Europeiska unionens råd

Bryssel den 11 juni 2025
(OR. en)

6302/25
COR 2

EF 34
ECOFIN 162
DELACT 10
ECB

FÖLJENOT

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	10 juni 2025
till:	Thérèse BLANCHET, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	C(2025) 3781 final
Ärende:	RÄTTELSE av den 6.6.2025 till kommissionens delegerade förordning 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 *C(2025) 885 final*

För delegationerna bifogas dokument – C(2025) 3781 final.

Bilaga: C(2025) 3781 final

EUROPEISKA
KOMMISSIONEN

Bryssel den 6.6.2025
C(2025) 3781 final

RÄTTELSE

av den 6.6.2025

till kommissionens delegerade förordning 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

C(2025) 885 final

RÄTTELSE

till kommissionens delegerade förordning 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

C(2025) 885 final

I skäl 5 ska det

i stället för: ”(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 ”vita lag”) 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”).”.

vara: ”(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”).”.

I skäl 10 ska det

i stället för: ”(10) Som framgår av de erfarenheter som gjorts inom TIBER-EU-ramen när det gäller det ”vita laget” 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.”.

vara: ”(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.”.

I artikel 2.3 första stycket ska det

i stället för: ”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 14.2 besluta huruvida kravet att genomföra hotbildsstyrd penetrationstestning på individuell nivå är relevant för dessa finansiella entiteter.”.

vara: ”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.”.

I artikel 5.1 inledningsfrasen ska det

i stället för: ”1. Under den förberedelsefas som avses i artikel 8 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”.

vara: ”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”.

I artikel 6.2 ska det

i stället för: ”2. Ledningslaget för den utsedda finansiella entitet som avses i artikel 14.3 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.”.

vara: ”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.”.

I artikel 7.2 ska det

i stället för: ”2. Ledningslaget ska föra register över den dokumentation som tillhandahålls av testarna och leverantörerna av underrättelser om hot för att styrka efterlevnaden av punkt 2 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 2 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.”.

vara: ”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.”.

I artikel 8.1 ska det

i stället för: ”1. Om flera finansiella entiteter, identifierade i enlighet med artikel 16.3 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.”.

vara: ”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.”.

I artikel 9.1 ska det

i stället för: ”1. En finansiell entitet som identifierats i enlighet med artikel 26.8 andra 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.”.

vara: ”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.”.

I artikel 9.6 ska det

i stället för: ”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 2. Den finansiella entitetens ledningsorgan ska godkänna omfattningsdokumentet.”.

vara: ”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.”.

I artikel 15.3 a ska det

i stället för: ”(a) De dokument för testets inledande som avses i artikel 9.”.

vara: ”(a) Den information för testets inledande som avses i artikel 9.”.

I artikel 16.5 a ska det

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

vara: ”(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.”.