Europeiska unionens
officiella tidning

SV
L-serien

2025/1190

18.6.2025

KOMMISSIONENS DELEGERADE FÖRORDNING (EU) 2025/1190

av den 13 februari 2025

om komplettering av Europaparlamentets och rådets förordning (EU) 2022/2554 vad gäller tekniska standarder för tillsyn som specificerar de kriterier som används för att identifiera finansiella entiteter som är skyldiga att genomföra hotbildsstyrd penetrationstestning, kraven och standarderna för användning av interna testare, kraven i fråga om omfattning, testmetod och tillvägagångssätt för varje fas av testningen, resultat och avslutnings- och åtgärdsfaser, samt typen av tillsynssamarbete och annat relevant samarbete som krävs för genomförandet av hotbildsstyrd penetrationstestning och för underlättandet av ömsesidigt erkännande

(Text av betydelse för EES)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 ([1]), särskilt artikel 26.11 fjärde stycket, och

av följande skäl:

(1) Denna förordning har utarbetats i enlighet med TIBER-EU-ramen och återspeglar den metod, process och struktur för hotbildsstyrd penetrationstestning som beskrivs i TIBER-EU. Finansiella entiteter som omfattas av hotbildsstyrd penetrationstestning får hänvisa till och tillämpa TIBER-EU-ramen eller något av dess nationella genomförandearrangemang, i den mån ramen eller genomförandearrangemanget uppfyller kraven i artiklarna 26 och 27 i förordning (EU) 2022/2554 och denna förordning. Utseendet av en enda offentlig myndighet inom finanssektorn som ansvarar för frågor som rör hotbildsstyrd penetrationstestning på nationell nivå enligt artikel 26.9 i förordning (EU) 2022/2554 bör inte påverka de behöriga myndigheternas behörighet som tilldelats på unionsnivå för tillsynen av vissa finansiella entiteter i enlighet med artikel 46 i den förordningen, till exempel vad gäller Europeiska centralbanken i fråga om betydande kreditinstitut där behörighet ska anses finnas för frågor som rör hotbildsstyrd penetrationstestning. Om endast vissa uppgifter som rör hotbildsstyrd penetrationstestning delegeras till en annan nationell myndighet inom finanssektorn i enlighet med artikel 26.10 i förordning (EU) 2022/2554 bör den finansiella entitetens behöriga myndighet som avses i artikel 46 i den förordningen förbli myndighet för de uppgifter som rör hotbildsstyrd penetrationstestning som inte har delegerats.

(2) Med tanke på komplexiteten hos den hotbildsstyrda penetrationstestningen och de risker som är förknippade med den, bör dess användning begränsas till de finansiella entiteter för vilka den är motiverad. Myndigheter med ansvar för frågor som rör hotbildsstyrd penetrationstestning (myndigheter på antingen unionsnivå eller nationell nivå med ansvar för hotbildsstyrd penetrationstestning) bör därför inte inkludera finansiella entiteter som är verksamma inom delsektorer för centrala finansiella tjänster, för vilka en hotbildsstyrd penetrationstestning inte är motiverad. Detta innebär att kreditinstitut, betalningsinstitut och institut för elektroniska pengar, värdepapperscentraler, centrala motparter, handelsplatser och försäkrings- och återförsäkringsföretag skulle kunna befrias från kravet på hotbildsstyrd penetrationstestning, även om de uppfyller de kvantitativa kriterierna, mot bakgrund av en övergripande bedömning av deras IKT-riskprofil och IKT-mognad, påverkan på finanssektorn och därmed sammanhängande risker för den finansiella stabiliteten.

(3) Myndigheter med ansvar för hotbildsstyrd penetrationstestning bör, mot bakgrund av en övergripande bedömning av IKT-riskprofilen och IKT-mognaden, av påverkan på finanssektorn och av därmed sammanhängande risker för den finansiella stabiliteten, bedöma huruvida andra typer av finansiella entiteter än kreditinstitut, betalningsinstitut, institut för elektroniska pengar, centrala motparter, värdepapperscentraler, handelsplatser och försäkrings- och återförsäkringsföretag bör omfattas av hotbildsstyrd penetrationstestning. Bedömningen av om sådana finansiella entiteter uppfyller dessa kvalitativa kriterier bör ha som mål att identifiera finansiella entiteter för vilka hotbildsstyrd penetrationstestning är lämplig genom användning av sektorsövergripande och objektiva indikatorer. Samtidigt bör bedömningen av om en finansiell entitet uppfyller dessa kvalitativa kriterier begränsa de entiteter som ska omfattas

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

av hotbildsstyrd penetrationstestning till de entiteter för vilka testningen är motiverad. Huruvida en finansiell entitet uppfyller dessa kvalitativa kriterier bör även bedömas mot bakgrund av ny marknadsutveckling och den ökande betydelsen av nya marknadsaktörer för finanssektorn i framtiden, inbegripet leverantörer av kryptotillgångstjänster som auktoriserats i enlighet med artikel 59 i Europaparlamentets och rådets förordning (EU) 2023/1114 ([2]).

(4) Finansiella entiteter kan ha samma koncerninterna IKT-tjänsteleverantör eller tillhöra samma koncern och förlita sig på gemensamma IKT-system. I så fall är det viktigt att myndigheter med ansvar för hotbildsstyrd penetrationstestning beaktar den finansiella entitetens struktur och betydelse för systemet som helhet eller betydelse för finanssektorn på nationell nivå eller unionsnivå vid bedömningen av huruvida en finansiell entitet bör omfattas av hotbildsstyrd penetrationstestning och huruvida den hotbildsstyrda penetrationstestningen bör genomföras på entitetsnivå eller koncernnivå (genom en samlad hotbildsstyrd penetrationstestning).

(5) För att avspegla TIBER-EU-ramen är det nödvändigt att testmetoden skapar förutsättningar för medverkan av följande huvuddeltagare: den finansiella entiteten, med ett ledningslag (motsvarande TIBER-EU:s ”ledningslag”) och ett blått lag (motsvarande TIBER-EU:s ”blå lag”), och myndigheten med ansvar för hotbildsstyrd penetrationstestning, i form av ett cyberlag för hotbildsstyrd penetrationstestning (motsvarande TIBER-EU:s ”TIBER-cyberlag”), en leverantör av underrättelser om hot, och testare (där testarna motsvarar TIBER-EU:s ”rött lag-leverantör”).

(6) För att se till att den hotbildsstyrda penetrationstestningen drar nytta av erfarenheterna från genomförandet av TIBER-EU och för att minska riskerna vid genomförandet av testningen, bör det säkerställas att ansvarsområdena för de cyberlag som ska inrättas vid myndigheterna med ansvar för hotbildsstyrd penetrationstestning motsvarar ansvarsområdena för TIBER-EU:s cyberlag så nära som möjligt. Följaktligen bör cyberlagen för hotbildsstyrd penetrationstestning ha testledare som ansvarar för att övervaka enskilda hotbildsstyrda penetrationstestningar och för att planera och samordna enskilda tester. Cyberlag för hotbildsstyrd penetrationstestning bör fungera som en gemensam kontaktpunkt för testrelaterad kommunikation till interna och externa intressenter, för insamling och bearbetning av återkoppling och lärdomar från tidigare utförda tester och för stöd till finansiella entiteter som genomgår hotbildsstyrd penetrationstestning.

(7) För att avspegla TIBER-EU-ramens metoder bör testledarna ha nödvändig förmåga och kompetens för att kunna ge råd och ifrågasätta testarnas förslag. Erfarenheterna från TIBER-EU-ramen har visat att det är värdefullt att ha ett lag bestående av minst två testledare för varje test. För att återspegla att hotbildsstyrd penetrationstestning är tänkt att uppmuntra till lärande, och för att skydda testernas konfidentialitet, uppmanas myndigheter med ansvar för hotbildsstyrd penetrationstestning starkt att, såvida de inte har brist på resurser och expertis, ta hänsyn till att testledarna då testningen pågår inte bör bedriva tillsynsverksamhet på samma finansiella entitet som genomgår hotbildsstyrd penetrationstestning.

(8) För att uppnå överensstämmelse med TIBER-EU-ramen är det viktigt att myndigheten med ansvar för hotbildsstyrd penetrationstestning noggrant följer testningen i varje steg. Med tanke på testningens karaktär och de risker som är förknippade med den är det av grundläggande betydelse att myndigheten med ansvar för hotbildsstyrd penetrationstestning är involverad i varje specifik testfas. I synnerhet bör myndigheten med ansvar för hotbildsstyrd penetrationstestning rådfrågas och validera de bedömningar eller beslut från de finansiella entiteternas sida som å ena sidan kan påverka testets effektivitet och å andra sidan kan påverka de risker som är förknippade med testet. Till de grundläggande steg som myndigheten med ansvar för hotbildsstyrd penetrationstestning specifikt måste vara involverad i hör validering av viss grundläggande testdokumentation och val av leverantörer av underrättelser om hot och testare samt riskhanteringsåtgärder. Involveringen av myndigheterna med ansvar för hotbildsstyrd penetrationstestning bör, särskilt när det gäller valideringar, inte leda till en alltför stor börda på dessa myndigheter och bör därför begränsas till sådan dokumentation och sådana beslut som direkt påverkar genomförandet av den hotbildsstyrda penetrationstestningen. Genom aktivt deltagande i varje fas av testningen kan myndigheterna med ansvar för hotbildsstyrd penetrationstestning på ett effektivt sätt bedöma de finansiella entiteternas efterlevnad av de relevanta kraven, vilket bör göra det möjligt för dessa myndigheter att utfärda intyg i enlighet med artikel 26.7 i förordning (EU) 2022/2554.

([2]) Europaparlamentets och rådets förordning (EU) 2023/1114 av den 31 maj 2023 om marknader för kryptotillgångar och om ändring av förordningarna (EU) nr 1093/2010 och (EU) nr 1095/2010 samt direktiven 2013/36/EU och (EU) 2019/1937 (EUT L 150, 9.6.2023, s. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj).

(9) Sekretess är av yttersta vikt för den hotbildsstyrda penetrationstestningen för att säkerställa att testförhållandena är realistiska. Av denna anledning bör den hotbildsstyrda testningen ske dolt, och försiktighetsåtgärder bör vidtas för att hålla den konfidentiell, vilket innefattar val av kodnamn som bör tas fram så att tredje part inte kan identifiera testningen. Om personal som ansvarar för den finansiella gruppens säkerhet skulle känna till en planerad eller pågående hotbildsstyrd penetrationstestning är det sannolikt att de skulle vara mer uppmärksamma och observanta än under normala arbetsförhållanden, vilket skulle leda till ett skevt resultat av testningen. Personal vid den finansiella entiteten som inte ingår i ledningslaget bör därför endast göras uppmärksam på planerade eller pågående hotbildsstyrda penetrationstestningar om det finns tvingande skäl för detta och efter godkännande i förhand från testledarna, till exempel för att säkerställa att testet hålls hemligt om en medlem i det blå laget har upptäckt testningen.

(10) Som framgår av de erfarenheter som gjorts inom TIBER-EU-ramen när det gäller ”ledningslaget” är det absolut nödvändigt att välja en lämplig ledare för ledningslaget för att den hotbildsstyrda penetrationstestningen ska kunna genomföras på ett säkert sätt. Ledningslagets ledare bör ha det mandat inom den finansiella entiteten som krävs för att leda alla aspekter av testningen, utan att dess sekretess äventyras. Av samma skäl bör medlemmarna i ledningslaget ha djupgående kunskap om den finansiella entiteten och om den yrkesroll och strategiska position som ledningslagets ledare har, samt ha erforderlig tjänstgöringstid och direkt tillgång till styrelsen. För att minska risken för att den hotbildsstyrda penetrationstestningen avslöjas bör ledningslaget vara så litet som möjligt.

(11) Det finns inneboende riskelement kopplade till hotbildsstyrd penetrationstestning eftersom kritiska funktioner testas i en produktionsmiljö som är i drift, med risk att orsaka överbelastningstillbud, oväntade driftsavbrott i system, skador på kritiska produktionssystem som är i drift eller förlust, ändring eller avslöjande av data. Dessa risker innebär att det krävs tillförlitliga riskhanteringsåtgärder. För att säkerställa att den hotbildsstyrda penetrationstestningen utförs på ett kontrollerat sätt under hela testningen är det mycket viktigt att de finansiella entiteterna hela tiden är medvetna om de särskilda risker som uppstår vid en hotbildsstyrd penetrationstestning och att dessa risker minskas. Utan att det påverkar den finansiella entitetens interna processer och det ansvar och de delegeringar som ledningslagets ledare redan har fått, kan det i detta sammanhang vara lämpligt med information om riskhanteringsåtgärder kopplade till hotbildsstyrd penetrationstestning eller, i specifika fall, godkännande av dessa riskhanteringsåtgärder av den finansiella entitetens ledningsorgan. För att kunna tillhandahålla effektiva och högt kvalificerade yrkesmässiga tjänster och minska dessa risker är det också viktigt att testare och leverantörer av underrättelser om hot (tillsammans kallade *leverantörer av hotbildsstyrd penetrationstestning*) har mycket hög kompetens och sakkunskap samt lämplig erfarenhet av underrättelser om hot och hotbildsstyrd penetrationstestning inom sektorn för finansiella tjänster.

(12) Traditionella penetrationstester ger en detaljerad och användbar bedömning av tekniska och konfigurationsrelaterade sårbarheter, ofta isolerade till ett enda system eller en enda miljö, men till skillnad från underrättelsestyrda rött lag-tester bedömer de inte hela scenariot med ett riktat angrepp mot en hel entitet, där samtliga personer, processer och tekniska system berörs. Under urvalsprocessen för leverantörer av hotbildsstyrd penetrationstestning bör finansiella entiteter därför säkerställa att dessa leverantörer har den kompetens som krävs för att utföra underrättelsestyrda rött lag-tester och inte bara penetrationstester. Det är således nödvändigt att fastställa heltäckande kriterier för testare, både interna och externa, och leverantörer av underrättelser om hot, som alltid är externa. När leverantörerna av hotbildsstyrd penetrationstestning tillhör samma företag bör personalen som utsetts att genomföra testningen hållas tillräckligt separerad.

(13) Det kan finnas exceptionella omständigheter som gör att finansiella entiteter inte lyckas ingå avtal med leverantörer av hotbildsstyrd penetrationstestning som uppfyller de heltäckande kriterierna. Finansiella entiteter bör därför, efter att ha bevisat att sådana leverantörer av underrättelser om hot inte finns att tillgå, tillåtas att använda personer som inte uppfyller samtliga av de heltäckande kriterierna, förutsatt att de på ett korrekt sätt minskar eventuella ytterligare risker som följer av detta och att myndigheten som ansvarar för hotbildsstyrd penetrationstestning bedömer alla dessa kriterier.

(14) Om flera finansiella entiteter och flera myndigheter med ansvar för hotbildsstyrd penetrationstestning deltar i en hotbildsstyrd penetrationstestning bör rollerna för alla parter i testprocessen specificeras så att ett så effektivt och säkert test som möjligt kan genomföras. Vid gemensam testning behövs särskilda krav för att specificera den utsedda finansiella entitetens roll, närmare bestämt att den bör ansvara för att tillhandahålla all nödvändig dokumentation till den ledande myndigheten med ansvar för hotbildsstyrd penetrationstestning och för att övervaka testprocessen. Den utsedda finansiella entiteten bör även ansvara för de gemensamma aspekterna av riskhanteringsbedömningen. Oberoende av den utsedda finansiella entitetens roll bör skyldigheterna för varje finansiell entitet som deltar i den gemensamma processen för hotbildsstyrd penetrationstestning förbli opåverkade under det gemensamma testet. Samma princip bör gälla för samlad hotbildsstyrd penetrationstestning.

(15) Som framgår av erfarenheterna från genomförandet av TIBER-EU-ramen är det effektivaste sättet att säkerställa ett korrekt genomförande av testningen att hålla fysiska eller virtuella möten med alla berörda intressenter (finansiella entiteter, myndigheter, testare och leverantörer av underrättelser om hot). Fysiska och virtuella möten bör därför hållas under flera olika skeden av processen, särskilt under förberedelsefasen vid starten av den hotbildsstyrda penetrationstestningen och för att fastställa dess omfattning, under testfasen för att färdigställa hotunderrättelserapporten och planen för rött lag-testning och de veckovisa uppdateringarna, samt under avslutningsfasen för att gå igenom testarnas och det blå lagets åtgärder och de lila lagövningarna och utbyta återkoppling om den hotbildsstyrda penetrationstestningen.

(16) För att säkerställa att testningen förlöper smidigt bör myndigheten med ansvar för hotbildsstyrd penetrationstestning tydligt redovisa sina förväntningar i fråga om testningen för den finansiella entiteten. I detta avseende bör testledarna säkerställa att ett lämpligt informationsflöde upprättas med ledningslaget inom den finansiella entiteten och med leverantörerna av hotbildsstyrd penetrationstestning.

(17) Den finansiella entiteten bör välja ut de kritiska eller viktiga funktioner som ska omfattas av den hotbildsstyrda penetrationstestningen. När den finansiella entiteten väljer ut dessa funktioner bör den basera valet på olika kriterier för hur viktig varje funktion är för den finansiella entiteten själv och för finanssektorn, på unionsnivå och på nationell nivå, och inte bara i ekonomiskt avseende utan även med beaktande av funktionens symboliska eller politiska status. För att underlätta en smidig övergång till fasen för insamling av underrättelser om hot bör ledningslaget förse testare och leverantörer av underrättelser om hot, som inte är involverade i processen för att identifiera omfattningen, med detaljerad information om den överenskomna omfattningen.

(18) För att förse testarna med den information som krävs för att simulera ett verkligt och realistiskt angrepp på den finansiella entitetens system i drift som stöder dess kritiska eller viktiga funktioner bör leverantören av underrättelser om hot samla in underrättelser eller information som omfattar minst två nyckelområden: målen, genom att identifiera potentiella angreppsytor inom hela den finansiella entiteten, och hoten, genom att identifiera relevanta hotaktörer och sannolika hotscenarier. För att säkerställa att leverantören av underrättelser om hot beaktar de relevanta hoten mot den finansiella entiteten bör testarna, ledningslaget och testledarna lämna återkoppling på utkastet till hotunderrättelserapport. Som utgångspunkt för den nationella hotbilden får leverantören av underrättelser om hot använda en generell hotbild som tillhandahålls av myndigheten som ansvarar för hotbildsstyrd penetrationstestning för finanssektorn i en medlemsstat, om en sådan finns tillgänglig. Baserat på tillämpningen av TIBER-EU-ramen tar processen för insamling av underrättelser om hot vanligtvis cirka fyra veckor.

(19) För att testarna ska kunna få insikt i och ytterligare granska omfattningsdokumentet och den målinriktade hotunderrättelserapporten, i syfte att slutföra rött lag-testplanen, är det viktigt att testarna före rött lag-testfasen i den hotbildsstyrda penetrationstestningen får detaljerade förklaringar av den målinriktade hotunderrättelserapporten och analysen av möjliga hotscenarier från leverantören av underrättelser om hot.

(20) För att testarna ska kunna utföra en realistisk och heltäckande testning där alla angreppsfaser utförs och alla flaggor nås bör tillräcklig tid avsättas för den aktiva rött lag-testfasen. Baserat på de erfarenheter som gjorts inom TIBER-EU-ramen bör den tid som avsätts vara minst tolv veckor och den bör fastställas med beaktande av antalet deltagande parter, omfattningen av den hotbildsstyrda penetrationstestningen, den eller de berörda finansiella entiteternas resurser, eventuella externa krav och tillgången till stödjande information som tillhandahålls av den finansiella entiteten.

(21) Under den aktiva rött lag-testfasen bör testarna använda olika taktiker, teknik och förfaranden för att på lämpligt sätt testa den finansiella entitetens produktionssystem i drift. Taktikerna, tekniken och förfarandena bör, när så är lämpligt, innefatta rekognosering (dvs. insamling av så mycket information som möjligt om ett mål), användning av information som vapen (dvs. analys av information om infrastruktur, anläggningar och anställda och förberedelse för insatser riktade specifikt mot målet), utförande (dvs. aktiv igångsättning av hela insatsen mot målet), utnyttjande (dvs. där testarnas mål är att angripa den finansiella entitetens servrar och nätverk och utnyttja dess personal genom social manipulering), kontroll och förflyttning (dvs. försök att gå över från de angripna systemen till andra sårbara eller värdefulla system) och åtgärder gentemot målet (dvs. få ytterligare tillgång till angripna system och få tillgång till tidigare överenskommen målinformation och tidigare överenskomna måldata, enligt vad som tidigare överenskommits i planen för rött lag-testning).

(22) När testare genomför en hotbildsstyrd penetrationstestning bör de agera med hänsyn till den tid som finns tillgänglig för att utföra angreppet, resurserna och etiska och rättsliga gränser. Om testarna inte kan gå vidare till nästa steg av angreppet enligt planen bör ledningslaget, efter överenskommelse med myndigheten som ansvarar för hotbildsstyrd penetrationstestning, ge tillfällig hjälp i form av hjälpinsatser. Hjälpinsatser kan i stora drag delas upp i hjälpinsatser som rör information respektive tillgång och kan innebära att tillgång ges till IKT-system eller interna nätverk för att fortsätta med testet och fokusera på följande angreppssteg.

(23) Om det är nödvändigt för att kunna fortsätta den hotbildsstyrda penetrationstestningen, som en sista utväg under exceptionella omständigheter och när alla andra alternativ har uttömts, bör under de aktiva rött lag-insatserna i testfasen en gemensam testverksamhet som innefattar både testarna och det blå laget tillämpas. I samband med en sådan begränsad lila lagövning kan följande metoder användas: ”fångst och återsläpp”, där testare försöker fortsätta scenarierna, blir upptäcka och sedan återupptar testningen, ”krigsspel”, som möjliggör mer komplexa scenarier för att testa strategiskt beslutsfattande, eller ”koncepttest under samverkan”, som låter testare och medlemmar i det blå laget gemensamt validera specifika säkerhetsåtgärder, säkerhetsverktyg eller säkerhetsteknik i en kontrollerad och samarbetsinriktad miljö.

(24) Den hotbildsstyrda penetrationstestningen bör användas som ett tillfälle till lärande för att öka de finansiella entiteternas digitala operativa motståndskraft. Av detta skäl bör det blå laget och testarna gå igenom angreppet och se över de steg som vidtogs för att dra lärdom av testerfarenheterna i samverkan med testarna. I detta syfte och för att möjliggöra lämplig förberedelse bör det röda lagets testrapport och det blå lagets testrapport göras tillgängliga för alla parter som deltar i genomgången innan någon genomgång av åtgärderna inleds. Dessutom bör en lila lagövning genomföras, under avslutningsfasen, för att maximera möjligheterna till lärande. Till metoderna som kan användas för lila lagövningar under avslutningsfasen bör höra diskussioner om alternativa angreppsscenarier, undersökning av system i drift i alternativa scenarier eller ny undersökning av planerade scenarier för system i drift som testarna inte kunde slutföra eller genomföra under testfasen.

(25) För att ytterligare underlätta lärandet för alla parter som deltar i den hotbildsstyrda penetrationstestningen, till nytta för framtida tester och för att främja finansiella entiteters digitala operativa motståndskraft, bör de deltagande parterna ge varandra återkoppling om den övergripande processen och i synnerhet identifiera vilka aktiviteter som förlöpte bra eller som kunde ha förbättrats, samt vilka aspekter av testningen som fungerade bra eller som kunde ha förbättrats.

(26) De behöriga myndigheter som avses i artikel 46 i förordning (EU) 2022/2554 och myndigheterna med ansvar för hotbildsstyrd penetrationstestning bör, om det inte rör sig om samma myndigheter, samarbeta för att införliva avancerad testning i form av hotbildsstyrd penetrationstestning i de befintliga tillsynsprocesserna. Av detta skäl och för att dela en korrekt förståelse av resultaten av den hotbildsstyrda penetrationstestningen och av hur de bör tolkas är det lämpligt, särskilt när det gäller den sammanfattande testrapporten och åtgärdsplanerna, att skapa ett nära samarbete mellan testledarna som var involverade i den hotbildsstyrda penetrationstestningen och ansvariga tillsynsmyndigheter.

(27) Enligt artikel 26.8 första stycket i förordning (EU) 2022/2554 ska de finansiella entiteterna anlita externa testare vid vart tredje test. Om de finansiella entiteterna har både interna och externa testare i gruppen av testare bör detta, vad gäller tillämpningen av den artikeln, betraktas som en hotbildsstyrd penetrationstestning som utförs med interna testare.

(28) Denna förordning grundar sig på det förslag till tekniska standarder för tillsyn som överlämnats till kommissionen av Europeiska bankmyndigheten, Europeiska försäkrings- och tjänstepensionsmyndigheten och Europeiska värdepappers- och marknadsmyndigheten (de europeiska tillsynsmyndigheterna) i samförstånd med Europeiska centralbanken.

(29) De europeiska tillsynsmyndigheterna har genomfört öppna offentliga samråd om det förslag till tekniska standarder för tillsyn som denna förordning bygger på, gjort en kostnads–nyttoanalys samt begärt råd från den bankintressentgrupp som inrättats i enlighet med artikel 37 i Europaparlamentets och rådets förordning (EU) nr 1093/2010 ([3]), den intressentgrupp för försäkring och återförsäkring och den intressentgrupp för tjänstepensioner som inrättats i enlighet med artikel 37 i Europaparlamentets och rådets förordning (EU) nr 1094/2010 ([4]) och den intressentgrupp för värdepapper och marknader som inrättats i enlighet med artikel 37 i Europaparlamentets och rådets förordning (EU) nr 1095/2010 ([5]).

(30) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([6]) och avgav ett yttrande den 20 augusti 2024.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Definitioner

I denna förordning gäller följande definitioner:

1. *ledningslag*: lag bestående av personal från den testade finansiella entiteten och, när så är relevant med hänsyn till omfattningen av den hotbildsstyrda penetrationstestningen, personal från dess tredjepartsleverantörer av tjänster och eventuella andra parter, vilket leder och hanterar testet.

2. *ledningslagets ledare*: den medarbetare hos den finansiella entiteten som ansvarar för genomförandet av all verksamhet som rör hotbildsstyrd penetrationstestning för den finansiella entiteten i samband med ett specifikt test.

3. *blått lag*: personal hos den finansiella entiteten och, när så är relevant, personal hos den finansiella entitetens tredjepartsleverantörer av tjänster och eventuella andra parter som anses relevanta med hänsyn till omfattningen av den hotbildsstyrda penetrationstestningen, som försvarar en finansiell entitets användning av nätverk och informationssystem genom att upprätthålla säkerheten gentemot simulerade eller verkliga angrepp och som inte känner till den hotbildsstyrda penetrationstestningen.

4. *blått lag-uppgifter*: uppgifter som normalt utförs av det blå laget, som driften av ett säkerhetscentrum (SOC, Security Operation Centre), IKT-infrastrukturtjänster, helpdesktjänster och incidenthanteringstjänster på operativ nivå.

5. *rött lag*: testare, interna eller externa, som anlitats för eller utsetts att genomföra en hotbildsstyrd penetrationstestning.

6. *lila lagövning*: en samarbetsinriktad testaktivitet som innefattar både testarna och det blå laget.

([3]) Europaparlamentets och rådets förordning (EU) nr 1093/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska bankmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/78/EG (EUT L 331, 15.12.2010, s. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Europaparlamentets och rådets förordning (EU) nr 1094/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska försäkrings- och tjänstepensionsmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/79/EG (EUT L 331, 15.12.2010, s. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Europaparlamentets och rådets förordning (EU) nr 1095/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska värdepappers- och marknadsmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/77/EG (EUT L 331, 15.12.2010, s. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

7. myndighet med ansvar för hotbildsstyrd penetrationstestning:

   a) en enda offentlig myndighet inom finanssektorn som har utsetts i enlighet med artikel 26.9 i förordning (EU) 2022/2554,

   b) den myndighet inom finanssektorn till vilken utförandet av vissa eller alla uppgifter kopplade till hotbildsstyrd penetrationstestning har delegerats i enlighet med artikel 26.10 i förordning (EU) 2022/2554, eller

   c) någon av de behöriga myndigheter som avses i artikel 46 i förordning (EU) 2022/2554.

8. *cybergrupp för hotbildsstyrd penetrationstestning*: personal inom myndigheterna med ansvar för hotbildsstyrd penetrationstestning som ansvarar för frågor som rör hotbildsstyrd penetrationstestning.

9. *testledare*: personal som utsetts att leda aktiviteterna hos myndigheten med ansvar för hotbildsstyrd penetrationstestning i fråga om en specifik hotbildsstyrd penetrationstestning för att övervaka efterlevnaden av denna förordning.

10. *leverantör av underrättelser om hot*: experter som anlitas av den finansiella entiteten för varje enskild hotbildsstyrd penetrationstestning som är externa i förhållande till den finansiella entiteten och eventuella koncerninterna IKT-tjänsteleverantörer, vilka samlar in och analyserar målinriktade underrättelser om hot som är relevanta för den finansiella entiteten sett till en specifik hotbildsstyrd penetrationstestning och tar fram matchande relevanta och realistiska hotscenarier.

11. *leverantörer av hotbildsstyrd penetrationstestning*: testare och leverantörer av underrättelser om hot.

12. *hjälpinsats*: den hjälp eller information som tillhandahålls av ledningslaget till testarna för att göra det möjligt för testarna att fortsätta genomförandet av en angreppsmetod när dessa inte klarar av att gå vidare på egen hand och när det inte finns något annat rimligt alternativ, i vilket innefattas brist på tid eller resurser i en specifik hotbildsstyrd penetrationstestning.

13. *angreppsmetod*: den väg som testarna följer under den aktiva rött lag-testfasen i den hotbildsstyrda penetrationstestningen för att nå de flaggor som specificerats för denna testning.

14. *flaggor*: centrala mål kopplade till de IKT-system som stöder en finansiell entitets kritiska eller viktiga funktioner vilka testarna försöker uppnå genom testet.

15. *känslig information*: information som lätt kan utnyttjas för att utföra angrepp mot den finansiella entitetens IKT-system, immateriella rättigheter, konfidentiella affärsdata eller personuppgifter, som direkt eller indirekt kan skada den finansiella entiteten och dess ekosystem om den skulle falla i händerna på fientliga aktörer.

16. *gemensam pool*: alla finansiella entiteter som deltar i en gemensam hotbildsstyrd penetrationstestning i enlighet med artikel 26.4 i förordning (EU) 2022/2554.

17. *värdmedlemsstat*: värdmedlemsstaten i enlighet med den sektorsspecifika unionsrätt som är tillämplig för varje finansiell entitet.

18. *samlad hotbildsstyrd penetrationstestning*: en annan hotbildsstyrd penetrationstestning än en gemensam hotbildsstyrd penetrationstestning enligt artikel 26.4 i förordning (EU) 2022/2554 som innefattar flera finansiella entiteter som använder samma koncerninterna IKT-tjänsteleverantör eller som tillhör samma koncern och delar IKT-system.

Artikel 2

Identifiering av finansiella entiteter som är skyldiga att genomföra hotbildsstyrd penetrationstestning

1. Myndigheter som ansvarar för hotbildsstyrd penetrationstestning ska bedöma huruvida finansiella entiteter är skyldiga att genomföra hotbildsstyrd penetrationstestning, med beaktande av dessa finansiella entiteters påverkan, betydelse för systemet och IKT-riskprofil, på grundval av samtliga av följande kriterier:

a) Faktorer relaterade till påverkan och till betydelse för systemet, enligt följande:

   i) Storleken på den finansiella entiteten, fastställd på grundval av huruvida den finansiella entiteten tillhandahåller finansiella tjänster i en eller flera medlemsstater och genom jämförelse av den finansiella entitetens verksamhet med verksamheten hos andra finansiella entiteter som tillhandahåller liknande tjänster.

   ii) Omfattningen och arten av den finansiella entitetens sammanlänkning med andra finansiella entiteter inom finanssektorn i en eller flera medlemsstater.

   iii) Hur pass kritiska eller viktiga de tjänster som den finansiella entiteten tillhandahåller finanssektorn är.

iv) Utbytbarheten hos de tjänster som den finansiella entiteten tillhandahåller.

v) Komplexiteten i den finansiella entitetens affärsmodell och tillhörande tjänster och processer.

vi) Huruvida den finansiella entiteten ingår i en koncern av betydelse för systemet på unionsnivå eller nationell nivå inom finanssektorn och delar IKT-system.

b) Faktorer relaterade till IKT-risk, enligt följande:

i) Den finansiella entitetens riskprofil.

ii) Den finansiella entitetens hotbild.

iii) Den finansiella entitetens grad av beroende av kritiska eller viktiga funktioner eller deras stödfunktioner sett till IKT-system och IKT-processer.

iv) Komplexiteten i den finansiella entitetens IKT-arkitektur.

v) De IKT-tjänster och IKT-funktioner som stöds av tredjepartsleverantörer av IKT-tjänster och kvantiteten och typen av kontraktsmässiga arrangemang med tredjepartsleverantörer av IKT-tjänster eller koncerninterna IKT-tjänsteleverantörer.

vi) Resultaten av eventuella tillsynsgranskningar som är relevanta för bedömningen av den finansiella entitetens IKT-mognad.

vii) Mognaden hos IKT-kontinuitetsplaner och åtgärds- och återställningsplaner avseende IKT.

viii) Mognaden hos de operativa upptäckts- och begränsningsåtgärderna för IKT-säkerhet, inbegripet förmågan att

1) permanent övervaka den finansiella entitetens IKT-infrastruktur,

2) upptäcka IKT-relaterade händelser i realtid,

3) analysera de händelser som avses i punkt 2,

4) reagera på de händelser som avses i punkt 2 på ett skyndsamt och effektivt sätt.

ix) Huruvida den finansiella entiteten ingår i en koncern som är verksam inom finanssektorn på unionsnivå eller nationell nivå och som delar IKT-system.

Vid tillämpning av led a i ska myndigheten med ansvar för hotbildsstyrd penetrationstestning om möjligt beakta

a) den finansiella entitetens marknadsandel på unionsnivå och nationell nivå,

b) utbudet av verksamheter som erbjuds av den finansiella entiteten,

c) marknadsandelen för de tjänster som tillhandahålls av den finansiella entiteten eller för de verksamheter som bedrivs på unionsnivå och nationell nivå.

Vid tillämpning av led a v ska myndigheten med ansvar för hotbildsstyrd penetrationstestning om möjligt beakta

a) huruvida den finansiella entiteten använder mer än en affärsmodell,

b) sammanlänkningen av olika affärsprocesser och tillhörande tjänster.

2. Myndigheter med ansvar för hotbildsstyrd penetrationstestning ska kräva att alla följande finansiella entiteter genomför hotbildsstyrd penetrationstestning, såvida inte den bedömning som avses i punkt 1 i fråga om en finansiell entitet indikerar att dess påverkan, riskerna för den finansiella stabiliteten kopplade till den finansiella entiteten eller dess IKT-riskprofil inte motiverar genomförandet av en hotbildsstyrd penetrationstestning:

a) Kreditinstitut som uppfyller något av följande villkor:

i) De har identifierats som globala systemviktiga institut (G-SII) i enlighet med artikel 131 i Europaparlamentets och rådets direktiv 2013/36/EU ([7]).

ii) De har identifierats som andra systemviktiga institut (O-SII) i enlighet med artikel 131 i direktiv 2013/36/EU.

iii) De utgör delar av globala systemviktiga institut eller andra systemviktiga institut.

([7]) Europaparlamentets och rådets direktiv 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut, om ändring av direktiv 2002/87/EG och om upphävande av direktiven 2006/48/EG och 2006/49/EG (EUT L 176, 27.6.2013, s. 338, ELI: http://data.europa.eu/eli/dir/2013/36/oj).

b) Betalningsinstitut som under vart och ett av de två kalenderår som föregick bedömningen av myndigheten med ansvar för hotbildsstyrd penetrationstestning hade betalningstransaktioner, enligt definitionen i artikel 4.5 i Europaparlamentets och rådets direktiv (EU) 2015/2366 ([8]), till ett totalt värde som översteg 150 miljarder euro.

c) Institut för elektroniska pengar som under vart och ett av de två kalenderår som föregick bedömningen av myndigheten med ansvar för hotbildsstyrd penetrationstestning antingen hade betalningstransaktioner, enligt definitionen i artikel 4.5 i direktiv (EU) 2015/2366, till ett totalt värde som översteg 150 miljarder euro eller hade utestående elektroniska pengar till ett totalt värde som översteg 40 miljarder euro.

d) Värdepapperscentraler.

e) Centrala motparter.

f) Handelsplatser med ett elektroniskt handelssystem som uppfyller något av följande kriterier:

i) Handelsplatsen hade den största marknadsandelen sett till omsättning på nationell nivå under vart och ett av de två kalenderår som föregick bedömningen av myndigheten med ansvar för hotbildsstyrd penetrationstestning i fråga om något av följande:

1. Överlåtbara värdepapper enligt definitionen i artikel 4.1.44 a i Europaparlamentets och rådets direktiv 2014/65/EU ([9]).

2. Överlåtbara värdepapper enligt definitionen i artikel 4.1.44 b i direktiv 2014/65/EU.

3. Derivat enligt definitionen i artikel 2.1.29 i Europaparlamentets och rådets förordning (EU) nr 600/2014 ([10]).

4. Strukturerade finansiella produkter enligt definitionen i artikel 2.1.28 i förordning (EU) nr 600/2014.

5. Utsläppsrätter enligt avsnitt C.11 i bilaga I till direktiv 2014/65/EU.

ii) Handelsplatsen hade en marknadsandel sett till omsättning på unionsnivå som översteg 5 % under vart och ett av de två kalenderår som föregick bedömningen av myndigheten med ansvar för hotbildsstyrd penetrationstestning i fråga om något av följande:

1. Aktier och andra värdepapper som motsvarar andelar i aktiebolag, bolag med personligt ansvar eller andra entiteter samt depåbevis för aktier.

2. Obligationer eller andra former av skuldförbindelser i värdepappersform, inbegripet depåbevis för sådana värdepapper.

3. Derivat enligt definitionen i artikel 2.1.29 i förordning (EU) nr 600/2014.

4. Strukturerade finansiella produkter enligt definitionen i artikel 2.1.28 i förordning (EU) nr 600/2014.

5. Utsläppsrätter enligt avsnitt C.11 i bilaga I till direktiv 2014/65/EU.

([8]) Europaparlamentets och rådets direktiv (EU) 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG (EUT L 337, 23.12.2015, s. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

([9]) Europaparlamentets och rådets direktiv 2014/65/EU av den 15 maj 2014 om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG och av direktiv 2011/61/EU (EUT L 173, 12.6.2014, s. 349, ELI: http://data.europa.eu/eli/dir/2014/65/oj).

([10]) Europaparlamentets och rådets förordning (EU) nr 600/2014 av den 15 maj 2014 om marknader för finansiella instrument och om ändring av förordning (EU) nr 648/2012 (EUT L 173, 12.6.2014, s. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

g) Försäkrings- och återförsäkringsföretag som uppfyller samtliga av följande kriterier:

i) De har en bruttopremieinkomst (GWP) som överstiger 1 500 000 000 euro.

ii) De har försäkringstekniska avsättningar som överstiger 10 000 000 000 euro.

iii) Försäkringsföretag som endast bedriver livförsäkringsverksamhet eller som bedriver både livförsäkrings- och skadeförsäkringsverksamhet och som har totala tillgångar som överstiger 3,5 % av summan av de totala tillgångarna, värderade i enlighet med artikel 75 i Europaparlamentets och rådets direktiv 2009/138/EG ([11]), för de försäkrings- och återförsäkringsföretag som är etablerade i medlemsstaten.

Vid tillämpning av led f ii ska, om handelsplatsen är en del av en koncern som delar IKT-system eller samma koncerninterna IKT-tjänsteleverantör, omsättningen av värdepapper och derivatavtal på alla handelsplatser som tillhör samma koncern och som är etablerade i unionen räknas med.

Vid tillämpning av led g ska myndigheter med ansvar för hotbildsstyrd penetrationstestning identifiera en undergrupp av alla försäkrings- och återförsäkringsföretag genom att tillämpa de kriterier som anges i leden g i, ii och iii. Försäkrings- och återförsäkringsföretag som ingår i denna undergrupp ska vara skyldiga att genomföra hotbildsstyrd penetrationstestning om de även uppfyller något av följande kriterier:

a) Bruttopremieinkomst (GWP) som överstiger 3 000 000 000 euro.

b) Tekniska avsättningar som överstiger 30 000 000 000 euro.

c) Totala tillgångar som överstiger 10 % av summan av de totala tillgångarna, värderade i enlighet med artikel 75 i direktiv 2009/138/EG, för de försäkrings- och återförsäkringsföretag som är etablerade i medlemsstaten.

3. Om fler än en finansiell entitet som tillhör samma koncern och delar IKT-system, eller om fler än en finansiell entitet som använder samma koncerninterna IKT-tjänsteleverantör, uppfyller de kriterier som anges i punkt 2 ska myndigheterna med ansvar för hotbildsstyrd penetrationstestning för dessa finansiella entiteter i enlighet med artikel 16.2 besluta huruvida kravet att genomföra hotbildsstyrd penetrationstestning på individuell nivå är relevant för dessa finansiella entiteter.

Om myndigheten med ansvar för hotbildsstyrd penetrationstestning för moderföretaget för en koncern med finansiella entiteter som avses i första stycket är en annan myndighet än myndigheterna med ansvar för hotbildsstyrd penetrationstestning för de finansiella entiteterna i koncernen ska denna myndighet rådfrågas av myndigheterna med ansvar för hotbildsstyrd penetrationstestning för de finansiella entiteterna som ingår i denna koncern huruvida det är lämpligt att genomföra hotbildsstyrd penetrationstestning på individuell nivå.

Artikel 3

Cybergrupp för hotbildsstyrd penetrationstestning och testledare för hotbildsstyrd penetrationstestning

1. En myndighet med ansvar för hotbildsstyrd penetrationstestning ska tilldela ansvaret för att samordna verksamheter kopplade till hotbildsstyrd penetrationstestning till en cybergrupp för hotbildsstyrd penetrationstestning. En cybergrupp för hotbildsstyrd penetrationstestning ska bestå av testledare som har till uppgift att övervaka en enskild hotbildsstyrd penetrationstestning.

2. För varje test ska myndigheten med ansvar för hotbildsstyrd penetrationstestning utse en testledare och minst en reserv.

3. Testledarna ska övervaka huruvida kraven i denna förordning uppfylls och säkerställa att de uppfylls.

([11]) Europaparlamentets och rådets direktiv 2009/138/EG av den 25 november 2009 om upptagande och utövande av försäkrings- och återförsäkringsverksamhet (Solvens II) (EUT L 335, 17.12.2009, s. 1, ELI: http://data.europa.eu/eli/dir/2009/138/oj).

4. Testledaren ska meddela kontaktuppgifterna för cybergruppen för hotbildsstyrd penetrationstestning till den finansiella entiteten genom den underrättelsefunktion som avses i artikel 9.1.

5. Myndigheten med ansvar för hotbildsstyrd penetrationstestning ska delta i alla faser av den hotbildsstyrda penetrationstestningen.

Artikel 4

Organisatoriska arrangemang för finansiella entiteter

1. Finansiella entiteter ska utse en ledare för ledningslaget som ska ansvara för den dagliga ledningen av den hotbildsstyrda penetrationstestningen och för ledningslagets beslut och åtgärder.

2. Finansiella entiteter ska upprätta organisatoriska och procedurrelaterade åtgärder för att säkerställa att

a) tillgången till information om planerad eller pågående hotbildsstyrd penetrationstestning på behovsenlig grund är begränsad till ledningslaget, ledningsorganet, testarna, leverantören av underrättelser om hot och myndigheten med ansvar för hotbildsstyrd penetrationstestning,

b) ledningslaget samråder med testledarna innan någon medlem av det blå laget involveras i en hotbildsstyrd penetrationstestning,

c) ledningslaget informeras om eventuell upptäckt av den hotbildsstyrda penetrationstestningen som görs av personal inom den finansiella entiteten eller dess tredjepartsleverantörer av tjänster, ledningslaget i händelse av eskalering av den resulterande incidenthanteringen vid behov begränsar sådan eskalering,

d) det finns arrangemang rörande sekretessen kring den hotbildsstyrda penetrationstestningen som är tillämpliga för den finansiella entitetens personal, personalen hos berörda tredjepartsleverantörer av IKT-tjänster, testare och leverantören av underrättelser om hot,

e) ledningslaget på begäran tillhandahåller all information rörande den hotbildsstyrda penetrationstestningen till testledarna,

f) de parter som deltar i den hotbildsstyrda penetrationstestningen om möjligt endast hänvisar till den med kodnamn.

Artikel 5

Riskhantering i samband med hotbildsstyrd penetrationstestning

1. Under den förberedelsefas som avses i artikel 9 ska ledningslaget bedöma de risker som är förknippade med testning av produktionssystem i drift för den finansiella entitetens kritiska eller viktiga funktioner, inbegripet potentiell påverkan på

a) finanssektorn,

b) den finansiella stabiliteten på unionsnivå eller nationell nivå.

Ledningslaget ska granska denna påverkan under hela testningen.

2. Vid riskbedömningen och riskhanteringen ska ledningslaget åtminstone beakta följande typer av riskområden:

a) Beviljande av tillgång till känslig information om den finansiella entiteten, i tillämpliga fall, till leverantören av underrättelser om hot och externa testare.

b) Bristande efterlevnad inom den hotbildsstyrda penetrationstestningen av förordning (EU) 2022/2554 och den här förordningen, där sådan bristande efterlevnad leder till att det intyg som avses i artikel 26.7 i förordning (EU) 2022/2554 inte tillhandahålls, inklusive när sådan bristande efterlevnad beror på överträdelser av konfidentialiteten rörande den hotbildsstyrda penetrationstestningen eller på bristande etiskt uppförande.

c) Eskalering av kriser och incidenter.

d) Den aktiva rött lag-fasen, inbegripet risker i samband med avbrott i kritisk verksamhet och korruption av data till följd av testarnas verksamhet, samt dess potentiella påverkan på tredje parter.

e) Det blå lagets verksamhet, inbegripet risker i samband med avbrott i kritisk verksamhet och korruption av data till följd av det blå lagets verksamhet, samt dess potentiella påverkan på tredje parter.

f) Ofullständig återställning av system som påverkats av den hotbildsstyrda penetrationstestningen.

Artikel 6

Riskhantering i samband med gemensam eller samlad hotbildsstyrd penetrationstestning

1. När det rör sig om en gemensam hotbildsstyrd penetrationstestning eller en samlad hotbildsstyrd penetrationstestning ska ledningslaget för varje finansiell entitet genomföra sin egen riskbedömning och upprätta sina egna riskhanteringsåtgärder.

2. Ledningslaget för den utsedda finansiella entitet som avses i artikel 16.3 b i denna förordning eller den finansiella entitet som utsetts i enlighet med artikel 26.4 i förordning (EU) 2022/2554 ska bedöma riskerna i samband med att flera finansiella entiteter deltar i den hotbildsstyrda penetrationstestningen. De deltagande finansiella entiteternas ledningslag ska samarbeta med den utsedda finansiella entitetens ledningslag för att identifiera potentiella gemensamma risker.

Artikel 7

Val av leverantörer av hotbildsstyrd penetrationstestning

1. Ledningslaget ska vidta åtgärder för att hantera riskerna i samband med hotbildsstyrd penetrationstestning och ska särskilt se till att följande gäller för varje hotbildsstyrd penetrationstestning:

a) Leverantören av underrättelser om hot och externa testare förser ledningslaget med en detaljerad meritförteckning och kopior av certifieringar som, enligt erkänd marknadspraxis, är lämpliga för utförandet av deras verksamhet.

b) Leverantören av underrättelser om hot och externa testare omfattas på vederbörligt sätt och fullt ut av lämpliga yrkesmässiga ansvarsförsäkringar, bland annat mot risker rörande tjänstefel och försummelse.

c) Leverantören av underrättelser om hot tillhandahåller minst tre referenser från tidigare uppdrag kopplade till penetrationstestning och rött lag-testning.

d) De externa testarna tillhandahåller minst fem referenser från tidigare uppdrag kopplade till penetrationstestning och rött lag-testning.

e) Följande gäller för personalen hos leverantören av underrättelser om hot som har utsetts att arbeta med den hotbildsstyrda penetrationstestningen:

   i) Personalen består av minst en ledare med åtminstone fem års erfarenhet av underrättelser om hot och minst en ytterligare medlem med åtminstone två års erfarenhet av underrättelser om hot.

   ii) Personalen uppvisar en bred uppsättning och en lämplig nivå av yrkesmässiga kunskaper och färdigheter, däribland inom följande områden:

      1. Taktiker, teknik och förfaranden för insamling av underrättelser.

      2. Geopolitisk, teknisk och sektorsspecifik kunskap.

      3. Tillräcklig kommunikationsförmåga för att på ett tydligt sätt kunna presentera och rapportera resultatet av uppdraget.

   iii) Personalen har tillsammans deltagit i minst tre tidigare uppdrag inom underrättelser om hot kopplade till penetrationstestning och rött lag-testning.

   iv) Personalen utför inte samtidigt några blått lag-uppgifter eller andra tjänster som kan utgöra en intressekonflikt med koppling till den finansiella entiteten, tredjepartsleverantören av IKT-tjänster eller en koncernintern IKT-tjänsteleverantör som deltar i den hotbildsstyrda penetrationstestning som personalen har utsetts att arbeta med.

   v) Personalen är åtskild från och rapporterar inte till personal hos samma leverantör av hotbildsstyrd penetrationstestning som tillhandahåller externa testare för denna hotbildsstyrda penetrationstestning.

f) För externa testare gäller följande för det röda lag som har utsetts för den hotbildsstyrda penetrationstestningen:

i) Laget består av minst en ledare med åtminstone fem års erfarenhet av penetrationstestning och rött lag-testning samt minst två ytterligare testare, var och en med åtminstone två års erfarenhet av penetrationstestning och rött lag-testning.

ii) Laget uppvisar en bred uppsättning och en lämplig nivå av yrkesmässiga kunskaper och färdigheter, däribland kunskaper om den finansiella entitetens verksamhet, rekognosering, riskhantering, utarbetande av angrepp mot sårbarheter, fysisk penetration, social manipulering, sårbarhetsanalys samt tillräcklig kommunikationsförmåga för att på ett tydligt sätt kunna presentera och rapportera resultatet av uppdraget.

iii) Laget har tillsammans deltagit i minst fem tidigare uppdrag kopplade till penetrationstestning och rött lag-testning.

iv) Laget är inte är anställt av och tillhandahåller inte tjänster till en leverantör av underrättelser om hot som samtidigt utför blått lag-uppgifter för antingen en finansiell entitet, en tredjepartsleverantör av IKT-tjänster eller en koncernintern IKT-tjänsteleverantör som deltar i den hotbildsstyrda penetrationstestningen.

v) Laget är åtskilt från all personal hos samma leverantör av hotbildsstyrd penetrationstestning som samtidigt tillhandahåller tjänster rörande underrättelser om hot för samma hotbildsstyrda penetrationstestning.

g) Testarna och leverantören av underrättelser om hot utför återställningsförfaranden i slutet av testningen, vilket innefattar säker radering av uppgifter rörande lösenord, identifieringsinformation och andra privata nycklar som angripits under den hotbildsstyrda penetrationstestningen, säker kommunikation till de finansiella entiteterna kring de konton som angripits och säker insamling, lagring, hantering och radering av andra data som samlats in under testningen.

h) Testarna utför, utöver de återställningsförfaranden i slutet av testningen som avses i led g, följande återställningsförfaranden:

i) Inaktivering av kanaler för fjärrstyrning (*command and control*).

ii) Nödbrytare (*kill switches*) baserade på omfattning och datum.

iii) Borttagning av bakdörrar och andra sabotageprogram.

iv) Avisering av potentiella säkerhetsöverträdelser.

v) Förfaranden för framtida återställning av säkerhetskopierade data som kan avse sabotageprogram eller verktyg som installerats under testet.

vi) Övervakning av det blå lagets aktiviteter och information till ledningslaget om eventuella möjliga upptäckter.

i) Testare och leverantören av underrättelser om hot utför inte, och deltar inte i, någon av följande verksamheter:

i) Obehörig förstörelse av utrustning som tillhör den finansiella entiteten eller, i förekommande fall, dess tredjepartsleverantörer av IKT-tjänster.

ii) Okontrollerad ändring av information och IKT-tillgångar som tillhör den finansiella entiteten eller, i förekommande fall, dess tredjepartsleverantörer av IKT-tjänster.

iii) Avsiktligt äventyrande av kontinuiteten hos den finansiella entitetens kritiska eller viktiga funktioner.

iv) Otillåten inkludering av system som ligger utanför den avsedda omfattningen.

v) Obehörigt yppande av testresultat.

2. Ledningslaget ska föra register över den dokumentation som tillhandahålls av testarna och leverantörerna av underrättelser om hot för att styrka efterlevnaden av punkt 1 led a–f.

Under exceptionella omständigheter får finansiella entiteter anlita externa testare och leverantörer av underrättelser om hot som inte uppfyller ett eller flera av kraven i punkt 1 led a–f, förutsatt att dessa finansiella entiteter vidtar lämpliga åtgärder för att minska riskerna kopplade till bristande efterlevnad av dessa led och dokumenterar dessa åtgärder.

Artikel 8

Särskilda specifikationer för gemensam eller samlad hotbildsstyrd penetrationstestning

1. Om flera finansiella entiteter, identifierade i enlighet med artikel 16.2 eller 16.4, deltar i en gemensam eller samlad hotbildsstyrd penetrationstestning ska varje finansiell entitet, om inte annat beslutas av den ledande myndigheten med ansvar för hotbildsstyrd penetrationstestning, följa vart och ett av de steg som anges i artiklarna 9–15.

2. Om flera myndigheter med ansvar för hotbildsstyrd penetrationstestning deltar i en samlad hotbildsstyrd penetrationstestning eller i en gemensam hotbildsstyrd penetrationstestning i enlighet med artikel 16.3 eller 16.5 ska, om inte annat föreskrivs i denna förordning, hänvisningar i artiklarna 9–15 till ”myndigheten med ansvar för hotbildsstyrd penetrationstestning” förstås som en hänvisning till den ledande myndigheten med ansvar för hotbildsstyrd penetrationstestning för en sådan gemensam eller samlad hotbildsstyrd penetrationstestning.

Artikel 9

Förberedelsefasen

1. En finansiell entitet som identifierats i enlighet med artikel 26.8 tredje stycket i förordning (EU) 2022/2554 ska inleda en hotbildsstyrd penetrationstestning efter en underrättelse från myndigheten med ansvar för hotbildsstyrd penetrationstestning att en testning ska genomföras.

2. En finansiell entitet ska, inom tre månader från mottagandet av den underrättelse som avses i punkt 1, lämna all följande information om inledning av hotbildsstyrd penetrationstestning till testledarna:

a) En projektbeskrivning med en översiktlig projektplan som innehåller den information som anges i bilaga I.

b) Kontaktuppgifter för ledningslagets ledare.

c) Information om den avsedda användningen av interna eller externa testare eller bådadera, när detta är relevant i enlighet med artikel 15.

d) Information om de kommunikationskanaler som ska användas under den hotbildsstyrda penetrationstestningen.

e) Kodnamnet för den hotbildsstyrda penetrationstestningen.

3. Om den information som avses i punkt 2 a–e är fullständig och säkerställer att testningen är lämplig och effektiv ska myndigheten med ansvar för hotbildsstyrd penetrationstestning validera den finansiella entitetens information om inledning av testning och underrätta den finansiella entiteten om detta.

4. Efter det att myndigheten med ansvar för hotbildsstyrd penetrationstestning har validerat informationen om inledning av testning ska den finansiella entiteten inrätta ett ledningslag som ska hjälpa ledningslagets ledare i arbetet med att

a) specificera kommunikationskanaler och kommunikationsprocesser inom ledningslaget och gentemot testarna och leverantörerna av underrättelser om hot inom alla frågor som rör den hotbildsstyrda penetrationstestningen,

b) informera den finansiella entitetens ledningsorgan om fortskridandet av den hotbildsstyrda penetrationstestningen och de därmed sammanhörande riskerna,

c) fatta beslut på grundval av sakkunskap genom hela den hotbildsstyrda penetrationstestningen,

d) genomföra den hotbildsstyrda penetrationstestningen i enlighet med denna förordning,

e) välja leverantör av underrättelser om hot för den hotbildsstyrda penetrationstestningen,

f) välja externa testare, interna testare eller bådadera,

g) utarbeta omfattningsdokumentet.

5. Om myndigheten med ansvar för hotbildsstyrd penetrationstestning anser att ledningslagets ursprungliga sammansättning och eventuella senare ändringar av denna sammansättning är tillfyllest för utförandet av de uppgifter som avses i punkt 4 ska myndigheten med ansvar för hotbildsstyrd penetrationstestning validera ledningslaget och underrätta ledningslagets ledare om detta.

6. Den finansiella entiteten ska överlämna ett omfattningsdokument som ska innehålla all information som anges i bilaga II till testledarna inom sex månader från mottagandet av den underrättelse från myndigheten med ansvar för hotbildsstyrd penetrationstestning som avses i punkt 1. Den finansiella entitetens ledningsorgan ska godkänna omfattningsdokumentet.

7. Finansiella entiteter ska beakta följande kriterier för att avgöra om kritiska eller viktiga funktioner ska omfattas av den hotbildsstyrda penetrationstestningen:

a) I vilken grad funktionen är kritisk eller viktig och dess möjliga påverkan på finanssektorn och på den finansiella stabiliteten på unionsnivå och nationell nivå.

b) Funktionens betydelse för den finansiella entitetens dagliga verksamhet.

c) Funktionens utbytbarhet.

d) Sammanlänkningen med andra funktioner.

e) Funktionens geografiska plats.

f) Andra entiteters sektorsspecifika beroende av funktionen.

g) Underrättelser om hot rörande funktionen, om sådana finns.

8. Ledningslaget ska dela informationen om inledning av testning och omfattningsdokumentet med testarna och leverantörerna av underrättelser om hot när dessa har anlitats. Ledningslaget ska informera testarna och leverantörerna av underrättelser om hot om den testprocess som ska följas.

9. Den finansiella entiteten ska säkerställa att kontrakteringen eller utnämningen av testare och leverantörer av underrättelser om hot är slutförd innan testfasen inleds.

10. Innan testfasen inleds ska ledningslaget samråda med testledarna om riskbedömningen rörande den hotbildsstyrda penetrationstestningen och om riskhanteringsåtgärderna. Ledningslaget ska se över riskbedömningen eller riskhanteringsåtgärderna om myndigheten med ansvar för hotbildsstyrd penetrationstestning anser att dessa inte på ett tillfredsställande sätt bemöter riskerna med den hotbildsstyrda penetrationstestningen.

11. Ledningslaget ska bedöma om leverantörer av underrättelser om hot och testare som ledningslaget överväger att engagera i den hotbildsstyrda penetrationstestningen uppfyller kraven i artikel 27 i förordning (EU) 2022/2554 och artikel 7.1 i den här förordningen och dokumentera resultatet av denna bedömning. Ledningslaget ska välja leverantörer av underrättelser om hot i enlighet med denna bedömning och i enlighet med dess riskhanteringsrutiner. Innan de utvalda leverantörerna av underrättelser om hot och de externa testarna anlitas ska ledningslaget förse testledarna med bevis på att dessa leverantörer av underrättelser om hot och testare uppfyller kraven i artikel 27 i förordning (EU) 2022/2554 och artikel 7.1 i den här förordningen. Ledningslaget får inte ingå avtal med de utvalda leverantörerna av underrättelser om hot och de externa testarna om myndigheten med ansvar för hotbildsstyrd penetrationstestning anser att de utvalda leverantörerna av underrättelser om hot och de externa testarna inte uppfyller kraven i artikel 27 i förordning (EU) 2022/2554 eller kraven i artikel 7.1 i den här förordningen eller andra krav som härrör från nationell säkerhetslagstiftning i enlighet med unionsrätten, eller om den finansiella entiteten inte uppfyller kraven i artikel 7.2 första stycket i den här förordningen eller om de omständigheter som avses i artikel 7.2 andra stycket i den här förordningen inte uppfylls.

12. Om omfattningsdokumentet är fullständigt och säkerställer att en lämplig och effektiv hotbildsstyrd penetrationstestning kan genomföras ska myndigheten med ansvar för hotbildsstyrd penetrationstestning godkänna detta dokument och informera ledningslagets ledare om detta.

Artikel 10

Testfasen: underrättelser om hot

1. Efter det att myndigheten med ansvar för hotbildsstyrd penetrationstestning har godkänt omfattningsdokumentet ska leverantören av underrättelser om hot analysera allmänna och sektorsspecifika underrättelser om hot som är av relevans för den finansiella entiteten. Om en allmän hotbild har tillhandahållits av myndigheten med ansvar för hotbildsstyrd penetrationstestning för finanssektorn i en medlemsstat får leverantören av underrättelser om hot använda denna hotbild som utgångspunkt för den nationella hotbilden. Leverantören av underrättelser om hot ska identifiera cyberhot och befintliga eller potentiella sårbarheter som berör den finansiella entiteten. Därutöver ska leverantören av underrättelser om hot samla in information om och analysera konkreta, praktiskt användbara och situationsanpassade underrättelser om mål och hot som rör den finansiella entiteten, bland annat genom samråd med ledningslaget och testledarna.

2. Leverantören av underrättelser om hot ska presentera relevanta hot och målinriktade underrättelser om hot och föreslå erforderliga scenarier för ledningslaget, testarna och testledarna. De föreslagna scenarierna ska skilja sig åt med avseende på de identifierade fientliga aktörerna och tillhörande taktiker, teknik och förfaranden och ska vara inriktade på varje kritisk eller viktig funktion som omfattas av den hotbildsstyrda penetrationstestningen.

3. Ledningslagets ledare ska välja ut minst tre scenarier, med syftet att genomföra den hotbildsstyrda penetrationstestningen baserat på samtliga av följande element:

a) Rekommendationen från leverantören av underrättelser om hot och den hotbildsstyrda karaktären hos varje scenario.

b) Uppgifter från testledarna.

c) Möjligheten att genomföra de föreslagna scenarierna, baserat på en expertbedömning från testarnas sida.

d) Den finansiella entitetens storlek, komplexitet och övergripande riskprofil samt typen av, omfattningen hos och komplexiteten av dess tjänster, aktiviteter och verksamheter.

4. Högst ett av de utvalda scenarierna får vara ej hotbildsstyrt och får baseras på ett framåtblickande och potentiellt fiktivt hot med hög rimlighet i fråga om förutsägelse, antagande, förmodan eller förväntan med tanke på den förväntade utvecklingen av hotbilden för den finansiella entiteten.

För gemensam hotbildsstyrd penetrationstestning ska, utan att det påverkar användningen av scenarier som är direkt inriktade på de kritiska eller viktiga funktionerna hos de finansiella entiteter som deltar i testningen, minst ett scenario omfatta relevanta underliggande IKT-system och IKT-processer och relevant underliggande IKT-teknik från tredjepartsleverantören av IKT-tjänster som stöder de kritiska eller viktiga funktionerna hos de finansiella entiteter som omfattas.

Om testningen är en samlad hotbildsstyrd penetrationstestning som innefattar en koncernintern IKT-tjänsteleverantör ska, utan att det påverkar användningen av scenarier som är direkt inriktade på de kritiska eller viktiga funktionerna hos de finansiella entiteter som deltar i testet, minst ett scenario omfatta den koncerninterna IKT-tjänsteleverantörens relevanta underliggande IKT-system och IKT-processer och relevant underliggande IKT-teknik som stöder de kritiska eller viktiga funktionerna hos de finansiella entiteter som omfattas.

5. Leverantören av underrättelser om hot ska lämna den målinriktade hotunderrättelserapporten till ledningslaget, inbegripet de scenarier som valts ut i enlighet med punkterna 3 och 4. Hotunderrättelserapporten ska innehålla den information som anges i bilaga III.

6. Ledningslaget ska överlämna den målinriktade hotunderrättelserapporten till testledaren för godkännande. Om den målinriktade hotunderrättelserapporten är fullständig och säkerställer att en effektiv hotbildsstyrd penetrationstestning kan genomföras ska myndigheten med ansvar för hotbildsstyrd penetrationstestning godkänna rapporten och informera ledningslagets ledare om detta.

Artikel 11

Testfasen: rött lag-testning

1. Efter det att myndigheten med ansvar för hotbildsstyrd penetrationstestning har godkänt den målinriktade hotunderrättelserapporten ska testarna utarbeta planen för rött lag-testning som ska innehålla den information som anges i bilaga IV. Testarna ska använda omfattningsdokumentet och den målinriktade hotunderrättelserapporten som grund för att ta fram angreppsscenarierna.

2. Testarna ska samråda med ledningslaget, leverantören av underrättelser om hot och testledarna om planen för rött lag-testning, inbegripet arrangemangen för kommunikation, rutiner och projektledning, förberedelserna och användningsfallen för hjälpinsatser, samt överenskommelserna kring rapportering till ledningslaget och testledarna.

3. Om planen för rött lag-testning är fullständig och säkerställer att en effektiv hotbildsstyrd penetrationstestning kan genomföras ska ledningslaget och myndigheten med ansvar för hotbildsstyrd penetrationstestning godkänna planen för rött lag-testning och myndigheten med ansvar för hotbildsstyrd penetrationstestning ska informera ledningslagets ledare om detta.

4. Efter godkännande av planen för rött lag-testning i enlighet med punkt 3 ska testarna genomföra den hotbildsstyrda penetrationstestningen under den aktiva rött lag-testfasen.

5. Varaktigheten för den aktiva rött lag-testfasen ska stå i proportion till den hotbildsstyrda penetrationstestningens omfattning och till de finansiella entiteter och tredjepartsleverantörer av IKT-tjänster eller koncerninterna IKT-tjänsteleverantörer som deltar i den hotbildsstyrda penetrationstestningen vad gäller deras storlek, verksamheter, komplexitet och antal, och ska under alla omständigheter sträcka sig över minst tolv veckor. Angreppsscenarier får genomföras i följd eller samtidigt. Ledningslaget, leverantören av underrättelser om hot, testarna och testledarna ska komma överens om slutet på den aktiva rött lag-testfasen.

6. Förutsatt att det säkerställs att planen för rött lag-testning förblir fullständig och gör det möjligt att genomföra en effektiv hotbildsstyrd penetrationstestning ska ledningslagets ledare och testledarna godkänna alla eventuella ändringar av planen för rött lag-testning som görs efter dess godkännande, inbegripet dess tidsplan, omfattning, målsystem eller flaggor.

7. Under hela den aktiva rött lag-testfasen ska testarna minst en gång i veckan rapportera till ledningslaget och testledarna om de framsteg som gjorts inom den hotbildsstyrda penetrationstestningen, och leverantören av underrättelser om hot ska vara tillgänglig för rådfrågning och ytterligare underrättelser om hot på begäran av ledningslaget.

8. Ledningslaget ska i rätt tid tillhandahålla hjälpinsatser som tagits fram utifrån planen för rött lag-testning. Hjälpinsatser får läggas till eller anpassas efter godkännande av ledningslaget och testledarna.

9. Om någon anställd vid den finansiella entiteten eller inom dess tredjepartsleverantörer av IKT-tjänster eller dess koncerninterna IKT-tjänsteleverantör upptäcker testverksamheten ska ledningslaget, när så är relevant och i samråd med testarna och utan att det påverkar tillämpningen av punkt 10, föreslå åtgärder som gör det möjligt att fortsätta den hotbildsstyrda penetrationstestningen samtidigt som dess sekretess säkerställs, och lägga fram dem till testledarna för validering.

10. Under exceptionella omständigheter som medför risker för påverkan på data, skador på tillgångar och avbrott i kritiska eller viktiga funktioner, tjänster eller verksamheter för den finansiella entiteten själv, dess tredjepartsleverantörer av IKT-tjänster eller dess koncerninterna IKT-tjänsteleverantörer eller för störningar av den finansiella entitetens motparter eller finanssektorn får ledningslagets ledare avbryta den hotbildsstyrda penetrationstestningen eller, som en sista utväg om det inte är möjligt att fortsätta testningen på annat sätt och med godkännande på förhand från myndigheten med ansvar för hotbildsstyrd penetrationstestning, fortsätta testningen i form av en begränsad lila lagövning. Längden på den begränsade lila lagövningen ska räknas med i den minimilängd på tolv veckor för den aktiva rött lag-testfasen som anges i punkt 5.

Artikel 12

Avslutningsfasen

1. Efter slutet av den aktiva rött lag-testfasen ska ledningslagets ledare informera det blå laget om att en hotbildsstyrd penetrationstestning har ägt rum.

2. Inom fyra veckor från slutet av den aktiva rött lag-testfasen ska testarna överlämna det röda lagets testrapport till ledningslaget med de uppgifter som anges i bilaga V.

3. Ledningslaget ska utan onödigt dröjsmål lämna det röda lagets testrapport till det blå laget och testledarna.

Om testledarna begär det ska den rapport som avses i det första stycket inte innehålla någon känslig information.

4. Efter att ha mottagit det röda lagets testrapport, och senast tio veckor efter det att den aktiva rött lag-testfasen avslutades, ska det blå laget överlämna blå lagets testrapport till ledningslaget med de uppgifter som anges i bilaga VI. Ledningslaget ska utan onödigt dröjsmål lämna blå lagets testrapport till testarna och testledarna.

Om testledarna begär det ska den rapport som avses i det första stycket inte innehålla någon känslig information.

5. Senast tio veckor efter det att den aktiva rött lag-testfasen avslutades ska det blå laget och testarna gå igenom de offensiva och defensiva åtgärder som utfördes under den hotbildsstyrda penetrationstestningen. Ledningslaget ska också genomföra en lila lagövning kring ämnen som identifierats gemensamt av det blå laget och testarna baserat på sårbarheter som identifierades under testet och, i förekommande fall, kring aspekter som inte kunde testas under den aktiva rött lag-testfasen.

6. När genomgången av åtgärderna och den lila lagövningen har slutförts ska ledningslaget, det blå laget, testarna och leverantörerna av underrättelser om hot ge varandra återkoppling om processen runt den hotbildsstyrda penetrationstestningen. Testledarna har möjlighet att ge återkoppling.

7. När myndigheten med ansvar för hotbildsstyrd penetrationstestning har underrättat ledningslagets ledare om att den har bedömt att det blå lagets testrapport och det röda lagets testrapport innehåller de uppgifter som anges i bilagorna V och VI, ska den finansiella entiteten inom åtta veckor i enlighet med artikel 26.6 i förordning (EU) 2022/2554 lämna in en rapport som sammanfattar de relevanta resultaten av den hotbildsstyrda penetrationstestningen, med de uppgifter som anges i bilaga VII, till myndigheten för godkännande.

Om myndigheten med ansvar för hotbildsstyrd penetrationstestning begär det ska den rapport som avses i det första stycket inte innehålla någon känslig information.

Artikel 13

Åtgärdsplan

1. Inom åtta veckor från den underrättelse som avses i artikel 12.7 i denna förordning ska den finansiella entiteten överlämna de åtgärdsplaner och den dokumentation som avses i artikel 26.6 i förordning (EU) 2022/2554 till myndigheten med ansvar för hotbildsstyrd penetrationstestning och, om det inte rör sig om samma myndighet, till den finansiella entitetens behöriga myndighet.

2. Den åtgärdsplan som avses i punkt 1 ska för varje resultat som framkommit i den hotbildsstyrda penetrationstestningen innehålla följande:

a) En beskrivning av de identifierade bristerna.

b) En beskrivning av de föreslagna åtgärderna och av deras prioritering och förväntade slutförande, i förekommande fall inklusive åtgärder för att förbättra kapaciteten för identifiering, skydd, detektering och respons.

c) En analys av grundorsakerna.

d) Personalen eller funktionerna inom den finansiella entiteten som ansvarar för genomförandet av de föreslagna åtgärderna eller förbättringarna.

e) De risker som är förknippade med att inte genomföra de åtgärder som avses i led b och, i förekommande fall, de risker som är förknippade med genomförandet av dessa åtgärder.

Artikel 14

Intyg

1. Det intyg som avses i artikel 26.7 i förordning (EU) 2022/2554 ska innehålla de uppgifter som anges i bilaga VIII.

2. Om flera myndigheter med ansvar för hotbildsstyrd penetrationstestning har deltagit i en testning är det den ledande myndigheten med ansvar för hotbildsstyrd penetrationstestning som ska tillhandahålla det intyg som avses i artikel 26.7 i förordning (EU) 2022/2554 till de finansiella entiteter som testats.

Artikel 15

Användning av interna testare

1. Finansiella entiteter ska upprätta samtliga av följande arrangemang vid användning av interna testare:

a) Upprättande och införande av riktlinjer för hanteringen av interna testare i samband med en hotbildsstyrd penetrationstestning.

b) Åtgärder för att säkerställa att användningen av interna testare för att genomföra en hotbildsstyrd penetrationstestning inte negativt påverkar den finansiella entitetens allmänna försvarsförmåga eller motståndskraft i fråga om IKT-relaterade incidenter eller i betydande grad påverkar tillgången till resurser avsatta för IKT-relaterade uppgifter under en hotbildsstyrd penetrationstestning.

c) Åtgärder för att säkerställa att interna testare har tillräckliga resurser och tillräcklig kapacitet för att genomföra en hotbildsstyrd penetrationstestning.

Riktlinjerna som avses i led a ska

a) innehålla kriterier för bedömning av de interna testarnas lämplighet, kompetens och potentiella intressekonflikter och specificera ledningens ansvar i testningsprocessen,

b) dokumenteras och regelbundet ses över,

c) föreskriva att den interna testgruppen har en testledare och åtminstone två ytterligare medlemmar,

d) kräva att alla medlemmar i testgruppen har varit anställda av den finansiella entiteten eller av en koncernintern IKT-tjänsteleverantör under de senaste tolv månaderna,

e) innehålla föreskrifter om utbildning kring hur penetrationstestning och rött lag-testning ska utföras av interna testare.

2. Om en myndighet med ansvar för hotbildsstyrd penetrationstestning godkänner användning av interna testare i enlighet med artikel 27.2 a i förordning (EU) 2022/2554 ska myndigheten med ansvar för hotbildsstyrd penetrationstestning beakta de krav som fastställs i artikel 7.1 i den här förordningen.

3. Vid användning av interna testare ska den finansiella entiteten se till att sådan användning nämns i följande dokument:

a) Den information för testets inledande som avses i artikel 9.

b) Det röda lagets testrapport som avses i artikel 12.2.

c) Den rapport som sammanfattar de relevanta resultaten av den hotbildsstyrda penetrationstestningen som avses i artikel 26.6 i förordning (EU) 2022/2554.

4. Testare som är anställda av en koncernintern IKT-tjänsteleverantör ska betraktas som interna testare hos den finansiella entiteten.

Artikel 16

Samarbete och ömsesidigt erkännande

1. I syfte att genomföra en hotbildsstyrd penetrationstestning gentemot en finansiell entitet som tillhandahåller tjänster i fler än en medlemsstat, inklusive genom en filial, ska den berörda myndigheten med ansvar för hotbildsstyrd penetrationstestning göra följande:

a) Fastställa vilka myndigheter med ansvar för hotbildsstyrd penetrationstestning i värdmedlemsstater som ska involveras, med beaktande av huruvida en eller flera kritiska eller viktiga funktioner bedrivs i eller delas mellan värdmedlemsstater.

b) Informera de myndigheter med ansvar för hotbildsstyrd penetrationstestning som identifierats enligt led a om beslutet att genomföra en hotbildsstyrd penetrationstestning för den finansiella entiteten.

c) Såvida inte annat överenskommits mellan myndigheterna med ansvar för hotbildsstyrd penetrationstestning ska myndigheten med ansvar för hotbildsstyrd penetrationstestning för den finansiella entiteten leda testningen.

Myndigheter med ansvar för hotbildsstyrd penetrationstestning i värdmedlemsstater får, inom 20 arbetsdagar från mottagandet av informationen om ett planerat genomförande av en hotbildsstyrd penetrationstestning, antingen anmäla sitt intresse att följa testningen som observatörer eller utse en testledare för att delta i testningen. Den ledande myndigheten med ansvar för hotbildsstyrd penetrationstestning ska förse alla myndigheter med ansvar för hotbildsstyrd penetrationstestning som agerar som observatörer vid testningen med omfattningsdokumentet, den sammanfattande testrapporten, åtgärdsplanen och intyget.

Den ledande myndigheten med ansvar för hotbildsstyrd penetrationstestning ska samordna alla deltagande myndigheter med ansvar för hotbildsstyrd penetrationstestning under hela testet och anta alla beslut som krävs för att genomföra testningen på ett lämpligt och effektivt sätt. Den ledande myndigheten med ansvar för hotbildsstyrd penetrationstestning får fastställa ett högsta antal deltagande myndigheter med ansvar för hotbildsstyrd penetrationstestning ifall ett effektivt genomförande av testningen annars skulle kunna äventyras.

2. Om en finansiell entitet använder samma koncerninterna IKT-tjänsteleverantör som finansiella entiteter som är etablerade i andra medlemsstater, eller tillhör en koncern och delar IKT-system med finansiella entiteter i samma koncern som är etablerade i andra medlemsstater, ska myndigheten med ansvar för hotbildsstyrd penetrationstestning för den finansiella entiteten kontakta myndigheterna med ansvar för hotbildsstyrd penetrationstestning för de andra finansiella entiteterna som använder samma koncerninterna IKT-tjänsteleverantör eller som delar IKT-system som en del av koncernen, och tillsammans med dessa bedöma om det är genomförbart och lämpligt att genomföra en samlad hotbildsstyrd penetrationstestning i fråga om dessa. En samlad hotbildsstyrd penetrationstestning ska föredras framför en enskild hotbildsstyrd penetrationstestning om den kan leda till lägre kostnader och mindre resursanvändning för de finansiella entiteterna och för myndigheterna med ansvar för hotbildsstyrd penetrationstestning, förutsatt att testningens sundhet och effektivitet inte påverkas negativt.

3. Vid genomförande av en samlad hotbildsstyrd penetrationstestning gäller följande:

a) Myndigheterna med ansvar för hotbildsstyrd penetrationstestning för de finansiella entiteterna ska enas om vilken finansiell entitet som ska utses att genomföra testningen, med beaktande av koncernstrukturen och testets effektivitet.

b) Myndigheten med ansvar för hotbildsstyrd penetrationstestning för den finansiella entitet som har utsetts i enlighet med led a ska leda testningen, såvida inte annat överenskommits bland myndigheterna med ansvar för hotbildsstyrd penetrationstestning för de finansiella entiteter som deltar i den samlade hotbildsstyrda penetrationstestningen.

c) Myndigheterna med ansvar för hotbildsstyrd penetrationstestning för de andra finansiella entiteterna än den utsedda finansiella entiteten som ska leda den samlade hotbildsstyrda penetrationstestningen kan antingen anmäla sitt intresse att följa testningen som observatörer eller utse en testledare för den testningen.

Den ledande myndigheten med ansvar för hotbildsstyrd penetrationstestning ska samordna alla myndigheter med ansvar för hotbildsstyrd penetrationstestning som deltar i den samlade testningen och anta alla beslut som krävs för att genomföra den samlade testningen på ett sunt och effektivt sätt.

4. Om en finansiell entitet avser att genomföra en gemensam hotbildsstyrd penetrationstestning i enlighet med artikel 26.4 i förordning (EU) 2022/2554 som eventuellt involverar finansiella entiteter som är etablerade i andra medlemsstater, ska dess myndighet med ansvar för hotbildsstyrd penetrationstestning kontakta de andra finansiella entiteternas myndigheter med ansvar för hotbildsstyrd penetrationstestning och tillsammans med dem bedöma om det är genomförbart och lämpligt att genomföra en gemensam hotbildsstyrd penetrationstestning i fråga om dessa i enlighet med artikel 26.4 i förordning (EU) 2022/2554.

5. Vid genomförande av en gemensam hotbildsstyrd penetrationstestning, i enlighet med artikel 26.4 i förordning (EU) 2022/2554, gäller följande:

a) Myndigheterna med ansvar för hotbildsstyrd penetrationstestning för de finansiella entiteterna ska komma överens om vilken finansiell entitet som ska utses att genomföra testningen, med beaktande av de IKT-tjänster som tillhandahålls av tredjepartsleverantören av IKT-tjänster till de finansiella entiteterna och testets effektivitet.

b) Myndigheten med ansvar för hotbildsstyrd penetrationstestning för den finansiella entitet som har utsetts i enlighet med led a ska leda testningen, såvida inte annat överenskommits bland myndigheterna med ansvar för hotbildsstyrd penetrationstestning för de finansiella entiteter som deltar i den gemensamma hotbildsstyrda penetrationstestningen.

c) Myndigheterna med ansvar för hotbildsstyrd penetrationstestning för de andra finansiella entiteterna än den utsedda finansiella entiteten som ska leda den gemensamma hotbildsstyrda penetrationstestningen kan antingen anmäla sitt intresse att följa testningen som observatörer eller utse en testledare för den testningen.

Den ledande myndigheten med ansvar för hotbildsstyrd penetrationstestning ska samordna alla myndigheter med ansvar för hotbildsstyrd penetrationstestning som deltar i den gemensamma testningen och anta alla beslut som krävs för att genomföra den gemensamma testningen på ett sunt och effektivt sätt.

6. Om en finansiell entitet som är skyldig att genomföra en hotbildsstyrd penetrationstestning har en annan myndighet med ansvar för hotbildsstyrd penetrationstestning än dess behöriga myndighet enligt artikel 46 i förordning (EU) 2022/2554 ska dessa myndigheter utbyta all relevant information om alla frågor som rör testningen i syfte att genomföra testningen eller utföra myndigheternas uppgifter i enlighet med denna förordning.

Artikel 17

Ikraftträdande

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 13 februari 2025.

På kommissionens vägnar
Ursula VON DER LEYEN
Ordförande

BILAGA I

Projektbeskrivningens innehåll (artikel 9.2 a)

Informationspost	Obligatoriska uppgifter
Person med ansvar för projektplanen, dvs. ledningslagets ledare	Namn Kontaktuppgifter
Testare	☐ Interna ☐ Externa ☐ Bådadera
Kommunikationskanaler som valts i enlighet med artikel 9.2 d och artikel 9.4 a, inklusive a) e-postkryptering som ska användas, b) online-baserade datarum som ska användas, c) snabbmeddelandetjänst som ska användas	
Kodnamn för den hotbildsstyrda penetrationstestningen	
I förekommande fall, kritiska eller viktiga funktioner som den finansiella entiteten bedriver i andra medlemsstater	1. Förteckning över kritiska eller viktiga funktioner som bedrivs i en annan medlemsstat 2. För varje kritisk eller viktig funktion, uppgift om i vilken medlemsstat eller vilka medlemsstater den bedrivs
I förekommande fall, kritiska eller viktiga funktioner som stöds av tredjepartsleverantörer av IKT-tjänster	3. Förteckning över kritiska eller viktiga funktioner som stöds av tredjepartsleverantörer av IKT-tjänster 4. För varje funktion, identifiering av tredjepartsleverantören av IKT-tjänster
Förväntade tidsfrister för slutförande av	
(1) Förberedelsefasen, enligt artikel 9	åååå-mm-dd
(2) Testfasen, enligt artiklarna 10 och 11	åååå-mm-dd
(3) Avslutningsfasen, enligt artikel 12	åååå-mm-dd
(4) Åtgärdsplanen, enligt artikel 13	åååå-mm-dd

BILAGA II

Innehåll i omfattningsdokumentet (artikel 9.6)

1. Omfattningsdokumentet ska innehålla en förteckning över alla kritiska eller viktiga funktioner som identifierats av den finansiella entiteten.

2. För varje identifierad kritisk eller viktig funktion ska följande information inkluderas:

   a) Ifall den kritiska eller viktiga funktionen inte omfattas av den hotbildsstyrda penetrationstestningen, en beskrivning av skälen till att den inte omfattas.

   b) Ifall den kritiska eller viktiga funktionen omfattas av den hotbildsstyrda penetrationstestningen, följande information:

      i) En beskrivning av skälen till att den omfattas.

      ii) Det identifierade IKT-systemet eller de identifierade IKT-systemen som stöder den kritiska eller viktiga funktionen.

      iii) För varje identifierat IKT-system, följande uppgifter:

         1. Huruvida det har utkontrakterats och i så fall namnet på tredjepartsleverantören av IKT-tjänster.

         2. De jurisdiktioner i vilka IKT-systemet används.

         3. En övergripande beskrivning av preliminära flaggor, med en indikering av vilken säkerhetsaspekt i fråga om konfidentialitet, integritet, autenticitet eller tillgänglighet som omfattas av varje flagga.

BILAGA III

Innehåll i den målinriktade hotunderrättelserapporten (artikel 10.5)

Den målinriktade hotunderrättelserapporten ska innehålla samtliga av följande uppgifter:

1. Övergripande omfattning av underrättelseuppgifterna, däribland minst följande:
   a) Kritiska eller viktiga funktioner som omfattas.
   b) Dessa funktioners geografiska plats.
   c) Det officiella EU-språk som används.
   d) Relevanta tredjepartsleverantörer av IKT-tjänster.
   e) Tidsperiod under vilken uppgifterna samlades in.
2. Övergripande bedömning av vilka konkreta och praktiskt användbara underrättelser som kan hittas i fråga om den finansiella entiteten, däribland följande:
   a) De anställdas användarnamn och lösenord.
   b) Look-alike-domäner som kan misstas för den finansiella entitetens officiella domäner.
   c) Teknisk rekognosering: programvaror, system och teknik med sårbarhet eller möjlighet till utnyttjande.
   d) Information om den finansiella entiteten som lagts ut på internet av anställda och som kan användas för ett angrepp.
   e) Information som är till salu på dark web.
   f) All annan relevant information som finns tillgänglig på internet eller i publika nät.
   g) I förekommande fall, information rörande inriktning på fysiska mål, inklusive sätt att få tillträde till den finansiella entitetens lokaler.
3. Analys av underrättelser om hot med beaktande av den allmänna hotbilden och den finansiella entitetens specifika situation, åtminstone inbegripet följande:
   a) Den geopolitiska miljön.
   b) Den ekonomiska miljön.
   c) De tekniska trenderna och andra trender kopplade till verksamheten inom sektorn för finansiella tjänster.
4. Hotprofiler för fientliga aktörer (specifik individ/grupp eller en generell klass) som skulle kunna inrikta sig på den finansiella entiteten, inklusive de system hos den finansiella entiteten som det är mest sannolikt att fientliga aktörer skulle angripa eller inrikta sig mot, den möjliga grunden, avsikten och förklaringen till den potentiella målinriktningen och angriparnas tänkbara tillvägagångssätt.
5. Hotscenarier: minst tre fullständiga hotscenarier för de hotprofiler som identifierats enligt punkt 4 och som uppvisar de högsta graderna av hot. Hotscenarierna ska beskriva hela angreppsvägen och ska åtminstone innefatta följande:
   a) Ett scenario som omfattar men inte är begränsat till påverkad tillgång till tjänster.
   b) Ett scenario som omfattar men inte är begränsat till äventyrad dataintegritet.
   c) Ett scenario som omfattar men inte är begränsat till äventyrad informationssekretess.
6. I förekommande fall, en beskrivning av det ej hotbildsstyrda scenario som avses i artikel 10.4.

BILAGA IV

Innehåll i planen för rött lag-testning (artikel 11.1)

Planen för rött lag-testning ska innehålla samtliga av följande uppgifter:

a) Kommunikationskanaler och kommunikationsrutiner.

b) Taktiker, teknik och förfaranden som är tillåtna respektive inte tillåtna att använda i angreppet, inklusive etiska gränser för social manipulering.

c) De riskhanteringsåtgärder som testarna ska följa.

d) En beskrivning av varje scenario, inklusive följande:

   i) Den simulerade hotaktören.

   ii) Dennes avsikt, motivation och mål.

   iii) Funktionen eller funktionerna som är angreppsmål och stödjande IKT-system (ett eller flera).

   iv) Konfidentialitets-, integritets-, tillgänglighets- och autenticitetsaspekter som utgör mål.

   v) Flaggor.

e) En detaljerad beskrivning av varje förväntad angreppsväg, inklusive förutsättningar och eventuella hjälpinsatser som ledningslaget kan tillhandahålla, inklusive tidsfrister för deras tillhandahållande och potentiella användning.

f) Planeringen av rött lag-aktiviteter, inklusive tidsplanering för genomförandet av varje scenario, åtminstone uppdelat i de tre faser som en testare genomgår under testfasen, närmare bestämt intrång i de finansiella entiteternas IKT-system, förflyttning genom IKT-systemen och slutligen genomförande av angrepp på målen samt därefter lämnande av IKT-systemen (faserna in, genom och ut).

g) Egenskaper hos de finansiella entiteternas infrastruktur som ska beaktas under testningen.

h) I förekommande fall, ytterligare information eller andra resurser som testarna behöver för att genomföra scenarierna.

BILAGA V

Innehåll i det röda lagets testrapport (artikel 12.2)

Det röda lagets testrapport ska åtminstone innehålla samtliga av följande uppgifter:

a) Information om det utförda angreppet, inklusive

   i) de kritiska eller viktiga funktioner som angreppet inriktades mot och identifierade IKT-system och IKT-processer och identifierad IKT-teknik som stöder dessa kritiska eller viktiga funktioner, enligt identifieringen i planen för rött lag-testning,

   ii) en sammanfattning av varje scenario,

   iii) flaggor som har nåtts respektive inte nåtts,

   iv) angreppsvägar som har följts med framgång respektive utan framgång,

   v) taktiker, teknik och förfaranden som har använts med framgång respektive utan framgång,

   vi) avvikelser från planen för rött lag-testning, i förekommande fall,

   vii) hjälpinsatser som gjorts, i förekommande fall.

b) Alla åtgärder som testarna känner till har utförts av det blå laget för att rekonstruera angreppet och mildra dess effekter.

c) Upptäckta sårbarheter och andra resultat, däribland

   i) en beskrivning av sårbarheter och andra resultat, inbegripet deras kritikalitet,

   ii) en analys av grundorsakerna till framgångsrika angrepp,

   iii) rekommenderade åtgärder, inklusive en indikering av åtgärdernas prioritering.

BILAGA VI

Innehåll i det blå lagets testrapport (artikel 12.4)

Det blå lagets testrapport ska åtminstone innehålla samtliga av följande uppgifter:

1. För varje angreppssteg som beskrivs av testarna i det röda lagets testrapport:
   a) En förteckning över upptäckta angreppsåtgärder.
   b) Loggposter som motsvarar dessa upptäckter.
2. En bedömning av testarnas resultat och rekommendationer.
3. Bevis på testarnas angrepp som samlats in av det blå laget.
4. Det blå lagets analys av grundorsaken till framgångsrika angrepp från testarnas sida.
5. En förteckning över lärdomar som dragits och identifierad förbättringspotential.
6. En förteckning över ämnen som ska tas upp i lila lagövningar.

BILAGA VII

Uppgifter i den rapport som sammanfattar de relevanta resultaten av den hotbildsstyrda penetrationstestningen som avses i artikel 26.6 i förordning (EU) 2022/2554

Den sammanfattande testrapporten ska åtminstone innehålla samtliga av följande uppgifter:

a) De deltagande parterna.

b) Projektplanen.

c) Den validerade omfattningen, inklusive motiveringen till att inkludera eller exkludera kritiska eller viktiga funktioner och identifierade IKT-system och IKT-processer och identifierad IKT-teknik som stöder de kritiska eller viktiga funktioner som omfattas av den hotbildsstyrda penetrationstestningen.

d) Valda scenarier och eventuella betydande avvikelser från den målinriktade hotunderrättelserapporten.

e) Genomförda angreppsvägar och taktiker, teknik och förfaranden som använts.

f) Flaggor som erhållits respektive inte erhållits.

g) Avvikelser från planen för rött lag-testning, i förekommande fall.

h) Upptäckter gjorda av det blå laget, i förekommande fall.

i) Lila lagövningar under testfasen, om sådana utfördes och aktuella förhållanden.

j) Hjälpinsatser som gjordes, i förekommande fall.

k) Riskhanteringsåtgärder som vidtagits.

l) Identifierade sårbarheter och andra resultat, inklusive deras kritikalitet.

m) En analys av grundorsakerna till framgångsrika angrepp.

n) En övergripande åtgärdsplan som kopplar samman sårbarheter och andra resultat, deras bakomliggande orsaker och prioriteringen av åtgärder.

o) Lärdomar som dragits från den mottagna återkopplingen.

BILAGA VIII

Uppgifter i det intyg för den hotbildsstyrda penetrationstestningen som avses i artikel 26.7 i förordning (EU) 2022/2554

Intyget ska åtminstone innehålla samtliga av följande uppgifter:

a) I fråga om den genomförda hotbildsstyrda penetrationstestningen:

   i) Start- och slutdatum för den hotbildsstyrda penetrationstestningen.

   ii) De kritiska eller viktiga funktioner som omfattades av testet.

   iii) I förekommande fall, information om kritiska eller viktiga funktioner som ingick i testets omfattning för vilka hotbildsstyrd penetrationstestning inte genomfördes.

   iv) I förekommande fall, andra finansiella entiteter som var involverade i den hotbildsstyrda penetrationstestningen.

   v) I förekommande fall, de tredjepartsleverantörer av IKT-tjänster som deltog i den hotbildsstyrda penetrationstestningen.

   vi) I fråga om testarna:

      1. Huruvida interna testare har använts.

      2. Huruvida artikel 5.3 andra stycket har tillämpats av den finansiella entiteten.

   vii) Varaktigheten, i kalenderdagar, för den aktiva rött lag-testfasen.

b) Om flera myndigheter med ansvar för hotbildsstyrd penetrationstestning har varit involverade i testningen, uppgift om de övriga myndigheterna med ansvar för hotbildsstyrd penetrationstestning och i vilken egenskap de varit involverade.

c) En förteckning över de dokument som har granskats av myndigheten med ansvar för hotbildsstyrd penetrationstestning i samband med utfärdandet av intyget.