2025/1190

18.6.2025

KOMMISSIONENS DELEGEREDE FORORDNING (EU) 2025/1190

af 13. februar 2025

om supplerende regler til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 for så vidt angår reguleringsmæssige tekniske standarder, der præciserer de kriterier, der anvendes til at identificere finansielle enheder, som skal gennemføre trusselsbaserede penetrationstest, kravene til og standarderne for anvendelsen af interne testere, kravene vedrørende testomfang, -metode og -tilgang for hver testfase samt resultater, afslutnings- og udbedringsfaser og den type tilsyn og andet relevant samarbejde, der er nødvendigt for gennemførelsen af TLPT og for at lette den gensidige anerkendelse

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 ([1]), særlig artikel 26, stk. 11, fjerde afsnit, og

ud fra følgende betragtninger:

(1) Denne forordning er udarbejdet i overensstemmelse med TIBER-EU-rammen og afspejler den metode, proces og struktur, som anvendes ved trusselsbaseret penetrationstest (TLPT), som beskrevet i TIBER-EU. Finansielle enheder, der er omfattet af TLPT, kan henvise til og anvende TIBER-EU-rammen eller en af dens nationale gennemførelser heraf, for så vidt som den pågældende ramme eller gennemførelse er i overensstemmelse med kravene i artikel 26 og 27 i forordning (EU) 2022/2554 og nærværende forordning. Udpegelsen af en fælles offentlig myndighed i den finansielle sektor, som har ansvar for TLPT-relaterede spørgsmål på nationalt plan i overensstemmelse med artikel 26, stk. 9, i forordning (EU) 2022/2554, bør ikke berøre den kompetence, som de kompetente myndigheder har fået overdraget på EU-plan til at føre tilsyn med visse finansielle enheder i overensstemmelse med nævnte forordnings artikel 46, f.eks. Den Europæiske Centralbank for signifikante kreditinstitutter, der skal anses for at være kompetente med hensyn til TLPT-relaterede spørgsmål. Hvis kun nogle af de opgaver, der vedrører TLPT'er, uddelegeres til en anden national myndighed i den finansielle sektor i henhold til artikel 26, stk. 10, i forordning (EU) 2022/2554, bør den kompetente myndighed for den finansielle enhed, der er omhandlet i nævnte forordnings artikel 46, fortsat være myndighed for de TLPT-relaterede opgaver, der ikke er uddelegeret.

(2) I betragtning af TLPT'ens kompleksitet og de risici, der er forbundet hermed, bør anvendelsen heraf begrænses til de finansielle enheder, for hvilke den er berettiget. Myndigheder med ansvar for TLPT-forhold (TLPT-myndigheder, enten på EU-plan eller nationalt plan) bør derfor udelukke de finansielle enheder, der opererer inden for centrale delsektorer for finansielle tjenesteydelser, for hvilke TLPT ikke er berettiget, fra anvendelsesområdet for TLPT. Det betyder, at kreditinstitutter, betalingsinstitutter og e-pengeinstitutter, værdipapircentraler, centrale modparter, markedspladser, forsikrings- og genforsikringsselskaber, selvom de opfylder de kvantitative kriterier, kan fritages for kravet om TLPT på grundlag af en samlet vurdering af deres IKT-risikoprofil og -modenhed, indvirkning på den finansielle sektor og dertil relaterede betænkeligheder vedrørende finansiel stabilitet.

(3) TLPT-myndighederne bør på grundlag af en samlet vurdering af IKT-risikoprofilen og -modenheden, af indvirkningen på den finansielle sektor og af dertil relaterede betænkeligheder vedrørende finansiel stabilitet vurdere, om andre typer finansielle enheder end kreditinstitutter, betalingsinstitutter, e-pengeinstitutter, centrale modparter, værdipapircentraler, markedspladser, forsikrings- og genforsikringsselskaber bør være omfattet af TLPT. Vurderingen af, om sådanne finansielle enheder opfylder disse kvalitative kriterier, bør tage sigte på at identificere finansielle enheder, for hvilke TLPT er hensigtsmæssig, ved hjælp af tværsektorielle og objektive indikatorer. Samtidig bør vurderingen af, om en finansiel enhed opfylder disse kvalitative kriterier, begrænse antallet af enheder, der er omfattet af TLPT, til dem, for

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

hvilke testforløbet er berettiget. Hvorvidt en finansiel enhed opfylder disse kvalitative kriterier, bør også vurderes i lyset af den nye markedsudvikling og nye markedsdeltageres stadig større betydning for den finansielle sektor i fremtiden, herunder udbydere af kryptoaktivtjenester, som er meddelt tilladelse i overensstemmelse med artikel 59 i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 ([2]).

(4) Finansielle enheder kan have samme koncerninterne IKT-tjenesteudbyder eller kan tilhøre samme koncern og forlade sig på brugen af fælles IKT-systemer. I så fald er det vigtigt, at TLPT-myndighederne tager hensyn til den pågældende finansielle enheds struktur og systemiske karakter eller betydning for den finansielle sektor på nationalt plan eller EU-plan, når de vurderer, om en finansiel enhed bør være omfattet af TLPT, og om TLPT'en bør gennemføres på enheds- eller koncernniveau (gennem en fælles TLPT).

(5) For at afspejle TIBER-EU-rammen er det nødvendigt, at testmetoden indeholder bestemmelser om inddragelse af følgende hoveddeltagere: den finansielle enhed — med et kontrolteam (der afspejler TIBER-EU-rammens »control team«) og et blåt team (der afspejler TIBER-EU's »blue team«) — og TLPT-myndigheden i form af et TLPT-cyberteam (der afspejler TIBER-EU-rammens »TIBER-EU-cyberteam«), en formidler af trusselsefterretninger og testere (testerne afspejler TIBER-EU-rammens »red team-provider«).

(6) For at sikre, at de erfaringer, der er indhøstet med gennemførelsen af TIBER-EU-rammen, inddrages i TLPT'en, og for at mindske de risici, der er forbundet med gennemførelsen af TLPT, bør det sikres, at ansvarsområderne for de TLPT-cyberteams, som TLPT- myndighederne skal oprette, i så høj grad som muligt svarer til »TIBER-EU-cyberteams«. TLPT-cyberteams bør derfor have testledere, som har ansvar for at føre tilsyn med individuelle TLPT'er og for at planlægge og koordinere individuelle test. TLPT-cyberteams bør fungere som et centralt kontaktpunkt for testrelateret kommunikation til interne og eksterne interessenter, for indsamling og behandling af feedback og indhøstede erfaringer fra tidligere gennemførte test og for støtte til finansielle enheder, der underlægges en TLPT-forløb.

(7) For at afspejle metoden efter TIBER-EU-rammen bør testledere have de færdigheder og evner, der er nødvendige for at yde rådgivning og bestride testernes forslag. Erfaringerne med TIBER-EU-rammen har vist, at det er værdifuldt at råde over et team bestående af mindst to testledere, som er udpeget til at gennemføre hver enkelt test. For at afspejle det forhold, at TLPT'en anvendes til at tilskynde til læringserfaring og garantere testfortroligheden — og medmindre de har vanskeligheder med ressourcer eller ekspertise — opfordres TLPT-myndighederne kraftigt til at tage hensyn til, at testledere, så længe en TLPT varer, ikke bør udøve tilsynsaktiviteter for samme finansielle enhed, der underlægges en TLPT.

(8) For at sikre overensstemmelse med TIBER-EU-rammen er det vigtigt, at TLPT-myndigheden følger testforløbet nøje i hver enkelt testfase. I betragtning af testforløbets art og de risici, der er forbundet hermed, er det afgørende, at TLPT-myndigheden inddrages i hver specifik testfase. TLPT-myndigheden bør navnlig høres og bør validere de af den finansielle enheders vurderinger eller beslutninger, som på den ene side kan få indflydelse på testens effektivitet og på den anden side har en indvirkning på de risici, der er forbundet med testen. De grundlæggende skridt, der kræver en særlig inddragelse af TLPT-myndigheden, omfatter validering af særlig grundlæggende dokumentation vedrørende testforløbet og udvælgelse af formidlere og testere af trusselsefterretninger samt risikostyringsforanstaltninger. Inddragelsen af TLPT-myndighederne, og navnlig med hensyn til valideringer, bør ikke medføre en uforholdsmæssig stor byrde for disse myndigheder og bør derfor begrænses til den dokumentation og de afgørelser, der har en direkte indvirkning på gennemførelsen af TLPT. Gennem aktiv deltagelse i hver enkelt testfase kan TLPT-myndighederne effektivt vurdere de finansielle enheders overholdelse af de relevante krav, hvilket bør gøre det muligt for disse myndigheder at udstede erklæringer i henhold til artikel 26, stk. 7, i forordning (EU) 2022/2554.

([2]) Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver og om ændring af forordning (EU) nr. 1093/2010 og (EU) nr. 1095/2010 og direktiv 2013/36/EU og (EU) 2019/1937 (EUT L 150 af 9.6.2023, s. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj).

(9) Fortroligheden af TLPT er af allerstørste betydning for at sikre, at testbetingelserne er realistiske. Derfor bør testforløbet hemmeligholdes, og der bør træffes forholdsregler for at sikre fortroligheden af TLPT'en, hvilket omfatter valget af kodebetegnelser, der skal udformes på en måde, der forhindrer tredjeparter i at detektere TLPT'en. Hvis de medarbejdere, der har ansvar for finansteamets sikkerhed, har kendskab til en planlagt eller igangværende TLPT, er det sandsynligt, at de vil være mere opmærksomme og årvågne end under normale arbejdsvilkår, hvilket vil resultere i et ændret testresultat. Medarbejdere i den finansielle enhed, som ikke er del af kontrolteamet, bør derfor kun gøres bekendt med en eventuel planlagt eller igangværende TLPT, hvis der er tungtvejende årsager hertil, og med forbehold af testledernes forudgående samtykke, bl.a. for at sikre testens fortrolighed, i tilfælde af at et medlem af det blå team har detekteret testforløbet.

(10) Som det fremgår af de erfaringer, der er indhøstet med TIBER-EU-rammen med hensyn til »kontrolteamet«, er det absolut nødvendigt at udvælge en tilfredsstillende leder af kontrolteamet for at sikre en sikker gennemførelse af TLPT. Kontrolteamets leder bør have det nødvendige mandat inden for den finansielle enhed til at udstikke retningslinjer for alle aspekter af testforløbet uden at kompromittere fortroligheden heraf. Af samme årsag bør kontrolteamets medlemmer have et indgående kendskab til den finansielle enhed, den rolle og strategiske placering, som kontrolteamets leder har, have den krævede anciennitet og have adgang til bestyrelsen. For at mindske risikoen for at kompromittere TLPT'en bør kontrolteamet være så lille som muligt.

(11) Der er iboende risikoelementer forbundet med TLPT, da kritiske funktioner testes i et live-produktionsmiljø med mulighed for at forårsage denial-of-service-hændelser, uventede systemsammenbrud, skader på kritiske live-produktionssystemer eller tab, ændring eller videregivelse af data. Disse risici understreger behovet for solide risikostyringsforanstaltninger. For at sikre, at TLPT'en gennemføres på en kontrolleret måde under hele testforløbet, er det meget vigtigt, at de finansielle enheder til enhver tid har kendskab til de særlige risici, der opstår i tilknytning til en TLPT, og at disse risici afbødes. Uden at det berører den finansielle enheds interne processer samt det ansvar og de bemyndigelser, der allerede er givet til kontrolteamets leder, kan det være hensigtsmæssigt at få oplysninger om TLPT-risikostyringsforanstaltningerne eller, i særlige tilfælde, opnå godkendelse af disse risikostyringsforanstaltninger fra selve ledelsesorganet i den finansielle enhed. For at kunne levere effektive og højst kvalificerede professionelle tjenesteydelser og mindske nævnte risici er det også afgørende, at testere og formidlere af trusselsefterretninger (sammen med TLPT-udbyderne) har det højeste niveau af færdigheder, ekspertise og passende erfaring med trusselsefterretninger og TLPT i sektoren for finansielle tjenesteydelser.

(12) Med konventionelle penetrationstest opnås en udførlig og nyttig vurdering af tekniske og konfigurationsrelaterede sårbarheder, ofte i et enkelt system eller miljø isoleret set. Men i modsætning til efterretningsbaserede test, der gennemføres af et rødt team, vurderer de ikke det samlede scenarie med et målrettet angreb mod en hel enhed, herunder det fulde omfang af personer, processer og teknologier i enheden. Under udvælgelsen af TLPT-udbydere bør de finansielle enheder derfor sikre, at disse udbydere har de nødvendige færdigheder til at udføre efterretningsbaserede test, der gennemføres af et rødt team, og ikke kun penetrationstest. Det er derfor nødvendigt at fastsætte omfattende kriterier for testere, både interne og eksterne, og formidlere af trusselsefterretninger, som altid er eksterne. Hvis TLPT-udbyderne tilhører samme virksomhed, bør det personale, som er udpeget til at gennemføre en TLPT, adskilles i tilstrækkelig grad.

(13) Der kan være ekstraordinære omstændigheder, under hvilke finansielle enheder ikke er i stand til at indgå kontrakter med TLPT-udbydere, der opfylder de omfattende kriterier. Finansielle enheder bør derfor, når de dokumenterer, at sådanne formidlere af trusselsefterretninger ikke er tilgængelige, have mulighed for at inddrage personer, der ikke opfylder alle omfattende kriterier, forudsat at de på passende vis afbøder eventuelle deraf følgende yderligere risici, og at TLPT-myndigheden vurderer alle disse kriterier.

(14) Hvis flere finansielle enheder og flere TLPT-myndigheder er involveret i en TLPT, bør alle parters roller i TLPT-processen beskrives nærmere med henblik på at gennemføre den mest effektive og sikre test. Med henblik på samlede testforløb er der behov for specifikke krav for at præcisere den udpegede finansielle enheds rolle, dvs. at den bør have ansvar for at levere al nødvendig dokumentation til den ledende TLPT-myndighed og for at overvåge testprocessen. Den udpegede finansielle enhed bør også have ansvar for de fælles aspekter af vurderingen af risikostyring. Uanset den udpegede finansielle enheds rolle bør forpligtelserne for hver enkel finansiel enhed, der deltager i den samlede TLPT-proces, forblive uændrede under det samlede testforløb. Det samme princip bør gælde for fælles TLPT'er.

(15) Som det fremgår af erfaringerne med gennemførelsen af TIBER-EU-rammen, er afholdelse af fysiske eller virtuelle møder, der inddrager alle berørte interessenter (finansielle enheder, myndigheder, testere og formidlere af trusselsefterretninger), den mest effektive måde til at sikre en hensigtsmæssig gennemførelse af testforløbet. Der bør derfor afholdes fysiske og virtuelle møder på forskellige trin i processen, navnlig i forberedelsesfasen og ved iværksættelsen af TLPT'en, for i løbet af testfasen at afslutte afgrænsningen af dens anvendelsesområde, for at færdiggøre trusselsefterretningsrapporten og det røde teams testplan og plan for de ugentlige opdateringer og i nedlukningsfasen for gennemspilninger af testeres og det blå teams tiltag, »purple teaming« og for at udveksle feedback om TLPT'en.

(16) For at sikre, at TLPT'en fungerer gnidningsløst, bør TLPT-myndigheden give en klar redegørelse for sine forventninger til testen over for den finansielle enhed. I den forbindelse bør testlederne sikre, at der etableres en passende informationsstrøm med kontrolteamet i den finansielle enhed og med TLPT-udbyderne.

(17) Den finansielle enhed bør vælge de kritiske eller vigtige funktioner, der skal indgå i TLPT'ens anvendelsesområde. Ved udvælgelsen af disse funktioner bør den finansielle enhed forlade sig på forskellige kriterier i relation til betydningen af hver funktion for selve den finansielle enhed og for den finansielle sektor, på EU-plan og på nationalt plan, ikke kun i økonomisk henseende, men også i betragtning af funktionens symbolske eller politiske status. For at lette overgangen til fasen med indsamling af trusselsefterretninger bør kontrolteamet give de testere og formidlere af trusselsefterretninger, der ikke er involveret i processen med afgrænsning af anvendelsesområdet, udførlige oplysninger om den fastlagte afgrænsning.

(18) For at give testerne de oplysninger, der er nødvendige for at simulere et virkeligt og realistisk angreb på den finansielle enheds live-systemer, som understøtter dens kritiske eller vigtige funktioner, bør formidleren af trusselsefterretninger indsamle efterretninger eller oplysninger, hvori mindst to centrale interesseområder indgår: målene, idet potentielle angrebsoverflader på tværs af den finansielle enhed identificeres, og truslerne, idet relevante trusselsaktører og sandsynlige trusselsscenarier identificeres. For at sikre, at formidleren af trusselsefterretninger tager hensyn til de relevante trusler mod den finansielle enhed, bør testerne, kontrolteamet og testlederne give feedback på udkastet til trusselsefterretningsrapport. Hvis det er tilgængeligt, kan formidleren af trusselsefterretninger anvende et generisk trusselsbillede, som er forelagt af TLPT-myndigheden, for den finansielle sektor i en medlemsstat som udgangspunkt for det nationale trusselsbillede. Baseret på anvendelsen af TIBER-EU-rammen varer processen med indsamling af trusselsefterretninger typisk ca. fire uger.

(19) For at testerne kan få indsigt i og yderligere gennemgå dokumentet om afgrænsning af anvendelsesområdet og den målrettede trusselsefterretningsrapport med henblik på at færdiggøre det røde teams testplan er det vigtigt, at testerne forud for det røde teams testfase i TLPT'en modtager udførlige redegørelser fra formidleren af trusselsefterretninger om den målrettede trusselsefterretningsrapport og analyse af mulige trusselsscenarier.

(20) For at gøre det muligt for testere at gennemføre et realistisk og omfattende testforløb, hvor alle angrebsfaser udføres og flagmål er nået, bør der afsættes tilstrækkelig tid til det røde teams aktive testfase. På grundlag af erfaringerne med TIBER-EU-rammen bør den tildelte tid være mindst 12 uger og bør fastsættes, idet der tages hensyn til antallet af involverede parter, omfanget af TLPT'ens anvendelsesområde, den eller de involverede finansielle enheders ressourcer, eventuelle eksterne krav og tilgængeligheden af understøttende oplysninger forelagt af den finansielle enhed.

(21) I det røde teams aktive testfase bør testerne anvende en række taktikker, teknikker og procedurer for i tilstrækkelig grad at teste den finansielle enheds live-produktionssystemer. De pågældende taktikker, teknikker og procedurer bør, hvis det er relevant, indeholde rekognoscering (dvs. indsamling af så mange oplysninger som muligt om et mål), instrumentalisering (dvs. analyse af oplysninger om infrastruktur, faciliteter og medarbejdere og forberedelse med henblik på de operationer, der er rettet specifikt mod målet), levering (dvs. aktiv iværksættelse af den fulde operation rettet mod målet), udnyttelse (dvs. hvor testerens mål er at kompromittere servere og netværk i den finansielle enhed og udnytte dens personale gennem social manipulation) kontrol og bevægelse (dvs. forsøg på at bevæge sig fra kompromitterede systemer til yderligere sårbare systemer eller systemer af høj værdi) og tiltag rettet mod mål (dvs. opnåelse af yderligere adgang til kompromitterede systemer og adgang til de tidligere fastlagte oplysninger og -data om mål, som tidligere vedtaget i det røde teams testplan).

(22) Når testere gennemfører en TLPT, bør de handle under hensyntagen til den tid, der er til rådighed til at udføre angrebet, ressourcerne samt de etiske og retlige grænser. Hvis testerne ikke er i stand til at gå videre til den programmerede næste fase af angrebet, bør kontrolteamet efter aftale med TLPT-myndigheden yde lejlighedsvis bistand i form af »forstærkninger«. Forstærkninger kan i store træk kategoriseres som informations- og adgangsbistand og kan bestå i at give adgang til IKT-systemer eller interne netværk for at fortsætte testen og fokusere på de følgende angrebstrin.

(23) Under den aktive »red teaming« i testfasen bør der, hvis det er nødvendigt for, at TLPT'en kan forsættes, som en sidste udvej under ekstraordinære omstændigheder, og når alle alternative muligheder er udtømt, anvendes en samarbejdsbaseret testaktivitet, der involverer både testerne og det blå team. I tilknytning til et således begrænset »purple teaming«-forløb kan følgende metoder anvendes: »catch-and-release«, hvor testere forsøger at videreføre scenarierne, blive detekteret og derefter genoptage testforløbet, »war gaming«, som giver mulighed for mere komplekse scenarier for at teste strategisk beslutningstagning, eller »collaborative proof-of-concept«, som gør det muligt for testere og medlemmer af det blå team i fællesskab at validere specifikke sikkerhedsforanstaltninger, værktøjer eller teknikker i et kontrolleret og samarbejdsbaseret miljø.

(24) TLPT'en bør anvendes som en læringserfaring for at øge finansielle enheders digitale operationelle modstandsdygtighed. I den henseende bør det blå team og testerne foretage en gennemspilning af angrebet og gennemgå de skridt, der er taget for at lære af testerfaringerne i samarbejde med testerne. Med henblik herpå og for at muliggøre tilstrækkelig forberedelse bør det røde teams testrapport og det blå teams testrapport stilles til rådighed for alle parter, der er involveret i gennemspilningsaktiviteterne, inden der udøves gennemspilningsaktiviteter. Desuden bør der gennemføres et »purple teaming«-forløb i afslutningsfasen for at maksimere læringserfaringen. De metoder, der kan anvendes til »purple teaming«-forløbet i afslutningsfasen, bør omfatte drøftelser af alternative angrebsscenarier, undersøgelse af alternative scenarier i live-systemer eller fornyet undersøgelse af planlagte scenarier i live-systemer, som testerne ikke havde været i stand til at færdiggøre eller foretage i testfasen.

(25) For yderligere at fremme læringserfaringen for alle parter, der er involveret i TLPT'en, til gavn for fremtidige test og for at øge finansielle enheders digitale operationelle modstandsdygtighed bør de berørte parter give hinanden feedback om den overordnede proces, og navnlig påpege, hvilke aktiviteter der forløb godt eller kunne have været forbedret, og hvilke aspekter af TLPT-processen der fungerede godt eller kunne forbedres.

(26) De kompetente myndigheder, der er omhandlet i artikel 46 i forordning (EU) 2022/2554, og TLPT-myndighederne, hvis de er forskellige herfra, bør samarbejde om at indarbejde avanceret testforløb ved hjælp af TLPT i de eksisterende tilsynsprocesser. I denne henseende og for at formidle den korrekte forståelse af TLPT-resultaterne og af, hvordan de skal fortolkes, bør der, navnlig for så vidt angår den sammenfattende testrapport og udbedringsplanerne, etableres et tæt samarbejde mellem de testledere, der var involveret i TLPT'en, og de ansvarlige tilsynsmyndigheder.

(27) I henhold til artikel 26, stk. 8, første afsnit, i forordning (EU) 2022/2554 skal finansielle enheder indgå kontrakt med eksterne testere ved hver tredje test. Hvis finansielle enheder inddrager både interne og eksterne testere i teamet, bør dette betragtes som en TLPT, der gennemføres med interne testere med henblik på nævnte artikel.

(28) Denne forordning er baseret på det udkast til reguleringsmæssige tekniske standarder, som Den Europæiske Banktilsynsmyndighed, Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger og Den Europæiske Værdipapir- og Markedstilsynsmyndighed (de europæiske tilsynsmyndigheder) efter aftale med den Europæiske Centralbank har forelagt for Kommissionen.

(29) De europæiske tilsynsmyndigheder har afholdt åbne offentlige høringer om det udkast til reguleringsmæssige tekniske standarder, som ligger til grund for denne forordning, analyseret de potentielle omkostninger og fordele samt anmodet interessentgruppen for banker, der er nedsat i henhold til artikel 37 i Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 ([3]), interessentgruppen for forsikrings- og genforsikringsordninger og interessentgruppen for arbejdsmarkedspensionsordninger, som er nedsat i henhold til artikel 37 i Europa-Parlamentets og Rådets forordning (EU) nr. 1094/2010 ([4]), og interessentgruppen for værdipapirer og markeder, der er nedsat i henhold til artikel 37 i Europa-Parlamentets og Rådets forordning (EU) nr. 1095/2010 ([5]), om en udtalelse.

(30) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([6]) og afgav en udtalelse den 20. august 2024 —

VEDTAGET DENNE FORORDNING:

Artikel 1

Definitioner

I denne forordning forstås ved:

1) »kontrolteam«: den gruppe, der består af personale fra den finansielle enhed, der underlægges en test, og, hvis det er relevant i betragtning af TLPT'ens anvendelsesområde, personalet hos dens tredjepartsudbyder af tjenester og enhver anden part, der gennemfører testen

2) »leder af kontrolteamet«: den medarbejder i den finansielle enhed, som har ansvar for gennemførelsen af alle TLPT-relaterede aktiviteter for den finansielle enhed med tilknytning til en given test

3) »blåt team«: personalet i den finansielle enhed og, hvis det er relevant, hos den finansielle enheds tredjepartsudbydere af tjenester og enhver anden part, der betragtes som relevant på grundlag af TLPT'ens anvendelsesområde, hos den finansielle enheds tredjepartsudbydere af tjenester, som forsvarer en finansiel enheds brug af net- og informationssystemer ved at opretholde dens sikkerhedsstatus over for simulerede eller reelle angreb, og som ikke har kendskab til TLPT'en

4) »blåt team-opgaver«: opgaver, der typisk varetages af det blå team, såsom sikkerhedsoperationscentret (SOC), IKT-infrastrukturtjenester, helpdesktjenester og hændelsesstyringstjenester på operationelt plan

5) »rødt team«: interne eller eksterne testere, som der er indgået kontrakt med, eller som er udpeget til at gennemføre en TLPT

6) »purple teaming«: en samarbejdsbaseret testaktivitet, der involverer både testerne og det blå team

([3]) Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Banktilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/78/EF (EUT L 331 af 15.12.2010, s. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Europa-Parlamentets og Rådets forordning (EU) nr. 1094/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger), om ændring af afgørelse 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/79/EF (EUT L 331 af 15.12.2010, s. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Europa-Parlamentets og Rådets forordning (EU) nr. 1095/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Værdipapir- og Markedstilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/77/EF (EUT L 331 af 15.12.2010, s. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

7) »TLPT-myndighed«: en af følgende:

   a) den fælles offentlige myndighed, som er udpeget i overensstemmelse med artikel 26, stk. 9, i forordning (EU) 2022/2554

   b) den myndighed i den finansielle sektor, til hvilken udførelsen af nogle af eller alle opgaverne i forbindelse med TLPT er delegeret i overensstemmelse med artikel 26, stk. 10, i forordning (EU) 2022/2554

   c) enhver af de kompetente myndigheder, der er omhandlet i artikel 46 i forordning (EU) 2022/2554

8) »TLPT-team« eller »TCT«: personalet i de TLPT-myndigheder, som har ansvar for TLPT-relaterede forhold

9) »testledere«: personale, der er udpeget til at lede TLPT-myndighedens aktiviteter for en specifik TLPT med henblik på at overvåge overholdelsen af denne forordning

10) »formidler af trusselsefterretninger«: eksperter, som den finansielle enhed har indgået kontrakt med for hver enkelt TLPT, og som er eksterne i forhold til den finansielle enhed og eventuelle koncerninterne udbydere af IKT-tjenester, som indsamler og analyserer målrettede trusselsefterretninger med relevans for de finansielle enheder, der er omfattet af anvendelsesområdet for et specifikt TLPT-forløb, og udvikler modsvarende relevante og realistiske trusselsscenarier

11) »TLPT-udbyder«: testere og formidlere af trusselsefterretninger

12) »forstærkning«: den bistand eller de oplysninger, som kontrolteamet giver testerne for at sætte dem i stand til at fortsætte gennemførelsen af en angrebsvej, hvis de ikke er i stand til at komme videre på egen hånd, og hvis der ikke findes andre rimelige alternativer, herunder med hensyn til utilstrækkelig tid eller utilstrækkelige ressourcer til en given TLPT

13) »angrebsvej«: den rute, som testeren følger i testfasen for det røde teams aktive testfase i TLPT'en for at nå de flagmål, der er angivet nærmere for den pågældende TLPT

14) »flagmål«: centrale mål i de IKT-systemer, der understøtter kritiske eller vigtige funktioner i en finansiel enhed, som testerne forsøger at nå gennem testen

15) »følsomme oplysninger«: oplysninger, der let kan udnyttes med henblik på at udføre angreb på den finansielle enheds IKT-systemer, intellektuelle ejendom, fortrolige forretningsdata eller personoplysninger, som kan forvolde direkte eller indirekte skade på den finansielle enhed og dens økosystem, hvis de falder i hænderne på ondsindede aktører

16) »pulje«: alle finansielle enheder, der deltager i en samlet TLPT i henhold til artikel 26, stk. 4, i forordning (EU) 2022/2554

17) »værtsland«: værtsmedlemsstaten i overensstemmelse med den sektorspecifikke EU-ret, der finder anvendelse på hver finansiel enhed

18) »fælles TLPT«: en TLPT, der er forskellig fra en samlet TLPT som omhandlet i artikel 26, stk. 4, i forordning (EU) 2022/2554, og som involverer flere finansielle enheder, der anvender den samme koncerninterne IKT-tjenesteudbyder eller tilhører samme koncern og deler IKT-systemer.

Artikel 2

Identifikation af finansielle enheder, der skal gennemføre TLPT

1. TLPT-myndighederne skal vurdere, om en finansiel enhed er forpligtet til at gennemføre TLPT, idet der tages hensyn til de pågældende finansielle enheders indvirkning, deres systemiske karakter og deres IKT-risikoprofil, på grundlag af alle følgende kriterier:

a) indvirkningsrelaterede og systemiske faktorer:

   i) den finansielle enheds størrelse fastlagt på grundlag af, om den finansielle enhed leverer finansielle tjenesteydelser i en eller flere medlemsstater, og ved at sammenligne den finansielle enheds aktiviteter med aktiviteterne i andre finansielle enheder, der leverer lignende tjenesteydelser

   ii) omfanget og arten af den finansielle enheds indbyrdes forbundethed med andre finansielle enheder i den finansielle sektor i en eller flere medlemsstater

   iii) den kritiske betydning eller vigtighed af de tjenesteydelser, som den finansielle enhed leverer til den finansielle sektor

iv) i hvilket omfang de tjenesteydelser, som den finansielle enhed leverer, kan erstattes

v) kompleksiteten af den finansielle enheds forretningsmodel og de dertil knyttede tjenesteydelser og processer

vi) hvorvidt den finansielle enhed er del af en koncern af systemisk karakter på EU-plan eller nationalt plan i den finansielle sektor og deler IKT-systemer

b) IKT-risikofaktorer:

i) den finansielle enheds risikoprofil

ii) trusselsbilledet i den finansielle enhed

iii) graden af den finansielle enheds afhængighed af kritiske eller vigtige funktioner eller deres understøttende funktioner i forhold til IKT-systemer og -processer

iv) kompleksiteten af den finansielle enheds IKT-arkitektur

v) de IKT-tjenester og -funktioner, der understøttes af tredjepartsudbydere af IKT-tjenester, og mængden og typen af kontraktlige ordninger med tredjepartsudbydere af IKT-tjenester eller koncerninterne udbydere af IKT-tjenester

vi) resultaterne af eventuelle tilsynskontroller med relevans for vurderingen af den finansielle enheds IKT-modenhed

vii) modenheden af planer for IKT-driftsstabilitet og IKT-indsats- og genopretningsplaner

viii) modenheden af de operationelle IKT-sikkerhedsforanstaltninger til detektion og afbødning, herunder evnen til:

1) permanent at overvåge den finansielle enheds IKT-infrastruktur

2) at detektere IKT-relaterede hændelser i realtid

3) analysere de hændelser, der er omhandlet nr. 2)

4) reagere rettidigt og effektivt på de hændelser, der er omhandlet i nr. 2)

ix) hvorvidt den finansielle enhed er del af en koncern, der er aktiv i den finansielle sektor på EU-plan eller nationalt plan, og som deler IKT-systemer.

Med henblik på litra a), nr. i), tager TLPT-myndigheden så vidt muligt hensyn til:

a) den finansielle enheds markedsposition på EU-plan og nationalt plan

b) de aktiviteter, som den finansielle enhed udbyder

c) markedsandelen for de tjenesteydelser, der leveres af den finansielle enhed, eller for de aktiviteter, der udøves på EU-plan og nationalt plan.

Med henblik på litra a), nr. v), tager TLPT-myndigheden så vidt muligt hensyn til:

a) hvorvidt den finansielle enhed opererer med mere end én forretningsmodel

b) de forskellige forretningsprocessers indbyrdes forbundethed og de dertil knyttede tjenesteydelser.

2. TLPT-myndighederne stiller krav om, at alle følgende finansielle enheder gennemfører TLPT, medmindre det fremgår af den i stk. 1 omhandlede vurdering med hensyn til en finansiel enhed, at dens indvirkning, betænkelighederne vedrørende finansiel stabilitet i relation til den pågældende finansielle enhed eller dens IKT-risikoprofil ikke berettiger gennemførelsen af en TLPT:

a) kreditinstitutter, der opfylder en af følgende betingelser:

i) de er blevet udpeget som globale systemisk vigtige institutter (G-SII'er) i henhold til artikel 131 i Europa-Parlamentets og Rådets direktiv 2013/36/EU ([7])

ii) de er blevet udpeget som andre systemisk vigtige institutter (»O-SII'er«) i henhold til artikel 131 i direktiv 2013/36/EU

iii) de er del af et G-SII eller O-SII

([7]) Europa-Parlamentets og Rådets direktiv 2013/36/EU af 26. juni 2013 om adgang til at udøve virksomhed som kreditinstitut og om tilsyn med kreditinstitutter, om ændring af direktiv 2002/87/EF og om ophævelse af direktiv 2006/48/EF og 2006/49/EF (EUT L 176 af 27.6.2013, s. 338, ELI: http://data.europa.eu/eli/dir/2013/36/oj).

b) betalingsinstitutter, der i begge af de to kalenderår, der gik forud for TLPT-myndighedens vurdering, oversteg 150 mia. EUR af værdien af de samlede betalingstransaktioner som defineret i artikel 4, nr. 5), i Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 ([8])

c) e-pengeinstitutter, der i begge af de to kalenderår, der gik forud for TLPT-myndighedens vurdering oversteg enten 150 mia. EUR af værdien af de samlede betalingstransaktioner som defineret i artikel 4, nr. 5), i direktiv (EU) 2015/2366 eller 40 mia. EUR af værdien af den samlede sum af udestående elektroniske penge

d) værdipapircentraler

e) centrale modparter

f) markedspladser med et elektronisk handelssystem, der opfylder et af følgende kriterier:

i) markedspladsen har den største markedsandel målt i omsætning på nationalt plan i begge af de to kalenderår, der gik forud for TLPT-myndighedens vurdering, i et af følgende:

1) værdipapirer som defineret i artikel 4, stk. 1, nr. 44), litra a), i Europa-Parlamentets og Rådets direktiv 2014/65/EU ([9])

2) værdipapirer som defineret i artikel 4, stk. 1, nr. 44), litra b), i direktiv 2014/65/EU

3) derivater som defineret i artikel 2, stk. 1, nr. 29), i Europa-Parlamentets og Rådets forordning (EU) nr. 600/2014 ([10])

4) strukturerede finansielle produkter som defineret i artikel 2, stk. 1, nr. 28), i forordning (EU) nr. 600/2014

5) emissionskvoter som omhandlet i afsnit C, punkt 11), i bilag I til i direktiv 2014/65/EU

ii) markedspladsen har en markedsandel i form af omsætning på EU-plan, der overstiger 5 % i begge af de to kalenderår, der gik forud for TLPT-myndighedens vurdering, i et af følgende:

1) aktier i selskaber og andre værdipapirer, der kan sidestilles med aktier i selskaber, partnerskaber og andre foretagender, samt depotbeviser vedrørende aktier

2) obligationer eller andre gældsinstrumenter, herunder depotbeviser vedrørende sådanne værdipapirer

3) derivater som defineret i artikel 2, stk. 1, nr. 29), i forordning (EU) nr. 600/2014

4) strukturerede finansielle produkter som defineret i artikel 2, stk. 1, nr. 28), i forordning (EU) nr. 600/2014

5) emissionskvoter som omhandlet i afsnit C, punkt 11), i bilag I til i direktiv 2014/65/EU

([8]) Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked, og om ændring af direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om ophævelse af direktiv 2007/64/EF (EUT L 337 af 23.12.2015, s. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

([9]) Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014 om markeder for finansielle instrumenter og om ændring af direktiv 2002/92/EF og direktiv 2011/61/EU (EUT L 173 af 12.6.2014, s. 349, ELI: http://data.europa.eu/eli/dir/2014/65/oj).

([10]) Europa-Parlamentets og Rådets forordning (EU) nr. 600/2014 af 15. maj 2014 om markeder for finansielle instrumenter og om ændring af forordning (EU) nr. 648/2012 (EUT L 173 af 12.6.2014, s. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

g) forsikrings- og genforsikringsselskaber, der opfylder alle følgende kriterier:

i) de har en bruttopræmie på over 1 500 000 000 EUR

ii) de har forsikringsmæssige hensættelser på over 10 000 000 000 EUR

iii) forsikringsselskaber, der kun udøver livsforsikringsvirksomhed, eller som udøver både livsforsikrings- og skadesforsikringsvirksomhed, og hvis samlede aktiver overstiger 3,5 % af summen af de samlede aktiver, der er værdiansat i overensstemmelse med artikel 75 i Europa-Parlamentets og Rådets direktiv 2009/138/EF ([11]), for de forsikrings- og genforsikringsselskaber, der er etableret i medlemsstaten.

Med henblik på litra f), nr. ii), hvis markedspladsen er del af en koncern, der deler IKT-systemer eller den samme koncerninterne IKT-tjenesteudbyder, skal omsætningen af værdipapirerne og derivatkontrakterne på alle markedspladser, der vedrører samme koncern og er etableret i Unionen, tages i betragtning.

Med henblik på litra g) skal TLPT-myndighederne identificere en undergruppe bestående af alle forsikrings- og genforsikringsselskaber ved at anvende kriterierne i litra g), nr. i), ii) og iii). Forsikrings- og genforsikringsselskaber, der indgår i denne undergruppe, skal udføre TLPT, hvis de også opfylder et af følgende kriterier:

a) en bruttopræmie på over 3 000 000 000 EUR

b) forsikringsmæssige hensættelser på over 30 000 000 000 EUR

c) samlede aktiver, der overstiger 10 % af summen af de samlede aktiver, der er værdiansat i overensstemmelse med artikel 75 i direktiv 2009/138/EF, for de forsikrings- og genforsikringsselskaber, der er etableret i medlemsstaten.

3. Hvis mere end én finansiel enhed, der tilhører samme koncern og deler IKT-systemer, eller hvis mere end én finansiel enhed, der anvender samme koncerninterne IKT-tjenesteudbyder, opfylder kriterierne i stk. 2, skal disse finansielle enheders TLPT-myndigheder i overensstemmelse med artikel 16, stk. 2, træffe afgørelse om, hvorvidt kravet om at gennemføre TLPT på individuelt grundlag er relevant for disse finansielle enheder.

Hvis TLPT-myndigheden for modervirksomheden i en koncern bestående af finansielle enheder, jf. første afsnit, er forskellig fra TLPT-myndighederne i koncernens finansielle enheder, skal denne myndighed høres af TLPT-myndighederne for de finansielle enheder, der tilhører den pågældende koncern, om, hvorvidt der bør gennemføres TLPT på individuelt grundlag.

Artikel 3

TCT- og TLPT-testledere

1. En TLPT-myndighed skal overdrage ansvaret for at koordinere TLPT-relaterede aktiviteter til et TCT. Et TCT skal bestå af testledere, der er udpeget til at føre tilsyn med en individuel TLPT.

2. For hver testforløb udpeger TLPT-myndigheden en testleder og mindst én suppleant.

3. Testlederne skal overvåge, om de i denne forordning fastsatte krav er opfyldt, og sikre, at de overholdes.

([11]) Europa-Parlamentets og Rådets direktiv 2009/138/EF af 25. november 2009 om adgang til og udøvelse af forsikrings- og genforsikringsvirksomhed (Solvens II) (EUT L 335 af 17.12.2009, s. 1, ELI: http://data.europa.eu/eli/dir/2009/138/oj).

4. Testlederen skal meddele den finansielle enhed kontaktoplysningerne for TCT'et gennem den underretning, der er omhandlet i artikel 9, stk. 1.

5. TLPT-myndigheden deltager i alle faser af TLPT.

Artikel 4

Organisatoriske ordninger for finansielle enheder

1. De finansielle enheder skal udpege en leder af kontrolteamet, som har ansvar for den daglige ledelse af TLPT'en samt for kontrolteamets beslutninger og tiltag.

2. De finansielle enheder skal træffe organisatoriske og proceduremæssige foranstaltninger for at sikre, at:

a) adgangen til oplysninger vedrørende planlagte eller igangværende TLPT er begrænset til kontrolteamet, ledelsesorganet, testerne, formidleren af trusselsefterretninger og TLPT-myndigheden på grundlag af need to know-princippet

b) kontrolteamet rådfører sig med testlederne, inden et medlem af det blå team inddrages i en TLPT

c) kontrolteamet underrettes om enhver detektion af TLPT'en foretaget af medarbejdere i den finansielle enhed eller dens tredjepartsudbyder af tjenester i tilfælde af eskalering af den deraf følgende hændelsesindsats bringer kontrolteamet om nødvendigt en sådan eskalering under kontrol

d) der er indført ordninger vedrørende fortroligheden af TLPT'en, som gælder for den finansielle enheds personale, personalet hos de berørte tredjepartsudbydere af IKT-tjenester, testere og formidleren af trusselsefterretninger

e) kontrolteamet efter anmodning stiller alle oplysninger vedrørende TLPT'en til rådighed for testlederne

f) de parter, der er involveret i TLPT, kun henviser til den pr. kodebetegnelse, hvis det er muligt.

Artikel 5

Risikostyring i tilknytning til TLPT

1. I forberedelsesfasen, jf. artikel 9, skal kontrolteamet vurdere de risici, der er forbundet med testforløbet for live-produktionssystemer i den finansielle enheds kritiske eller vigtige funktioner, herunder potentielle indvirkninger på:

a) den finansielle sektor

b) den finansielle stabilitet på EU-plan eller nationalt plan.

Kontrolteamet skal gennemgå disse indvirkninger under hele testforløbet.

2. Med henblik på risikovurderingen og -styringen skal kontrolteamet som minimum tage hensyn til følgende typer risici, som er forbundet med:

a) at give formidleren af trusselsefterretninger og de eksterne testere, alt efter hvad der er relevant, adgang til følsomme oplysninger om den finansielle enhed

b) TLPT'ens manglende overholdelse af forordning (EU) 2022/2554 og nærværende forordning, hvis en sådan manglende overholdelse resulterer i manglende erklæringsudstedelse som omhandlet i artikel 26, stk. 7, i forordning (EU) 2022/2554, herunder hvis en sådan manglende overholdelse skyldes brud på fortroligheden af TLPT'en eller mangelfuld etisk adfærd

c) eskalering af kriser og hændelser

d) det røde teams aktive fase, herunder risici forbundet med afbrydelse af kritiske aktiviteter og datakorruption som følge af testernes aktiviteter, og dens potentielle indvirkning på tredjeparter

e) det blå teams aktivitet, herunder risici forbundet med afbrydelse af kritiske aktiviteter og datakorruption som følge af det blå teams aktiviteter, og dens potentielle indvirkning på tredjeparter

f) ufuldstændig gendannelse af systemer, der er berørt af TLPT'en.

Artikel 6

Risikostyring i tilknytning til samlede eller fælles TLPT'er

1. Hvis der er tale om en fælles TLPT eller en samlet TLPT, skal kontrolteamet i hver finansiel enhed foretage sin egen risikovurdering og træffe sine egne risikostyringsforanstaltninger.

2. Kontrolteamet i den udpegede finansielle enhed, der er omhandlet i nærværende forordnings artikel 16, stk. 3, litra b), eller den finansielle enhed, der er udpeget i overensstemmelse med artikel 26, stk. 4, i forordning (EU) 2022/2554, skal vurdere de risici, der er forbundet med involvering af flere finansielle enheders i TLPT'en. De involverede finansielle enheders kontrolteam samarbejder med den udpegede finansielle enheds kontrolteam for at identificere potentielle fælles risici.

Artikel 7

Udvælgelse af TLPT-udbydere

1. Kontrolteamet skal træffe foranstaltninger til at styre de risici, der er forbundet med TLPT'en, og skal navnlig for hver TLPT sikre, at:

a) formidleren af trusselsefterretninger og de eksterne testere forsyner kontrolteamet med et udførligt curriculum vitæ og kopier af certificeringer, der i henhold til anerkendte markedsstandarder er velegnede med henblik på udøvelsen af deres aktiviteter

b) formidleren af trusselsefterretninger og de eksterne testere er behørigt og fuldt ud dækket af de rette erhvervsansvarsforsikringer, herunder mod risici for forseelser og forsømmelighed

c) formidleren af trusselsefterretninger forelægger mindst tre referencer fra tidligere opgaver med tilknytning til penetrationstest og »red team testing«

d) de eksterne testere forelægger mindst fem referencer fra tidligere opgaver med tilknytning til penetrationstest og »red team testing«

e) det personale hos formidleren af trusselsefterretninger, der er udpeget til at gennemføre TLPT'en:

   i) består af mindst én leder med mindst fem års erfaring inden for trusselsefterretninger og mindst ét yderligere medlem med mindst to års erfaring inden for trusselsefterretninger

   ii) besidder en bred vifte af og et passende niveau af faglig viden og færdigheder, herunder:

      1) taktikker, teknikker og procedurer vedrørende indsamling af efterretninger

      2) geopolitisk, teknisk og sektorspecifik viden

      3) tilstrækkelige kommunikationsfærdigheder til klart at fremlægge og rapportere om resultatet af indsatsen

   iii) samlet set har deltaget i mindst tre tidligere opgaver inden for trusselsefterretninger med tilknytning til penetrationstest og »red team testing«

   iv) ikke samtidig varetager blåt team-opgaver eller andre tjenesteydelser, der kan udgøre en interessekonflikt med hensyn til den finansielle enhed, tredjepartsudbyderen af IKT-tjenester eller en koncernintern IKT-tjenesteudbyder, der er involveret i TLPT, som de er udpeget til at gennemføre

   v) er adskilt fra og ikke rapporterer til personale hos den samme TLPT-udbyder, der stiller eksterne testere til rådighed for den samme TLPT

f) med hensyn til eksterne testere gælder følgende det røde team, der er udpeget til at gennemføre TLPT'en:

i) det består af mindst én leder, som har mindst fem års erfaring med penetrationstest og »red team testing« samt mindst to yderligere testere, som hver har mindst to års erfaring med penetrationstest og »red team testing«

ii) det besidder en bred vifte af og et passende niveau af faglig viden og færdigheder, herunder viden om den finansielle enheds aktiviteter, rekognoscering, risikostyring, udviklingsudnyttelse, fysisk indtrængning, social manipulation, sårbarhedsanalyse samt tilstrækkelige kommunikationsfærdigheder til klart at fremlægge og rapportere om resultatet af indsatsen

iii) det har samlet set deltaget i mindst fem tidligere opgaver med tilknytning til penetrationstest og »red team testing«

iv) det er ikke ansat af eller leverer tjenester til en formidler af trusselsefterretninger, der samtidig udfører blåt team-opgaver for enten en finansiel enhed, en tredjepartsudbyder af IKT-tjenester eller en koncernintern IKT-tjenesteudbyder, der er involveret i TLPT'en

v) det er adskilt fra alt personale hos samme TLPT-udbyder, der samtidig leverer trusselsefterretningstjenester med henblik på samme TLPT

g) testeren og formidleren af trusselsefterretninger gennemfører gendannelsesprocedurer efter testforløbets afslutning, herunder sikker sletning af oplysninger vedrørende adgangskoder, identifikationsoplysninger og andre hemmelige nøgler, der er kompromitteret under TLPT'en, sikker meddelelse til de finansielle enheder af de konti, der er kompromitteret, sikker indsamling, lagring, forvaltning og bortskaffelse af andre data, der er indsamlet under testforløbet

h) ud over gendannelsesprocedurerne ved testforløbets afslutning, jf. litra g), gennemfører testeren følgende gendannelsesprocedurer:

i) deaktivering af kommando og kontrol

ii) omfangs- og datobestemte nødstopmekanismer (»scope and date kill switches«)

iii) fjernelse af »bagdøre« og andet malware

iv) anmeldelse af potentielle brud

v) procedurer for fremtidig gendannelse af sikkerhedskopiering, som kan vedrøre malware eller værktøj, der er installeret under testforløbet

vi) overvågning af det blå teams aktiviteter og informering af kontrolteamet om eventuelle mulige detektioner

i) testere og formidleren af trusselsefterretninger må ikke udøve eller deltage i nogen af følgende aktiviteter:

i) uautoriseret destruktion af udstyr, som tilhører den finansielle enhed og dens eventuelle tredjepartsudbydere af IKT-tjenester

ii) ukontrolleret ændring af oplysninger og IKT-tjenester, som tilhører den finansielle enhed og dens eventuelle tredjepartsudbydere af IKT-tjenester

iii) forsætlig kompromittering af kontinuiteten i den finansielle enheds kritiske eller vigtige funktioner

iv) uautoriseret inddragelse af systemer uden for anvendelsesområdet

v) uautoriseret videregivelse af testresultater.

2. Kontrolteamet skal føre register over den dokumentation, som testerne og formidlerne af trusselsefterretninger har fremlagt for at dokumentere overensstemmelse med stk. 1, litra a)-f).

Under ekstraordinære omstændigheder kan finansielle enheder indgå kontrakt med eksterne testere og formidlere af trusselsefterretninger, som ikke opfylder et eller flere af kravene i stk. 1, litra a)-f), forudsat at disse finansielle enheder vedtager passende foranstaltninger til at afbøde de risici, der forbundet med manglende overholdelse af sådanne punkter, og registrerer disse foranstaltninger.

Artikel 8

Risikostyring af samlede eller fælles TLPT'er

1. Hvis flere finansielle enheder, der er identificeret i overensstemmelse med artikel 16, stk. 2 eller 4, er involveret i en samlet eller fælles TLPT, skal den enkelte finansielle enhed følge hvert af de trin, der er fastsat i artikel 9-15, medmindre den ledende TLPT-myndighed træffer anden afgørelse herom.

2. Hvis flere TLPT-myndigheder er involveret i en fælles TLPT eller i en samlet TLPT, jf. artikel 16, stk. 3, eller 5, skal henvisninger i artikel 9-15 til »TLPT-myndigheden« forstås som en henvisning til den ledende TLPT-myndighed for en sådan samlet eller fælles TLPT, medmindre andet er fastsat i denne forordning.

Artikel 9

Forberedelsesfasen

1. En finansiel enhed, der er identificeret i henhold til artikel 26, stk. 8, andet afsnit, i forordning (EU) 2022/2554, skal indlede en TLPT efter en meddelelse fra TLPT-myndigheden om, at en TLPT skal gennemføres.

2. En finansiel enhed skal senest tre måneder efter modtagelsen af den i stk. 1 omhandlede meddelelse indsende alle følgende oplysninger om indledning af TLPT til testlederne:

a) et projektcharter, herunder en projektplan på højt niveau, der indeholder de i bilag I fastsatte oplysninger

b) kontaktoplysninger for lederen af kontrolteamet

c) oplysninger om den påtænkte anvendelse af interne eller eksterne testere eller begge, hvis det er relevant, jf. artikel 15

d) oplysninger om de kommunikationskanaler, der skal anvendes under TLPT-forløbet

e) kodebetegnelsen for TLPT'en.

3. Hvis de oplysninger, der er omhandlet i stk. 2, litra a)-e), er fuldstændige og sikrer TLPT'ens egnethed og en effektiv gennemførelse heraf, validerer TLPT-myndigheden den finansielle enheds oplysninger om indledning af TLPT'en og giver den finansielle enhed meddelelse herom.

4. Efter TLPT-myndighedens validering af dokumenterne om indledning af TLPT'en skal den finansielle enhed oprette et kontrolteam, som skal bistå lederen af kontrolteamet med dennes opgaver, der består i at:

a) præcisere kommunikationskanaler og -processer internt i kontrolteamet, med testerne og formidleren af trusselsefterretninger vedrørende alle TLPT-relaterede forhold

b) give ledelsesorganet i den finansielle enhed meddelelse om fremskridtene med TLPT-forløbet og de dermed forbundne risici

c) træffe beslutninger på grundlag af ekspertise inden for emneområdet gennem hele TLPT-forløbet

d) gennemføre TLPT'en i overensstemmelse med denne forordning

e) udvælge formidlere af trusselsefterretninger til TLPT'en

f) udvælge eksterne testere, interne testere eller begge dele

g) udarbejde dokumentet om afgrænsning af anvendelsesområdet.

5. Hvis TLPT-myndigheden finder, at kontrolteamets oprindelige sammensætning og eventuelle efterfølgende ændringer heraf er tilstrækkelig(e) til at varetage de i stk. 4 omhandlede opgaver, validerer TLPT-myndigheden kontrolteamet og giver lederen af kontrolteamet meddelelse herom.

6. Den finansielle enhed skal indsende et dokument om afgrænsning af anvendelsesområdet, der indeholder alle de i bilag II fastsatte oplysninger, til testlederne senest seks måneder efter modtagelsen af meddelelsen fra TLPT-myndigheden, jf. stk. 1. Den finansielle enheds ledelsesorgan skal godkende dokumentet om afgrænsning af anvendelsesområdet.

7. Finansielle enheder skal tage hensyn til følgende kriterier for inddragelse af kritiske eller vigtige funktioner i TLPT'ens anvendelsesområde:

a) funktionens kritiske betydning eller vigtighed og dens mulige indvirkning på den finansielle sektor og på den finansielle stabilitet på EU-plan og nationalt plan

b) funktionens vigtighed for den finansielle enheds daglige forretningsaktiviteter

c) muligheden for at udskifte funktionen

d) den indbyrdes forbundethed med andre funktioner

e) funktionens geografiske placering

f) andre enheders sektorspecifikke afhængighed af funktionen

g) hvis det er muligt, trusselsefterretninger vedrørende funktionen.

8. Kontrolteamet skal dele oplysningerne om indledning af TLPT og dokumentet om afgrænsning af anvendelsesområdet med testerne og formidlerne af trusselsefterretninger, når der er indgået kontrakt med disse. Kontrolteamet skal underrette testerne og formidlerne af trusselsefterretninger om den testproces, der skal følges.

9. Den finansielle enhed skal sikre, at tilvejebringelsen eller udpegelsen af testere og trusselsefterretningsudbydere afsluttes, inden testfasen indledes.

10. Inden testfasen indledes, skal kontrolteamet rådføre sig med testlederne om TLPT-risikovurderingen og om risikostyringsforanstaltningerne. Kontrolteamet skal gennemgå risikovurderingen eller risikostyringsforanstaltningerne, hvis TLPT-myndigheden er af den opfattelse, at de ikke i tilstrækkelig grad imødegår de risici, der er forbundet med TLPT'en.

11. Kontrolteamet skal vurdere, om de formidlere af trusselsefterretninger og testere, som de overvejer at inddrage i TLPT'en, overholder kravene i artikel 27 i forordning (EU) 2022/2554 og nærværende forordnings artikel 7, stk. 1, og dokumentere resultatet af denne vurdering. Kontrolteamet skal udvælge formidlere af trusselsefterretninger i overensstemmelse med denne vurdering og sin risikostyringspraksis. Inden der indgås kontrakt med de udvalgte formidlere af trusselsefterretninger og eksterne testere, skal kontrolteamet forelægge dokumentation for testlederne for, at disse formidlere af trusselsefterretninger og testere overholder kravene i artikel 27 i forordning (EU) 2022/2554 og nærværende forordnings artikel 7, stk. 1. Kontrolteamet må ikke indgå kontrakter med de udvalgte formidlere af trusselsefterretninger og eksterne testere, hvis TLPT-myndigheden er af den opfattelse, at de udvalgte formidlere af trusselsefterretninger og eksterne testere ikke overholder kravene i artikel 27 i forordning (EU) 2022/2554 eller kravene i nærværende forordnings artikel 7, stk. 1, eller yderligere krav, der hidrører fra national sikkerhedslovgivning i overensstemmelse med EU-retten, eller hvis den finansielle enhed ikke overholder nærværende forordnings artikel 7, stk. 2, første afsnit, eller hvis de omstændigheder, der er omhandlet i nærværende forordnings artikel 7, stk. 2, andet afsnit, ikke gør sig gældende.

12. Hvis dokumentet om afgrænsning af anvendelsesområdet er fuldstændigt og sikrer en passende og effektiv gennemførelse af TLPT'en, godkender TLPT-myndigheden dette dokument og underretter kontrolteamet herom.

Artikel 10

Testfasen: trusselsefterretninger

1. Når TLPT-myndigheden har godkendt dokumentet om afgrænsning af anvendelsesområdet, skal formidleren af trusselsefterretninger analysere generiske og sektorspecifikke trusselsefterretninger med relevans for den finansielle enhed. Hvis TLPT-myndigheden har forelagt et generisk trusselsbillede for den finansielle sektor i en medlemsstat, kan formidleren af trusselsefterretninger anvende dette billede som udgangspunkt for det nationale trusselsbillede. Formidleren af trusselsefterretninger skal identificere cybertrusler og eksisterende eller potentielle sårbarheder, som vedrører den finansielle enhed. Desuden skal formidleren af trusselsefterretninger indsamle oplysninger om og analysere konkrete, håndterbare og kontekstualiserede mål- og trusselsefterretninger, som vedrører den finansielle enhed, herunder gennem høring af kontrolteamet og testlederne.

2. Formidleren af trusselsefterretninger skal fremlægge de relevante trusler og målrettede trusselsefterretninger og foreslå kontrolteamet, testeren og testlederne de nødvendige scenarier. De foreslåede scenarier skal være forskellige med hensyn til de identificerede trusselsaktører og dertil knyttede taktikker, teknikker og procedurer og skal være rettet mod hver kritisk eller vigtig funktion inden for TLPT'ens anvendelsesområde.

3. Lederen af kontrolteamet skal udvælge mindst tre scenarier med henblik på gennemførelse af TLPT'en på grundlag af alle følgende elementer:

a) anbefalingen fra formidleren af trusselsefterretninger og hvert scenaries trusselsbaserede karakter

b) input fra testlederne

c) hvorvidt de foreslåede scenarier kan gennemføres på grundlag af testernes ekspertvurdering

d) den finansielle enheds størrelse, kompleksitet og overordnede risikoprofil og arten, omfanget og kompleksiteten af dens tjenester, aktiviteter og operationer.

4. Højst et af de udvalgte scenarier må være ikketrusselsbaseret og kan være baseret på en fremadskuende og potentielt fiktiv trussel med høj prædiktiv, foregribende, opportunistisk eller fremadrettet værdi i betragtning af den forventede udvikling i det trusselsbillede, der vedrører den finansielle enhed.

Med hensyn til samlede TLPT'er, skal mindst ét scenarie, uden at det berører de scenarier, der direkte er rettet mod de kritiske eller vigtige funktioner i de finansielle enheder, der er involveret i testforløbet, omfatte tredjepartsudbyderen af IKT-tjenesters relevante underliggende IKT-systemer, -processer og -teknologier, som understøtter de kritiske eller vigtige funktioner i de finansielle enheder, der er omfattet af anvendelsesområdet.

Hvis testforløbet er en fælles TLPT, der involverer en koncernintern udbyder af IKT-tjenester, skal mindst ét scenarie, uden at det berører de scenarier, der direkte er rettet mod de kritiske eller vigtige funktioner i de finansielle enheder, der er involveret i testforløbet, omfatte den koncerninterne udbyder af IKT-tjenesters relevante underliggende IKT-systemer, -processer og -teknologier, som understøtter de kritiske eller vigtige funktioner i de finansielle enheder, der er omfattet af anvendelsesområdet.

5. Formidleren af trusselsefterretninger skal forelægge den målrettede trusselsefterretningsrapport for kontrolteamet, herunder de scenarier, der er udvalgt i overensstemmelse med stk. 3 og 4. Trusselsefterretningsrapporten skal indeholde de i bilag III fastsatte oplysninger.

6. Kontrolteamet skal forelægge den målrettede trusselsefterretningsrapport for testlederen til godkendelse. Hvis den målrettede trusselsefterretningsrapport er fuldstændig og sikrer en passende og effektiv gennemførelse af TLPT'en, godkender TLPT-myndigheden den målrettede trusselsefterretningsrapport og underretter kontrolteamet herom.

Artikel 11

Testfasen: det røde teams testforløb

1. Når TLPT-myndigheden har godkendt den målrettede trusselsefterretningsrapport, skal testerne udarbejde det røde teams testplan, som skal indeholde de i bilag IV fastsatte oplysninger. Testerne skal anvende dokumentet om afgrænsning af anvendelsesområdet og den målrettede trusselsefterretningsrapport som grundlag for udarbejdelsen af angrebsscenarierne.

2. Testerne skal rådføre sig med kontrolteamet, formidleren af trusselsefterretninger og testlederne om det røde teams testplan, herunder ordningen vedrørende kommunikation, procedurer og projektstyrings, forberedelsen og de tilfælde, hvor der gøres brug af forstærkningsaktivering, og aftalerne om rapportering til kontrolteamet og testlederne.

3. Hvis det røde teams testplan er fuldstændig og sikrer en passende og effektiv gennemførelse af TLPT'en, godkender kontrolteamet og TLPT-myndigheden røde teams testplan og underretter kontrolteamet herom.

4. Efter godkendelse af det røde teams testplan i overensstemmelse med stk. 3 skal testeren gennemføre TLPT'en i det røde teams aktive testfase.

5. Varigheden af det røde teams aktive testfase skal stå i rimeligt forhold til TLPT'ens anvendelsesområde, omfanget, aktiviteten, kompleksiteten og antallet af de finansielle enheder og tredjepartsudbydere af IKT-tjenester eller koncerninterne udbydere af IKT-tjenester, der er involveret i TLPT, og skal under alle omstændigheder være på mindst 12 uger. Angrebsscenarier kan gennemføres i rækkefølge eller samtidig. Kontrolteamet, formidleren af trusselsefterretninger, testerne og testlederne skal nå til enighed om afslutningen af det røde teams aktive testfase.

6. Med forbehold af at det sikres, at det røde teams testplan fortsat er fuldstændig og gør det muligt at gennemføre en effektiv TLPT, skal lederen af kontrolteamet og testlederne godkende eventuelle ændringer af det røde teams testplan efter godkendelsen heraf, herunder af tidsplanen, omfanget, målsystemerne eller flagmålene.

7. I hele det røde teams aktive testfase skal testeren mindst en gang om ugen rapportere til kontrolteamet og testlederne om de fremskridt, der er gjort med TLPT'en, og formidleren af trusselsefterretninger skal være til rådighed med henblik på konsultation og yderligere trusselsefterretninger, når kontrolteamet anmoder herom.

8. Kontrolteamet skal rettidigt stille de forstærkninger, der er udformet på grundlag af det røde teams testplan, til rådighed. Forstærkninger kan tilføjes eller tilpasses efter godkendelse fra kontrolteamet og testlederne.

9. Hvis en ansat i den finansielle enhed eller dens tredjepartsudbydere af IKT-tjenester eller en koncernintern IKT-tjenesteudbyder detekterer testaktiviteterne, skal kontrolteamet, hvis det er relevant, i samråd med testerne, og uden at det berører stk. 10, foreslå og forelægge foranstaltninger, der gør det muligt at fortsætte TLPT-forløbet, samtidig med at testlederne forsikres om fortroligheden heraf med henblik på validering.

10. Under ekstraordinære omstændigheder, der udløser risici for indvirkning på data, skade på aktiver og forstyrrelser af kritiske eller vigtige funktioner, tjenester eller operationer i den finansielle enhed selv, hos dens tredjepartsudbydere af IKT-tjenester eller koncerninterne udbydere af IKT-tjenester eller forstyrrelser, der berører dens modparter eller den finansielle sektor, kan kontrolholdet suspendere TLPT'en eller, som en sidste udvej, hvis det ikke på anden måde er muligt at videreføre TLPT'en, og med forbehold af TLPT-myndighedens forudgående validering heraf, fortsætte TLPT'en ved hjælp af et begrænset »purple teaming«-forløb. Varigheden af det begrænsede »purple teaming«-forløb regnes med i minimumsvarigheden på 12 uger af det røde teams aktive testfase, der er omhandlet i stk. 5.

Artikel 12

Afslutningsfasen

1. Efter afslutningen af det røde teams aktive testfase skal lederen af kontrolteamet underrette det blå team om, at der er gennemført en TLPT.

2. Senest fire uger efter afslutningen af det røde teams aktive testfase skal testerne forelægge kontrolteamet det røde teams testrapport, som indeholder de i bilag V fastsatte oplysninger.

3. Kontrolteamet skal uden unødigt ophold forelægge det røde teams testrapport for det blå team og testlederne.

Hvis testlederne anmoder herom, må den i første afsnit omhandlede rapport ikke indeholde følsomme oplysninger.

4. Efter modtagelse af det røde teams testrapport og senest ti uger efter afslutningen af det røde teams aktive testfase skal det blå team forelægge kontrolteamet det blå teams testrapport, som indeholder de i bilag VI fastsatte oplysninger. Kontrolteamet skal uden unødigt ophold forelægge det blå teams testrapport for testerne og testlederne.

Hvis testlederne anmoder herom, må den i første afsnit omhandlede rapport ikke indeholde følsomme oplysninger.

5. Senest ti uger efter afslutningen af det røde teams aktive testfase skal det blå team og testerne gennemspille de offensive og defensive tiltag, der er gennemført under TLPT-forløbet. Kontrolteamet skal også gennemføre et »purple teaming«-forløb for emner, som det blå team og testerne har identificeret i fællesskab, baseret på de sårbarheder, der blev konstateret under testforløbet, og, hvis det er relevant, på forhold, der ikke kunne testes i det røde teams aktive testfase.

6. Når gennemspilningen og »purple teaming«-forløbet er afsluttet, skal kontrolteamet, det blå team, testerne og formidlerne af trusselsefterretninger give hinanden indbyrdes feedback om TLPT-processen. Testlederne kan give feedback.

7. Når TLPT-myndigheden har underrettet kontrolteamet om, at den har vurderet, at det blå teams testrapport og det røde teams testrapport indeholder de i bilag V og VI fastsatte oplysninger, skal den finansielle enhed inden for otte uger forelægge den rapport, der sammenfatter de relevante TLPT-resultater, for TLPT-myndigheden, jf. artikel 26, stk. 6, i forordning (EU) 2022/2554, og som indeholder de i bilag VII fastsatte elementer til godkendelse.

Hvis TLPT-myndigheden anmoder herom, må den i første afsnit omhandlede rapport ikke indeholde følsomme oplysninger.

Artikel 13

Udbedringsplanen

1. Senest otte uger efter den meddelelse, der er omhandlet i nærværende forordnings artikel 12, stk. 7, skal den finansielle enhed forelægge de udbedringsplaner og den dokumentation, der er omhandlet i artikel 26, stk. 6, i forordning (EU) 2022/2554, for TLPT-myndigheden og, hvis den er forskellig herfra, for den finansielle enheds kompetente myndighed.

2. Den i stk. 1 omhandlede udbedringsplan skal for hvert resultat, der forekommer som led i TLPT'en, omfatte:

a) en beskrivelse af de konstaterede mangler

b) en beskrivelse af de foreslåede afhjælpende foranstaltninger samt prioriteringen og den forventede afslutning heraf, herunder, hvis det er relevant, foranstaltninger til forbedring af identifikations-, beskyttelses-, detektions- og indsatskapaciteten

c) analyse af de grundlæggende årsager

d) den finansielle enheds personale eller funktioner, som har ansvar for gennemførelsen af de foreslåede afhjælpende foranstaltninger eller forbedringer

e) de risici, der er forbundet med ikke at gennemføre de i litra b) omhandlede foranstaltninger, og, hvis det er relevant, de risici, der er forbundet med gennemførelsen af sådanne foranstaltninger.

Artikel 14

Erklæringsudstedelse

1. Den erklæring, der er omhandlet i artikel 26, stk. 7, i forordning (EU) 2022/2554, skal indeholde de i bilag VIII omhandlede oplysninger.

2. Hvis flere TLPT-myndigheder har været involveret i en TLPT, udsteder den ledende TLPT-myndighed den erklæring, der er omhandlet i artikel 26, stk. 7, i forordning (EU) 2022/2554, til de testede finansielle enheder.

Artikel 15

Brugen af interne testere

1. De finansielle enheder skal indføre alle følgende ordninger for brugen af interne testere:

a) fastlæggelse og gennemførelse af en politik for forvaltning af interne testere i et TLPT-forløb

b) foranstaltninger til at sikre, at brugen af interne testere til at gennemføre en TLPT ikke har en negativ indvirkning på den finansielle enheds generelle kapaciteter i form af forsvar eller modstandsdygtighed i tilknytning til IKT-relaterede hændelser eller i væsentlig grad påvirker tilgængeligheden af ressourcer, der afsættes til IKT-relaterede opgaver under et TLPT-forløb

c) foranstaltninger til at sikre, at interne testere har tilstrækkelige ressourcer og kapaciteter til at gennemføre en TLPT.

Den i litra a) omhandlede proces skal:

a) indeholde kriterier for vurdering af de interne testeres egnethed, kompetence og potentielle interessekonflikter og angive ledelsesansvar i testprocessen

b) dokumenteres og revideres regelmæssigt

c) fastsætte, at det interne testteam omfatter en testleder og mindst to yderligere medlemmer

d) indeholde krav om, at alle medlemmer af testteamet har været ansat hos den finansielle enhed eller en koncernintern IKT-tjenesteudbyder i de foregående 12 måneder

e) indeholde bestemmelser om kurser for interne testere i, hvordan man gennemfører penetrationstest og det røde teams test.

2. Hvis en TLPT-myndighed godkender brugen af interne testere i overensstemmelse med artikel 27, stk. 2, litra a), i forordning (EU) 2022/2554, tager TLPT-myndigheden hensyn til de krav, der er fastsat i nærværende forordnings artikel 7, stk. 1.

3. Når den finansielle enhed gør brug af interne testere, skal den sikre, at en sådan brug nævnes i følgende dokumenter:

a) oplysningerne om indledning af et testforløb, jf. artikel 9

b) det røde team testrapport, jf. artikel 12, stk. 2

c) den rapport, der sammenfatter de relevante TLPT-resultater, jf. artikel 26, stk. 6, i forordning (EU) 2022/2554.

4. Testere, der er ansat af en koncernintern IKT-tjenesteudbyder, betragtes som interne testere i den finansielle enhed.

Artikel 16

Samarbejde og gensidig anerkendelse

1. Med henblik på gennemførelse af en TLPT i tilknytning til en finansiel enhed, der leverer tjenesteydelser i mere end én medlemsstat, herunder gennem en filial, sørger dens TLPT-myndighed for:

a) at bestemme, hvilke TLPT-myndigheder i værtslandene der skal inddrages, idet der tages hensyn til, om en eller flere kritiske eller vigtige funktioner drives i eller deles på tværs af værtslande

b) at underrette de TLPT-myndigheder, der er identificeret i overensstemmelse med litra a), om beslutningen om at gennemføre en TLPT af den pågældende finansielle enhed

c) medmindre andet aftales af TLPT-myndighederne, er det den finansielle enheds TLPT-myndighed der fungerer som leder af TLPT'en.

Værtslandenes TLPT-myndigheder kan senest 20 arbejdsdage efter modtagelsen af oplysningerne om en fremtidig gennemførelse af en TLPT enten tilkendegive deres interesse i at følge TLPT-forløbet som observatører eller udpege en testleder, som skal deltage i TLPT'en. Den ledende TLPT-myndighed forelægger dokumentet om afgrænsning af anvendelsesområdet, den sammenfattende testrapport, udbedringsplanen og erklæringen for alle TLPT-myndigheder, der fungerer som observatører i TLPT-forløbet.

Den ledende TLPT-myndighed koordinerer alle deltagende TLPT-myndigheder under hele testforløbet og træffer alle de beslutninger, der er nødvendige for sikre en passende og effektiv gennemførelse af TLPT'en. Den ledende TLPT-myndighed kan fastsætte et maksimalt antal deltagende TLPT-myndigheder, hvis den effektive gennemførelse af TLPT'en ellers kan blive bragt i fare.

2. Hvis en finansiel enhed anvender den samme koncerninterne IKT-tjenesteudbyder som finansielle enheder, der er etableret i andre medlemsstater, eller tilhører en koncern og deler IKT-systemer med finansielle enheder i samme koncern, der er etableret i andre medlemsstater, kontakter den finansielle enheds TLPT-myndighed de andre finansielle enheders TLPT-myndigheder, der anvender den samme koncerninterne IKT-tjenesteudbyder eller deler IKT-systemer som en del af koncernen, og vurderer sammen med disse, om det er praktisk muligt og hensigtsmæssigt at gennemføre en fælles TLPT for dem. En fælles TLPT foretrækkes frem for en individuel TLPT, hvis det kan medføre en reduktion af omkostninger og ressourcer for de finansielle enheder og for TLPT-myndighederne, forudsat at det ikke er til skade for testens soliditet og effektivitet.

3. Med henblik på gennemførelse af en fælles TLPT:

a) de finansielle enheders TLPT-myndigheder aftaler, hvilken finansiel enhed der skal udpeges til at gennemføre TLPT'en, idet der tages til koncernstrukturen og testens effektivitet

b) TLPT-myndigheden i den finansielle enhed, der er udpeget i overensstemmelse med litra a), fungerer som leder af TLPT'en, medmindre der er truffet aftale om andet mellem TLPT-myndighederne for de finansielle enheder, der deltager i den fælles TLPT

c) TLPT-myndighederne i andre finansielle enheder end den finansielle enhed, der er udpeget til at lede den fælles TLPT, kan enten tilkendegive deres interesse i at følge TLPT-forløbet som observatører eller udpege en testleder for den pågældende TLPT.

Den ledende TLPT-myndighed koordinerer alle de TLPT-myndigheder, der er involveret i den fælles TLPT, og træffer alle de beslutninger, der er nødvendige for sikre, at den fælles TLPT gennemføres på en solid og effektiv måde.

4. Hvis en finansiel enhed har til hensigt at gennemføre en samlet TLPT som omhandlet i artikel 26, stk. 4, i forordning (EU) 2022/2554, som eventuelt involverer finansielle enheder, der er etableret i andre medlemsstater, kontakter dens TLPT-myndighed de andre finansielle enheders TLPT-myndigheder og vurderer sammen med dem, om det er praktisk muligt og hensigtsmæssigt at gennemføre en samlet TLPT for dem i overensstemmelse med artikel 26, stk. 4, i forordning (EU) 2022/2554.

5. Med henblik på gennemførelsen af en samlet TLPT, jf. artikel 26, stk. 4, i forordning (EU) 2022/2554, gælder følgende:

a) de finansielle enheders TLPT-myndigheder aftaler, hvilken finansiel enhed der skal udpeges til at gennemføre den samlede TLPT, idet der tages hensyn til de IKT-tjenester, som tredjepartsudbyderen af IKT-tjenester leverer til de finansielle enheder, og testens effektivitet

b) TLPT-myndigheden i den finansielle enhed, der er udpeget i overensstemmelse med litra a), fungerer som leder af TLPT'en, medmindre der er truffet aftale om andet mellem TLPT-myndighederne for de finansielle enheder, der deltager i den samlede TLPT

c) TLPT-myndighederne i andre finansielle enheder end den finansielle enhed, der er udpeget til at lede den samlede TLPT, kan enten tilkendegive deres interesse i at følge TLPT-forløbet som observatører eller udpege en testleder for den pågældende TLPT.

Den ledende TLPT-myndighed koordinerer alle de TLPT-myndigheder, der er involveret i den samlede TLPT, og træffer alle de beslutninger, der er nødvendige for sikre, at den samlede TLPT gennemføres på en solid og effektiv måde.

6. Hvis en finansiel enhed, der skal gennemføre en TLPT, har en TLPT-myndighed, som er forskellig fra dens kompetente myndighed, jf. artikel 46 i forordning (EU) 2022/2554, udveksler disse myndigheder alle relevante oplysninger om alle TLPT-relaterede forhold med henblik på at gennemføre TLPT'en eller varetage deres opgaver i overensstemmelse med nævnte forordning.

Artikel 17

Ikrafttræden

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 13. februar 2025.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

BILAG I

Indhold af projektcharteret (artikel 9, stk. 2, litra a))

Oplysningsfelt	Påkrævede oplysninger:
Den person, der har ansvar for projektplanen, dvs. lederen af kontrolteamet	Navn Kontaktoplysninger
Testere	☐ interne ☐ eksterne ☐ begge
Udvalgte kommunikationskanaler i overensstemmelse med artikel 9, stk. 2, litra d), og artikel 9, stk. 4, litra a), herunder: a) kryptering af e-mail, der skal anvendes b) onlinedatarum, der skal anvendes c) chatprogrammer, der skal anvendes	
Kodebetegnelse for TLPT'en	
Eventuelle kritiske eller vigtige funktioner, som den finansielle enhed opererer i andre medlemsstater	1. liste over kritiske eller vigtige funktioner, der opereres i en anden medlemsstat 2. for hver kritisk eller vigtig funktion, angivelse af den eller de medlemsstat(er), hvor de opereres
Eventuelle kritiske eller vigtige funktioner, der understøttes af tredjepartsudbydere af IKT-tjenester	3. liste over kritiske eller vigtige funktioner, der understøttes af tredjepartsudbydere af IKT-tjenester 4. for hver funktion, angivelse af tredjepartsudbyderen af IKT-tjenester
Forventede frister for afslutning af:	
1. Forberedelsesfasen, i overensstemmelse med artikel 9	åååå-mm-dd
2. Testfasen, i overensstemmelse med artikel 10 og 11	åååå-mm-dd
3. Afslutningsfasen, i overensstemmelse med artikel 12	åååå-mm-dd
4. Udbedringsplanen, i overensstemmelse med artikel 13	åååå-mm-dd

BILAG II

Indhold af dokumentet om afgrænsning af anvendelsesområdet (artikel 9, stk. 6)

1. Dokumentet om afgrænsning af anvendelsesområdet skal indeholde en liste over alle kritiske eller vigtige funktioner, som den finansielle enhed har identificeret.

2. For hver identificeret kritisk eller vigtig funktion skal følgende oplysninger tages med:
   a) hvis den kritiske eller vigtige funktion ikke indgår i TLPT'ens anvendelsesområde, en redegørelse for årsagerne til, at den ikke er taget med
   b) hvis den kritiske eller vigtige funktion er taget med i TLPT'ens anvendelsesområde:
      i) en redegørelse for årsagerne til, at det er taget med
      ii) det eller de identificerede IKT-system(er), der understøtter denne kritiske eller vigtige funktion
      iii) for hvert identificeret IKT-system:
         1. hvorvidt det er outsourcet, og i givet fald navnet på tredjepartsudbyderen af IKT-tjenester
         2. de jurisdiktioner, hvor IKT-systemet anvendes
         3. en overordnet beskrivelse af det eller de foreløbige flagmål med angivelse af, hvilket sikkerhedsaspekt af fortrolighed, integritet, autenticitet eller tilgængelighed de enkelte flag dækker over.

BILAG III

Indhold af den målrettede trusselsefterretningsrapport (artikel 10, stk. 5)

Den målrettede trusselsefterretningsrapport skal indeholde oplysninger om følgende:

1. Det overordnede omfang af efterretningsefterforskningen, herunder mindst følgende:
   a) kritiske eller vigtige funktioner inden for anvendelsesområdet
   b) deres geografiske placering
   c) det officielle anvendte EU-sprog
   d) relevante tredjepartsudbydere af IKT-tjenester
   e) det tidsrum, inden for hvilket efterforskningen er indsamlet.
2. Den overordnede vurdering af, hvilke konkrete anvendelige efterretninger der kan findes om den finansielle enhed, herunder:
   a) medarbejderens brugernavne og adgangskoder
   b) de lignende områder, som kan forveksles med officielle områder i den finansielle enhed
   c) teknisk rekognoscering: sårbar software, sårbare systemer og teknologier, der kan udnyttes
   d) oplysninger, som ansatte ligger op på internettet, og som vedrører den finansielle enhed og kan anvendes i forbindelse med et angreb
   e) oplysninger til salg på det mørke internet
   f) eventuelle andre relevante oplysninger, der er tilgængelige på internettet eller offentlige net
   g) hvis det er relevant, oplysninger om fysisk målretning, herunder måder at få adgang til den finansielle enheds lokaler på.
3. Trusselsefterretningsanalyse, der tager hensyn til det generelle trusselsbillede og den finansielle enheds særlige situation, herunder som minimum:
   a) det geopolitiske miljø
   b) det økonomiske miljø
   c) teknologiske tendenser og andre tendenser, som er forbundet med aktiviteterne i sektoren for finansielle tjenesteydelser.
4. Trusselsprofiler for de ondsindede aktører (specifik enkeltperson/gruppe eller generisk klasse), der kan have den finansielle enhed som mål, herunder den finansielle enheds systemer, som ondsindede aktører med størst sandsynlighed vil kompromittere eller have som mål, den mulige motivation, hensigt og begrundelse for den potentielle målretning og angribernes mulige modus operandi.
5. Trusselsscenarier: mindst tre ende-til-ende-trusselsscenarier for de trusselsprofiler, der er identificeret i overensstemmelse med punkt 4, og som udviser den højeste grad af trusselsalvor. Trusselsscenarierne skal beskrive ende-til-ende-angrebsvejen og som minimum omfatte:
   a) et scenarie, der omfatter, men ikke er begrænset til kompromitterede tjenesters tilgængelighed
   b) et scenarie, der omfatter, men ikke er begrænset til kompromitteret dataintegritet
   c) et scenarie, der omfatter, men ikke er begrænset til fortroligheden af oplysninger.
6. Hvis det er relevant, en beskrivelse af det ikketrusselsbaserede scenarie, der er omhandlet i artikel 10, stk. 4.

BILAG IV

Indhold af det røde teams testplan (artikel 11, stk. 1)

Det røde teams testplan skal indeholde oplysninger om følgende:

a) kommunikationskanaler og -procedurer

b) de taktikker, teknikker og procedurer, som det er tilladt og ikke tilladt at anvende i forbindelse med angrebet, herunder etiske grænser for social manipulation

c) de risikostyringsforanstaltninger, som testerne skal følge

d) en beskrivelse for hvert scenarie, herunder:

   i) den simulerede trusselsaktør

   ii) deres hensigt, motivation og mål

   iii) målfunktionen/målfunktionerne og det eller de understøttende IKT-system(er)

   iv) de aspekter vedrørende fortrolighed, integritet, tilgængelighed og autenticitet, som udgør målet

   v) flagmål

e) en detaljeret beskrivelse af hver forventet angrebsvej, herunder forudsætninger og eventuelle forstærkninger, som kontrolteamet skal stille til rådighed, herunder frister for tilvejebringelse og potentiel anvendelse heraf

f) planlægning af »red teaming«-aktiviteter, herunder tidsplanen for gennemførelsen af hvert scenarie, med en minimumsopdeling efter de tre faser, som en tester følger i løbet af testfasen, og som henholdsvis går ind i finansielle enheders IKT-systemer, bevæger sig gennem IKT-systemerne og i sidste ende gennemfører tiltag til opfyldelse af mål og i sidste ende trækker sig ud af IKT-systemerne (faserne »indtrængen, gennemførelse og tilbagetrækning«)

g) særlige forhold ved de finansielle enheders infrastruktur, der skal tages i betragtning under testforløbet

h) eventuelle yderligere oplysninger eller andre ressourcer, der er nødvendige for testerne til gennemførelse af scenarierne.

BILAG V

Indhold af det røde teams testrapport (artikel 12, stk. 2)

Det røde teams testrapport skal som minimum indeholde oplysninger om følgende:

a) oplysninger om det udførte angreb, herunder:
   i) de målrettede kritiske eller vigtige funktioner og identificerede IKT-systemer, -processer og -teknologier, der understøtter den kritiske eller vigtige funktion, som identificeret i det røde teams testplan
   ii) sammenfatning af hvert scenarie
   iii) flagmål, der er nået og ikke er nået
   iv) angrebsveje, som er fulgt med gode og dårlige resultater
   v) taktikker, teknikker og procedurer, der er anvendt med gode og dårlige resultater
   vi) eventuelle afvigelser fra det røde teams testplan
   vii) eventuelle modtagne forstærkninger
b) alle tiltag, som testerne er bekendt med, og som blev gennemført af det blå team for at gennemspille angrebet og afbøde virkningerne heraf
c) detekterede sårbarheder og andre konstateringer, herunder:
   i) beskrivelse af sårbarhed og andre konstateringer, herunder deres kritiske betydning
   ii) analyse af de grundlæggende årsager til vellykkede angreb
   iii) anbefalinger til udbedring, herunder angivelse af udbedringsprioriteten.

BILAG VI

Indhold af det blå teams testrapport (artikel 12, stk. 4)

Det blå teams testrapport skal som minimum indeholde oplysninger om følgende:

1. for hvert angrebsskridt, som testerne har beskrevet i det røde teams testplan:
   a) liste over detekterede angrebstiltag
   b) logfiler, som svarer til disse detektioner
2. vurdering af testernes konstateringer og anbefalinger
3. dokumentation for testernes angreb, som er indsamlet af det blå team
4. det blå teams analyse af den grundlæggende årsag til vellykkede angreb
5. liste over indhøstede erfaringer og identificerede muligheder for forbedringer
6. liste over emner, der skal behandles i tilknytning til »purple teaming«.

BILAG VII

Detaljer i den rapport, der sammenfatter de relevante TLPT-resultater, jf. artikel 26, stk. 6, i forordning (EU) 2022/2554

Den sammenfattende testrapport skal som minimum indeholde oplysninger om følgende:

a) de involverede parter

b) projektplanen

c) det validerede anvendelsesområde, herunder begrundelsen for at medtage eller udelukke kritiske eller vigtige funktioner og identificerede IKT-systemer, -processer og -teknologier, som understøtter de kritiske eller vigtige funktioner, der er omfattet af TLPT

d) udvalgte scenarier og enhver væsentlig afvigelse fra den målrettede trusselsefterretningsrapport

e) udførte angrebsveje og anvendte taktikker, teknikker og procedurer

f) opfyldte og ikkeopfyldte flagmål

g) eventuelle afvigelser fra det røde teams testplan

h) eventuelle detektioner af blåt hold

i) »purple teaming« i testfasen, hvis det gennemføres, og de dermed forbundne betingelser

j) eventuelle anvendte forstærkninger

k) risikostyringsforanstaltninger, der er truffet

l) detekterede sårbarheder og andre konstateringer, herunder deres kritiske betydning

m) analyse af de grundlæggende årsager til vellykkede angreb

n) overordnet udbedringsplan, sammenkædning af sårbarheder og andre konstateringer, de grundlæggende årsager her til og afhjælpningsprioriteten herfor

o) erfaringer, der er indhøstet gennem den modtagne feedback.

BILAG VIII

Detaljer i den erklæring, der udstedes om TLPT'en, jf. artikel 26, stk. 7, i forordning (EU) 2022/2554

Erklæringen skal som minimum indeholde følgende oplysninger:

a) om den gennemførte TLPT:
   i) start- og slutdatoerne for TLPT'en
   ii) den kritiske eller vigtige funktion indgår i testens anvendelsesområde
   iii) hvis det er relevant, oplysninger om kritiske eller vigtige funktioner, der indgår i testens anvendelsesområde, i relation til hvilke TLPT'en ikke blev gennemført
   iv) hvis det er relevant, andre finansielle enheder, der var involveret i TLPT'en
   v) hvis det er relevant, de tredjepartsudbydere af IKT-tjenester, der deltog i TLPT'en
   vi) med hensyn til testere:
      1. om der blev gjort brug af interne testere
      2. om den finansielle enhed anvendte artikel 5, stk. 3, andet afsnit
   vii) varigheden, angivet i kalenderdage, af det røde teams testfase
b) hvis flere TLPT-myndigheder har været involveret i TLPT'en, de andre TLPT-myndigheder og i hvilken egenskab
c) liste over de dokumenter, som TLPT har gennemgået med henblik på udstedelse af erklæringen.