Protokollsbilaga B
Direktionens protokoll 2026-05-13, § 4

REMISSVAR

DATUM:	2026-05-13
ER REFERENS:	Fö2026/00576
DIARIENUMMER:	Dnr 2026-00635

Försvarsdepartementet

Europeiska kommissionens cybersäkerhetspaket med förslag om ändringar i cybersäkerhetsakten (EU 2019/881) samt riktade ändringar i NIS 2-direktivet (EU 2022/2555) KOM (2026)11,13

Sammanfattning

Riksbanken är positiv till EU-kommissionens förslag om ett EU-gemensamt ramverk för att hantera icke-tekniska risker i leveranskedjor för informations- och kommunikationstjänster (IKT), exempelvis till följd av en leverantörs hemvist. Eftersom den finansiella sektorn är gränsöverskridande och sammankopplad är det viktigt att förebygga risker för IKT-leveranskedjor inom hela EU som ett komplement till nationella krav. Därtill är Riksbanken positiv till att leverantörer av europeiska digitala identitetsplånböcker och företagsplånböcker oavsett storlek ska klassificeras som väsentliga entiteter och därmed omfattas av höga cybersäkerhetskrav. Möjligheten till säker och effektiv digital identifiering och signering är avgörande för många av de finansiella tjänster, inte minst betalningar, som företag och hushåll använder sig av.

Inledande kommentarer

I både funktionen som Sveriges centralbank och utifrån Riksbankens ansvar att bidra till finansiell stabilitet, och till att allmänheten ska kunna göra betalningar, är säkra leveranskedjor för informations- och kommunikationstjänster (IKT) av stor

Postadress: 103 37 Stockholm, **Besöksadress:** Brunkebergstorg 11
Telefon: 08-787 00 00, **Webb:** riksbank.se

betydelse. Det handlar följaktligen om såväl Riksbankens egen verksamhet, till exempel att tillhandahålla ett system för avveckling av betalningar, som Riksbankens ansvar i förhållande till den finansiella sektorn. Avseende det senare kan i sammanhanget lyftas fram att Riksbanken analyserar och övervakar cyberrisker i det finansiella systemet och ansvarar för att övervaka och samordna penetrationstester i enlighet med EU:s förordning om digital operativ motståndskraft för finanssektorn (DORA) [1]. Riksbanken har vidare till uppgift att definiera vilka företag som bedriver verksamhet som är av särskild betydelse för genomförandet av betalningar. Riksbanken ska övervaka dessa företags planering och förberedelser för att kunna fortsätta sin betalningsverksamhet även under fredstida krissituationer och vid höjd beredskap. Riksbanken föreslås från den 1 juli 2026 leda en ny operativ krishanteringsfunktion för att hantera allvarliga driftstörningar i det finansiella systemet.

Riksbankens yttrar sig över de förslag i remissen som bedöms vara relevanta utifrån Riksbankens verksamhet och ansvarsområden.

Ett nytt EU-ramverk för stärkt säkerhet i IKT-leveranskedjor

Riksbanken är positiv till EU-kommissionens förslag om ett EU-gemensamt ramverk för att hantera icke-tekniska risker med IKT-leveranskedjor, exempelvis till följd av en leverantörs hemvist. Den finansiella sektorn är i stor utsträckning digitaliserad. Det innebär ett omfattande beroende av informations- och kommunikationstjänster samt elförsörjning. För att minska den finansiella sektorns sårbarhet mot cyberangrepp behöver därför IKT-leveranskedjor vara robusta. Den geopolitiska utvecklingen understryker vikten av god beredskap mot operativa risker, inklusive antagonistiska hot från länder utanför EU. Det är därför viktigt att även risker i IKT-leveranskedjor som inte är av teknisk natur förebyggs.

Riksbanken anser att ett ändamålsenligt ramverk för att förebygga icke-tekniska risker bör bestå av en EU-gemensam del och en nationell del. På EU-nivå bör ramverket säkerställa en lägsta nivå av motståndskraft inom hela unionen. Detta eftersom den finansiella sektorn inom EU är gränsöverskridande och sammankopplad, vilket ger upphov till betydande spridningsrisker, bland annat i den nordisk-baltiska regionen som är av särskild betydelse för svenskt vidkommande. Det innebär att det är lämpligt att ha ett ramverk som möjliggör beslutfattande och mandat att agera på identifierade risker utifrån hela unionens intressen och som inte gör det möjligt för enskilda, eller ett fåtal, medlemsstater

[1] Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn.

att förhindra åtgärder. Det är därför ändamålsenligt att EU-kommissionen har en central roll i processen.

Riksbanken konstaterar vidare att beslut om förebyggande åtgärder kan få stora konsekvenser för företag och verksamheter inom EU. Beslut om att införa sådana åtgärder behöver därför vara välgrundade. Följaktligen bör beslutfattandet vara transparent och dels ge medlemsstaterna god insyn, dels ge utpekade leverantörer en möjlighet att höras.

Riksbanken anser att ramverket tydligt måste tillåta medlemsstater att ställa högre nationella krav. En lägsta nivå inom EU är som nämnts viktig för att undvika spridningsrisker, men givet vikten av en hög motståndskraft mot cyberangrepp för samhället och den nationella säkerheten måste det finnas möjlighet att kunna ställa högre krav nationellt för att förebygga icke-tekniska risker i IKT-leveranskedjor förknippade med tredjeländer. Den här typen av risker kan variera inom unionen exempelvis beroende på en medlemsstats geografiska läge.

Det föreslagna EU-ramverket för att hantera icke-tekniska risker med IKT-leveranskedjor har sin utgångpunkt i de samordnade säkerhetsriskbedömningarna som ska genomföras enligt artikel 22 i NIS 2-direktivet[2]. Riksbanken vill med anledning av detta uppmärksamma att den finansiella sektorn även omfattas av EU-förordningen DORA som innehåller ett EU-övergripande tillsynsramverk för kritiska tredjepartsleverantörer av IKT-tjänster och syftar till att hantera system- och koncentrationsrisker. Eftersom DORA är lex specialis i förhållande till NIS 2-direktivet,[3] anser Riksbanken att det är angeläget att klargöra hur förslaget om det nya EU-ramverket för icke-tekniska risker förhåller sig till DORA.[4] Klargörandet bör säkerställa en ändamålsenlig och likvärdig skyddsnivå för den finansiella sektorn, även avseende icke-tekniska risker i IKT-leveranskedjorna.

Ändringar i NIS 2-direktivet

Riksbanken är positiv till att EU-kommissionen föreslår att leverantörer av europeiska digitala identitetsplånböcker och företagsplånböcker oavsett storlek klassificeras som väsentliga entiteter och därmed omfattas av höga cybersäkerhetskrav. Möjligheten till säker och effektiv digital identifiering och signering är avgörande för många av de finansiella tjänster, inte minst betalningar, som företag och hushåll använder sig av.

[2] Europaparlamentets och rådets direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen.

[3] Direktivets bestämmelser om riskhanterings- och rapporteringsskyldigheter ska inte tillämpas på finansiella verksamhetsutövare som omfattas av DORA.

[4] Jfr prop. 2024/25:44 s.64.

I sammanhanget vill Riksbanken även lyfta fram vikten av att den finansiella sektorn inom EU och i Sverige aktivt förebygger de risker för nuvarande krypteringsmetoder som kvantdatorer kan innebära.

Avslutande kommentarer

Riksbanken är redo att bistå regeringen i förhandlingarna i EU om förslaget till cybersäkerhetspaket utifrån den roll och det ansvar som Riksbanken har och som har redogjorts för inledningsvis i detta yttrande.

På Riksbankens vägnar

Erik Thedéen
Riksbankschef

Erik Lenntorp
Biträdande stabschef

Beslutet har fattats av direktionen (riksbankschefen Erik Thedéen, förste vice riksbankschefen Aino Bunge samt vice riksbankscheferna Per Jansson och Göran Hjelm) efter föredragning av biträdande stabschefen Erik Lenntorp. I den slutliga handläggningen har chefen för stabsavdelningen, Susanna Grufman, medverkat.