieb pre každú funkciu |
| *Očakávané lehoty na dokončenie:* | |
| 1. prípravnej fázy v súlade s článkom 9 | rrrr-mm-dd |
| 2. testovacej fázy v súlade s článkami 10 a 11 | rrrr-mm-dd |
| 3. záverečnej fázy v súlade s článkom 12 | rrrr-mm-dd |
| 4. plánu nápravy v súlade s článkom 13 | rrrr-mm-dd |

*PRÍLOHA II*

**Obsah dokumentu so špecifikáciou rozsahu (článok 9 ods. 6)**

1. Dokument so špecifikáciou rozsahu musí obsahovať zoznam všetkých kritických alebo dôležitých funkcií identifikovaných finančným subjektom.

2. Pre každú identifikovanú kritickú alebo dôležitú funkciu sa uvádzajú tieto informácie:
   a) ak kritická alebo dôležitá funkcia nie je zahrnutá do rozsahu pôsobnosti TLPT, vysvetlenie dôvodov, pre ktoré nie je zahrnutá;
   b) ak je kritická alebo dôležitá funkcia zahrnutá do rozsahu pôsobnosti TLPT:
      i) vysvetlenie dôvodov jej zahrnutia;
      ii) identifikovaný IKT systém alebo identifikované IKT systémy podporujúce túto kritickú alebo dôležitú funkciu;
      iii) pre každý identifikovaný IKT systém:
         1. či je externe zabezpečovaný, a ak áno, názov externého poskytovateľa IKT služieb;
         2. jurisdikcie, v ktorých sa IKT systém používa;
         3. všeobecný opis predbežnej vlajky alebo predbežných vlajok s uvedením, na ktorý bezpečnostný aspekt dôvernosti, integrity, pravosti alebo dostupnosti sa každá vlajka vzťahuje.

*PRÍLOHA III*

**Obsah cielenej správy o spravodajských informáciách o hrozbách (článok 10 ods. 5)**

Cielená správa o spravodajských informáciách o hrozbách musí obsahovať informácie o všetkých týchto aspektoch:

1. Celkový rozsah výskumu spravodajských informácií, ktorý zahŕňa aspoň:
   a) kritické alebo dôležité funkcie v rozsahu pôsobnosti;
   b) ich geografickú polohu;
   c) používaný úradný jazyk EÚ;
   d) príslušných externých poskytovateľov IKT služieb;
   e) časové obdobie, počas ktorého sa výskum uskutočňuje.
2. Celkové posúdenie toho, aké konkrétne využiteľné spravodajské informácie možno nájsť o finančnom subjekte, vrátane:
   a) používateľských mien a hesiel zamestnancov;
   b) podobných domén, ktoré sa môžu omylom pokladať za oficiálne domény finančného subjektu;
   c) technického prieskumu: zraniteľného alebo napadnuteľného softvéru, systémov a technológií;
   d) informácií zverejnených zamestnancami na internete týkajúcich sa finančného subjektu, ktoré by sa mohli použiť na účely útoku;
   e) informácií na predaj na dark webe;
   f) akýchkoľvek iných relevantných informácií dostupných na internete alebo verejných sieťach;
   g) v relevantných prípadoch informácií o fyzickom cielení vrátane spôsobov prístupu do priestorov finančného subjektu.
3. Analýza spravodajských informácií o hrozbách so zreteľom na všeobecnú panorámu hrozieb a konkrétnu situáciu finančného subjektu vrátane aspoň:
   a) geopolitického prostredia;
   b) hospodárskeho prostredia;
   c) technologických trendov a akýchkoľvek iných trendov súvisiacich s činnosťami v sektore finančných služieb.
4. Profily hrozieb aktérov s nekalými úmyslami (konkrétna osoba/skupina alebo všeobecná trieda), ktorí sa môžu zamerať na finančný subjekt, vrátane systémov finančného subjektu, pri ktorých je najpravdepodobnejšie, že ich aktéri s nekalými úmyslami ohrozia alebo zacielia, možnej motivácie, zámeru a odôvodnenia potenciálneho cielenia a možného spôsobu práce útočníkov.
5. Scenáre hrozieb: najmenej tri scenáre hrozieb medzi koncovými bodmi pre profily hrozieb identifikované v súlade s bodom 4, ktoré vykazujú najvyššie skóre závažnosti hrozby. Scenáre hrozieb opisujú dráhu útoku medzi koncovými bodmi a zahŕňajú aspoň:
   a) jeden scenár, ktorý zahŕňa okrem iného napadnutú dostupnosť služieb;
   b) jeden scenár, ktorý zahŕňa okrem iného napadnutú integritu údajov;
   c) jeden scenár, ktorý zahŕňa okrem iného napadnutú dôvernosť informácií.
6. V relevantných prípadoch opis scenára bez konkrétnej hrozby uvedeného v článku 10 ods. 4.

*PRÍLOHA IV*

**Obsah plánu testu červeného tímu (článok 11 ods. 1)**

Plán testu červeného tímu musí obsahovať informácie o všetkých týchto aspektoch:

a) komunikačné kanály a postupy;

b) taktiky, techniky a postupy, ktoré je povolené a nepovolené použiť pri útoku, vrátane etických hraníc pri sociálnom inžinierstve;

c) opatrenia na riadenie rizík, ktorými sa majú riadiť testovacie subjekty;

d) opis každého scenára vrátane:

   i) simulovaného aktéra hrozby;

   ii) ich zámeru, motivácie a cieľov;

   iii) cieľovej funkcie alebo cieľových funkcií a podporného IKT systému alebo systémov;

   iv) cielených aspektov dôvernosti, integrity, dostupnosti a pravosti;

   v) vlajok;

e) podrobný opis každej očakávanej dráhy útoku vrátane predpokladov a možných opôr, ktoré má poskytnúť kontrolný tím, vrátane lehôt na ich poskytnutie a potenciálne používanie;

f) plánovanie činností červeného tímu vrátane časového plánovania pre vykonanie každého scenára s minimálnym rozdelením na tri fázy, ktoré testujúci subjekt vykonáva počas testovacej fázy, resp. vstupovanie do IKT systémov finančných subjektov, prechod cez IKT systémy a v konečnom dôsledku vykonávanie akcií týkajúcich sa cieľov a napokon stiahnutie sa z IKT systémov (fázy dnu, cez a von);

g) osobitosti infraštruktúry finančných subjektov, ktoré sa majú zohľadniť počas testovania;

h) prípadné dodatočné informácie alebo iné zdroje potrebné pre testovacie subjekty na realizáciu scenárov.

*PRÍLOHA V*

**Obsah správy o teste červeného tímu (článok 12 ods. 2)**

Správa o teste červeného tímu musí obsahovať informácie aspoň o všetkých týchto aspektoch:

a) informácie o uskutočnenom útoku vrátane:

   i) cielených kritických alebo dôležitých funkcií a identifikovaných IKT systémov, procesov a technológií podporujúcich kritickú alebo dôležitú funkciu, ako sa uvádza v pláne testov červeného tímu;

   ii) zhrnutia každého scenára;

   iii) dosiahnutých a nedosiahnutých vlajok;

   iv) úspešných aj neúspešných dráh útoku;

   v) úspešných aj neúspešných taktík, techník a postupov;

   vi) prípadných odchýlok od plánu testu červeného tímu;

   vii) prípadných poskytnutých opôr;

b) všetky opatrenia, pri ktorých je testovacím subjektom známe, že ich vykonal modrý tím na rekonštrukciu útoku a zmiernenie jeho účinkov;

c) zistené zraniteľné miesta a iné zistenia vrátane:

   i) opisu zraniteľných miest a iných zistení vrátane ich kritickosti;

   ii) analýzy základných príčin úspešných útokov;

   iii) odporúčaní na nápravu vrátane uvedenia priority nápravy.

*PRÍLOHA VI*

**Obsah správy o teste modrého tímu (článok 12 ods. 4)**

Správa o teste modrého tímu musí obsahovať informácie aspoň o všetkých týchto aspektoch:

1. pre každý krok útoku opísaný testovacími subjektmi v správe o teste červeného tímu:
   a) zoznam odhalených útočných akcií;
   b) zápisy logov zodpovedajúce týmto odhaleniam;
2. posúdenie zistení a odporúčaní testovacích subjektov;
3. dôkazy o útoku testovacích subjektov, ktoré zhromaždil modrý tím;
4. analýza základných príčin úspešných útokov testovacích subjektov vypracovaná modrým tímom;
5. zoznam získaných poznatkov a identifikovaný potenciál na zlepšenie;
6. zoznam tém, ktoré sa majú riešiť fialovým tímovým cvičením.

*PRÍLOHA VII*

**Podrobnosti o správe, v ktorej sú zhrnuté príslušné zistenia TLPT podľa článku 26 ods. 6 nariadenia (EÚ) 2022/2554**

Súhrnná správa o teste musí obsahovať informácie aspoň o všetkých týchto aspektoch:

a) zúčastnené strany;

b) projektový plán;

c) potvrdený rozsah pôsobnosti vrátane odôvodnenia začlenenia alebo vylúčenia kritických alebo dôležitých funkcií a identifikovaných IKT systémov, procesov a technológií podporujúcich kritické alebo dôležité funkcie, na ktoré sa vzťahuje TLPT;

d) vybrané scenáre a všetky významné odchýlky od cielenej správy o spravodajských informáciách o hrozbách;

e) vykonané dráhy útoku a použité taktiky, techniky a postupy;

f) ukoristené aj neukoristené vlajky;

g) prípadné odchýlky od plánu testov červeného tímu;

h) prípadné odhalenia modrého tímu;

i) fialové tímové cvičenie v testovacej fáze, ak sa vykonalo, a súvisiace podmienky;

j) prípadné použité opory;

k) prijaté opatrenia na riadenie rizík;

l) identifikované zraniteľné miesta a iné zistenia vrátane ich kritickosti;

m) analýza základných príčin úspešných útokov;

n) všeobecný plán pre nápravu, ktorý prepája zraniteľné miesta a iné zistenia, ich základné príčiny a prioritu nápravy;

o) ponaučenia získané z prijatej spätnej väzby.

*PRÍLOHA VIII*

**Podrobnosti o osvedčení o TLPT uvedenom v článku 26 ods. 7 nariadenia (EÚ) 2022/2554**

Osvedčenie musí obsahovať aspoň všetky tieto informácie:

a) o vykonanom TLPT:

   i) dátum začatia a dátum ukončenia TLPT;

   ii) kritické alebo dôležité funkcie spadajúce do rozsahu pôsobnosti testu;

   iii) v relevantných prípadoch informácie o kritických alebo dôležitých funkciách spadajúcich do rozsahu pôsobnosti testu, v súvislosti s ktorými sa TLPT nevykonalo;

   iv) v relevantných prípadoch iné finančné subjekty, ktoré boli zapojené do TLPT;

   v) v relevantných prípadoch externí poskytovatelia IKT služieb, ktorí sa zúčastnili na TLPT;

   vi) vo vzťahu k testovacím subjektom:

      1. či sa využili interné testovacie subjekty;

      2. či finančný subjekt použil článok 5 ods. 3 druhý pododsek;

   vii) trvanie fázy aktívneho testovania prostredníctvom červeného tímu v kalendárnych dňoch;

b) ak sa do TLPT zapojilo viacero orgánov TLPT, iné orgány TLPT a v akom postavení;

c) zoznam dokumentov preskúmaných orgánom TLPT na účely osvedčenia.