

BESLUT

DATUM: 2025-12-03
AVDELNING: Avdelningen för finansiell stabilitet
DIARIENUMMER: 2025–00974
HANTERINGSKLASS: Ö P P E N

Nya föreskrifter om avgifter för Riksbankens övervakning och samordning av hotbildsstyrda penetrationstester

Riksbankens beslut

Riksbanken fastställer

- Riksbankens föreskrifter om avgifter för Riksbankens övervakning och samordning av hotbildsstyrda penetrationstester
- beslutspromemorian Riksbankens föreskrifter om avgifter för Riksbankens övervakning och samordning av hotbildsstyrda penetrationstester, se bilagor.

Föreskrifterna träder i kraft den 1 januari 2026. Föreskrifterna offentliggörs i Riksbankens författningssamling.

Skälen för beslutet

Tillämpliga bestämmelser

Riksbanken får med stöd av 2 kap. 6 § lagen (2024:1278) med kompletterande bestämmelser till EU:s förordning om digital motståndskraft för finanssektorn ta ut avgifter från de finansiella entiteter som genomför hotbildstyrda penetrationstester och meddela föreskrifter om avgifterna.

Bedömning

Riksbanken gör bedömningen att föreskrifterna gör avgifterna mer transparenta och förutsägbara än alternativet att fatta separata beslut för varje enskilt företag.

Beslutet har fattats av direktionen (riksbankschefen Erik Thedéen, förste vice riksbankschefen Aino Bunge samt vice riksbankscheferna Per Jansson och Anna Seim) efter föredragning av Magnus Georgsson. I den slutliga handläggningen har avdelningschefen Olof Sandstedt och chefsjuristen Annica Sandberg medverkat.

BESLUTSPROMEMORIA

DATUM: 2025-12-03



SVERIGES RIKSBANK
SE-103 37 Stockholm
(Brunkebergstorg 11)

Tel +46 8 787 00 00
Fax +46 8 21 05 31
registratorn@riksbank.se
www.riksbank.se

DNR 2025-00974

Riksbankens föreskrifter om avgifter för hotbildsstyrda penetrationstester

Sammanfattning

EU:s förordning om digital operativ motståndskraft för finanssektorn, den så kallade DORA-förordningen,¹ innehåller bland annat bestämmelser om testning av de finansiella företagens digitala operativa motståndskraft, så kallade hotbildsstyrda penetrationstester.

Enligt lagen (2024:1278) med kompletterande bestämmelser till EU:s förordning om digital operativ motståndskraft ska Finansinspektionen besluta om vilka företag som ska genomföra sådana hotbildsstyrda penetrationstester.

Riksbanken ska enligt samma lag övervaka och samordna de hotbildsstyrda penetrationstesterna. Uppgiften innebär kostnader för Riksbanken. Dessa kostnader ska finansieras med avgifter från de företag som enligt Finansinspektionens beslut ska låta genomföra testerna. Syftet med föreskrifterna är att reglera hur avgifterna ska tas ut.

Föreskrifterna träder i kraft den 1 januari 2026.

¹ 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.

Innehåll

1	UTGÅNGSPUNKTER.....	3
1.1	NYTT REGELVERK OM TESTNING AV DIGITAL MOTSTÅNDSKRAFT	3
1.2	SYFTET MED FÖRESKRIFTERNA.....	4
1.3	ALTERNATIV REGLERING	4
1.4	RÄTTSLIGA FÖRUTSÄTTNINGAR	4
1.5	ÄRENDETS BEREDNING	4
1.6	REMISSINSTANSEARNAS GENERELLA SYNPUNKTER.....	5
2	RIKSBANKENS STÄLLNINGSTAGANDEN.....	5
2.1	RIKSBANKENS KOSTNADER SKA FINANSIERAS MED EN ÅRLIG AVGIFT	5
2.2	FÖRDELNINGSMODELL FÖR DEN ÅRLIGA AVGIFTEN	7
2.3	JUSTERING AV AVGIFTEN FÖR DEL AV ÅR.....	9
2.4	BESLUT OCH BETALNING AV AVGIFT.....	9
3	IKRAFTTRÄDANDE.....	10
4	FÖRSLAGETS KONSEKVENSER.....	10
4.1	KONSEKVENSER FÖR SAMHÄLLET OCH KONSUMENTERNA	11
4.2	KONSEKVENSER FÖR FÖRETAGEN	11
4.3	KONSEKVENSER FÖR RIKSBANKEN.....	12
4.4	KONSEKVENSER FÖR FÖRVALTNINGSMYNDIGHETER OCH DOMSTOLAR	12
4.5	SÅ FÖRHÅLLER SIG FÖRSLAGET TILL UNIONS RÄTTEN	12
4.6	IKRAFTTRÄDANDE OCH SÄRSKILDA INFORMATION INSATSER.....	12
4.7	ÖVRIGA KONSEKVENSER	13

1 Utgångspunkter

1.1 Nytt regelverk om testning av digital motståndskraft

Genom EU:s förordning om digital operativ motståndskraft för finanssektorn (DORA-förordningen)² införs nya krav på företag³ inom den finansiella sektorn. Kraven avser bland annat företagets riskhantering av informations- och kommunikationsteknik, incidentrapportering, hantering av utlagd verksamhet och testning av digital operativ motståndskraft. Testning av digital motståndskraft innebär att företagen ska inrätta, upprätthålla och se över ett sunt och heltäckande program för tester. Ett sådant testprogram ska bland annat innehålla sårbarhetsanalyser, bedömning av nätverkssäkerhet, fysiska säkerhetsgranskningar och penetrationstester.

Lagen (2024:1278) med kompletterande bestämmelser till EU:s förordning om digital operativ motståndskraft (kompletteringslagen) trädde i kraft den 17 januari 2025 och är en del av det svenska genomförandet av DORA-förordningen. Både förordningen och kompletteringslagen tillämpas från och med den 17 januari 2025.

Vissa företag bedriver verksamhet som är av central betydelse för det finansiella systemets funktionalitet. Sådana företag kan bli ålagda av Finansinspektionen att genomföra särskilt avancerad testning baserad på hotbildsstyrda penetrationstester i enlighet med ett särskilt testramverk, TIBER-EU⁴. Ramverket omfattar bland annat så kallade red-team-tester där en extern aktör har i uppdrag att försöka göra intrång. När ett test har avslutats ska företaget förses med ett intyg som bekräftar att testet genomförts i enlighet med kraven i DORA-förordningen. Syftet med intyget är att möjliggöra ömsesidigt erkännande av hotbildsstyrda penetrationstester mellan behöriga myndigheter i olika medlemsstater.

Enligt 2 kap. 2 § kompletteringslagen ska Riksbanken ha till uppgift att övervaka och samordna dessa obligatoriska hotbildsstyrda penetrationstester. Riksbanken ska delta i planeringen och genomförandet av testningen genom att bland annat validera vilka delar inom den finansiella entiteten som ska omfattas av testningen och säkerställa att den testare som anlitas för utförandet av testet uppfyller de krav som ställs i DORA-förordningen. Riksbanken ska även utfärda intyg om att ett test har utförts i enlighet med kraven i förordningen. De nya uppgifterna utgör myndighetsutövning mot enskilda och innebär ökade kostnader för Riksbanken.⁵

Riksbanken övervakar och koordinerar redan i dag tester som vissa företag genomför enligt TIBER-ramverket⁶ på frivillig basis genom bilaterala avtal med Riksbanken. Sådana frivilliga tester omfattas inte av föreskrifterna. De av företagen som Finansinspektionen beslutat ska genomföra obligatoriska tester enligt DORA-förordningen kommer heller inte

² 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.

³ I DORA-förordningen används begreppet finansiella entiteter.

⁴ TIBER står för Threat Intelligence-Based Ethical Red teaming.

⁵ Prop. 2024/25:44 sid. 137.

⁶ TIBER-EU är ett ramverk framtaget av Europeiska centralbanken som gör det möjligt att på ett standardiserat sätt testa motståndskraften mot cyberrisker hos aktörer i det finansiella systemet. Testen (så kallade Red-team tester) innebär att en cyberattack under kontrollerade former simuleras mot en organisations anställda, processer och teknik. Testen är inte "pass or fail", utan syftar till att identifiera brister för att sedan kunna förbättra motståndskraften.

fortsättningsvis att omfattas av det frivilliga TIBER-programmet. Vissa företag som inte omfattas av DORA eller Finansinspektionens beslut kan dock även fortsättningsvis få avtala med Riksbanken om att genomföra frivilliga tester enligt TIBER-ramverket.

Enligt 2 kap. 6 § kompletteringslagen får Riksbanken ta ut avgifter från de företag som enligt Finansinspektionens beslut är skyldiga att genomföra hotbildsstyrd penetrationstestning och meddela föreskrifter om dessa avgifter.

1.2 Syftet med föreskrifterna

Riksbanken ska ta ut avgifter som över tid ger Riksbanken full kostnadstäckning för övervakning och samordning av de hotbildsstyrda penetrationstesterna. Syftet med föreskrifterna är att reglera hur avgifterna ska beräknas och tas ut av de företag som i enlighet med Finansinspektionens beslut ska genomföra hotbildsstyrd penetrationstestning.

1.3 Alternativ reglering

Ett alternativ till att meddela föreskrifter är att i stället fatta separata beslut om avgiften för varje enskild finansiell entitet utifrån kompletteringslagen. Dessa hotbildsstyrda penetrationstester är obligatoriska och innebär att enskilda företag blir föremål för Riksbankens myndighetsutövning. Föreskrifter gör beräkningen av avgifterna förutsägbar och remissbehandlingen ger företagen och andra intressenter möjlighet att lämna synpunkter.

Riksbankens överväganden kring avgiftsmodellen finns i avsnitt 2.2. Ett alternativ till den föreslagna avgiftsmodellen vore en rak avgiftsmodell där alla företag betalar en lika stor andel av Riksbankens kostnader för övervakning och samordning av de hotbildsstyrda penetrationstesterna. Ett annat alternativ skulle kunna vara att avgifterna helt och hållet bestäms av storleken på företagets balansomslutning.

1.4 Rättsliga förutsättningar

Riksbanken har enligt 2 kap. 6 § andra stycket kompletteringslagen bemyndigande att meddela föreskrifter om uttag av avgifter från de företag som genomför hotbildsstyrd penetrationstestning.

1.5 Ärendets beredning

Den 11 juli 2025 remitterade Riksbanken förslag till föreskrifter och en remisspromemoria till 22 företag, myndigheter och organisationer. Av dessa remissinstanser har tolv svarat på remissen. Nasdaq Clearing AB och Nasdaq Stockholm AB har svarat gemensamt, i det följande räknad som en enda remissinstans och refererad till som Nasdaq.

Tre instanser är positiva eller tillstyrker förslaget (*Ekonomistyrningsverket, Konkurrensverket* och *Nasdaq*), tre instanser har inga synpunkter på förslaget (*Finansinspektionen, Sparbankernas riksförbund* och *Svensk försäkring*) och sju instanser har synpunkter på förslaget (*Euroclear Sweden AB, Finansbolagens förening, Finansiell Id-Teknik Bid AB, Konkurrensverket, Nasdaq, Regelrådet* och *Svenska Bankföreningen*).

1.6 Remissinstansernas generella synpunkter

Flera företag och branschorganisationer har synpunkter på kostnadernas fördelning i den föreslagna avgiftsmodellen, främst utifrån en oro att avgifternas fördelning kan komma att missgynna företag med en mindre balansomslutning. Flera remissinstanser inklusive myndigheter efterfrågar en tydligare beskrivning av främst avgiftsmodellen.

Regelrådet bedömer att förslagets konsekvensutredning inte uppfyller tre av kraven i förordningen (2024:183) om konsekvensutredningar. Även *Konkurrensverket* har synpunkter på konsekvensutredningen och efterfrågar en tydligare redogörelse.

2 Riksbankens ställningstaganden

Nedanstående avsnitt sammanfattar remissinstansernas synpunkter på det förslag till föreskrifter och den remisspromemoria som remitterats samt beskriver Riksbankens överväganden och ställningstaganden.

2.1 Riksbankens kostnader ska finansieras med en årlig avgift

Riksbankens ställningstagande: De svenska företag (finansiella entiteter) som Finansinspektionen beslutar ska genomföra hotbildsstyrda penetrationstester ska betala en årlig avgift till Riksbanken.

Avgifterna ska över tid ge full täckning för Riksbankens direkta och indirekta kostnader med övervakning och samordning av entiteternas hotbildsstyrda penetrationstester samt utfärdande av intyg som avses i 2 kap. 2 § kompletteringslagen.

Remisspromemorian: Förslaget hade materiellt samma innehåll men med delvis andra författningstekniska lösningar.

Remissinstanserna: *Konkurrensverket* efterfrågar tydlighet om företagen ska betala avgiften årligen eller endast de år de utför tester. *Nasdaq* efterlyser närmare specificering av vad som inkluderas i kostnaderna och menar att avgifterna endast bör vara kopplade till själva genomförandet av testet. Vidare menar *Nasdaq* att deltagande i gränsöverskridande tester och kunskapsutbyte med övriga EU-länder inte ska finansieras genom avgifterna. *Finansiell Id-Teknik Bid* föreslår att föreskrifterna även ska omfatta avgiftsuttaget från de aktörer som genomför de frivilliga TIBER-testerna.

Riksbankens skäl: DORA-förordningen är tillämplig på de flesta företag som är verksamma inom den finansiella sektorn. I förordningen benämns dessa som finansiella entiteter.⁷ I denna beslutspromemoria används dock begreppet företag.

Hotbildsstyrda penetrationstester

Som exempel omfattar DORA-förordningen kreditinstitut, betalningsinstitut, värdepapperscentraler, centrala motparter och försäkringsföretag. Ett mindre antal av dessa företag anses ha en central betydelse för det finansiella systemet. Vissa av dessa företag kan enligt Finansinspektionen bli skyldiga att utföra särskilda hotbildsstyrda

⁷ Se artikel 2.1 i DORA-förordningen.

penetrationstester.⁸ Närmare kriterier finns i artikel 26 i DORA-förordningen och i artikel 2 i kommissionens delegerade förordning gällande hotbildsstyrda penetrationstester.⁹ Enligt 2 kap. 1 § kompletteringslagen är det Finansinspektionen som beslutar vilka företag som är av central betydelse för systemet och därför ska genomföra hotbildsstyrda penetrationstester.

Enligt 2 kap. 2 § kompletteringslagen ska Riksbanken ha till uppgift att övervaka och samordna de hotbildsstyrda penetrationstester som i enlighet med Finansinspektionens beslut. I uppgiften ingår bland annat att validera vilka kritiska eller viktiga funktioner som ska omfattas av de tester företagen låter utföra (artikel 26.2 tredje stycket DORA-förordningen) och att säkerställa att den som företaget anlitar för att utföra testet uppfyller de krav som ställs i DORA-förordningen (artikel 27). Med att övervaka och samordna avses även att säkerställa att företaget tillämpar den testmetod och det tillvägagångssätt som föreskrivs för varje specifik fas i testprocessen.

Avgifter ska täcka Riksbankens kostnader

Riksbanken får enligt 2 kap. 6 § kompletteringslagen ta ut avgifter från de företag som ska genomföra hotbildsstyrda penetrationstester och meddela föreskrifter om avgifterna.

Riksbanken är en myndighet under riksdagen och omfattas därför inte av avgiftsförordningen (1992:191). Riksbankens bedömning är dock att de principer som framgår av avgiftsförordningen bör vara en utgångspunkt även för den föreslagna avgiften. En av dessa är principen om full kostnadstäckning. Enligt Ekonomistyrningsverkets föreskrifter och allmänna råd (ESVFA 2022:5) om avgifter innebär principen att avgifter ska beräknas så att de på ett eller några års sikt täcker alla kostnader som direkt eller indirekt hör till den avgiftsbelagda verksamheten.¹⁰ Detta kan även uttryckas som att avgiftsnivån ska beräknas så att den långsiktiga självkostnaden täcks. En sådan prissättning innebär att det finns ett tydligt samband mellan avgiften och myndighetens kostnad för den avgiftsbelagda varan eller tjänsten.

Avgiften ska täcka Riksbankens direkta och indirekta kostnader relaterade till Riksbankens övervakning och samordning av företagens hotbildsstyrda penetrationstester. Här ingår kostnader för Riksbankens planering, genomförande och uppföljning av testerna. I den utsträckning det behövs för att utföra uppdraget kommer Riksbanken att ha kunskapsutbyte med relevanta myndigheter såväl inom Sverige som i övriga EU-länder. Slutligen ska avgiften även täcka kostnaden för de intyg som Riksbanken utfärdar enligt 2 kap. 2 § andra stycket kompletteringslagen.

Den årliga avgiften ska ge Riksbanken full kostnadstäckning över tid. Med att Riksbankens kostnader ska täckas över tid menas dels att avgifterna kommer att debiteras i efterhand, dels att de direkta och indirekta kostnaderna kan variera över tid. Riksbankens uppdrag är långsiktigt och löpande. Planering och utvärdering av uppgifterna förväntas uppkomma

⁸ Se Prop. 2024/25:44 avsnitt 7.1.

⁹ 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.

¹⁰ Se 5 § i Ekonomistyrningsverkets föreskrifter och allmänna råd (ESVFA 2022:5) om avgifter.

såväl året före som efter det år testet genomförs. Företagen ska genomföra minst ett test vart tredje år. Finansinspektionen kan emellertid besluta om att test ska utföras oftare. Sammantaget kan ett enskilt företags avgifter inte begränsas till det år företaget låter utföra ett test. Därför behöver avgifterna debiteras varje år, oaktat om det enskilda företaget utfört ett test det året. Av samma skäl kan avgiftens storlek skilja sig åt mellan åren utan koppling till Riksbankens kostnader för det enskilda företaget just det året.

Bestämmelserna framgår av 1–3 §§ i föreskrifterna.

2.2 Fördelningsmodell för den årliga avgiften

Riksbankens ställningstagande: Riksbankens sammanlagda kostnader för den verksamhet som behövs för att genomföra övervakning och samordning av hotbildsstyrda penetrationstester och utfärdande av intyg ska fördelas på de företag som Finansinspektionen beslutat ska genomföra hotbildsstyrda penetrationstester genom en årlig avgift. Avgiften ska bestå av en fast och en rörlig del.

Den fasta delen ska uppgå till ett belopp som motsvarar 70 procent av Riksbankens totala kostnader jämnt fördelade mellan de företag som Finansinspektionen beslutat ska genomföra hotbildsstyrda penetrationstester.

Den rörliga delen utgör de resterande 30 procenten av Riksbankens totala kostnader. Den rörliga avgiftdelen ska motsvara det enskilda företags proportionella andel av den sammanlagda balansomslutningen för de företag som Finansinspektionen beslutat ska låta genomföra testerna.

Remisspromemorian: Förslaget hade materiellt och i allt väsentligt samma innehåll.

Remissinstanserna: *Konkurrensverket* framhåller att det kan finnas redovisningstekniska aspekter som försvårar jämförelsen mellan olika företags balansomslutningar och att det är oklart hur exempelvis kostnader för extra tester ska fördelas. *Svenska Bankföreningen* föreslår att avgiften för respektive företag ska spegla Riksbankens kostnad. *Finansbolagens förening*, *Euroclear Sweden*, *Finansiell Id-teknik Bid* och *Nasdaq* anser att den föreslagna modellen missgynnar mindre företag. I stället vill de se en modell som tar större hänsyn till skillnader i företagens balansomslutning. *Finansiell Id-teknik Bid* efterlyser en skyddsregel om att avgiften inte ska överskrida en viss andel av aktörens balansomslutning. *Euroclear Sweden* anser dessutom att Riksbankens kostnader bör fördelas på alla marknadens aktörer eftersom testerna har betydelse för hela den finansiella marknaden samt att en del av kostnaden bör finansieras med statliga anslag motiverat av testernas betydelse för Sveriges säkerhet som helhet.

Riksbankens skäl: Enligt Riksbankens preliminära bedömning kommer Riksbankens direkta och indirekta kostnader för samordning och övervakning av testerna inte att påverkas i någon avgörande grad av hur stort respektive företag är.

Samtidigt föreligger skillnader vad avser såväl storlek som verksamhet mellan de företag som kan bli föremål för Finansinspektionens beslut om krav på hotbildsstyrda penetrationstester. Enligt Riksbankens bedömning är det därför ändå mindre lämpligt att endast tillämpa en rak avgiftsmodell där alla företag betalar en lika stor andel av Riksbankens kostnader. Att avgifterna helt och hållet bestäms av storleken på företags balansomslutning skulle å andra sidan leda till en snedfördelning av avgifterna som enligt

Riksbankens bedömning skulle ligga alltför långt ifrån Riksbankens reella kostnader för respektive företag. Anledningen är att det finns stora skillnader i balansomslutning mellan de berörda företagen, inte minst vid en jämförelse mellan kreditinstitut och vissa finansiella infrastrukturbolag.

Med syfte att beakta både den preliminärt bedömda reella kostnadsfördelningen och skillnaderna i storlek mellan de omfattade företagen, har Riksbanken därför valt en modell där huvuddelen fördelas jämnt mellan företagen men som ändå tar hänsyn till företagens balansomslutning i proportion till de omfattade företagens samlade balansomslutning.

Avgiftsmodellen bygger således på en fast och en rörlig del. Den fasta delen fördelar 70 procent av Riksbankens totala kostnader jämnt mellan de företag som omfattas av föreskrifterna det aktuella året. Den rörliga delen uppgår till resterande 30 procent av Riksbankens totala kostnader och beräknas utifrån respektive företags andel av de omfattade företagens samlade balansomslutningar vid utgången av räkenskapsåret närmast före det år som avgiften avser. Bakgrunden är att Riksbanken inte ska behöva invänta företagens rapporter för det år som avgiften avser.

Avgiftsmodellen innebär att om Finansinspektionen exempelvis fattat beslut om tio företag som är skyldiga att utföra testerna och Riksbankens kostnader uppgår till tio miljoner kronor det året, kan avgiften komma att beräknas enligt följande: Den fasta avgiften uppgår till sju miljoner kronor vilket innebär att varje företag ska betala minst 700 000 kronor. Den rörliga avgiften kommer i exemplet att uppgå till sammanlagt tre miljoner kronor. Om två av företagens respektive balansomslutningar uppgår till fem respektive 20 procent av de omfattade företagens samlade balansomslutning, hamnar företagens rörliga del på 150 000 respektive 600 000 kronor. I exemplet kommer då den totala avgiften för de två företagen att uppgå till 850 000 respektive 1,3 miljoner kronor.

Oavsett skillnader i storlek på balansomslutningen sinsemellan, har alla de omfattade företagen bedömts ha en central betydelse för det finansiella systemets funktionalitet. Utifrån den premissen är gruppen omfattade företag homogen jämfört med alla andra aktörer i det finansiella systemet. Som nämnts förväntas heller inte skillnaderna i företagens storlek återspeglas i Riksbankens kostnad för respektive företag. Riksbanken bedömer sammantaget att avgiftsmodellen är proportionerlig givet förutsättningarna.

I framtagandet av fördelningsmodellen har Riksbanken i tillämpliga delar och så långt möjligt tagit intryck av redan existerande och beprövade motsvarigheter för att få en väl avvägd och enkel modell. Finansinspektionen använder exempelvis företagens balansomslutning som grund för fördelning av tillsynsavgiften.¹¹ Såväl kostnader som avgiftsmodell kommer att efterhand bli föremål för uppföljning och utvärdering.

De företag som ska utföra tester enligt DORA-förordningen kommer inte längre att utföra frivilliga TIBER-tester. De aktörer som inte omfattas av DORA-förordningen och de som omfattas av förordningen men inte av något beslut från Finansinspektionen kan även fortsättningsvis genomföra frivilliga tester enligt TIBER-ramverket, samordnade och övervakade av Riksbanken enligt bilaterala civilrättsliga avtal. Riksbanken kommer över tid att se över modellen för avgiftsberäkningen av testerna under TIBER-ramverket.

¹¹ Se 5 § förordningen (2007:1135) om årliga avgifter för finansiering av Finansinspektionens verksamhet.

Bestämmelsen finns i 5 § i föreskrifterna.

2.3 Justering av avgiften för del av år

Riksbankens ställningstagande: Avgiften ska beräknas med hänsyn tagen till vid vilken tidpunkt under året skyldigheten enligt Finansinspektionens beslut inträder. Om Finansinspektionen beslutar att ett företag inte längre ska genomföra hotbildsstyrd penetrationstestning ska avgiften minskas med hänsyn tagen till vid vilken tidpunkt under året skyldigheten upphör enligt beslutet.

Remisspromemorian: Förslaget innehöll en bestämmelse om att Riksbanken kan sätta ned avgiften om det finns särskilda skäl. I övrigt hade förslaget i allt väsentligt samma innehåll.

Remissinstanserna: *Nasdaq* är tveksam till möjligheten till nedsättning av avgiften grundat på särskilda skäl och frågar hur avgiftsbortfallet ska hanteras.

Riksbankens skäl: Bestämmelsen syftar till att reglera avgiften i de fall företagets skyldighet enligt Finansinspektionens beslut uppkommer eller upphör vid andra tidpunkter under året än vid ett årsskifte.

När Finansinspektionen har beslutat att ett företag ska genomföra tester träder Riksbankens skyldighet in att övervaka och samordna testerna och att utfärda intyg enligt 2 kap. 2 § kompletteringslagen, liksom företagets arbete med att förbereda och genomföra testerna. När ett företag inte längre omfattas av skyldigheten, upphör även Riksbankens ansvar. Det medför att om Finansinspektionens beslut innebär att ett företag endast omfattas av skyldigheten att genomföra tester under en del av ett år, ska avgiften justeras för det företaget med hänsyn tagen till vid vilken tidpunkt under året skyldigheten inträdde eller upphörde.

Skrivningen om nedsättning av avgiften om det finns särskilda skäl har tagits bort eftersom den bedömts som obehövlig i förhållande till den kategori av företag som avgiften omfattar. Riksbanken har dock som sagt för avsikt att se över och utvärdera den avgiftsmodell som valts.

Bestämmelsen finns i 6 § i föreskrifterna.

2.4 Beslut och betalning av avgift

Riksbankens ställningstagande: Riksbanken ska för varje år besluta den totala avgiftens storlek och skicka en faktura till respektive företag. Riksbankens beslut om avgift ska fattas under året efter det år som avgiften avser dock senast den 30 november samma år.

Dröjsmålsränta kommer att tas ut på avgifter som inte betalas i rätt tid, om det inte finns särskilda skäl emot det.

Remisspromemorian: Enligt förslaget skulle Riksbanken fatta beslut om avgifterna under första kvartalet året efter det år som kostnaderna uppkommit.

Remissinstanserna: *Bankföreningen* anser att den föreslagna ordningen gör det svårt för företagen att budgetera för avgiften och efterlyser uppgift om Riksbankens uppskattade avgiftsnivå minst 18 månader före beslut om avgift.

Riksbankens skäl: En bestämmelse om den praktiska hanteringen införs i föreskrifterna som anger när Riksbanken ska fatta beslut om den totala avgiftens storlek för ett visst år och skicka en faktura till de omfattade företagen. Riksbanken ska fatta sitt beslut senast den 30 november året efter det år som avgiften avser. Avgiften regleras i efterhand, eftersom det är först vid denna tidpunkt som Riksbanken har den fullständiga bilden av hur många företag som Finansinspektionen har beslutat ska genomföra tester och när under året företagens skyldighet inträder. Information om hur betalning ska ske ska anges på fakturan. Det föreslås att sedvanlig dröjsmålsränta enligt räntelagen (1975:635) tas ut vid dröjsmål med betalningen. Den föreslagna bestämmelsen om dröjsmålsränta är därför utformad med 6 § räntelagen som förebild. Bestämmelsen överensstämmer i tillämpliga delar med sin motsvarighet i Finansinspektionens avgiftsförordning.¹²

Bestämmelserna finns i 7 och 8 §§ i föreskrifterna.

Enligt 5 kap. 2 § andra stycket kompletteringslagen får Riksbankens beslut om avgift inte överklagas.

3 Ikraftträdande

Riksbankens ställningstagande: De nya föreskrifterna ska träda i kraft den 1 januari 2026.

Remisspromemorian: Förslaget hade samma innehåll.

Remissinstanserna: De remissinstanser som yttrat sig har inte haft några synpunkter på förslaget.

Riksbankens skäl: DORA-förordningen började tillämpas den 17 januari 2025 (artikel 64 andra stycket). Kompletteringslagen och övriga lagändringar som föranleds av DORA-förordningen trädde i kraft den 17 januari 2025. För att få tillräckligt med tid för att bereda förslaget, ha ett remissförfarande och vidta anpassningsåtgärder ska Riksbankens nya föreskrifter om avgifter träda i kraft den 1 januari 2026.

Den föreslagna avgiften är en ny avgift och några äldre bestämmelser behöver inte ändras. Något behov av övergångsbestämmelser till de föreslagna föreskrifterna finns därför inte.

4 Förslagets konsekvenser

Föreskrifterna är en följd av DORA-förordningen. Företag som är undantagna från förordningens tillämpningsområde enligt artikel 2.3 i DORA-förordningen omfattas inte av föreskrifterna. Av de företag som omfattas av DORA-förordningen avser föreskrifterna endast företag som har central betydelse för det finansiella systemet och som Finansinspektionen beslutat ska utföra särskilda hotbildsstyrda penetrationstester. Antalet företag som kommer att omfattas av föreskrifterna från och med ikraftträdandet är än så länge okänt men förväntas vara mellan tio och tolv företag.

Regelrådet bedömer att konsekvensutredningen inte uppfyller kraven i förordningen (2024:183) om konsekvensutredningar: Enligt Regelrådet är beskrivningen av berörda företag otydlig, beskrivningen av alternativa lösningar otillräcklig och det saknas en

¹² Förordningen (2007:1135) om årliga avgifter för finansiering av Finansinspektionens verksamhet.

redogörelse för förslagens påverkan på företagens intäkter. Regelrådet saknar även motivering till bedömning av konkurrenssituationen för särskilt små och medelstora företag. Regelrådet finner övriga delar tillräckligt tydligt redovisade och därmed godtagbara. *Konkurrensverket* efterlyser mer klarhet i konkurrenssituationen mellan de omfattade företagen och företag som inte omfattas av föreskrifterna.

4.1 Konsekvenser för samhället och konsumenterna

Riksbanken bedömer att föreskrifterna inte innebär några direkta konsekvenser för samhället och konsumenterna. Dessa föreskrifter är dock ett led i genomförandet av DORA-förordningens identifikation av svagheter, brister och luckor i den digitala motståndskraften hos företag av central betydelse för det finansiella systemet. I förlängningen syftar således föreskrifterna till att öka motståndskraften i inte minst betalningssystemet, att öka säkerheten för finansiella tjänster och tillgängligheten till vardagliga banktjänster genom att minska risken för dels driftsavbrott, dels att känsliga uppgifter kommer i orätta händer. Därmed kommer föreskrifterna till nytta för såväl enskilda konsumenter och hushåll som samhället i stort.

4.2 Konsekvenser för företagen

Föreskrifterna beräknas från ikraftträdandet att omfatta cirka tolv svenska företag som Finansinspektionen bedömt ha så central betydelse för det finansiella systemet att företagen måste genomföra hotbildsstyrda penetrationstester. Exempel på sådana företag är större kreditinstitut, försäkringsföretag, börser och värdepapperscentraler. Enligt förarbetena till kompletteringslagen kan det sammanlagt röra sig om högst ett 20-tal svenska företag.¹³ De företag som Finansinspektionen beslutar ska genomföra hotbildsstyrda penetrationstester kommer att få ökade kostnader med anledning av föreskrifterna.

Riksbankens årliga avgift för övervakning och samordning av företagens hotbildsstyrda penetrationstester kommer att variera beroende på vilket typ av företag det handlar om. Avgiftsmodellen syftar till att vara väl avvägd och proportionell, se avsnitt 2.2 för en närmare motivering och redogörelse för alternativa lösningar.

De föreslagna föreskrifterna bedöms inte få någon avgörande påverkan på konkurrensen inbördes mellan de företag som omfattas av föreskrifterna. Riksbanken har genom den avgiftsmodell som valts strävat efter att begränsa sådana effekter. Även om inte Riksbanken idag har uppgifter om exakt vilka företag Finansinspektionen kommer att besluta om, så omfattar DORA flera olika typer av aktörer med skilda verksamheter som till exempel marknadsplatser, kreditinstitut och försäkringsbolag. Riksbankens avgiftsuttag är emellertid grundat på bemyndigande i svensk lag. Eftersom avgiftsuttag och hantering av kostnader inte är EU-harmoniserade går det inte att utesluta att andra länder valt alternativa lösningar som kan påverka det egna landets företag mer eller mindre jämfört deras svenska motsvarigheter.

Det är osäkert att i förväg ge en mer konkret uppgift om avgiftens storlek, men enligt Riksbankens preliminära antaganden torde det handla om omkring en miljon kronor beroende på företag, se avsnitt 2.2. Även om avgiften kan uppfattas som hanterbar för de

¹³ Prop. 2024/25:44 s. 150.

företag som kan komma i fråga, kan den, som alla kostnader, potentiellt påverka företagets resultat. Det ska dock i sammanhanget understrykas att de företag som omfattas av föreskrifterna är av central betydelse för det finansiella systemet. Testerna som avgifterna avser syftar till att göra både företagen och det finansiella systemet mer motståndskraftigt mot digital påverkan genom identifikation av svagheter, brister och luckor i den digitala motståndskraften. I förlängningen syftar således föreskrifterna till att öka säkerheten genom att minska risken för driftsavbrott och risken för att känsliga uppgifter kommer i orätta händer.

Den del av Riksbankens verksamhet som utgör grunden för avgiftsuttag enligt föreskrifterna är beroende av flera faktorer som Riksbanken inte kontrollerar, exempelvis Finansinspektionens beslut om vilka företag som ska omfattas av testerna. Hur väl Riksbankens antaganden om arbetsinsats och kostnader kommer att överensstämja med de faktiska är något som får visa sig när arbetet bedrivits under tillräckligt lång period. Den valda avgiftsmodellen kommer därför att bli föremål för utvärdering som i sin tur kan ge skäl till justering.

4.3 Konsekvenser för Riksbanken

Riksbanken får genom kompletteringslagen nya uppgifter och befogenheter. En av dessa befogenheter är att besluta om att täcka Riksbankens kostnader för att övervaka och samordna genomförandet av de omfattade företagens hotbildsstyrda penetrationstester. Riksbanken kommer således att genom föreskrifterna erhålla full kostnadstäckning för arbetet med de hotbildsstyrda penetrationstesterna vilket medför att verksamheten inte innebär några ökade kostnader för Riksbanken.

Riksbanken kommer att utvärdera den föreslagna avgiftsmodellen.

4.4 Konsekvenser för förvaltningsmyndigheter och domstolar

Föreskrifterna bedöms inte få några konsekvenser för andra förvaltningsmyndigheter. Eftersom Riksbankens beslut om avgifter inte får överklagas enligt kompletteringslagen bedöms förslaget inte få några konsekvenser för domstolarna.

4.5 Förhållandet till unionsrätten

Riksbanken bedömer att de föreslagna föreskrifterna överensstämmer med och inte går utöver Sveriges skyldigheter som medlemsstat i EU.

4.6 Ikraftträdande och särskilda informationsinsatser

Föreskrifterna ska träda i kraft den 1 januari 2026. Vissa av företagen som kan komma att omfattas av Finansinspektionens beslut om hotbildsstyrda penetrationstester har tidigare genomfört tester inom ramen för TIBER-programmet. Testerna under DORA-förordningen bygger också de på TIBER-ramverkets som flera av företagen redan frivilligt genomför tester under. Dessa företag kommer därmed att kunna dra nytta av sina tidigare erfarenheter av hotbildsstyrda penetrationstester. Om ett företag som ska genomföra hotbildsstyrda penetrationstester inte tidigare har varit föremål för tester under TIBER-ramverket kan de emellertid kunna ha behov av de särskilda informationsinsatser som Riksbanken planerar.

4.7 Övriga konsekvenser

Föreskrifterna bedöms inte få några konsekvenser för jämställdheten mellan kvinnor och män. De bedöms inte heller medföra några sociala konsekvenser eller konsekvenser för miljön.

Riksbankens föreskrifter om avgifter för hotbildsstyrda penetrationstester

RBFS 2025:2

Beslutade den 3 december 2025

Riksbanken föreskriver följande med stöd av 2 kap. 6 § andra stycket lagen (2024:1278) med kompletterande bestämmelser till EU:s förordning om digital operativ motståndskraft för finanssektorn.

Tillämpningsområde

1 § Dessa föreskrifter innehåller bestämmelser om årliga avgifter för att finansiera Riksbankens verksamhet enligt 2 kap. 2 och 6 §§ lagen (2024:1278) med kompletterande bestämmelser till EU:s förordning om digital operativ motståndskraft för finanssektorn (kompletteringslagen).

2 § Termer och uttryck i dessa föreskrifter har i tillämpliga delar samma betydelse som i kompletteringslagen.

Vilka finansiella entiteter som omfattas

3 § Dessa föreskrifter gäller för de finansiella entiteter som Finansinspektionen beslutat ska genomföra hotbildsstyrda penetrationstester enligt 2 kap. 1 § kompletteringslagen.

Beräkning och uttag av avgifter

4 § Avgifterna ska över tid ge full täckning för Riksbankens direkta och indirekta kostnader för övervakning och samordning av de finansiella entiteternas genomförande av hotbildsstyrda penetrationstester samt utfärdande av sådana intyg som avses i 2 kap. 2 § andra stycket kompletteringslagen.

5 § Riksbanken ska årligen fördela de sammanlagda kostnader som avses i 4 § på de finansiella entiteter som avses i 3 § genom en avgift. Avgiften ska bestå av en fast och en rörlig del.

När det gäller den fasta delen ska 70 procent av de årliga kostnaderna fördelas jämnt mellan de finansiella entiteterna.

När det gäller den rörliga delen ska 30 procent av de årliga kostnaderna fördelas proportionellt mellan de finansiella entiteterna. Fördelningen ska baseras på den enskilda entitetens balansomslutning i förhållande till den samlade balansomslutningen för entiteter som avses i 3 §. Fördelningen ska utgå från entiteternas balansomslutning vid utgången av närmast föregående räkenskapsår.

6 § Om en finansiell entitet enligt ett sådant beslut som avses i 3 § omfattas av skyldigheten att genomföra hotbildsstyrda penetrationstester endast under en del av det år som avgiften avser ska entitetens avgift beräknas efter hur stor del av året som skyldigheten avser.

Beslut om avgift och betalning

7 § Riksbanken ska senast den 30 november året efter det år som avgiften avser besluta avgiftens storlek och skicka en faktura på det belopp som ska betalas samt ange när avgiften senast ska vara betald. Avgiften ska betalas genom insättning på det konto Riksbanken anger.

8 § Riksbanken får ta ut dröjsmålsränta på avgifter som inte betalas i rätt tid. Dröjsmålsräntan ska beräknas för varje år enligt en räntefot som motsvarar den av Riksbanken fastställda vid varje tid gällande referensräntan enligt 9 § räntelagen (1975:635) med ett tillägg av åtta procentenheter.

Dessa föreskrifter träder i kraft den 1 januari 2026.