2024-10-03 Finansinspektionen

Bankföreningens synpunkter på förslag till nya och ändrade föreskrifter till följd av Dora-förordningen

Svenska Bankföreningen har getts möjlighet yttra sig över rubricerad remiss från Finansinspektionen (FI). Bankföreningen begränsar sitt yttrande till de föreskrifter som gäller för banker.

Generella synpunkter

Bankföreningen ser positivt på FI:s ambition att undvika dubbelreglering i anslutning till att Dora-förordningen ska börja tillämpas den 17 januari 2025. Frågorna kring bankernas styrning, hantering av operativa risker, kontinuitetshantering, informationssäkerhet och it-verksamhet är dock djupt integrerade med övriga krav i Finansinspektionens föreskrifter om styrning, riskhantering och kontroll (FFFS 2014:1), operativa risker (FFFS 2014:4) samt informationssäkerhet och it-verksamhet (FFFS 2014:5). I de ändringsförslag som FI remitterat har IKT-relaterade aspekter i föreskrifterna ofta tagits bort utan vidare nyansering eller förklaring till hur ändringen ska tolkas i förhållande till Dora-förordningen. Detta medför att en rad tolkningsfrågor uppstår, vilka Bankföreningen redogör för nedan.

Bankföreningen förordar därför att FI beskriver hur Dora-förordningen förehåller sig till föreskrifterna i relation till bankernas styrning och samlade riskhantering där även kraven enligt 6 kap. 2 § lag om bank- och finansieringsrörelse behöver beaktas. Syftet med detta är att främja en tydlig och sammanhängande regelverksstruktur.

Föreskrifter om ändring i Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:1) om styrning, riskhantering och kontroll i kreditinstitut;

2 kap. 1 §

I remissprommemorian punkt 2.3.6 har FI angivit att kap. 2 föreskrifterna inte ska gälla för hantering av IKT-risker enligt Dora-förordningen. I Remissexemplar – SRK-föreskrifterna verkar hela 2 kap. 1 § föreskrifterna ha ändrats. Det bör förtydligas att detta enbart är ett tillägg (se motsvarande reglering i 5 kap. 1 § nytt andra stycke samt 10 kap. 1 § nytt andra stycke i föreskrifterna).

Besök (Visit):
Blasieholmsgatan 4B
Stockholm
Sverige (Sweden)

Post:
Box 7603
SE-103 94 Stockholm
Sverige (Sweden)

t: +46 (0)8 453 44 00

e: info@swedishbankers.se
www.swedishbankers.se

2 kap. 2 §
I remisspromemorian Nya och ändrade föreskrifter och allmänna råd till följd av Dora-förordningen punkt 2.3.6 har FI angivit att 2 kap. 2 § i föreskrifterna ska upphöra att gälla. I Remissexemplar – SRK-föreskrifterna har det inte noterats att 2 kap. 2 § föreskrifterna utgår. Vi tolkar det som att 2 kap. 2 § föreskrifterna ska utgå i sin helhet, detta bör förtydligas.

2 kap. 3 §
Aktuell paragraf anger att ett företag ska ha en dokumenterad riskaptit som omfattar företagets *alla slag av risker*. Samtidigt anger FI i remisspromemorian att bestämmelserna i 2 kap. föreskrifterna inte ska gäller för hantering av IKT-risker enligt Dora-förordningen vilket är motsägelsefullt. FI bör korrigera aktuell paragraf, alternativt beskriva hur aktuell paragraf ska tolkas i förhållandet till Dora-förordningen vad gäller omfattningen av de riskslag som ingår i aktuell föreskrift. I en sådan tolkning bör FI beakta att det i Dora-förordningen, artikel 6.1 anges att finansiella entiteter ska ha en sund, heltäckande och väldokumenterad IKT-riskhanteringsram *som en del av sitt övergripande riskhanteringssystem.*

2 kap. 9 §
Aktuell paragraf anger att ett företag ska ha en väl fungerande kontinuitetshantering som säkerställer att företagets viktigaste information bevaras samt att verksamheten upprätthålls vid ett avbrott eller en större verksamhetsstörning. Samtidigt ställer Dora-förordningen krav på åtgärder för att säkerställa kontinuiteten i den finansiella entitetens kritiska eller viktiga funktioner i artikel 11 och krav på förfaranden och metoder för återskapande och återställning i artikel 12. FI bör korrigera aktuell paragraf i föreskrifterna, alternativt beskriva hur aktuell paragraf ska tolkas vad gäller krav på kontinuitetshantering i förhållandet till Dora-förordningen. I förlängningen bör FI överväga att anpassa de kontinuitetsrelaterade delarna av föreskriften mot Basel Committee on Banking Supervision:s ”Principles for Operational Resilience”.

3 kap. 1 §
I remisspromemorian punkt 2.3.6 har FI angivit att kap. 3 föreskrifterna inte ska gälla för hantering av IKT-risker enligt Dora-förordningen. I Remissexemplar – SRK-föreskrifterna verkar hela 3 kap. 1 § föreskrifterna ha ändrats. Det bör förtydligas att detta enbart är ett tillägg (se motsvarande reglering i 5 kap. 1 § nytt andra stycke samt 10 kap. 1 § nytt andra stycke föreskrifterna).

5 Kap. 4 §
7 Kap. 3 § 9 p.
8 Kap. 3 § 5 p.
I remisspromemorian punkt 2.3.6 har FI angivit att bestämmelsen om riskhantering i samband med större förändringar (5 kap. 4 § föreskrifterna) inte längre ska gälla vid

införandet av nya eller väsentligt förändrade it-system vilket återges i remissexemplaret av SRK-föreskrifterna.

Införandet av nya eller väsentligt förändrade it-system har sällan ett egensyfte utan är i de flesta fall en del av nya, eller väsentligt förändrade, produkter, tjänster, marknader och processer. Detta gör den nya utformningen av aktuell paragraf svår att tolka. Bankföreningen delar inte heller FI:s bedömning att motsvarande krav i Dora-förordningen återfinns i artiklarna 6 och 7. I viss mån kan kraven i artikel 8.3 i Dora-förordningen sägas motsvara kraven rörande it-system i aktuella paragrafer men där i saknas helt koppling till it-systems funktion i att stödja produkter, tjänster, marknader och processer.

Synpunkterna ovan gäller även för 7 Kap. 3 § 9 p. föreskrifterna och notera att i denna punkt har begreppet ”it-system” behållits. Synpunkterna ovan gäller även 8 Kap. 3 § 5 p. föreskrifterna där kraven på funktionen för regelefterlevnad beskrivs. Även i denna paragraf har begreppet ”it-system” behållits.

FI bör korrigera aktuella paragrafer, alternativt beskriva hur aktuella paragrafer ska tolkas vad gäller krav på riskhantering i samband med större förändringar i förhållandet till Dora-förordningen. FI bör i sammanhanget på paragrafnivå ange vilka krav i Dora-förordningen som motsvarar aktuell paragraf i SRK-föreskriften.

7 kap. 3 §
Aktuell paragraf anger att funktionen för riskkontroll ska kontrollera att *alla väsentliga risker* som företaget exponeras för eller kan förväntas komma att exponeras för identifieras och hanteras. Samtidigt anger FI i remisspromemorian att det i 2 kap. föreskrifterna införs en begränsning som innebär att föreskrifterna inte gäller för sådan hantering av IKT-risker som avses i Dora-förordningen.

FI bör beskriva hur aktuell paragraf ska tolkas i förhållande till Dora-förordningen vad gäller omfattningen av de riskslag som funktionen för riskkontroll ska kontrollera. Exempelvis bör FI utreda och beskriva om den kontrollfunktion som beskrivs i Dora-förordningen artikel 6.4 motsvarar funktionen för riskkontroll i aktuell paragraf.

Föreskrifter om ändring i Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:4) om hantering av operativa risker;

5 kap. 1 §
Aktuell paragraf anger att ett företag ska fastställa och i en förteckning ange vilka processer i verksamheten som är av väsentlig betydelse. Samtidigt ställer Dora-förordningen en rad krav på finansiella entiteters riskhantering av kritiska eller viktiga funktioner. Att två snarlika begrepp, som har mycket central betydelse för företagens riskhantering, nu återfinns i aktuell föreskrift respektive Dora-förordningen gör det utmanande för företagen i anpassningen till Dora-förordningen.

FI bör därför beskriva hur aktuell paragraf ska tolkas i förhållande till Dora-förordningen och det i Dora-förordningen definierade begreppet ”kritisk eller viktig funktion”.

5 kap.
Process för godkännande
Nya 8 § och 9 § 1 p.
I 8 § föreskrifterna har begreppet ”it-system” tagits bort. Därmed uppstår samma otydlighet i förhållande till Dora-förordningen som Bankföreningen noterat ovan i relation till reglerna i FFFS 2014:1; införandet av nya eller väsentligt förändrade it-system har sällan ett egensyfte utan är i de flesta fall en del av nya, eller väsentligt förändrade, produkter, tjänster, marknader och processer. Bankföreningen delar inte heller FI:s bedömning att motsvarande krav i Dora-förordningen återfinns i artiklarna 6 och 7. I viss mån kan kraven i artikel 8.3 i Dora-förordningen sägas motsvara kraven rörande it-system i aktuella paragrafer men där i saknas helt koppling till it-systems funktion i att stödja produkter, tjänster, marknader och processer.

I 9 § 1 p. föreskrifterna finns dock begreppet ”it-system” kvar vilket ytterligare försvårar förståelsen av reglerna för processen för godkännande.

FI bör korrigera aktuella paragrafer, alternativt beskriva hur aktuella paragrafer ska tolkas vad gäller krav på riskhantering i samband med större förändringar i förhållandet till Dora-förordningen. FI bör i sammanhanget på paragrafnivå ange vilka krav i Dora-förordningen som motsvarar aktuell paragraf i SRK-föreskriften.

Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:5) om informationssäkerhet, it-verksamhet och insättningssystem;

I remisspromemorian punkt 2.3.8 har FI angivit att it-föreskrifterna upphävs och ersätts av nya allmänna råd om insättningssystem. Bestämmelserna om informationssäkerhet och it-verksamhet försvinner därmed. I anslutning till de hänvisningar som FI gör till ett antal artiklar i Dora-förordningen på sidan 21 i remisspromemorian uppstår ett antal otydligheter i relation till de tidigare kraven i it-föreskrifterna;

- Kravet på ett ledningssystem för informationssäkerhet försvinner (2 kap. 1 § föreskrifterna). Är det därmed FI:s ståndpunkt att ett ledningssystem för informationssäkerhet är att likställa med en IKT-riskhanteringsram i enlighet med Dora-förordningen artikel 6?

- Kravet på att utse en person som ansvarar för att leda och samordna arbetet med informationssäkerhet försvinner (2 kap. 4 § föreskrifterna). De flesta banker har betraktat detta som CISO eller CSO. Bankföreningen utgår från att det även

fortsättningsvis ska vara möjligt för bankerna att ha en roll som CSO eller CISO i första försvarslinjen. Självfallet kommer funktion för riskkontroll, andra försvarslinjen, att ha ett ansvar för att övervaka och kontrollera även dessa risker, jfr artikel 5.2 c i Dora-förordningen.

Finansinspektionens föreskrifter om rapportering av incidenter och informationsregister enligt EU:s förordning om digital operativ motståndskraft för finanssektorn

Allmänna synpunkter på kraven om inrapportering av incidenter och informationsregister

Bankföreningen föreslår att FI bör erbjuda utbildning och förevisning av den nya inrapporteringen av incidenter och informationsregistret för företagen innan föreskrifterna träder i kraft. Detta borgar för att företagen förstår de nya inrapporteringsrutinerna vilket minskar risken för felaktig rapportering. Företagen får då också möjlighet att återkoppla eventuella förslag på förbättringar av rutinerna och inrapporteringssystemet.

Bankföreningen ställer sig också bakom Svensk Försäkrings förslag i sitt remissvar att flytta fram rapporteringen av informationsregistret till åtminstone den 31 maj 2025 med samma skäl som Svensk Försäkring anger.

4 §

I remisspromemorian punkt 2.1 har FI angivit att finansiella entiteter varje år ska skicka in hela sitt informationsregister till FI på det sätt som anges på FI:s webbplats med hänvisning till artikel 28.3 i Dora-förordningen. I aktuell artikel finns dock två olika bestämmelser om inrapportering i stycke tre respektive stycke fyra. I stycke tre ställs krav på att finansiella entiteter minst en gång per år ska rapportera till de behöriga myndigheterna om antalet nya arrangemang för användningen av IKT-tjänster m.m. medan det i stycke fyra ställs krav på att finansiella entiteter på begäran ska ge den behöriga myndigheten tillgång till det fullständiga registret. Såsom 4 § är formulerad i förslaget till nya föreskrifter är det oklart vilken av dessa två bestämmelser om inrapportering i Dora-förordningen som avses, eller om det är båda bestämmelserna som avses.

FI bör korrigera aktuell paragraf, alternativt beskriva hur aktuella stycken ska tolkas vad gäller krav på inrapportering av informationsregistret.

Finansinspektionens allmänna råd om rapportering av händelser av väsentlig betydelse;

FI föreslår att den incidentrapportering som ska ske enligt Dora-förordningen inte ska omfattas av Finansinspektionens allmänna råd om rapportering av händelser av väsentlig betydelse. Dock kvarstår skrivelser i de allmänna råden om att företagen bör rapportera händelser som kan härröra från fel i tekniska system.

FI bör korrigera aktuella skrivningar, alternativt beskriva hur termen ”tekniska system” förhåller sig till incidentrapporteringskraven i Dora-förordningen och mer specifikt förhållandet till FI förslag till föreskrifter om rapportering av incidenter och informationsregister.

SVENSKA BANKFÖRENINGEN

Hans Lindberg

Magnus Jacobson