2014-01-14

Finansinspektionen
Box 7821
103 97 Stockholm

Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker

Inledning och sammanfattning

Svenska Bankföreningen (Bankföreningen) och Svenska Fondhandlareföreningen (FHF) vill inledningsvis framhålla att vi sätter värde i att Finansinspektionen (FI) har lyssnat och tagit till sig av branschens synpunkter i det förberedande arbete som har genomförts inom ramen för detta föreskriftsprojekt. På ett övergripande plan ställer vi oss positiva till förslaget som upplevs som genomarbetat och gediget med ett fokuserat innehåll. Förslaget väcker dock flera principiella frågeställningar bl.a. kopplat till ägandefrågor, bolagsstyrning och ansvarsfrågor där vi hänvisar till vårt remissyttrande i dnr 11-5610 (förslag till föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut). Vi anser också att förslaget i vissa delar bör omarbetas och i andra delar förtydligas eller tas bort helt.

Det är viktigt att föreskriften antar en neutral ställning i förhållande till företagen och inte har som utgångspunkt att samtliga företag har eller ska ha samma typ av riskmodeller.

En annan viktig fråga är ikraftträdandetidpunkten. Av förslaget framgår att föreskriften ska träda i kraft den 1 maj 2014. Några övergångsbestämmelser föreslås inte. Även om det är rimligt att tro att många av företagen som omfattas av bestämmelserna redan har stora delar av nödvändiga regler, rutiner och processer på plats så kommer det i en del fall att krävas ett omfattande arbete för att säkerställa att man till fullo lever upp till de nya kraven i föreskrifterna. Detta ska ses i ljuset av att nuvarande regler på området till stor del utgörs av allmänna råd och/eller rekommendationer som kan ha införts på olika sätt inom respektive företag. En annan viktigt aspekt är att FIs styrelse förväntas fatta beslut först under våren 2014. Innan föreskriften har fått sin slutliga utformning är det inte möjligt för företagen att bedöma i vilka avseenden och i vilken utsträckning FI kommer att ta intryck av de synpunkter som berörda intressenter redan lämnat vid olika seminarier, och som FI sagt sig komma att överväga, samt de synpunkter som berörda intressenter kommer att lämna in. Till detta kommer att företagen måste anpassa

Besök (Visit):
Regeringsgatan 38
Stockholm
Sverige (Sweden)

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

t: +46 (0)8 453 44 00
f: +46 (0)8 796 93 95
e: info@swedishbankers.se
www.swedishbankers.se

och implementera ett stort antal andra regelkomplex som kommer i närtid, bl.a. CRD 4. Eftersom företagen inte kan tillämpa regler som är under bearbetning så finns det starka skäl att överväga att införa en övergångsbestämmelse. För att företagen ska ges en rimlig möjlighet att anpassa sig till de nya kraven anser vi att en övergångsperiod på minst tolv månader är nödvändig.

För att nå en ändamålsenlig hantering bör en samordning ske mellan förslagets bestämmelser och övriga nationella och internationella regler som hanterar samma frågeställningar, inte minst med lagstiftning på området och kommande föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut. Vad som avses med t.ex. olika begrepp måste klaras ut och vara logisk, samt helt stämma med internationellt språkbruk och etablerade standarder. Ett exempel är uttrycket "critical" i GL 44 (EBA) som i EBAs översättning till svenska har tolkats som "viktig", medan FI i förslaget översatt/tolkat begreppet som "väsentlig". Om en avvikelse i begreppsapparaten sker från GL 44 eller om FI avser att samordna begreppsapparaten med annan svensk lagstiftning (t.ex. lagen om värdepappersmarknaden) bör det framgå av remisspromemorian var begrepp och definitioner är hämtade.

För att underlätta läsbarheten och nå effektivitet i hanteringen bör även hänvisningar till andra regelverk undvikas. Bland annat bör tillämpningsområdet och föreslagna definitioner skrivas ut i förslaget. Vidare bör sådana krav som instituten ändock har att följa enligt annan reglering i lag eller föreskrift tas bort, exempelvis att ett institut ska beakta tystnadsplikten som följer enligt lag.

Vi vill också framhålla att det stora antalet allmänna råd i förslaget, med hänsyn till att bestämmelserna i bland annat GL 44 (EBA) gäller som allmänna råd i Sverige, innebär att regelmassan sammantaget blir ogenomtränglig och svår att tillämpa. Det föreligger vidare en otydlighet och inkonsekvens vad gäller detaljnivån i regleringen genom att föreskrifter och allmänna råd har sammanblandats. De krav som företag har att uppfylla bör anges i föreskriftform. Exempel och förtydligande till föreskriftstexten bör ges i remisspromemorian och inte som allmänna råd i föreskriften. En sammanblandning av krav och råd ökar inte tydligheten eller förståelsen utan skapar förvirring. Som en konsekvens av detta bör namnet på föreskriften inte innehålla termen "allmänna råd".

Nedan lämnar vi mer detaljerade synpunkter på föreskriftens olika delområden.

Förslag till föreskrifter

1 kap. Definitioner

För att öka tydligheten anser vi att angivna definitioner ska vara ömsesidigt uteslutande. I 5 § är definitionen av beredskapsplan, kontinuitetsplan och återställningsplan snarlika. Det är oklart vad det bakomliggande syftet är med att dela upp dessa begrepp. Genom att definitionerna av begreppen är överlappande finns en klart ökad risk för begreppsförvirring. Vissa typer av planer hanterar vissa typer av risker vilket innebär att samtliga planer inte är relevanta för samtliga nivåer/produkter. Begreppet beredskapsplaner finns t.ex. i flera olika regelverk. Vi föreslår därför att definitionerna omarbetas så att det tydligt framgår att de olika planerna kan samlas i ett dokument som innehåller planer för såväl beredskap, kontinuitet och återställning och att det överlåts till företagen att använda egna namn på dokumenten. Detta påpekades även vid FI:s informationsmöte 10 december 2013 där FI ställde sig positiv till förslaget.

Vi föreslår därför att namn och definitioner följer standarderna i GL44 och i "Principles for the sound management of operational risk" så långt det är möjligt enligt följande:

- Kontinuitetshantering – ett institut ska etablera en god kontinuitetshantering för att säkerställa institutets förmåga att upprätthålla verksamheten och begränsa förlusterna vid en allvarlig störning i verksamhetens IT-system, kommunikationssystem och byggnader. Baserat på ovanstående bör institutet utarbeta:
    - beredskaps- och kontinuitetsplaner som säkerställer att det reagerar på nödsituationer på lämpligt sätt och kan upprätthålla sin viktigaste verksamhet om de vanliga rutinerna störs och
    - återställningsplaner för viktiga resurser, så att det kan återgå till sina vanliga rutiner inom rimlig tid. Eventuella återstående risker till följd av verksamhetsstörningar bör vara förenliga med institutets risktolerans/riskaptit
- Återställning definieras som återställning av viktiga resurser så som IT-system, kommunikationssystem och byggnader.

Ovan angiven formulering om planer för såväl beredskap, kontinuitet och återställning är relevant även för kap. 5 kap. 16 § punkt 1, 22 -24 §§.

Vidare anser vi att definitioner bör skrivs ut i föreskriften tillsammans med eventuell hänvisning till annan reglering, t.ex. definitionen av operativa risker där definitionen bör skrivas ut i paragrafen tillsammans med en hänvisning till EU förordning 575/2013 om tillsynskrav för kreditinstitut och värdepappersföretag.

2 kap. Styrning och ansvar

2 § andra stycket

I förslaget anges att "Om företaget använder risköverföring ska det ange principerna för detta i interna regler."

Bankföreningen och FHF anser att meningen skall strykas. Om FI finner att det inte är lämpligt bör begreppet risköverföring förtydligas.

Det är för närvarande otydligt vad begreppet risköverföring avser i föreskriften. En tolkning är att begreppet avser försäkringar och andra mekanismer för risköverföring, som har en märkbart riskreducerande effekt, i så motto att de medför lättnader i kapitalkravet för operativa risker. Om så är fallet är skrivningen relevant endast för institut som har Finansinspektionens godkännande att tillämpa en internmätningsmetod för operativa risker (AMA). Frågan om risköverföring är en av flera frågor som hanteras i ett AMA-godkännande, och det är oklart varför just risköverföring blir föremål för föreskriften, varför den bör strykas ur föreskriften.

Om begreppet risköverföring i föreskriften avser något annat, bör det framgå vad som avses, och inkludera väsentlighetsprincipen.

2 § sjätte stycket

Av förslaget framgår att "Styrelsen ska besluta om de interna reglerna".

Bankföreningen och FHF anser att det är styrelsens ansvar att fastställa dokument av policykaraktär medan VD ansvarar för att fastställa instruktioner och interna regler. Som definitionen är skriven ska samtliga skriftliga dokument fastställas av styrelsen vilket är en orimlig detaljering av arbetsfördelningen.

I aktiebolagslagen (ABL) och Svensk kod för bolagsstyrning regleras bl.a. styrelsens ansvar och uppgifter. Styrelsen ansvarar bl.a. för bolagets organisation och förvaltningen av bolagets angelägenheter. Styrelsen har möjlighet att delegera uppgifter till en eller flera av styrelsens ledamöter eller till andra. Oavsett om delegation har skett, inom eller utom styrelsekretsen, kan styrelsen aldrig avhända sig det yttersta ansvaret. Vid delegering bör styrelsen handla med omsorg och fortlöpande kontrollera om delegationen kan upprätthållas. Någon begränsning avseende styrelsens delegationsmöjlighet finns inte i bank- och finansieringsrörelselagen. Utgångspunkten måste därför vara, när det gäller vad som i föreskriften anges om styrelsens uppgifter, att dessa bestämmelser ska grundas på bl.a. ABLs regler. Det innebär att styrelsen även när den tillämpar föreskriften kan delegera uppgifter till kommittéer, utskott eller liknande. Det ställs till och med krav på inrättandet av kommittéer i en rad olika befintliga och föreslagna regleringar

såsom i ABL, Svensk kod för bolagsstyrning, GL 44 och CRD 4. Som anges i den associationsrättsliga regleringen har styrelsen dock alltid det yttersta ansvaret. Detta bör förtydligas så att det inte råder någon tveksamhet om att de möjligheter och skyldigheter som följer av ABL, såsom rätten att delegera frågor till kommittéer, också är tillämpliga för företag som är aktiebolag.

3 kap. Identifiering och mätning

1 §

I förslaget anges att "Ett företag ska identifiera operativa risker i sina produkter, tjänster, funktioner, processer och it-system".

Bankföreningen och FHF anser att bestämmelsen skulle bli tydligare om det anges att "Ett företag skall identifiera operativa risker i sin verksamhet" istället för att räkna upp ett visst antal områden. Detta ger företagen bättre möjlighet att anpassa identifieringen av operativa risker till den verksamhet som respektive företag driver. Föreslagen text gör det tydligare att riskarbetet bör fokuseras med utgångspunkt från företagets viktigaste leveranser och underliggande beroenden såsom IT, anläggningar och leverantörer.

4 § Riskindikatorer

I förslaget anges att "Ett företag ska fastställa indikatorer och gränsvärden för sina operativa risker som ger en förvarning om när riskerna har ökat".

Bankföreningen och FHF anser att följande ordalydelse är bättre: "ett företag ska fastställa egna indikatorer och gränsvärden för sina operativa risker som ger en indikation på att risken ökar".

Vi vill i detta sammanhang åter påpeka vikten av en övergångsbestämmelse för att ge företagen en rimlig möjlighet att införa meningsfulla riskindikatorer med kalibrerade gränsvärden.

Allmänna råd

Som vi inledningsvis nämnt anser vi att de allmänna råden bör placeras i remisspromemorian. Även om de allmänna råden placeras i promemorian saknar de produkt-, kund-, och systemdimensionen för att fungera som fullvärdiga indikatorer för operativa risker. Om syftet med indikatorerna ska kunna uppfyllas behöver de anpassas till det specifika företagets verksamhet. Det är därför viktigt att det av föreskrifterna framgår att företagen ska fastställa egna indikatorer som är baserade på verksamhetens art, omfattning och komplexitet. I remisspromemorian bör således tydligt klargöras att det endast är fråga om en exemplifiering av indikatorer och att

instituten inte behöver välja just dessa. Värdeord som frekvent, hög och många bör utgå.

6 § Incidenter

I förslaget anges att "Ett företag ska när det inträffar en incident dokumentera och analysera incidenten. Företaget ska även dokumentera de förluster som kan uppstå i samband med denna".

Bankföreningen och FHF anser att texten bör ändras till att " Ett företag ska dokumentera sina incidenter. Inträffade incidenter som har eller kan få en väsentlig negativ inverkan på företagets verksamhet, tillgångar eller förtroende ska analyseras".

Vi anser att det är viktigt att det införs ett väsentlighetskriterium och att väsentlighet bedöms bäst av företagen själv.

7 § Utläggning av verksamhet

I förslaget anges hur företaget ska hantera verksamhet som är utlagd i fråga om incidenter och förluster i den utlagda verksamheten.

Bankföreningen och FHF har svårt att förstå syftet med att dela upp incidenter som inträffat i olika delar av verksamheten oavsett om den är outsourcad eller ej. Vi anser att denna paragraf är onödig då kraven i paragrafen omfattas av 5 och 6 §§ samma kapitel. I sista meningen i 6 § anges att "Företaget ska använda uppgifterna i första stycket [uppgifter om incidenter] när det identifierar och mäter operativa risker enligt 3 §". Detta måste innefatta alla typer av incidenter, även sådana som inträffar i utlagd verksamhet. Skrivelsen i 7 § blir därför en dubbelreglering och bör därför tas bort.

4 kap. Rapportering

1 § tredje stycket

I förslaget anges att "företaget ska dessutom minst årligen informera styrelsen om resultatet från tester av beredskapsplaner, kontinuitetsplaner och återställningsplaner".

Bankföreningen och FHF föreslår att texten ändras till "att företaget ska dessutom minst årligen informera styrelsen om status för kontinuitetshantering". Begreppet kontinuitetshantering ger, enligt vårt förslag till förändring i 1 kap, mer relevant information till styrelsen.

5 kap. Hantering av operativa risker i verksamheten

Bankföreningen och FHF anser att en processdokumentation kan vara till hjälp för att identifiera brister och risker. För att detta ska vara effektivt måste dock processägarna ges ett så starkt mandat att detta i praktiken leder till att ett företags verksamhetsmodell kommer att vara processbaserad. Det kan inte vara så att valet av verksamhetsmodell ska styras av föreskriften för operativ risk, utan verksamhetsmodell måste rimligen bestämmas av verkställande ledning och styrelse. Dessutom krävs en mycket detaljerad kartläggning av processer, produkter och system för att fånga alla tänkbara risker. Det finns en risk att detta sker på bekostnad av andra, mer relevanta, riskmildrande åtgärder.
Vi anser därför att 1-4 §§ bör strykas i sin helhet.

Om FI inte är beredd att stryka 5 kap. 1-4§ i sin helhet så vill Bankföreningen och FHF få till stånd en övergångsperiod och övergångsregler så som angetts i inledningen av denna skrivelse. Detta för att företagen ska ges förutsättningar att implementera föreskrifterna samt att FI beaktar följande:

2 §
I förslaget anges att "Ett företag ska dokumentera processerna enligt 1 § och utse en ansvarig person för varje sådan process".

Bankföreningen och FHF anser att om FI inte anser att det är möjligt att stryka 2 § bör paragrafen förtydligas. Det bör framgå att dokumentationen måste anpassas till att vara relevant och användbar för institutet och att "processägaren ansvarar för processen" samt att processägaren skall vara en funktion och inte en person (se definitioner I föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut).

Vi vill åter påpeka vikten av en övergångsbestämmelse för att ge företagen en rimlig möjlighet att fullt ut uppdatera relevant dokumentation.

3 § Allmänna råd
Som nämnts inledningsvis bör de allmänna råden placeras i remisspromemorian. Av de allmänna råden framgår att företagets processdokumentation bör beskriva åtta komponenter. Vi anser att det bör vara upp till varje enskilt företag att bestämma hur processerna ska se ut och vilka relevanta beroenden som ska dokumenteras för att processdokumentationen ska vara värdefull och användbar för institutet.

5 § Personal
Av förslaget punken 1 framgår att ett företag ska "kontrollera nödvändiga uppgifter". Av samma punkt framgår att "kontroll ska ske av personal med sådana befattningar som har särskild betydelse för företagets riskexponering".

Bankföreningen och FHF anser att begreppet "nödvändiga uppgifter" är otydligt eftersom det inte framgår för vilket syfte uppgifterna ska vara nödvändiga. I remisspromemorian anges som förklaring bl.a. att uppgifter ska inhämtas för referenser eller verifiering av uppgifter vilket inte ger någon närmare vägledning. Syftet med kravet bör därför förtydligas i remisspromemorian. Det bör därvid beaktas att komponenterna kan ändras över tiden.

Vi anser också att det är oklart vad som avses med "personal med sådana befattningar som har betydelse för företagets riskexponering". Är avsikten att denna personalkategori ska definieras på samma sätt som risktagare definieras inom ramen för ersättningsregleringen eller ska kategorin avgränsas på annat sätt? Även detta bör förtydligas i författningstexten eller i remisspromemorian.

Av förslaget punkten 6 framgår att ett företag ska ha rutiner för hur det hanterar operativa risker i fråga om sin personal där det framgår hur företaget hanterar den tystnadsplikt som regleras i lag.

Bankföreningen och FHF anser, som anges inledningsvis, att generella krav som framgår av lagstiftning, som exempelvis tystnadsplikten, inte behöver nämnas i dessa föreskrifter. Denna del bör därför tas bort.

Av förslaget punkten 7 framgår att ett företag ska ha rutiner för hur det hanterar operativa risker i fråga om sin personal där det framgår hur företaget identifierar och hanterar operativa risker som kan uppstå i samband med personalens ledighet.

Bankföreningen och FHF anser att denna punkt kan strykas. Detta krav framgår redan indirekt av punkterna 2-4 samma stycke. I och med att dessa punkter anger att företaget ska ha tillräckligt med personal, se till att personalen har rätt kompetens och kunskap samt se till att kompetensen upprätthålls. Vidare framgår av den arbetsrättsliga regleringen och praxis att det är en arbetsgivarfråga att definiera hur många anställda ett företag ska ha. Ett företag har vissa uppgifter och regelverkskrav på sig att uppfylla. För detta behövs personal. Det kan därför ifrågasättas om det är nödvändigt att också uppställa ett krav på att det ska finnas personal. Det är också svårt att förutse hur ett sådant krav ska kunna granskas vid ett tillsynsärende eller hur efterlevnaden av detta krav ska bedömas om företaget uppfyller kraven i övrigt.

6 § Legala risker

Av förslaget framgår att med legala risker avses risken för att avtal eller andra rättshandlingar inte kan genomföras enligt angivna förutsättningar eller att rättsliga processer inleds som på ett negativt sätt kan påverka företagets verksamhet.

Bankföreningen och FHF noterar att det inte framgår vilken grund FI har använt för definitionen av legal risk. Enligt såväl CRD4/CRR, Basel II och BIS principer (Principles for the sound management of operational risk) ingår legal risk som en del av de operativa riskerna. Det saknas dock en tydlig definition av själva begreppet legal risk. Av Basel II framgår dock att "Legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements", vilket måste anses som en något otydlig och ofullständig definition som till viss del överlappar definitionen av regelefterlevnadsrisk. Mot denna bakgrund anser vi att grunden för definitionen bör beröras närmare i remisspromemorian. I remisspromemorian bör även anges vad som kan inbegripas i begreppet "andra rättshandlingar". Vidare bör en gränsdragning ske mot regelefterlevnadsrisk, framför allt i fråga om vad som ska anses omfattas av "på ett negativt sätt". Att något påverkas negativt kan innebära en påverkan av såväl finansiell som icke finansiell natur. Det innebär att definitionen av legal risk även kan inbegripa ryktesrisk till följd av att en rättsprocess inleds, oaktat om företaget vinner processen eller inte, eller risk för sanktioner. Detta innebär en överlappning med definitionen av regelefterlevnadsrisk.

Även om bakgrunden till definitionen i förslaget är okänd anser vi att texten bör omformuleras något. Med legala risker avses risken för att företaget lider skada på grund av att avtal eller andra rättshandlingar inte kan genomföras på avsett sätt eller inte får avsedd effekt eller att rättsliga processer inleds som på ett negativt sätt kan påverka företagets verksamhet.

7 §

Av förslaget punkten 1 framgår att ett företag ska i de interna reglerna ange på vilket sätt det säkerställer och följer upp att ingångna avtal eller andra rättshandlingar är korrekta och giltiga.

Bankföreningen och FHF anser att begreppet "andra rättshandlingar" bör förtydligas och avgränsas. Förtydligandet bör framgå av beslutspromemorian i enlighet med kommentaren för 6 §. Det är också oklart vad som avses med att "följa upp" vilket också bör framgå av föreskriften eller beslutspromemorian.

Av förslaget punkten 3 framgår att ett företag ska i de interna reglerna ange på vilket sätt det dels bevakar nya eller ändringar i de författningar som reglerar företagets tillståndspliktiga verksamhet, dels säkerställer att de följs.

Bankföreningen och FHF anser i första hand att punkten 3 skall strykas då hantering av ändrade regler inte ingår i definitionen av legal risk. Om FI inte anser att det är lämpligt anser vi att bestämmelsen måste samordnas med kraven, ansvarsfördelningen och terminologin i 8 kap. föreskrifterna om styrning, riskhantering och kontroll i kreditinstitut.

Av förslaget punkten 4 framgår att företaget ska ange på vilket sätt det arkiverar avtal och andra rättshandlingar.

Bankföreningen och FHF anser att det måste förtydligas vad som avses med "andra rättshandlingar" – är det en aktivitet eller ett dokument? Vidare bör i stycke 2 ändras så att det framgår att "De interna reglerna enligt första stycket ska även ange *vilken funktion* som ansvarar för hanteringen av 1-4".

8 § It-system

I förslaget anges att bestämmelser om hur ett företag ska hantera it-system finns i FIs föreskrifter om it-system, informationssäkerhet och insättningssystem.

Bankföreningen och FHF anser att paragrafen bör tas bort eftersom den inte fyller något syfte. Bestämmelserna i it-systemföreskriften gäller oavsett hänvisningen.

9 § Allmänna råd

Som vi inledningsvis nämnt anser vi att de allmänna råden bör placeras i remisspromemorian. Vidare anser vi att den andra meningen "När sådana händelser inträffar…" kan raderas eftersom den bör hanteras inom ramen för incidenthanteringen och blir därmed överflödig.

10 §

I förslaget anges var bestämmelserna om informationssäkerhet finns.

Bankföreningen och FHF anser, på samma sätt som ovan, att paragrafen raderas då den endast hänvisar till krav i annan föreskrift.

13 § Process för godkännande

Av förslaget punkten 2 framgår att ett företag ska se till att följande moment finns med i processen för godkännande: analys av om företagets risknivåer kan öka eller om nya risker kan uppstå och om detta kan påverka företagets kapitalnivå.

Bankföreningen och FHF anser att operativa risker inte ska sammanblandas med affärsbeslut (företagets kapitalbehov) och att texten bör ändras till "analys av om företagets risknivåer kan öka eller om nya risker kan uppstå".

15 §

Av förslaget framgår att när ett företag beslutar om en ny produkt, tjänst, process eller it-system ska det fastställa vilken funktion eller organisatorisk enhet som ska ansvara för att hantera risker förenade med dessa.

Bankföreningen och FHF anser att bestämmelsen bör ändras enligt följande, vilket också diskuterades vid FIs informationsmöte 10 december 2013, "När ett företag beslutar om en ny produkt, tjänst, process eller it-system ska det fastställa vilken funktion som ska ha huvudansvar för denna."

16 § punkt 1

I förslaget anges att "de metoder och rutiner som företaget ska följa för att ha en väl fungerande kontinuitetshantering. Metoderna och rutinerna ska omfatta beredskapsplaner, kontinuitetsplaner och återställningsplaner".

Bankföreningen och FHF föreslår att texten ändras till "de metoder och rutiner som företaget ska följa för att ha en väl fungerande kontinuitetshantering. Metoderna och rutinerna ska omfatta plan för beredskap, kontinuitet och återställning".
Vi anser att detta är en bättre formulering eftersom företag använder olika namn på planerna i enlighet med anförandet i 1 kap definitioner.

Allmänna råd (under 16, 19 och 20 §§)

Som vi inledningsvis nämnt anser vi att de allmänna råden bör placeras i remisspromemorian.

17 §

I förslaget anges att "ett företag ska för varje process enligt 5 kap 1 § fastställa den längst tillåtna tiden för avbrott".

Bankföreningen och FHF föreslår att paragrafen stryks alternativt att meningen ändras till att "ett företag ska för väsentliga processer enligt 5 kap 1 § fastställa acceptabla tider för avbrott". Den föreslagna språkliga förändringen återspeglar bättre det språkbruk som används i branschpraxis.

20 §

Bankföreningen och FHF anser att denna bestämmelse bör flyttas till föreskriften om it-system, informationssäkerhet och insättningssystem eftersom den bättre passar in i det sammanhanget.

22 §

Av förslaget framgår att ett företag ska regelbundet utbilda och informera relevant personal om hur beredskapsplaner, kontinuitetsplaner och återställningsplaner används.

Bankföreningen och FHF anser att bestämmelsen bör ändras så att det framgår att ett företag regelbundet ska utbilda och informera sin personal om var och hur plan för beredskap, kontinuitet och återställning återfinns respektive används. Omformuleringen är också applicerbar för 23 och 24 §§.

6 kap. Särskilda krav på hantering av operativa risker inom värdepappersrörelse och valutahandel

Bankföreningen och FHF uppfattar att CEBS "Guidelines on the management of operational risks in market related activities", som enligt remisspromemorian 6 kap. i första hand är baserat på, främst avser handel med finansiella instrument för egen räkning (2 kap. 1 § 3 punkten lagen om värdepappersmarknaden) samt endast i vissa begränsade delar utförande av order avseende finansiella instrument på kunders uppdrag (2 kap. 1 § 2 punkten lagen om värdepappersmarknaden) och då i förhållande till marknadsmotparter mot vilka kunders uppdrag utförs. Däremot uppfattar vi inte att CEBS vägledning omfattar mottagande och vidarebefordran av order (2 kap. 1 § 1 punkten lagen om värdepappersmarknaden) och ej heller diskretionär portföljförvaltning avseende finansiella instrument (2 kap. 1 § 4 punkten lagen om värdepappersmarknaden). Bankföreningen och FHF anser således att 6 kap. 1 § bör ändras till att, vad gäller värdepappersrörelsen, endast omfatta verksamhet som bedrivs enligt 2 kap. 1 § 2-3 lagen om värdepappersmarknaden.

Vidare behövs vissa språkliga justeringar för att anpassa bestämmelserna till den form av handel och värdepappersrörelse som är gängse i Sverige, i stället för den anglosachsiska modell som förefaller vara utgångspunkten i CEBS vägledning. Detta gäller särskilt förtydligande av om reglerna gäller för trading boken/egen handel samt att det med motpart avses marknadsmotpart och inte kunder.

Ytterligare en generell kommentar avser hänvisningen till riskkontroll. Vanligen reserveras denna term för riskkontroll inom den andra linjen, medan termen här används för den riskbevakning som förekommer inom första linjen och således är en del av stödfunktionerna. Därför föreslås att alla referenser till riskkontroll tas bort.

3 § Personal

Av förslaget framgår att ett företag ska se till att personal som initierar och genomför affärstransaktioner, under minst tio arbetsdagar i följd under en tolvmånadersperiod, inte har möjlighet att 1) initiera och genomföra transaktioner 2) godkänna eller bekräfta transaktioner, eller 3) hantera betalningar kopplade till sådana transaktioner. Detta gäller även för personal på funktionen för riskkontroll och de stödfunktioner som följer upp eller på något sätt hanterar transaktioner.

Bankföreningens och FHF uppfattar att den använda terminologin motsvarar den som används i CEBS vägledning där personal som initierar och genomför affärstransaktioner refererar till "traders". Genom att använda denna begränsning undviks den sammanblandning mellan första och andra försvarslinjen som nu skett i bestämmelsen.

Vi föreslår därför att bestämmelsen ändras enligt följande. "Ett företag ska se till att personal som initierar och genomför affärstransaktioner, under minst tioarbetsdagar i följd under en tolvmånadersperiod, inte initierar eller genomför transaktioner".

Vidare bör punkterna 2, 3 och stycke två, där hänvisning görs till personal på funktionerna för riskkontroll och stödfunktioner, strykas. Eftersom personer inom funktionerna för riskkontroll och stödfunktioner varken genomför eller initierar transaktioner saknar bestämmelserna relevans. Dessa funktioners behörighet till system hanteras inom ramen för systembehörigheten som regleras i 11 § samma kapitel.

4 § Transaktionshantering

Av förslaget punkten 3 framgår att ett företag ska se till att dels skriftligt komma överens med en motpart vid transaktioner där motparten önskar villkor som avviker från företagets normala rutiner, dels se till att villkoren bekräftas av motparten.

Bankföreningen och FHF noterar att det är oklart vad FI avser med denna regel eftersom skriftliga krav vanligen kräver stöd i svensk lag. Vi anser att det måsta vara tillfyllest att informationen dokumenteras. Ett generellt skriftlighetskrav i denna del av marknaden där en stor del av dokumentationen sker genom bandupptagning är inte påkallat. I detta sammanhang bör en jämförelse ske med kravet i punkten 31 i CEBS vägledning där det inte finns ett skriftlighetskrav, men väl ett krav på dokumentation. Vi anser också att det framstår som onödigt att först skriftligen komma överens med motparten och därefter dessutom kräva att motparten bekräftar villkoren.

Av förslaget punkten 6 framgår att ett företag ska se till att informera funktionen för riskkontroll eller lämplig stödfunktion om transaktioner som har gett upphov till missförstånd som företaget och motparten inte kan lösa omgående.

Bankföreningen och FHF anser med referens till den inledande kommentaren, att rapportering ska ske till stödfunktionerna. Först därefter sker, om förutsättningar föreligger enligt de interna riktlinjerna, rapportering till andra linjens riskontroll. Denna punkt bör rent logiskt byta plats med punkt 7.

Av förslaget punkten 7 framgår att ett företag ska se till att bekräftelser på transaktioner så snart som möjligt utväxlas mellan motpartens och företagets funktion för riskkontroll eller lämplig stödfunktion.

Bankföreningen och FHF utgår från att denna punkt avser bekräftelse till marknadsmotpart, medan kravet på bekräftelse till kunder framgår av FFFS 2007:16, 17 kap. Vid utformning av texten bör även hänsyn tas till att bekräftelserna ofta sker i datasystem såsom i VP-systemet och att det i dessa fall inte finns några pappersbekräftelser, det ske inte heller någon fysisk "utväxling" av bekräftelser. I marknaden refereras oftast till denna verksamhet som matchning. Slutligen är aldrig andra linjens riskontroll involverad i bekräftelser och utväxling av dessa, varför dessa bör strykas. Denna punkt bör rent logiskt byta plats med punkt 6.

Av förslaget punkterna 8 och 9 framgår att företaget ska se till att det dels finns fastställda rutiner för att hantera och rapportera obekräftade affärer, dels följa upp dessa samt dagligen stämma av transaktioner, likvider och positioner för samtliga konton och portföljer och händelser kopplade till dessa.

Bankföreningen och FHF uppfattar att båda dessa punkter avser handelslager och andra egna lager, varför punkterna kan läggas samman i en (1) punkt. Det bör tydliggöras att med motpart avses marknadsmotpart. För närvarande förekommer bekräftelser i stor omfattning i elektroniska system som t ex VP-systemet varvid termen matchning är mer vanligt förekommande. Rent språkligt anser vi att termen hantera inkluderar rapportera vilket är anledningen till att "och rapportera" kan raderas. Slutligen bör "händelser" i punkten 9 strykas eftersom dessa rimligen inte kan stämmas av.

6 § Hantering av säkerheter

Av förslaget framgår att ett företag ska ha it-system som under pågående handel löpande kan sammanställa information om hur företaget utnyttjar motpartslimiter.

Bankföreningen och FHF anser att paragrafen bör strykas. Oavsett var en sådan funktionalitet placeras så bedömer vi inte att detta begränsar riskerna. Med hänsyn till den administrativa börda detta krav innebär för att få ett sådant system på plats måste kostnadsaspekten analyseras mer utförligt. Vi ansluter oss i denna del till Regelrådets bedömning att de administrativa kostnaderna är ofullständigt beskrivna.

Vidare bör påpekas att utbyte av säkerheter hanteras utifrån föregående dags stängningskurser och är en process som är skiljd från processen övervakning av limiter, dvs. det är olika funktioner som utför, ansvarar och kontrollerar arbetet. Kraven i 6 kap. 9 och 10 §§ täcker in även detta område.

7 § övervakning

I förslaget anges att "Ett företag ska vid väsentliga avvikelser eller orimliga resultat vid handel analysera om dessa är orsakade av misstag, oegentligheter eller andra händelser i verksamheten".

Bankföreningen och FHF anser att det räcker att skriva att "Ett företag ska vid handel analysera väsentliga avvikelser eller orimliga resultat". Resultatet av en sådan analys kan visa att händelsen var orsakad av misstag, en oegentlighet eller av en annan händelse.

11 §
Av förslaget framgår att ett företag ska minst en gång i kvartalet kontrollera att behörigheter till de it-system som används i verksamheten är begränsade till respektive användares arbetsuppgifter.

Bankföreningen och FHF anser inte att det är rimligt att kontroller ska ske varje kvartal. Frekvensen bör anpassas till den verksamhet som kontrolleras. Överdrivet täta kontroller riskerar att ta resurser från andra riskmildrande åtgärder, och kan riskera att utmynna i en "ticking the box"-aktivitet i stället för en kontroll med hög kvalitet. Vi anser att det är mer lämpligt att uppställa ett krav om kontroll minst två gånger per år.

Förslagets konsekvenser och regleringsalternativ

Bankföreningen och FHF kan inledningsvis notera att det i remisspromemorian konstateras att det redan i dag finns riktlinjer från EBA och rekommendationer från CEBS avseende hantering av operativa risker. Någon närmare analys av hur företagen anpassat sig till dessa regelverk görs inte i promemorian. Det saknas också en närmare analys av vilka brister FI faktiskt avser att komma åt med den förslagna bindande regleringen. FI konstaterar endast att eftersom hanteringen av operativa risker kostar pengar finns det en uppenbar risk för att företagen inte ger området tillräckligt med uppmärksamhet och att operativa risker kan medföra betydande kostnader för företag, konsumenter och samhället. Samtidigt konstaterar FI att flertal företag sannolikt redan gjort en del av det arbete som föreskriften kommer att innebära. Vi anser mot denna bakgrund att konsekvensutredningen i denna del inte kan anses uppfylla kraven i förordningen om konsekvenser i regelgivningen på att beskrivningen ska innehålla vilka alternativa lösningar som finns för det man vill uppnå och vilka effekterna blir om någon reglering inte kommer till stånd.

När det gäller FIs bedömning av de kostnader som förslaget kan medföra för företagen anser vi att det finns flera brister i de antaganden eller uppskattningar FI gör. Initialt bör noteras att vissa av kraven i förslaget innebär att företagen måste göra en kartläggning av samtliga sina befintliga processer, rutiner och system vilket inte alls har beaktats i utredningen. En sådan genomgång kräver resurser både i form av tid och personal. Till detta kommer de resurser som krävs för att uppdatera/utveckla interna regler enligt förslaget vilket, enligt FI kan beräknas till 50 000 kr per företag och regel och sammanlagt 103 mnkr för branschen. Denna

siffra kan vara riktig om man avgränsar den till att endast omfatta nedtecknandet av de befintliga regler som organisationen redan har analyserat och arbetat fram. Om man däremot även ska beakta de resurser som krävs för att analysera i vilken mån befintliga regler behöver uppdateras och på vilka områden nya interna regler behöver utvecklas menar vi att siffran är betydligt underskattad. I detta sammanhang måste även beaktas de resurser som krävs för förändringsledning samt utbildning av och information till personalen om de nya interna reglema. Den förväntade implementeringskostnaden av de nya reglerna inom respektive organisation och den fortlöpande övervakning och utbildning som krävs enligt förslaget överstiger vida den tidsåtgång och de kostnadsberäkningar FI gjort. Även för ett mindre företag måste man utgå från att ett sådant arbete kräver mer resurser än en person under en vecka per regel. Tidsaspekten måste också beaktas i fråga om möjligheten för företagen att på kort tid implementera kraven i förslaget. Vi vill därför åter påpeka vikten av att det införs en rimlig tid för företagen att implementera kraven.

Utöver ett behov av att se över och vidareutveckla interna regler så återstår behovet att se över, ändra och i många fall utöka nya rutiner, processer och styrdokument vilket FI också lyfter fram. Vi delar inte FIs uppfattning att investeringar i it-system sannolikt till stora delar är av engångskaraktär. Även om investeringspuckeln är högst inledningsvis så medför ett it-system, utöver personalkostnaden, alltid återkommande licens-, drifts- och utvecklingskostnader. Kostnadsmassan i en bank består förenklat av personal-, lokal- och IT-kostnader och att skapa interna regler och styrdokument påverkar främst personalkostnadssidan (65 mdkr för de fyra svenska storbankerna 2012) medan förändringar av rutiner och processer driver både personal- och it-kostnader. Eftersom banker är it-kostnadsintensiva (6,9 mdkr för de fyra svenska storbankerna 2012) med ett stort antal applikationer, en hög komplexitet och många skräddarsydda lösningar, så innebär en ökning av personalkostnaderna nästan alltid också en ökning it-kostnaderna.

Precis som FI påpekar så behöver företagen för att fatta ett investeringsbeslut som automatiserar en lösning ett informerat beslutsunderlag. Underlaget bör identifiera vad som är på plats, vad de tillkommande kraven består av, identifiera och prioritera initiativ och slutligen bedöma alternativkostnaden av att inte automatisera. Även om det är så att det inte införs ett särskilt krav på automatiserade lösningar kan det, mot bakgrund av kraven i förslaget, ifrågasättas om inte företagen kommer att bli tvungna att automatisera sin hantering för att kunna driva sin verksamhet i enlighet med de uppställda kraven. Den initiala kostnaden för att införa en sådan automatisering skulle, med tillämpning av FIs antaganden, uppgå till 12 950 000 – 129 500 000 kr för företagen (259 företag i förhållande till 50 000 – 500 000 kr) vilket vi bedömer är i underkant.

Sammantaget anser vi att såväl konsekvensanalysen av som analysen av regleringsalternativ inte uppfyller kraven i förordningen om konsekvenser i regelgivningen. I detta sammanhang vill vi också hänvisa till Regelrådets remissvar.

SVENSKA BANKFÖRENINGEN

Thomas Östros

Peter Göransson

SVENSKA FONDHANDLAREFÖRENINGEN

Kerstin Hermansson