Remissvar

Försvarsdepartementet
103 33 Stockholm
fo.remissvar@regeringskansliet.se

Finansinspektionen
Box 7821
103 97 Stockholm
Tel +46 8 408 980 00
finansinspektionen@fi.se
www.fi.se

2026-05-07

FI dnr 26-9731
(Anges alltid vid svar)

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

Ert dnr: Fö2026/00576

Sammanfattning

Finansinspektionen (FI) tillstyrker i huvudsak förslaget, men lämnar synpunkter på sju områden: (i) förhållandet CSA2–DORA, (ii) samordning med tillsynsramverket för kritiska IKT-tredjepartsleverantörer, (iii) IKT-försörjningskedjans säkerhetsramverk, (iv) incidentrapportering, (v) cyber-posture-certifiering, (vi) NIS2-ändringarnas effekter och (vii) proportionalitet och det nationella tillsynsmandatet.

FI ser positivt på det övergripande syftet att stärka unionens motståndskraft och cyberresiliens, samt att etablera ett ramverk för försörjningskedjor inom informations- och kommunikationsteknik (IKT).

FI anser dock att förslagen behöver utformas så att överlappande eller motstridiga krav gentemot finansiella företag och deras IKT-leverantörer undviks, samt att ansvarsfördelningen mellan CSA2[1], NIS2[2] och DORA[3] tydliggörs i såväl författningstext som motivering. Detta är särskilt viktigt mot bakgrund av NIS2:s bestämmelser om att sektorsspecifika EU-rättsakter som uppställer minst likvärdiga krav ska ges företräde.

1 Förhållandet mellan föreslagna CSA2 och DORA

(CSA2 artikel 1)

Förslagets innebörd

Cybersäkerhetsakten2 (CSA2) innehåller ett ramverk för IKT-försörjningskedjor som omfattar alla sektorer som faller under direktivet Nätverk och informationssystem 2 (NIS2), däribland finanssektorn. Förslaget saknar uttrycklig samordningsbestämmelse gentemot DORA-förordningen (EU) 2022/2554.

FI:s synpunkter

Den finansiella sektorn omfattas redan av ett sektorsspecifikt och direkt tillämpligt regelverk för digital operativ motståndskraft, DORA-förordningen, med krav på IKT-riskhantering, incidentrapportering, tredjepartsriskhantering och EU-tillsyn av kritiska IKT-tredjepartsleverantörer (CTPP).

[1] Förslag till Europaparlamentets och rådets förordning om ändring av Europaparlamentets och rådets förordning (EU) 2019/881 vad gäller mandatet för Europeiska unionens cybersäkerhetsbyrå (Enisa), den europeiska ramen för cybersäkerhetscertifiering och inrättande av ett ramverk för säkerhet i leveranskedjor för informations- och kommunikationsteknik (IKT), KOM(2026) 11 (cybersäkerhetsakten 2, CSA 2).

[2] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

[3] 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 (DORA-förordningen).

FI förordar att CSA2 kompletteras med en uttrycklig bestämmelse som klargör att DORA-förordningen äger företräde inom sitt tillämpningsområde, i syfte att säkerställa rättssäkerhet, konsekvent tillsyn och för att undvika överlappande eller motstridiga krav för finansiella entiteter.

2 Samordning med tillsynsramverket för kritiska IKT-tredjepartsleverantörer

(CSA2 artiklarna 3–5)

Förslagets innebörd

Förslaget utvidgar Enisas mandat avseende högriskleverantörbedömningar, riskanalyser och rapporteringsplattformar.

FI:s synpunkter

FI bedömer att leveranskedjeåtgärder kan vara relevanta även för finanssektorns systemrisker, men att samordning med tillsynsram för kritiska tredjepartsleverantörer av IKT-tjänster är nödvändig för att undvika motstridiga signaler och för bedömningar om leverantörsrisk och överlappande uppföljning. FI förordar därför obligatoriskt samråd och ömsesidigt erkännande av bedömningar mellan Enisa och ESA-systemet i frågor som direkt påverkar finansiella sektorn och leverantörer som är centrala för finanssektorn för att undvika parallella bedömningar av samma leverantörer.

3 IKT-försörjningskedjans säkerhetsramverk

(CSA2 artiklarna 98–111)

Förslagets innebörd

Kommissionen får identifiera nyckeltillgångar för IKT och peka ut högriskleverantörer. Berörda entiteter åläggs fasa ut komponenter från sådana leverantörer med sanktioner på upp till 7 procent av global omsättning.

FI:s synpunkter

FI förordar att eventuella beslut om identifiering av högriskleverantörer och krav på utfasning enligt CSA2 åtföljs av tydliga och proportionella övergångsbestämmelser. Det krävs även en nära samordning med DORA:s

ramverk för hantering av IKT-tredjepartsrisk och tillsyn av kritiska tredjepartsleverantörer av IKT-tjänster. Syftet är att undvika rättsliga konflikter, genomföranderisker och inkonsekvenser i finanssektorns avtals- och registerhantering, samt klargöranden av sanktionsbestämmelsernas förhållande till DORA för att säkerställa logisk tillämpning mellan olika rättsakter.

4 Incidentrapportering

(CSA2 artikel 15)

Förslagets innebörd

Förslaget etablerar en central inrapporteringspunkt under Enisa enligt principen one-incident-one-report.

FI:s synpunkter

Gällande förslaget om att etablera en central inrapporteringspunkt på EU-nivå under Enisa anser FI att detta måste följa utvecklingen och vara i linje med förslaget om incidentrapportering i Digital Omnibus.

Samtidigt bedömer FI att förslaget aktualiserar viktiga rättsliga, tillsynsmässiga och operativa frågor, särskilt för sektorer som redan omfattas av sektorsspecifika och direkt tillämpliga rapporteringsregimer, såsom finanssektorn enligt DORA-förordningen.

FI anser att en central inrapporteringspunkt under Enisa inte får leda till att DORA:s rapporteringssystem försvagas, kringgås eller i praktiken ersätts för finansiella företag. Genom DORA finns det redan ett fungerande rapporteringssystem för allvarliga IKT-relaterade incidenter som även har implementerats av de finansiella företagen. FI förordar därför att förslaget måste klargöra att DORA fortsatt utgör lex specialis för incidentrapportering i finanssektorn.

5 Cyber-posture-certifiering

(CSA2 artikel 71)

Förslagets innebörd

Förslaget utvidgar cybersäkerhetscertifiering till entiteters samlade cybersäkerhetsstatus. Certifieringen kan användas som antagande för överensstämmelse med regelkrav.

FI:s synpunkter

Om cyber-posture-certifiering används som presumtion för regelefterlevnad på ett sätt som i praktiken reducerar kraven på riskbaserad styrning, internkontroll och tillsynsprövning enligt DORA finns en påtaglig risk att DORA:s grundläggande ansats undergrävs. FI anser därför att cyber-posture-certifiering inte bör tillmätas tillsynsmässig verkan inom DORA:s tillämpningsområde, utan tydlig reglering som säkerställer att certifiering fungerar som ett komplement (och inte ersättning) till sektorsspecifik tillsyn och krav enligt DORA.

6 NIS2-ändringarnas effekter

(COM(2026) 13)

Förslagets innebörd

NIS2-ändringarna syftar till harmonisering och förenkling, inklusive certifiering som kontrollverktyg (compliance) för att demonstrera överensstämmelse med NIS2:s riskhanteringskrav.

FI:s synpunkter

FI förordar att DORA:s ställning som *lex specialis* för finansiella entiteters digitala operativa motståndskraft förblir fullt ut intakt, och att de förenklings- och harmoniseringsåtgärder som föreslås inom ramen för NIS2 inte ges någon rättslig eller tillsynsmässig verkan inom DORA:s tillämpningsområde.

7 Proportionalitet och nationellt tillsynsmandat

Förslagets innebörd

Förslagen ger kommissionen och Enisa väsentliga befogenheter avseende riskbedömning och åtgärder gentemot leverantörer.

FI:s synpunkter

FI förordar att beslut om EU-gemensamma riskbedömningar och åtgärder gentemot leverantörer som berör finansiella entiteter föregås av obligatoriskt samråd med berörda sektors- och tillsynsmyndigheter, i syfte att säkerställa proportionalitet, rättssäkerhet och samstämmighet med DORA:s tillsynsram, som nyligen trätt i tillämpning.

FINANSINSPEKTIONEN

Johan Almenberg
Generaldirektör

Stefan Sundman
Rådgivare

I detta ärende har generaldirektören Johan Almenberg beslutat. Rådgivaren Stefan Sundman har varit föredragande. I den slutliga handläggningen har också enhetschefen Erik Wingstrand deltagit.