2017-10-11

REMISSPROMEMORIA

Dnr 14-17730

Finansinspektionen
Box 7821
SE-103 97 Stockholm
[Brunnsgatan 3]
Tel +46 8 408 980 00
Fax +46 8 24 13 35
finansinspektionen@fi.se
www.fi.se

Förslag till tydligare krav på clearingorganisationers hantering av operativa risker

Sammanfattning

Finansinspektionen föreslår att företag som har tillstånd att driva clearingverksamhet enligt 19 kap. lagen (2007:528) om värdepappersmarknaden (LV) ska omfattas av bestämmelserna om informationssäkerhet och it-verksamhet i Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:5) om informationssäkerhet, it-verksamhet och insättningssystem. Enligt förslaget ska företagen även omfattas av vissa av bestämmelserna om kontinuitetshantering i 5 kap. Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:4) om hantering av operativa risker.

Tidigare har Finansinspektionen inte haft något bemyndigande att meddela föreskrifter om vad clearingorganisationer med tillstånd enligt LV ska iaktta i fråga om it-verksamhet och informationssäkerhet för att tillgodose de säkerhetskrav som är förenade med verksamheten. Från och med den 3 januari 2018 kommer myndigheten att ha ett sådant bemyndigande.

Finansinspektionen anser att det är viktigt att även clearingorganisationer med tillstånd enligt LV i sitt arbete med informationssäkerhet och kontinuitetshantering arbetar strukturerat och metodiskt. Det är också viktigt att det finns en tydlig målsättning och ansvarsfördelning för clearingorganisationers it-verksamhet och att de har ändamålsenliga processer för att hantera sina it-system. Därför föreslår Finansinspektionen att dessa företag ska omfattas av samma regler om it-verksamhet och informationssäkerhet som banker och kreditmarknadsföretag. Företagen bör redan i dag uppfylla krav motsvarande de nu föreslagna och förslaget bör därför påverka företagen i begränsad omfattning.

Samtidigt föreslås en ändring i Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker som inte berör clearingorganisationer. Genom en ändringsföreskrift som träder i kraft den 3 januari 2018 tas ett stycke bort i 1 kap. 5 §. Denna ändring var inte avsedd och stycket föreslås därför införas på nytt.

Ändringarna föreslås träda i kraft den 1 mars 2018.

Innehåll

1 Utgångspunkter

1.1 Bakgrund och målet med regleringen

Bristande hantering av operativa risker kan leda till förluster och störningar som allvarligt kan skada finansiella företag liksom förtroendet för och stabiliteten i hela den finansiella sektorn. Risker relaterade till informationssäkerhet och it-verksamhet är några av de största operativa riskerna för clearingorganisationer.

Det har under senare år förekommit angrepp mot finansiella företag genom till exempel dataintrång och överbelastningsattacker. Eftersom clearingorganisationer hanterar stora ekonomiska värden och känslig information är de naturliga mål för den här typen av angrepp.

Finansinspektionen anser att det är viktigt att clearingorganisationer i sitt arbete med informationssäkerhet och kontinuitetshantering arbetar strukturerat och metodiskt. Det är också viktigt att det finns en tydlig målsättning och ansvarsfördelning för clearingorganisationers it-verksamhet samt att de har ändamålsenliga processer för att hantera sina it-system.

För banker, kreditmarknadsföretag och värdepappersbolag gäller Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:4) om hantering av operativa risker och Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:5) om informationssäkerhet, it-verksamhet och insättningssystem. Vissa clearingorganisationer omfattas av regler om informationssäkerhet, it-verksamhet och kontinuitetsplaner genom EU-förordningar.

För de företag som har tillstånd att driva clearingverksamhet enligt 19 kap. lagen (2007:528) om värdepappersmarknaden (LV) saknas i dag detaljerade regler om vad företagen ska iaktta i fråga om it-verksamhet och informationssäkerhet för att tillgodose de säkerhetskrav som är förenade med verksamheten. Finansinspektionen har tidigare saknat bemyndigande att meddela föreskrifter i frågan. Från och med den 3 januari 2018 kommer myndigheten att ha ett sådant bemyndigande, vilket är skälet till att Finansinspektionen nu föreslår föreskrifter även för dessa företag.

I Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker passar Finansinspektionen dessutom på att återinföra 1 kap. 5 § andra stycket. Stycket togs bort av misstag i samband med genomförandet av en EU-rättsakt, genom Finansinspektionens föreskrifter (FFFS 2017:9) om ändring i Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker som träder i kraft den 3 januari 2018.

1.2 Nuvarande och kommande regelverk

De clearingorganisationer som står under Finansinspektionens tillsyn har huvudsakligen tre olika regelverk att förhålla sig till, nämligen
– LV,
– Europaparlamentets och rådets förordning (EU) nr 648/2012 av den 4 juli 2012 om OTC-derivat, centrala motparter och transaktionsregister (Emir), och
– Europaparlamentets och rådets förordning (EU) nr 909/2014 av den 23 juli 2014 om förbättrad värdepappersavveckling i Europeiska unionen och om värdepapperscentraler samt om ändring av direktiv 98/26/EG och 2014/65/EU och förordning (EU) nr 236/2012 (CSDR).

Förordningarna Emir och CSDR innehåller regler om informationssäkerhet, it-verksamhet och kontinuitetshantering för centrala motparter och värdepapperscentraler. Något motsvarande regelverk finns som sagt inte för de clearingorganisationer som har tillstånd enligt LV.

1.2.1 Nationella regler

Enligt 20 kap. 1 § LV har en clearingorganisation, som har tillstånd enligt samma lag, en skyldighet att driva verksamheten hederligt, rättvist och professionellt och på ett sätt så att allmänhetens förtroende för värdepappersmarknaden upprätthålls. Clearingorganisationen ska tillgodose de säkerhetskrav som är förenade med verksamheten.

Enligt Finansinspektionens allmänna råd (FFFS 2005:1) om intern styrning och kontroll av finansiella företag kan god intern kontroll bland annat säkerställas genom effektiv drift och förvaltning av informationssystem och uppnås till exempel genom kontroller för informationssäkerhet. De allmänna råden innehåller också regler om uppdragsavtal.

1.2.2 Internationella principer

De internationella organen Committee on Payments and Market Infrastructures (CPMI) och Internationella organisationen för värdepapperstillsyn (Iosco) har tagit fram principer som riktar sig till finansiella infrastrukturföretag (Principles for financial market infrastructures), främst centrala motparter, värdepapperscentraler och andra clearingorganisationer. Dessa internationella principer innehåller en mängd olika krav som finansiella infrastrukturföretag, som står under tillsyn, måste leva upp till för att betraktas som säkra och effektiva. Principerna omfattar bland annat informationssäkerhet, it-verksamhet och kontinuitetshantering.

Principerna har i stor utsträckning förts in i både Emir och CSDR, och därmed blivit bindande regler som centrala motparter och värdepapperscentraler ska följa.

Principerna riktar sig också till tillsynsmyndigheter och andra relevanta myndigheter, som övervakar och har tillsyn över marknaden för den finansiella infrastrukturen. Finansinspektionen följer principerna i sitt tillsynsarbete.

1.3 Regleringsalternativ

Kraven på de företag som har tillstånd att driva clearingverksamhet enligt LV i 20 kap. 1 § samma lag är allmänt hållna och de internationella principerna saknar motsvarighet i lag eller bindande föreskrifter.

Alternativet till bindande föreskrifter är att Finansinspektionen fortsätter att tillämpa Finansinspektionens allmänna råd om styrning och kontroll av finansiella företag eller meddelar nya allmänna råd med utgångspunkt från de internationella principerna. Eftersom informationssäkerhet, it-verksamhet och kontinuitetshantering är av stor vikt för de aktuella företagens verksamhet bedömer Finansinspektionen att det bör komma till uttryck i bindande föreskrifter vad som förväntas av företagen.

1.4 Rättsliga förutsättningar

Regeringen eller den myndighet som regeringen utser får enligt 20 kap. 8 § 1 LV meddela föreskrifter om vad en clearingorganisation ska iaktta i fråga om it-verksamhet och informationssäkerhet för att tillgodose de säkerhetskrav som är förenade med verksamheten enligt 20 kap. 1 § första stycket samma lag.

Regeringen har gett Finansinspektionen bemyndigande att från och med den 3 januari 2018 meddela föreskrifter om vad en clearingorganisation ska iaktta i fråga om it-verksamhet och informationssäkerhet för att tillgodose de säkerhetskrav som är förenade med verksamheten enligt 20 kap. 1 § första stycket LV (6 kap. 1 § 54 förordning [2017:712] om ändring i förordningen [2007:572] om värdepappersmarknaden som träder i kraft den 3 januari 2018).

Bemyndiganden till stöd för att införa det stycke som av förbiseende tagits bort i Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker finns i 5 kap. 2 § 5 förordningen (2004:329) om bank- och finansieringsrörelse och i 6 kap. 1 § 10–12 förordningen om värdepappersmarknaden.

1.5 Ärendets beredning

Finansinspektionen har i arbetet med att ta fram detta förslag till ändrade föreskrifter använt sig av en extern referensgrupp med representanter från Bankgirocentralen BGC AB och Euroclear Sweden AB. Referensgruppen har fått möjlighet att lämna synpunkter på att clearingorganisationer med tillstånd enligt LV ska omfattas av reglerna om kontinuitetshantering i 5 kap. Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker och reglerna om informationssäkerhet i 2 kap. och it-verksamhet i 3 kap. Finansinspektionens föreskrifter och allmänna råd om informationssäkerhet, it-verksamhet och insättningssystem.

2 Motivering och överväganden

Finansinspektionen redogör i avsnitt 2.1 för vissa inledande överväganden. I avsnitt 2.2 redogörs för förslaget att clearingorganisationer ska omfattas av 2 och 3 kap. Finansinspektionens föreskrifter och allmänna råd om informationssäkerhet, it-verksamhet och insättningssystem. I avsnitt 2.3 redogörs för förslaget till ändringar i Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker. Slutligen, i avsnitt 2.4 behandlas frågan om tidpunkten för ikraftträdande av de föreskriftsändringar som föreslås.

2.1 Inledande överväganden

Det framgår av 20 kap. 1 § LV att en clearingorganisation, som har tillstånd enligt LV, ska tillgodose de säkerhetskrav som är förenade med verksamheten. Enligt förarbetena till LV motsvaras 20 kap. 1 § närmast av 8 kap. 1 § i den upphävda lagen om börs- och clearingverksamhet (prop. 2006/07:115 s. 624). Av äldre förarbeten framgår att det är lagstiftarens avsikt att tillsynsmyndigheten, med stöd av bestämmelsen, ska ha möjlighet att ställa höga krav på att clearingorganisationer upprätthåller säkra tekniska system och att dessa system har en hög tillförlitlighet (prop. 1991/92:113 s. 59 och prop. 1995/96:50 s. 85). Lagstiftaren har dock, med hänsyn tagen till den snabba tekniska utvecklingen, valt att inte närmare precisera de tekniska kraven utan i stället överlåtit till tillsynsmyndigheten att pröva om de tekniska systemen är utformade så att de uppfyller olika krav.

Finansinspektionen föreslår att clearingorganisationer som har tillstånd enligt LV, ska tillämpa 2 och 3 kap. Finansinspektionens föreskrifter och allmänna råd om informationssäkerhet, it-verksamhet och insättningssystem och bestämmelserna om kontinuitetshantering i 5 kap. Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker. Härigenom blir det tydligare vad en clearingorganisation ska iaktta i fråga om informationssäkerhet, it-verksamhet och kontinuitetshantering för att tillgodose de säkerhetskrav som är förenade med verksamheten enligt 20 kap. 1 § LV.

Finansinspektionens förslag innebär att det är företagens it-verksamhet som kommer att omfattas av Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker. Med it-verksamhet avses företagets organisation, processer och personal för att hantera it-system. Begreppet är således inte nödvändigtvis begränsat till att omfatta det som i vissa företag traditionellt har benämnts som företagets it-avdelning.

CPMI och Iosco gav år 2016 ut en kompletterande vägledning om cybersäkerhet (Guidance on cyber resilience for financial market infrastructures) som beskriver hur finansiella infrastrukturföretag, som clearingorganisationer, kan arbeta för att upprätthålla sin motståndskraft mot cyberangrepp. Finansinspektionen har i arbetet med att ta fram det förslag som behandlas i

denna promemoria beaktat CPMI-Ioscos kompletterande vägledning om cybersäkerhet och övervägt alternativet att ge ut nya föreskrifter baserade på dessa principer. Finansinspektions sammantagna bedömning är att de förslagna reglerna om informationssäkerhet, it-verksamhet och kontinuitetshantering är tillräckliga.

2.2 Finansinspektionens föreskrifter och allmänna råd om informationssäkerhet, it-verksamhet och insättningssystem

Finansinspektionen föreslår att en clearingorganisation med tillstånd enligt LV ska omfattas av bestämmelserna om informationssäkerhet i 2 kap. och it-verksamhet i 3 kap. Finansinspektionens föreskrifter och allmänna råd om informationssäkerhet, it-verksamhet och insättningssystem.

Informationssäkerhet syftar till att skydda information. I detta ligger att ett företag ska kunna upprätthålla rätt nivå på informationens konfidentialitet, riktighet och tillgänglighet.

Bestämmelserna om it-verksamhet handlar om att ett företags tekniska system ska ha en viss säkerhet, att det ska finnas en tydlig målsättning för företagets it-verksamhet, att ansvaret för verksamheten är tydligt samt att det ska finnas ändamålsenliga processer och rutiner för hanteringen av systemen.

I 3 kap. 6 § hänvisas till var det finns föreskrifter om uppdragsavtal för andra företag än clearingorganisationer med tillstånd enligt LV. För clearing-organisationernas uppdragsavtal tillämpas även fortsättningsvis i stället 7 kap. Finansinspektionens allmänna råd om styrning och kontroll av finansiella företag.

I beslutspromemorian den 11 april 2014 (FI Dnr 11-11528 och 12-4167), som togs fram i samband med Finansinspektionens föreskrifter och allmänna råd om informationssäkerhet, it-verksamhet och insättningssystem, framgår mer om skälen för de bestämmelser som clearingorganisationer med tillstånd enligt LV ska tillämpa enligt Finansinspektionens förslag samt en förklaring av vissa kravs avsedda innebörd.

2.3 Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker

Finansinspektionen föreslår att clearingorganisationer med tillstånd enligt LV ska omfattas av bestämmelserna om kontinuitetshantering i 5 kap. Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker.

Företag som omfattas av Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker ska ha väl fungerande metoder för kontinuitets-hantering. Metoderna ska omfatta beredskapsplaner, kontinuitetsplaner och återställningsplaner.

I 1 kap. 2 och 3 §§ föreslås nödvändiga ändringar i tillämpningsområdet.

Enligt de föreslagna ändringarna i Finansinspektionens föreskrifter och allmänna råd om informationssäkerhet, it-verksamhet och insättningssystem ska en clearingorganisation ha ändamålsenliga processer för hur den hanterar sina it-system och dokumentera dem (se 3 kap. 4 §). Clearingorganisationerna föreslås dock inte omfattas av skyldigheten i 5 kap. 1 § Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker att i en förteckning fastställa vilka av processerna som är av väsentlig betydelse.

Eftersom hänvisningen i 5 kap. 16 § Finansinspektionens föreskrifter och allmänna råd om hanteringen av operativa risker till 5 kap. 1 § därmed inte omfattar clearingorganisationer föreslås ett nytt andra stycke i 5 kap. 16 §. Det nya stycket innebär att clearingorganisationerna ska, inom sin kontinuitetshantering, fastställa den längst tillåtna tiden för avbrott för sina processer av väsentlig betydelse.

Även i 5 kap. 23 § föreslås ett nytt stycke med anledning av att clearingorganisationer inte är skyldiga att fastställa processer enligt 5 kap. 1 §. Enligt det nya stycket ska clearingorganisationer minst årligen testa beredskapsplaner, kontinuitsplaner och återställningsplaner för sina processer av väsentlig betydelse.

Tilläggen i 5 kap. 16 och 23 §§ innebär att clearingorganisationerna indirekt måste ta ställning till vilka av deras processer som är av väsentlig betydelse.

I 5 kap. 18 § föreskrivs att en konsekvensanalys enligt 17 § samma kapitel ska genomföras på alla affärsenheter och stödfunktioner och ta hänsyn till deras beroende av varandra. Mot bakgrund av att begreppet it-verksamhet ska omfatta företagets organisation, processer och personal för att hantera it-system blir bestämmelsen tillämplig även på clearingorganisationernas affärsenheter och stödfunktioner i de fall dessa är en del av företagets it-verksamhet.

I den beslutspromemoria som nämnts i avsnitt 2.2 framgår mer om skälen för bestämmelserna i 5 kap. om kontinuitetshantering.

Finansinspektionen föreslår dessutom att 1 kap. 5 § andra stycket ska återinföras. Stycket togs bort av misstag i samband med genomförandet av en EU-rättsakt, genom Finansinspektionens föreskrifter (FFFS 2017:9) om ändring i Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker som träder i kraft den 3 januari 2018.

2.4 Ikraftträdande

Finansinspektionen föreslår att ändringarna ska träda ikraft den 1 mars 2018. Det bör ge berörda företag tillräckligt med tid för att, efter det att ändringarna har beslutats, göra nödvändiga förberedelser.

3 Förslagets konsekvenser

För en beskrivning av vad Finansinspektionen vill uppnå med ändringsförslagen och en beskrivning av vilka alternativa lösningar som finns för detta, och vilka effekterna blir om vi inte reglerar, se avsnitten 1.1 och 1.3. Se även en redogörelse för de bemyndiganden som ligger till grund för de föreslagna ändringarna i avsnitt 1.4.

Sverige har ingen skyldighet att införa regler om informationssäkerhet och it-verksamhet för clearingorganisationer som hanterar annat än finansiella instrument, men som framgår ovan anser Finansinspektionen att föreskrifter behövs för att tydliggöra det lagkrav om säkerhet som finns. Finansinspektionen bedömer att regleringen överensstämmer med och inte går utöver de skyldigheter som följer av Sveriges medlemskap i Europeiska unionen.

Nedan behandlas konsekvenserna av föreslagna ändringar som gäller clearingorganisationer med tillstånd enligt LV. Finansinspektionen gör bedömningen att det inte får några konsekvenser att ett stycke i 1 kap. 5 § Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker, som av misstag fallit bort, förs tillbaka.

3.1 Konsekvenser för samhället och konsumenterna

Finansinspektionen bedömer att de föreslagna ändringarna inte får några konsekvenser för samhället eller konsumenterna eftersom förslagen inte bedöms få några kostnadsmässiga konsekvenser för företagen.

3.2 Konsekvenser för företagen

Föreskrifter som närmare preciserar vilka krav som ställs på clearingorganisationers informationssäkerhet, it-verksamhet och kontinuitetshantering underlättar förutsägbarheten avseende vad lagkravet om säkerhet innebär för företagen.

3.2.1 Berörda företag

Föreskriftsändringarna berör för närvarande Bankgirocentralen BGC AB och Euroclear Sweden AB.

3.2.2 Kostnader för företagen

Kravet i LV på att clearingorganisationer ska tillgodose de säkerhetskrav som är förenade med verksamheten innebär, som anges ovan, att företagen redan bör uppfylla krav motsvarande de som nu föreslås. Finansinspektionen förslag

bör därför påverka berörda företag i begränsad omfattning och inte medföra några nämnvärda kostnadsökningar.

3.2.3 Konsekvenser för små företag

De föreslagna ändringarna bedöms inte få några konsekvenser för andra företag än de som nämns ovan.

3.3 Konsekvenser för Finansinspektionen

Som anges ovan anser Finansinspektionen att de föreslagna kraven på clearingorganisationerna redan tidigare har kunnat tolkas in i det krav som finns i LV. De föreslagna ändringarna innebär således inte ett ökat resursbehov.

3.4 Ikraftträdande och informationsinsatser

Ändringarna föreslås träda i kraft den 1 mars 2018.

Finansinspektionen bedömer inte att någon särskild hänsyn behöver tas när det gäller tidpunkten för ikraftträdande. Eftersom de föreslagna ändringarna i dag endast träffar ett fåtal företag är bedömning att det inte heller finns behov av speciella informationsinsatser utöver löpande dialog med de berörda företagen.