



REMISSPROMEMORIA

DATUM: 2025-07-04

AVDELNING: AFS

HANDLÄGGARE: AFS/EIC

HANTERINGSKLASS: [Hanteringsklass]

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 1925-00974

Nya föreskrifter om avgifter för hotbildsstyrda penetrationstester

Sammanfattning

Riksbanken föreslår nya föreskrifter om avgifter för företag som genomför hotbildsstyrd penetrationstestning.

Bakgrunden till förslaget är EU:s förordning om digital operativ motståndskraft för finanssektorn (DORA-förordningen)¹. I förordningen finns det bestämmelser om testning av digital operativ motståndskraft vilket innebär att vissa företag (finansiella entiteter) ska genomföra 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 (finansiella entiteter) som ska genomföra hotbildsstyrd penetrationstestning samt hur ofta ett företag ska genomföra sådan testning. Riksbanken ska övervaka och samordna de hotbildsstyrda penetrationstesterna som ska genomföras enligt DORA-förordningen. Detta kommer innebära nya kostnader för Riksbanken. Dessa kostnader ska finansieras med avgifter från de företag som ska genomföra testerna.

Föreskrifterna föreslås träda 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	BAKGRUND	FEL! BOKMÄRKET ÄR INTE DEFINIERAT.
1.2	SYFTET MED FÖRESKRIFTERNA.....	4
1.3	ALTERNATIV REGLERING	4
1.4	RÄTTSLIGA FÖRUTSÄTTNINGAR	4
2	FÖRSLAG OCH MOTIVERING	4
2.1	FÖRETAG SKA BETALA EN ÅRLIG AVGIFT TILL RIKSBANKEN	4
2.2	STORLEK PÅ DEN ÅRLIGA AVGIFTEN	6
2.3	MINSKNING OCH NEDSÄTTNING AV ÅRLIG AVGIFT I VISSA FALL.....	7
2.4	BESLUT OCH BETALNING AV AVGIFT.....	8
3	IKRAFTTRÄDANDE	8
4	FÖRSLAGETS KONSEKVENSER	9
4.1	KONSEKVENSER FÖR SAMHÄLLET OCH KONSUMENTERNA	9
4.2	KONSEKVENSER FÖR FÖRETAGEN	9
4.3	KONSEKVENSER FÖR RIKSBANKEN.....	10
4.4	KONSEKVENSER FÖR FÖRVALTNINGSMYNDIGHETER OCH DOMSTOLAR	10
4.5	SÅ FÖRHÅLLER SIG FÖRSLAGET TILL UNIONSRÄTTEN	10
4.6	IKRAFTTRÄDANDE OCH SÄRSKILDA INFORMATIONSSINSATSER.....	10
4.7	ÖVRIGA KONSEKVENSER	11

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. Detta gäller bland annat krav på företagets riskhantering när det gäller informations- och kommunikationsteknik, incidentrapportering, hantering av utlagd verksamhet och testning av digital operativ motståndskraft. 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.

Bestämmelserna om testning av digital motståndskraft innebär att företagen ska inrätta, upprätthålla och se över ett sunt och heltäckande program för testning. Testprogrammet ska innehålla bestämmelser om utförande av lämpliga tester såsom bland annat sårbarhetsanalyser, nätverkssäkerhetsbedömningar, fysiska säkerhetsgranskningar och penetrationstester.

Vissa företag som har en central betydelse för det finansiella systemet ska dessutom regelbundet genomföra avancerad testning baserad på hotbildsstyrda penetrationstester. Dessa tester ska utformas i enlighet med det av Europeiska centralbanken utvecklade testramverket TIBER-EU⁴ och innehålla så kallade red-team-tester. Med red-team-tester menas att det anlitas en aktör som utger sig för att vara en antagonistisk part och som sedan har i uppdrag att försöka göra ett intrång mot en organisation. När ett test har avslutats ska företaget förse 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.

Riksbanken har antagit TIBER-programmet⁵ i Sverige och övervakar och koordinerar i dag de frivilliga tester som genomförs av systemviktiga företag inom ramen för programmet. I samband med att DORA-förordningen har trätt i kraft kommer vissa företag som idag genomför TIBER-tester i stället att genomgå obligatoriska tester enligt DORA-förordningen. Enligt 2 kap. 2 § kompletteringslagen ska Riksbanken övervaka och samordna de hotbildsstyrda penetrationstester som ska genomföras enligt artikel 26 och 27 i DORA-förordningen. Vidare ska Riksbanken utfärda sådana intyg som avses i artikel 26.7 i DORA-förordningen.

Eftersom Riksbankens verksamhet med övervakning och samordning kommer att utvidgas med anledning av det nya uppdraget kommer det även att innebära kostnader för

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= Threat Intelligence-Based Ethical Red teaming.

⁵ 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. Testerna är frivilliga.

Riksbanken. Enligt 2 kap. 6 § kompletteringslagen får Riksbanken ta ut avgifter från de företag som genomför hotbildsstyrd penetrationstestning. Vidare får Riksbanken meddela föreskrifter om dessa avgifter.

1.2 Syftet med föreskrifterna

Inom den finansiella sektorn finansieras myndighetsutövning mot enskilda vanligtvis genom avgifter. Enligt kompletteringslagen ska även Riksbankens verksamhet som rör hotbildsstyrda penetrationstester enligt DORA-förordningen finansieras genom avgifter. Syftet med föreskrifterna är att reglera hur avgifterna ska beräknas och tas ut av de företag som ska genomföra hotbildsstyrd penetrationstestning.

1.3 Alternativ reglering

Ett alternativ till att utfärda föreskrifter är att inte utfärda några föreskrifter och i stället besluta om avgiften enligt kompletteringslagen. De frivilliga testerna som i dag genomförs inom TIBER-programmet regleras genom avtal mellan Riksbanken och de företag som testas. I avtalen finns bland annat bestämmelser om avgifter. De hotbildsstyrda penetrationstesterna enligt DORA-förordningen kommer att bli obligatoriska och enskilda företag kommer att bli föremål för myndighetsutövning från Riksbankens sida. För att det ska bli förutsägbart hur avgifterna beräknas och för att berörda företag och andra instanser ska få lämna synpunkter på förslaget om avgifter, bör avgifterna regleras genom föreskrifter.

Riksbankens överväganden kring avgiftsmodellen finns i avsnitt 2.2. Som alternativ till den föreslagna avgiftsmodellen skulle avgifterna också kunna bestämmas genom 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.

2 Förslag och motivering

2.1 Företag ska betala en årlig avgift till Riksbanken

Riksbankens förslag: De svenska företag (finansiella entiteter) som Finansinspektionen beslutar ska genomföra hotbildsstyrda penetrationstester ska betala en årlig avgift till Riksbanken. Avgiften ska över tid ge Riksbanken full kostnadstäckning för den verksamhet som är hänförlig till övervakning och samordning av de hotbildsstyrda penetrationstesterna.

Skälen för förslaget: DORA-förordningen är tillämplig på de flesta företag som är verksamma inom den finansiella sektorn. I förordningen benämns dessa som finansiella

entiteter.⁶ Som exempel omfattas kreditinstitut, betalningsinstitut, värdepapperscentraler, centrala motparter och försäkringsföretag. För att det ska bli tydligt vilka som omfattas av de föreslagna föreskrifterna används begreppet finansiella entiteter för de företag som föreslås omfattas av föreskrifterna. I förslaget till föreskrifter görs en dynamisk hänvisning till DORA-förordningen, dvs. hänvisningarna avser förordningen vid den vid varje tidpunkt gällande lydelsen. Det innebär bland annat att om tillämpningsområdet för DORA-förordningen förändras, kan det påverka tillämpningsområdet för de föreslagna föreskrifterna. I denna remisspromemoria används både begreppen företag och finansiella entiteter för de företag som omfattas av de föreslagna föreskrifterna.

Bestämmelser om vilka företag som kan bli föremål för hotbildsstyrda penetrationstester finns i artikel 26 i DORA-förordningen. Kriterierna för vilka företag som kan bli föremål för tester specificeras ytterligare i artikel 2 i kommissionens delegerade förordning gällande hotbildsstyrda penetrationstester.⁷ Enligt kompletteringslagen är det Finansinspektionen som beslutar vilka företag som ska genomföra hotbildsstyrda penetrationstester. Riksbanken får ta ut avgifter från de företag som genomför hotbildsstyrda penetrationstester och meddela föreskrifter om avgifterna. Riksbanken föreslår att samtliga företag som Finansinspektionen beslutar ska genomföra tester ska betala en avgift till Riksbanken.

Avgifter i statlig verksamhet regleras av avgiftsförordningen (1992:191). Den gäller dock endast myndigheter under regeringen. Riksbanken är en myndighet under riksdagen och omfattas således inte av förordningen. 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 och som enligt Ekonomistyrningsverkets föreskrifter om avgifter innebär att myndigheten ska beräkna avgifterna så att de på ett eller några års sikt täcker alla kostnader som direkt eller indirekt hör till den avgiftsbelagda verksamheten.⁸ Det 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.

Mot denna bakgrund föreslår Riksbanken att den avgift som ska betalas av de företag som Finansinspektionen beslutar ska genomföra hotbildsstyrda penetrationstester ska täcka samtliga kostnader (både direkta och indirekta kostnader) för Riksbankens verksamhet som är relaterad till övervakning och samordning av de hotbildsstyrda penetrationstester som ska genomföras inom ramen för kompletteringslagen och DORA-förordningen. I Riksbankens arbete med övervakning och samordning av de hotbildsstyrda penetrationstesterna ingår planering, genomförande och uppföljning av testerna. Vidare omfattar Riksbankens arbete även deltagande i gränsöverskridande tester samt

⁶ Se artikel 2.1 i DORA-förordningen.

⁷ 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.

⁸ Se 5 § i Ekonomistyrningsverkets föreskrifter och allmänna råd (ESVFA 2022:5) om avgifter.

internationellt arbete kopplat till samarbete och kunskapsutbyte med övriga EU-länder. Avgiften ska även täcka kostnaden för de intyg som Riksbanken utfärdar enligt 2 kap. 2 § andra stycket kompletteringslagen.

Den årliga avgiften ska ge full kostnadstäckning över tid. Det innebär att företagen ska bära både direkta och indirekta kostnader. Dessa kostnader kan variera över tid. Därför kan avgiften ett visst år bli högre eller lägre med anledning av att både de indirekta och direkta kostnaderna har ökat eller minskat.

Förslagen finns i 1–4 §§ i de föreslagna föreskrifterna.

2.2 Storlek på den årliga avgiften

Riksbankens förslag: De företag som Finansinspektionen beslutat ska genomföra hotbildsstyrda penetrationstester ska betala en årlig avgift till Riksbanken. Avgiften ska bestå av en grundavgift och ett avgiftstillägg.

Grundavgiften ska uppgå till ett belopp som motsvarar 70 procent av de totala kostnaderna som är hänförliga till Riksbankens verksamhet med övervakning och samordning av hotbildsstyrda penetrationstester och utfärdande av intyg för det år som avgiften avser. Grundavgiften ska fördelas jämnt mellan de finansiella entiteter som genomför hotbildsstyrda penetrationstester.

Avgiftstillägget utgör resterande 30 procenten av Riksbankens totala kostnader som är hänförliga till Riksbankens verksamhet med övervakning och samordning av hotbildsstyrda penetrationstester och utfärdande av intyg för det år som avgiften avser. Avgiftstillägget ska fördelas på de finansiella entiteter som genomför hotbildsstyrda penetrationstester under det år som avgiften avser. Balansomslutningen ska utgöra grund för fördelningen.

Skälen för förslaget: Enligt 2 kap. 2 § kompletteringslagen ska Riksbanken övervaka och samordna de hotbildsstyrda penetrationstester som ska genomföras enligt DORA-förordningen. I detta ingår bland annat att validera vilka kritiska eller viktiga funktioner som ska omfattas av testningen (artikel 26.2 tredje stycket) och att säkerställa att den testare som anlitas för utförandet av testet uppfyller de krav som ställs i förordningen (artikel 27). Med att övervaka och samordna avses även att säkerställa att den finansiella entiteten tillämpar den testmetod och det tillvägagångssätt som ska följas för varje specifik fas i testprocessen. Riksbanken uppskattar att antalet årsarbetskrafter som kommer att arbeta med övervakning och samordning samt utfärdande av intyg av de hotbildsstyrda penetrationstesterna under DORA-förordningen uppgår till mellan 3 och 4 stycken. Detta är en uppskattning som är gjord med utgångspunkt i att antalet företag som kommer att genomföra hotbildsstyrda penetrationstester uppskattas till mellan 8 och 12 stycken årligen. Detta innebär en ungefärlig årlig kostnad mellan 9 och 12 miljoner kronor (uppskattning för 2025). Både direkta och indirekta kostnader är då inkluderade.

Mellan 2 och 4 aktörer, som inte omfattas av DORA, kommer fortsättningsvis att genomföra frivilliga tester enligt TIBER-ramverket. Grunden för att ta ut avgifter enligt TIBER-programmet kommer fortsättningsvis att vara civilrättsliga avtal. Riksbanken kommer att se över modellen för avgiftsberäkningen av testerna under TIBER-programmet.

De företag som kan bli föremål för hotbildsstyrda penetrationstester varierar både vad gäller storlek och verksamhet. Riksbanken bedömer därför att det är mindre lämpligt att tillämpa en rak avgiftsmodell där alla företag betalar en lika stor andel av Riksbankens kostnader för övervakning och samordning av de hotbildsstyrda penetrationstesterna. I stället föreslås en modell där hänsyn tas till företagens balansomslutning. Eftersom det kan vara stor skillnad på de aktuella företagens balansomslutningar och de största företagen inte ska betala merparten av Riksbankens kostnader, delas avgiften upp i en fast och en rörlig del. Den fasta delen föreslås uppgå till 70 procent av Riksbankens totala kostnader och fördelas jämnt mellan de företag som är föremål för tester ett visst år. Den rörliga delen föreslås uppgå till resterande 30 procent av Riksbankens totala kostnader och beräknas utifrån företagens balansomslutningar. Enligt förslaget ska avgiftstillägget beräknas med utgångspunkt i företagens balansomslutning vid utgången av räkenskapsåret närmast före det år som avgiften avser. Bakgrunden till detta förslag är att Riksbanken inte ska behöva invänta företagets rapporter för det år som avgiften avser.

Den föreslagna avgiftsmodellen innebär att om det är 10 företag som är föremål för tester ett visst år och Riksbankens kostnader uppgår till 10 miljoner det året, kan avgiften komma att beräknas enligt följande exempel. Den fasta avgiften uppgår till 7 miljoner kronor vilket innebär att varje företag ska betala 700 000 kronor i fast avgift. Den rörliga avgiften kommer att uppgå till 3 miljoner kronor och om ett visst företag står för 5 alternativt 20 procent av företagets totala balansomslutning under det räkenskapsår som är närmast före det år som avgiften avser, ska det företaget betala ett avgiftstillägg på 150 000 respektive 600 000 kronor. Det innebär att den totala avgiften för det företaget uppgår till 850 000 alternativt 1,3 miljoner kronor.

Riksbanken bedömer att den föreslagna avgiftsstrukturen är proportionerlig eftersom avgiftens storlek kommer att vara beroende av respektive företags storlek. Mindre företag kommer att betala en lägre avgift och större företag kommer att betala en högre avgift. Även om vissa företag är mindre bedriver de en kritisk verksamhet eftersom Finansinspektionen har bedömt att de ska genomföra hotbildsstyrda penetrationstester. Därför bör inte avgiften endast beräknas med utgångspunkt i företagets storlek utan de mindre företagen måste också bära en del av kostnaden för Riksbankens verksamhet. Mot denna bakgrund bedömer Riksbanken att förslaget också är proportionerligt i förhållande till de större företagen eftersom avgiften är uppdelad i två delar vilket innebär att det inte endast är företagets storlek som utgör grund för beräkning av avgiftens storlek.

Förslagen finns i 5–7 §§ i de föreslagna föreskrifterna.

2.3 Minskning och nedsättning av årlig avgift i vissa fall

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

Om det finns särskilda skäl får Riksbanken i ett enskilt fall besluta att sätta ned avgiften.

Skälen för förslaget: Förslaget tar sikte på situationen när Finansinspektionen beslutar att ett företag ska genomföra hotbildsstyrda penetrationstester eller att ett företag inte längre ska genomföra sådana tester vid en viss tidpunkt på året.

Enligt 2 kap. 1 § kompletteringslagen ska Finansinspektionen besluta om vilka företag som ska genomföra hotbildsstyrda penetrationstester. Finansinspektionen ska också besluta om hur ofta en finansiell entitet ska genomföra sådana tester. Utgångspunkten är att ett test ska genomföras minst vart tredje år. När Finansinspektionen har beslutat att ett företag ska genomföra tester träder Riksbankens skyldighet in att övervaka och samordna och utfärda intyg dessa tester enligt 2 kap. 2 § kompletteringslagen och arbetet med att förbereda och genomföra testerna inleds. Det är alltså först när ett företag omfattas av skyldigheten att genomföra tester som Riksbanken ansvarar för att övervaka och samordna dessa tester. När ett företag inte längre omfattas av skyldigheten, upphör även Riksbankens ansvar för testerna. 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 när under året skyldigheten inträdde eller upphörde.

Riksbanken föreslår även att avgiften i ett enskilt fall ska kunna sättas ned om det finns särskilda skäl. Detta skulle kunna vara fallet om den beräknade avgiften inte står i proportion till ett företags storlek och ekonomiska möjligheter att betala avgiften.

Om avgiften minskas eller sätts ned för ett företag påverkar det avgifterna för de övriga företagen eftersom den totala avgiften för samtliga företag ett visst år ska ge Riksbanken full kostnadstäckning.

Förslagen finns i 8 och 9 §§ i de föreslagna föreskrifterna.

2.4 Beslut och betalning av avgift

Riksbankens förslag: Riksbanken ska för varje år besluta den totala avgiftens storlek och skicka en faktura till respektive företag. Riksbankens beslut om avgift ska fattas under det första kvartalet året efter det år som avgiften avser. Dröjsmålsränta kommer att tas ut på avgifter som inte betalas i rätt tid, om det inte finns särskilda skäl emot det.

Skälen för förslaget: En praktisk bestämmelse införs i föreskrifterna som anger att Riksbanken ska fatta beslut om den totala avgiftens storlek för ett visst år och skicka en faktura till respektive företag. Riksbanken ska fatta sitt beslut senast under det första kvartalet 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 företagen blev skyldiga att genomföra tester. 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.

Förslagen finns i 10 - 12 §§ i de föreslagna föreskrifterna.

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

3 Ikraftträdande

Riksbankens förslag: Riksbanken föreslår att de nya föreskrifterna ska träda i kraft den 1 januari 2026.

Skälen för förslaget: DORA-förordningen började tillämpas den 17 januari 2025 (artikel 64 andra stycket). Kompletteringslagen och övriga lagändringar som föranleds av DORA-förordningen och ändringsdirektivet trädde i kraft den 17 januari 2025. Riksbanken får enligt kompletteringslagen ta ut avgifter från de finansiella entiteter som genomför hotbildsstyrda penetrationstester utan att meddela föreskrifter om avgifterna. Riksbanken föreslår dock att föreskrifter meddelas för att det ska vara förutsägbart hur avgifterna beräknas och för att berörda företag och även andra instanser ska få lämna synpunkter på förslaget om avgifter.

Utformningen av föreskrifterna påverkas av Finansinspektionens beslut. Föreskrifterna gäller för de företag som Finansinspektionen beslutar ska genomföra hotbildsstyrda penetrationstester. Riksbanken har därför inväntat att Finansinspektionen påbörjat att ta beslut om vilka företag som ska genomföra hotbildsstyrda penetrationstester. De företag Finansinspektionen har beslutat ska genomföra tester har då möjlighet att lämna synpunkter på förslaget när det skickas ut på remiss. För att få tillräckligt med tid för att bereda förslaget, ha ett remissförfarande och vidta anpassningsåtgärder bör Riksbankens nya föreskrifter om avgifter träda i kraft den 1 januari 2026. Detta påverkar dock inte Riksbankens möjligheter att få full kostnadstäckning från företagen eftersom Riksbanken redan kan ta ut avgifter med stöd av den föreslagna kompletteringslagen.

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

4 Förslagets konsekvenser

Nedan redogör Riksbanken för de konsekvenser som Riksbanken bedömer att de föreslagna föreskrifterna får för samhället och konsumenterna, företagen, Riksbanken, förvaltningsmyndigheter och domstolar samt förhållandet till unionsrätten.

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-förordningen och som i förlängningen kan komma till nytta för enskilda konsumenter och hushåll. Detta eftersom förordningen syftar till 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.

4.2 Konsekvenser för företagen

Föreskrifterna träffar de företag som Finansinspektionen beslutar ska genomföra hotbildsstyrda penetrationstester. Det bör i första hand beröra större kreditinstitut, enstaka försäkringsföretag, börser och värdepapperscentraler. Enligt förarbetena till kompletteringslagen kan det sammanlagt röra sig om högst ett 20-tal svenska företag.⁹ De företag som Finansinspektionen beslutar ska genomföra hotbildsstyrda penetrationstester kommer få ökade kostnader med anledning av föreskrifterna. Dock

⁹ Prop. 2024/25:44 s. 150.

genomför redan flera av dessa företag motsvarande tester, dels i egen regi, dels inom ramen för TIBER-programmet. Företagens kostnader för genomförandet av ett test är dels egna interna kostnader men även kostnader för de konsulter som ska genomföra testerna.

Riksbankens årliga avgift för övervakning och samordning av hotbildsstyrda penetrationstester kommer att variera beroende på vilket typ av företag det handlar om. Uppskattningsvis kan den årliga avgiften variera mellan 500 000 och 1 500 000 kronor för respektive företag. Särskild hänsyn har tagits till mindre företag dels genom att avgiften delvis baseras på ett företags balansomslutning, dels genom att förslaget innehåller en bestämmelse som innebär att Riksbanken kan sätta ned avgiften om det finns särskilda skäl.

De föreslagna föreskrifterna bedöms inte påverka konkurrensen mellan företagen på marknaden.

4.3 Konsekvenser för Riksbanken

Riksbanken får genom förslaget till kompletteringslag nya uppgifter och befogenheter. En av dessa befogenheter är att besluta om avgifter för de företag som ska genomföra hotbildsstyrda penetrationstester. Arbetet med att administrera avgifterna kommer dock att vara en mindre del av Riksbankens arbete med dessa tester. Riksbanken bedömer därför att de föreslagna föreskrifterna endast kommer att medföra begränsade konsekvenser för Riksbanken. Riksbanken kommer genom de föreslagna föreskrifterna erhålla full kostnadstäckning för arbetet med de hotbildsstyrda penetrationstesterna vilket medför att förslaget inte innebär några ökade kostnader för Riksbanken.

Riksbanken kommer att utvärdera den föreslagna avgiftsmodellen efter tre år för att se om den kan behöva justeras.

4.4 Konsekvenser för förvaltningsmyndigheter och domstolar

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

4.5 Så förhåller sig förslaget 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

Det föreslås att de nya 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. Eftersom testerna under DORA-förordningen kan genomföras utifrån TIBER-ramverket kommer dessa företag ha tidigare erfarenhet från hotbildsstyrda penetrationstester. Om ett företag som ska genomföra hotbildsstyrda penetrationstester inte tidigare har varit föremål för tester under TIBER-programmet kan det finnas behov av särskilda

informationsinsatser för dessa företag. Riksbanken kommer vid behov att genomföra informationsinsatser.

4.7 Övriga konsekvenser

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